

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ZVYŠOVÁNÍ SPOLEHLIVOSTI KOMUNIKAČNÍ SÍŤE

INCREASING RELIABILITY OF COMMUNICATION NETWORKS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Richard Hausner

VEDOUCÍ PRÁCE

SUPERVISOR

prof. Ing. Jaroslav Koton, Ph.D.

BRNO 2021

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Richard Hausner

ID: 211496

Ročník: 3

Akademický rok: 2020/21

NÁZEV TÉMATU:

Zvyšování spolehlivosti komunikační sítě

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte problematiku stohování, klastrování a kaskádování síťových prvků. Popište a porovnejte jednotlivé přístupy. Na základě získaných poznatků o místě nasazení jednotlivých přístupů vytvořte sady scénářů, na kterých bude možné ukázat charakteristické vlastnosti každého z nich, jako propustnost, spolehlivost provozu.

DOPORUČENÁ LITERATURA:

[1] Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE, dostupné online: <https://bit.ly/3mvGpay>, [cit.: 2020-09-14]

[2] Sakandar, B., Barnes, D.: Cisco LAN Switching Fundamentals, ISBN: 1587058499, 2004.

Termín zadání: 1.2.2021

Termín odevzdání: 31.5.2021

Vedoucí práce: prof. Ing. Jaroslav Koton, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Abstrakt

Bakalářská práce se zabývá vybranými možnostmi zvyšováním spolehlivosti komunikačních sítí. V rámci práce jsou popsány základní protokoly a topologie sítí. Ve druhé kapitole jsou probrány technologie kaskádování, klastrování a stohování síťových přepínačů. Jsou popsány scénáře zapojení a výsledky praktických pokusů, na základě kterých je navrženo (doporučeno) použití (využití) v praxi.

Klíčová slova

Kaskádování, klastrování, redundance, síťové protokoly, stohování, topologie sítě.

Abstract

The bachelor's thesis deals with selected options for increasing reliability of communication networks. The basic protocols and network topologies are described in the thesis. In the second section the technologies of cascading, clustering and stacking network switches are discussed. The practical experiments and scenerios of connections, which are described in the aforementioned section, form a basis of their practical use proposal.

Keywords

Cascading, clustering, redundancy, network protocols, stacking, network topology.

Bibliografická citace

HAUSNER, Richard. *Zvyšování spolehlivosti komunikační sítě* [online]. Brno, 2021 [cit. 2021-05-31]. Dostupné z: <https://www.vutbr.cz/studenti/zav-prace/detail/133390>. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Jaroslav Koton.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	<i>Richard Hausner</i>
VUT ID studenta:	<i>211496</i>
Typ práce:	<i>Bakalářská práce</i>
Akademický rok:	<i>2020/21</i>
Téma závěrečné práce:	<i>Zvyšování spolehlivosti komunikační sítě</i>

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne: 31. května 2021

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce Prof. Ing. Jaroslavovi Kotonovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne:

podpis autora

Obsah

SEZNAM OBRÁZKŮ	8
SEZNAM TABULEK.....	9
ÚVOD	10
1. TEORETICKÝ ÚVOD	11
1.1 JEDINÝ BOD SELHÁNÍ.....	11
1.2 ZÁKLADNÍ TOPOLOGIE SÍTÍ.....	11
1.3 TOPOLOGIE SÍTÍ SE ZVÝŠENOU SPOLEHLIVOSTÍ	14
1.3.1 <i>Loukoťové kolo</i>	15
1.3.2 <i>Jehlan</i>	16
1.3.3 <i>Kostka</i>	16
1.4 PROTOKOLY PRO ŘÍZENÍ REDUNDANCE V SÍTÍCH	19
1.4.1 <i>Univerzální protokoly</i>	20
1.4.2 <i>Protokoly pro řízení kruhových sítí</i>	22
1.4.3 <i>Další protokoly</i>	23
1.5 AKTIVNÍ PRVKY SÍTÍ.....	23
1.6 ZÁLOŽNÍ NAPÁJENÍ.....	25
1.7 BEZPEČNÉ ULOŽENÍ SÍŤOVÝCH PRVKŮ	26
1.8 SERVERY S VYSOKOU DOSTUPNOSTÍ	27
2. STOHOVÁNÍ, KLASTROVÁNÍ A KASKÁDOVÁNÍ PŘEPÍNAČŮ	30
2.1 VÝCHOZÍ SCÉNÁŘ.....	30
2.2 STOHOVÁNÍ PŘEPÍNAČŮ	31
2.2.1 <i>Scénář zapojení číslo 1</i>	32
2.2.2 <i>Scénář zapojení číslo 2</i>	33
2.3 KLASTROVÁNÍ PŘEPÍNAČŮ	34
2.3.1 <i>Scénář zapojení číslo 3</i>	36
2.4 KASKÁDOVÁNÍ PŘEPÍNAČŮ	37
2.4.1 <i>Scénář zapojení číslo 4</i>	38
2.5 PRAKTICKÉ POKUSY	41
ZÁVĚR	47
LITERATURA.....	48
SEZNAM SYMBOLŮ A ZKRATEK	49

SEZNAM OBRÁZKŮ

Obrázek 1.1: Příklad SPOF a jeho důsledek [1]	11
Obrázek 1.2: Topologie sběrnice	12
Obrázek 1.3: Topologie hvězda	12
Obrázek 1.4: Topologie kruh	13
Obrázek 1.5: Topologie strom	13
Obrázek 1.6: Topologie polygon a neúplný polygon.....	14
Obrázek 1.7: Topologie sítě zobrazené v prostoru [7].....	14
Obrázek 1.8: Loukoťové kolo, centrální prvek	15
Obrázek 1.9: Loukoťové kolo, kruh.....	16
Obrázek 1.10: Topologie jehlan.....	16
Obrázek 1.11: Topologie kostka zobrazená ve 3D a 2D prostoru.....	17
Obrázek 1.12: Příklad řízení topologie kostka [6]	17
Obrázek 1.13: Jednoduchý Sub-Ring [5].....	18
Obrázek 1.14: Složitější varianta Sub-Ringu [5]	18
Obrázek 1.15: Další zapojení Sub-Ringu [5]	19
Obrázek 1.16: Nevhodná varianta zapojení Sub-Ringu [5]	19
Obrázek 1.17: Ring Coupling [4].....	23
Obrázek 1.18: Přepínač komunikačního systému napájený přes záložní zdroj.....	26
Obrázek 1.19: Dočasná kabeláž	27
Obrázek 1.20: Dočasné několika leté uložení přepínače.....	27
Obrázek 1.21: Vyvážený server [10]	28
Obrázek 1.22: Failover [10].....	29
Obrázek 1.23: Konfigurace a) aktivní-aktivní b) aktivní-pasivní [10].....	29
Obrázek 2.1: Výchozí scénář zapojení.....	31
Obrázek 2.2: Propojení přepínačů speciálním kabelem do stohu [9].....	32
Obrázek 2.3: Scénář stoh	33
Obrázek 2.4: Zapojení z managementu přepínače	34
Obrázek 2.5: Objevení nových přepínačů [3]	35
Obrázek 2.6: Hlavní a pohotovostní přepínač klastru [3]	36
Obrázek 2.7: Klastr s vytvořenými záložními spoji.....	37
Obrázek 2.8: Kaskádování přepínačů kombinované s LACP [6]	38
Obrázek 2.9: Kaskáda bez záložních spojů.....	39
Obrázek 2.10: Scénář kaskáda	40
Obrázek 2.11: Průběh stahování 1	41
Obrázek 2.12: Rozpojení kruhu v managementu přepínače	42
Obrázek 2.13: Průběh stahování 2	43
Obrázek 2.14: Průběh stahování 3	43
Obrázek 2.15: Ukázka výpisu z managementu přepínače.....	44
Obrázek 2.16: Průběh stahování 4	45
Obrázek 2.17: Ztrátovost po přenosu.....	46
Obrázek 2.18: Graf ztrát a přenesených paketů	46

SEZNAM TABULEK

Tabulka 1 Porovnání stavů portů RSTP vs STP	21
---	----

ÚVOD

V současném moderním světě se stále více spoléháme na počítačové sítě, které jsou velice často nutností a již si bez nich nedokážeme představit život. Počítačové sítě jsou pro řadu firem nutností jak k jejich fungování tak i získávání finančního kapitálu. V případě nedostupnosti sítě, to může znamenat vážné problémy nejen pro podnikatele a banky, ale i pro celou veřejnou a státní správu. V současné době jsou z důvodu distanční výuky kladeny zvýšené požadavky na spolehlivost sítí. Spolehlivost komunikačních sítí je dnes významným parametrem a je na předním místě při návrhu sítě. Spolehlivost by se měla řešit na více úrovních, jak na úrovni elektronických součástek či dílů tak i na úrovni síťových uzlů nebo spojů a nakonec i na úrovni sítě, jako celku.

Sítě si můžeme hierarchicky dle modelu firmy Cisco rozdělit do tří vrstev. Přístupová síť umožňuje přístup koncových uživatelů k síti. Distribuční síť propojuje přístupovou a páteřní síť. Nejdůležitější je páteřní síť, přes ni proudí veškerý provoz rozlehlých počítačových sítí jako například celosvětové sítě internet. V případě výpadku některého prvku je nutné mít minimálně jednu záložní cestu. Proto využíváme redundanci, jejímž smyslem je snížení možnosti výpadku počítačové sítě v případě selhání některého z prvků sítě.

Z pohledu uživatele je ovšem nejdůležitější přístupová síť. Zvýšení spolehlivosti na této síti lze provést použitím různých způsobů zapojení prepínačů. Mezi tato zapojení patří i kaskádování, klastrování a stohování prepínačů. Právě těmto technikám se dále věnuje tato bakalářská práce.

1. TEORETICKÝ ÚVOD

V této kapitole budou představeny základní topologie sítí, sítě se zvýšenou redundancí, protokoly používané pro řízení těchto komunikačních sítí, aktivní prvky používané v počítačových sítích.

Spolehlivost komunikační sítě musí být řešena jako celek od návrhu samotné topologie až po výběr jednotlivých komponent sítě.

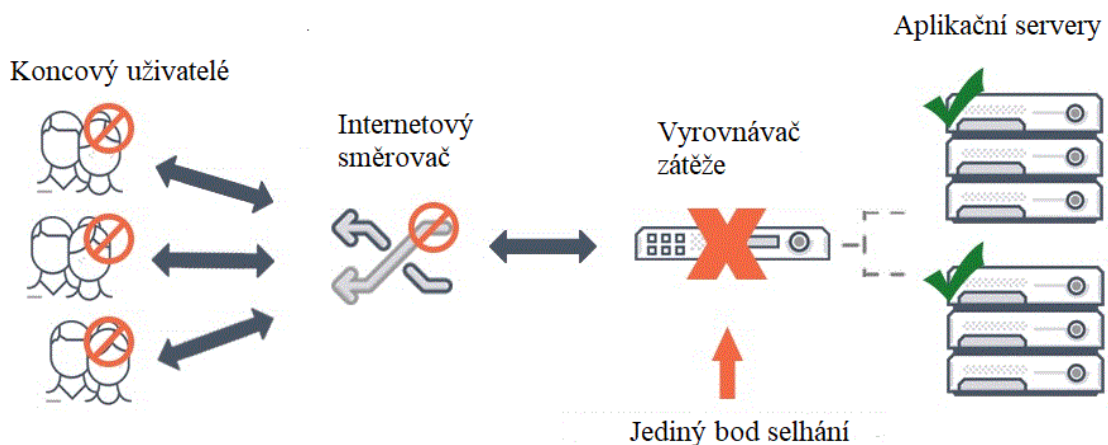
Důležitým parametrem sítě je propustnost, která udává, jaké množství dat lze za jednotku času sítí přenést.

1.1 Jediný bod selhání

V angličtině se tento termín označuje jako Single Point of Failure (SPOF). Tento jediný bod selhání v síti, je vlastně chybou v návrhu nebo konfiguraci obvodu nebo součásti. Tato chyba může představovat riziko, kdy i jedna porucha způsobí nefunkčnost celého systému. Například výpadek jednoho přepínače může způsobit, nedostupnost všech serverů a tím omezit práci ve firmě. [1]

Jednotlivé body selhání jsou nežádoucí pro systémy, které vyžadují vysokou dostupnost a spolehlivost, jako je státní a veřejná zpráva, velké dodavatelské logistické řetězce, sítě a softwarové aplikace. [1]

Základem zabránění vzniku SPOF je redundance. Pokud některá součást počítačové sítě selže, měla by ji okamžitě nahradit jiná součást. [1]



Obrázek 1.1: Příklad SPOF a jeho důsledek [1]

1.2 Základní topologie sítí

Síťová topologie popisuje vzájemné upořádání a propojení jednotlivých prvků sítě. Topologii sítí dělíme nejen způsobem propojení jednotlivých prvků, ale i její dimenzí (1D, 2D, 3D, 4D).

Sběrnice (Bus)

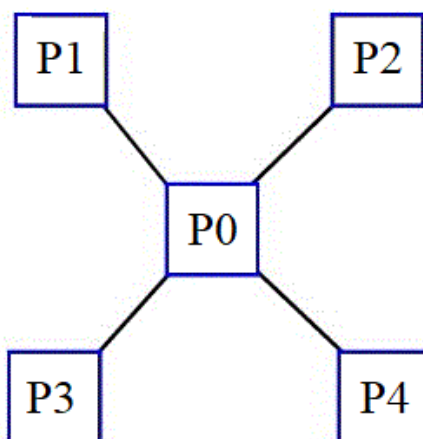
V této topologii jsou všechny prvky připojené ke sdílenému přenosovému médiu. Výhodou této topologie je její jednoduchost. Nevýhodou je složitější proces přístupu a řízení přenosu dat a navíc se všechna zařízení musí dělit o společnou přenosovou kapacitu. Čím větší počet zařízení bude připojen, tím více bude docházet ke kolizím, které budou snižovat spolehlivost. [6]



Obrázek 1.2: Topologie sběrnice

Hvězda (Star)

Tato topologie má jeden centrální prvek, ke kterému jsou připojeny ostatní prvky sítě. Centrálním prvkem může být například hub nebo přepínač. Přerušení jednoho připojovacího kabelu nenaruší provoz celé sítě. Výpadek celé sítě může způsobit nefunkčnost centrálního prvku. [6]

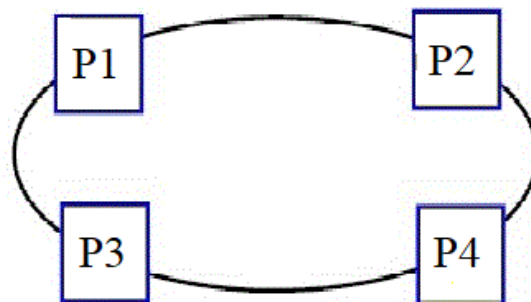


Obrázek 1.3: Topologie hvězda

Kruh (Ring)

V topologii kruh jsou všechny prvky na společném přenosovém médiu podobně jako u topologie sběrnice, ale na rozdíl od sběrnice je médium uzavřeno do kruhu.

