

# IMPLEMENTACE SÍŤOVÝCH PRVKŮ CISCO VE STŘEDNĚ VELKÉ NADNÁRODNÍ SPOLEČNOSTI

Bc. Ivo Špičák

---

Diplomová práce  
2015



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2014/2015

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Ivo Špičák**  
Osobní číslo: **A13397**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Návrh a konfigurace aktivních prvků ve středně velké nadnárodní společnosti**  
Téma anglicky: **The Design and Configuration of Active Elements in Medium-sized Multinational Companies**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Analyzujte současný stav sítě konkrétní společnosti.
3. Navrhněte formou projektu možné technické řešení.
4. Navržené řešení zrealizujte a vyhodnoťte.
5. Uvedte cenovou rozvahu řešení.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BIGELOW, Stephen J.** Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.
2. **DOSTÁLEK, Libor.** Velký průvodce protokoly TCP/IP: bezpečnost. Vyd. 1. Praha: Computer Press, 2001, xvi, 565 s. ISBN 80-722-6513-X.
3. **EMPSON, Scott.** CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 336 s. ISBN 978-80-251-2286-0.
4. **HORÁK, Jaroslav a Milan KERŠLÁGER.** Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-80-251-3176-3.
5. **LAMMLE, Todd.** CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.
6. **VELTE, Toby J a Anthony T VELTE.** Síťové technologie Cisco: velký průvodce. Vyd. 1. Brno: Computer Press, 2003, 759 s. ISBN 80-722-6857-0.
7. **MCQUERRY, Steve, David JANSEN a Dave HUCABY.** Cisco LAN switching configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2009, 333 p. Cisco Press networking technology series. ISBN 15-870-5610-0.
8. **CISCO SYSTEMS, Inc.** Catalyst 3750 Switch Software Configuration Guide. Cisco IOS Release 12.2(52)SE. San Jose, USA: Cisco Systems, Inc., 2009, 1394 s.  
Dostupné z:  
[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2\\_52\\_se/configuration/guide/3750scg.pdf](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_52_se/configuration/guide/3750scg.pdf)

Vedoucí diplomové práce:

**Ing. Miroslav Matýsek, Ph.D.**

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

**12. ledna 2015**

Termín odevzdání diplomové práce:

**15. května 2015**

Ve Zlíně dne 6. února 2015

doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

### **Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- Že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

## **ABSTRAKT**

Diplomová práce se věnuje implementaci síťových prvků do středně velké nadnárodní společnosti. Cílem práce je provést návrh zavedení síťových prvků, u kterých jsou použity různé síťové protokoly.

V první části je popsána tematika sítí a síťových protokolů. Dále se věnuje tématu přenosových médií, jež se používají pro propojení jednotlivých síťových prvků.

Druhá část zahrnuje audit stávající sítě společnosti, jeho vyhodnocení a doporučení, dále se věnuje samotné implementaci navrhnutého řešení. Závěrečná část popisuje koncepty možné vyšší dostupnosti sítě a rozvahu cenových nabídek jednotlivých dodavatelů na realizaci projektu.

Klíčová slova: Cisco směrovač, Cisco přepínač, síťové protokoly, přenosová média, MAC, zabezpečení.

## **ABSTRACT**

The Master thesis deals with the implementation of network elements into middle-sized international company. The target of the thesis is to develop the proposal of network elements, where the varied network protocols are being used.

The first part describes the theme of networks and network protocols. Further on it focuses on the topic of transmission media that can be used for connection of the individual network elements.

The second part includes the audit of current company network, its evaluation and recommendation, hereinafter it concentrates on the implementation of proposed solution. Final part covers the proposals of possible higher network accessibility and comparison of price estimations from individual suppliers for project execution.

Key words: Cisco router, Cisco switch, network protocols, transmission media, MAC, security.

Rád bych poděkoval vedoucímu práce Ing. Miroslavu Matýskovi Ph.D., za vedení mé práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

