Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Řešení výpadků kritických síťových prvků

Libuše Moravcová

Bakalářská práce
2014

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Libuše Moravcová**
Osobní číslo:	**I10142**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Řešení výpadků kritických síťových prvků**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je vytvořit konfiguraci kritických přepínačů a směrovačů tak, aby při výpadku hlavního prvku přešel provoz plynule na prvek záložní. Student v teoretické části rozebere problematiku protokolu STP, jeho nastavení a parametrů. V praktické části student sestaví v laboratorních podmínkách UPCE FEI vzorovou topologii na které otestuje chování vypracované konfigurace a provede její otestování, měření a vyhodnocení získaných dat.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.
EMPSON, Scott. CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 336 s. ISBN 978-80-251-2286-0.
HUCABY, Dave. CCNP SWITCH 642-813 official certification guide: autorizovaný výukový průvodce. Vyd. 1. Indianapolis: Cisco Press, c2010, xxvii, 459 s. ISBN 978-1-58720-243-8.

Vedoucí bakalářské práce: **Ing. Ondřej Mařík**
Katedra softwarových technologií

Datum zadání bakalářské práce: **20. prosince 2013**
Termín odevzdání bakalářské práce: **9. května 2014**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2014

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 9. 5. 2014 Libuše Moravcová

Poděkování

Na tomto místě bych ráda poděkovala svému vedoucímu práce Ing. Ondřeji Maříkovi za trpělivost a cenné rady. Také své rodině a přátelům, kteří mě v průběhu studia podporovali.

Anotace a klíčová slova

ANOTACE

Bakalářská práce pojednává o výpadku kritických síťových prvků a jejich následném řešení záložními cestami. Porovnává různé protokoly, které lze na tuto problematiku nasadit, shrnuje jejich výhody a nevýhody.

KLÍČOVÁ SLOVA

STP, RSTP, HSRP, počítačové sítě, přepínač, směrovač, protokol, časovač, řešení, model, příkazový řádek

TITLE

Deal with shortfalls of critical network elements.

ANNOTATION

This bachelor work describes the failure of critical network elements and their subsequent solution. Compare different protocols that can be deployed on this issue, summarizes their advantages and disadvantages.

KEYWORDS

STP, RSTP, HSRP, computer networks, switch, router, protocol, timer, solution, model, command prompt

OBSAH

SEZNAM ZKRATEK

TCP/IP	Transmission Control Protocol/Internet Protocol
ISO/OSI	International Standards Organization / Open Systen Interconnection
VLSM	Variable Length Subnet Masking
OSPF	Open Shortest Path First
IGRP	Interior Gateway Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
ARP	Adress Resolution Protocol
RARP	Reverse Adress Resolution Protocol
STP	Spanning Tree Protocol
BPDU	Bridge Protocol Data Units
MAC	Media Access Control
CST	Common Spanning Tree
PVST	Per-VLAN Spanning Tree
PVST+	Per-VLAN Spanning Tree Plus
HSRP	Hot Standby Router Protocol
UDP	User Datagram Protocol
vMAC	virtual MAC
vIP	virtual IP
OS	Operating System
MTU	Maximum Transmission Unit
RTT	Round-trip Time
IS	Internet Suite

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1 ÚVOD

V dnešní době není Internet centralizovaný systém počítačových sítí, a proto v něm neexistuje jednotná správa. Nejen tento fakt je důvodem k nekonzistenci směrování dat v Internetu. V dosavadním průběhu rozvoje Internetu vznikaly různé protokoly, definující směrování dat na základě různých algoritmů a stále jsou postupně vylepšovány.

Výpadek jakéhokoli aktivního prvku nebo kabelu ve velké síti by mohl mít neblahé následky pro celou síť. Mnoho firem, organizací, vzdělávacích zařízení atd. se v dnešní době bez Internetu neobejde. Proto je příhodné mít na paměti na počátku tvorby počítačové sítě v dané organizaci, kromě efektivní, rychlé komunikace a zálohování, také tvorbu záložních řešení. Na tuto problematiku lze nasadit celou řadu konkrétních protokolů. V této práci však byly vybrány a představeny protokoly níže zmiňované.

Cílem bakalářské práce je vysvětlení principů protokolů EIGRP, STP, RSTP a HSRP a zobrazení jejich vzájemné spolupráce. Tato práce čerpá ze znalostí a problematiky směrování dat na úrovni kurzů CCNA Exploration 1-4 společnosti Cisco, případně kurz CCNP 642-813 SWITCH [6] nebo studium zdrojů [4], [14].

První kapitola práce je věnována úvodu do problematiky, kterou je třeba znát před samotným řešením praktické části. Informacím o modelu TCP/IP a referenčnímu modelu ISO/OSI. Popisu VLSM, díky kterému je možné efektivněji využívat rozsahu adresního prostoru. Úvodu do protokolů OSPF, IGRP a EIGRP a následnému výběru protokolu EIGRP pro praktické představení.

Druhá kapitola popisuje první ze stěžejních protokolů použitých v praktické části, protokol STP. Vysvětluje jeho funkčnost, použitelnost a představuje typy STP. Třetí kapitola se zabývá druhým protokolem využitým v této práci - RSTP protokolem. Vysvětluje princip činnosti protokolu, konfiguraci a jeho s rovnání s protokolem STP. Ve čtvrté kapitole jsou popsány principy a činnost HSRP protokolu nasazeného v praktické části na směrovače, který v případě výpadku zajistí záložní cestu přes směrovač nastavený jako záložní.

Poslední kapitola práce představuje praktické nasazení protokolů v rámci případové studie datacentra. Znázorňuje na zadané topologii, jakým způsobem budou nahrazeny výpadky směrovačů a přepínačů a jaké záložní cesty budou použity. Kompletní konfigurace směrovačů použitá v případové studii je přiložena v přílohách.

Veškeré uvedené příkazy a konfigurace uvedené v bakalářské práci jsou použitelné v operačním systému Cisco IOS (Internetwork Operating System).

2 ÚVOD DO TCP/IP

Od roku 1982, kdy byl vynalezen protokol TCP/IP podle [4], je heterogenita sítí dále rozšířena o nasazení Ethernetu, Token Ringu, Fiber Distributed Data Interface (FDDI), X.25, Frame Relay, Switched Multimegabit Data Service (SMD), Integrated Services Digital Network (ISDN) a nejnověji Asynchronous Transfer Mode (ATM).

Internet Protocol suite zahrnuje nejen požadavky na nižších úrovních, jako je Transmission Control Protocol (TCP) a Internet Protocol (IP), ale specifikuje i běžné aplikace jako elektronickou poštu, emulaci terminálu a přenos souborů. Obrázek 1 ukazuje protokoly TCP/IP - ve vztahu k referenčnímu modelu OSI. Obrázek 2 ukazuje některé z důležitých internetových protokolů a také jejich vztah k OSI referenčního modelu.

2.1 Technologie TCP/IP

2.1.1 **TCP**

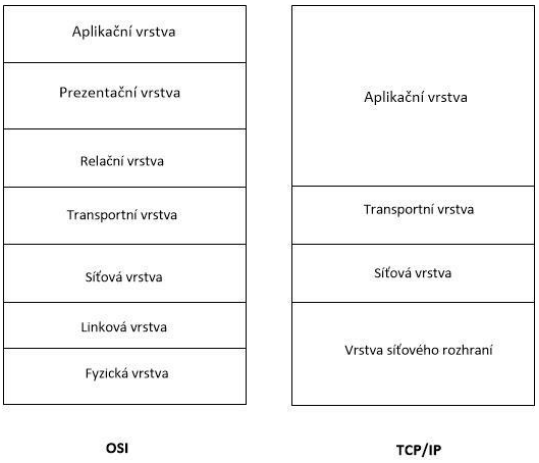
TCP je spojově orientovaný protokol pro přenos toku bajtů na transportní vrstvě se spolehlivým doručováním. V současnosti je zdokumentován v IETF RFC 793 [7].

V sadě protokolů Internetu, jak je uvedeno v [8], je TCP prostřední vrstvou mezi IP protokolem pod ním a aplikací nad ním. Aplikace ke vzájemné komunikaci využívají spolehlivé spojení na způsob roury, zatímco IP protokol neposkytuje takové streamy, ale jen nespolehlivý přenos. TCP využívá služby IP protokolu opakovaným odesíláním nespolehlivých paketů, při ztrátě paketu zajišťuje spolehlivost a seřazováním přijatých paketů zajišťuje správné pořadí. Tím TCP plní úlohu transportní vrstvy ve zjednodušeném modelu ISO/OSI.

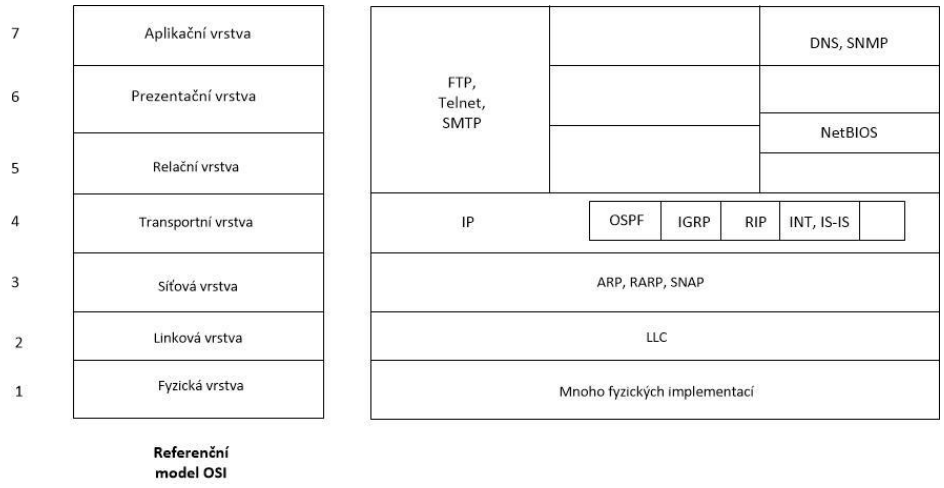
Aplikace posílá proud (stream) bajtů TCP protokolu, TCP rozděluje proud bajtů do přiměřeně velkých segmentů. Velikost segmentů je určena parametrem MTU (maximum transmission unit) linkové vrstvy sítě, ke které je počítač připojen. TCP pak předá takto vzniklé pakety IP protokolu k přepravě internetem. TCP ověří, že se pakety neztratily tím, že každému paketu přidělí pořadové číslo, které se také použije k ověření, že data byla přijata ve správném pořadí.

TCP modul na straně příjemce posílá zpět potvrzení pro pakety, které byly úspěšně přijaty. Pokud by se odesílateli potvrzení nevrátilo do rozumné doby (round-trip time, RTT), vypršel by odesílatelův časovač a (pravděpodobně ztracená) data by vyslal znovu.

TCP protokol ověřuje, zda přenesená data nebyla poškozena šumem tím, že před odesláním spočte kontrolní součet, uloží jej do odesílaného paketu a příjemce kontrolní součet vypočte znovu a ověří, že se shodují.



Obrázek 1 - TCP/IP Protocol suite ve vztahu k OSI Referenčnímu modelu



Obrázek 2 - Internetové protokoly ve vztahu k OSI refer. modelu

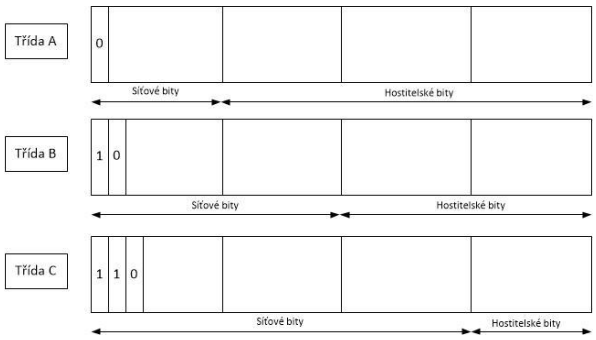
2.1.2 **IP**

IP je primární protokol vrstvy tři v IS. Kromě směrování IP umožňuje zasílání chybových zpráv, fragmentaci a opětovné složení informačních jednotek nazývaných datagramy, pro přenos v sítích s různou maximální velikostí datové jednotky. IP představuje srdce Internet Protocol Suite.

Základem pro komunikaci protokolu IP jsou IP adresy. Jedná se o unikátní 32 bitová čísla přiřazovaná každému síťovému zařízení. Unikátnost IP adresy umožňuje propojování sítí a vyhledávání nejvhodnějších cest po celém světě.

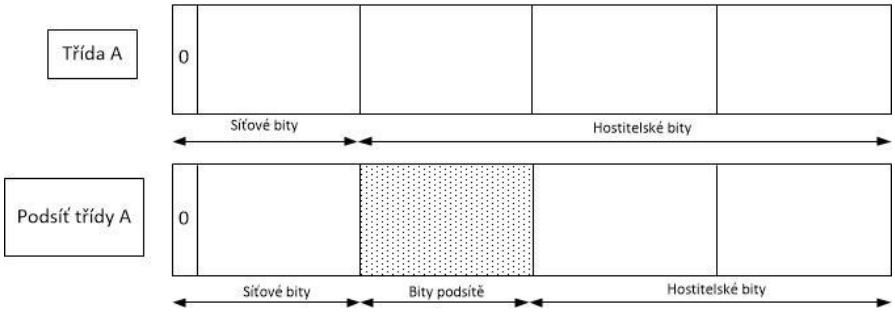
IP adresa je rozdělena do dvou částí. První část určuje adresu sítě, zatímco druhá část určuje adresu hostitele.

Adresní prostor IP je rozdělen do tříd sítí. Sítě třídy A jsou určeny především pro použití na několik velmi velkých sítí, protože poskytují pouze 8 bitů pro pole síťové adresy. Sítě třídy B přidělují 16 bitů a sítě třídy C přidělují 24 bitů. Třída C poskytuje pouze 8 bitů pro hostitelské oblasti, nicméně počet počítačů na síti může být limitujícím faktorem. Ve všech třech případech, bit(y) nejvíce vlevo označují třídu sítě. IP adresy jsou psány v tečkovém desítkovém formátu; například 34.0.0.1. Obrázek 3 znázorňuje formáty adres pro třídy A, B, C a IP sítí.



Obrázek 3 - Adresní formát pro Třídu A, B a C IP sítí

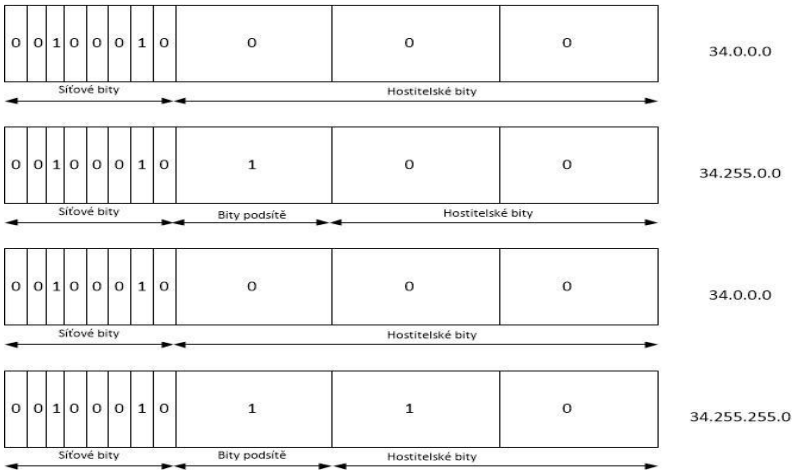
IP sítě mohou být také rozděleny do menších jednotek nazývaných podsítě. Podsítě poskytují speciální flexibilitu pro správce sítě. Například, síti byla přiřazena adresa třídy A a všechny uzly v síti používají adresu třídy A. Tečková desítková reprezentace adresy této sítě je 34.0.0.0. (všechny nuly v hostitelské oblasti specifikují adresu sítě). Správce může rozdělit síť pomocí podsítí. To se provádí pomocí "půjčování" bitů z hostitelské části adresy a jejich použití jako podsítě pole, jak je znázorněno na Obrázku. 4.