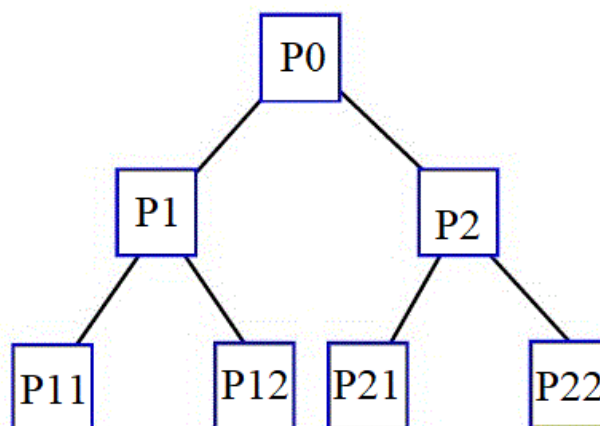
Komunikace v síti probíhá předáváním přes ostatní prvky sítě.[6]



Obrázek 1.4: Topologie kruh

Strom (Tree)

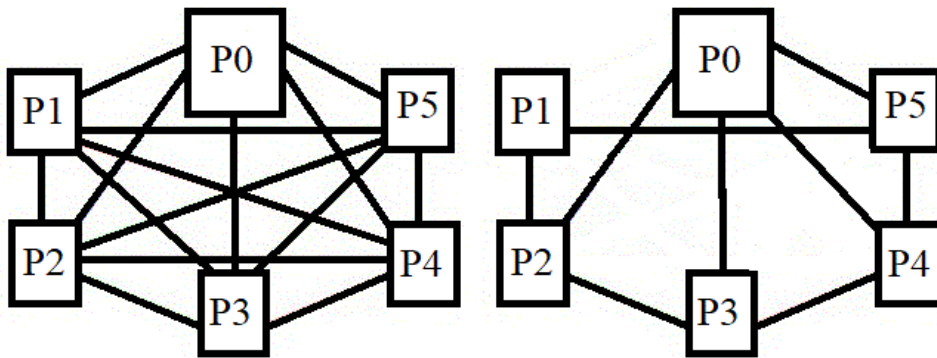
Topologie strom vznikla hierarchickým spojením topologie hvězda. Přerušení některého prvku, způsobí vyřazení příslušné větve stromu. [6]



Obrázek 1.5: Topologie strom

Polygon

Tato topologie vychází z topologie hvězda a je možné propojit všechny prvky navzájem. Všechny prvky jsou si rovnocenné a při přerušení některého spoje existuje mnoho redundantních spojení. Často také vzniká neúplný polygon. [6]

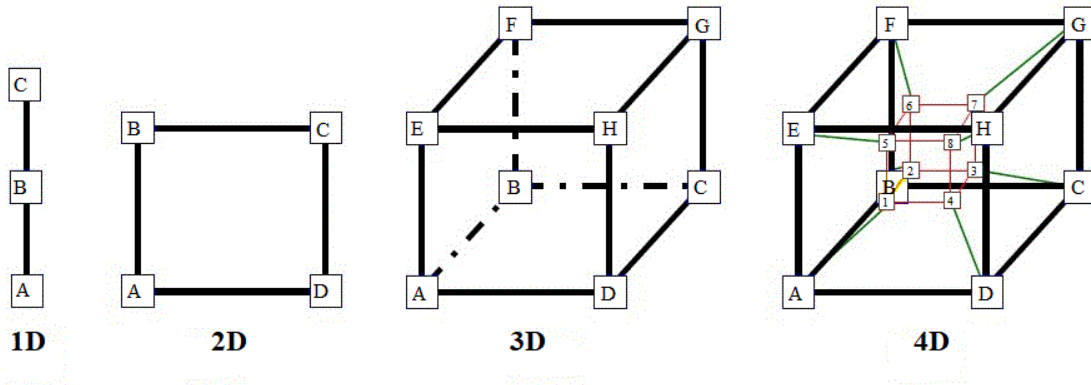


Obrázek 1.6: Topologie polygon a neúplný polygon

Dimenze topologií

Sítě můžeme, kromě výše uvedených topologií rozdělit i podle prostoru. [6]

- 1D je jednorozměrný prostor, který můžeme znázornit na ose x.
- 2D je dvojrozměrný prostor, který popisujeme pomocí os x a y.
- 3D je trojrozměrný prostor, který můžeme vyjádřit pomocí os x, y a z.
- 4D přidává k 3D prostoru čas a tento prostor je prezentován tesseractem.



Obrázek 1.7: Topologie sítí zobrazené v prostoru [7]

Díky popisu topologie v různých dimenzích máme reálnější představu o konkrétním rozmístění prvků v prostoru a komunikačních vazbách.

1.3 Topologie sítí se zvýšenou spolehlivostí

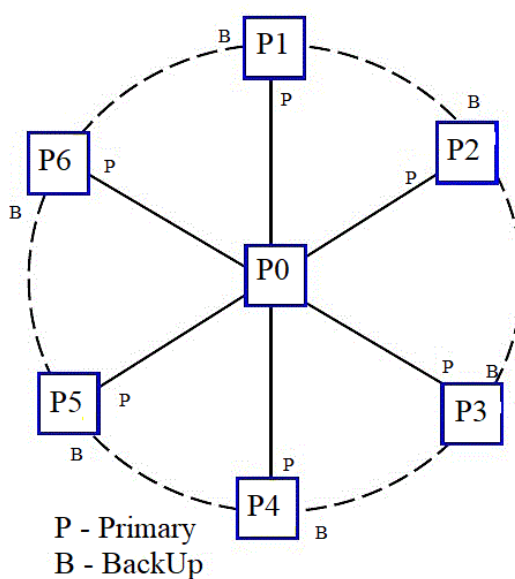
Některými úpravami vzájemného propojení prvků, můžeme dosáhnout sítí se zvýšenou spolehlivostí vůči výpadku některého prvku. Protokoly pro řízení kruhových sítí jsou popsány v kapitole 1.4, podkapitole 1.4.2.

1.3.1 Loukoťové kolo

Tato topologie se vytváří jednoduchou úpravou základní topologie hvězda. Krajní prvky jsou v této topologii propojené do kruhu. Je několik možností jak tuto topologii řídit. [6]

Centrální prvek

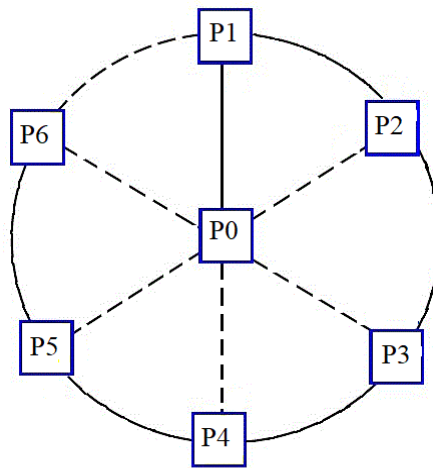
V této variantě vedou k centrálnímu prvku hlavní linky od okrajových prvků a záložní cesta je okrajový kruh. Na každém okrajovém prvku je port směřující k centrálnímu prvku nastaven jako primární (P), druhý port jako záložní (B – BackUp) a třetí port zůstává nenastaven. Záložní linka musí být vždy jedním směrem. [6]



Obrázek 1.8: Loukoťové kolo, centrální prvek

Kruh

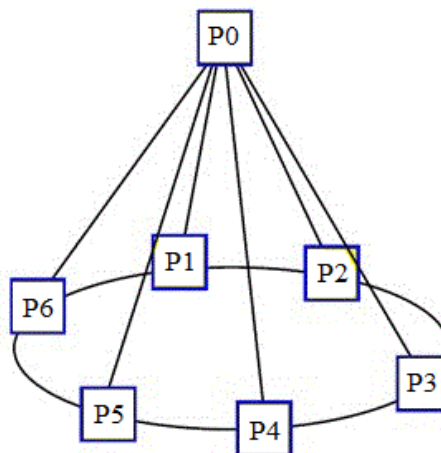
V této variantě je hlavní komunikační cestou kruh a záložní jsou přímé spoje s hlavním prvkem. Je důležité, aby linky v kruhu byly nastaveny jako primární a linky směrem k centrálnímu prvku jako záložní. [6]



Obrázek 1.9: Loukoťové kolo, kruh

1.3.2 Jehlan

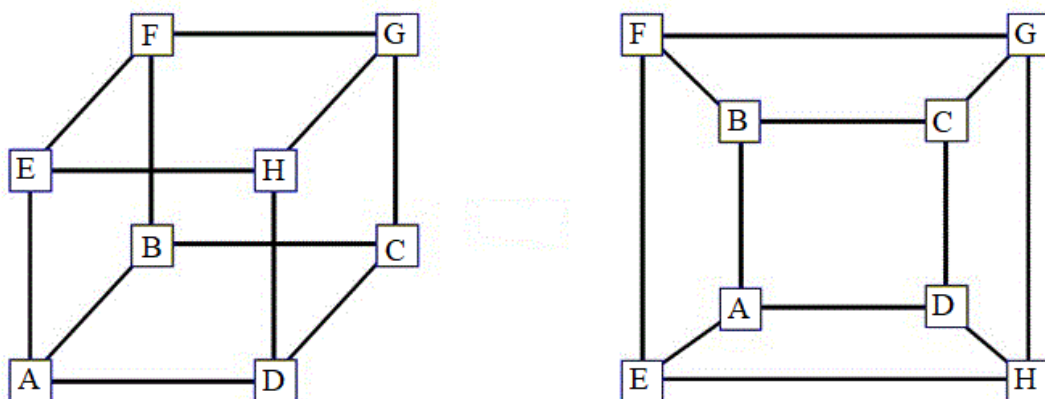
Topologie jehlan vychází z topologie loukoťové kolo, ale je zobrazena ve 3D prostoru a umožňuje konkrétnější představu o rozmístění aktivních prvků v prostoru. [7]



Obrázek 1.10: Topologie jehlan

1.3.3 Kostka

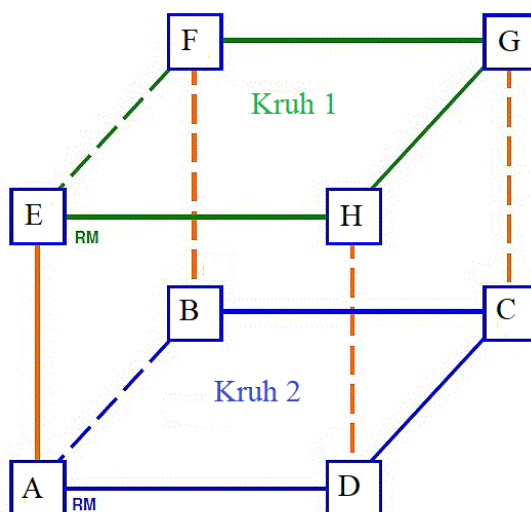
Tato topologie se dá zakreslit jak ve 2D prostoru tak i ve 3D prostoru. Tuto topologii je možné řídit několika způsoby, podobně jako loukoťové kolo, jeden z příkladů je uveden níže. Složením několika kostek na sebe vznikne topologie věž. [7]



Obrázek 1.11: Topologie kostka zobrazená ve 3D a 2D prostoru

Příklad řízení topologie kostka

Spodní plocha kostky tvoří jeden kruh a horní plocha druhý kruh. Z prvku A je vedena aktivní linka do horního kruhu, uzly B, C a D jsou záložní. V každém kruhu je nutné na jednom přepínači použít protokol pro řízení kruhu (Ring Manager) více viz 1.4.2. [6]



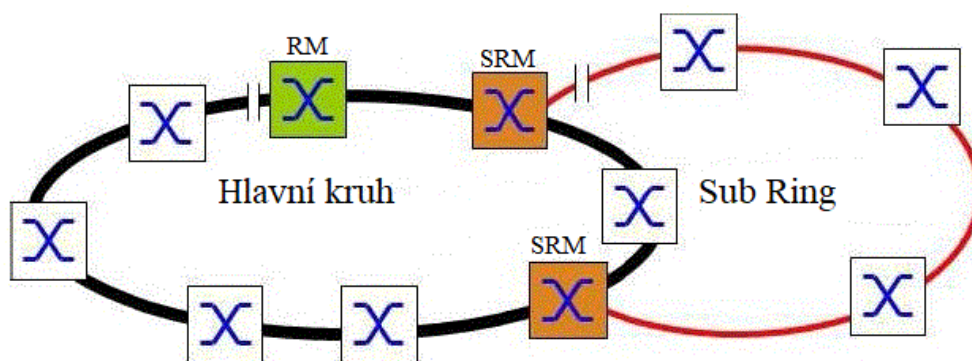
Obrázek 1.12: Příklad řízení topologie kostka [6]

Sub-Ring

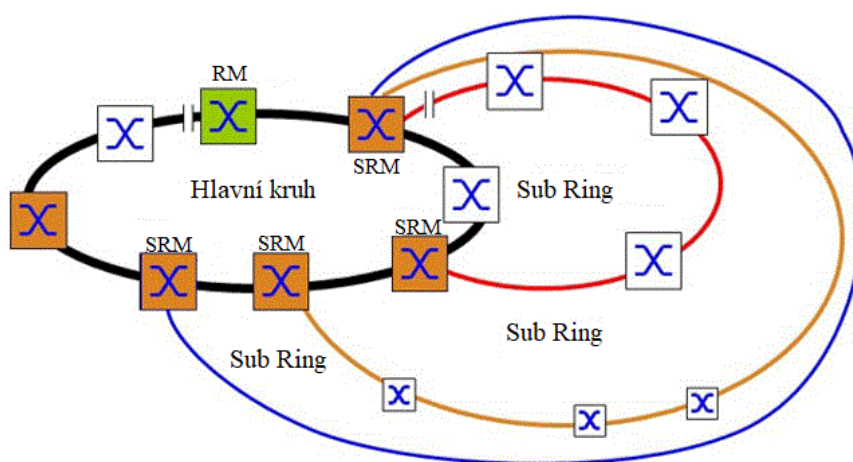
Je patentované proprietární řešení, které umožňuje jednoduché rozšíření základního kruhu o nové redundantní prvky sítě. Tyto prvky můžeme přidávat i za provozu základního kruhu. [4]

