ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

NÁVRH A PROVEDENÍ MODERNIZACE PODNIKOVÉ DATOVÉ SÍTĚ

BAKALÁŘSKÁ PRÁCE

Vladislav Merhout
Přírodovědná studia, obor Informatika se zaměřením na vzdělávání

Vedoucí práce: Dr. Ing. Jiří Toman

Plzeň, 2017

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 18. dubna 2017

.....

vlastnoruční podpis

PODĚKOVÁNÍ

Chtěl bych poděkovat svému vedoucímu bakalářské práce Dr. Ing. Jiřímu Tomanovi za odborné vedení, za pomoc a rady při zpracování této práce.

ZDE SE NACHÁZÍ ORIGINÁL ZADÁNÍ KVALIFIKAČNÍ PRÁCE.

OBSAH

SEZNAM ZKRATEK

SAGE	–	Semi-Automatic Ground Enviroment
ENIAC	–	Electronic Numerical Integrator And Computer
USA	–	United States of America
SSSR	–	Svaz sovětských socialistických republik
IPTO	–	Information Processing Techniques Office
ARPANET	–	Advanced Research Project Agency Network
ARPA	–	Advanced Research Project Agency
DARPA	–	Defense Advanced Research Project Agency
UCLA	–	University of California, Los Angeles
UCSB	–	University of California, Santa Barbara
SCRI	–	Stanford Central Research Institute
NPC	–	Network Control Protocol
IMP	–	Interface Message Processor
TCP/IP	–	Transmission Control Protocol / Internet Protocol
UDP	–	User Datagram Protocol
MILNET	–	Military Network
NSFNET	–	National Science Foundation Network
NSF	–	National Science Foundation
VBNS	–	Very high-speed Backbone Network Service
SDN	–	Software Defined Networks
HP	–	Hewlett-Packard
ATM	–	Asynchronous Transfer Mode
OSPF	–	Open Short Path First
iBGP	–	internal Border Gateway Protocol
eBGP	–	external Border Gateway Protocol
P router	–	Provider router
RR	–	Route Reflector
AC	–	Alternating Current
SIP	–	SPA Interface Procesor
SPA	–	Shared Port Adapters
SFP	–	Small Form-Factor Pluggable
RJ45	–	Registered Jack 45
DWDM	–	Dense Wavelength Division Multiplexing
PE router	–	Provider Edge router
PA	–	Port Adapter
L3	–	Layer 3
ISO-OSI	–	International Standards Organization – Open System Intercon
OUI	–	Organizationally Unique Identifier
MAC	–	Media Access Control
CDP	–	Cisco Discovery Protocol
VLAN	–	Virtual Local Area Network
LAN	–	Local Area Network
IEEE	–	Institute of Electrical and Electronics Engineers

L2	–	Layer 2
FCS	–	Frame Check Sequence
RADIUS	–	Remote Authentication Dial In User Service
STP	–	Spanning-Tree Protocol
NIX	–	Neutral Internet Exchange
BPDU	–	Bridge Protocol Data Units
TCN	–	Topology Change Notification
TCA	–	Topology Change Acknowledgement
MPLS	–	Multiprotocol Label Switching
MP-BGP	–	Multiprotocol-Border Gateway Protocol
IGP	–	Interior Gateway Protocol
RFC	–	Request For Comments
IPv6	–	Internet Protocol version 6
VLSM	–	Variable Length Subnet Mask
SPF	–	Short Path First
LSU	–	Link State Update
LSR	–	Link State Request
LSA	–	Link State Advertisements
DR	–	Designated Router
BDR	–	Backup Designated Router
IP	–	Internet Protocol
IPv4	–	Internet Protocol version 4
IETF	–	Internet Engineering Task Force
QoS	–	Quality of Service
SONET	–	Synchronous Optical Network
AToM	–	Any Transport over MPLS
VPN	–	Virtual Private Network
BoS	–	Bottom of Stack
TTL	–	Time To Live
LDP	–	Label Distribution Protocol
BFD	–	Bidirectional Forwarding Detection
LLDP	–	Link Layer Discovery Protocol
DSCP	–	Differentiated Services Code Point
MIC	–	Modular Interface Cards
LSP	–	Label Switch Path
RSVP-TE	–	Resource Reservation Protocol – Traffic Engineering
RSVP	–	Resource Reservation Protocol
EF	–	Expedited Forwarding
SSHv2	–	Secure Shell version 2
SNMP	–	Simple Network Management Protocol
RTT	–	Road Trip Time
ICMP	–	Internet Control Message Protocol

1 ÚVOD

V polovině 20. století jsme naučili počítače spolu mluvit. Stálo to hodně úsilí naučit je stejné a následně vzájemné řeči. Jejich komunikační schopnosti jsme v průběhu let posunuli do téměř nepředstavitelné roviny. Počítačová síť umožňuje komunikaci na velké vzdálenosti v reálných časech, poskytuje a vyžaduje data. První komunikační protokoly a datové uzly vznikají v národních vědeckých laboratořích a na univerzitách v polovině 20. století. Síť, tak jak ji známe dnes, je tu od přelomu tisíciletí. A neplatí to jen pro veřejnou síť – internet, ale i pro podnikovou síť – intranet. Podnikové sítě vznikají z důvodu vysokého tempa nasazování počítačů. Je to reakce na požadavek rychlejší vzájemné komunikace a spolupráce. Totiž časová úspora mezi odesláním a příjmem emailu, nebo naopak dopisu je zjevná.

Denně se generují a přesouvají data, vyvíjejí se nové aplikace a služby. Datová síť tyto informace přenáší, avšak není schopna reflektovat neočekávané změny, protože na ně není připravena. Datová síť může vykazovat flexibilitu v propustnosti dat, ale z hlediska konfigurace bude vždy rigidní architekturou. Každá síť je limitována vlastním nastavením a každá síť je druhý den zastaralá, protože byla konfigurována na základě požadavků dneška. Je běžnou praxí, že nedojde k přenosu informace datovou sítí, což má vždy svůj důvod. Potíže většinou identifikuji v nedostatečné kapacitě linky. Analýzou stavu sítě téměř vždy jen potvrdím domněnku její nutné modernizace.

Předmětem zájmu je podniková datová síť, jejíž rostoucí nespolehlivost a ztrátu funkcionalit lze vyřešit pouze vhodnou modernizací. Zabývám se návrhem modernizace datové sítě a její realizací dle požadavků uživatele. Pokud stav sítě těmto požadavkům nevyhovuje, tak je potřeba navrhnout změny vedoucí k navýšení její propustnosti a spolehlivosti. Tedy je nevyhnutelné infrastrukturu modernizovat na roveň požadavků uživatele.

Jako první vždy analyzuji datovou síť a zjišťuji její stav. Následně zvolím vhodnou technologii a topologii s redundantními datovými spoji, vyberu adekvátní síťový protokol a zabývám se konfigurací. Na závěr je nutné takto modernizovanou sít otestovat a tím ověřit navýšení rychlosti přenosu dat, prioritizaci, redundanci datových cest a zatížení směrovače. Cílem práce je modernizovat datovou síť na základě požadovaných funkcionalit.

2 POČÍTAČOVÁ DATOVÁ SÍŤ

2.1 HISTORIE

Globální mezilidskou nesnášenlivost v uplynulém století lidstvo řeší dvěma světovými válkami. Propuknutí třetí, a zřejmě na dlouho poslední, svět odvrací na bojišti bez fronty. Taková je studená válka, válka bez bitvy. Mocenské manýry USA a USSR sleduje celý svět z pohledu rukojmích velmi obezřetně, avšak se strachem, neboť na mysl se dostává reálné vypuknutí atomové války. Jenže každá strana má rub a líc. Zní paradoxně, že války jsou bezprecedentním hybatelem výzkumu a vývoje v mnoha odvětvích, že válka přináší objevy (NATO Rewiev, 2015). Významně jsou reflektovány změny v lékařství (moderní chirurgie, psychiatrie), což je určitou splátkou civilnímu obyvatelstvu, jenže pozornost se v první řadě vždy věnuje vývoji nových zbraní (atomové zbraně), strojů (bezpilotní prostředky) nebo materiálů (titan).

Elektronický boj a špionáž je také forma války, ale zde hraje prim počítač. Vývoji počítačů se za druhé světové války dostalo nebývalé pozornosti, podpora vývoje a jejího potencionálního využití podstatně urychlilo technický pokrok (Marlib, 2017). Díky válečným okolnostem vznikají samostatné skupiny výpočetních systémů – šifrovací a dešifrovací zařízení. V Německu byly vyrobeny kalkulátory Z1 a Z2 (K. Zuse a H. Schreyer), v Americe těžké zařízení Harvard Mark 1 (Howard H. Aiken) a ještě těžší ENIAC (John W. Masuchly, John P. Eckert, John von Neumann). ENIAC byl čistě vojenský projekt na sestavování dělostřeleckých zaměřovacích tabulek (VTM, 2017). Alan Turing položil svoji prací základy informatiky a pomocí zařízení Turingova Bomba se dařilo dešifrovat německé zprávy šifrované Enigmou.

Za studené války docházelo k velkým pokrokům na poli vědy a techniky, zejména pak v rámci vesmírného programu. Vědecký pracovník vývoje raketového nosiče byl Wernher von Braun. Jedná se o téhož člověka, který stál za vývojem německé balistické rakety V-2. V tomto období ukázal velký potenciál propojení počítačových systémů. V roce 1954, na základě požadavku vzdušných sil USA, vznikl program SAGE, který měl za úkol vybudovat kontinentální systém protivzdušné obrany před jaderným útokem ze Sovětského svazu (Technet, 2013). Systém byl uveden do provozu v roce 1963 a skládal se z 24 řídících center, 3 bojových center a více než 100 radarových pozic po celé zemi, které byly

s řídícími centry propojeny dálkovými telefonními kabely, čímž je vytvořena první rozsáhlá počítačová síť. Na programu SAGE spolupracoval i Joseph Licklider, který se později stal ředitelem oddělení IPTO, která iniciovala výzkum vedoucí k vytvoření ARPANETu. Síť SAGE zůstala v provozu až do roku 1983.

2.2 VÝVOJ A STRUKTURA

Ve vývoji datových sítí existují milníky, které ovlivnili vývoj sítí do podoby, jak je známe dnes. Například síť ARPANET, která byla předchůdcem sítě Internet. Síť ARPANET vznikla jako požadavek ministerstva obrany USA. Tato síť by řešila komunikaci orgánů administrativy USA v případě jaderné války. Důraz byl kladen na decentralizaci, v případě výpadku části sítě (nebo její zničení), aby nedošlo ke zhroucení celé sítě a tím i systému řízení (Peterka, 2015). Projektu se ujala firma RAND, která přišla v roce 1964 s možným řešením – síť nebude mít centrální složku a bude navržena tak, aby fungovala i v případě, že jsou některé její části nedostupné (zničené, vypnuté). V tomto případě si budou všechny uzly sobě rovné a počítaly s přenosy, které budou nespolehlivé.

Tyto požadavky stály u zrodu, v té době, revoluční myšlenky – rozdělit datový provoz na stejně velké části a budou se sítí přenášet jako samostatné celky. Každý samostatný celek bude mít informaci o adrese svého příjemce a cesta k příjemci vždy bude volena samostatně, bez vlivu ostatních celků. Samostatnému celku se začalo říkat paket a technice přenosu přepojování paketů (ang. packet switching). Poprvé byla tato technika implementována ve Velké Británii (experimentální síť National Physical Laboratory) počátkem roku 1968 (SystemOnLine, 2017). Obdobný experiment se odehrál i v USA za finanční podpory grantové agentury ARPA patřící pod ministerstvo obrany USA. Podle této agentury byla tato síť pojmenována.

První datové uzly se začaly budovat na univerzitách a jejich výpočetních centrech. V těchto centrech se nacházeli superpočítače, vzájemně propojené sítí ARPANET. Cílem bylo umožnit k těmto superpočítačům vzdálený přístup. Od roku 1969 byly uzly umístěny na UCLA, UCSB, SRI a univerzitě v Utahu a byly propojeny pevnými okruhy o rychlosti 50kb/s. Uzel byl realizován pomocí počítače Honeywell DDP516 a protokol byl použit NCP (network control protocol). Počítače Honeywell byly naprogramovány tak, aby fungovaly jako IMP (interface message processor). ARPANET se začal rychle rozšiřovat o další uzly, v roce 1971 bylo

součástí sítě 15 uzlů, v roce 1972 bylo součástí již 37 uzlů a v roce 1973 se připojily první zahraniční uzly v Norsku a Velké Británii. Záhy však dochází k vystřízlivění, co se způsobu využití týče.

Původní záměr spočíval ve využití vzdáleného připojení k práci, ale v reálu z ARPANETu vznikl elektronický poštovní úřad. Uživatelé si začali posílat osobní i pracovní vzkazy, na dálku začali spolupracovat na projektech, předávali si zkušenosti a případně poznatky. V této době již možnost komunikovat s ostatními lidmi uživatele lákala mnohem více, než práci na vzdálených superpočítačích.

Další z milníků byl vznik rodiny protokolů TCP/IP. Tento milník byl financován agenturou ARPA (v této době již přejmenovanou na DARPA) a první verze protokolu TCP byla prezentována v roce 1973 na univerzitě v Sussex. Postupem času dochází k zásadní koncepční změně, protokol TCP měl převzít veškeré akce spojené s nápravou chyb při přenosu, se ztrátou dat, resp. z TCP byl vytvořen „spolehlivý protokol“, negativní vlastností byla zvýšená režie přenosu (Juniper, 2015). Časem se ukázalo, že tento spolehlivý protokol není vhodný pro určité aplikace, kterým poškozené soubory nevadí tolik, jako případně zpoždění (přenos hlasu).

Na základě těchto poznatků došlo k rozdělení původního TCP na protokol IP, který se staral o přenos a neřešil spolehlivost a na nový protokol TCP, který využíval služeb protokolu IP a k tomu přidával ještě spolehlivost přenosu. Vedle nového TCP protokolu byl vytvořen UDP protokol. Tento protokol také využíval služeb IP protokolu, ale nezajišťoval spolehlivý přenos (Hanks, a další, 2012). Dával přednost rychlosti a pravidelnému přísunu dat než spolehlivosti.

V roce 1982 došlo ze strany Pentagonu k radikálnímu rozhodnutí, všechny počítače připojené do ARPANETu musí povinně přejít na protokoly TCP/IP (ARPANET byl z rozpočtu Pentagonu financován). Tímto rozhodnutím byl ARPANET od 1. 1. 1983 neprůchozí pro jakékoliv pakety protokolu NCP. V roce 1983 Pentagon oddělil od ARPANETu ty části, které měli něco společného s vojenstvím a vytvořil samostatnou síť MILNET, schopnost komunikovat s ARPANETem byla zachována (Peterka, 2015). ARPANET tímto získal mnohem civilnější náplň práce. Postupem času se síť ARPANET dostávala do pozadí a sloužila jako páteřní síť, na kterou se začali připojovat další a další sítě. Toto neustálé nabalování a propojování sítí vedlo ke vzniku velké sítě složené z menších

sítí – internet. K tomuto nabalování a dalšímu připojování sítí k ARPANETu pomohlo i „dozrání“ technologie ethernet.

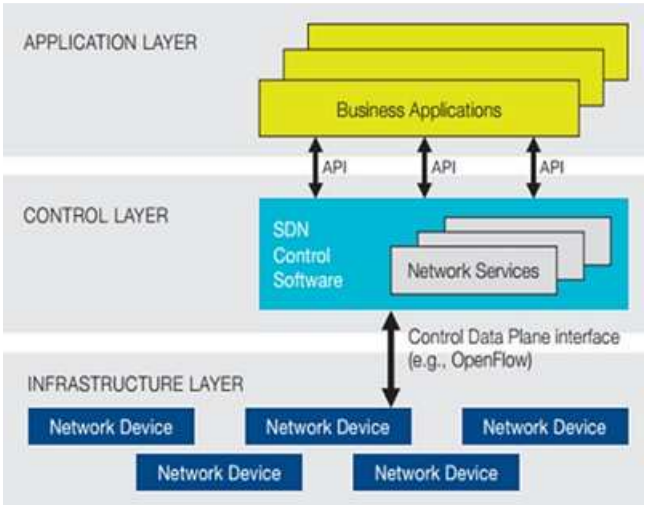
Pro další vývoj sítě ARPANET byl přelomový okamžik připojení sítě NSFNET, která byla zřízena institucí NSF (v USA má tato instituce na starosti podporu vědy a výzkumu). Po neshodách při připojení 5 výpočetních středisek do ARPANETu se NSF rozhodlo vystavět vlastní síť. Díky štědrému přísunu peněz bylo možné NSFNET připojit u dosud nepřipojených univerzit a akademických institucí. Při tomto masovém připojování byly průběžně navyšovány páteřní linky, nejdříve z 1,5 Mb/s (1989) a o něco později na 45Mb/s.

V roce 1990 byl ARPANET v tichosti vypnut a zrušen, NSFNET do této doby úplně převzal úlohu páteřní sítě všech připojených sítí. Od tohoto okamžiku začínají vznikat sítě komerční, které přebírají i funkci NSFNETu (tato síť omezuje komerční provoz) a v dnešní době existují globální datové sítě tvořící páteř Internetu (Hanks, a další, 2012). NSF pomalu tlumí provoz této sítě, ale zdaleka nekončí – zaměřila se na rozvoj vysokorychlostních síťových technologií programu VBNS, která bude mít za úkol opět propojit 5 akademických datových středisek vybavených superpočítači.

2.3 SOUČASNÝ TREND

V současně době existuje ve světě bezpočet datových sítí, některé jako privátní, experimentální (výzkumné), veřejné nebo komerční. Tyto sítě se i nadále vyvíjejí, aby splňovali požadavky svých uživatelů. Pro uživatele to znamená nižší latence, vyšší přenosovou rychlost a spolehlivost. Ze strany správců je v současnosti kladen důraz na jednodušší a centralizovanou konfiguraci, spolehlivost a případnou jednoduchou nahraditelnost datových prvků (cisco, 2017).