Obrázek 4 - "Půjčené" bity

Pokud se správce sítě rozhodne použít 8 bitů podsítě, druhý oktet IP adresy třídy určuje číslo podsítě. V tomto případě adresa 34.1.0.0 odkazuje na síť 34, podsíť 1; adresa 34.2.0.0 odkazuje na síť 34, podsíť 2 a tak dále.

Počet bitů, které si lze půjčit na adresu podsítě, se liší. Masky podsítě používají stejný formát jako IP adresy. Maska podsítě, která určuje 8 bitů podsítě pro třídy A 34.0.0.0 je 255.255.0.0. Maska podsítě, která určuje 16 bitů podsítě pro třídu A 34.0.0.0 je 255.255.255.0. Obě tyto masky podsítě jsou znázorněny na Obrázku 5.



Obrázek 5 - Masky podsítí

Obvykle všechny podsítě stejného čísla sítě používají stejnou masku podsítě. Jinými slovy, správce sítě by si vybral osmi-bitovou masku pro všechny podsítě v síti. Tato strategie je snadná na správu, jak pro síťové administrátory, tak pro směrovací protokoly. Nicméně, tato praxe plýtvá v některých sítích adresním prostorem. Některé podsítě mají mnoho hostitelů a některé mají jen málo, ale každá z nich spotřebuje celé číslo podsítě.

2.1.3 **VLSM**

Jak podsítě IP rostly, správci hledali způsoby, jak využívat svůj adresní prostor efektivněji. Jednou z technik, která k tomu vedla, se nazývá variabilní délka masky podsítě (VLSM). S VLSM může správce sítě využít dlouhou masku na sítích s několika hostiteli a krátkou masku podsítě s velkým počtem počítačů.

2.1.4 **OSPF, IGRP, EIGRP a statické směrování**

Aby bylo možné používat VLSM, správce sítě musí používat směrovací protokol, který jej podporuje. Cisco směrovače podporují VLSM s Open Shortest Path First (OSPF), Integrated Intermediate System to Intermediate System (Integrovaný IS-IS), Enhanced Interior Gateway Routing Protocol (Rozšířený IGRP) a statické směrování.

2.1.5 **ARP a RARP**

Na některých médiích, jako je IEEE 802 LAN, jsou IP adresy dynamicky zjištěny pomocí dvou dalších členů internet suite modelu: Address Resolution Protocol (ARP) a Reverse Address Resolution Protocol (RARP). ARP využívá broadcastové vysílání zpráv ke stanovení MAC adresy odpovídající konkrétní adrese síťové vrstvy. RARP používá broadcastové zprávy ke stanovení adresy síťové vrstvy spojené s určitou hardwarovou adresou.

2.1.6 **EIGRP**

Vylepšená verze protokolu IGRP se nazývá Enhanced (rozšířený) IGRP. Rozšířený IGRP kombinuje snadnost použití tradičních směrovacích protokolů s rychlou úpravou trasy novějších link state routing protokolů.

Rozšířený IGRP spotřebuje podstatně menší šířku pásma než IGRP, protože je schopen omezit výměnu směrovacích informací tak, aby zahrnovala pouze změněné informace. Kromě toho je Enhanced IGRP schopen zvládnout AppleTalk a Novell IPX routing information stejně jako IP routing information.

Tato práce se zabývá vnitřními protokoly, další takové protokoly jsou uvedeny dále v [4] stejně tak jako i vnější protokoly, například Exterior Gateway Protocol (EGP) a Border Routing Protocol (BGP), jimiž se tato práce přímo nezabývá.

3 SPANNING TREE PROTOCOL

3.1 IEEE 802.1D (STP)

Robustní síťový návrh zahrnuje nejen efektivní přenos paketů nebo rámců, jak se píše v [5], ale také uvažuje, jak se rychle zotavit z poruch v síti. Na třetí vrstvě se směrovací protokoly používají ke sledování redundantních cest do cílové sítě. Po selhání primární cesty se přepne na cestu sekundární. Vrstva tři udržuje mnoho aktivních cest k cíli pomocí sdílení zátěže mezi tyto cesty.

Ve vrstvě dvě však nejsou použity žádné směrovací protokoly a aktivní redundantní cesty nejsou ani povoleny ani žádoucí. Místo toho poskytují přenos dat mezi sítěmi nebo porty přepínače. Spanning Tree Protocol (STP) umožňuje přenos dat mezi sítí či porty přepínače. Spanning Tree Protocol umožňuje síťové propojení redundance, takže se ze selhání může vrstva dvě zotavit včas a bez zásahu. STP je definován v normě IEEE 802.1D uvedené v [11].

3.2 Komunikace Spanning Tree: BPDU (Bridge Protocol Data Units)

STP pracuje stejně, jako mezi sebou komunikují přepínače. Datové zprávy jsou vyměňovány ve formě *Bridge Protocol Data Units (BPDU).* Přepínač pošle BPDU rámec na port použitím unikátní MAC adresy portu samotného jako zdrojové adresy. Přepínač neví o ostatních přepínačích kolem sebe, takže BPDU rámce jsou odesílány s cílovou adresou dobře známé adresy vícesměrového vysílání STP 01-80-c2-00-00-00.

Jsou definovány dva typy BPDU zpráv:

- Konfigurační BPDU zprávy, používané pro spanning-tree výpočet
- Topology Change Notification *(*TCN*)* BPDU zprávy, používané pro oznámení změn v topologii sítě

Tabulka 1- Obsah konfigurační BPDU zprávy

Popis	Počet bajtů
ID protokolu (vždy 0)	2
Verze (vždy 0)	1
Typ zprávy (konfigurace nebo TCN BPDU)	1
Vlajky	1
Root Bridge ID	8
Cena cesty Root Bridge	4
Bridge ID odesílatele	8
ID portu	2
Stáří zprávy	2
Max age	2
Hello interval	2
Forward delay	2

Význam polí BPDU zprávy podle [9]:

- **ID protokolu** - označuje typ použitého protokolu a obsahuje hodnotu nula
- **Verze** - označuje verzi protokolu a obsahuje hodnotu nula
- **Typ zprávy** - označuje typ zprávy a obsahuje hodnotu nula
- **Vlajky** - zahrnuje následující: BIT ZMĚNY TOPOLOGIE (TC - TOPOLOGY CHANCE), který signalizuje změnu topologie v případě, že cesta k root bridgi byla narušena. BIT POTVRZENÍ ZMĚNY TOPOLOGIE (TCA - TOPOLOGY CHANCE ACKNOWLEDGEMENT), který je nastaven na potvrzení o přijetí konfigurační zprávy s TC bitem.
- **Root Bridge ID** - označuje prioritu root bridge, ta má 2 bajty a ID MAC adresy, která má 6 bajtů.
- **Cena cesty root bridge** - označuje cenu cesty z bridge posíláním konfigurační zprávy k root bridgi. Toto pole je aktualizováné přepínačemi na cestě k root bridgi.
- **Bridge ID odesílatele** - označuje prioritu a ID MAC adresy bridge posíláním zpráv. To dovoluje BPDU identifikovat odkud zpráva pochází tak dobře, jako identifikovat více cest.
- **ID portu** - označuje číslo portu, ze kterého byla zpráva odeslána. Toto pole umožňuje smyčky způsobené více spojenými bridgi, které mají být odhaleny a opraveny.
- **Stáří zprávy** - označuje dobu, která uplynula od té doby, co root bridge poslal konfigurační zprávu, na které je založená aktuální zpráva.
- **Max age** - označuje, kdy bude stávající konfigurační zpráva vymazána. Když stáří zprávy dosáhne maxima, přepínači vyprší aktuální konfigurace a proběhne nová volba k určení root bridge. Výchozí hodnota je 20 vteřin ale může se změnit na hodnotu mezi 6 a 40 vteřinami.
- **Hello interval** - označuje dobu mezi konfiguračnimi zprávami root bridge. Výchozí hodnota je 2 vteřiny ale může se změnit na hodnotu mezi 1 a 10 vteřinami.
- **Forward delay** - označuje čas, po který by měly bridge čekat, než se po změně topologie přejde do nového stavu. Výchozí hodnota je 15 vteřin ale může se změnit na hodnotu mezi 4 a 30 vteřinami.

Výměna BPDU zpráv probíhá směrem k cíli volbou referenčním bodů, což je základ pro stabilní spanning-tree topologii. Smyčky mohou být také identifikovány a vymazány umístěním specifických redundantních portů v blokačním nebo pohotovostním stavu.

Několik klíčových polí v BPDU zprávě se vztahuje k překlenutí (nebo přepnutí) identifikace, ceny cesty a hodnoty časovače. Všechny pracují společně tak, že síť přepínačů může konvergovat na společné spanning-tree topologii a vybrat stejné referenční body v rámci sítě. Tyto referenční body jsou definovány v sekci, která následuje.

Ve výchozím nastavení, jsou BPDU zprávy rozeslány všem portům přepínače každé dvě vteřiny, takže aktuální informace o topologii se vyměňují a tím jsou smyčky rychle identifikovány.

3.3 Volba Root Bridge

Pro všechny přepínače v síti na loop-free topologii musí existovat společný referenční rámec sloužící jako vodítko. Tento referenční bod je nazýván *Root Bridge.* (Termín *bridge* je používán i v přepínaném prostředí, protože STP byl vyvinut pro použití na bridgích. Proto, když bude zmiňován *bridge*, myslí se tím *přepínač).*

Každý přepínač má unikátní *Bridge ID,* které ho identifikuje před ostatními přepínači. Bridge ID je 8 bajtová hodnota skládající se z následujících polí:

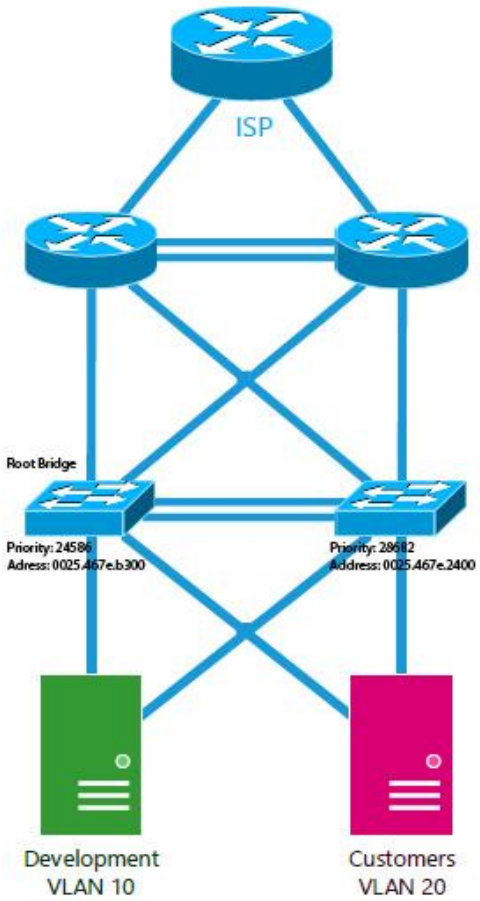
- **Bridge Priority** (2 bajty) – priorita nebo váha přepínače ve vztahu ke všem ostatním přepínačům. Pole priority může mít hodnotu od 0 do 65 535 a výchozí do 32 768 (nebo 0x8000) na každém Catalyst přepínači.
- **MAC adresa** (9 bajtů) - MAC adresa používaná přepínačem může být od supervizora modulu, sběrnice nebo to může být 1024 adres, které jsou přiřazeny ke každému supervizorovi nebo sběrnici v závislosti na modelu přepínače. V každém případě je tato adresa pevná, unikátní a uživatel ji nemůže měnit.

Další podrobnější informace o supervisorech modulů nebo dalších protokolech řešících redundanci lze najít v [14], v kapitole 13.

Po spuštění má přepínač úzký pohled na své okolí a předpokládá, že je root bridge. (Tento stav se pravděpodobně změní, jak to ostatní přepínače zjistí a spustí volební proces). Volební proces pak probíhá následovně: Každý přepínač začne posílat vlastní bridge ID. Odesílatel bridge ID jednoduše řekne ostatním přepínačům, kdo je aktuální odesílatel BPDU zprávy. (Po rozhodnutí kdo je root bridge, jsou konfigurační BPDU zprávy zasílány pouze root bridgi. Všechny ostatní bridge musí zaslat nebo předat BPDU zprávy přidáním vlastního bridge ID odesílatele).

Přijaté BPDU zprávy jsou analyzovány, aby se zjistilo, jestli je oznámen „lepší“ root bridge. Root bridge je považován za lepší, když je hodnota root bridge ID *nižší* než porovnávaná. Pokud jsou dvě hodnoty bridge priority stejné, nižní MAC adresa rozhodne, že dané bridge ID je lepší. Když přepínač zjistí lepší root bridge, přepíše vlastní root bridge ID s root bridge ID oznámeným v BPDU zprávě. Přepínač pak musí oznámit nový root bridge ID ve vlastní BPDU zprávě.

Dříve nebo později se síť zkonverguje a všechny přepínače se shodnou na názoru, že jeden z nich je root bridge. Když se zapne nový přepínač s nižší bridge prioritou, začne se sám označovat jako root bridge. Protože nový přepínač má skutečně nižší bridge ID, všechny přepínače se brzy přehodnotí a zaznamenají si ho jako nový root bridge. Totéž se může stát, jestliže nový přepínač má bridge prioritu stejnou jako stávající root bridge, ale má nižší MAC adresu. Volba root bridge probíhá každé 2 vteřiny.



Obrázek 6 - Volba root bridge

3.4 Volba Root Portů

Po volbě referenčního bodu, který byl nominován a zvolen pro celou přepínanou síť, musí každý nerootovský přepínač přijít na to, v jakém je vztahu vzhledem k root bridgi. Tato akce může být prováděna výběrem pouze jednoho *root portu* na každý nerootovský přepínač. Root port vždy ukazuje k aktuálnímu root bridgi.

STP používá koncept ceny k určení mnoha věcí. Vybírání root portu zahrnuje hodnocení *ceny root cesty*. Tato hodnota je souhrnná cena všech odkazů vedoucích k root bridgi. Zejména odkaz přepínače má také cenu všech odkazů s tím spojenou, nazývanou *cena cesty* a pouze cenu root cesty nese uvnitř BPDU zpráva. (Tabulka 1). Jak se cena root cesty mění, mohou ostatní přepínače měnit svou hodnotu, aby byla kumulativní (souhrnná).

Ceny cesty jsou definované jako 1 bajtová hodnota s výchozí hodnotou zobrazenou v Tabulce 2. Obvykle vyšší šířka pásma odkazu znamená nižší cenu přenosu dat. Originál standard IEEE 802.1D [11] definuje cenu cesty jako 1000 Mbps rozdělenou odkazy šířky pásma v megabitech za vteřinu. Tyto hodnoty jsou zobrazeny v prostředním sloupci tabulky. Moderní sítě běžně používají Gigabit Ethernet a OC-48 ATM. V současné době IEEE používá nelineární rozsah pro cenu cesty, jak je zobrazeno v pravém sloupci tabulky.