Sub-Ring Manager (SRM) je přepínač, který je součástí základního kruhu a je přes něj připojen Sub-Ring. Jeden SRM má funkci Manager a druhý má funkci Redundancy Manager. [4]

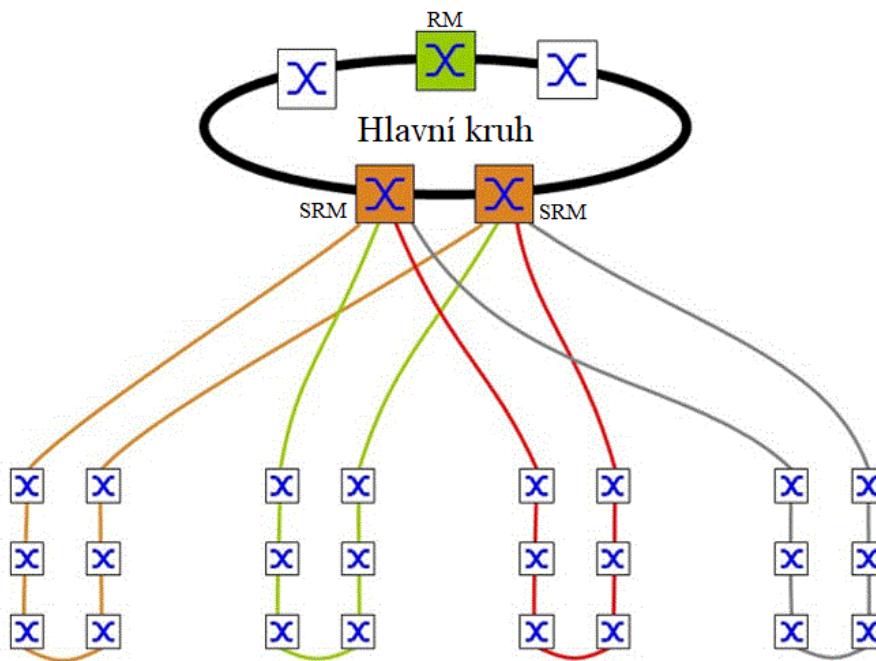
V každém Sub-Ringu může být až 200 prvků, SRM se mezi ně nepočítají. Začátky a konce Sub-Ringů lze libovolně kombinovat mezi jednotlivými uzly základního kruhu. Čas přepnutí Sub-Ringu na redundantní trasu bývá obvykle menší než 100 ms. [4]



Obrázek 1.13: Jednoduchý Sub-Ring [5]

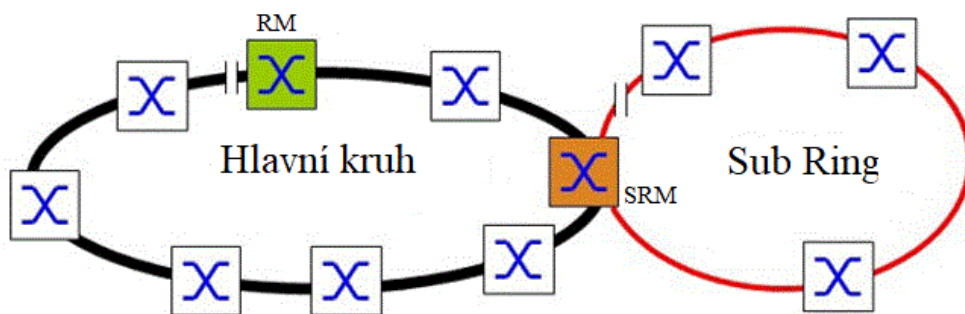


Obrázek 1.14: Složitější varianta Sub-Ringu [5]



Obrázek 1.15: Další zapojení Sub-Ringu [5]

Jako velice nevhodnou možností, z pohledu redundance, je vytvoření Sub-Ringu, u kterého sub ring začíná i končí na stejném prvku (viz. Obrázek 1.16). V tomto případě vzniká riziko, že při výpadku SRM, dojde ke ztrátě komunikace v celém Sub-Ringu. [4]



Obrázek 1.16: Nevhodná varianta zapojení Sub-Ringu [5]

1.4 Protokoly pro řízení redundance v sítích

Vzájemným propojováním přepínačů vícero linkami sice zvyšujeme redundanci, ale zároveň se zvyšuje možnost vzniku smyček. Bez dodatečného ošetření mohou tyto smyčky způsobit řadu problémů (v kritických případech i nedostupnost sítě). Z tohoto

důvodu vzniklo několik protokolů pro řízení redundance v sítích.

1.4.1 Univerzální protokoly

Spanning Tree Protocol (STP)

STP byl standardizován organizací IEEE pod označením 802.1D. Jde o síťový protokol, který pracuje na linkové vrstvě a je převážně implementován do přepínačů. Hlavním důvodem pro jeho používání je zabránění vzniku nežádoucích smyček v síti. [4]

Pomocí Spanning Tree Algoritmu (STA, Spanning Tree Algorithm) vytvoří STP v síti topologii stromu, která neobsahuje žádnou smyčku. Linky, které nejsou součástí vytvořeného stromu, jsou zablokovány a tím je ponechána jediná cesta mezi libovolnými uzly sítě. [4]

Topologie stromu je vytvořena následujícím postupem:

- Výběr root přepínače – ten je zvolen na základně nejnižší hodnoty identifikátoru Bridge ID, který je tvořen správcem konfigurovatelnou prioritou přepínače (první 2 B) a jeho MAC adresou (6B). Jako kořenovým je zvolen přepínač s nejnižší hodnotou priority. V případě, stejné priority, je zvolen ten s nejnižší MAC adresou. [4]
- Zjišťování nejlepších cest, volba portů root a designated – každý přepínač zjistí cenu všech cest k root přepínači a vybere tu s nejnižší cenou cesty. Port propojující přepínač s touto cestou je označen jako root port. Přepínače také zjišťují, který přepínač má nejnižší cenu cesty ze síťového segmentu k root přepínači. Port propojující tento přepínač k síťovému segmentu je označen jako designated port. [4]
- Blokace ostatních cest k root přepínači – každý port, který není ve stavu root port, nebo designated port musí být zablokován - blocked port. [4]

Pro vzájemnou informovanost mezi přepínači se používá zvláštní typ rámců, které se nazývají BPDU (Bridge Protocol Data Unit). Rámce se vysílají každé dvě sekundy. Máme tři typy těchto rámců:

- Konfigurační BPDU – Používají se při výpočtu kostry grafu a pro poskytnutí informací všem přepínačům. [4]
- Topology Change Notification (TCN) – Informace o změně v síťové topologii. [4]
- Topology Change Acknowledgment (TCA) – Potvrzení příjmu zprávy TCN. [4]

Spanning Tree Protocol definuje následující stavy portů přepínačů:

- Blocking – Nepřepošílají se přes něj žádná data, ale přijímá BPDU rámce.
- Listening – Přepínač přijímá a vysílá BPDU rámce a čeká na informace, které by způsobily návrat portu do blokujícího stavu. V tomto stavu se naplňuje tabulky MAC adres a nepřepošílají se datové rámce.

- Learning – Port nepřeposílá rámce, ale už naplňuje tabulku MAC adres podle přijatých rámců.
- Forwarding – Port přímá i odesílá data a monitoruje BPDU, aby přešel do blokujícího stavu v případě vzniku smyčky.
- Disabled – Port je vypnutý.

Velkou nevýhodou protokolu STP je dlouhá doba rekonfigurace při změně topologie nebo konfiguraci. Tato doba je standardně do 50 sekund. [4]

Rapid Spanning Tree Protocol (RSTP)

Oproti STP vylepšený RSTP snižuje dobu rekonfigurace maximálně na 2 sekundy. Zároveň byl vytvořen nový formát rámců BPDU a přepínače bez podpory RSTP těmto novým rámcům nerozumí a zahazují je. Rámce BPDU jsou vysílány každé 2s a pokud na libovolném portu nebude doručen 3x za sebou, dojde ke ztrátě spojení. [4]

V RSTP existují celkem tři stavy portů, stavy disabled, blocking a listening byly sjednoceny do stavu discarding. Vlastnosti stavů portů s porovnáním RSTP a STP jsou uvedeny níže, viz Tabulka 1. [4]

Tabulka 1 Porovnání stavů portů RSTP vs STP

Stav portu STP	Stav portu RSTP	Port je součástí aktivní topologie	Port se učí MAC adresy
Disabled	Discarding	Ne	Ne
Blocking	Discarding	Ne	Ne
Listening	Discarding	Ano	Ne
Learning	Learning	Ano	Ano
Forwarding	Forwarding	Ano	Ano

Parallel Redundancy Protocol (PRP)

Tento protokol má proti STP téměř nulovým čas na rekonfiguraci sítě a je nezávislý na topologii. Každý uzel má dva porty, které mají stejnou MAC adresu i IP adresu. Každý z těchto portů je napojen do jedné ze dvou fyzicky oddělených paralelně fungujících sítí. [4]

Každý dvojnásobně připojený uzel s PRP má rozhraní pro každou LAN. Zdroj odešle rámec současně do obou LAN, cíl dostane v běžném provozu oba rámce a zahodí

duplikát. Jednotlivě připojené zařízení obdrží pouze jeden rámeček. Pokud selže jedna LAN, pracuje s rámy z druhé LAN. [4]

1.4.2 Protokoly pro řízení kruhových sítí

Ring Manager (RM)

RM propojuje konce linky na redundantní kruh a udržuje uzavřenou redundantní linku. V případě nefunkčnosti některého prvku otevře redundantní linku na funkční lineární strukturu. [4]

Media Redundancy Protocol (MRP)

Tento protokol může řídit kruhovou síť, která obsahuje až 50 zařízení s časovým limitem rekonfigurace 500ms nebo 200ms. Všechny prvky zařazené do kruhu musí tento protokol podporovat. Jeden přepínač má funkci Media Redundancy Manager (MRM), který monitoruje, řídí kruh a reaguje na případné selhání sítě, ostatní jsou nastaveni jako Media Redundancy Clienti (MRC). [4]

Kontrola funkčnosti kruhu se provádí posíláním testovacích rámečků jedním ring portem a na druhém se kontroluje jejich přijetí. Proces se potom opakuje v opačném směru. Media Redundancy Clienti (MRC) přepošílají testovací rámeček od MRM z jednoho portu na druhý a zároveň reagují na rámeček informující o změně topologie. Zároveň oznamují MRM změny stavu svých portů. Výhodou tohoto protokolu proti RSTP je to, že testovací rámeček jsou ihned přepošílány na druhý ring port a tím dochází k menšímu zpoždění. [4]

HiPer Ring (HR)

HR podporuje až 100 přepínačů v kruhové síti s délkou kruhu až 3 000km a vzdáleností dvou sousedních přepínačů do 100km. Maximální přípustná doba rekonfigurace pro 100 přepínačů a maximální délku kruhu je 500ms. Typická doba přepnutí na záložní trasu při uvedené velikosti sítě je 250 až 270ms. Každých 20ms vysílá Ring Manager (RM) testovací rámeček, podobně jako u MRP, ale pouze jedním směrem a tím testuje správnou funkci kruhu. Díky tomu má rychlejší rekonfiguraci na záložní trasu a umožňuje agregaci linek mezi přepínači (více o agregaci linek viz podkapitola 1.4.3). Tento protokol není kompatibilní s RSTP. [4]

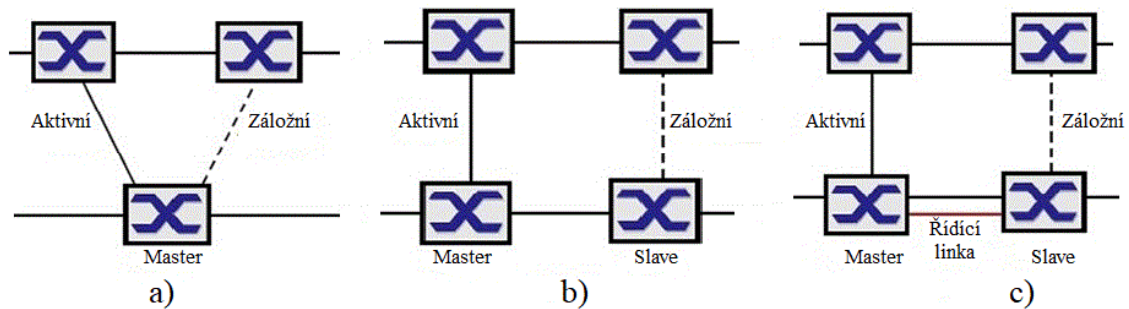
Ring Coupling

Ring Coupling umožňuje propojení dvou a více kruhů. Toto propojení je možné třemi způsoby. [4]

V první variantě (viz Obrázek 1.17 bod a)) se jeden přepínač jednoho kruhu připojí dva přepínače druhého kruhu. [4]

Ve druhé variantě (viz Obrázek 1.17 bod b)) se oba kruhy propojí samostatnými dvěma přepínači jednoho kruhu s dvěma přepínači druhého kruhu. Jeden z přepínačů je řídicí (Master) a druhý podřízený (Slave). [4]

Ve třetí variantě (viz Obrázek 1.17 bod c)) je propojení stejné jako ve druhé variantě a navíc je doplněno ještě o řídicí linku mezi přepínačem Master a Slave. [4]



Obrázek 1.17: Ring Coupling [4]

1.4.3 Další protokoly

Agregace linek

LACP (Link Aggregation Control Protocol – IEEE 802.3ad) je protokol pro sloučení fyzických linek do jednoho komunikačního kanálu (trunku) a tím dosáhneme větší šířky pásma komunikačního kanálu. [4]

Při sloučení minimálně dvou linek do jednoho kanálu můžeme trunk nastavit do dvou režimů a to redundance nebo vyrovnávání zátěže (Load Balancing). [4]

V režimu redundance je jedna linka aktivní a druhá záložní, která je aktivována v případě výpadku aktivní linky. [4]

V režimu vyrovnávání zátěže se rozděluje automaticky zátěž mezi linky dle aktuální zátěže linky. [4]

Link Backup

Link Backup umožňuje řízení redundance mezi třemi prvky, nastavením hlavního a záložního portu na řídicím přepínači. [4]

1.5 Aktivní prvky sítě

Aktivní prvky sítě slouží k vzájemnému propojení jednotlivých síťových segmentů. Kvalitní aktivní prvky jsou základem každé počítačové sítě. Činnost těchto prvků závisí na tom, jaké protokoly používají.

Jednotlivá zařízení propojující síť můžeme rozdělit podle toho na, které vrstvě modelu ISO/OSI pracují:

- Zařízení fyzické vrstvy: opakovač (repeater) a rozbočovač (hub).
- Zařízení linkové vrstvy: most (bridge) a přepínač (switch).
- Zařízení síťové vrstvy: smerovač (router).
- Zařízení transportní až aplikační vrstvy: brána (gateway).