Dnes se hovoří o softwarově definovaných sítích (SDN). Koncept SDN umožňuje oddělit směrovací logiku od řídící (obr. 1). To znamená, že se řízení sítě předá ze zařízení, která provádí směrování paketů, do řídící jednotky (SDN kontroler). Tím síť SDN umožní mít lepší centralizovanou správu a možnost jednoduše definovat a konfigurovat služby (SystemOnLine, 2017). Jedná se o vysoký stupeň automatizace. Sítí SDN se v současné době zabývají významní výrobci, od Barracuda Networks, Cisco, HP až Huawei (Odom, a další, 2009). Ve skutečnosti, pokud nastane potřeba udělat v síti změny, lze tyto změny provézt z jednoho místa bez nutnosti aktualizovat každý prvek sítě zvlášť, což je pracné a náročné na lidské zdroje.



Obr. 1 Schéma konceptu SDN.

Zdroj: https://image.slidesharecdn.com/frescosdnsecurity20130419-130913021956-phpapp01/95/fresco-sdn-security-ndss2013-presentation-slides-3-1024.jpg?cb=1379038857

V tomto okamžiku je SDN konceptem, který není zralý na komerční nasazení ve velkém měřítku. V tom menším jej již využívá Google ve své páteřní části sítě (pro řízení sítě si vytvořil vlastní zařízení). Díky SDN získal globální pohled i dohled nad sítí a zlepšil využití svých stávajících datových linek (Anuta Networks, 2013). Na koncept SDN se upírá pozornost i poskytovatelům datových center, kteří budou moci těžit z optimalizace datových přenosů.

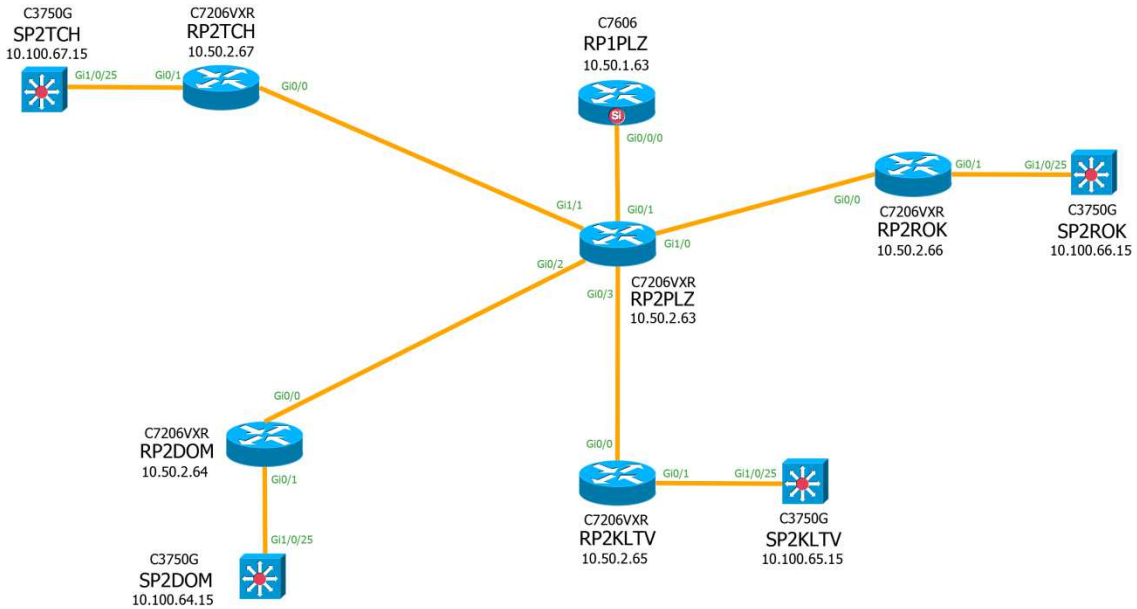
Zavedením SDN sítí bude mít dopad na architekturu, flexibilitu sítě i na služby jako takové. Bude se jednat o sítě reagující okamžitě na požadavky zákazníka. I zde jsou ale věci, které je nutné vyřešit. Prvním problémem je standardizace celého řešení, další neznámou je zpětná kompatibilita funkcí známých z dnešních sítí a často chybějící podpora spanning-tree může v takto otevřené architektuře mít za následek vznik smyček.

3 METODIKA

Tato kapitola se zabývá rozborem současného stavu datové sítě, specifikací nedostatků, návrhem nové datové sítě splňující vstupní požadavky a konfigurací jednotlivých datových prvků.

3.1 VYMEZENÍ A CHARAKTERISTIKA PROBLÉMU

Původní datová síť byla vybudována jako neveřejná, podniková datová síť pokrývající území České republiky do úrovně okresních měst. V této práci se budu zabývat modernizací sítě v Plzeňském kraji. Výstavba páteřní optické sítě byla realizována v roce 2006 nákupem vlastních optických vláken z hlavního technologického centra v Plzni do okresních technologických center v Tachově, Domažlicích, Klatovech a Rokycanech (obr. 2).



Obr. 2 Ilustrace topologie sítě před modernizací.
Zdroj: Vlastni

3.2 ANALÝZA SÍTĚ PŘED MODERNIZACÍ

Původní datová síť byla vybudována v roce 2007, kdy nahradila předchozí síť typu ATM a Frame-relay vystavěnou na zařízení Newbridge MainStreet Xpress a směrovačích řady Cisco 3600. I když v té době pracovalo zařízení spolehlivě, přenosovou kapacitou nestačilo na stále zvyšující se požadavky přenosu dat, zejména obrázků, zvýšené režii programů a multimediálních webových stránek. Řešení tohoto nevyhovujícího stavu spočívalo v migraci páteřní sítě z ATM na

technologii ethernet a obměnu směrovačů Cisco 3600 za výkonnější Cisco 7600 a 7200, včetně úpravy topologie a nasazení nových směrovacích protokolů OSPF a iBGP.

Nyní v roce 2017 opět stojíme před projektem modernizace původní datové sítě, která má za úkol odstranit technologické nedostatky, které se za těchto 10 let provozu objevily. Nedostatky sítě jsou:

1. Nedostatečná kapacita datové sítě.
2. Nedostupnost rozhraní vyšších rychlostí.
3. Chybějící redundance datových linek.
4. Chybějící prioritizace datového provozu.

3.2.1 SÍŤOVÁ ZAŘÍZENÍ

V krajském technologickém centru se nachází směrovače Cisco C7606 a C7206VXR. Cisco C7606 – jedná se o šasi se šesti sloty pro rozšiřující karty (obr. 3). Směrovač je nakonfigurován v roli „P router“ a zároveň plní funkci RR pro iBGP protokol, je osazen dvěma napájecími AC zdroji (redundance napájení – funkčnost zajištěna i v případě výpadku jednoho zdroje) a ve slotu č. 5 se nachází řídící modul WS-SUP720-3B Supervisor Engine.

Obr. 3 Řídící modul WS-SUP720-3B.
Zdroj: http://www.cisco.com/c/dam/en/us/products/collateral/switches/mgx-8800-series-switches/product_data_sheet09186a0080159856.doc/_jcr_content/renditions/product_data_sheet09186a0080159856-1.jpg

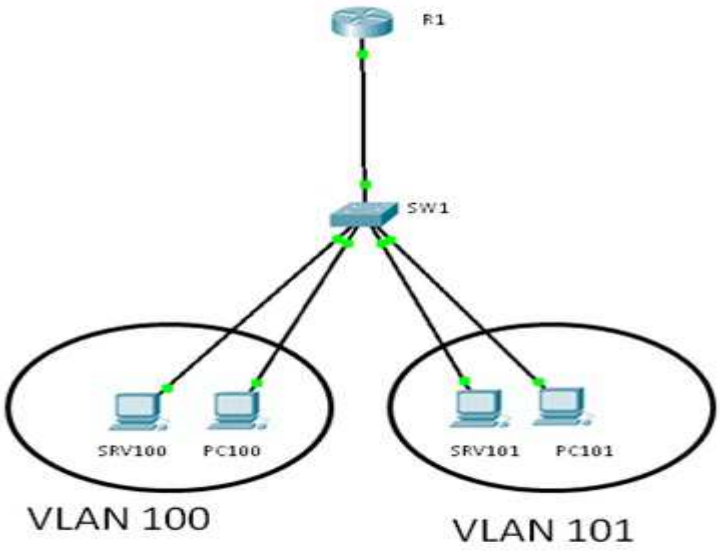
Sloty 1–4 jsou osazeny rozšiřujícími SIP moduly. Každý SIP modul disponuje čtyřmi SPA pozicemi, do kterých se vládají Shared Port Adapter s již klasickým rozhraním SFP nebo RJ45. Propoj mezi C7606 a DWDM ONS15530 je realizován

pomocí multimode optického kabelu rychlostí 1 Gb/s. DWDM řeší datový provoz pouze na první vrstvě.

Okresní technologická centra jsou osazena směrovači C7206VXR (obr. 4). Jedná se o velmi často nasazované směrovače v „enterprise“ a „service provider“ sítích jako „PE router“. Směrovač je osazen řídícím modulem NPE-G2 se třemi SFP šachtami. Má k dispozici 6 slotů pro rozšiřující karty PA, napájení je řešeno dvěma zdroji. Opět v případě výpadku jednoho zdroje je druhý zdroj schopný udržet směrovač v provozu. Za oblibou a četností výskytu tohoto boxu hovoří i široká škála podporovaných protokolů a rozhraní, pro příklad – FastEthernet, STM-1, T1/E1, T3/E3, ATM, X21.

Obr. 4 Směrovač Cisco C7206VXR.
Zdroj: http://i.ebayimg.com/images/g/S6EAAOxyn9BRZbfO/s-l1600.jpg

Mimo Cisco C7206VXR je v okresním technologickém centru i přepínač Cisco C3750G. Tento 24 portový gigabitový přepínač je se směrovačem propojen multimode optickým kabelem v modu trunk, rozhraní LC-LC. Přepínač má možnost pracovat i na L3 (routovat), ale momentálně se tato funkce nevyužívá (obr. 5). V tomto případě se jedná o tzv. „router-on-stick“.



Obr. 5 Router-on-stick.
Zdroj: Vlastní

3.2.2 FYZICKÁ VRSTVA

Na optických vláknech jsou nasazeny multiplexery Cisco ONS 15530, které vytváří jednu přenosovou kapacitu 2,5 Gb/s. Nejedná se zde o klasické pojetí DWDM, kdy je do optického vlákna vyzařováno více vlnových délek. V tomto případě je využívána pouze jedna vlnová délka o kapacitě 2,5 Gb/s, do které jsou multiplexovány vstupní timesloty (celkem 48). Tyto timesloty jsou následně přiděleny jednotlivým kanálům, které jsou reprezentovány vstupními/výstupními porty na kartě multiplexeru. Na jedné kartě se nachází 8 portů. Pro připojení směrovače slouží první port (kanál) s celkem 20 timesloty.

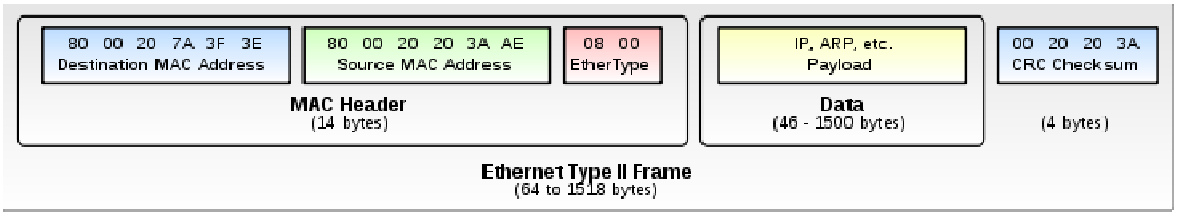
Pro každý propoj centrum – okres je použita jedna karta s 8 porty, v případě Plzně je DWDM osazeno 4 kartami (směr Tachov, Domažlice, Klatovy a Rokycany) a v okresních technologických centrech je DWDM zařízení osazeno jednou kartou (pouze směr Plzeň). Z výše uvedených důvodů bylo nutné provést modernizaci i samotné DWDM technologie, která bude plnohodnotná (vysílání na více vlnových délkách) a umožní přenos škály rychlostí od 1 Gb/s do 10 Gb/s, s možností výhledově navýšit přenos až na 100 Gb/s.

3.2.3 SPOJOVÁ VRSTVA

Druhá vrstva ISO-OSI, z ang. „data-link layer“. Datové jednotky přenášené spojovou vrstvou se nazývají rámce (obr. 6). Tato vrstva zajišťuje v síti komunikaci s dalšími datovými prvky v rámci jednoho síťového segmentu na sdíleném médiu,

detekuje a opravuje chyby vzniklé na fyzické vrstvě. Komunikace je zajišťována pomocí MAC adres, což je 48bitové číslo zapsané v hexadecimálním tvaru v 6 oktetech – první 3 oktety reprezentují identifikaci výrobce (OUI) a další tři oktety jsou již výrobcem přidělovány jakkoli. Příklad známých výrobců a jejich OUI:

Dell:	00-14-22
Nortel:	00-04-DC
Cisco:	00-40-96
Belkin:	00-30-BD



Obr. 6 Schéma datového rámce.

Zdroj: http://crankypotato.com/wp-content/uploads/2010/05/1000px-Ethernet_Type_II_Frame_format.svg_.png

- Protokol CDP

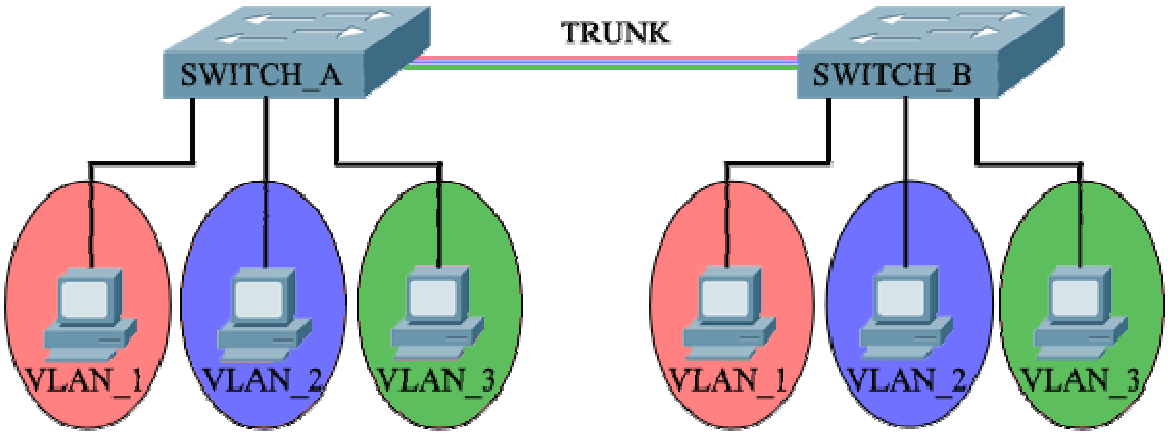
Jedná se o cisco proprietární protokol pro detekci přímo připojených zařízení, které jsou také od firmy Cisco. I když některé zařízení jiných výrobců (např. Huawei nebo Mikrotik) umějí s CDP pracovat. Protokol funguje na druhé vrstvě, komunikace probíhá jednocestně a nedochází k potvrzování přijatého oznámení, pro detekci se využívá multicastový rámec s cílovou adresou 01-00-0c-cc-cc-cc, který obsahuje informaci o zařízení, operačním systému, IP adrese a fyzickém portu, ze kterého je CDP oznámení odesláno.

Zařízení odesílá CDP oznámení každých 60 sekund, v CDP tabulce si záznamy drží 180 sekund (holdtime) a každým příchozím CDP oznámením se holdtime nastaví zpět na 180. V případě přerušení datového spojení je tento záznam po 180 sekundách z tabulky vymazán. V původní datové síti je protokol nakonfigurován na všech datových prvcích Cisco.

- Virtuální LAN

VLAN specifikuje norma IEEE 802.1q. Umožňuje nám vytvořit v rámci jedné fyzické lokální sítě více virtuálních sítí, které mezi sebou nemohou přímo komunikovat. Tuto možnost poté umožní až směrovač, tzv. interVLAN routing.

Nejlepší využití VLAN – VLAN 1, 2, 3 – počítače jsou připojené do jednotlivých virtuálních sítí (obr. 7). V praxi toto rozdělení může být založeno na organizační struktuře (obchodní oddělení / vývojové oddělení / oddělení nákupu) nebo podle využívaných služeb, např. ve VLAN 1 se mohou nacházet servery a není žádoucí, aby v té samé síti se nacházely uživatelské stanice. Takového rozdělení LAN sítě je dosaženo pomocí TAGování.

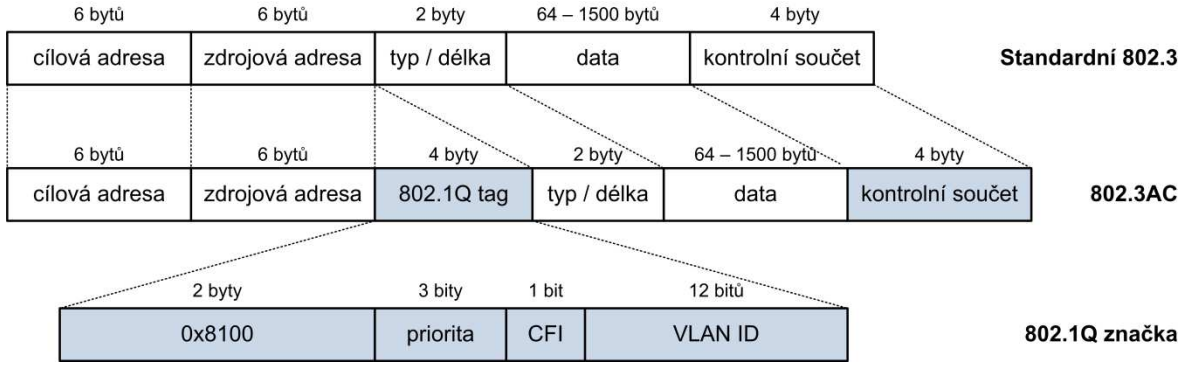


Obr. 7 Počítače připojené do jednotlivých virtuálních sítí.
Zdroj: Vlastní

Každá hlavička ETH rámce je doplněna o čtyřbajtovou značku, která obsahuje:

- TPID – identifikátor typu rámce (v tomto případě obsahuje hodnotu 0 x 8100), pro zařízení podporující VLANy je to informace, že další dva bajty ponesou informace o VLAN.
- PCP – tříbitová hodnota uživatelské priority rámce, definováno normou IEEE 802.1p.
- CPI – jednobitový identifikátor říkající v jakém tvaru je MAC adresa (kanonický/nekanonický).
- VID – dvanáctibitová hodnota specifikující číslo VLANy (1–4094, čísla 0 a 4095 jsou rezervována pro 0 x 000 a 0 x FFF).