Tabulka 2 - Cena cesty STP

Šířka pásma odkazu	Stará STP cena	Nová STP cena
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

Hodnota ceny root cesty je určena následujícím způsobem:

1. Root bridge pošle BPDU zprávu s hodnotou ceny root cesty z 0 protože jeho porty jsou připojeny přímo k root bridgi.

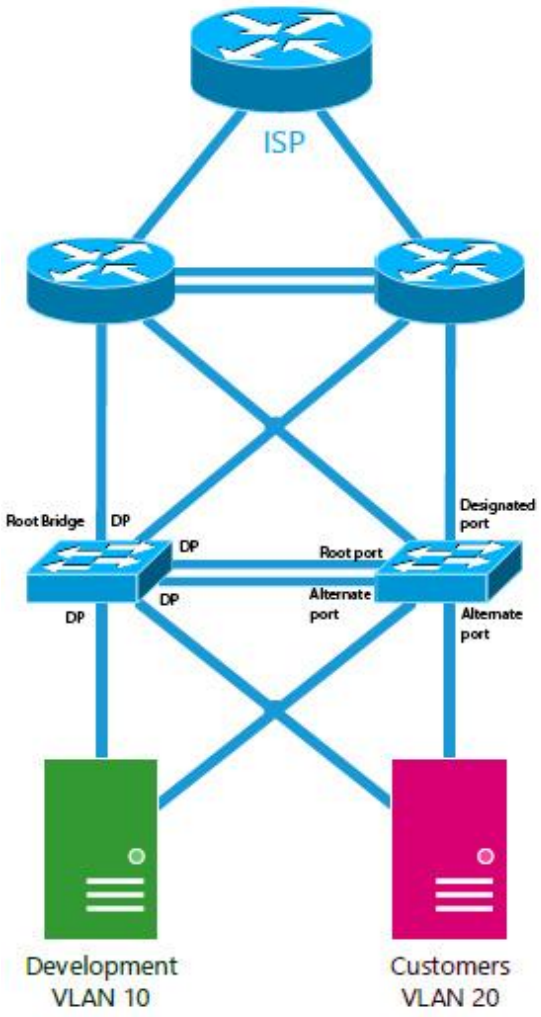
2. Když další nejbližší soused obdrží BPDU zprávu, přidá cenu cesty vlastního portu na kterém BPDU zpráva přišla. (K dokončení dojde, jakmile je BPDU zpráva přijata).

3. Soused pošle BPDU zprávu s touto novou kumulativní hodnotou jako cenu root cesty.

4. Cena root cesty je inkrementována přístupovým portem ceny cesty stejně jako je BPDU zpráva přijímána každým přepínačem.

5. Důraz je kladen na inkrementování cen root cest jako BPDU zpráv, které jsou přijímány. Při manuálním výpočtu spanning tree algoritmu, je třeba pamatovat na výpočet nové ceny root cesty jako BPDU zpráv, které *přijdou* na port přepínače.

6. Po inkrementování ceny root cesty, přepínač také zaznamená hodnotu ve vlastní paměti. Když je BPDU zpráva přijata na další port a nová cena root cesty je nižší než předchozí zaznamenaná hodnota, tato nižní hodnota se stane novou cenou root cesty. Přepínač má nyní určeno který z jeho portů má nejlepší cestu k rootovi: root portu.



Obrázek 7 - Volba Root portu

3.5 Volba designated portů

Při proces rozvíjení byl zjištěn počáteční nebo referenční bod a každý přepínač „se připojí“ k tomuto referenčnímu bodu s jednou linkou, která má nejlepší cestu. Začíná se rýsovat stromová struktura, ale linky byly identifikovány pouze v tomto bodě. Všechny linky jsou ale stále připojeny a mohou být aktivní, takže vzniká přemostění smyčky.

K odstranění možnosti přemostění smyčky, provede STP konečný výpočet, aby identifikoval jeden *designated port* na každém síťovém segmentu. Existuje předpoklad, že dva nebo více přepínačů mají porty připojené k jednomu společnému síťovému segmentu.

Pokud přepínač obdrží rámec tohoto segmentu, všechny bridge (mosty) se jej pokusí doručit do cíle. Toto chování je základem přemostění smyčky a je třeba se mu vyhnout.

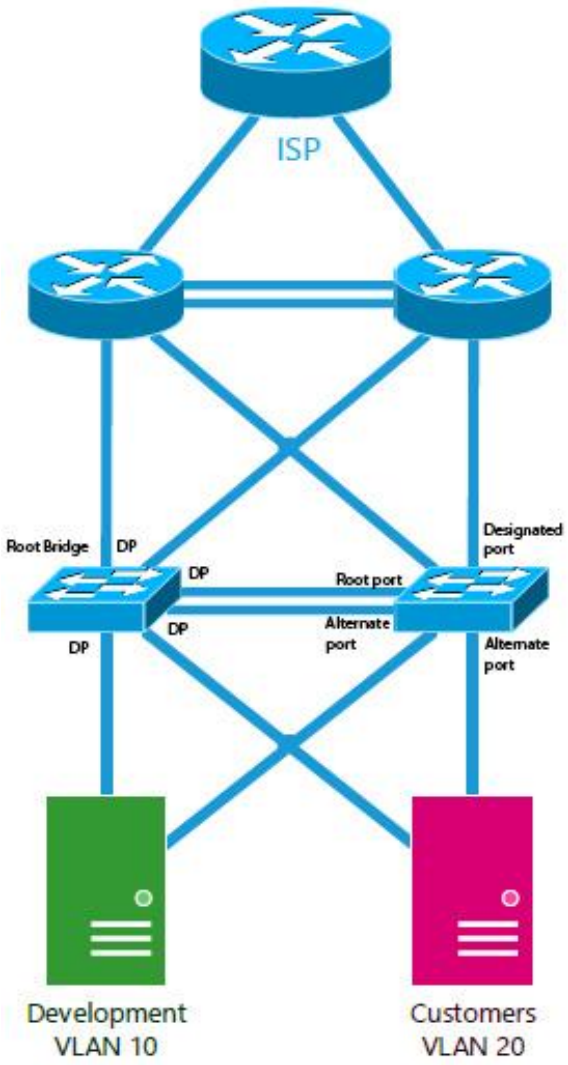
Místo toho by měl předávat provoz pouze jeden port, ten který je vybrán jako designated port. Přepínače volí designated port na základě nejnižší souhrnné ceny root cesty k root bridgi. Například, přepínač má vždy představu o své vlastní ceně root cesty, o které

oznamuje ve své vlastní BPDU zprávě. Jestliže sousední přepínač na sdíleném LAN segmentu posílá BPDU zprávu oznamující nižší cenu root cesty, soused musí mít designated port.

Přepínač se naučí pouze tu vyšší cenu root cesty od ostatních BPDU zpráv přijatých na port a pak se korektně předpokládá, že jeho vlastní přijímací port je designated port.

Všechna STP rozhodnutí jsou na základě následující sekvence čtyř podmínek:

1. Nejnižší root bridge ID
2. Nejnižší cena root cesty k root bridgi
3. Nejnižší bridge ID odesílatele
4. Nejnižší port ID odesílatele



Obrázek 8 - Výběr Designated Portů

3.6 Stavy portů STP

Ve výchozím stavu je port v režimu disabled (zakázaném) stavu, projde přes několik pasivních stavů a nakonec skončí na aktivním stavu, pokud je povoleno předávat provoz. Stavy STP portů jsou následující:

- **Disabled** – Porty, které jsou administrativně vypnuté síťovým administrátorem nebo systémem kvůli poruše jsou v disabled stavu. Tento stav je speciální a není částí normálního postupu pro port STP.

- **Blocking** – Po inicializování portů se začne v blocking stavu, takže se žádné přemostění smyčky nemůže vytvořit. V blocking stavu port nemůže přijmout nebo přenést data a nemůže přidat MAC adresy své vlastní adresní tabulce. Místo toho, má port dovoleno přijmout jen BPDU zprávy tak, že přepínač naslouchá od ostatních sousedních přepínačů. Porty, které jsou uváděny do pohotovostního režimu k odstranění přemostění smyčky, vstupují do blocking stavu.

- **Listening** – Port je přepnut z blocking do listening stavu, jestliže přepínač určí, že může být port vybrán jako root port nebo designated port.

  Port v listening stavu stále nemůže posílat nebo přijímat datové rámce. Ačkoli má dovoleno přijímat a posílat BPDU zprávy, čímž se aktivně účastní na procesu spanning tree topologie. Nakonec má port dovoleno stát se root portem nebo designated portem, protože ho přepínač může oznámit posláním BPDU zprávy ostatním přepínačům. Jestliže port ztratí svůj root port nebo designated port status, vrátí se do blocking stavu.

- **Learning** – Po uplynutí času nazývaného *forwarding delay (zpoždění)* v listening stavu, má port dovoleno přepnout se do learning stavu. Port stále posílá a přijímá BPDU zprávy jako předtím. Navíc se teď přepínač může naučit nové MAC adresy přidáním do své adresní tabulky. To dá portu čas navíc a dovolí přepínači shromáždit alespoň některé informace do adresní tabulky ačkoli port ještě nemůže poslat jakékoli datové rámce.

- **Forwarding** – Po dalším uplynutí času forward delay v learning stavu, má port dovoleno přepnout se do forwarding stavu. Port teď může posílat a odesílat BPDU zprávy a je plně funkční.

Je ovšem třeba pomatovat, že port přepínače má dovoleno přepnout se do forwarding stavu pouze, jestliže se nedetekují žádné redundantní odkazy (nebo smyčky) a pokud má nejlepší cestu k root bridgi jako root port nebo designated port.

Další nastavení portů přepínače lze najít v [14] v kapitole 4.

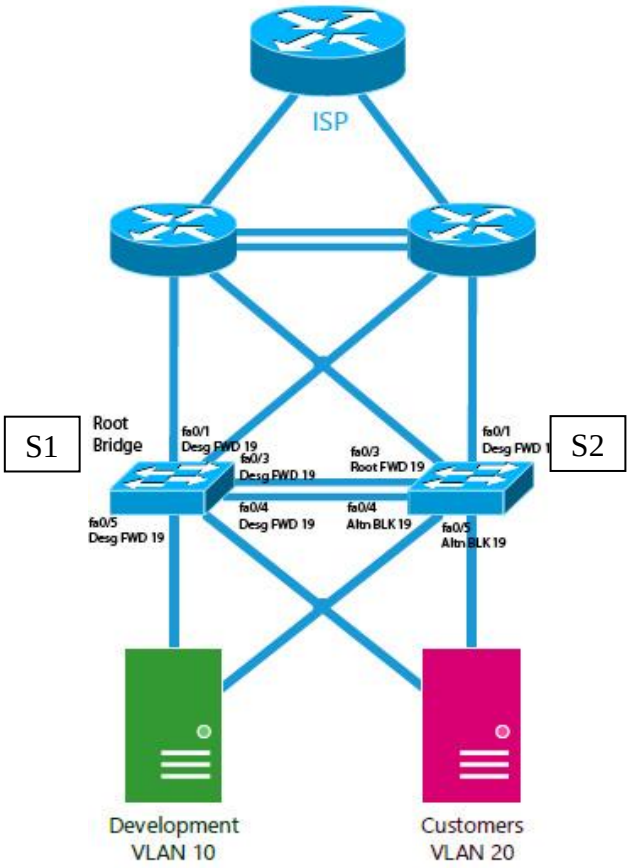
3.6.1 **Stavy STP portů**

S1 (Root Bridge) – VLAN 10

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg[1]	FWD[2]	19[3]	128.1	P2p Edge
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/4	Desg	FWD	19	128.4	P2p
Fa0/5	Desg	FWD	19	128.5	P2p

S1 (Root Bridge) – VLAN 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Desg	FWD	19	128.2	P2p Edge
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/4	Desg	FWD	19	128.4	P2p
Fa0/6	Desg	FWD	19	128.6	P2p



Obrázek 9 - STP stavy portů

[1] Role portu designated
[2] Stav portu forwarding
[3] Cena cesty k root bridge 19

3.7 Časovače STP

STP pracuje jako přepínače posílající BPDU zprávy, ve snaze vytvořit topologii bez smyček. BPDU zprávy mají na cestu od přepínače k přepínači omezené množství času. Nové změny v topologii (jako je například selhání root bridge) mohou mít na svědomí zpoždění průchodu cestováním z jedné strany sítě na druhou.

STP používá tři časovače, k ujištění, že je síť správně zkonvergována před přemostěním smyček, které se mohou tvořit. Následují časovače a jejich výchozí hodnoty:

- **Hello Interval** – Časový interval mezi konfiguračními BPDU zprávami poslanými root bridgem. Hodnota hello intervalu nakonfigurovaná v root bridgi přepínače určuje hello interval pro všechny nerootovské přepínače, protože přenášejí, po jejich obdržení od roota, pouze konfigurační BPDU zprávy. Všechny přepínače mají lokální konfigurační hello interval, který se používá k času TCN BPDU zpráv. IEEE 802.1D [11] standard specifikuje výchozí hello interval na hodnotu 2 vteřiny.

- **Forwarding Delay** – Časový interval, který port přepínače stráví v obou listening i learning stavu. Výchozí hodnota je 15 vteřin.

- **Max (maximum) Age** – Časový interval ve kterém přepínač ukládá BPDU zprávu před tím, než ji zahodí. Zatímco se provádí STP, každý port přepínače drží kopii „nejlepší“ BPDU zprávy, kterou slyšel. Jestliže port přepínače ztratí kontakt se zdrojem BPDU zpráv (už BPDU zprávy nepřijímá), přepínač předpokládá, že ke změně topologie musí dojít až po uplynutí max age (maximální doby) intervalu, a proto už nejsou BPDU zprávy aktuální. Výchozí hodnota je 20 vteřin.

STP časovače mohou být konfigurovány nebo upraveny z příkazového řádku přepínače. Hodnota časovače by se nikdy neměla změnit z výchozí hodnoty bez pečlivého zvážení. Hodnota by pak měla být změněna pouze na root bridge přepínače. Je důležité připomenout, že hodnoty časovače jsou známy v polích BPDU zprávy. Root bridge zajišťuje, že hodnota časovače bude propagována na všechny ostatní přepínače.

3.8 Typy STP

- CST (Common Spanning Tree)

The IEEE 802.1Q [10] standard specifikuje, jak jsou přepínače schopny přenášet VLAN sítě pomocí trunku. Příkladem je *Common Spanning Tree (CST)*. Všechny BPDU zprávy jsou přeneseny přes trunk linky pomocí nativní VLAN sítě s neoznačenými rámci.

– PVST (Per-VLAN Spanning Tree)

Cisco má proprietární verzi STP, která nabízí větší flexibilitu než CST verze. *Per-VLAN Spanning Tree (PVST)* provozuje samostatnou instanci STP pro každou individuální VLAN síť. To umožňuje konfigurovat STP na každé VLAN síti nezávisle, nabízí lepší výkon a ladění pro konkrétní podmínky.

Mnohonásobné spanning-stromy také mohou vyvažovat zátěž přes redundantní linky, které jsou přiřazeny do odlišné VLAN sítě. Jedna linka může předat jednu sadu VLAN sítí, zatímco jiná redundantní linka může předat odlišnou sadu.

– PVST+ (Per-VLAN Spanning Tree Plus)

Cisco má druhou proprietární verzi STP, která dovoluje zařízením spolupracovat s předchozími verzemi STP - PVST i CST. *Per-VLAN Spanning Tree Plus (PVST+)* efektivně podporuje tři skupiny STP působící ve stejném areálu sítě:

- Catalyst switche bežící na PVST
- Catalyst switche běžící na PVST+
- Switche běžící na CST přes 802.1Q

Podrobnější informace o nastavení trunk spojů a VLAN sítí s trunky spojenými je možné najít v kapitole 5 ze zdroje [14].

4 RAPID SPANNING TREE PROTOCOL A JEHO POROVNÁNÍ S PROTOKOLEM STP

Standard IEEE 802.1D [11] Spanning Tree Protocol byl navržen k udržení přepínané nebo přemostěné sítě bez smyček, s nastavením vytvořeným pro sítě s dynamickou topologií podle [2]. Změny v topologii se obvykle projeví po 30 vteřinách pohybem portu ze stavu blocking do stavu forwarding po dvou intervalech forward delay časovače. Jak se technologie zdokonalovala, 30 vteřin se začalo zdát jako velice dlouhá doba čekání na vytvoření sítě na failover (převzetí služeb při selhání).

Standard IEEE 802.1w [12] byl navržen k využití hlavních konceptů standardu 802.1D [11] a k vytvoření výsledné mnohem rychlejší konvergence. To je RSTP (Rapid Spanning Tree Protocol) protokol, který definuje, jak spolu přepínače musí spolupracovat, aby udržely topologii bez smyček účinným způsobem.