Opakovač (Repeater)

Hlavním úkolem opakovače je přenést a zesílit přijatý signál do ostatních připojených prvků. Nemá vnitřní paměť, je nezávislý na protokolech vyšších vrstev. Při průchodu signálu opakovačem dochází k mírnému zpoždění signálu a proto je množství opakovačů omezené. [8]

Rozbočovač (Hub)

Hlavní funkcí rozbočovače je možnost rozvětvení sítě. Každý příchozí paket do rozbočovače je rozesláný všemi výstupními porty dále. V současné době se již nevyužívají a byly nahrazeny přepínači. [8]

Most (Bridge)

Hlavní funkcí mostů je přenos rámců linkové vrstvy mezi částmi sítě na základě MAC adres a kontrola struktury přenášených rámců. O obsah datové části se nestarají. [8]

Každý most musí vědět, ve které části se nachází daný uzel s MAC adresou, aby mohl rámec přeposlat. Informace získá buď staticky (ruční konfigurací), nebo dynamicky (vyšle rámec do všech částí a vyčká na odpověď). [8]

Přepínač (Switch)

Přepínače na rozdíl od starších Hubů nerozesílají pakety všemi porty a podobně jako mosty se učí MAC adresy připojených prvků. Podporují virtuální lokální síť (VLAN, Virtual Local Area Network). Tyto VLAN mohou vzniknout v lokální síti například z důvodu oddělení různých částí za účelem snížení zátěže nebo bezpečnosti. [8]

Přepínač rozpoznává členství ve virtuální síti:

- Podle přiřazení VLAN fyzickému portu přepínače.
- Podle fyzických adres, které byly přiřazeny do dané VLAN.

Některé přepínače bývají osazeny dvěma nebo čtyřmi porty s vyšší rychlostí. Tyto porty můžeme použít k propojení do vyšších úrovní (např. Internetu), protože v tomto směru dochází k větší vytíženosti linky. Podobné řešení lze provést i pomocí agregace linek, více viz 1.4.3. [8]

Směrovač (Router)

Směrovač je prvek, který pracuje s pakety. Přepojuje dvě a více sítí. Zajišťuje správné směrování paketu (routing) a jeho odeslání do zvoleného směru (forwarding). [8]

Směrování se provádí podle směrovací tabulky. Tabulka obsahuje informace o cílové síti, a ceně trasy. Směrovač vyhledá IP adresu, kterou obsahuje paket, v směrovací tabulce a odešle paket daným směrem. Směrovací tabulky, které směrovač obsahuje, jsou statické (vytvořené uživatelem/administrátorem) nebo dynamické (vytvořené směrovačem na základě směrovacích protokolů). [8]

Brána (Gateway)

Brána je zařízení nebo program k propojení různých typů sítí. Brány překládají adresy, síťové protokoly a data. [8]

1.6 Záložní napájení

Záložní napájení aktivních prvků sítě v případě výpadku napájení je dalším důležitým bodem při zvyšování spolehlivosti sítě. Během přerušení dodávky elektrické energie nebo nenadálém výpadku, může dojít ke ztrátě cenných dat nebo rozpracovaných důležitých dokumentů. Z tohoto důvodu je vhodné používat záložní zdroje.

Ve spoustě firem dnes používají zaměstnanci ke své práci přenosné počítače a přerušení elektrické energie jim nezpůsobí takové problémy jako nedostupnost sítě, místního serveru nebo úložiště.

Přepínače a jiné prvky, které jsou umístěny v montážní skříni, bývají většinou napájeny přes záložní zdroj, který bývá součástí této skříně. Přepínače umístěné v místnostech je vhodné také napájet ze záložního zdroje.

Další možností je použití přepínačů, které už v sobě obsahují redundantní napájení (např. 230V AC a 12 V DC).

V montážních skříních je možné použít napájecí přepínače, které mohou mít dva napájecí vstupy (jeden přímo ze sítě a druhý z UPS) a několik výstupů pro zařízení.

Vždy ovšem záleží na finančních možnostech a přístupu k této problematice ze strany firmy nebo zákazníka.



Obrázek 1.18: Přepínač komunikačního systému napájený přes záložní zdroj

1.7 Bezpečné uložení síťových prvků

Jednou z posledních a často opomíjených možností zvýšení spolehlivosti je bezpečné uložení aktivních a pasivních prvků sítě.

Tyto prvky je nutno umístit tak, aby se zabránilo neodborné manipulaci s nimi ze strany uživatelů. Jakýkoliv sebekvalitnější prvek sítě, který je nevhodně umístěn může způsobit vážné problémy. Často je přepínač uložen “dočasně” někde na zemi bez jakékoliv ochrany (viz Obrázek 1.20). Nejen, že uživatel může do přepínače kopnout a způsobit výpadek sítě nebo jeho zničení, ale může si i sám způsobit úraz.

Stejná pravidla pro ukládání přepínačů platí hlavně i pro kabely. Kabely je vhodné umístit do patřičných instalačních lišt, aby se zabránilo jejich poškození. Zároveň se zabrání případnému úrazu pokud by uživatel o kabel zakopnul a pádem si způsobil úraz (viz Obrázek 1.19).



Obrázek 1.19: Dočasná kabeláž



Obrázek 1.20: Dočasné niekoľika leté uložení přepínače

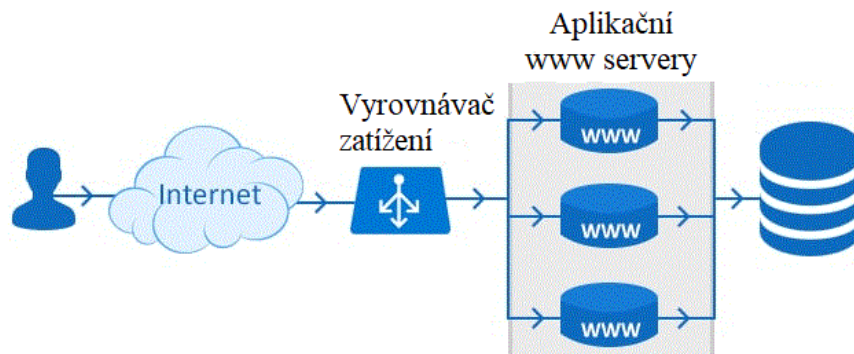
1.8 Servery s vysokou dostupností

Dnes se všichni spoléhají na internet a spousta lidí si ukládá nebo zálohuje svá data a různé informace na internetové servery. Podobná situace je i ve velkých firmách nebo státní a veřejné správě, které potřebují své vlastní servery pro sdílení dat. K tomu slouží vysoce výkonné servery navržené pro maximální výkon a dostupnost High Availability Dedicated Server (HADS).

Vyvážený server

Příchozí provoz je rozdělován mezi skupinu serverů, tak aby nedocházelo k zahlcení

jednoho serveru. Hardwarové nebo softwarové zařízení, které umožňuje vyvážení zatížení, se nazývá Load Balancer. [10]



Obrázek 1.21: Vyvážený server [10]

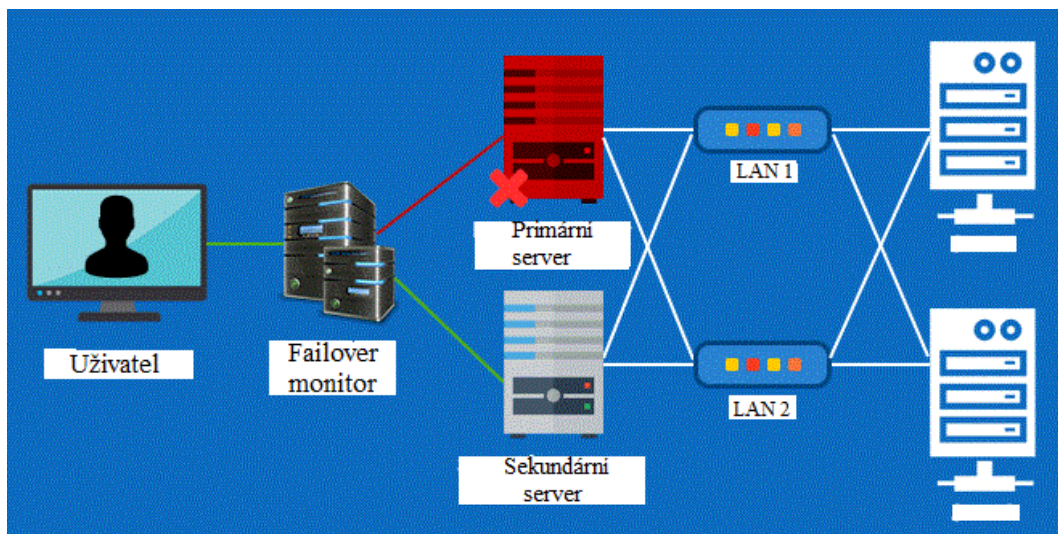
Failover server clustering

Failover znamená okamžité přepnutí na pohotovostní server při selhání primárního serveru. Když primární server selže nebo potřebuje údržbu, pracovní zátěž se automaticky přepne na sekundární server. Failover tak zabraňuje jedinému bodu selhání (SPoF), příklad zapojení viz Obrázek 1.22. [10]

System se skládá ze dvou identických serverů (primárního serveru a sekundárního serveru) a třetího serveru, použitého k monitorování primárního serveru. Pokud tento třetí server zjistí problém, automaticky přesměruje provoz z primárního na sekundární server. [10]

Cold Failover je metoda kdy se druhý server spustí až po vypnutí prvního. To jasně znamená, že musíte být schopni tolerovat malé množství prostojů během přechodu. [10]

Hot Failover je metoda, kdy jeden server běží současně se stejným primárním serverem a při jeho selhání ho okamžitě nahradí. Data se však stále zrcadlí v reálném čase, takže oba systémy mají stejná data. [10]



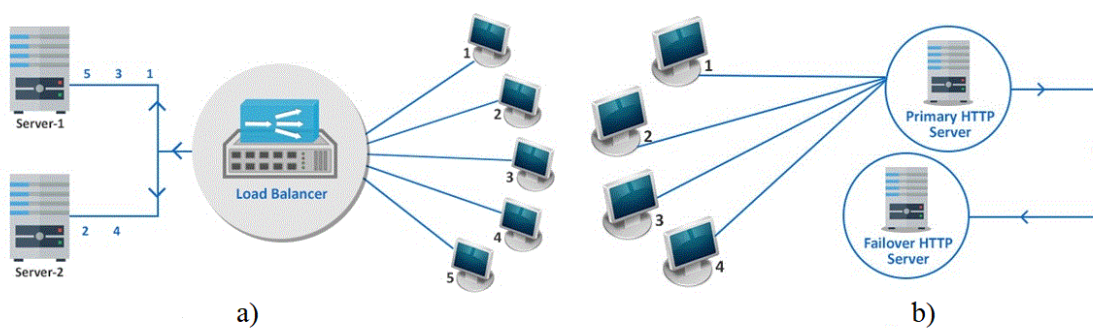
Obrázek 1.22: Failover [10]

Klastr s vysokou dostupností

Klastr s vysokou dostupností je skupina serverů, které lze využít s minimálním množstvím prostojů, když některý uzel serveru selže nebo dojde k přetížení. Nejběžnější typy konfigurace klastru jsou aktivní-aktivní a aktivní-pasivní. [10]

Aktivní-aktivní se skládá alespoň ze dvou serverů, přičemž oba jsou aktivní a provozují stejnou službu. [10]

Aktivní-pasivní se také sestává z alespoň dvou serverů, ale jeden zůstává v pasivním nebo pohotovostním režimu. [10]



Obrázek 1.23: Konfigurace a) aktivní-aktivní b) aktivní-pasivní [10]

2. STOHOVÁNÍ, KLASTROVÁNÍ A KASKÁDOVÁNÍ PŘEPÍNAČŮ

Pro zvýšení spolehlivosti provozu sítě na úrovni přepínačů, je možné využít například stohování, klastrování nebo kaskádování. Dále je možné vytváření záložních cest. V dalším textu se budu soustředit na popis využívající přepínačů firmy Cisco.

V této kapitole se dále budu věnovat možnostem využití zapojení jednotlivých technologií, které budou popsány na hypotetickém modelu školící a výukové firmy. K jednotlivým variantám budou popsány klady a zápory těchto zapojení.

Smyslená školící firma XY využívá 6 místností rozmístěných v různých patrech budovy. Výhledově je očekáváno stěhování firmy. V přízemí budovy se nachází jedna místnost a v ní 5 pracovních stanic. V prvním patře jsou dvě místnosti a v každé je 10 pracovních stanic. Ve druhém patře se nachází tři místnosti a v každé je 10 pracovních stanic.

Základním požadavkem firmy byla spolehlivost a bezúdržbovost s možností snadného přemístění prvků z důvodu případné možnosti přestěhování firmy do nových prostorů.

2.1 Výchozí scénář

V tomto výchozím scénáři je ve firmě kompletně vybudována a instalována strukturovaná kabeláž (viz Obrázek 2.1). Kabeláž je v každé místnosti zakončena zásuvkou, kterou nelze lehce přemísťovat. Ze zásuvek vedou kabely k jednotlivým účastníkům, které je nutno uložit do ochranných lišt. A to jak z důvodu ochrany samotné kabeláže, tak i samotných uživatelů.

Strukturovaná kabeláž je ukončena v serverovně v patch panelech. Z těchto panelů je provedeno další propojení kabely se samotnými přepínači.

Podle počtu účastníků, je možné použít k jejich propojení v serverovně pouze jeden přepínač, ale z hlediska spolehlivosti je tato variant nebezpečná. Při výpadku tohoto jediného přepínače, dojde k nedostupnosti celé sítě pro všechny uživatele.