Díky přidání 802.1q TAGu se zvětší L2 rámec o 4bajty a dojde k přepočtu FCS. Takový rámec specifikuje norma IEEE 802.1ac (obr. 8).



Obr. 8 Ilustrace změn v hlavičce.

Zdroj: Vlastní

Výhody takového rozdělení do virtuálních sítí jsou:

- Zmenšení broadcastové domény – broadcast se šíří pouze mezi členy dané VLANy.
- Jednodušší správa – připojení v dané VLANě se řeší pouze konfigurační změnou, nemusí se provádět fyzické přepojení nebo natažení nového datového kabelu.
- Méně switchů – díky logickému rozdělení sítě na switchi a možnosti přiřadit fyzický port do dané VLANy není nutné pro danou síť mít další hardware.

Možnost přiřadit uživatele do VLAN jsou:

- Podle portu – konfigurace konkrétního portu do konkrétní VLANy.
- Podle MAC adresy – port se zařadí do VLANy podle zdrojové MAC adresy uživatelské stanice.
- Podle protokolu/IP adresy – zde se provede přiřazení portu do VLANy na základě informace z 3. vrstvy.
- Podle autentizace – pomocí protokolu IEEE 802.1x dojde k ověření uživatele a na základě informací z RADIUSu dojde k přiřazení portu do VLANy.

➢ Trunk

Trunk přímo souvisí s VLAN, jedná se o dvoubodový spoj mezi datovými prvky (nejčastěji dva přepínače), který umožňuje přenos více VLAN. Pokud by nebyla funkce trunk k dispozici, muselo by existovat pro každou virtuální sít vlastní fyzické propojení. Přepínač rozlišuje VLANy podle VLAN TAGu, který se nachází v L2 hlavičce datového rámce. Díky tomu nedochází k „promíchání“ datového provozu.

➢ Spanning-tree protokol (STP)

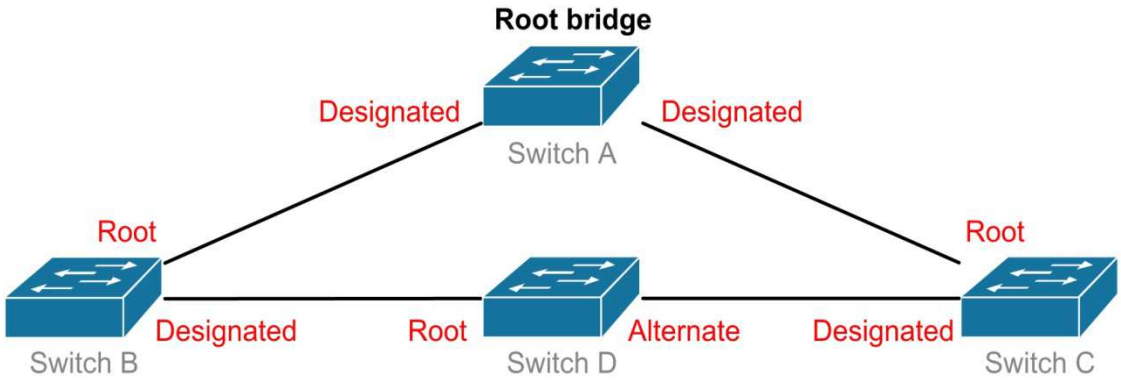
STP je další z celé řady protokolů pracujících na druhé vrstvě ISO-OSI modelu (obr. 9). V roce 1985 Radia Perlmanová vyvinula ve firmě Digital Equipment Corporation algoritmus pro první verzi STP. V roce 1990 byl protokol standardizován jako IEEE 802.1d. Do dnešních dní dochází k vylepšování a urychlování práce protokolu.

Hlavní úlohou protokolu je odstraňovat v přepínané síti smyčky. Protokol garantuje, že mezi dvěma přepínači v síti existuje jediná aktivní cesta. STP je ve výchozím nastavení na Cisco přepínači zapnutý a nedoporučuje se vypínat. V dnešní době rozlehlých lokálních sítí může nastat okamžik, kdy bude vytvořena smyčka – ať úmyslně (redundantní zapojení, load-balancing), nebo neúmyslně (chyba administrátora, opětovné propojení switchů mezi sebou).

V případě absence STP je vysoká pravděpodobnost výskytu tzv. „Broadcastové bouře“. S výskytem Broadcastové bouře má v České republice zkušenost i samotné peeringové centrum NIX. STP používá ke své činnosti zprávy zvané BPDU, TCN a TCA. Pomocí těchto zpráv se vytváří logický strom nad kruhovou fyzickou topologií (volba root bridge, určení rolí portů, blokování portů).

Role portů:

- Root – port, který je připojen k root bridge, každý přepínač má pouze jeden root port.
- Designated – na tento port je připojená další část sítě (další přepínač).
- Non-designated – v tomto případě dochází na switchi k blokování odchozího provozu tímto portem. Záložní cesta – v případě výpadku root portu se stav Non-designated portu mění na root. Rozlišuje dva stavy – Alternate (záložní cesta k root bridge) a Backup (záložní cesta do jiného segmentu).



Obr. 9 Kruhová topologie přepínačů a role portů STP.

Zdroj: Vlastní

V čase se protokol STP vyvíjel s požadavky na LAN sítě, např. použití VLAN nebo jiného TAGovacího mechanismu (místo Cisco proprietárního trunk protokolu ISL použit 802.1q).

Verze protokolu STP:

- Rapid Spanning-tree Protocol (RSTP) – definován normou IEEE 802.1w, poskytuje rychlejší konvergenci, cca 1 vteřinu, v případě změny topologie, v roce 2004 došlo k revizi a protokol byl sloučen do normy 802.1d.
- Per-Vlan Spanning Tree (PVSTP) – vychází z IEEE 802.1d, jedná se o cisco proprietární protokol, pro každou VLAN běží samostatná STP instance (pomocí konfigurace lze rozprostřít datovou zátěž jednotlivých VLAN na jiné porty – load balancing), pouze pro ISL trunk.
- Per-Vlan Spanning Tree Plus (PVSTP+) – od předchozího typu STP pouze přidává podporu dot1q trunku (IEEE 802.1q), jedná se také o cisco proprietární protokol.
- Multiple Spanning Tree Protocol (MSTP) – definován IEEE 802.1s a později sloučen do IEEE 802.1q-2005. Jedná se o rozšíření RSTP, lze definovat skupinu VLAN do jedné STP instance.
- Rapid Per-Vlan Spanning Tree Plus (RPVSTP+) – vychází z IEEE802.1w, přidává podporu samostatné RSTP instance pro každou VLAN.

Princip funkčnosti Spanning-tree protokolu:

1. V síti musí být zvolen tzv. root bridge a to dle zadané priority v konfiguraci a MAC adresy, výchozí hodnota priority = 32768, lze zadat manuálně a to pomocí násobků 4096 (0-4096-8192-12288-atd.) s tím, že nižší číslo má vyšší váhu. Volba probíhá výměnou BPDU rámců mezi přepínači s uvedenou prioritou (v případě defaultní nebo stejné hodnoty priority se přepínače rozhodují dle nejnižší MAC adresy).
2. Následuje volba root portů – což je zjištění nejkratší, případně nejlepší cesty k root bridge. Nejkratší cesta nemusí být cestou nejlepší, během vyjednávání

jsou ohodnoceny jednotlivé linky dle rychlosti – tzv. cena linky, čím nižší cena, tím lepší cesta (tab. 1). Pokud existují na jednom přepínači dvě cesty k root bridge se stejnou cenou, rozhodne číslo portu (nižší vyhrává). Ceny linek hodnocené STP.

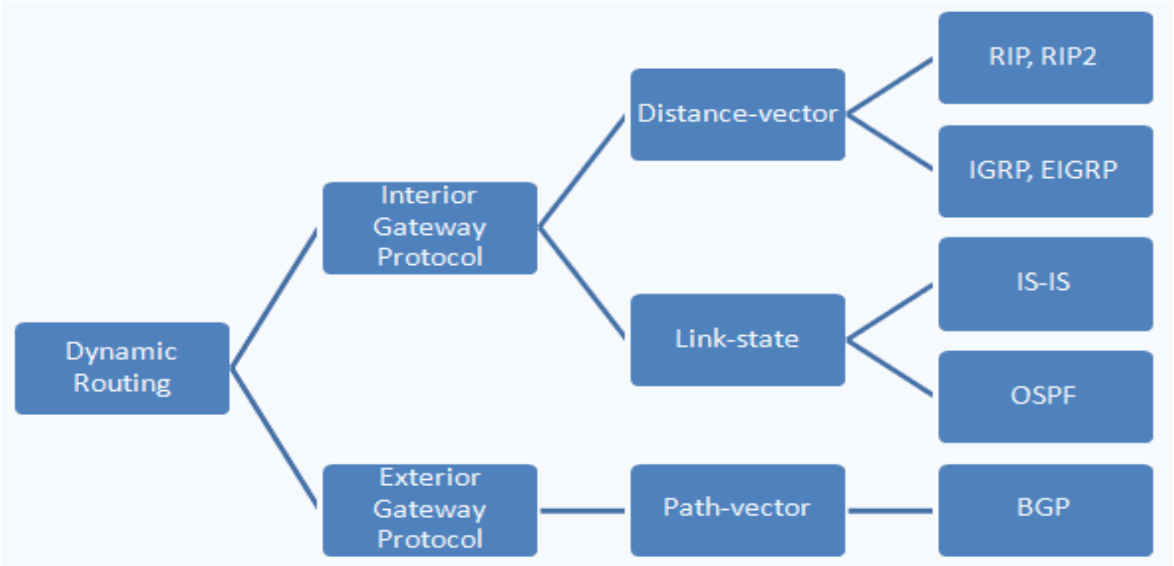
Tab. 1 Ceny linek hodnocené STP

Rychlost linky	Cena linky
10 Mb/s	2 000 000
100 Mb/s	200 000
1 Gb/s	20 000
10 Gb/s	2 000

3. Volba designated a non-designated portů – již probíhá během volby root portu, pokud na port přijde BPDU rámec s vyšší prioritou než má switch sám, tento port se nastaví jako designated a analogicky protilehlý port přejde do stavu non-designated/alternate (tím se zamezí vzniku smyčky).

3.2.4 SÍŤOVÁ VRSTVA

Původní IP infrastruktura je realizována na bázi technologie Gigabit Ethernet a MPLS. Topologie se sestává ze směrovače Cisco 7606 (krajské technologické centrum) a Cisco 7206VXR (krajské technologické centrum a okresní technologická centra) zapojených do hvězdy bez redundantních spojů. V síti funguje několik dynamických směrovacích protokolů, které se primárně dělí podle oblasti použití (obr. 10).



Obr. 10 Schéma rozdělení směrovacích protokolů.

Zdroj: http://www.samuraj-cz.com/gallery2/000771.gif

Každý z dynamických protokolů je oceněn tzv. „administrative distance“ (administrativní vzdálenost). Pokud směrovač pracuje s více směrovacími protokoly, tak tato hodnota říká, který z nich je „důvěryhodnější“ – čím nižší číslo, tím důvěryhodnější (obr. 11). Původní datová síť používá „přepínací“ protokol MPLS a dynamické protokoly OSPF a MP-BGP.

Route Source	Default Distance	Routing Table Entry
Connected interface	0	C
Static route out an interface	0	S
Static route to a next-hop address	1	S
EIGRP summary route	5	D
External BGP	20	B
Internal EIGRP	90	D
IGRP	100	I
OSPF	110	O
IS-IS	115	i
RIPv1, RIPv2	120	R
Exterior Gateway Protocol (EGP)	140	E
ODR	160	O
External EIGRP	170	D EX
Internal BGP	200	B
Unknown	255	

Obr. 11 Směrovací protokol – důvěryhodnost.

Zdroj: https://i2.wp.com/www.ebrahma.com/wp-content/uploads/2013/10/Administrative-Distance.png

- Protokol OSPF

Protokol se používá pro interní směrování uvnitř autonomního systému (AS). Jde o Link-state IGP. AS může být infrastruktura celorepublikového operátora, podniková síť anebo i menší bezdrátová síť. V dnešní době se používá OSPFv2 definovaná normou RFC 2328. Normou RFC 5340 byl OSPF rozšířen o podporu IPv6 – OSPFv3 (verze v2 a v3 nejsou navzájem kompatibilní). OSPF podporuje VLSM, sumarizaci je nutné konfigurovat ručně.

V rámci protokolu je možné směrovače umisťovat do oblastí (area). Hlavní oblastí je AREA 0 (backbone), která slouží jako tranzitní oblast. Pokud se objeví AREA, která nemůže být přímo připojena do AREA 0, musí se vytvořit virtuální linka (virtual-link), která vytvoří logický propoj do AREA 0 skrze tranzitní AREU. I

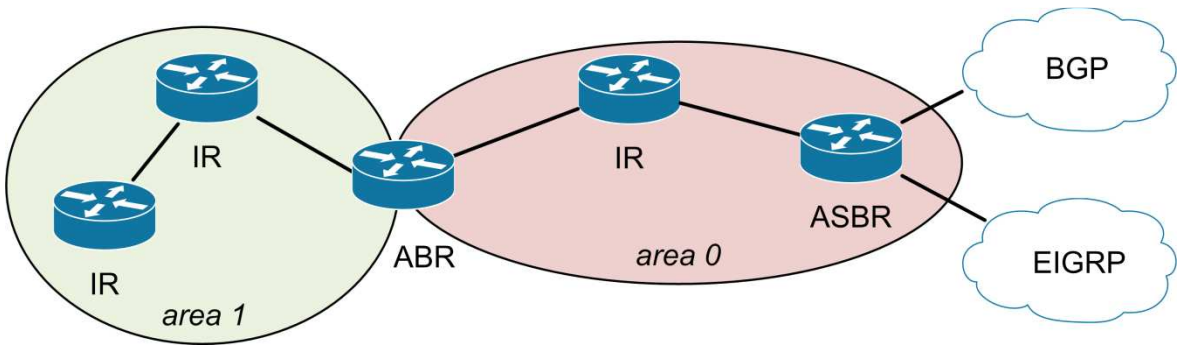
díky oblastem je možné vytvořit hierarchickou topologii, snížit výpočet SPF a snížit počet LSU.

OSPF rozeznává několik typů sítí, pro každou se chová trochu odlišně:

- Point-to-Point (PtP) – síť, která propojuje pouze dva směrovače, protokol OSPF v této síti komunikuje přes multicast adresu 224.0.0.5.
- Point-to-Multipoint (PtMP) – v subnetu (např. /27) se nachází více směrovačů, ale OSPF se konfiguruje jako Point-to-Point ke každému směrovači zvlášť. Komunikace probíhá na multicast adrese 224.0.0.5.
- Broadcast Multiaccess (BMA) – v subnetu (např. /27), kde je možné vysílat broadcasty, je připojeno více než dva směrovače. V síti je volen DR (designated router) se kterým následně ostatní naváží „sousedství". Komunikace probíhá na multicast adresách 224.0.0.5 a 224.0.0.6.
- Nonbroadcast Multiaccess (NBMA) – filozofie vychází z BMA sítě, jen nelze přes síť přenášet broadcast, ten je nahrazen unicastem a v konfiguraci protokolu je nutné specifikovat sousedy.

Nejen, že OSPF rozeznává sítě, ale směrovače mají v rámci AS i určitě funkce v závislosti na umístění (obr. 12).

- Internal router (IR) – má všechny své porty v jedné oblasti (AREA).
- Area Border Router (ABR) – propojuje dvě a více oblastí a v každé oblasti má alespoň jeden port.
- Autonomous Systém Boundary Router (ASBR) – propojuje dva a více AS. Například provádí redistribuci rout z jiného směrovacího protokolu do vlastní OSPF instance.



Obr. 12 Funkce směrovače v závislosti na umístění.

Zdroj: Vlastní

V první řadě, po správné konfiguraci protokolu, dochází k navazování „sousedství“, které má čtyři fáze:

1. INIT – směrovač obdržel hello paket od souseda, nastavení procesu vyjednávání.
2. EXCHANGE – dochází k výměně Database Descriptions (DBD).
3. LOADING – pomocí LSR se směrovače vzájemně dotazují na konkrétní informaci z DBD, jako odpověď slouží LSU.
4. FULL – navázané sousedství a kompletně synchronizovaný link-state databáze.

V případě sítí BMA a NBMA jsou fáze ještě doplněny o stav EXSTART, kdy dochází k volbě DR a BDR, následně navazování sousedství pokračuje fází EXCHANGE. OSPF protokol je velmi citlivý na konfiguraci, pro vytvoření sousedství jen nutné nastavit shodně hello interval, dead interval, IP adresu sítě (vč. wildcard masky) a číslo oblasti. V našem případě je procesem OSPF směrována i IP adresa Loopbacku (vnitřní interface), který vždy ve stavu „UP“. V tomto případě bude IP adresa Loopbacku dostupná vždy, pokud bude existovat alespoň jedna funkční cesta přes OSPF. Toto bude důležité pro protokol BGP.