4.1 Chování portu RSTP

Ve standardu 802.1D [11] měl každý přepínač přidělenu roli a stav v daném čase. V závislosti na blízkosti portu od root bridge má port jednu z následujících rolí:

- **Root port**
- **Designated port**
- **Blocking port** (ani root ani designated)

Každý port přepínače má také přiřazen jeden z pěti možných stavů:

- **Disabled**
- **Blocking**
- **Listening**
- **Learning**
- **Forwarding**

Pouze forwarding stav dovoluje data odesílat a přijímat. Stav portu je vázán na svou roli. Například blocking port nemůže být root nebo designated port.

RSTP dosahuje své povahy tím, že nechá každý přepínač v interakci s jeho sousedem skrz každý port. Tato interakce se provádí na základě role portu, ne striktně na BPDU zprávách, které jsou vysílány z root bridge. Poté co je role přidělena, každý port může mít stav, který určuje, co se bude dělat s příchozími daty.

Root bridge v síti s použitím RSTP je zvolen stejně jako u 802.1D, tedy nejnižším bridge ID.

Poté co přepínače dokončí volbu root přepínače, jsou přiděleny následující role:

- **Root port –** Jeden port na každém přepínači, který má nejlepší cenu root cesty k rootu. To je stejné i u 802.1D. (Root Bridge nemá root porty).
- **Designated port –** Port přepínače v síťovém segmentu, který má nejlepší root cenu cesty k rootu.
- **Alternate port –** Port, který má alternativní cestu k rootu, jinou než je cesta k root portu. Tato cesta je méně žádoucí než ta k root portu. (Například na přístupové vrstvě přepínače s dvěma uplink porty; jeden se stane root portem a druhý alternate portem).
- **Backup port –** Port, který poskytuje redundantní (ale méně žádoucí) spojení k segmentu, kde je již jiný port přepínače připojen. V případě, že je společná část ztracena, přepínač může mít a nemusí definovanou cestu zpět k rootu.

RSTP definuje stavy portů pouze podle toho, co port dělá s příchozími rámci. Pokud jsou příchozí rámce ignorovány nebo zahozeny, stanou se odchozími rámci. Každá role portu může mít jakýkoli z těchto stavů:

- **Discarding** – Příchozí rámce jsou jednoduše zahozeny; nejsou naučeny žádné MAC adresy. (Tento stav kombinuje 802.1D disabled, blocking a listening stavy, protože všechny tři efektivně nic nepředávaly. Listening stav není potřeba, protože RSTP může změnu stavu převést rychle bez předchozího naslouchání BPDU zpráv).
- **Learning** – Příchozí rámce jsou zahozeny, ale MAC adresa je naučena.
- **Forwarding** – Příchozí rámce jsou předány podle MAC adres, které byly (a jsou) naučeny.

4.2 BPDU v RSTP

V 802.1D BPDU zprávy v podstatě pocházejí z root bridge a jsou vysílány všemi přepínači dolů skrz strom. U takové propagace BPDU zpráv musela konvergence v 802.1D čekat na steady-state (ustálený stav) podmínek před tím, než se mohlo pokračovat.

RSTP používá BPDU zprávy ve stejném formátu jako 802.1D kvůli zpětné kompatibilitě. Odesílající port přepínače identifikuje sám sebe rolí a stavem RSTP.

RSTP používá interaktivní proces tak, že mohou dva sousední přepínače vyjednávat změny stavů. Některé BPDU bity jsou během tohoto vyjednávání použity na flag zprávy.

BPDU zprávy jsou posílány každému portu přepínače jako hello intervaly, bez ohledu na to, zda jsou přijaté z roota. V tomto případě, může hrát aktivní roli jakýkoliv přepínač kdekoli v síti, aby zachoval topologii. Přepínače také mohou očekávat příchozí pravidelné BPDU zprávy od svých sousedů. Když jsou v řadě tři BPDU zprávy ztraceny, sousední přepínač předpokládá výpadek a všechny příbuzné informace vedoucího portu okamžitě zastarají. To znamená, že přepínač může detekovat selhání souseda ve třech hello intervalech (výchozí hodnota je 6 vteřin), proti intervalu max age (výchozí hodnota je nastavena na 20 vteřin) pro 802.1D.

Protože RSTP rozlišuje svoje BPDU zprávy od BPDU zpráv 802.1D protokolu, může stále spolupracovat s přepínači použitím 802.1D. Každý port se pokouší pracovat podle BPDU zpráv, které přijal. Například když 802.1D BPDU přijme zprávu na port, port začne pracovat podle 802.1D pravidel.

4.3 Konvergence RSTP

Konvergence STP v síti je proces, který vyzve všechny přepínače ze stavu nezávislosti (každý si myslí, že musí být STP root) k jednotnosti,ve kterém má každý přepínač místo ve stromové topologii bez smyček. Konvergence prochází dvěma procesy:

1. Musí být „detekován“ jeden společný root bridge a všechny přepínače o něm musí vědět.

2. Stav každého portu přepínače v STP doméně musí být přenesen z blocking stavu do odpovídajícího stavu, který předchází smyčkám.

Protože jsou zprávy propagovány z přepínače na přepínač, konvergence obvykle trvá. Tradiční 802.1D také vyžaduje vypršení několika časovačů předtím, než je přepínačům umožněno bezpečně předávat data.

Když se přepínač potřebuje rozhodnout jak se bude účastnit ve stromové topologii, RSTP použije jiný přístup. Když se přepínač poprvé připojí do topologie (nebo je jen zapnut) nebo detekuje selhání v existující topologii se RSTP rozhoduje na základě přesměrování na typ portu.

4.4 Typy portů

Každý port přepínače může mít přiřazen jeden z následujících typů:

- **Edge port –** Port na „okraji“sítě, připojený jen k jednomu hostovi. Port nemůže vytvořit smyčku, když je připojen jen k jednomu hostovi, což může způsobit okamžitý přechod do forwarding stavu. V případě, kdy je BPDU zpráva přijata na hraniční port, port okamžitě ztrácí status hraničního portu.

- **Root port –** Port, který má nejlepší cenu k rootu. Pouze jeden root port může být vybrán a aktivní v jednu chvíli, ačkoli alternativní cesty k rootu mohou existovat skrz jiné porty. Když je alternativní cesta detekována, tyto porty jsou identifikovány jako alternativní root porty a okamžitě mohou být přepnuty do forwarding stavu, kdyby existující root port selhal.

- **Point-to-point port** – Každý port, který se připojí k jinému přepínači a stane se designated portem. Rychlá výměna se sousedním přepínačem, rozhoduje o stavu portu. BPDU zprávy jsou vyměněny tam a zpět ve formě návrhu a dohody. Jeden přepínač navrhuje, že se jeho port stane designated portem; jestliže druhý přepínač souhlasí, odpoví zprávou o dohodě.

Point-to-point porty jsou určeny pro použití v duplex módu. Full-duplex porty jsou určeny k point-to-point, protože mohou být současně na lince pouze dva přepínače. K rychlé STP konvergenci může dojít přes point-to-point link výměnou zpráv RSTP.

RSTP zpracovává kompletní STP konvergenci ze sítě propagováním výměny přes point-to-point linky. Pokud přepínač potřebuje udělat STP rozhodnutí, výměna je realizována s nejbližším sousedem. Když je tento způsob úspěšný, výměnná sekvence je přesunuta k dalšímu přepínači a opět dalšímu.

4.5 RSTP konfigurace

Ve výchozím stavu přepínač pracuje v Per-VLAN Spanning Tree Plus (PVST+) modu použitím tradičního 802.1D. Proto se RSTP nemůže použít, dokud není odlišný spanning-tree mode (MST nebo RPVST+) povolen. RSTP je pouze základní mechanismus, který může spanning-tree mód použít k detekování změn v topologii a konvergování sítě do bezsmyčkové topologie.

Pouze konfigurační změny související s RSTP ovlivní port nebo typ linky. Typ linky je použit k určení, jakým způsobem přepínač vyjedná informace o topologii s jeho sousedy.

Konfigurace portu jako RSTP hraničního portu. Použit je následující konfigurační příkaz:

```
Switch(config-if)#spanning-tree portfast
```

Ke změně z STP modu na RSTP je potřeba pouze jeden konfigurační příkaz:

```
Switch(config)# spanning-tree mode rapid-pvst
```

Další informace například o rozšíření RSTP protokolu nazývaného Multiple Spanning Tree Protocol (MSTP) a konfiguraci, které jsou nad rámec této práce lze najít v [14], v kapitole 11.

4.6 Rozdíly mezi STP a RSTP

Tabulka 3 - Rozdíly STP a RSTP

STP (802.1D)	Rapid STP (802.1W)
Ve stabilní topologii posílá pouze root BPDU zprávy které si ostatní předávají.	Ve stabilní topologii generují BPDU zprávy všechny bridge každé 2 vteřiny (Hello): použitím "*keepalives*" mechanismu
Stavy portů	
Disabled	Root (Forwarding)
Blocking	Designated (Forwarding)
Listening	Alternate (Discarding)
Learning	Backup (Discarding)
Forwarding	
Další konfigurace k vytvoření koncového uzlu **port fast** (v případě, že je BPDU zpráva přijata)	Edge port (koncový uzel portu) je integrovaný typ spojení závislý na duplexu: Point-to-point pro full duplex & sdílený pro half duplex
Změna topologie a konvergence	
Používá časovače pro konvergenci (oznamuje root):	Návrh a dohoda procesu synchronizace trvá méně než 1 vteřinu. Hello, Max Age a Forward delay časovače jsou použity pouze pro zpětnou kompatibilitu se standardem STP
Hello (2 vteřiny)	
Max Age (20 vteřin)	Pouze RSTP port přijímá STP (802.1D) zprávy, které se budou chovat jako standartní STP
Forward delay times (15 vteřin)	
Pomalý přechod **(50 vteřin):** Blocking (20 vteřin) => Listening (15 vteřin) => Learning (15 vteřin) => Forwarding	Rychlejší přechod na point-to-point a pouze hraniční porty: Méně stavů - **Žádný learning state,** nečeká na informace ostatních, místo toho, **aktivně** sleduje možný výpadek **RLQ** (Request Link Query) mechanismem zpětné vazby
Využívá pouze 2 bity z flag oktetu:	Využívá ostatních 6 bitů flag oktetu (BPDU typ 2/verze 2):
Bit 7: Změna topologie potvrzení	Bit 1: Návrh
Bit 0: Změna topologie	Bit 2,3: Role portu
	Bit 4: Learning
	Bit 5: Forwarding
	Bit 6: Dohoda
	Bit 0, 7: TCA & TCN pro zpětnou kompatibilitu

Bridge, který objeví změny v síti informuje roota, který informuje všechny ostatní tím, že pošle BPDU s TCA bit set a informuje je aby vyčistili DB záznamy po té, co vyprší "krátký časovač" (Forward delay).	TC zaplavila celou síť, každý bridge generuje TC (změna topologie) a informuje sousedy, že si je vědom změny topologie a **okamžitě odstraní staré DB záznamy**.
Jestliže bridge, který není root nepřijme Hello po dobu 10*Hello (oznamuje root), začne prohlašovat root roli generováním svých vlastních Hello zpráv.	Čeká po dobu 3*Hello (znamuje root) před rozhodnutím jednat.
Čeká dokud TC nedosáhne až k rootu + vyprší krátký časovač, pak blikají všechny položky root DB.	Okamžitě smaže lokální DB kromě MAC adresy portu přijímající změnu topologie (návrh)

5 HOT STANDBY ROUTER PROTOCOL

HSRP je Cisco proprietární protokol vyvinutý s cílem umožnění se několika směrovačům (nebo multilayer přepínačům) jevit jako jednotná vstupní brána IP adres podle [1], [3] a [15]. Detailněji popisuje tento protokol RFC 2281 [13].

Existuje ve dvou verzích:

- **HSRPv1** (RFC 2281 [13])

  Používá UDP/1985, pakety posílá na 224.0.0.2

  Na jednom rozhraní dovoluje vytvořit maximálně 256 různých virtuálních směrovačů

- **HSRPv2**

  Používá také UDP/1985, pakety posílá na 224.0.0.102

  Na jednom rozhraní dovoluje vytvořit maximálně 4096 různých virtuálních směrovačů

  Podporuje časovače na úrovni milisekund

Předvolená verze je verze 1. Dále jen HSRPv1.

HSRP definuje tzv. standby skupinu, která obsahuje:

- **Active směrovač**

  Nositel identity virtuálního směrovače (vMAC, vIP).

  Je zodpovědný za obsluhu paketů posílaných na identitu virtuálního směrovače.

  V HSRP skupině je vždy jen jeden Active směrovač

- **Standby směrovač**

  Záložní směrovač pro Active.

  Když Active směrovač přestane pracovat, Standby směrovač přebírá na sebe vMAC a vIP.

  V HSRP skupině je vždy jen jeden Standby směrovač.

- **Ostatní směrovače**

  Ostatní směrovače v HSRP skupině, které nejsou ani active ani standby. Monitorují dostupnost active a standby směrovačů.

  V případě potřeby mohou přejít do role standby a následně active.

- **Virtuální směrovač**

  Celá standby skupina.

5.1 Virtuální IP adresa HSRP skupiny

HSRP skupina vytváří jeden virtuální směrovač s virtuální IP adresou. Při konfiguraci HSRP bude mít každý člen HSRP skupiny nastavenou jistou vIP adresu aby mohl kdykoli začít plnit úlohu active směrovače.

Virtuální IP adresa musí být z rozsahu IP adres rozhraní, na kterém je HSRP spuštěn. V HSRP tato IP adresa nesmí být stejná jako skutečná IP adresa některého člena HSRP skupiny. Doporučené použití je: virtuální IP je nejnižší, reálné směrovače mají nejvyšší IP v síti nebo virtuální IP je nejvyšší a reálné směrovače mají nejnižší IP v síti.

5.2 Činnost HSRP – Active a standby směrovače

Active směrovač je nositelem vMAC/vIP. Volba probíhá na základě priority (0-255, předvolená hodnota je 100, vyšší číslo znamená vyšší prioritu). Jestliže jsou priority stejné, vyhrává směrovač s vyšší IP adresou, vIP adresa je daná konfigurací. vMAC adresa je odvozená od čísla HSRP skupiny:

- HSRPv1: 000.0c07.acxx, kde xx je číslo skupiny v hexadecimálním tvaru
- HSRPv2: 0000.0C9F.Fxxx

Standby směrovač se také volí na základě priority/vyšší IP adresy. Active a standby směrovače posílají hello pakety. Informují o svojí existenci sebe i všechny ostatní směrovače ve skupině. Jak standby zjistí, že se active směrovač neozývá, převezme na sebe jeho funkce a stane se novým active směrovačem. Ostatní směrovače ve skupině neposílají hello, jen monitorují přítomnost active a standby směrovačů a v případě potřeby se zúčastní voleb na neobsazené pozice.

V podstatě každý ze směrovačů, který zajišťuje redundanci vzhledem k adrese brány, má přiřazenu společnou HSRP skupinu. Jeden směrovač je zvolen jako primární nebo a*ktivní* HSRP směrovač; jiný je zvolen jako *standby* HSRP směrovač; a všechny ostatní zůstanou v *listen* stavu. Směrovače mění HSRP hello zprávy v pravidelných intervalech tak, že dávají pozor na existenci sousedního a aktivního směrovače.

HSRP skupina může být přiřazena libovolnému číslu skupiny, od 0 do 255. Když se konfigurují HSRP skupiny pro více VLAN rozhraní, může být užitečné vytvořit číslo skupiny stejné jako číslo VLAN, ačkoli většina Catalyst přepínačů podporuje čísla pouze do 16 unikátních HSRP skupin. Když bude více jak 16 VLAN sítí, čísla skupin rychle dojdou. Alternativou je vytvořit skupinu stejných čísel pro každé VLAN rozhraní. Tedy HSRP skupina 1 na rozhraní VLAN 10 je unikátní a nezávislá od HSRP skupiny 1 na rozhraní VLAN 11.