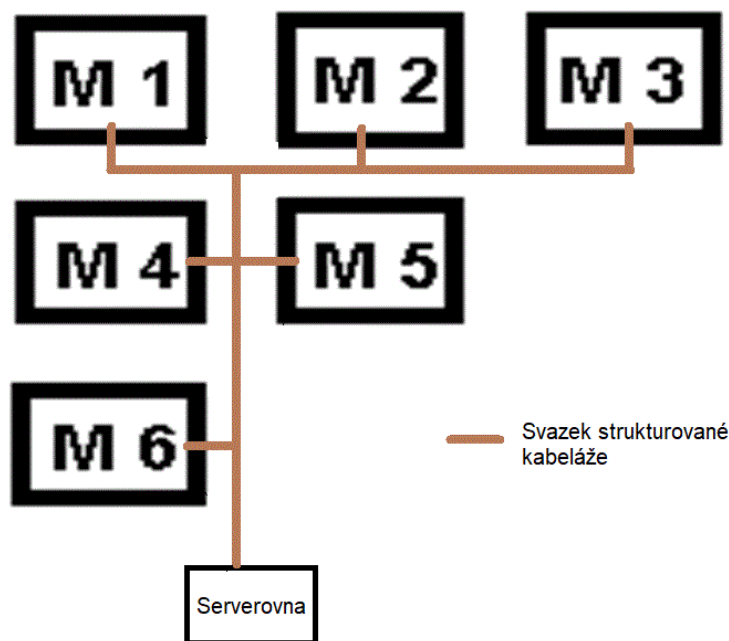
Jako vhodnější řešení tohoto problému, samozřejmě s ohledem na finanční a spolehlivostní požadavky uživatele, je použití více přepínačů, např. místo jednoho přepínače 48 portů použijeme dva přepínače 24 portů. Při výpadku některého z přepínačů, dojde k nedostupnosti pouze jedné části sítě a druhá část uživatelů bude mít stále možnost připojení do sítě.

Jednou z výhod je použití napájení přepínačů ze záložního zdroje UPS, který je umístěn v montážní skříni společně s přepínači.

Jako další možná výhoda je využití napájecího přepínače. Tento přepínač může mít jeden napájecí přívod přímo z rozvodné sítě 230 V a druhý ze záložního zdroje UPS. V případě závady na UPS přepne na napájení z rozvodné sítě a naopak.

Hlavní nevýhoda tohoto scénáře je složitá příprava celkového zapojení, která je vytvářena pro konkrétní požadavky uživatele a nesnadná možnost rozšiřování. Pro přípravu a uložení kabelů musí být provedeny složité stavební úpravy. Takto vytvořená zapojení nelze snadno modifikovat a jsou většinou stálé.

Dalším omezením tohoto způsobu, je omezení v délce kabeláže na 100 m bez použití opakovače nebo přepínače.



Obrázek 2.1: Výchozí scénář zapojení

2.2 Stohování přepínačů

Stoh je seskupení přepínačů, které jsou propojeny speciální sběrnicí do kruhové topologie a společně se chovají jako jedno zařízení. Technologii používáme převážně v montážních skříních a umožňuje snadné rozšíření počtu portů tam, kde očekáváme jejich značný nárůst.

Tato technologie umožňuje stohovat až 9 síťových prvků do jednoho celku. Všechny prvky mají společnou konfiguraci, stejný operační systém a směrovací informace. Tím, že jsou prvky stohu propojeny do kruhu, přerušení topologie v jednom místě nezpůsobí havárii stohu, pouze poklesne propustnost. Celý stoh řídí jeden hlavní přepínač (master), ostatní přepínače se označují jako členové (members) stohu. Pomocí master přepínače lze nakonfigurovat všechny ostatní prvky stohu. Master přepínač má v sobě uložené konfigurační soubory s nastavením pro každého člena a každý člen má aktuální kopii těchto souborů. [2]

Celý stoh je konfigurován pomocí jedné IP adresy i v případě odebrání hlavního přepínače. Každý prvek ve stohu se může stát master přepínačem v případě jeho výpadku. Členové stohu si mezi sebou zvolí nový hlavní přepínač podle toho, který má novější verzi IOS, existující konfiguraci, nebo nejnižší MAC adresu. Nový hlavní přepínač po svém zvolení rozkopíruje svou verzi IOS na ostatní členy stohu, z důvodu zajištění vzájemné kompatibility. K nastavování lze využít Network Assistant (z webu Cisco.com), příkazový řádek při propojení přes port libovolného člena stohu nebo pomocí Simple Network Management Protocolu. [2]

Přidání nového člena do stohu probíhá zcela automaticky. Nový přepínač se připojuje vypnutý za chodu zbytku stohu. Po zapnutí by měl přepínač sám zjistit připojení do stohu a master přepínač provede nahrání potřebných konfiguračních souborů a restart přepínače. Zároveň se výchozí číslo přepínače, které je z výroby nastaveno na 1, změní na nejnižší dostupné číslo člena v zásobníku. Ve stohu nemohou být přepínače, které mají stejné číslo. [2]

Přepínače ve stohu lze propojit pomocí sběrnice StackWise (propustnost až 32Gbps), StackWise plus (propustnost až 64Gbps) nebo pomocí gigabitových portů za pomoci speciálního konvertoru Gigabit Interface Converter (GBIC). [2]



Obrázek 2.2: Propojení přepínačů speciálním kabelem do stohu [9]

Výhodou je jednoduché přidávání a odebírání členů stohu, konfigurace pomocí jedné IP adresy (úspora adresního prostoru). Stoh lze takto spravovat i v případě odebrání hlavního přepínače. Členové stohu si zachovávají svou IP adresu, proto je vhodné ji při odebírání přepínače ze stohu změnit. [2]

Hlavní nevýhodou je vysoká pořizovací cena přepínačů.

2.2.1 Scénář zapojení číslo 1

Jednoduchou modifikací výchozího scénáře se zabudovanou strukturovanou kabeláží popsaného v kapitole 2.1, je výměna použitých přepínačů za přepínače podporující stohování a současně změna zapojení těchto přepínačů do stohu. Zbývající kabeláž

zůstává beze změny.

Výhodou je použití pouze jedné IP adresy pro celý stoh a konfigurace jednoho přepínače, který bude nastaven jako master. Ostatní přepínače budou nastaveny podle tohoto hlavního přepínače. Při přidávání dalšího přepínače není nutná žádná jeho další konfigurace a po připojení je do něj konfigurace nahrána z hlavního přepínače.

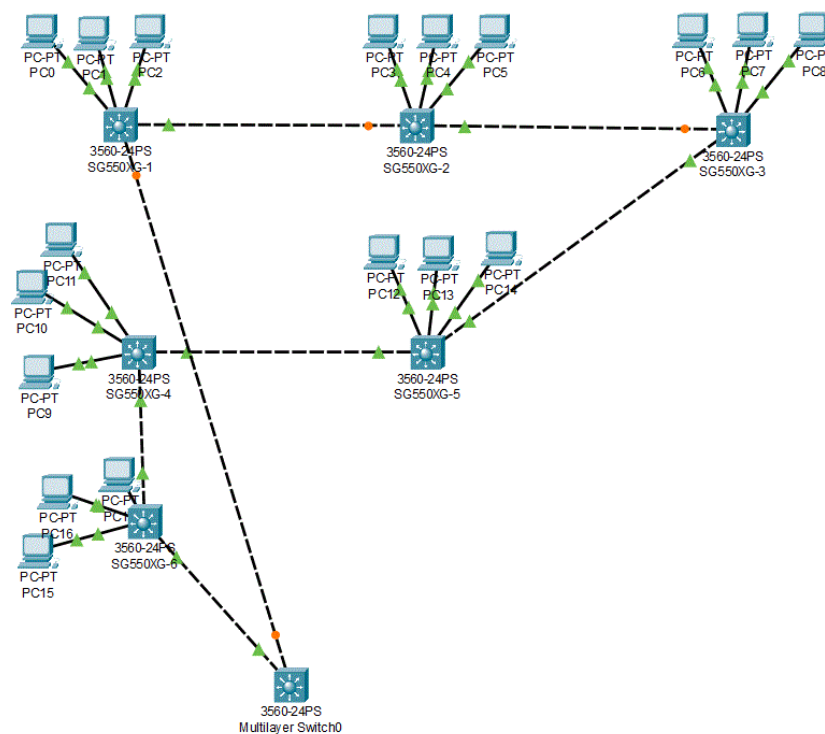
Nevýhodou je vyšší cena těchto přepínačů a pro zabezpečení správného chodu i stejné typy a řady přepínačů, které použijeme. Další možnou nevýhodou je možnost rozpadnutí stohu při poruše prostředního přepínače. V tomto případě je nutné vadný přepínač odpojit, propojit přepínače (nebo provést výměnu vadného za nový) a provést restart celého stohu.

Při přerušení kabelu mezi přepínači se změní kruhová topologie na sběrnicovou čímž je zabezpečena spolehlivost toku dat.

Samozřejmostí je možnost použití záložního zdroje UPS pro případ výpadku napájení stejně jako v případě výchozího scénáře.

2.2.2 Scénář zapojení číslo 2

V této verzi zapojení jsou přepínače nastaveny v módu stoh, ale nejsou fyzicky umístěny v serverovně, jako v předchozím scénáři, nýbrž stoh je vytvořen virtuálně. Přepínače jsou umístěny v jednotlivých místnostech firmy a jsou navzájem mezi sebou propojeny do kruhu pomocí optického kabelu. Při tomto způsobu zapojení odpadají složité stavební úpravy spojené s naplánováním a vybudováním strukturované kabeláže.

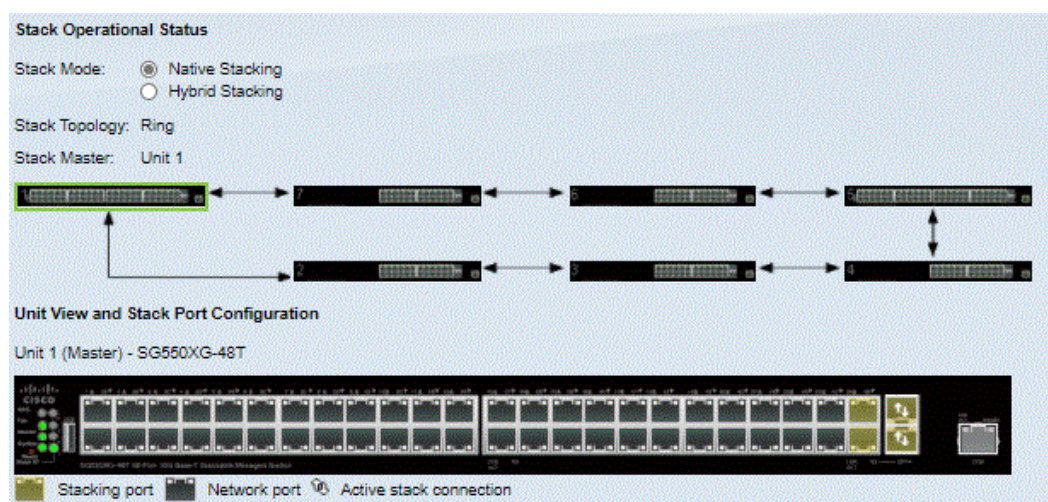


Obrázek 2.3: Scénář stoh

Toto zapojení umožňuje díky propojení přepínačů optickými kabely rychlost až 10 Gbs.

V případě selhání některého přepínače se topologie kruh přepne na sběrnicovou topologii. Sít' bude nedostupná pouze v místnosti, ve které je vadný přepínač.

Nevýhodou je vyšší pořizovací cena přepínačů a optického kabelu. Jako další možná nevýhoda je to, že každý přepínač je v místnosti umístěn do montážní skříně. Možným důsledkem umístění víceportového přepínače přímo v místnosti je zvýšený hluk od chladících ventilátorů. V této skříně je i optická vana pro ukončení optického kabelu. Pro zabezpečení záložního napájení zde může být i záložní zdroj napájení.



Obrázek 2.4: Zapojení z managementu přepínače

2.3 Klastrování přepínačů

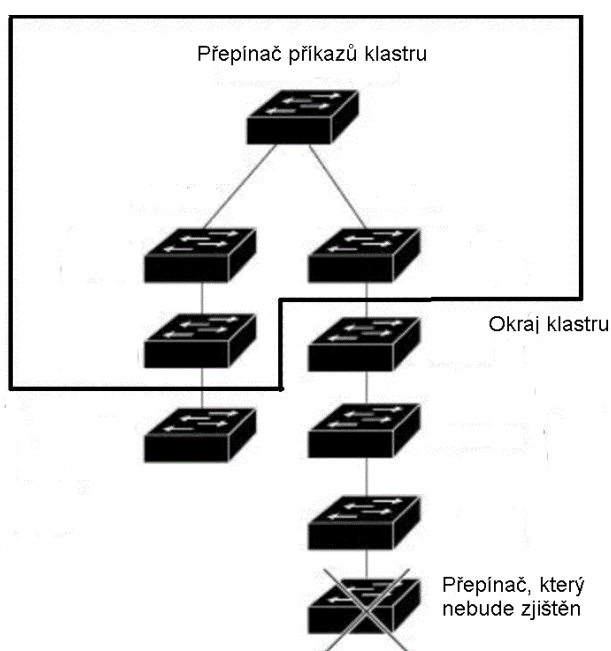
Tato technologie umožňuje připojit až 16 přepínačů do jednoho klastru. Všechny přepínače v klastru je možné díky technologii klastrování nakonfigurovat prostřednictvím jedné IP adresy podobně jako u stohování. Přepínače v klastru však nejsou propojeny jako ve stohu speciálními porty a kabelem, ale prostřednictvím LAN portů. [3]

V klastru musí být vždy jeden přepínač zvolen jako přepínač příkazů klastru a ostatní jsou nastaveny jako členové klastru. Přepínač příkazů klastru je jako jediný používán ke konfiguraci a správě klastru. Tento přepínač musí mít svou IP adresu, povolený Cisco Discovery Protokol (CDP) a nesmí být členem jiného klastru. [3]

Členové klastru mohou být součástí pouze jednoho klastru. Aby nedošlo ke ztrátě kontaktu s ostatními členy v případě selhání přepínače příkazů klastru, je jeden nebo více přepínačů označeno jako pohotovostní příkazové přepínače klastru. Tyto

pohotovostní přepínače příkazů klastru musí být stejného typu jako přepínač příkazů klastru. [3]

Nově připojované přepínače do klastru musí mít spuštěný software na podporu klastrování, povolený CDP a nesmí být členy jiného klastru. Je vhodné, aby všechny použité přepínače byly od stejného výrobce (z důvodu vzájemné kompatibility). Pomocí CDP může přepínač příkazů klastru objevit, v základním nastavení, přepínače až do tří přeskočení CDP od okraje klastru (viz Obrázek 2.5). Přepínače, které jsou dále, nebudou objeveny. Toto počáteční nastavení lze změnit až na sedm přeskočení. Okraj clusteru je místo, kde jsou poslední přepínače klastru připojeny ke kandidátským přepínačům. [3]



Obrázek 2.5: Objevení nových přepínačů [3]