Pro výpočet nejkratší cesty se používá Dijkstrův algoritmus (SPF), který se spouští nad link-state databází. Důležitým parametrem pro výpočet nejkratší cesty je cena (metrika), která je tvořena součtem cen jednotlivých linek do cílové sítě.

Cena je vyjádřena vztahem:

$$\text{Cena} = \frac{\text{Referenční šířka pásma}}{\text{šířka pásma}}$$

Referenční šířka pásma je ve směrovačích Cisco nastavena na výchozí hodnotu 100 Mb/s. Šířka pásma je rychlost daného portu. Problém nastává u výpočtu linek rychlejších než 100 Mb/s, neboť jsou stejně ohodnoceny jako právě 100 Mb/s. Referenční šířku pásma lze v konfiguraci změnit, tato změna se musí provést na všech OSPF směrovačích v daném AS. Referenční šíře pásma ve třetím sloupci je ponechána na výchozí hodnotě a ve čtvrtém sloupci navýšena na 10 Gb/s (tab. 2).

Tab. 2 Referenční šíře pásma.

Linka/ technologie	Nomin. Rychlost	Ref. bandwidth 100 Mb/s	Ref. bandwidth 10 Gb/s
Ethernet	10 Mb/s	10	1 000
FastEthernet	100 Mb/s	1	100
GigabitEthernet	1 Gb/s	1	10

10GbE	10 Gb/s	1	1

Výsledkem SPF je vytvoření stromu nejkratších cest, ze kterého je sestavena směrovací tabulka. Pokud v oblasti nastane změna v topologii (výpadek nebo připojení dalšího portu), směrovač, na kterém změna nastala, vygeneruje LSA a ten je v celé oblasti šířen formou záplavy (flooding), každý směrovač v zaplavené oblasti LSA zpracuje, tzn. provede změnu link-state databáze a odstartuje přepočet cest pomocí SPF, LSA je přeposláno na další směrovače, ale jen v rámci dané oblasti.

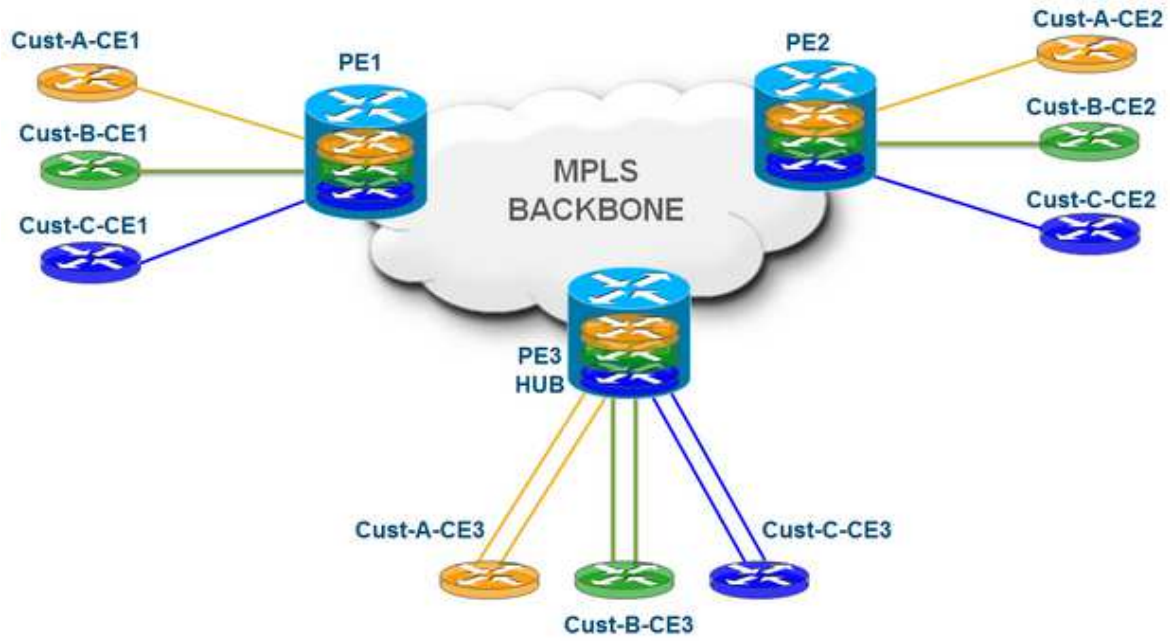
- MPLS

Protokol sloužící k přepínání paketů pomocí labelu (návěstí), který je umístěn mezi L2 a L3 hlavičkou. Z tohoto důvodu se MPLS technologii říká také layer 2.5 technologie. Historie protokolu začíná v roce 1996, kdy Ipsilon Networks navrhla technologii IP switching (pomocí „flow management protocol“) určenou pouze pro ATM sítě. Vedle toho firma Cisco přišla s vlastním návrhem, který nebyl omezen jen na ATM sítě, tzv. tag switching. Návrh byl předán organizaci IETF ke standardizaci.

První RFC na MPLS bylo vydáno v roce 2001 (RFC 3031). Z pohledu zákazníka lze na MPLS pohlížet jako na transportní infrastrukturu, obdobně jako na Frame-relay nebo ATM. V podstatě vybírá to nejlepší ze síťových technologií. Z ATM a Frame-relay využívá bezpečnost a QoS, z IP zas flexibilitu a rozšiřitelnost. Technologie MPLS je protokolově nezávislá a dokáže přenášet různé druhy provozu – IP pakety, přenos ATM, SONET i ethernetové rámce (technologie AToM).

Mezi benefity použití MPLS v datové síti je:

- Nedochází ke směrování, ale forwardování – směrovač nahlíží pouze do L2, kde se nachází MPLS Label, šetří čas procesoru a paměť
- Traffic Engineering – funkcionalita umožňující upravit cestu určitého datového provozu skrze MPLS páteř na základě definovaných pravidel a požadavků
- MPLS/VPN – privátní datová síť oddělená od dalších privátních datových sítí (obr. 13).



Obr. 13 MPLS/VPN.

Zdroj: http://www.anutanetworks.com/wp-content/uploads/2014/06/mpls-backbone.png

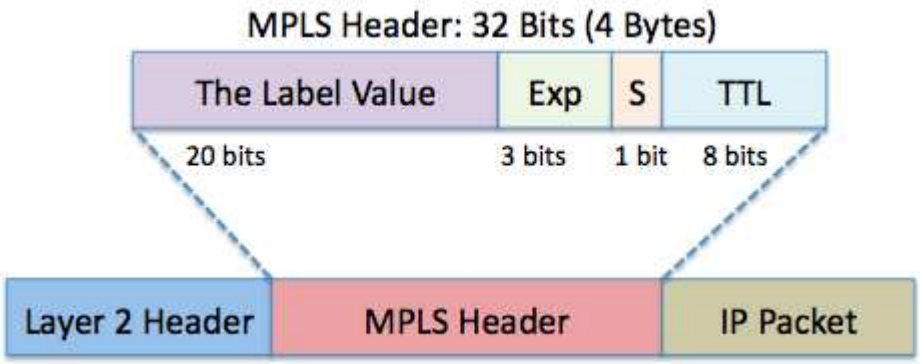
I v MPLS síti mají jednotlivé směrovače své funkce:

- Ingress LSR (LER) – nachází se na hranici MPLS sítě a slouží jako vstupní bod, přidává do příchozího datového provozu návěstí (label) – operace push, podle kterého je dál forwardován.
- Transit LSR – stará se pouze o forwardování paketů dle návěstí, v případě změny návěstí se provádí operace swap.
- Egress LSR (LER) – nachází se na hranici MPLS sítě, který odebírá návěstí z paketu – operace pop, a paket je dál směrován mimo MPLS síť.

Z důvodu velkého vytížení hraničního směrovače je možné operaci „pop“ přenechat předposlednímu LSR směrovači (soused s hraničním egress LSR). Jedná se o funkci PHP (ang. Penultimate Hop Popping), kdy předposlední směrovač odstraní návěstí z paketu a odešle jej na egress LSR, který již provede směrování mimo MPLS síť.

Samotné MPLS návěstí je velké 32bitů a obsahuje (obr. 14):

20 bitů – návěstí
3 bity – Experimental (slouží pro QoS)
1 bit – BOS indikátor
8 bit – TTL

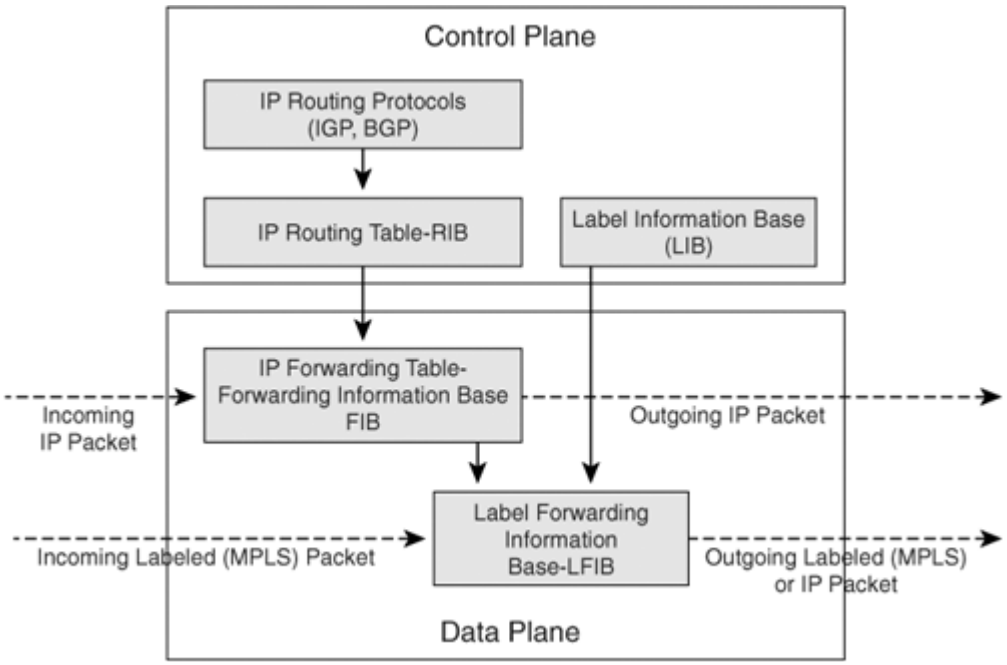


Obr. 14 MLPS návěstí.
Zdroj: https://i.stack.imgur.com/KOX1A.png

Protokol LDP – v MPLS síti je nutná komunikace mezi směrovači a k této komunikaci právě slouží tento protokol. Je definován RFC 5036 a slouží pro distribuci návěstí v prostředí MPLS. LDP se navazuje přímo mezi sousedy, v první části je vysílán „LDP discovery" na multicast adresu 224.0.0.2, port UDP 646. Poté, co je sousedství navázáno přechází provoz do unicastu na port TCP 646.

Jak funguje MPLS (obr. 15):

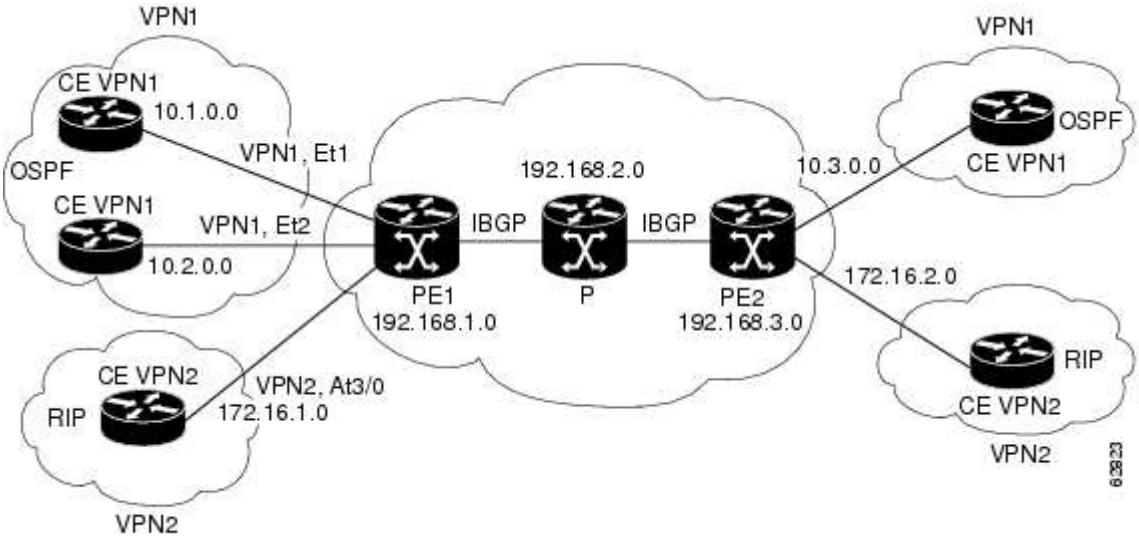
- IGP protokol na ingress LSR zjistí dostupnost cílové sítě (zda ve směrovací tabulce existuje prefix cílové sítě).
- LDP protokol zajistí MPLS návěstí pro daný paket, návěstí se vloží mezi L2 a L3 hlavičku (push) a následně dojde k odeslání dat do MPLS sítě.
- LSR skrze MPLS síť přepínají paket dle návěstí, případně návěstí během transportu mění (swap).
- Na Egress LSR je návěstí odebráno (pop) a jako standardní IP paket je směrován mimo síť MPLS.



Obr. 15 Směrování a přepínání v rámci směrovače.

Zdroj: http://flylib.com/books/2/686/1/html/2/images/1587051990/graphics/01fig09.gif

MPLS/VPN – jedna z velmi ceněných vlastností umožňující sdílení, případně pronájem transportní infrastruktury dalším subjektům (obr. 16). Zjednodušeně řečeno, každý subjekt může mít v rámci MPLS svoji vlastní síť (VPN), která neovlivňuje ostatní sítě a také není ovlivňována ostatními sítěmi (překrývání IP rozsahů s dalším subjektem).

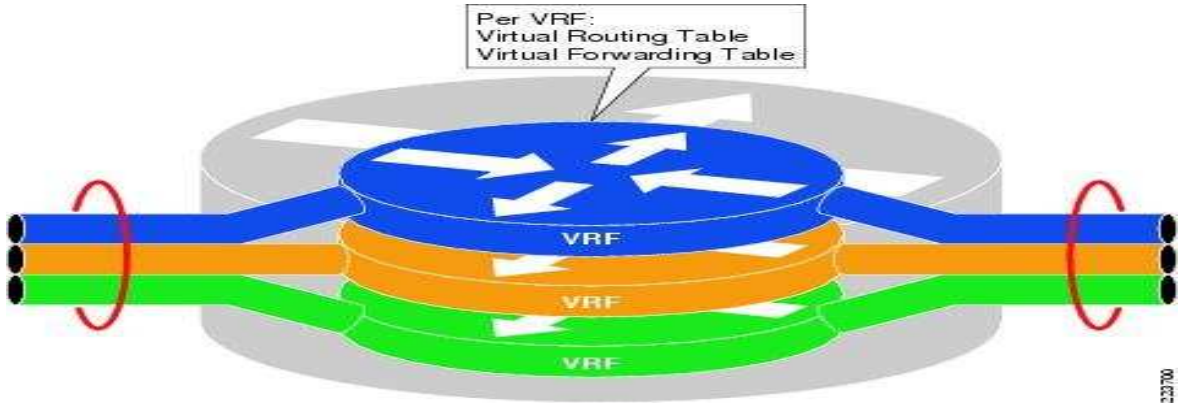


Obr. 16 MPLS/VPN

Zdroj:
http://www.cisco.com/c/dam/en/us/td/docs/ios/12_0s/feature/guide/fsvnmb25.fm/_jcr_content/renditions/62823.jpg

Rozdělení sítě a přiřazení paketů do takové sítě docílíme pomocí route-distinguisher (RD) nakonfigurovaný na PE směrovačích. RD definuje 64 bitové číslo dané VPN (je jedinečné v MPLS síti), které slouží jako rozšíření k již stávajícím 32 bitům IP v4 adresy paketu. Tím vzniká 96 bitová VPN v4 adresa, podle které je prováděno směrování na příslušný „PE router" pomocí protokolu iBGP. Pro každý RD vzniká na „PE routeru" vlastní směrovací tabulka.

V případě více skupin sítí se stejným požadavkem na připojení je možné vytvořit na „PE routeru" „Virtual Routing and Forwarding Table" – VRF. Nejdříve se VRF vytvoří a poté se v rámci VRF definuje RD, route-target a porty routeru směrem k externímu subjektu (obr. 17). Tímto způsobem máme připravenou šablonu pro konfiguraci této VPN pro další sítě daného subjektu, stačí jen do konfigurace portu přidat název VRF.