5.3 HSRP volba směrovače a konfigurace

Volba HSRP směrovače vychází z prioritních hodnot (0-255), které jsou konfigurovány na každém směrovači ve skupině. Výchozí hodnota je 100. Směrorvač s vyšší prioritní hodnotou (255 a vyšší) se stává pro skupinu aktivním směrovačem. Jestliže budou všechny priority směrovačů stejné nebo nastaveny na výchozí hodnoty, směrovač s vyšší IP adresou se na HSRP rozhraní stane aktivním směrovačem. K nastavení priority se používá následující příkaz konfigurace rozhraní:

```
Switch(config-if)#standby group priority priority
```

Například jeden přepínač bude mít nastavenou prioritu na 100, zatímco lokální přepínač bude určen, aby vyhrál aktivní volbu role. Je třeba zadat příkaz k nastavení HSRP priority 200:

```
Switch(config-if)#standby 1 priority 200
```

Když je HSRP nakonfigurován, projde si směrovač sérií stavů, než se stane aktivním. To nutí směrovač naslouchat ostatním ve skupině. Zařízení spolupracující s HSRP musí projít touto sekvencí stavů:

1. **Init / Disabled** (Směrovač není schopný podílet se na činnosti skupiny (např. vypnuté rozhraní).
2. **Learn** (Inicializace HSRP, směrovač se snaží zjistit IP adresu virtuálního směrovače a přítomnost active/standby. Směrovač ještě nedostal hello paket).
3. **Listen** - 10 vteřin (Směrovač začal dostávat hello zprávy. Monitoruje přítomnost active a standby směrovače).
4. **Speak** – 10 vteřin (Směrovač posílá a přijímá hello zprávy. Podílí se na volbě standby nebo active směrovače).
5. **Standby** (Při existenci standby se obyčejný směrovač označí jako standby. Při existenci active směrovače zůstává ve stavu standby. Posílá hello zprávy. Monitoruje přítomnost active směrovače).
6. **Active** (Při neexistenci active směrovače se standby označí jako active. Posílá hello zprávy. Přivlastní si vMAC/vIP).

Pouze standby (jeden směrovač s druhou nejvyšší prioritou) kontroluje hello zprávy od aktivního směrovače. Výchozí stav vypadá tak, že se hello zprávy posílají každé 3 vteřiny. Jestliže se hello zprávy ztratí během doby trvání časovače, holdtime (výchozí hodnota 10 vteřin, nebo 3x hello časovač), aktivní směrovač je považován za neaktivní. Standby směrovač po té převezme aktivní roli.

Jestliže ostatní směrovače přetrvávají v listen stavu, směrovač s další nejvyšší prioritou má dovoleno stát se novým standby směrovačem.

Pro změnu hodnoty časovače se používá následující příkaz. Je třeba při změně časovače na směrovači změnit i časovač na všech ostatních směrovačích HSRP skupiny.

```
Switch(config-if)#standby group timers [msec]hello[msec]holdtime
```

Hodnoty hello a holdtime mohou být v sekundách nebo milisekundách. Čas hello může mít rozsah od 1 do 154 sekund nebo od 15 do 999 milisekund. Hodnota holdtime by měla být alespoň třikrát časovač hello v rozsahu od 1 do 255 sekund nebo od 50 do 3000 milisekund.

Například následující příkaz může být použit k nastavení hello na 100 milisekund a holdtime na 300 milisekund:

```
Switch(config-if)#standby 1 timers msec100msec 300
```

Obvykle poté, co selže aktivní směrovač a aktivním se stane standby, původní aktivní směrovač se nemůže stát aktivním ihned po té, co se obnoví. Jinými slovy, jesliže ještě směrovač není aktivní, nemůže se aktivním stát znovu, dokud současný aktivní směrovač neselže – dokonce i když má vyšší prioritu než aktivní směrovač. Rozhraní prvního směrovače se stane HSRP aktivním směrovačem, dokonce i když má nejnižší prioritu ze všech.

5.4 HSRP multicast zprávy a preempce

Zpráva hello

- Posílá active a standby.
- Obsahuje informace o virtuální adrese skupiny, prioritě a stavu odesílatele.

Zpráva Coup

- Používá se, když chce směrovač převzít úlohu active směrovače.
- Používá se nejčastěji při preempci.

Zpráva Resign

- Používá se, když se active směrovač zříká své funkce.

Preempce je schopnost jiného směrovače, převzít na sebe roli active směrovače, i když active stále žije, avšak jeho priorita je měnší než priorita standby. Standartně je preempce vypnutá, v takové situaci standby přebere na sebe roli active jen tehdy, když active úplně vypadne.

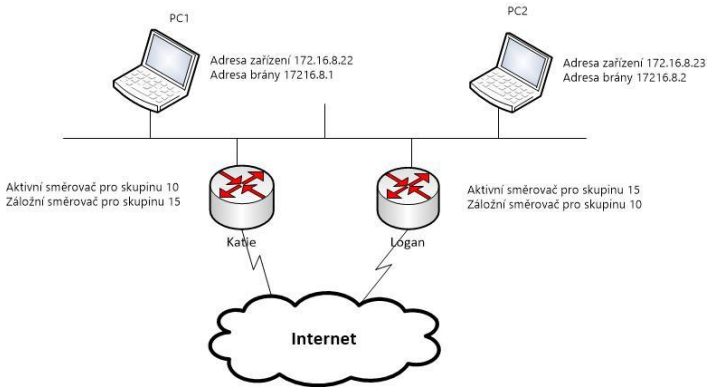
Na konfigurace směrovače na preemptci nebo okamžité převzetí aktivní role, se používá následující příkaz:

```
Switch(config-if)#standby group preempt [delay [minimum seconds] [reload seconds]]
```

5.5 Příklad konfigurace HSRP

Obrázek 10 podle [1] ukazuje dva směrovače s nastaveným HSRP. Na směrovačích jsou nastaveny dvě skupiny, takže provoz lze distribuovat přes obě zařízení. Pokud jeden směrovač vypadne, bude všem systémům sloužit zbývající směrovač. Směrovače navíc sledují své sériové rozhraní. Pokud dojde k výpadku sériového rozhraní, sníží se priorita směrovače o 10 a roli aktivního tak převezme druhý směrovač.

```
Katie

Interface ethernet 0
      ip address 172.16.18.3 255.255.255.0
      standby 10 ip 172.16.18.1
      standby priority 200
      standby preempt
      standby track serial 0 10
      standby 15 ip 1.2.2.2
      standby priority 190
      standby preempt

Logan

Interface ethernet 0
      ip address 172.16.18.4 255.255.255.0
      standby 10 ip 172.16.18.2
      standby priority 195 preempt
      standby 15 ip 1.2.2.2
      standby priority 200 preempt
      standby track serial 0
```



Obrázek 10 - Příklad konfigurace HSRP

6 PŘÍPADOVÁ STUDIE VYUŽITÍ STP, RSTP A HSRP PROTOKOLŮ

Praktické využití protokolů je v této kapitole popsáno na příkladu fiktivní sítě v datacentru poskytovatele webových služeb. Tato síť je rozdělena do dvou VLAN sítí – zákaznickou a vývojovou. Cílem této práce je dosáhnout maximální redundance, dostupnosti a výpadku na STP protokolu se změnou parametrů časovačů maximálně 1-2 pingy.

Řeší se výpadky kritických síťových prvků a následné znovu zprovoznění sítě, tedy pokud vypadne root směrovač, přepne se na záložní, což obstará protokol HSRP nebo pokud vypadne root přepínač, veškerá komunikace se přepne na záložní cestu přes záložní přepínač díky protokolu STP nebo RSTP.

Protokoly splňující dnešní požadavky pro směrování dat jsou EIGRP, IS-IS a OSPF. Nakonec jsem se rozhodla, že použiji protokol EIGRP. Omezení použitelnosti tohoto protokolu pouze na směrovače Cisco nebude nevýhoda, jelikož jsou v této práci použity pouze směrovače od této firmy.

Případová studie byla zpracována v síťových laboratořích na přepínačích Cisco řady Catalyst 2960 a směrovačích řady 2801 a v simulátoru Cisco Packet Tracer 6.0.1 na přepínačích Cisco řady 2950-24 a směrovačích řady 1841. V přílohách této práce je přiložená veškerá konfigurace směrovačů s podrobným popisem všech prováděných kroků ve formě komentářů. Výchozí a výsledný stav topologie je nakreslen v nástroji MS Visio 2010. Vytvořený projekt v simulátoru Packet Tracer 6.0.1 je přiložen na CD i částečně použit v této práci.

6.1 Použité adresy

6.1.1 Virtuální adresy HSRP

Tabulka 4 - Použité virtuální adresy HSRP

HSRP adresy	
VLAN	**IP Adresa**
10	10.0.10.1/24
20	10.0.20.1/24

6.1.2 **Adresy VLAN 10 a 20**

Tabulka 5 - Použité adresy VLAN 10

VLAN 10			
Zařízení	**IP adresa**	**Maska**	**Výchozí brána**
R1	10.0.10.2	255.255.255.0	10.0.10.1
R2	10.0.10.3	255.255.255.0	10.0.10.1
PC1	10.0.10.4	255.255.255.0	10.0.10.1

Tabulka 6 - Použité adresy VLAN 20

VLAN 20			
Zařízení	**IP adresa**	**Maska**	**Výchozí brána**
R1	10.0.20.2	255.255.255.0	10.0.20.1
R2	10.0.20.3	255.255.255.0	10.0.20.1
PC2	10.0.20.4	255.255.255.0	10.0.20.1

6.1.3 **Adresy ISP, R1, R2**

Tabulka 7 - Použité adresy ISP - R1

ISP – R1		
Zařízení	**ISP**	**R1**
IP adresa	10.0.40.2	10.0.40.1
Maska	255.255.255.252	255.255.255.252

Tabulka 8 - Použité adresy ISP - R2

ISP – R2		
Zařízení	**ISP**	**R2**
IP adresa	10.0.40.6	10.0.40.5
Maska	255.255.255.252	255.255.255.252

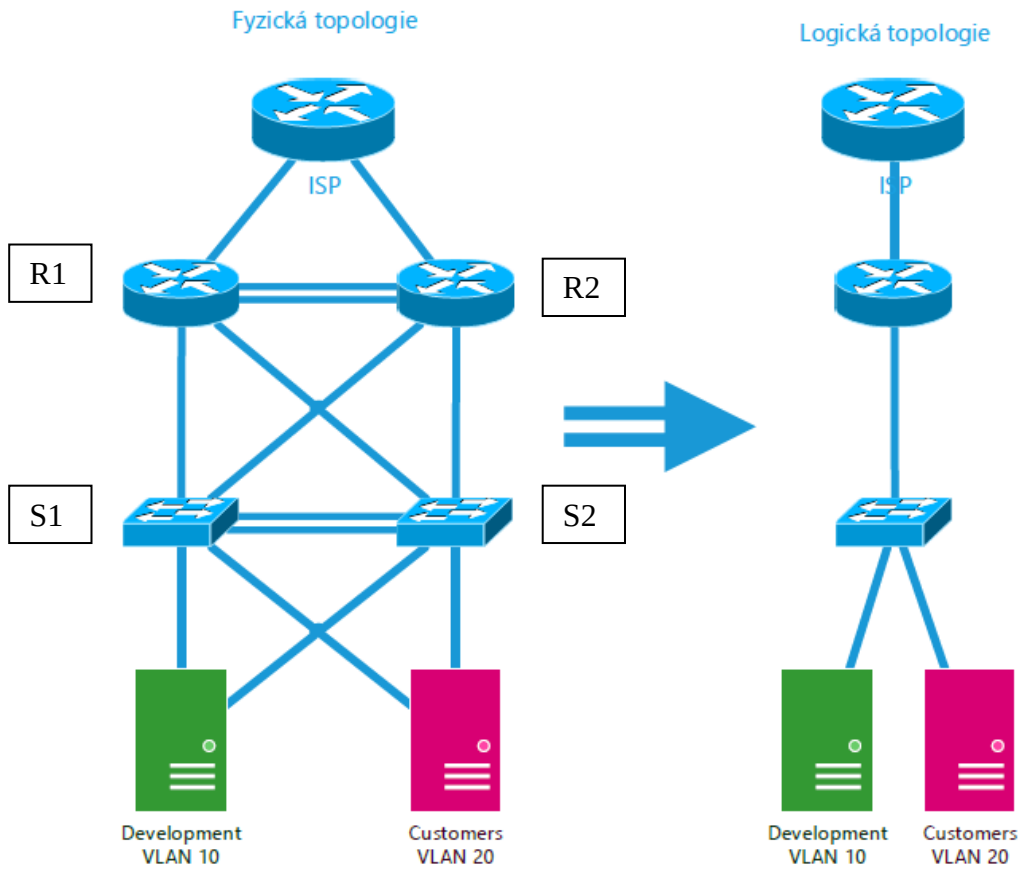
Tabulka 9 - Použité adresy R1 - R2

R1 – R2				
Zařízení	**R1-R2_1**	**R1-R2_2**	**R2-R1_1**	**R2-R1_2**
IP adresa	10.0.30.1	10.0.30.2	10.0.30.5	10.0.30.6
Maska	255.255.255.252	255.255.255.252	255.255.255.252	255.255.255.252

Tabulka 10 - Loopback

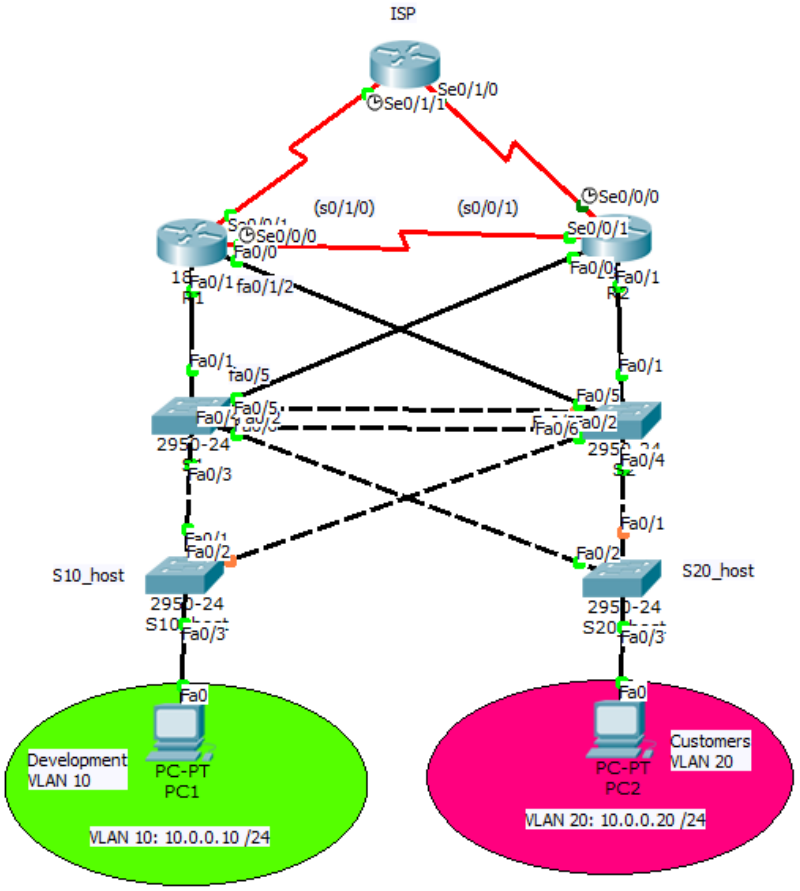
Loopback ISP	
IP adresa	1.1.1.1
Maska	255.255.255.255

6.2 Použitá topologie a výsledek studie



Obrázek 11 - Fyzická a logická topologie

Fyzická topologie znázorňuje od shora směrovač ISP, který slouží jako poskytovatel webových služeb. Na směrovači ISP je vytvořen loopback (zpětná smyčka) k otestování komunikace. Dále směrovače ISP, R1 a R2, mezi kterými funguje protokol EIGRPv1. Mezi ISP, R1 a R2 je dále nakonfigurován protokol HSRP, jsou vytvořeny virtuální adresy pro záložní cesty v případě výpadku aktivního směrovače. Ve výsledku logické topologie je znázorněno, jak se aktivní směrovač přepne na záložní směrovač. Mezi S1 a S2 poběží protokol STP nebo RSTP. V případě výpadku této větve, se díky těmto protokolům přepne také na záložní zařízení a výsledek je opět znázorněn v logické topologii. Dále tu figurují dvě VLAN sítě, VLAN 10 Development a VLAN 20 Costumers. V nástroji Packet Tracer by simulace vypadala takto:



Obrázek 12 - Topologie Packet Tracer

Kvůli nedostatku fastethernet rozhraní na počítačích se v simulátoru zvolil ještě jeden mezikrok a to vložení dalších dvou přepínačů. Na funkčnost a konfiguraci tyto přepínače navíc nemají velký vliv, vše zůstalo zachováno. Pouze jeden spoj mezi R1 a R2 je tu namodelován kvůli nedostatku portů v laboratořích. Na funkčnost také nemá výrazný vliv.