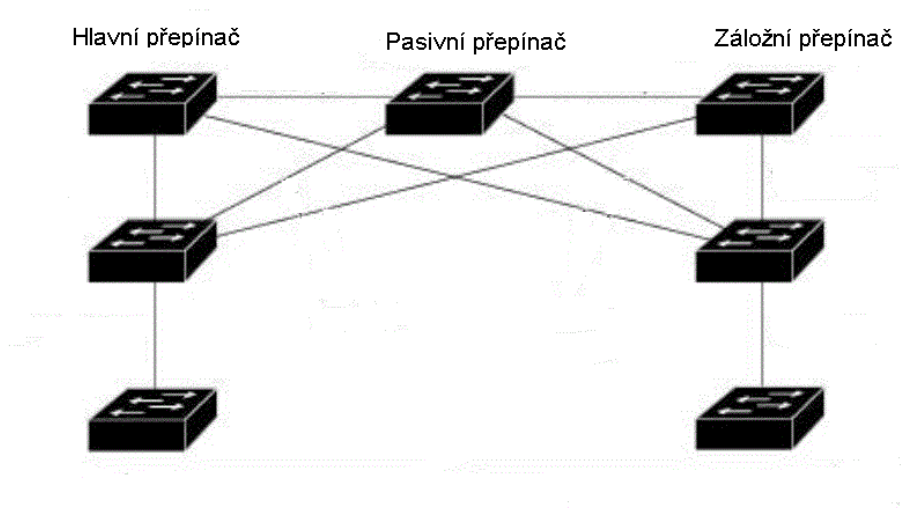
Každý záložní pohotovostní přepínač (viz Obrázek 2.6) musí být připojen k příkazovému přepínači klastru a zároveň musí být redundantně připojen k ostatním přepínačům klastru. [3]

Aktivní příkazový přepínač klastru neustále přeposílá informace o konfiguraci klastru (ale nikoli informace o konfiguraci zařízení) do pohotovostního příkazového přepínače klastru, aby zajistil převzetí klastru ihned po svém selhání. [3]

Pokud aktivní a pohotovostní příkazový přepínač klastru selžou současně, pasivní příkazový přepínač klastru s nejvyšší prioritou se stane aktivním příkazovým přepínačem klastru. Protože do pasivního přepínače klastru se nezasílají informace o konfiguraci, musí se klustr znovu sestavit. [3]

Když dříve aktivní přepínač příkazů klastru obnoví svou aktivní roli, obdrží kopii nejnovější konfigurace klastru z aktivního přepínače příkazů klastru, včetně členů, kteří

byli přidáni, když byl vypnutý. Přepínač příkazů aktivního klastru odešle kopii konfigurace klastru do pohotovostní skupiny klastru. [3]



Obrázek 2.6: Hlavní a pohotovostní přepínač klastru [3]

Výhodou tohoto způsobu je konfigurace celého klastru pomocí jedné IP adresy a propojení porty LAN.

2.3.1 Scénář zapojení číslo 3

Zapojení přepínačů v této variantě je obdobné jako v případě kaskádování přepínačů, více viz 2.4.1. Rozdíl spočívá ve využití přepínačů, které umožňují funkci klastrování a možnosti použití pouze jedné adresy IP pro nastavování a konfiguraci celého klastru.

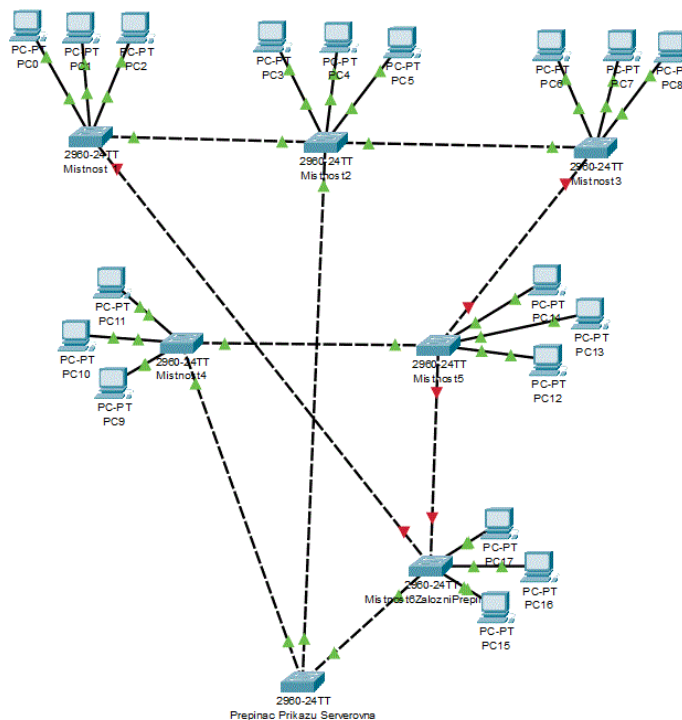
Cena přepínačů, které umožňují klastrování je vyšší než cena jednoduchých přepínačů, které tuto funkci nepodporují, a proto záleží opět na finančních možnostech uživatele.

V případě selhání některého z členských přepínačů klastru, bude síť nedostupná pouze v dané místnosti.

Kritickým místem je hlavní příkazový přepínač klastru, jehož selhání způsobí nedostupnost sítě jako celku. Z tohoto důvodu musí být minimálně jeden přepínač nastaven jako záložní příkazový přepínač, který převzme funkci hlavního přepínače v případě jeho selhání.

Aby mohl záložní příkazový přepínač převzít funkci hlavního přepínače, musí být propojen s ostatními přepínači v klastru (viz Obrázek 2.7). Pokud nebude mít záložní přepínač vytvořené záložní spojení s ostatními členy klastru, zůstane síť jako celek nefunkční.

Pokud bychom požadovali záložní napájení přepínačů, je nutné ke každému přepínači umístit záložní napájecí zdroj. Je možné i použití přepínačů s redundantními zdroji v samotném přepínači.



Obrázek 2.7: Klastř s vytvořenými záložními spoji

2.4 Kaskádování přepínačů

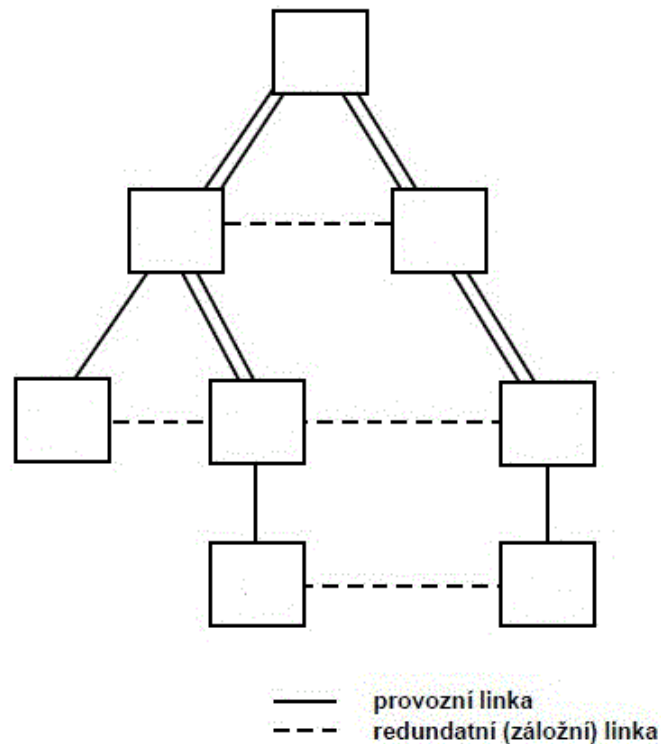
Jedná se o nejjednodušší způsob rozšiřování počtu přípojných portů pro uživatele. Toto rozšiřování je realizováno pomocí síťového kabelu připojeného do jakéhokoliv výstupního portu jednoho přepínače a následném propojení s přímým portem druhého přepínače. Jednotlivé přepínače jsou konfigurovány samostatně.

Aby se zabránilo možnému vzniku smyček, měli by všechny přepínače, které jsou propojeny do kaskády podporovat minimálně STP. [8]

V případě výskytu smyčky, mohou vzniknout tyto problémy:

- **Broadcastové bouře** – množství všesměrových zpráv může zahltit síť.
- **Nestabilita tabulky MAC adres** – zpráva je doručena na přepínač z více portů a přepínač stále mění adresu zdroje zprávy.
- **Několikanásobné doručení** – zpráva, která koluje v síti neustále dokola je několikrát doručena.

Největší výhodou této technologie je jednoduché rozšiřování topologie sítě. Nevýhodou je složitější konfigurace každého přepínače samostatně.



Obrázek 2.8: Kaskádování přepínačů kombinované s LACP [6]

2.4.1 Scénář zapojení číslo 4

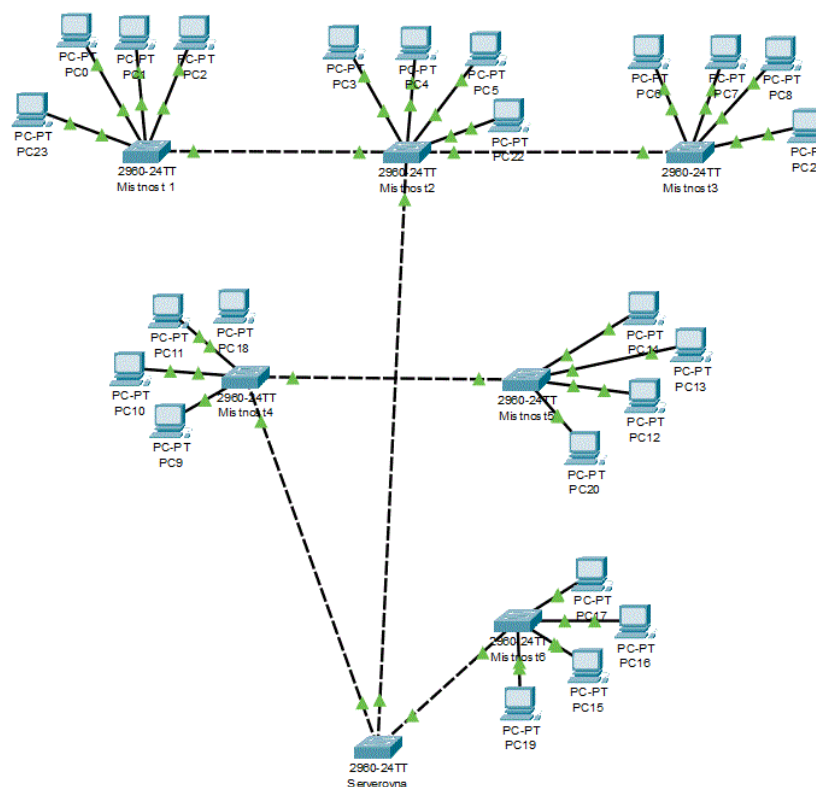
Tento model nevyžaduje složité stavební úpravy jako v případě strukturované kabeláže, která obsahuje velký svazek kabelů odcházejících ze serverovny.

V každé místnosti je umístěn přepínač s počtem portů dle požadavku uživatele. Tímto je zajištěno snadné přizpůsobení požadavkům uživatele. Cena přepínačů, které nemusí podporovat stohování nebo klastrování je mnohem nižší než u přepínačů s touto funkcí. Zároveň při závadě některého z přepínačů odpadá pořizování přesně daného přepínače jako ve variantě stoh.

Kritickým místem tohoto způsobu zapojení je přepínač umístěný v serverovně. Při jeho selhání dojde ke ztrátě spojení mezi jednotlivými místnostmi a tím nefunkčnosti sítě jako celku.

Zcela nevhodný je způsob zapojení bez záložních spojů viz Obrázek 2.9. V tomto případě je síť jako celek nefunkční. Zůstává funkční pouze spojení v jednotlivých místnostech nebo v rámci patra.

Pro zamezení celkové nefunkčnosti je nutné pro zajištění spolehlivosti provést záložní propojení přepínačů. Toto záložní propojení zamezí nedostupnosti sítě při poruše přepínače umístěného v serverovně viz Obrázek 2.10.

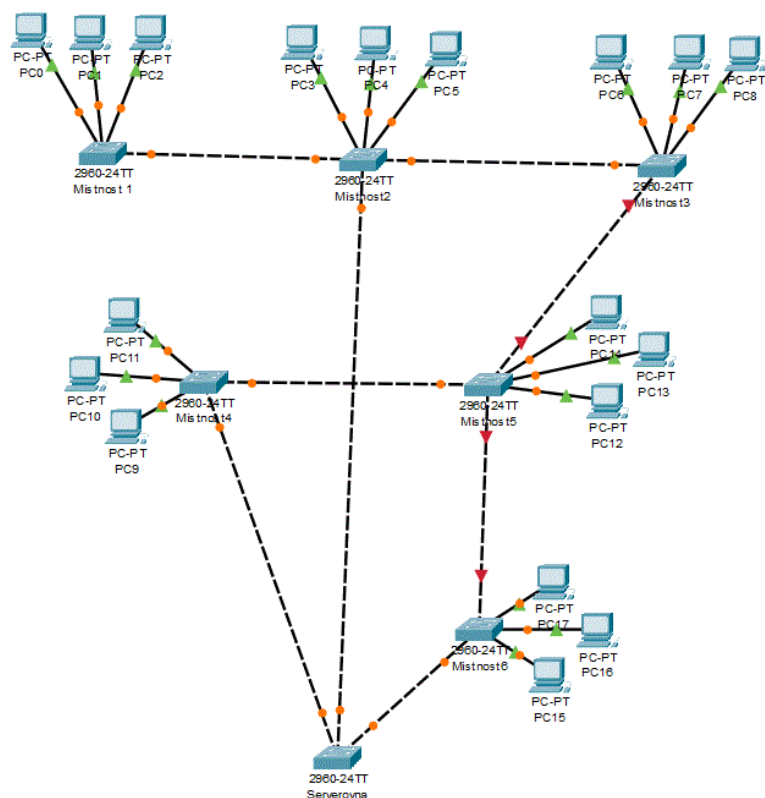


Obrázek 2.9: Kaskáda bez záložních spojů

Při závadě některého z přepínačů umístěných v místnostech, dojde pouze k nedostupnosti sítě v dané místnosti, zbytek sítě zůstává funkční.

Dalším kritickým místem je přepínač v místnosti číslo 2. Při jeho selhání, bez záložních spojů, dojde ke ztrátě komunikace nejen mezi patry, ale i v rámci patra.

Pokud bychom požadovali záložní napájení přepínačů, je nutné ke každému přepínači umístit záložní napájecí zdroj UPS. Toto ovšem zvyšuje cenu tohoto způsobu zapojení. Je možné i použití přepínačů s redundantními zdroji v samotném přepínači.



Obrázek 2.10: Scénář kaskáda

Dílčí zhodnocení

Na základě zhodnocení jednotlivých scénářů se jako, neekonomičtější a nejjednodušší varianta, jeví zapojení přepínačů do kaskády. Zároveň toto řešení umožňuje jednoduchou rozšiřitelnost sítě bez nutnosti složitější konfigurace. Pro správnou funkci je nutné vytvoření záložních spojů, aby byl zabezpečen provoz sítě v případě selhání některého prvku nebo spoje.