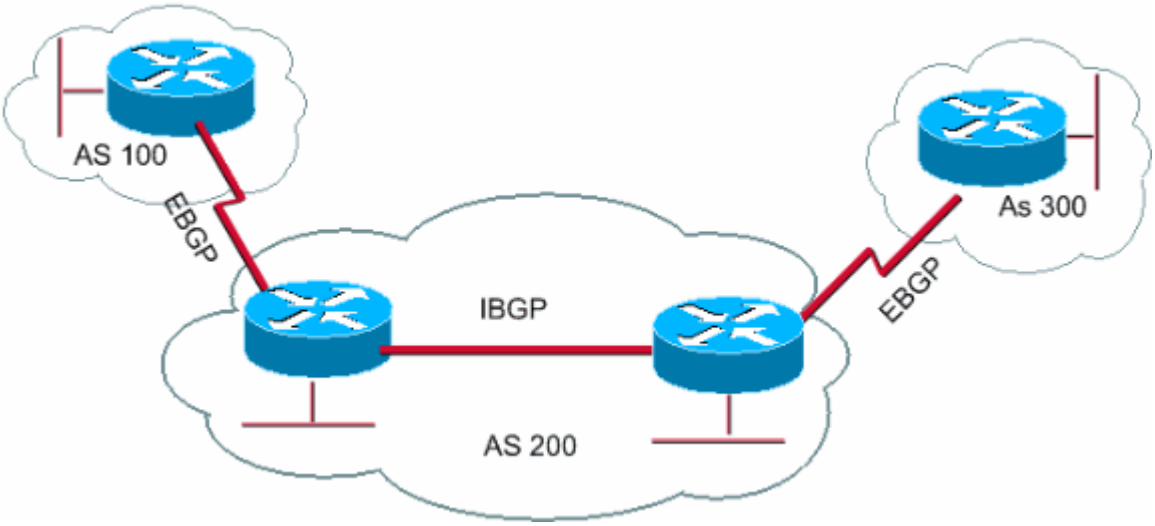


Obr. 17 VRF v rámci směrovače.
Zdroj: https://cdn.plixer.com/wp-content/uploads/2009/12/vrfDiagram.jpg

- BGP

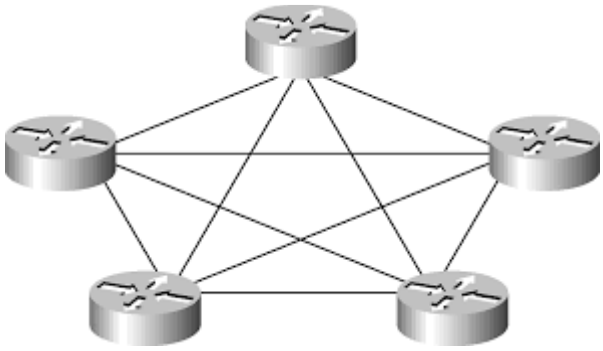
Jedná se o vnější, path-vector směrovací protokol, který realizuje směrování mezi autonomními systémy (eBGP) nebo mezi „PE routery" uvnitř AS (iBGP) a jako metriku používá počet AS v cestě (hop count, čím méně tím lépe) a velmi pestrou paletu politik a pravidel. Používá port TCP 179 a směrovač informuje své sousedy pouze o změnách (neposílá celou směrovací tabulku).

Aktuální verze je BGP-4 definována RFC 4271 z roku 2006 a v současném Internetu je v provozu již od roku 1994. V tomto odstavci se budeme věnovat spíše verzi iBGP (konkrétně MP-BGP), který je použit v původní tak i v modernizované datové síti. Vazbu mezi BGP směrovači v různých AS nazýváme eBGP, vyžaduje přímé spojení sousedů (nastavené TTL na 1). Zato iBGP vazba vzniká mezi směrovači v rámci jednoho AS, zde stačí vazba pouze logická (obr. 18).



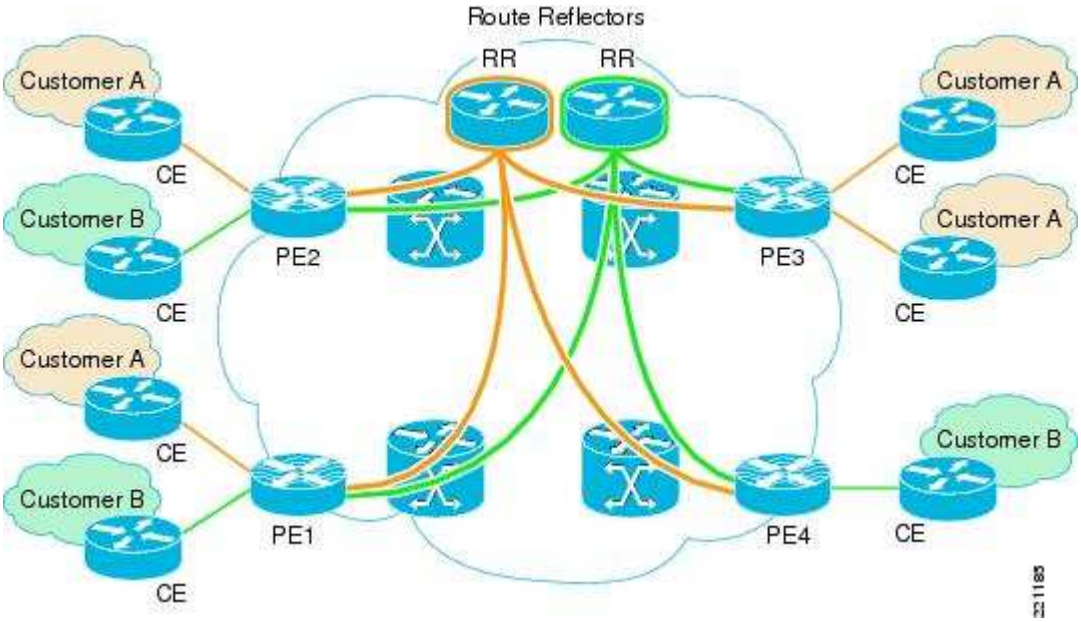
Obr. 18 Schéma BGP.
Zdroj: Vlastní

Pro stabilní iBGP vazbu se používá IP adresa Loopbacku (nikdy nejde do stavu DOWN), která je směrována IGP (např. OSPF). Takto se vytváří BGP vazby mezi loopbacky jednotlivých směrovačů. Routy naučené z iBGP se neposílají dalším iBGP sousedům, takže pokud se chtějí naučit směrovače všechny routy, musí být logické zapojení typu full-mesh (obr. 19).



Obr. 19 Zapojení full-mesh.
Zdroj: http://flylib.com/books/1/594/1/html/2/images/f0508.jpg

Tuto podmínku je možné obejít nasazením BGP „route-reflectoru“, se kterým mají všechny iBGP směrovače vytvořenou vazbu. „Route-reflector“ se stará o propagaci rout naučených z iBGP i eBGP (snížení počtu BGP vazeb). Situaci sítě s RR ilustruje obr. 20. V původní i v modernizované datové síti se používá MP-BGP, který umožňuje přenos různých typů adres, např. IPv4, IPv6, unicast i multicast. Standardní protokol BGP podporuje pouze IPv4 unicast adresy.



Obr. 20 Topologie sítě s RR.

Zdroj: https://patelrasesh.files.wordpress.com/2014/09/rr2.png

3.3 MODERNIZACE DATOVÉ SÍTĚ

V procesu modernizace datové sítě je důležité nezanedbat analýzu stavu původní infrastruktury. Specifické požadavky na novou datovou síť jsou obvykle předem nastavené, tedy známé. Nesnižuje to ale preciznost, s jakou se musí celá operace provést. Může se totiž stát, že požadovanému a tedy očekávanému výsledku budeme velmi vzdáleni. Na počátku je vždy nějaký nedostatek nebo problém, který je nutné identifikovat a řešit. Proto vzniká něco jako soupis požadavků na novou datovou síť. Návrh modernizace pak z těchto požadavků přímo vychází.

3.3.1 ANALÝZA VSTUPNÍCH POŽADAVKŮ

Nedostatky původní sítě:

- Nedostatečná kapacita datové sítě – maximální dostupná kapacita DWDM je v původní síti 1 Gb/s, cílem je navýšení rychlosti na 10 Gb/s s možností rozšíření až na 100 Gb/s.
- Obměna zastaralých typů směrovačů – směrovače řady Cisco C7600 a C7200 jsou již na hranici své životnosti (poruchy zdrojů napájení).
- Nedostupnost rozhraní vyšších rychlostí – původní směrovače nepodporují porty rychlejší než 1 Gb/s, nové zařízení musí být připraveno na rychlosti 10 Gb/s, výhledově až na 40 Gb/s.

- Chybějící redundance datových linek – v původní síti existuje pouze jediná datová cesta mezi krajským a okresním technologickým centrem, cílem je toto spojení zdvojit nezávislou datovou linkou o minimální rychlosti 1 Gb/s.
- Chybějící podpora IPv6 – původní směrovače nejsou schopny efektivně pracovat s IP v6 provozem, nové směrovače musí být připraveny na případný přechod na IP v6 bez snížení kvality datových služeb (zpomalení, enormní vytížení).
- Chybějící prioritizace datového provozu – v původní datové síti zcela neřešená problematika, v novém řešení datové sítě je vytvořen 8 úrovňový model QoS.

Specifické požadavky na datovou síť:

- Modulární platforma – možnost výměny HW komponent za běhu.
- Redundantní platforma – redundance zdrojů, ventilátorů a řídících jednotek.
- Neblokující architektura – při plném osazení se předpokládá dostatečná propustnost (kapacita) směrovače bez ponížení rychlosti datového provozu.
- Podpora MPLS.
- Podpora rychlé detekce výpadku datové linky.
- Počet rozhraní ve směrovači:
    - Minimálně 20x SFP 1 Gb/s.
    - Minimálně 4x XFP 10 Gb/s.

3.3.2 SPECIFIKACE SÍŤOVÝCH PROTOKOLŮ

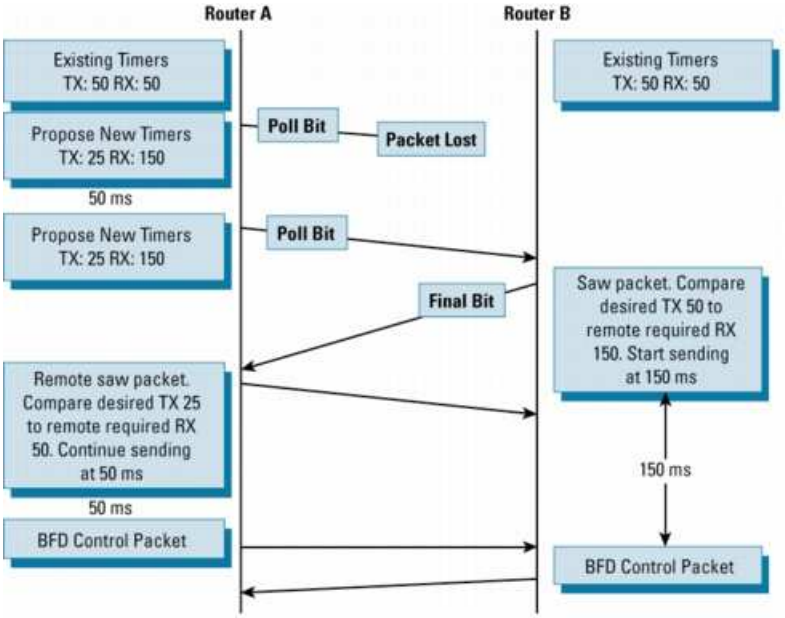
V nové datové síti byly použity nové protokoly a nastavení, které v původní síti nebylo možné použít a to nejčastěji z důvodu stáří předchozích prvků. V nové datové síti bude nakonfigurován IGP OSPFv2, MPLS a pro směrování jednotlivých sítí ve VRF mezi „PE routery“ MP-BGP. Jedná se o standardní design service-provider sítí. Jednotlivé směrovací protokoly jsou doplněny o protokol BFD a MPLS o konfiguraci QoS. Pro L2 discovery je použit místo CDP (cisco proprietární) protokol LLDP.

- Protokol BFD

Protokol z dílny firem Juniper Networks a Cisco Systems, definovaný IETF RFC 5880. Jedná se o jednoduchý „hello“ protokol, který pravidelně posílá BFD pakety

(UDP) mezi dvěma směrovači, které mají za úkol detekovat výpadek datové linky. Informaci o výpadku poté předá směrovacímu protokolu, který provede okamžitě změnu ve směrování.

BFD protokol je v modernizované síti použit s protokolem OSPF a BGP a je provozován v asynchronním režimu. Jeden směrovač sehraje hlavní roli, kdy sousedovi je poslán BFD paket s nízkou frekvencí, soused vysílá také své vlastní BFD pakety, ale do „H bit" parametru nastaví „Slyším tě" jako reakci na příchozí BFD paket (obr. 21). Tímto je navázána komunikace a v dalším kroku dochází ke zvýšení frekvence zasílaných BFD paketů (rychlejší zjištění výpadku linky). Frekvence zasílaných BFD paketů může dosahovat již 100ms, z tohoto důvodu musí být protokol snadno zpracovatelný a s nízkou režií.



Obr. 21 Proces vyjednávání BFD protokolu.

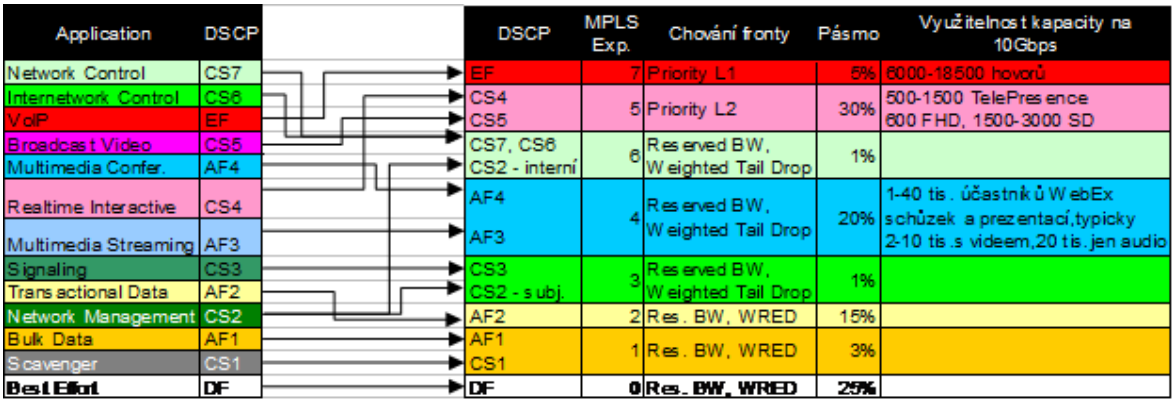
Zdroj:
http://www.cisco.com/en/US/technologies/tk648/tk365/tk480/images/0900aecd80244005_null_null_null_02_28_05-03.jpg

- MPLS QoS

QoS se v počítačových sítích v současné době skloňuje ve všech pádech. Umožňuje nám konkrétní provoz zvýhodnit, omezit, vyhradit, třídit a následně pro provoz spravedlivě rozdělit pásmo. V této kapitole se budeme zajímat o QoS v MPLS síti.

Pro zachování propustnosti sítě je na hraničních směrovačích nakonfigurován QoS, který zajistí sdílení kapacity linek mezi jednotlivé druhy provozu. Během datového přenosu v MPLS síti páteřní směrovače neprohlíží IP hlavičku paketu (z důvodu kontroly DSCP hodnoty), ale řídí se informacemi z MPLS hlavičky, kde se

nachází 3bitové pole „EXPERIMENTAL“ – to znamená možné zakódování 8 hodnot. Vzhledem k omezení plynoucí z velikosti pole, pouze 3bity, byl model o 12 provozních třídách snížen na 8, třídy s podobným typem provozu byly sloučeny do společné fronty (obr. 22). MPLS směrovač provádí klasifikaci provozu na vstupním rozhraní na základě hodnoty přenášené pomocí DSCP bitů a přiřazuje jej do jednotlivých tříd (forwarding class). Například forwarding class MULTIMEDIA (af31, af32, af33, af41, af42, af43) nebo forwarding class PRIORITY (af21, af22, af23).



Obr. 22 MPLS QoS třídy.

Zdroj: Vlastní

Při přenosu provozu se DSCP značky z příchozích paketů na hraničním vstupním MPLS směrovači překopírují do pole „EXPERIMENTAL“ a na základě této informace ostatní MPLS směrovače v cestě přiřazují tento provoz do již připravených tříd.

3.3.3 SPECIFIKACE NOVÝCH SMĚROVAČŮ

Tato část práce poskytne základní technické údaje směrovače Juniper MX 40 a MX 80, které byly použity pro modernizaci datové sítě, fungují na operačním systému JunOS a mají možnost rozšíření HW díky MIC modulům. V portfoliu firmy Juniper se jedná o edge-routery, MX 40 je možné povýšit na vyšší model pomocí SW licence bez nutnosti výměny HW. Aktuálně dosahuje maximální propustnosti 60 Gb/s u verze MX 40 a 80 Gb/s u verze MX 80. Vzhledově se od sebe oba typy neliší, jedná se o to samé šasi.

Specifikace centrálních směrovačů:

MX80-T-AC – šasi osazené dvěma AC zdroji, třemi MIC sloty a čtyřmi 10Gb XFP transceivery.

MIC-3D-2XGE-XFP – rozšiřující karta do MIC slotu s 2 x 10 Gb XFP porty.

MIC-3D-20GE-SFP – rozšiřující karta do MIC slotu s 20 x 1 Gb SFP porty.

XFP-10G-S – XFP 10Gb/s optický transceiver.

4x SFP-T – SFP metalický port RJ 45.

Specifikace okresních routerů:

MX40-T-AC – šasi osazené dvěma AC zdroji, dvěma MIC sloty a dvěma 10 Gb XFP transceivery.

MIC-3D-2XGE-XFP – rozšiřující karta do MIC slotu s 2 x 10 Gb XFP porty.

MIC-3D-20GE-SFP – rozšiřující karta do MIC slotu 20 x 1 Gb SFP porty.

2x XFP-10G-S – XFP 10 Gb/s optický transceiver.

1x SPF-T – SPF metalický port RJ 45.

Pomocí SW licence nejen že dochází k navýšení maximální propustnosti směrovače, ale také k „odemčení" dalších portů a MIC slotů. V případě MX 40 jsou odemčeny dva přední MIC sloty a dva přední XFP porty ze čtyř, u MX 80 se odemykají všechny čtyři vestavěné XFP porty a tři MIC sloty (dva vpředu a jeden vzadu).

3.3.4 KONFIGURACE

V této části dojde ke konfiguraci směrovače RPLZ1, který se nachází v krajském technologickém centru. Jeho funkcionalita v rámci sítě bude poměrně jedinečná. Nejen, že se jedná o „PE router" (stejně jako ostatní směrovače), ale je i součástí BGP RR Clusteru pro směrovače Plzeňského kraje (tab. 3).