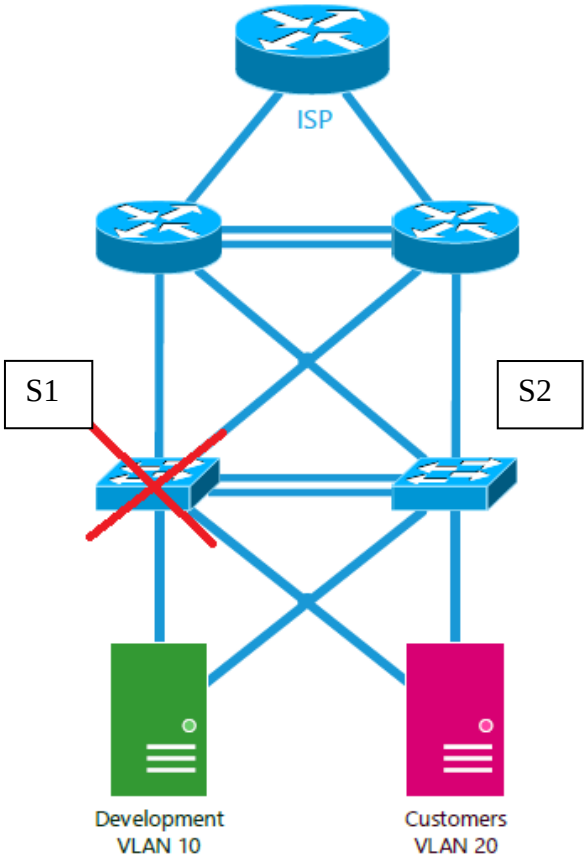
Výsledná konfigurace směrovačů a přepínačů se skládá z těchto kroků:

- nastavení všech spojení mezi jednotlivými směrovači,
- konfigurace EIGRP na směrovačích R1 a R2,
- nastavení defaultní cesty k ISP a nastavení jejího šíření v EIGRP na směrovačích R1 a R2,
- konfigurace STP nebo RSTP na přepínačích S1 a S2,
- nastavení záložních cest v případě výpadku stávající konfigurace,
- nastavení portfast kvůli omezení smyček.

6.3 Výpadek přepínače - zobrazení na STP a RSTP

Výše zmíněná topologie se poté testovala na výpadky a následné vyřešení záložních cest. Na reakce, dobu výpadků, přepnutí jednotlivých protokolů a zda je možné dostat se na výpadek pouze 1-2 pingy.

6.3.1 Výpadek S1 protokol STP s výchozím nastavením časovačů



Obrázek 13 - Výpadek přepínače S1

Konfigurace přepínače S1 na STP je uvedena v příloze B.

Výpis uvedený v příloze získáme příkazem:

```
S1#show spanning-tree
```

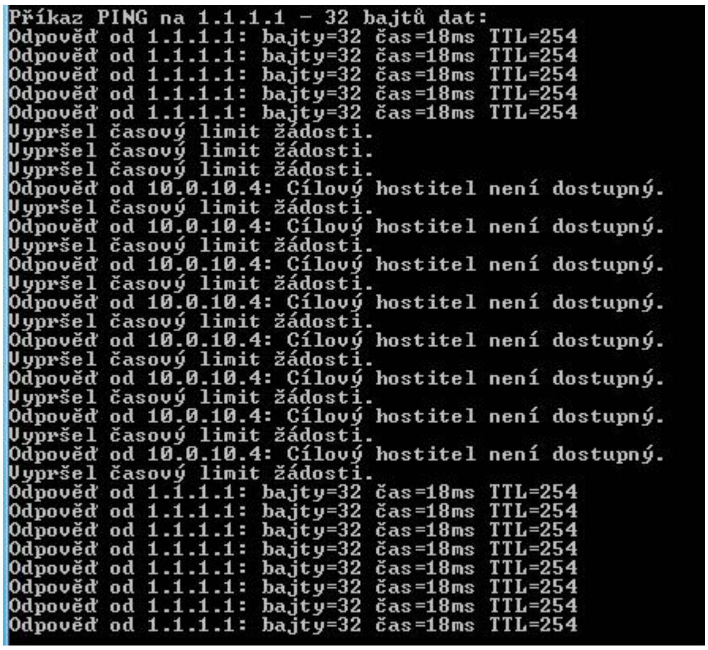
Poté uvidíme, že přepínač S1 je root pro VLAN 10 i VLAN 20, dále lze vidět priority, fyzickou adresu, přes které porty primárně vede cesta pro jednotlivé VLAN, který port je hraniční, jakou má daný port roli nebo status a cenu atd. Výchozí nastavení časovačů je zde vidět také, tedy 2 vteřiny hello time interval, 20 vteřin max age a 15 vteřin forward delay.

Když vypadl přepínač S1, který byl konfigurován jako primární, záložní přepínač S2 převzal jeho roli.

Výpadek a následné přepnutí na záložní cestu se testovalo v příkazovém řádku počítačů a na konzoli směrovačů. V příkazovém řádku počítače PC1 test probíhal zadáním příkazu ping na adresu brány ISP 1.1.1.1:

```
ping –w 1000 –t 1.1.1.1.
```

Přepínač –w a 1000 je časový limit čekání na odpověď v ms, 1000ms neboli po 1s a přepínač –t znamená, že opakovaně odešle určenému hostiteli žádost o ozvěnu, tento výpis může být ukončen zásahem uživatele. Zde je vidět jak dlouhý byl výpadek a následný přechod na záložní přepínač S2 (19s).



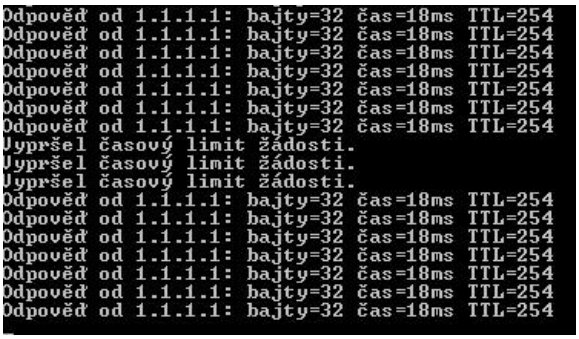
```
Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 14 - Výpadek S1 z PC1 ping

Cílem bylo dosáhnout maximálně jednoho nebo dvou pingů (ve výchozím stavu je ping 4 vteřiny), zde je ping měřen po 1 vteřině a výpadek trval 19 vteřin. Při výchozích hodnotách nastavení STP časovačů se nepodařilo splnit požadovaný výpadek 4-8 vteřin.

V příloze B je také uvedena konfigurace přepínače S2 na STP.

Na obrázku 15 je vidět, jak dlouho trvalo přepínači S2 přepnout se ze záložního do aktivního stavu (3s).

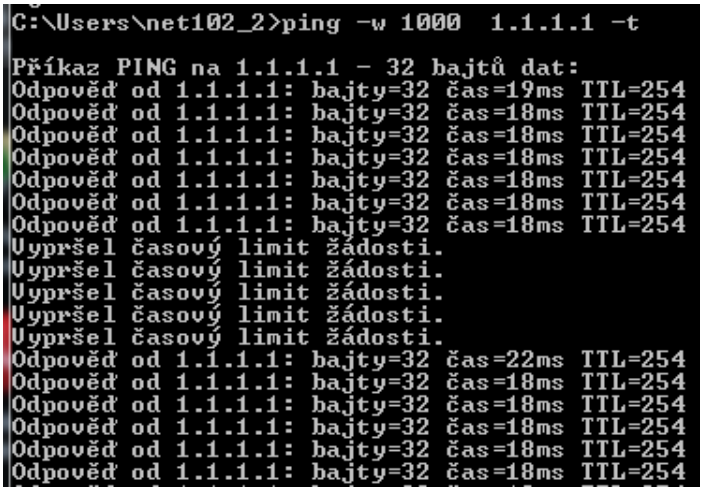


Obrázek 15 - Záložní cesta přes přepínač S2 z PC2 ping

6.3.2 Výpadek S1 protokol STP s minimálními hodnotami časovačů

Minimální hodnoty časovače hello time byly nastaveny na 1 vteřinu, max age na 6 vteřin a forward delay na 4 vteřiny.

Zde se podařilo splnit maximální výpadek 4-8 vteřin, protože to trvalo 5 vteřin.



Obrázek 16 - Výpadek S1 z PC1 ping - nejnižší hodnoty časovačů

6.3.3 **Výpadek S1 protokol STP s jiným nastavením časovačů**

Pro porovnání, třetí případ nastavení STP časovačů byl následující: hello time interval zůstal na výchozích 2 vteřinách, forward delay 7 vteřin a max age 10 vteřin.

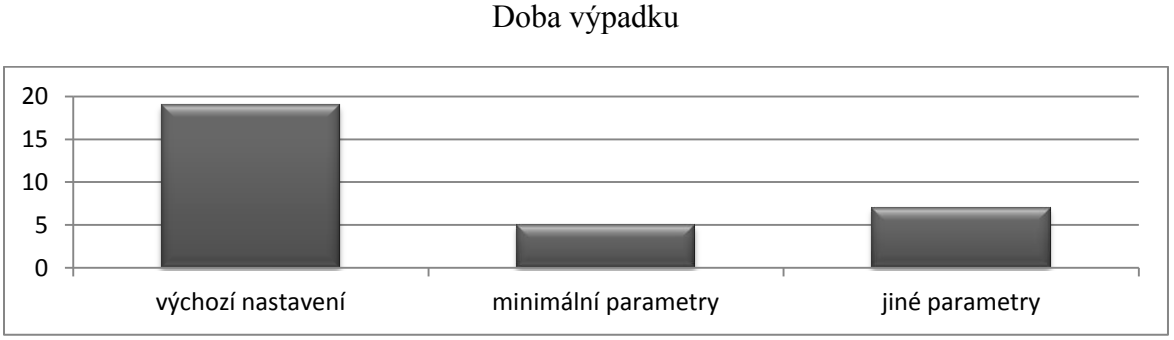
```
C:\Users\net102_2>ping -w 1000  1.1.1.1 -t

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 17 - Výpadek S1 z PC1 ping - jiné hodnoty časovačů

Výpadek tedy trval 7 vteřin, což je podle očekávání hodnota mezi výchozím nastavením STP časovačů a tím nejrychlejším možným nastavením. Tato hodnota by se také dala považovat za splnění požadavků na 1-2 pingy.

6.3.4 **Porovnání výpadků při různém nastavení časovačů STP - S1**

	hello time	**forward delay**	**max age**	**doba výpadku**
výchozí	2s	15s	20s	19s
minimální	1s	4s	6s	5s
jiné	2s	7s	10s	7s



Obrázek 18 - Graf porovnání výpadků při různém nastavení časovačů STP - S1

6.3.5 Výpadek S1 protokol RSTP

Jak byl nakonfigurován přepínač S1 na RSTP je uvedeno v příloze C.

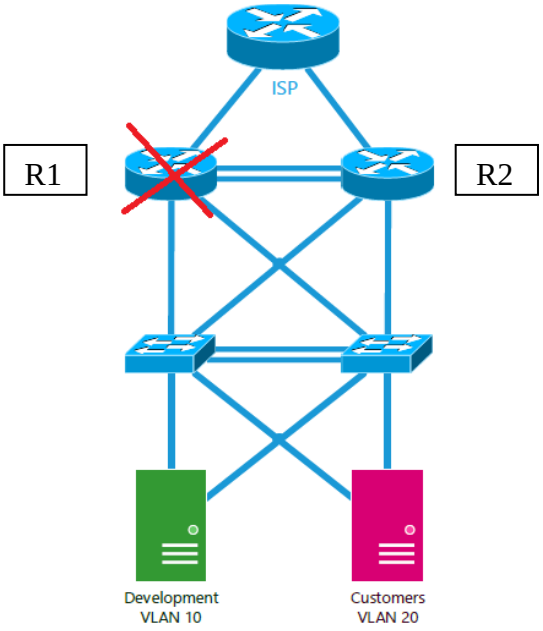
Výpadek trval 4s, což je mnohonásobně méně než jak tomu bylo ve stejném případě při použití protokolu STP ve výchozím nastavení a stále méně při použití minimálních hodnot časovačů na STP. RSTP tedy sám o sobě splňuje výpadek maximálně 1 pingu a to přesně 4 vteřiny.

```
C:\Users\net102_2>ping -w 1000 -t 1.1.1.1

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 19 - Výpadek S1 ping

6.4 Výpadek směrovače - zobrazení na HSRP

6.4.1 Výpadek R1



Obrázek 20– Výpadek směrovače R1

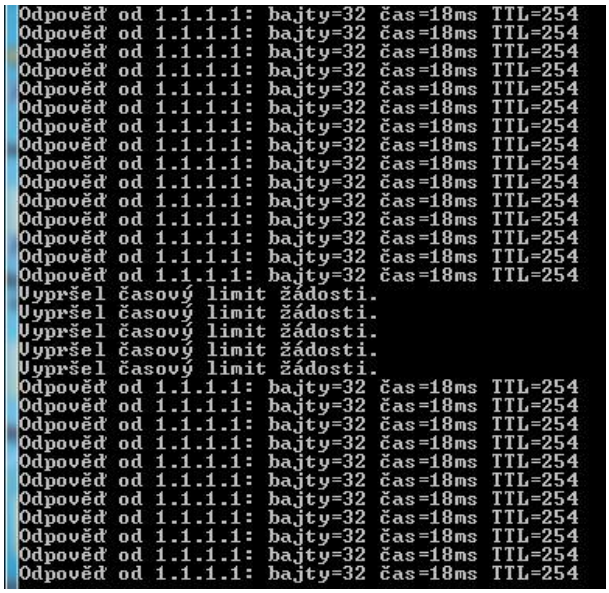
Informace o HSRP na směrovači zjistíme příkazem:

```
R1#show standby brief a R1#show standby
```

Konfigurace směrovače R1 se nachází v příloze D:

V tomto výpisu zjistíme prioritu 200 pro obě VLAN sítě 10 i 20 směrem k přepínačům. Dále skupinu, ve které je daná VLAN, virtuální IP i MAC adresy, záložní cestu i její prioritu, název skupiny nebo například stav zařízení.

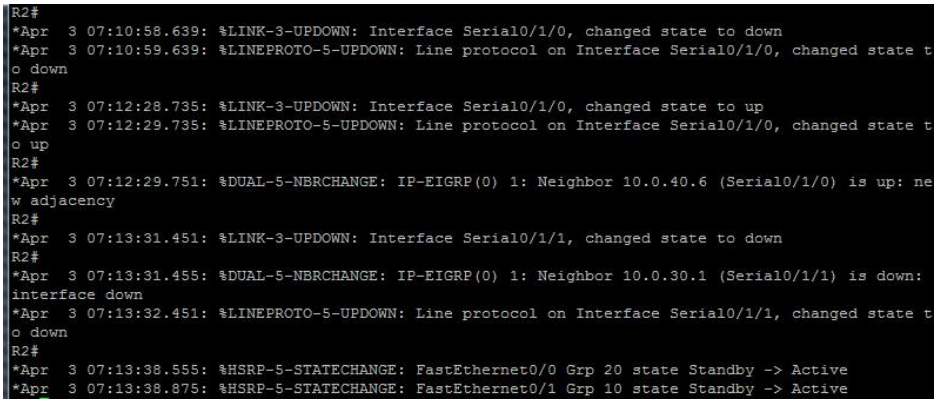
Když vypadl směrovač R1, příkazem ping z počítače PC1 na 1.1.1.1 zjistíme, že přepnutí na záložní cestu trvalo 5s.



Obrázek 21 - Výpadek R1 ping

Konfigurace směrovače R2 je také uvedena v příloze D.

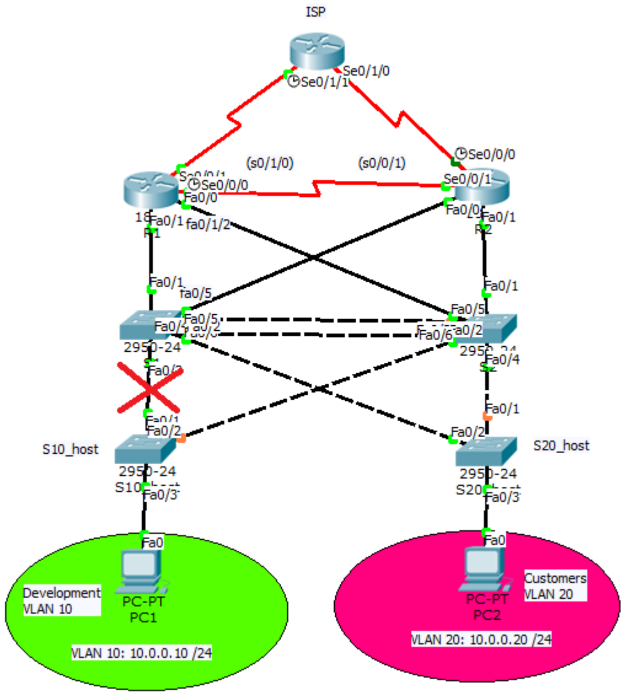
Na směrovači R2 vypadalo přepnutí do aktivního stavu následovně:



Obrázek 22- Přepnutí R2 do aktivního stavu na R2

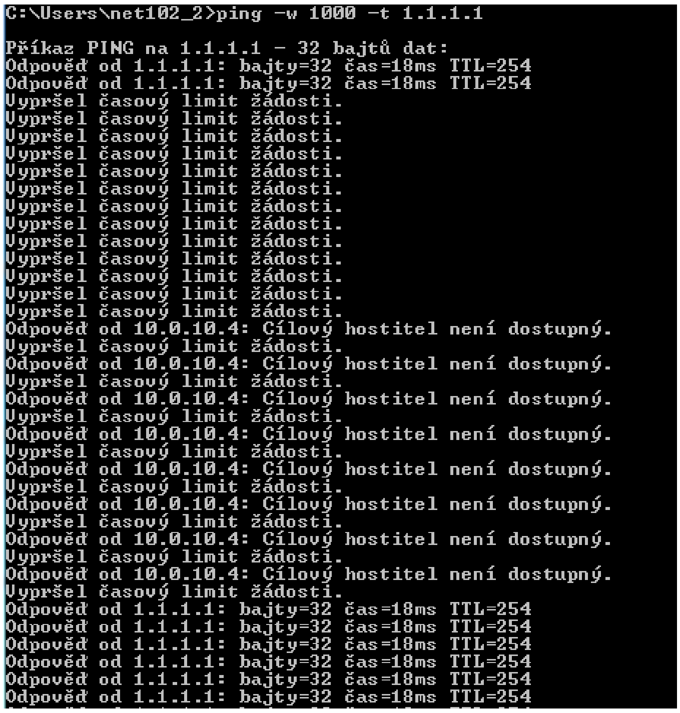
6.5 Výpadek kabelu – zobrazení na STP a RSTP

6.5.1 Výpadek kabelu S1-S10_host STP s výchozím nastavením časovačů



Obrázek 23 - Výpadek kabelu z R1-S1 model Packet Tracer

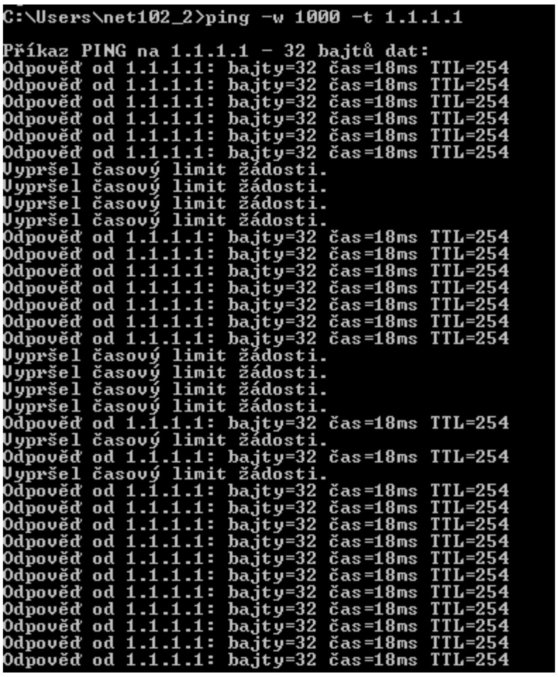
Takto vypadal výpadek testováním ping na 1.1.1.1 z PC1. Když vypadl kabel z S1 na S10_host. Poměrně dlouho trvalo, než se zprovoznily záložní cesty (29s).



```
C:\Users\net102_2>ping -w 1000 -t 1.1.1.1

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 10.0.10.4: Cílový hostitel není dostupný.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 24 – Výpadek kabelu z S1 na S10_host ping

A takto to vypadalo, když se původní cesta zase obnovila. Tedy byl připojen zpět kabel z S1 na S10_host.

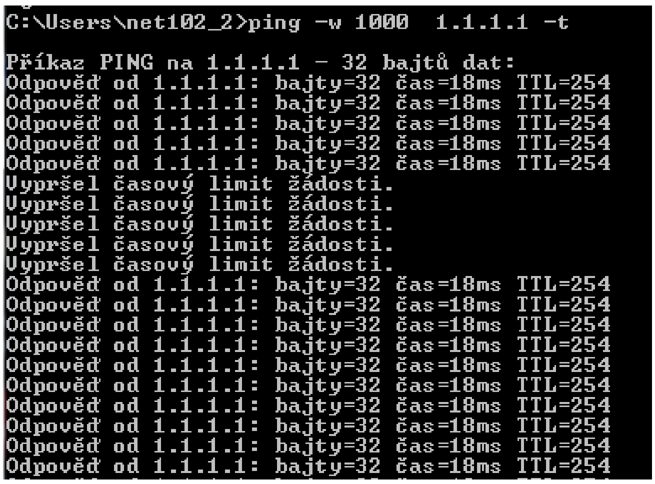


```
C:\Users\net102_2>ping -w 1000 -t 1.1.1.1

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 25 - Obnovení původní cesty z S1 na S10_host ping

6.5.2 Výpadek kabelu S1-S10_host STP s minimálními hodnotami časovačů

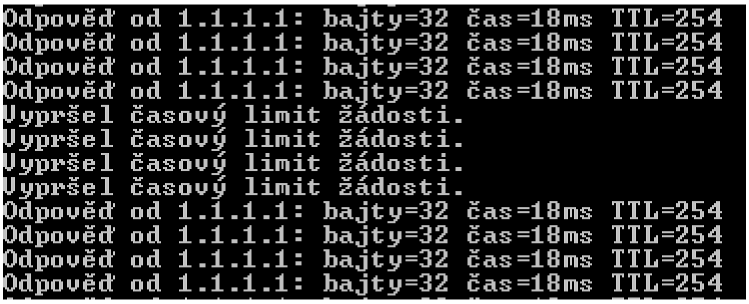
S minimálními hodnotami časovačů STP, tedy s hello time intervalem 1 vteřina, forward delay 4 vteřiny a max age 6 vteřin výpadek trval 5 vteřin. To znamená, že se podařilo splnit limit maximálně jednoho nebo dvou pingů.



```
C:\Users\net102_2>ping -w 1000  1.1.1.1 -t

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 26 - Výpadek kabelu z S1 na S10_host ping - nejnižší hodnoty časovačů

Opětovné zprovoznění původních cest trvalo 4 vteřiny.

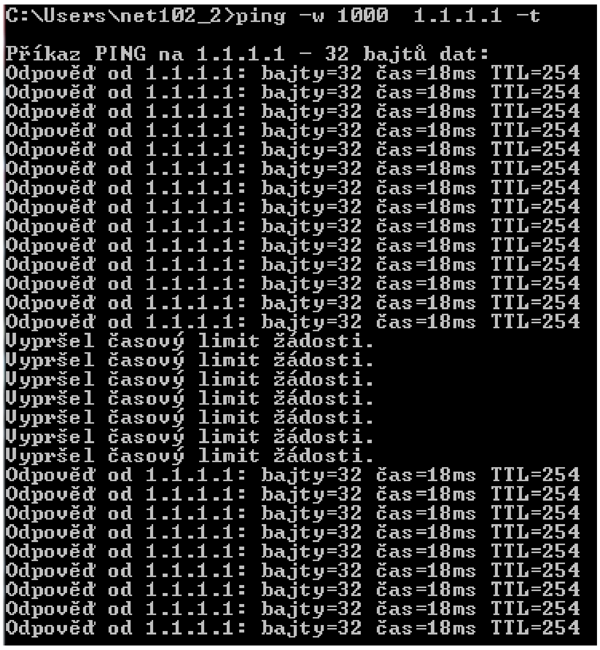


```
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 27 - Obnovení původní cesty z S1 na S10_host ping - nejnižší hodnoty čas.

6.5.3 Výpadek kabelu S1-S10_host STP s jinými hodnotami časovačů

S jinými hodnotami časovačů STP, tedy s hello time intervalem ve výchozím stavu 2 vteřin, forward delay 7 vteřin a max age 10 vteřin, výpadek trval 7 vteřin. Opět v mezích požadavků.

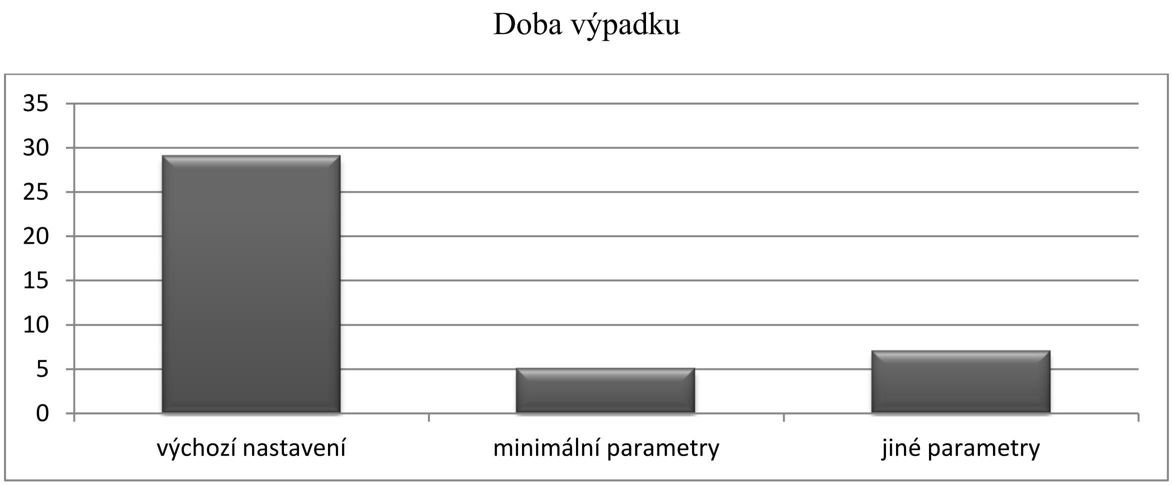


```
C:\Users\net102_2>ping -w 1000  1.1.1.1 -t

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 28 - Výpadek kabelu z S1 na S10_host ping - jiné hodnoty časovačů

6.5.4 Porovnání výpadků při různém nastavení časovačů STP - kabel

STP	hello time	forward delay	max age	doba výpadku
Výchozí	2s	15s	20s	29s
minimální	1s	4s	6s	5s
jiné	2s	7s	10s	7s

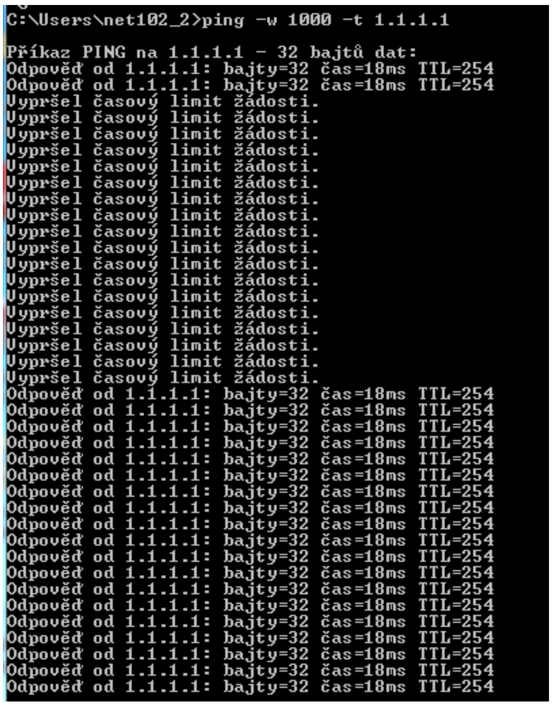


Obrázek 29 - Graf porovnání výpadků při různém nastavení časovačů STP - kabel

6.5.5 Výpadek kabelu S1-S10_host RSTP

Jak vypadal výpis na S1 při výpadku kabelu z S1 na S1_host na RSTP, je uvedeno v příloze E.

Ping vypadal následovně:



```
C:\Users\net102_2>ping -w 1000 -t 1.1.1.1

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

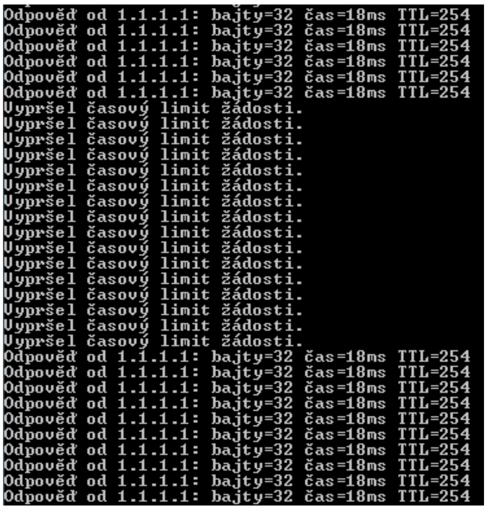
Obrázek 30 - Výpadek kabelu z S1 do S10_host ping

Výpadek trval 18s, lze tedy říci, že protokol RSTP je v tomto případě o 11s rychlejší než protokol STP ve výchozím nastavení ale pomalejší než když jsou nastavené nejnižší hodnoty časovačů na STP.

6.5.6 Výpadek dvou kabelů S1-S10_host a S1-S2 RSTP

Po výpadku obou kabelů z S1 do S10_host a z S1 do S2 (jeden trunk spoj) výpis vypadal na S1 tak, jak je uvedeno opět v příloze E.

A ping vypadal takto:



```
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 31 - Výpadek kabelů S1-S10_host a S1-S2 ping

Tento výpadek, ač dvou kabelů zároveň, trval méně než výpadek jednoho kabelu a to 16s.