Jako optimální řešení z hlediska spolehlivosti a nenáročnosti v instalaci kabeláže, je řešení popsané ve scénáři číslo 2 (viz 2.2.2). Nevýhodou tohoto způsobu jsou vyšší pořizovací náklady (cena přepínačů a optických kabelů) a náročnější počáteční konfigurace.

Technologie zapojení jako stohování a klastrování jsou vhodné do míst se složitějším počátečním nastavením aktivních prvků sítě. V případě selhání aktivního prvku a jeho nahrazení novým prvkem, je do tohoto nového prvku automaticky nahrána konfigurace, bez nutnosti zásahu správce sítě.

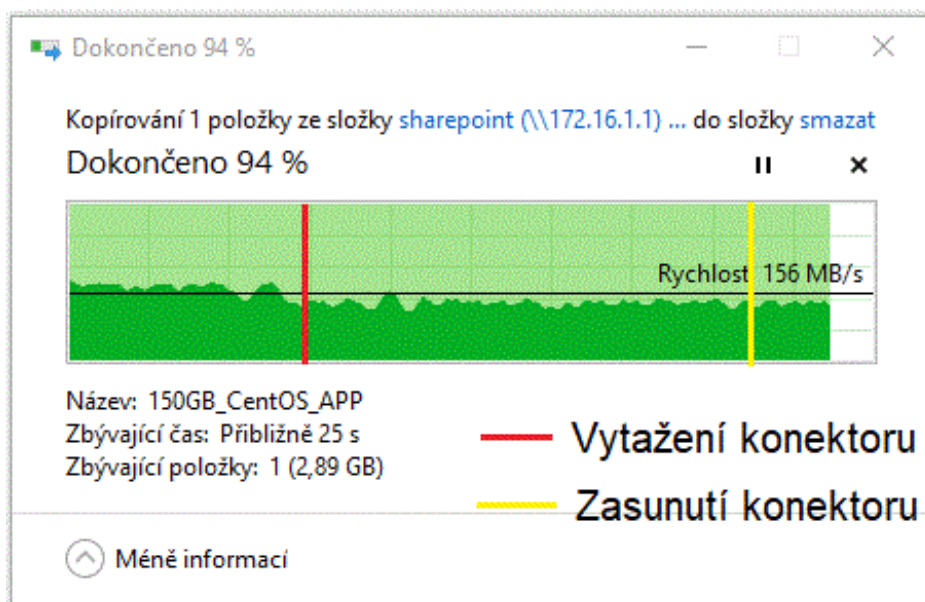
2.5 Praktické pokusy

Praktický pokus byl proveden na zapojení popsaném v podkapitole 2.2.2. Toto zapojení je reálně využíváno firmou XY. V zapojení jsou používány přepínače firmy Cisco řady SG550X, výstup zapojení z managementu viz Obrázek 2.4. Z jednotlivých přepínačů je provedeno připojení koncových stanic pomocí kabelu CAT 6. Všechny pracovní stanice mají srovnatelnou konfiguraci a jsou osazeny síťovou kartou 10 Gbs.

Každý dílčí pokus byl proveden pouze dvakrát. Během pokusu bylo v každé místnosti spuštěno 5 pracovních stanic s běžnými kancelářskými aplikacemi. Během praktických pokusů se kopíroval soubor o velikosti 56,3 GB z pracovní stanice umístěné v místnosti číslo 3.

Pokus číslo 1 (mezi patry)

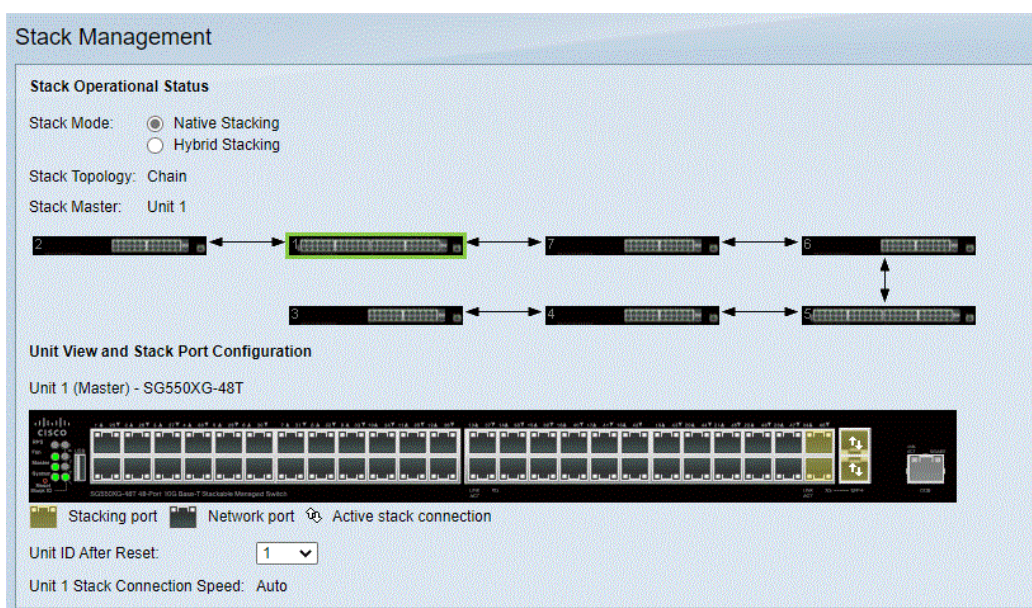
Při prvním pokusu byl během stahování souboru do pracovní stanice v místnosti číslo 4, odpojen optický kabel do přepínače. Tímto odpojením se simulovalo přerušení optického kabelu mezi přepínači. Při tomto pokusu nebylo zjištěno žádné výrazné snížení přenosové rychlosti nebo nějaká časová prodleva spojená s přepnutím na sběrníkovou topologii. To je předpokládám dáno pouze změnou topologie kruh na sběrnici, při zachování počtu přepínačů. Průměrná rychlost při stahování byla přibližně 145 MB/s. Tato rychlost nebyla nijak ovlivněna ani po zpětném připojení optického kabelu zpět do přepínače (viz).



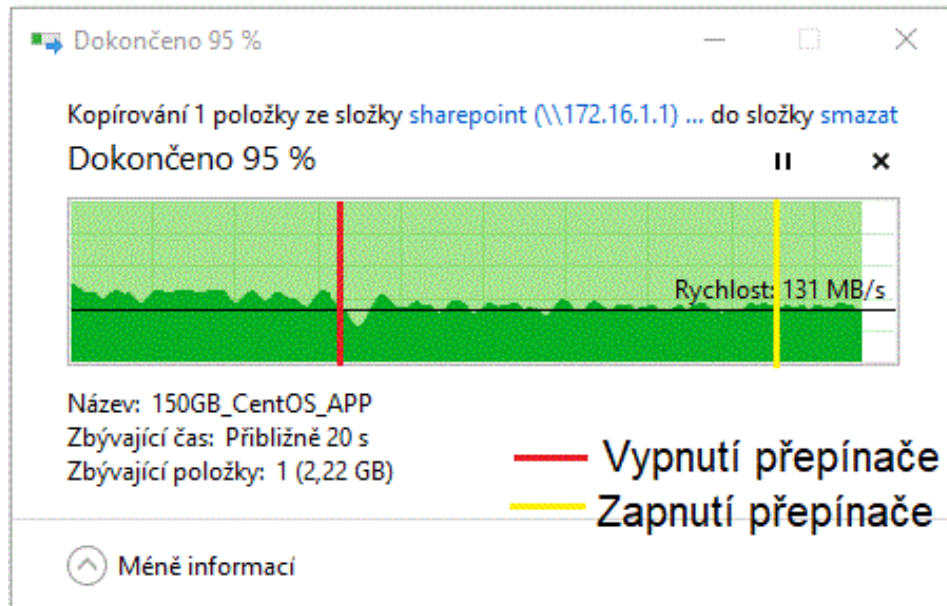
Obrázek 2.11: Průběh stahování 1

Pokus číslo 2 (mezi patry)

Při druhém pokusu byl z napájecí sítě odpojen přepínač v místnosti číslo 5 a tím se simulovala selhání jednoho z přepínačů. Po vypnutí přepínače došlo ke krátkodobému výraznějšímu poklesu přenosové rychlosti, který trval přibližně 2 sekundy (více viz Obrázek 2.13). Následně se rychlost přenosu vrátila do původního stavu a nezvýšila se ani po opětovném zapnutí přepínače. Zapnutí přepínače a jeho zpětné načtení konfigurace trvalo přibližně 90 sekund. Pokles po vypnutí přepínače je především ovlivněn rekonfigurací celého stohu, protože došlo ke změně počtu přepínačů v zapojení. Vnitřní servisní komunikace přepínačů při rekonfiguraci měla vyšší prioritu než přenášená data. Průměrná rychlost stahování byla přibližně 130 MB/s.



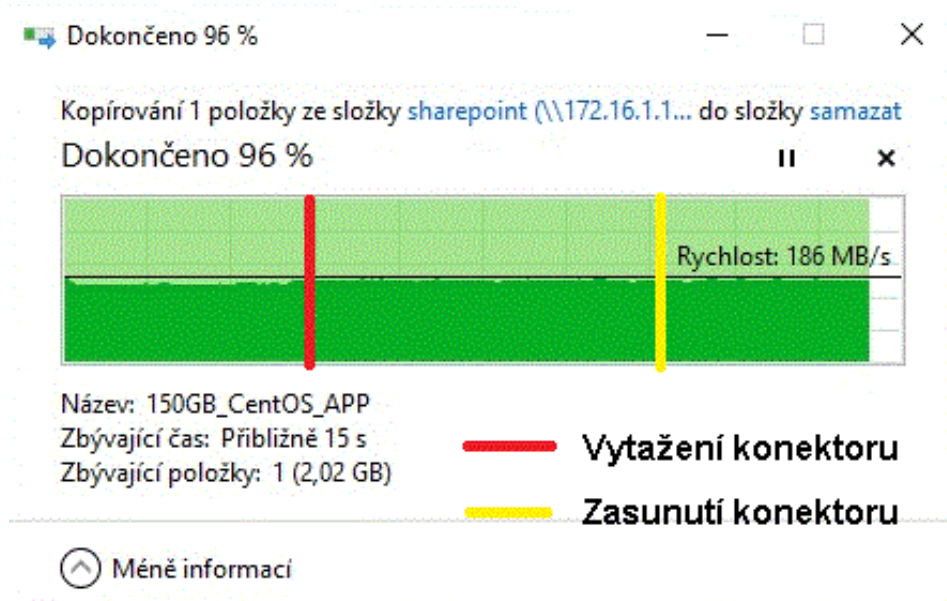
Obrázek 2.12: Rozpojení kruhu v managementu přepínače



Obrázek 2.13: Průběh stahování 2

Pokus číslo 3 (v rámci patra)

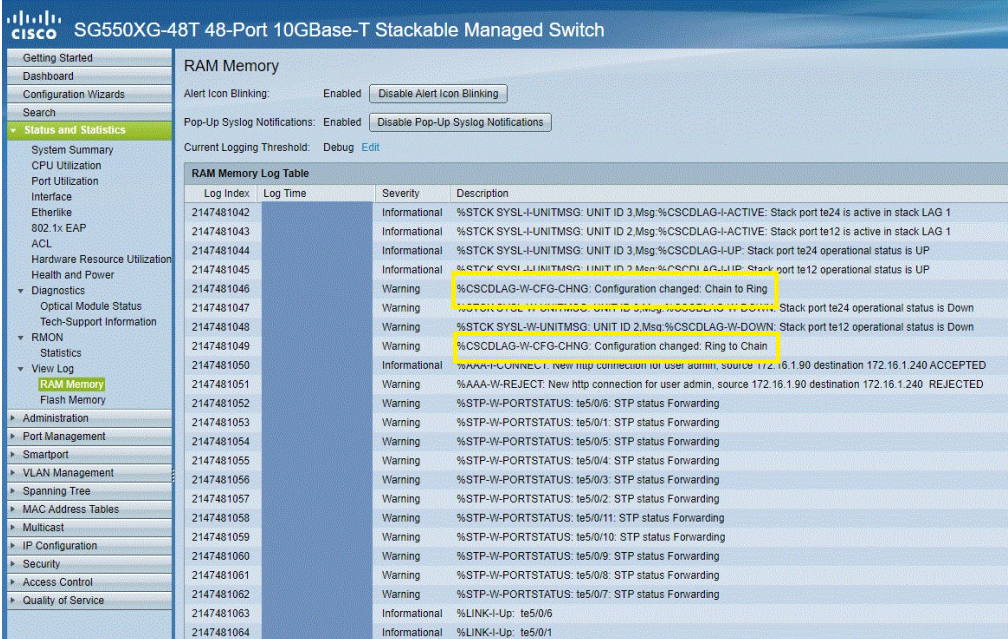
Při tomto pokusu byl během stahování souboru do pracovní stanice umístěné v místnosti číslo 1, odpojen optický kabel z přepínače umístěného v této místnosti. Stejně jako v případě prvního praktického pokusu nemělo odpojení vodiče žádný vliv na přenosovou rychlost během stahování souboru. Průměrná rychlost stahování byla přibližně 180 MB/s.



Obrázek 2.14: Průběh stahování 3

Pokus číslo 4 (v rámci patra)

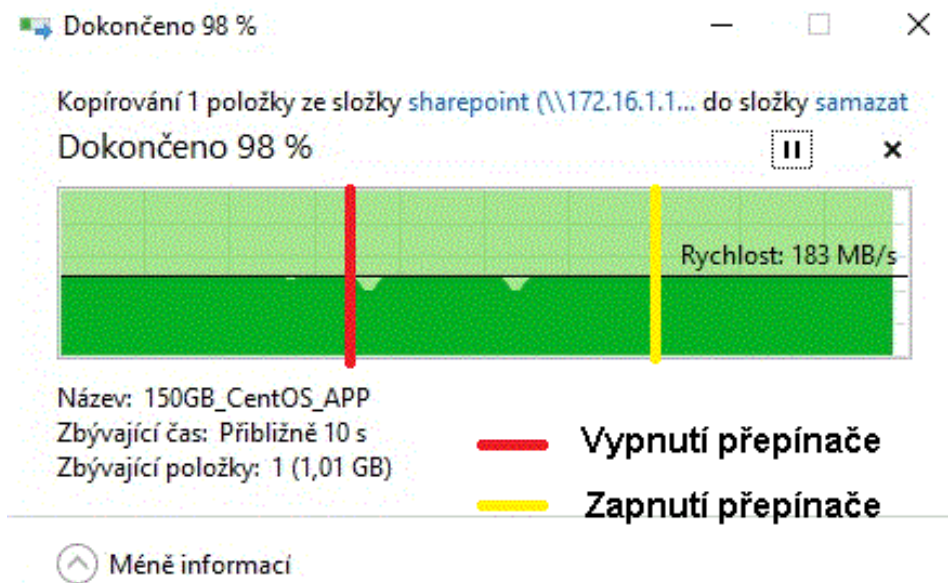
Při tomto pokusu byl během stahování souboru z napájecí sítě odpojen přepínač umístěný v místnosti číslo 2. Opět jako v případě pokusu číslo 2 došlo ke krátkodobému snížení rychlosti během stahování, trvajících přibližně 2 sekundy, daného rekonfigurací stohu z kruhové topologie na sběrnicevou. Zpětné zapnutí přepínače a naběhnutí do funkčního stavu trvalo přibližně 90 sekund. Toto opětovné zapnutí přepínače opět nemělo vliv na přenosovou rychlost. Průměrná rychlost stahování byla přibližně 180 MB/s.