Tab. 3 Ukázka základní konfigurace portů

set interfaces xe-0/0/0 description RPLZ2 set interfaces xe-0/0/0 mtu 9192 set interfaces xe-0/0/0 unit 0 family inet address 10.100.63.33/30
set interfaces xe-0/0/1 description RDOM1 set interfaces xe-0/0/1 mtu 9192 set interfaces xe-0/0/1 unit 0 family inet address 10.100.60.33/30
set interfaces xe-0/0/2 description RKLT1 set interfaces xe-0/0/2 mtu 9192 set interfaces xe-0/0/2 unit 0 family inet address 10.100.60.41/30
set interfaces xe-0/0/3 description RROK1 set interfaces xe-0/0/3 mtu 9192 set interfaces xe-0/0/3 unit 0 family inet address 10.100.60.49/30
set interfaces xe-1/2/0 description RTCH1 set interfaces xe-1/2/0 mtu 9192 set interfaces xe-1/2/0 unit 0 family inet address 10.100.60.57/30

```
set interfaces lo0 unit 0 description Loopback0
set interfaces lo0 unit 0 family inet address 10.100.1.63/32
```

- Konfigurace OSPF

Dále bylo nutné nakonfigurovat IGP, kterým je OSPF (tab. 4). OSPF je konfigurován na všech „PE routrech“ a propaguje všechny dvoubodové sítě a loopback adresy jednotlivých páteřních směrovačů. V protokolu je zapnutý „traffic-engineering shortcuts“, který umožní použít sestavenou LSP jako „next-hop“ (v důsledku to znamená, pokud má směrovač cílovou síť dostupnou s nižší metrikou přes LSP, je použita tato cesta, navazuje na technologii RSVP-TE, která bude popsána níže). Zároveň je v protokolu nakonfigurováno BFD pro rychlou detekci výpadku sousedního směrovače a LDP synchronizace.

V případě výpadku LDP spojení nebo nebylo LDP spojení plně ustanoveno, začne IGP propagovat tuto cestu s nejvyšší metrikou (vlastně tím dojde k vyřazení linky z provozu – ochrana před ztrátou MPLS rámců). K zabezpečení navázání OSPF spojení mezi směrovači je použit šifrovací mechanismus MD5, pro každý spoj je použito jedinečné heslo. Router-ID (identifikace směrovače v OSPF procesu) byl nakonfigurován podle loopback IPv4 adresy.

Tab. 4 Ukázka konfigurace OSPF, BFD, LDP synchronizace a TE-shortcut.

```
//konfigurace shortcut
set protocols ospf traffic-engineering shortcuts

//přiřazení Loopback do OSPF
set protocols ospf area 0 interface lo0.0 passive

//smer RPLZ2
set protocols ospf area 0 interface xe-0/0/0.0 interface-type p2p
set protocols ospf area 0 interface xe-0/0/0.0 authentication md5 0 key <_>
set protocols ospf area 0 interface xe-0/0/0.0 bfd-liveness-detection minimum-interval 2000
set protocols ospf area 0 interface xe-0/0/0.0 bfd-liveness-detection multiplier 2
set protocols ospf area 0 interface xe-0/0/0.0 bfd-liveness-detection full-neighbors-only
//směr RDOM1(Domažlice)
set protocols ospf area 0 interface xe-0/0/1.0 interface-type p2p
set protocols ospf area 0 interface xe-0/0/1.0 authentication md5 0 key <_>
set protocols ospf area 0 interface xe-0/0/1.0 bfd-liveness-detection minimum-interval 2000
set protocols ospf area 0 interface xe-0/0/1.0 bfd-liveness-detection multiplier 2
set protocols ospf area 0 interface xe-0/0/1.0 bfd-liveness-detection full-neighbors-only

//směr RKLT1(Klatovy)
set protocols ospf area 0 interface xe-0/0/2.0 interface-type p2p
set protocols ospf area 0 interface xe-0/0/2.0 authentication md5 0 key <_>
set protocols ospf area 0 interface xe-0/0/2.0 bfd-liveness-detection minimum-interval 2000
set protocols ospf area 0 interface xe-0/0/2.0 bfd-liveness-detection multiplier 2
set protocols ospf area 0 interface xe-0/0/2.0 bfd-liveness-detection full-neighbors-only

//směr RROK1(Rokycany)
set protocols ospf area 0 interface xe-0/0/3.0 interface-type p2p
set protocols ospf area 0 interface xe-0/0/3.0 authentication md5 0 key <_>
set protocols ospf area 0 interface xe-0/0/3.0 bfd-liveness-detection minimum-interval 2000
set protocols ospf area 0 interface xe-0/0/3.0 bfd-liveness-detection multiplier 2
set protocols ospf area 0 interface xe-0/0/3.0 bfd-liveness-detection full-neighbors-only

//směr RTCH1(Tachov)
set protocols ospf area 0 interface xe-1/2/0.0 interface-type p2p
set protocols ospf area 0 interface xe-1/2/0.0 authentication md5 0 key <_>
set protocols ospf area 0 interface xe-1/2/0.0 bfd-liveness-detection minimum-interval 2000
set protocols ospf area 0 interface xe-1/2/0.0 bfd-liveness-detection multiplier 2
set protocols ospf area 0 interface xe-1/2/0.0 bfd-liveness-detection full-neighbors-only

//zapnutí synchronizace LDP s OPSF
set protocols ospf area 0 interface all ldp-synchronization

//nastavení router-id
set routing-options router-id 10.100.1.63
```

- Konfigurace MPLS

Protokol MPLS, jako protokol 2.5 vrstvy, je konfigurován na jednotlivých rozhraních propojujících jednotlivá okresní centra s krajským centrem (tab. 5). Pro výměnu MPLS tagů je mezi jednotlivými směrovači nakonfigurován protokol LDP.

Tab. 5 Ukázka konfigurace MPLS a LDP.

```
set interfaces xe-0/0/0 unit 0 family mpls
set interfaces xe-0/0/1 unit 0 family mpls
set interfaces xe-0/0/2 unit 0 family mpls
set interfaces xe-0/0/3 unit 0 family mpls
set interfaces xe-1/2/0 unit 0 family mpls

set protocols mpls interface xe-0/0/0.0
set protocols mpls interface xe-0/0/1.0
set protocols mpls interface xe-0/0/2.0
set protocols mpls interface xe-0/0/3.0
set protocols mpls interface xe-1/2/0.0

set protocols ldp interface xe-0/0/0.0
set protocols ldp interface xe-0/0/1.0
set protocols ldp interface xe-0/0/2.0
set protocols ldp interface xe-0/0/3.0
set protocols ldp interface xe-1/2/0.0
```

- Konfigurace RSVP

Díky konfiguraci rozšíření RSVP-TE dochází k dynamickému vytváření jednotlivých P2P LSP mezi „PE routery“ (tab. 6). Pro rychlou konvergenci LSP na záložní linku v případě poruchy hlavní linky nebo sousedního směrovače je použita funkce “RSVP extension fast-reroute” definována RFC 4090. Směrovač provádí každých 3600 vteřin optimalizaci LSP, v případě nalezení lepší cesty provede automaticky přepnutí LSP. Sestavení RSVP je zabezpečeno heslem šifrovaným algoritmem MD5 a počet směrovačů, přes který může LSP procházet je nastaven na 20.

Tab. 6 Konfigurace _RSVP a RSVP-TE.

```
//spuštění RSVP na portech
set protocols rsvp interface xe-0/0/0.0 authentication-key <_>
set protocols rsvp interface xe-0/0/1.0 authentication-key <_>
set protocols rsvp interface xe-0/0/2.0 authentication-key <_>
set protocols rsvp interface xe-0/0/3.0 authentication-key <_>
set protocols rsvp interface xe-1/2/0.0 authentication-key <_>
//konfigurace template
set protocols mpls label-switched-path P2P-RSVP template
set protocols mpls label-switched-path P2P-RSVP optimize-timer 3600
set protocols mpls label-switched-path P2P-RSVP adaptive
set protocols mpls label-switched-path P2P-RSVP fast-reroute
set protocols mpls label-switched-path P2P-RSVP hop-limit 20
//konfigurace RSVP-TE
set routing-options dynamic-tunnels DYNTUN rsvp-te RSVP-TE1 label-switched-path-template
P2P-RSVP
set routing-options dynamic-tunnels DYNTUN rsvp-te RSVP-TE1 destination-networks
10.100.1.0/24
set routing-options dynamic-tunnels DYNTUN rsvp-te RSVP-TE1 destination-networks
10.100.2.0/24
```

Destination-networks představuje seznam IP adres, se kterými bude směrovač navazovat LSP tunely. Jedná se o segment IP adres loopbacků ostatních směrovačů.

- Konfigurace BGP

Směrování IP rozsahů v MPLS VPN je prováděno protokolem MP-BGP. Pro výměnu směrovacích informací je použit autonomní systém 65000, který je využíván v původní nemodernizované síti.

V modernizované síti je v krajském technologickém centru nakonfigurován BGP RR cluster, kterého jsou součástí směrovače RPLZ1 a RPLZ2 a se kterými navazují iBGP spojení všechny směrovače v okresních centrech (tab. 7). Navazování iBGP spojení je zabezpečeno jedinečným heslem šifrovaným algoritmem MD5. V konfiguraci BGP nechybí i konfigurace BFD a datový provoz v L3VPN je možný pouze pro unicast.

Tab. 7 Ukázka konfigurace iBGP clusteru a iBGP klientů.

```
set routing-options autonomous-system 65000
set protocols bgp group BGP-RR type internal
set protocols bgp group BGP-RR local-address 10.100.1.63
set protocols bgp group BGP-RR family inet-vpn unicast
set protocols bgp group BGP-RR cluster 10.100.1.63
set protocols bgp group BGP-RR bfd-liveness-detection minimum-interval 1000
//router RPLZ2
set protocols bgp group BGP-RR neighbor 10.100.2.63 authentication-key <_>

//Routery Domažlice
set protocols bgp group BGP-RR neighbor 10.100.1.64 authentication-key <_>
set protocols bgp group BGP-RR neighbor 10.100.2.64 authentication-key <_>

//Routery Klatovy
set protocols bgp group BGP-RR neighbor 10.100.1.65 authentication-key <_>
set protocols bgp group BGP-RR neighbor 10.100.2.65 authentication-key <_>

//Routery Rokycany
set protocols bgp group BGP-RR neighbor 10.100.1.66 authentication-key <_>
set protocols bgp group BGP-RR neighbor 10.100.2.66 authentication-key <_>

//Routery Tachov
set protocols bgp group BGP-RR neighbor 10.100.1.67 authentication-key <_>
set protocols bgp group BGP-RR neighbor 10.100.2.67 authentication-key <_>
```

- Konfigurace MPLS QoS

V MPLS QoS bylo nutné z 12 tříd provozu vytvořit 8 tříd. Došlo k tomu díky sloučení podobného provozu. V této části si ukážeme jen prioritizaci hlasového provozu s DSCP EF, v celku se jedná o poměrně rozsáhlou konfiguraci. V prvním kroku je na směrovači vytvořena třída (CLASS) „FC-VOICE“, do které bude přiřazen provoz se značkou EF. V druhém kroku dochází, na základě identifikace

třídy v předchozím kroku, k doplnění tří bitů do EXP v MPLS, v tomto případě „111“. Ve třetím kroku dochází k přiřazení sedmé fronty s vysokou prioritou ke třídě „FC-VOICE“. Ve čtvrtém kroku se vytváří tzv. „Schedulers“ (plánovač), který již třídám určuje maximální možné využití datové linky (tab. 8).

V případě plánovače SC-VOICE je přiřazeno na odesílání 5 % z celkové přenosové rychlosti linky (na to navazuje i velikost vnitřního bufferu routeru) a vysoká priorita. V pátém kroku je vytvořen „scheduler-maps“ (soupis plánovačů), který má v sobě nakonfigurovaný pouze jeden soupis „QUEUEING-WAN-OUT“. Tento soupis dává dohromady všechny výše definovaná pravidla a rozdělení – do QUEUEING-WAN-OUT je přiřazena třída FC-VOICE s plánovačem SC-VOICE, zjednodušeně řečeno – na výstupním portu routeru je připravena fronta (queue) pro datový provoz s EXP 111 pro který je rezervováno 5 % z rychlosti datové linky. V šestém kroku již dochází k mapování „Scheduler-maps“ na konkrétní porty routeru.

Tab. 8 Prioritizace provozu EF.

set class-of-service classifiers dscp CLASS forwarding-class FC-VOICE loss-priority low code-points ef
set class-of-service classifiers exp MPLS-EXP-CLASSIFIER forwarding-class FC-VOICE loss-priority low code-points 111
set class-of-service forwarding-classes class FC-VOICE queue-num 7
set class-of-service forwarding-classes class FC-VOICE priority high
set class-of-service schedulers SC-VOICE transmit-rate percent 5
set class-of-service schedulers SC-VOICE buffer-size percent 5
set class-of-service schedulers SC-VOICE priority high
set class-of-service scheduler-maps QUEUEING-WAN-OUT forwarding-class FC-VOICE scheduler SC-VOICE
set class-of-service interfaces xe-0/0/0 scheduler-map QUEUEING-WAN-OUT
set class-of-service interfaces xe-0/0/0 unit 0 rewrite-rules exp MPLS-EXP-REWRITE
set class-of-service interfaces xe-0/0/1 scheduler-map QUEUEING-WAN-OUT
set class-of-service interfaces xe-0/0/1 unit 0 rewrite-rules exp MPLS-EXP-REWRITE
set class-of-service interfaces xe-0/0/2 scheduler-map QUEUEING-WAN-OUT
set class-of-service interfaces xe-0/0/2 unit 0 rewrite-rules exp MPLS-EXP-REWRITE
set class-of-service interfaces xe-0/0/3 scheduler-map QUEUEING-WAN-OUT
set class-of-service interfaces xe-0/0/3 unit 0 rewrite-rules exp MPLS-EXP-REWRITE
set class-of-service interfaces xe-1/2/0 scheduler-map QUEUEING-WAN-OUT
set class-of-service interfaces xe-1/2/0 unit 0 rewrite-rules exp MPLS-EXP-REWRITE
set class-of-service routing-instances all classifiers exp MPLS-EXP-CLASSIFIER
set class-of-service rewrite-rules exp MPLS-EXP-REWRITE forwarding-class FC-VOICE loss-priority low code-point 111

- Konfigurace vzdáleného připojení

Vzdálený přístup pro administraci je prováděn pomocí protokolu SSHv2 (tab. 9). Root login je pro SSH vypnutý. Pro přístup se využívá inband rozhraní. Počet paralelních připojení přes SSH protocol je omezen na 10. Počet pokusů pro připojení je nastaven na 4 pokusy/min.

Tab. 9 Konfigurace SSH.

```
set system services ssh root-login deny
set system services ssh protocol-version v2
set system services ssh max-sessions-per-connection 2
set system services ssh connection-limit 10
set system services ssh rate-limit 4
```

4 VÝSLEDKY

4.1 NÁVRH NOVÉ TOPOLOGIE

V návrhu topologie musely být zohledněny specifické požadavky i výstupy z analýzy původní datové sítě. Důraz byl kladen na redundanci datového spojení, velmi rychlou detekci výpadku datové linky a následný výpočet nové datové cesty. Nová datová síť bude propojovat celkem 5 lokalit, jedna lokalita je centrální technologické centrum a zbylé čtyři jsou okresní technologická centra, typem zapojení „do hvězdy“ (v drtivé většině dochází ke komunikaci pouze mezi okresním a krajským centrem). V každém technologickém centru se bude nacházet jedno DWDM zařízení Cisco a dvojice „PE routerů“ Juniper. V prvním kroku došlo k adresaci směrovačů, v druhém kroku jejich pojmenování a v posledním kroku byla navržena topologie.

Adresace je řešena z rozsahu IPv4 adres, konkrétně ze segmentu 10.100.0.0/16. Bylo nutné zvolit část pro adresaci loopbacků (maska /32) a poté dvoubodových sítí (maska /30) pro jednotlivé propojení směrovačů v rámci každého technologického centra a pro spojení mezi krajským a okresním centrem. IP adresy konkrétních technologických center byly odvozeny od jejich identifikačních čísel (tab. 10).

Tab. 10 Identifikační čísla okresů a přidělené IP rozsahy

Technologická místnost	Identifikační číslo	IP rozsah
Plzeň	63	10.100.63.0/24
Domažlice	64	10.100.64.0/24
Klatovy	65	10.100.65.0/24
Rokycany	66	10.100.66.0/24
Tachov	67	10.100.67.0/24

Rozsah adres 10.100.1.xx/24 je určen pro adresaci loopbacku routerů RXXX1. Rozsah adres 10.100.2.xx/24 je určen pro adresaci loopbacku routerů RXXX2. Následující rozsah 10.100.xx.0 až 10.100.xx.124 je určen pro adresaci dvoubodových spojů v rámci technologického centra. Adresace 10.100.60.0/24 je určena pro adresaci dvoubodových spojů mezi technologickými centry.