6.6 Výpadek kabelu – zobrazení na HSRP

6.6.1 Výpadek kabelu R1-S1

Konfigurace směrovače R1 je stejná jako v kapitole 5.3, tedy v příloze D.

Testováním ping na bránu ISP se zjistilo, že výpadek trval 4s.

```
C:\Users\net102_2>ping -w 1000 -t 1.1.1.1

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 32 - Výpadek kabelu R1-S1 ping

Na směrovači R1 vypadala detekce výpadku takto:

```
R1#
*Aug  4 13:54:28.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Aug  4 13:54:28.487: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 10 state Active -> Init
R1#
```

Obrázek 33 - Výpadek kabelu R1-S1 na R1

Na směrovači R2 vypadala detekce výpadku a následné přepnutí ze záložního do aktivního stavu takto:

```
R2#
*Apr  7 07:02:34.307: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 10 state Standby
-> Active
R2#
```

Obrázek 34 - Výpadek kabelu R1-S1 na R2

6.7 Výpadek kabelu EIGRP

6.7.1 **Výpadek kabelu R1-ISP**

Pouze 1s trvalo přepnutí na záložní cestu z R1 na R2, zjištěním ping na bránu ISP z PC1.

```
C:\Users\net102_2>ping -w 1000 -t 1.1.1.1

Příkaz PING na 1.1.1.1 - 32 bajtů dat:
Odpověď od 1.1.1.1: bajty=32 čas=19ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Vypršel časový limit žádosti.
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
```

Obrázek 35 - Výpadek kabelu R1-ISP ping

Detekce výpadku na R1 vypadala takto:

```
R1#
*Aug  4 13:50:03.715: %LINK-3-UPDOWN: Interface Serial0/1/1, changed state to down
R1#
*Aug  4 13:50:03.719: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.40.2 (Serial0/1/1) is do
wn: interface down
*Aug  4 13:50:04.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed sta
te to down
```

Obrázek 36 - Výpadek kabelu R1-ISP na R1

Následné zprovoznění původní cesty po zapojení kabelu zpět se přepnulo téměř okamžitě z 27ms zpět na 18ms.

```
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=27ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
Odpověď od 1.1.1.1: bajty=32 čas=18ms TTL=254
```

Obrázek 37 - Obnovení cesty z R1 na ISP

7 ZÁVĚR

Cílem bakalářské práce bylo vysvětlení funkčnosti protokolů řešících redundanci v síti a problematiku failover. Pro názornější zobrazení byl popis kromě obecných vlastností těchto protokolů zaměřen na konkrétní protokoly EIGRP, STP v porovnán s RSTP a HSRP. Práce byla vytvořena na základě informací získaných během studia kurzu CCNA, vlastních zkušeností a dostudování informací z uvedené literatury.

V teoretické části byly nejdříve popsány principy STP a RSTP protokolů, jejich vzájemné porovnání a poté HSRP principy protokolu.

Praktická část bakalářské práce se věnuje případové studii v datacentru poskytovatele webových služeb. Studie zahrnuje názornou konfiguraci všech směrovačů a přepínačů datacentra, ve které jsou použity protokoly EIGRP, STP nebo RSTP a HSRP.

V první části případové studie je popsána konfigurace všech směrovačů a přepínačů, které se nacházejí v zadané konfiguraci. Případová studie tak ukázala rychlejší zpětnou vazbu protokolu RSTP nad STP a fungující přepínání na záložní zařízení a cesty protokolu obou protokolů STP nebo RSTP a HSRP. Případová studie byla zpracována na směrovačích a přepínačích Cisco. V simulátoru dostupném pro instruktory Networking Academy, studenty, absolventy a administrátory, kteří jsou registrovaní členové NetSpace, Packet Traceru pak na směrovačích Cisco s operačním systémem 12.4 a na přepínačích Cisco s operačním systémem 12.1. Vytvořený projekt je přiložen na CD a konfigurace všech směrovačů je přiložena v přílohách.

Bakalářská práce pro mě byla velice zajímavým tématem na vypracování a určitě by bylo praktickou část možné aplikovat na reálnou počítačovou síť i větších rozměrů. Pochopila jsem tuto problematiku tak, abych byla toto řešení schopná použít v praxi.

Zadání bylo splněno v rámci možností laboratoře a simulátoru Packet Tracer . V reálném prostředí, kde by se navrhovala počítačová síť nebo její záložní cesty, by bylo možné tuto práci rozšířit například o použití kombinace dalších směrovacích protokolů nebo jiných protokolů řešících redundanci. Menší problém by mohl nastat při výpadku jiného zařízení, než je směrovač, přepínač nebo kabel, na který tato studie byla testována ale s těmito znalostmi by nemělo trvat dlouho tento problém vyřešit.

8 POUŽITÁ LITERATURA

[1] Hucaby, David a McQuerry, Steve. Protokol HSRP. [autor knihy] David Hucaby a Steve McQuerry. *Konfigurace směrovačů Cisco.* Brno : Computer Press, 2004, 6.

[2] Hucaby, David. Rapid Spanning Tree Protocol. *CCNP BCMSN official certification guide.* Indianapolis : Cisco Press, 2007b, 11, pp. 263 - 266.

[3] Hucaby, David.. Hot Standby Router Protocol. *CCNP BCMSN offical exam certification guide.* 4. Indianapolis : Cisco Press, 2007c, 13, pp. 318-320.

[4] Cisco Systems, Inc. TCP/IP Overview - Cisco. *IP Routing.* [Online] 12 02, 2013. [Cited: 04 20, 2014.] http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html#tcpiptech. 13769.

[5] Hucaby, David. IEEE 802.1D Overview. *CCNP BCMSN official exam certification guide.* 4. Indianapolis : Cisco Press, 2007a, 8, pp. 185-207.

[6] Hucaby, David. *CCNP Switch 642-813 Official Cerftification Guide.* Indianapolis : Cisco Press, c2010. 978-1-58720-243-8.

[7] Hucaby, David.TRANSMISSION CONTROL PROTOCOL. *The Internet Engineering Task Force (IETF®).* [Online] 1981. [Citace: 03. 05 2014.] http://www.ietf.org/rfc/rfc793.txt.

[8] Transmission Control Protocol. *Wikipedie, otevřená encyklopedie.* [Online] 22. 2 2014. [Citace: 3. 5 2014.] http://cs.wikipedia.org/wiki/Transmission_Control_Protocol.

[9] BPDU FIELDS IN A BPDU FRAME. *Bel's Blog.* [Online] [Citace: 5. 5 2014.] http://beautbelsblog.wordpress.com/2010/05/14/bpdu-fields-in-a-bpdu-frame/.

[10] IEEE 802.1: 802.1Q - Virtual LANs. [Online] [Citace: 5. 5 2014.] http://www.ieee802.org/1/pages/802.1Q.html.

[11] IEEE Standards Status Report - 802.1D. *IEEE STANDARDS ASSOCIATION.* [Online] [Citace: 3. 5 2014.] http://standards.ieee.org/cgi-bin/status?Designation:%20802.1D.

[12] IEEE 802.1: 802.1w - Rapid Reconfiguration of Spanning Tree. [Online] [Citace: 5. 5 2014.] http://www.ieee802.org/1/pages/802.1w.html.

[13] RFC 2281. *Cisco Hot Standby Router Protocol (HSRP).* [Online] [Citace: 5. 5 2014.] http://www.ietf.org/rfc/rfc2281.txt.

[14] Hucaby, David. *CCNP BCMSN official certification guide.* Indianapolis : Cisco Press. 1-58729-171-2.

[15] Cisco Systems, Inc. *Stretnutie 5: Niektoré protokoly pre redundanciu.* [Prezentace]

PŘÍLOHA A – KONFIGURACE SMĚROVAČŮ A PŘEPÍNAČŮ

Směrovač ISP

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
!
!
!
ip cef
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
crypto pki token default removal timeout 0
!
!
!
!
license udi pid CISCO2801 sn FCZ131811YZ
!
redundancy
!
!
!
!
!
!
!
```

```
!
!
!nastaveni smycky
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 10.0.40.6 255.255.255.252
!
interface Serial0/1/1
 ip address 10.0.40.2 255.255.255.252
 clock rate 64000
!
!nastaveni EIGRP procesu cislo 1, zapnuti pro site 1.1.1.1/0, 10.0.40.0
0.0.0.255
router eigrp 1
 network 1.1.1.1 0.0.0.0
 network 10.0.40.0 0.0.0.255
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
```

```
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

Směrovač R1

```
!nastaveni jmena zarizeni
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip cef
!
!
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 10.0.20.2 255.255.255.0
 duplex auto
 speed auto
 standby 20 ip 10.0.20.1
 standby 20 priority 200
 standby 20 preempt
!
interface FastEthernet0/1
 ip address 10.0.10.2 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 10.0.10.1
 standby 10 priority 200
 standby 10 preempt
!
interface Serial0/1/0
 ip address 10.0.30.1 255.255.255.252
 clock rate 64000
!
interface Serial0/1/1
 ip address 10.0.40.1 255.255.255.252
!
!nastaveni EIGRP procesu cislo 1, zapnuti pro sit 10.0.0.0
!zapnuti pasivnich rozhrani
```

```
router eigrp 1
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 10.0.0.0
 auto-summary
!
ip forward-protocol nd
!
!
no ip http server
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

Směrovač R2

```
!nastaveni jmena zarizeni
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip cef
!
!
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 10.0.20.3 255.255.255.0
 duplex auto
 speed auto
 standby 20 ip 10.0.20.1
 standby 20 priority 100
```

```
 standby 20 preempt
!
interface FastEthernet0/1
 ip address 10.0.10.3 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 10.0.10.1
 standby 10 priority 100
 standby 10 preempt
!
interface Serial0/1/1
 ip address 10.0.30.2 255.255.255.252
!
interface Serial0/1/0
 ip address 10.0.40.5 255.255.255.252
 clock rate 64000
!
!nastaveni EIGRP procesu cislo 1, zapnuti pro sit 10.0.0.0
!zapnuti pasivnich rozhrani
router eigrp 1
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 10.0.0.0
 auto-summary
!
ip forward-protocol nd
!
!
no ip http server
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

Přepínač S1

```
!nastaveni jmena zarizeni
hostname S1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
!
!
!
```

```
!
!
!
!
!
!
!
!nastaveni STP a priority vlan 10 a 20
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 10,20 priority 24576
!
vlan internal allocation policy ascending
!
!
!
!
!
!nastaveni vlan a role portu rozhrani
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
```

```
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 no ip address
!
ip http server
ip http secure-server
!
!
line con 0
line vty 5 15
!
End
```

Přepínač S2

```
!nastaveni jmena zarizeni
hostname S2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
!
!
!vytvoreni vlan 10 a 20
vlan 10
name Development
exit
vlan 20
name Customers
exit
!
```

```
!
!
!
!
!nastaveni STP a priority vlan 10 a 20
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 10 root secondary
spanning-tree vlan 20 root secondary
!
vlan internal allocation policy ascending
!
!
!
!
!
!nastaveni vlan a role portu rozhrani
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
```

```
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 no ip address
!
ip http server
ip http secure-server
!
!
line con 0
line vty 5 15
!
end
```

PŘÍLOHA B - KONFIGURACE PŘEPÍNAČŮ NA STP

Přepínač S1

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0025.467e.b300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0025.467e.b300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/1               Desg FWD 19        128.1    P2p Edge
Fa0/3               Desg FWD 19        128.3    P2p
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/5               Desg FWD 19        128.5    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0025.467e.b300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0025.467e.b300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/2               Desg FWD 19        128.2    P2p Edge
Fa0/3               Desg FWD 19        128.3    P2p
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/6               Desg FWD 19        128.6    P2p
```

Přepínač S2

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0025.467e.b300
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
             Address     0025.467e.2400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/1               Desg FWD 19        128.1    P2p Edge
Fa0/3               Root FWD 19        128.3    P2p
Fa0/4               Altn BLK 19        128.4    P2p
Fa0/6               Altn BLK 19        128.6    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0025.467e.b300
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     0025.467e.2400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/2               Desg FWD 19        128.2    P2p Edge
Fa0/3               Root FWD 19        128.3    P2p
Fa0/4               Altn BLK 19        128.4    P2p
Fa0/5               Desg FWD 19        128.5    P2p
```

PŘÍLOHA C - KONFIGURACE PŘEPÍNAČE NA RSTP

Přepínač S1

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0025.467e.b300
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
             Address     0025.467e.2400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/1               Desg FWD 19        128.1    P2p Edge
Fa0/3               Root FWD 19        128.3    P2p
Fa0/4               Altn BLK 19        128.4    P2p
Fa0/6               Altn BLK 19        128.6    P2p

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0025.467e.b300
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     0025.467e.2400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/2               Desg FWD 19        128.2    P2p Edge
Fa0/3               Root FWD 19        128.3    P2p
Fa0/4               Altn BLK 19        128.4    P2p
Fa0/5               Altn BLK 19        128.5    P2p
```

PŘÍLOHA D - KONFIGURACE SMĚROVAČŮ NA HSRP

Směrovač S1

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       20   200 P Active  local           10.0.20.3       10.0.20.1
Fa0/1       10   200 P Active  local           10.0.10.3       10.0.10.1

R1#show standby
FastEthernet0/0 - Group 20
  State is Active
    2 state changes, last state change 00:23:07
  Virtual IP address is 10.0.20.1
  Active virtual MAC address is 0000.0c07.ac14
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.968 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.20.3, priority 100 (expires in 9.968 sec)
  Priority 200 (configured 200)
  Group name is "hsrp-Fa0/0-20" (default)
FastEthernet0/1 - Group 10
  State is Active
    2 state changes, last state change 00:22:59
  Virtual IP address is 10.0.10.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.420 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.10.3, priority 100 (expires in 8.568 sec)
  Priority 200 (configured 200)
  Group name is "hsrp-Fa0/1-10" (default)
```

Směrovač S2

```
R2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       20   100 P Standby 10.0.20.2       local           10.0.20.1
Fa0/1       10   100 P Standby 10.0.10.2       local           10.0.10.1

R2#show standby
FastEthernet0/0 - Group 20
  State is Standby
    10 state changes, last state change 00:12:39
  Virtual IP address is 10.0.20.1
  Active virtual MAC address is 0000.0c07.ac14
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.744 secs
  Preemption enabled
  Active router is 10.0.20.2, priority 200 (expires in 8.732 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/0-20" (default)
FastEthernet0/1 - Group 10
  State is Standby
    10 state changes, last state change 00:12:38
  Virtual IP address is 10.0.10.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.188 secs
  Preemption enabled
  Active router is 10.0.10.2, priority 200 (expires in 9.188 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/1-10" (default)
```

PŘÍLOHA E - KONFIGURACE PŘEPÍNAČŮ NA RSTP PŘI VÝPADKU KABELU/Ů

Přepínač S1

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0025.467e.b300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0025.467e.b300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/1               Desg FWD 19        128.1    P2p Edge
Fa0/3               Desg FWD 19        128.3    P2p
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/5               Desg FWD 19        128.5    P2p

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0025.467e.b300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0025.467e.b300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/2               Desg FWD 19        128.2    P2p Edge
Fa0/3               Desg FWD 19        128.3    P2p
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/6               Desg FWD 19        128.6    P2p
```

Přepínač S2

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0025.467e.b300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0025.467e.b300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/1               Desg FWD 19        128.1    P2p Edge
Fa0/4               Desg FWD 19        128.4    P2p


VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0025.467e.b300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0025.467e.b300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
-------
Fa0/2               Desg FWD 19        128.2    P2p Edge
Fa0/4               Desg FWD 19        128.4    P2p
Fa0/6               Desg FWD 19        128.6    P2p
```