The screenshot displays the management interface of a Cisco SG550XG-48T switch. The left sidebar shows a navigation menu with 'Status and Statistics' selected. The main content area is titled 'RAM Memory' and includes a 'RAM Memory Log Table' with the following data:

Log Index	Log Time	Severity	Description
2147481042		Informational	%STCK SYSL-I-UNITMSG: UNIT ID 3.Msg.%CSCDLAG-I-ACTIVE: Stack port te24 is active in stack LAG 1
2147481043		Informational	%STCK SYSL-I-UNITMSG: UNIT ID 2.Msg.%CSCDLAG-I-ACTIVE: Stack port te12 is active in stack LAG 1
2147481044		Informational	%STCK SYSL-I-UNITMSG: UNIT ID 3.Msg.%CSCDLAG-I-UP: Stack port te24 operational status is UP
2147481045		Informational	%STCK SYSL-I-UNITMSG: UNIT ID 2.Msg.%CSCDLAG-I-UP: Stack port te12 operational status is UP
2147481046		Warning	%CSCDLAG-W-CFG-CHNG: Configuration changed: Chain to Ring
2147481047		Warning	%CSCDLAG-W-UNITWDO: UNIT ID 3.Msg.%CSCDLAG-W-DOWN: Stack port te24 operational status is Down
2147481048		Warning	%CSCDLAG-W-UNITWDO: UNIT ID 2.Msg.%CSCDLAG-W-DOWN: Stack port te12 operational status is Down
2147481049		Warning	%CSCDLAG-W-CFG-CHNG: Configuration changed: Ring to Chain
2147481050		Informational	%AAA-W-CONNECT: New http connection for user admin, source 172.16.1.90 destination 172.16.1.240 ACCEPTED
2147481051		Warning	%AAA-W-REJECT: New http connection for user admin, source 172.16.1.90 destination 172.16.1.240 REJECTED
2147481052		Warning	%STP-W-PORTSTATUS: te5/0/6: STP status Forwarding
2147481053		Warning	%STP-W-PORTSTATUS: te5/0/1: STP status Forwarding
2147481054		Warning	%STP-W-PORTSTATUS: te5/0/5: STP status Forwarding
2147481055		Warning	%STP-W-PORTSTATUS: te5/0/4: STP status Forwarding
2147481056		Warning	%STP-W-PORTSTATUS: te5/0/3: STP status Forwarding
2147481057		Warning	%STP-W-PORTSTATUS: te5/0/2: STP status Forwarding
2147481058		Warning	%STP-W-PORTSTATUS: te5/0/11: STP status Forwarding
2147481059		Warning	%STP-W-PORTSTATUS: te5/0/10: STP status Forwarding
2147481060		Warning	%STP-W-PORTSTATUS: te5/0/9: STP status Forwarding
2147481061		Warning	%STP-W-PORTSTATUS: te5/0/8: STP status Forwarding
2147481062		Warning	%STP-W-PORTSTATUS: te5/0/7: STP status Forwarding
2147481063		Informational	%LINK-I-Up: te5/0/6
2147481064		Informational	%LINK-I-Up: te5/0/1

Obrázek 2.15: Ukázka výpisu z managementu přepínače



Obrázek 2.16: Průběh stahování 4

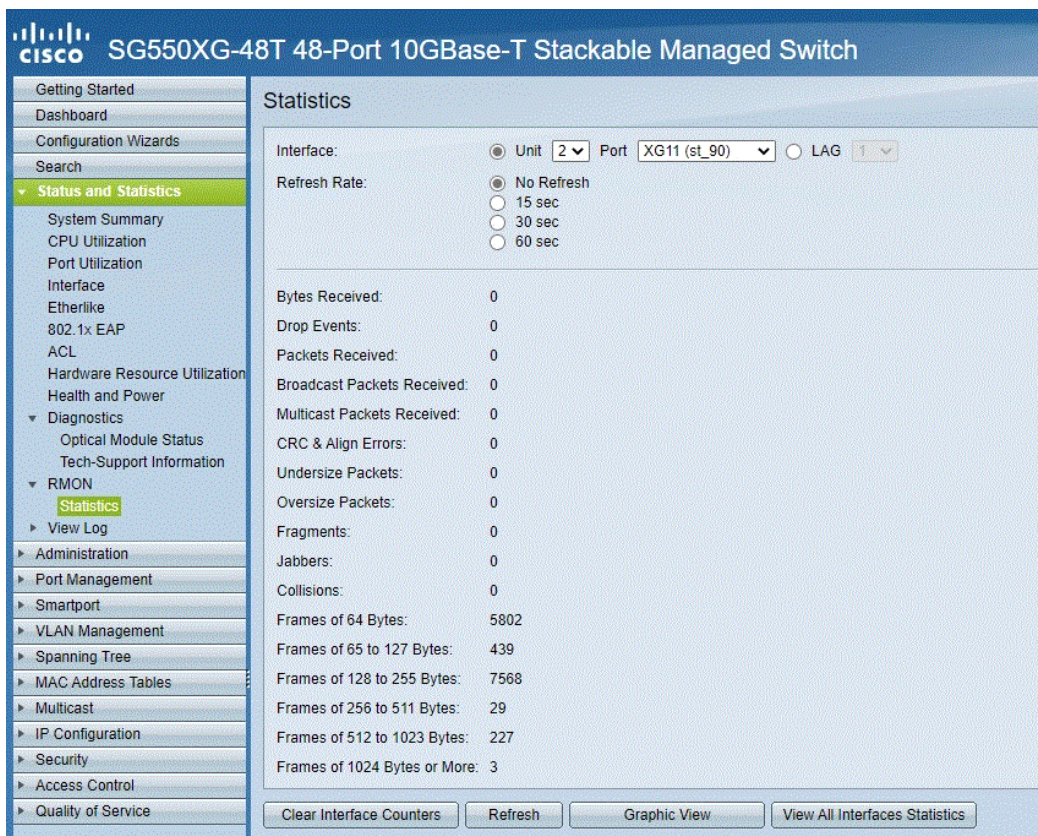
Dílčí zhodnocení

Na praktických pokusech byla ověřena spolehlivost a funkčnost zapojení jak v případě vysunutí konektoru, simulující přerušení optického kabelu, tak i v případě vypnutí přepínače. Zapojení se automaticky změnilo z kruhové topologie na sběrníkovou. Byla ověřena zpětná rekonfigurace s přepnutím ze sběrníkové topologie na kruhovou a celková funkčnost stohu, po simulovaných závadách, bez nutnosti zásahu uživatele. Po žádném z pokusů nebyla v managementu přepínače zjištěna jakákoliv ztrátovost (viz Obrázek 2.17 a Obrázek 2.18).

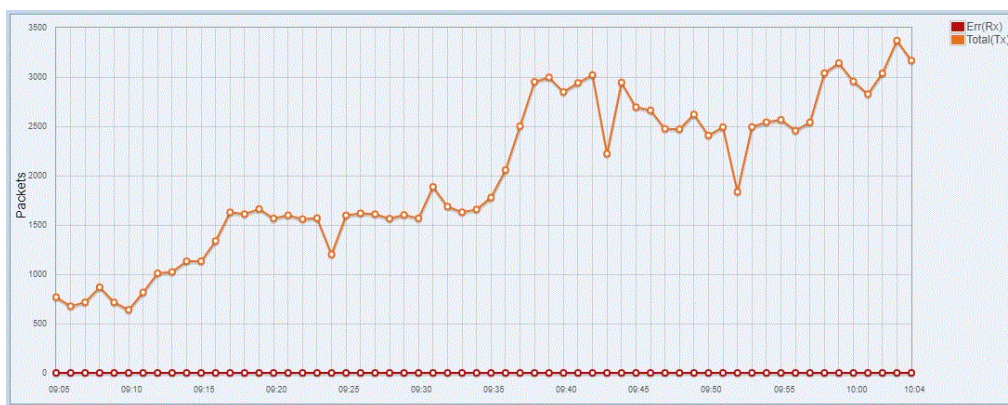
Pro zjištění vzájemné komunikace mezi přepínači by bylo nutné mít přepínač vyšší řady s rozsáhlejším managementem, který umožňuje zobrazit vzájemnou komunikaci přepínačů.

Ověření ostatních zapojení jsem nemohl provést z důvodu zaměření na konkrétní, reálně používané zapojení.

Nevýhodou je doba rekonfigurace stohu, po kompletním restartu celého stohu, která trvala téměř 25 minut.



Obrázek 2.17: Ztrátovost po přenosu



Obrázek 2.18: Graf ztrát a přenesených paketů

ZÁVĚR

Tématem bakalářské práce bylo zvyšování spolehlivosti komunikační sítě. Komunikační síť je složená ze spousty prvků a spolehlivost musí být řešena u každého z nich samostatně. Na úrovni přepínačů se používá na zvýšení spolehlivosti stohování, klastrování a kaskádování přepínačů.

Stohování přepínačů umožňuje snadné rozšiřování portů přepínačů umístěných v montážní skříni, konfigurace přepínačů pomocí jedné IP adresy, konfigurace je uložena v každém členu stohu a celý stoh se chová jako jeden systém. Nevýhodou je vyšší cena přepínačů, nutnost speciálního portu a propojování přepínačů speciálním kabelem.

Stohování je vhodné do přístupové části sítě, kde je vysoký počet přístupových míst a zároveň se očekává zvyšování přístupových míst ve vyšším počtu (školy, velké firmy apod.). Přepínače ve stohu jsou umístěny nejčastěji v rozvodné místnosti.

Klastrování umožňuje také konfiguraci všech přepínačů v klastru pomocí jedné IP adresy jako stohování. Konfigurační soubory jsou uloženy v přepínači příkazů klastru a záložním přepínači. Členové klastru mají samostatné konfigurační soubory. Nové přepínače se musí přidávat ručně.

Kaskádování je nejjednodušší možností rozšiřování topologie sítě, ale každý přepínač musí být konfigurován samostatně a musí minimálně podporovat Spanning Tree Protocol, aby se zabránilo smyčkám. Kaskádovat lze všechny přepínače.

Kaskádování a klastrování lze použít jak v distribuční, tak i v přístupové části sítě. Obě technologie umožňují jednoduché rozšiřování sítě (jak velkých, tak i menších firem, škol apod.).

Při praktických pokusech, na reálně používaném, zapojení přepínačů do stohu se ověřila spolehlivost a funkčnost tohoto způsobu zapojení, bez nutnosti zásahu správce. Toto zapojení se ukazuje jako velice vhodná alternativa kvůli využití stále více používaných optických kabelů, díky snižující se ceně za tyto kabely, k vzájemnému propojení přepínačů do kruhové topologie a nastavením stohovacího managementu. Nevýhodou tohoto zapojení je dlouhá doba rekonfigurace v případě nutného restartu celého stohu.

LITERATURA

- [1] Avinetworks: Single point of failure. [online]. Avinetworks [cit 2020-11-30]. Dostupné z:
<https://avinetworks.com/glossary/single-point-of-failure/>
- [2] Catalyst 3750-X and 3560-X Switch Software Configuration Guide. [online]. Cisco [cit 2020-11-30]. Dostupné z:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html
- [3] Catalyst 3750-X and 3560-X Switch Software Configuration Guide. [online]. Cisco [cit 2020-11-30]. Dostupné z:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swclus.html
- [4] Jordán, V., Ondrák, V.: Infrastruktura komunikačních systémů II: kritické aplikace. Brno: CERM, Akademické nakladatelství 2015. ISBN 978-80-214-5240-4
- [5] Jordán, V.: Redundance - Multiple Ring - Sub-Ring a Ring-Coupling. [online]. 2017. Dostupné z:
<https://www.kybez.cz/clanky/detail?urltitle=spolehlivost-nedilna-a-casto-opomijena-soucast-bezpecnos-3>
- [6] Kritická komunikační infrastruktura – Centrum technické pomoci. Kki-ctp [online]. KKI-CTP [cit 2020-11-30]. Dostupné z:
<http://www.kki-ctp.cz/rizeni-slozenych-topologii/>
- [7] Kritická komunikační infrastruktura – Centrum technické pomoci. Kki-ctp [online]. KKI-CTP [cit 2020-11-30]. Dostupné z:
<http://www.kki-ctp.cz/23100-topologie/>
- [8] Novotný, V.: Architektura sítí. Brno: Vysoké učení technické 2012. ISBN 978-80-214-4450-8
- [9] Svatuška, J., Hubáček, M.: Možnosti stohování přepínačů směrovačů Cisco. [online]. 2010 Dostupné z:
<http://wh.cs.vsb.cz/sps/images/4/40/Svatuska-Hubacek-StackWise.pdf>
- [10] Top 5 high availability dedicated server solutions [cit 2020-11-30]. Dostupné z:
<https://www.accuwebhosting.com/blog/top-5-high-availability-dedicated-server-solutions/>

SEZNAM SYMBOLŮ A ZKRATEK

Zkratky:

BPDU	Bridge Protocol Data Unit
CDP	Cisco Discovery Protokol
GBIC	Gigabit Interface Converter
HADS	High Availability Dedicated Server
HiPer Ring	High Performance Ring
IOS	Input Output System
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Media Acces Control
MRP	Media Redundancy Protokol
PRP	Parallel Redundancy Protocol
RSTP	Rapid Spanning Tree protocol
RM	Ring Manager
SPOF	Single Point of Failure
SRM	Sub Ring Manager
STP	Spanning Tree Protocol
STA	Spanning Tree Algorithm
TCA	Topology Change Acknowledgment
TCN	Topology Change Notification
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network