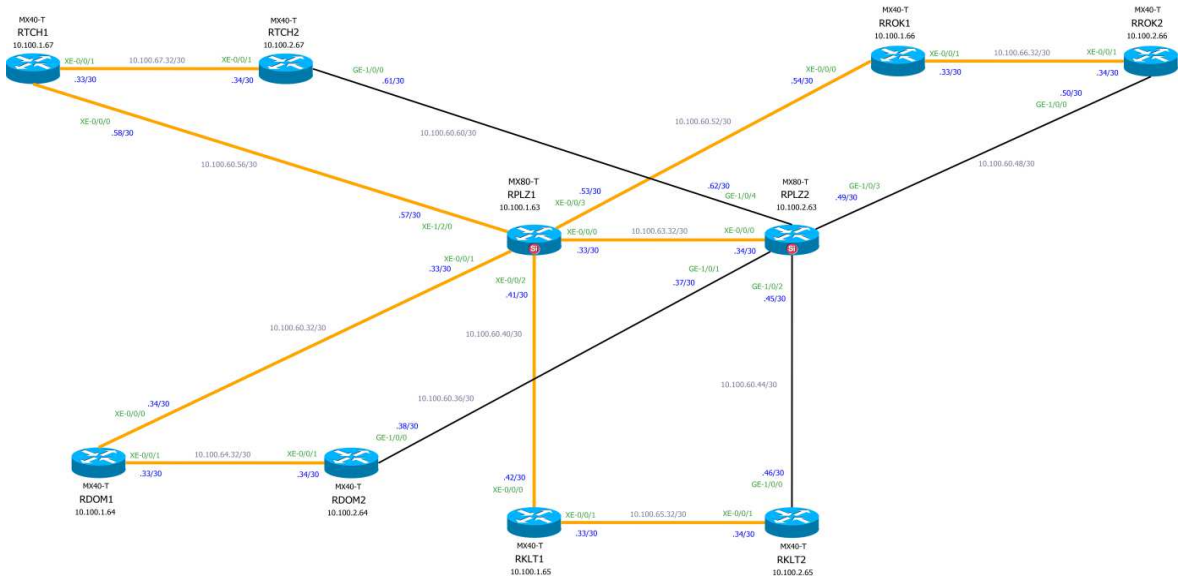
Zároveň s novou adresací byla zavedena i nová koncepce tvoření „hostname“ směrovačů. Jméno se skládá z RXXXY kde:

- R je označení zařízení, R – směrovač (router)
- XXX zkratka města, kde se směrovač nachází
- Y je pořadové číslo směrovače v lokalitě

Tab. 11 Přehled hostname směrovačů

Technologická místnost	Hostname routeru
Plzeň	RPLZ1
	RPLZ2
Domažlice	RDOM1
	RDOM2
Klatovy	RKLT1
	RKLT2
Rokycany	RROK1
	RROK2
Tachov	RTCH1
	RTCH2

Topologie je řešena formou zapojení „do hvězdy“, v tomto případě se bude jednat o dvojitou hvězdu (obr. 23) – první je tvořena soustavou optického zapojení a přenosu datového provozu přes DWDM a druhá hvězda je tvořena záložními linkami, které fungují na jiné technologii než první hvězda, konkrétně jsou záložní linky realizovány bezdrátovými pojítky.



Obr. 23 Nákres topologie nové datové sítě.

Zdroj: Vlastní

4.2 TESTOVÁNÍ

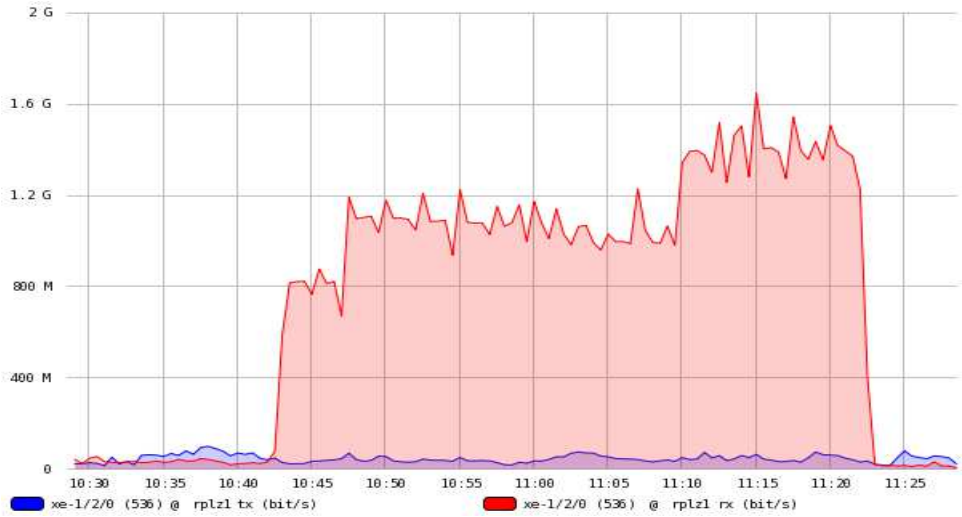
Pro ověření správné konfigurace a zapojení datových prvků je nutné na nové datové síti provést testy. Testy jsou rozděleny na testování propustnosti datové linky mezi krajským a okresním centrem, testování funkčnosti QoS, testování redundantního datového zapojení a následné konvergence. V posledním testu budou vypsány hodnoty vytížení procesoru směrovače během předešlých testů.

Byly provedeny celkem 4 stěžejní testy s cílem zjistit funkčnost a chování nové datové sítě. Tři testy se zaměřili přímo na vytížení a chování datové sítě, čtvrtý test sledoval zatížení samotného směrovače.

4.2.1 MĚŘENÍ PROPUSTNOSTI DATOVÝCH LINEK

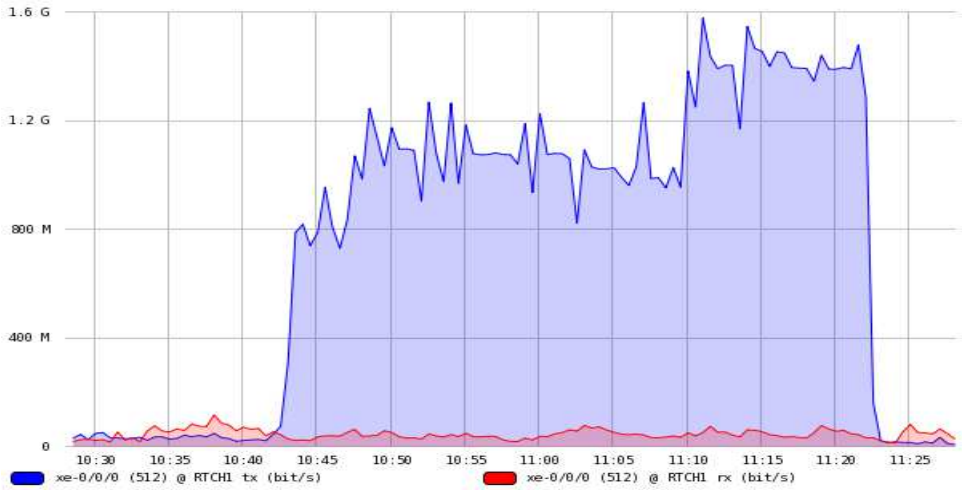
V tomto testu bylo nutné improvizovat. Nebylo dostupné zařízení, které bylo schopné vytížit linku o rychlosti 10 Gb/s. Bylo zvoleno řešení v podobě dvou měřících zařízení JDSU MTS-5800 a JDUS SC. Měření bylo prováděno z měřících zařízení (celková rychlosti 1,5 Gb/s) v krajském centru na IP adresu lokální stanice v okresním centru.

Cílem je zjistit, zda je možné skrze datovou linku posílat více než 1 Gb/s. Graf zatížení datové linky byl zaznamenán programem „The Dude“ vyčítáním hodnot přijatých/odeslaných dat portů na obou směrovačích přes protokol SNMP. Zatížení datové linky mezi směrovači RPLZ1 a RTCH1 je zřejmé (obr. 24 a obr. 25).



Obr. 24 RPLZ1-prijato

Zdroj: Vlastní



Obr. 25 RTCH1-odeslano
Zdroj: Vlastní

V prvním testu propustnosti datové sítě došlo k improvizaci z důvodu nedostupného zařízení, které by dokázalo generovat tak vysoký datový tok. Cílem testu bylo zjistit, zda je možné skrze datovou linku mezi okresním a krajským centrem dosahovat vyšší přenosové rychlosti než 1Gb/s. Během testování nedošlo k výpadkům nebo nedostupnosti směrovačů z důvodu zahlcení linky. Rychlost byla na portech směrovačů detekována a realizována bez problémů. Test prokázal možnost v datové síti dosahovat vyšší přenosové rychlosti než 1Gb/s.

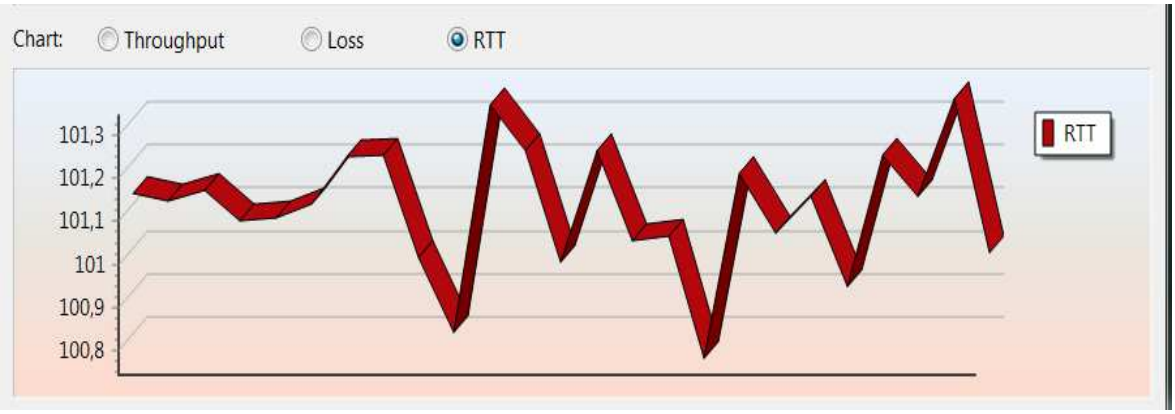
4.2.2 TESTOVÁNÍ FUNKČNOSTI QOS

Cílem měření bylo zjištění, zda směrovač detekuje prioritizovaný provoz, řadí jej do správné třídy a prioritně jej odesílá. Pro toto testování byla upravena rychlost datové linky z 10 Gb/s na 1 Gb/s. Měřicí přístroj JDSU MTS-5800 bude generovat EF provoz rychlostí 7 Mb/s a druhý měřicí přístroj JDSU-SC bude záměrně hltit datovou linku, provoz bude součástí vlastní VRF. Výsledkem budou dva grafy zachycující RTT (obr. 26 a obr. 27).

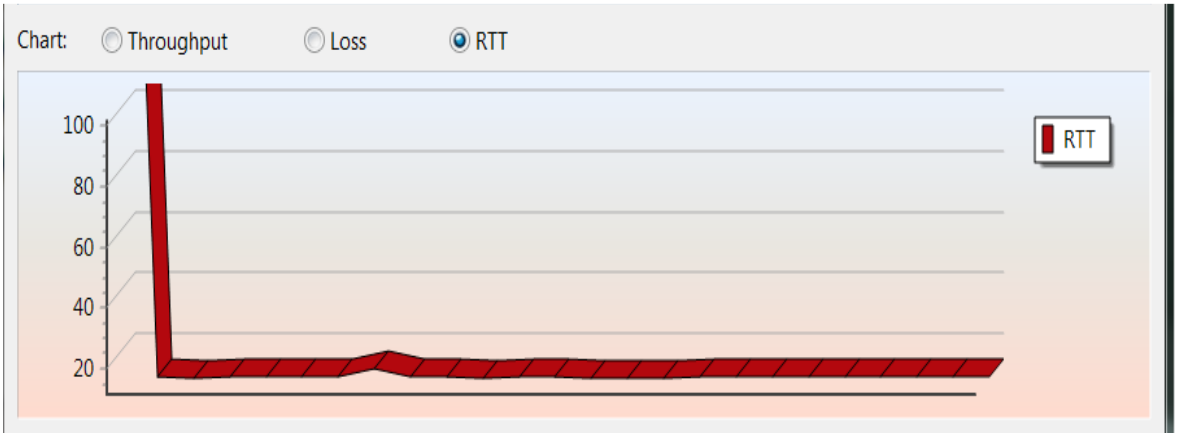
V prvním grafu je jasně patrný nárůst odezvy až k hranici 102ms a vysoká ztrátovost (rychlost přenosu se pohybuje kolem 1 Mb/s). V druhém grafu, po zapnutí funkce QoS, směrovač okamžitě reaguje na prioritizovaný datový provoz, rychlost se ustálila na 6,9 Mb/s a odezva na 12ms. V záznam „pingu“, který byl prováděn na IP adresu loopbacku okresního směrovače v síti OSPF, bylo jasné patrné vypnutí a následné zapnutí funkce QoS (obr. 28).

V druhém testu, který ověřoval funkčnost QoS v MPLS, bylo využito dvou měřicích přístrojů firmy JDSU, které generovaly datový prioritizovaný

a neprioritizovaný provoz. V první části testu byla funkce QoS vypnuta a datová linka zahlcena vygenerovanými daty. Druhá část testu spočívala v aktivaci QoS během zahlcení datové linky a následném sledování chování směrovačů. Zapnutí QoS bylo během testování jasně detekovatelné a mělo zásadní, pozitivní vliv na funkčnost sítě během zahlcení.



Obr. 26 Zpoždění RTT při vypnutém QoSu.
Zdroj: Vlastní



Obr. 27 Zpoždění RTT při zapnutém QoS.
Zdroj: Vlastní

Ping 10.100.67.1

Z adresy: server | Počet paketů: | Spustit
Komu: 10.100.67.1 | Velikost paketu: 32 | Zastavit
Interval: 1000 ms | TTL: 64 | Zavřít

#	Hostitel	Název	Čas	Velikost odpovědi	TTL	Stav
1	10.100.67.1	RTCH1	<1 ms	32	254	
2	10.100.67.1	RTCH1	16 ms	32	254	
3	10.100.67.1	RTCH1	<1 ms	32	254	
4	10.100.67.1	RTCH1	<1 ms	32	254	
5	10.100.67.1	RTCH1	<1 ms	32	254	
6	10.100.67.1	RTCH1	<1 ms	32	254	
7	10.100.67.1	RTCH1	<1 ms	32	254	
8	10.100.67.1	RTCH1	<1 ms	32	254	
9	10.100.67.1	RTCH1	<1 ms	32	254	
10	10.100.67.1	RTCH1	<1 ms	32	254	
11	10.100.67.1	RTCH1	78 ms	32	254	
12	10.100.67.1	RTCH1	484 ms	32	254	
13	10.100.67.1	RTCH1	359 ms	32	254	
14						vypršel časový limit
15						vypršel časový limit
16	10.100.67.1	RTCH1	312 ms	32	254	
17	10.100.67.1	RTCH1	156 ms	32	254	
18	10.100.67.1	RTCH1	250 ms	32	254	
19	10.100.67.1	RTCH1	281 ms	32	254	
20	10.100.67.1	RTCH1	281 ms	32	254	
21	10.100.67.1	RTCH1	375 ms	32	254	
22	10.100.67.1	RTCH1	328 ms	32	254	
23	10.100.67.1	RTCH1	218 ms	32	254	
24	10.100.67.1	RTCH1	500 ms	32	254	
25	10.100.67.1	RTCH1	375 ms	32	254	
26	10.100.67.1	RTCH1	328 ms	32	254	
27	10.100.67.1	RTCH1	250 ms	32	254	
28	10.100.67.1	RTCH1	390 ms	32	254	
29	10.100.67.1	RTCH1	453 ms	32	254	
30	10.100.67.1	RTCH1	<1 ms	32	254	
31	10.100.67.1	RTCH1	<1 ms	32	254	
32	10.100.67.1	RTCH1	<1 ms	32	254	

Obr. 28 Záznam hodnot zpoždění.

Zdroj: Vlastní

4.2.3 TESTOVÁNÍ REDUNDANTNÍHO ZAPOJENÍ

Třetí test spočíval ve zjištění času konvergence datové sítě při výpadku datové linky, nebo směrovače. Test byl proveden fyzickým odpojením hlavní datové linky ze směrovače v okresním centru a sledování doby výpadku komunikace mezi dvěma koncovými stanicemi ve vlastní VRF.

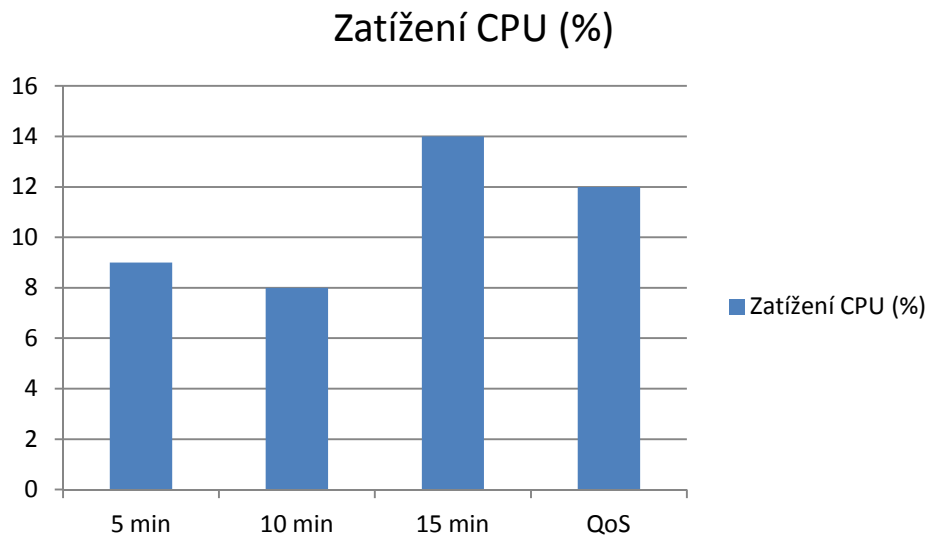
V případě výpadku byl výslední čas maximálně 2 sekundy, v případě obnovení datového spojení přes hlavní linku byly potřeba maximálně 4 vteřiny. Síť se v případě výpadku zachovala předvídatelně. Test byl proveden fyzickým odpojením hlavní datové linky v okresním centru. K testování byla zvolena funkce ping z testovací stanice v krajském centru na IP adresu testovací stanice v okresním centru. Obě stanice jsou adresovány ve stejné VRF. Výpadkem se nesleduje konvergence jednotlivých protokolů, ale sleduje se konvergence sítě jako celku. Proto testování probíhá v rámci VRF, které simuluje datový provoz konkrétního oddělení. Velikost ICMP paketu byla nastavena na 500 bajtů, timeout 1 sekunda.

- První část testu – vypojení optického kabelu z routeru RDOM1 mělo za následek výpadek datového provozu do cíle na maximálně 2 sekundy. Za tuto dobu dokázal OSPF díky BFD protokolu detekovat výpadek, spustit přepočet cesty algoritmem SPF a zjistit náhradní nejvýhodnější datovou cestu. Na základě výpočtu OSPF byl vytvořen v MPLS nový LSP.
- Druhá část testu – znovu zprovoznění hlavní datové linky připojením optického kabelu do směrovače RDOM1. Pingem byla zjištěna delší konvergence a to maximálně 4 vteřiny. Test byl několikrát opakován se stejným výsledkem. Delší čas přisuzuji nutnosti doplnit OSPF link-state databázi a na to navazující přepočty SPF a následně vytvoření nové LSP.

4.2.4 ANALÝZA VYTÍŽENÍ NOVÝCH ROUTERŮ

Vytížení směrovačů probíhalo průběžně při plnění předchozích testů. Hlavním sledovaným parametrem bylo vytížení procesoru při měření rychlosti datové linky a poslední sloupec grafu ukazuje zatížení procesoru při zahlcení datové linky a spuštěnou funkcí QoS (obr. 29).

Sledování bylo prováděno na směrovači RPLZ1. Čtvrtý test probíhal zároveň s předešlými testy. Průběžně byly zaznamenávány hodnoty vytížení procesoru směrovače během testování. Dle předpokladu, testování zatížilo CPU směrovače jen minimálně, směrovač je schopný většinu standardního datového provozu řešit v logice jednotlivých karet.



Obr. 29 Graf zatížení CPU (v procentech)

Zdroj: Vlastní

Podle předpokladu byl sledovaný vliv testování na vytížení procesoru minimální. Směrovač většinu operací zvládá „v hardwaru“ – na kartách a portech. Do procesoru už jdou jen některé atypické požadavky, např. přepočet SPF při výpadcích linek v rámci OSPF oblasti.

5 ZÁVĚR

V této práci je podrobně popsán průběh návrhu a realizace modernizace datové sítě. Exaktně vymezené činnosti jsou totožné s postupem v reálné situaci. Vývoj datových sítí nemá dlouhou historii, přesto nelze mezi prvopočátky a dnešní dobou hledat jakoukoli podobnost. Změnilo se všechno. Tento prudký vývoj urychluje stárnutí současných zařízení, která postupně ztrácí schopnost odolávat datovému toku. Je důležité vědět, k čemu bude primárně datová infrastruktura určena, protože je realizována o jistých parametrech, čemuž odpovídá specifická konfigurace a vybavení síťových zařízení.

V první části byla představena původní datová síť a její specifické problémy, které se staly jedním z podkladů pro návrh nové topologie, druhým podkladem byly konkrétní požadavky na novou datovou síť.

Ve druhé části práce již probíhá návrh nové topologie, specifikace nových směrovačů, dochází k výběru a konfiguraci protokolů. Součástí této části je i ukázka konfigurace jednoho z hlavních směrovačů.

Třetí část byla věnována testování, které zodpověděli na hlavní otázky práce. Cílem práce bylo vyhodnocení úspěšnosti modernizace datové podnikové sítě na základě definovaných dílčích cílů, které spočívají v navýšení přenosové rychlosti mezi technologickými centry, prioritizaci datového provozu a rychlé konvergenci. Výsledky testů dokazují splnění cílů na akceptovatelné úrovni, určité rezervy spatřuji v rychlosti konvergence sítě.

Velký potenciál takto projektovaných sítí vidím ve školství. Díky vysokým přenosovým rychlostem by bylo možné centralizovat aplikace, využít sdílení síťových prostředků i kapacity. Ze dne na den je možné udělat z počítačové sítě službu, kterou je možné nabídnout i dalším, nejen vysokým, školám. Otevírá možnosti výzkumu a testování nových protokolů nebo technologií. Sítě tady jsou a budou, současnou pedagogickou činnost si bez sítí možná lze představit, ale nelze ji realizovat. Studijní materiály, e-kurzy i školení a přednášky, vše je dnes realizováno „na dálku“, tím je uspořen čas studentů, ale i učitelů. Sice je to vše o aplikacích, ale na pozadí bude stále ta datová síť, která bude tyto informace přenášet a bohužel v dnešní době není počítačovým sítím jak v praxi, tak i v pedagogice věnována dostatečná pozornost.

Bakalářská práce mi umožnila detailněji nahlédnout do problematiky rozlehlých počítačových sítí, použitých protokolů i načerpání zkušeností s návrhem topologie a konfigurace. Díky práci jsem podrobně prostudoval jednotlivé protokoly a získával přehled o jejich funkčnosti, vazbách na datový provoz a obtížnosti konfigurace.

RESUMÉ

V této práci jsem se věnoval popisu protokolů a aktivních datových prvků v původní síti, analýzou původní datové sítě, jejíž výstup byl jeden z podkladů pro specifikaci návrhu modernizace. V práci jsou dále definovány uživatelské požadavky na modernizaci, které byly zahrnuty společně s výstupem analýzy původní sítě do celkového návrhu topologie. Na základě návrhu nové topologie jsem provedl specifikaci nových směrovačů a následně jejich konfiguraci. Závěrem jsem provedl sadu testů ověřující splnění dílčích cílů. Tím se otevírají další možnosti zkoumání, přímo se nabízí oblast zabezpečení směrovačů a MPLS sítě proti útokům – v případě směrovačů případ neautorizovaného přístupu, v případě MPLS a datových linek DDoS útoky.

In this work, I described protocols, active data elements and analysis of the current network, which was the basis for specifying the design of the modernization. There are defined user requirements for modernization, which were used together with the analysis of the current network to design the final topology. Based on the new topology design, I specified new routers and then their configuration. Finally, I ran a set of tests which verify meeting the partial goals. This opens new reseach possibilities, starting from securing routers and MPLS from attacks - in the case of routers unauthorized access, in the case of MPLS and data lines DDoS attacks.

Klíčová slova:

směrovač, počítačová síť, cisco, juniper, qos

Keywords:

router, computer network, cisco, juniper, qos

SEZNAM LITERATURY

Anuta, Networks. 2013. mpls-backbone. *Anutanetworks.* [Online] 2013. [Citace: 8. 2 2017.] http://www.anutanetworks.com/mpls-backbone/.

Cisco. 2017. Spanning Tree Protocol - Cisco. *Cisco.* [Online] 2017. [Citace: 4. 12 2016.] http://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html.

Hanks, Douglas, Reynolds, Harry a Roy, David. 2012. *Juniper MX Series.* Sebastopol : O´Reilly Media, 2012. 978-1-449-31971-7.

Juniper. 2015. Juniper Networks. *MX5, MX10, MX40, and MX80 Router Overview.* [Online] 2015. [Citace: 19. 11 2016.] http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/concept/mx5-mx10-mx40-mx80-description.html.

Marlib. 2017. Historie počítačů. *Marlib.* [Online] 2017. [Citace: 15. 3 2017.] http://marlib.cmsps.cz/historie/historie.htm.

NATO, Rewiev. 2015. Byla První světová válka užitečná pro lékařství? *NATO Rewiev.* [Online] 2015. [Citace: 12. 1 2017.] http://www.nato.int/docu/review/2014/war-medicine/WWI-WW1-Health-care-medicine/CS/index.htm.

Odom, Wendell, Healy, Rus a Mehta, Naren. 2009. *Směrování a přepínání sítí.* Brno : Computer Press, 2009. 9788025125205.

Peterka, Jiří. 2015. Na počátku byl ARPANET. *eArchiv.* [Online] 2015. [Citace: 14. 3 2017.] http://www.earchiv.cz/a95/a504c502.php3.

SystemOnLine. 2017. Kam kráčí softwarově definované sítě? [Online] 2017. [Citace: 16. 3 2017.] https://www.systemonline.cz/clanky/kam-kraci-softwarove-definovane-site.htm.

Technet. 2013. Kontroverzní otec raketové techniky von Braun se narodil před 100 lety. *TechNet.* [Online] 2013. [Citace: 11. 1 2017.] http://technet.idnes.cz/pred-sto-lety-se-narodil-.

VTM. 2017. Souboj s nacistickou Enigmou nastartoval éru počítačů. *VTM.* [Online] 2017. [Citace: 20. 2 2017.] http://vtm.e15.cz/souboj-s-nacistickou-enigmou-nastartoval-eru-pocitacu.

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ

PŘÍLOHY

Příloha A

Ukázka konfigurace okresního směrovače RDOM1

Příloha B

Obsah CD:

- složka Konfigurace
- složka Software
- VladislavMerhout2017.docx
- VladislavMerhout2017.pdf

```
version 13.3R6.5;
system {
    host-name RDOM1;

    }

    services {
        ssh {
            root-login deny;
            protocol-version v2;
            max-sessions-per-connection 2;
            connection-limit 10;
            rate-limit 4;
             }
            }

}
chassis {
    network-services all-ethernet;
}

interfaces {
    xe-0/0/0 {
        description "RPLZ1 XE-0/0/1";
        mtu 9192;
        unit 0 {
            family inet {
                address 10.100.60.34/30;
            }
            family mpls;
```

```
        }
    }
    xe-0/0/1 {
        description "RDOM2 XE-0/0/1";
        mtu 9192;
        unit 0 {
            family inet {
                address 10.100.64.33/30;
            }
            family mpls;
        }
    }
    lo0 {
        description "Loopback0";
        unit 0 {
            family inet {
                address 10.100.1.64/32;
            }
        }
    }
}
routing-options {
    router-id 10.100.1.64;
    autonomous-system 65000;
    dynamic-tunnels {
        DYNTUN {
            rsvp-te RSVP-TE1 {
                label-switched-path-template {
                    P2P-RSVP;
                }
                destination-networks {
                    10.100.1.0/24;
                    10.100.2.0/24;

                }
            }
        }
    }
}
protocols {
    rsvp {
     interface xe-0/0/0.0 {
            authentication-key //heslo//;
        }
     interface xe-0/0/1.0 {
            authentication-key //heslo//;
        }
    }
    mpls {
      label-switched-path P2P-RSVP {
            template;
            optimize-timer 3600;
            adaptive;
            fast-reroute {
                hop-limit 20;
            }
```

```
        }
           interface xe-0/0/0.0;
           interface xe-0/0/1.0;
    }
    bgp {
        group BGP-RR {
            type internal;
            local-address 10.100.1.64;
            family inet-vpn {
                unicast;
            }

            bfd-liveness-detection {
                minimum-interval 1000;
            }
            neighbor 10.100.1.63 {
                authentication-key //heslo//;
            }
            neighbor 10.100.2.63 {
                authentication-key //heslo//;
            }
    }
    ospf {
        traffic-engineering {
            shortcuts;
        }
        reference-bandwidth 10g;
        area 0.0.0.0 {
            interface xe-0/0/0.0 {
                interface-type p2p;
                authentication {
                    md5 0 key //heslo//;
                }
                bfd-liveness-detection {
                    minimum-interval 2000;
                    multiplier 2;
                    full-neighbors-only;
                }
            }
            interface xe-0/0/1.0 {
                interface-type p2p;
                authentication {
                    md5 0 key //heslo//;
                }
                bfd-liveness-detection {
                    minimum-interval 2000;
                    multiplier 2;
                    full-neighbors-only;
            }
            interface lo0.0 {
                passive;
            }
            interface all {
                ldp-synchronization;
            }
    }
```

```
    ldp {
        interface xe-0/0/0.0;
        interface xe-0/0/1.0;
    }
    lldp {
        management-address 10.100.1.64;
        port-id-subtype interface-name;
        interface xe-0/0/0;
        interface xe-0/0/1;
        }
}
class-of-service {
    classifiers {
        dscp CLASS {
            forwarding-class FC-VOICE {
                loss-priority low code-points ef;
            }
            forwarding-class FC-VIDEO {
                loss-priority low code-points [ cs4 cs5 ];
            }
            forwarding-class FC-NETWORK {
                loss-priority low code-points [ cs6 cs7 ];
            }
            forwarding-class FC-MULTIMEDIA {
                loss-priority low code-points [ af31 af32 af33
           af42 af43 af41 ];
            }
            forwarding-class FC-SIGNALING {
                loss-priority low code-points [ cs2 cs3 ];
            }
            forwarding-class FC-PRIORITY {
                loss-priority medium-low code-points af21;
                loss-priority medium-high code-points af22;
                loss-priority high code-points af23;
            }
            forwarding-class FC-BULK {
                loss-priority low code-points cs1;
                loss-priority medium-low code-points af11;
                loss-priority medium-high code-points af12;
                loss-priority high code-points af13;
            }
            forwarding-class FC-BESTEFFORT {
                loss-priority high code-points be;
            }
        }
        exp MPLS-EXP-CLASSIFIER {
            forwarding-class FC-VOICE {
                loss-priority low code-points 111;
            }
            forwarding-class FC-VIDEO {
                loss-priority low code-points 110;
            }
            forwarding-class FC-NETWORK {
                loss-priority low code-points 101;
            }
            forwarding-class FC-MULTIMEDIA {
```

```
                loss-priority low code-points 100;
            }
            forwarding-class FC-SIGNALING {
                loss-priority low code-points 011;
            }
            forwarding-class FC-PRIORITY {
                loss-priority low code-points 010;
            }
            forwarding-class FC-BULK {
                loss-priority high code-points 001;
            }
            forwarding-class FC-BESTEFFORT {
                loss-priority high code-points 000;
            }
        }
    }
    drop-profiles {
        DP-BULK-CS1 {
            fill-level 40 drop-probability 80;
        }
        DP-BULK-AF11 {
            fill-level 80 drop-probability 100;
        }
        DP-BULK-AF12 {
            fill-level 70 drop-probability 100;
        }
        DP-BULK-AF13 {
            fill-level 60 drop-probability 100;
        }
        DP-PRIORITY-AF21 {
            fill-level 80 drop-probability 100;
        }
        DP-PRIORITY-AF22 {
            fill-level 70 drop-probability 100;
        }
        DP-PRIORITY-AF23 {
            fill-level 60 drop-probability 100;
        }
    }
    forwarding-classes {
        class FC-VOICE queue-num 7 priority high;
        class FC-VIDEO queue-num 6 priority high;
        class FC-NETWORK queue-num 3 priority high;
        class FC-MULTIMEDIA queue-num 4 priority high;
        class FC-SIGNALING queue-num 5 priority low;
        class FC-PRIORITY queue-num 2 priority low;
        class FC-BULK queue-num 1 priority low;
        class FC-BESTEFFORT queue-num 0 priority low;
    }
    interfaces {
      xe-0/0/0 {
            scheduler-map QUEUEING-WAN-OUT;
            unit 0 {
                rewrite-rules {
                    exp MPLS-EXP-REWRITE;
                }
```

```
            }
        }
        xe-0/0/1 {
            scheduler-map QUEUEING-WAN-OUT;
            unit 0 {
                rewrite-rules {
                    exp MPLS-EXP-REWRITE;
                }
            }
        }

    }
    routing-instances {
        all {
            classifiers {
                exp MPLS-EXP-CLASSIFIER;
            }
        }
    }
    rewrite-rules {
        exp MPLS-EXP-REWRITE {
            forwarding-class FC-VOICE {
                loss-priority low code-point 111;
            }
            forwarding-class FC-VIDEO {
                loss-priority low code-point 110;
            }
            forwarding-class FC-NETWORK {
                loss-priority low code-point 101;
            }
            forwarding-class FC-MULTIMEDIA {
                loss-priority low code-point 100;
            }
            forwarding-class FC-SIGNALING {
                loss-priority low code-point 011;
            }
            forwarding-class FC-PRIORITY {
                loss-priority low code-point 010;
                loss-priority medium-low code-point 010;
                loss-priority medium-high code-point 010;
            }
            forwarding-class FC-BULK {
                loss-priority high code-point 001;
                loss-priority low code-point 001;
                loss-priority medium-low code-point 001;
                loss-priority medium-high code-point 001;
            }
            forwarding-class FC-BESTEFFORT {
                loss-priority high code-point 000;
            }
        }
    }
    scheduler-maps {
        QUEUEING-WAN-OUT {
            forwarding-class FC-BESTEFFORT scheduler SC-
           BESTEFFORT;
```

```
            forwarding-class FC-BULK scheduler SC-BULK;
            forwarding-class FC-PRIORITY scheduler SC-
                PRIORITY;
            forwarding-class FC-SIGNALING scheduler SC-
           SIGNALING;
            forwarding-class FC-MULTIMEDIA scheduler SC-
           MULTIMEDIA;
            forwarding-class FC-NETWORK scheduler SC-NETWORK;
            forwarding-class FC-VIDEO scheduler SC-VIDEO;
            forwarding-class FC-VOICE scheduler SC-VOICE;
        }
    }
    schedulers {
        SC-BULK {
            transmit-rate percent 3;
            priority medium-low;
            drop-profile-map loss-priority low protocol any
           drop-profile DP-BULK-CS1;
            drop-profile-map loss-priority medium-low protocol
           any drop-profile DP-BULK-AF11;
            drop-profile-map loss-priority medium-high
           protocol any drop-profile DP-BULK-AF12;
            drop-profile-map loss-priority high protocol any
           drop-profile DP-BULK-AF13;
        }
        SC-PRIORITY {
            transmit-rate percent 15;
            priority medium-high;
            drop-profile-map loss-priority medium-low protocol
           any drop-profile DP-PRIORITY-AF21;
            drop-profile-map loss-priority medium-high
           protocol any drop-profile DP-PRIORITY-AF22;
            drop-profile-map loss-priority high protocol any
           drop-profile DP-PRIORITY-AF23;
        }
        SC-SIGNALING {
            transmit-rate percent 1;
            priority medium-high;
        }
        SC-BESTEFFORT {
            transmit-rate {
                remainder;
            }
            priority low;
        }
        SC-VOICE {
            transmit-rate percent 5;
            buffer-size percent 5;
            priority high;
        }
        SC-VIDEO {
            transmit-rate percent 30;
            buffer-size percent 30;
            priority high;
        }
        SC-NETWORK {
```

```
            transmit-rate percent 1;
            priority high;
        }
        SC-MULTIMEDIA {
            transmit-rate percent 20;
            buffer-size percent 20;
            priority medium-high;
        }
    }
}
```