ÚVOD.....	9
<b>I TEORETICKÁ ČÁST.....</b>	<b>10</b>
<b>1 DATOVÉ SÍTĚ A JEJICH PROSTŘEDKY .....</b>	<b>11</b>
1.1 DATOVÁ SÍŤ .....	11
1.2 SÍŤOVÉ PROTOKOLY .....	12
1.2.1 Vrstvy referenčního modelu <i>OSI</i> a dané síťové protokoly: .....	13
1.2.2 Protokol <i>NTP</i> .....	15
1.2.3 Protokol <i>TCP</i> .....	16
1.2.4 Protokol <i>DHCP</i> .....	17
1.2.5 Protokol <i>OSPF</i> .....	17
1.2.6 Protokol <i>VTP</i> .....	20
1.3 SÍŤE <i>VLAN</i> .....	22
1.3.1 <i>IEEE 802.1q</i> .....	23
1.3.2 Statické síťe <i>VLAN</i> .....	24
1.3.3 Dynamické síťe <i>VLAN</i> .....	24
1.3.4 Identifikace sítí <i>VLAN</i> .....	25
1.4 PŘEPÍNÁNÍ.....	25
1.5 SMĚROVÁNÍ.....	26
1.6 PŘENOSOVÁ MÉDIA .....	27
1.6.1 Kroucená dvojlinka .....	28
1.6.2 Optický kabel .....	29
<b>II PRAKTICKÁ ČÁST .....</b>	<b>33</b>
<b>2 IMPLEMENTACE SÍŤOVÝCH PRVKŮ .....</b>	<b>34</b>
2.1 AUDIT SOUČASNÉHO STAVU .....	34
2.1.1 Sběr dat.....	34
2.1.2 Analýza dat a vyhodnocení .....	37
2.1.3 Doporučení .....	38
<b>3 IMPLEMENTACE .....</b>	<b>41</b>
3.1 HLAVNÍ PŘEPÍNAČ CISCO CATALYST 3750X.....	41
3.1.1 Konfigurace zabezpečení přepínače Catalyst 3750X.....	42
3.1.2 Nastavení <i>NTP</i> , logování a hostname .....	43
3.1.3 Konfigurace <i>VLAN</i> a protokolu <i>VTP</i> .....	44
3.1.4 Konfigurace portů .....	48
3.1.5 Nastavení směrování .....	49
3.1.6 Konfigurace <i>DHCP</i> protokolu .....	51
3.2 KONFIGURACE PŘEPÍNAČŮ CISCO CATALYST 2960S .....	54
3.2.1 Konfigurace <i>VTP</i> .....	54
3.2.2 Konfigurace portů .....	57
3.2.3 Vzdálená správa .....	58
3.3 KONFIGURACE SMĚROVAČE CISCO 2801 .....	60
3.3.1 Zabezpečení, <i>NTP</i> a změna názvu směrovače .....	60
3.3.2 Konfigurace portů .....	61
3.3.3 Konfigurace protokolu <i>OSPF</i> .....	63
<b>4 MOŽNOSTI DALŠÍHO ROZŠÍŘENÍ SÍŤE .....</b>	<b>68</b>

4.1	VNITŘNÍ SÍŤ.....	68
4.2	VPN.....	69
<b>5</b>	<b>ROZPOČET PROJEKTU.....</b>	<b>71</b>
	<b>ZÁVĚR.....</b>	<b>75</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>77</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>79</b>
	<b>SEZNAM OBRÁZKŮ.....</b>	<b>81</b>
	<b>SEZNAM TABULEK.....</b>	<b>83</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>84</b>

## ÚVOD

Počítačové sítě jsou v dnešní době již nedílnou součástí komunikace a propojením společností s celým světem či propojením lokálních firemních sítí různých společností navzájem mezi sebou takovým způsobem, aby jejich vzájemně sdílené informace nemohly být zneužity třetí stranou.

Toto téma je stále více diskutované a názory na kvalitní podnikovou síť se výrazně liší, ať už v použití síťových prvků, co se týče typů, výrobců nebo na druhu použití komunikačního média, které síťové prvky vzájemně propojí. Nicméně volba správného řešení realizace lokální sítě společnosti a její připojení přímo do veřejné sítě (Internetu) či virtuální sítě, jejímž prostřednictvím se propojí podniky mezi sebou privátní linkou, je individuální a ve většině případů podléhá vnitřním bezpečnostním pravidlům a potřebám daných společností. Není možné použít žádné multifunkční řešení, které by vyhovovalo všem možným podmínkám, nicméně existují standardy v rámci síťové problematiky, jako jsou přenosová média, síťové prvky či síťové protokoly.

Kvalitně realizovaná podniková síť zajišťuje bezpečný přenos dat a také dává možnost maximálního využití výpočetní techniky. To vše umožňuje efektivní práci zaměstnanců, kteří spravují a vytvářejí důležitá data organizace.

Také pro bezpečnostní aplikace, které využívají počítačovou síť, je nutné zajistit dostupnost veškerých komponent (servery, diskové police, databáze) pro jejich správnou funkčnost a pro zajištění bezpečnosti přenášených informací.

Tato práce se věnuje auditu stávající sítě středně velké nadnárodní společnosti, jeho vyhodnocení a návrhu nového řešení.

První část práce je věnována problematice datových sítí, síťových protokolů a přenosových médií. Druhá a následující části se zabývají auditem sítě podniku a následně navrhuje vhodné řešení sítě podniku. Navrhované řešení je realizováno v praxi a jsou popsány konfigurace jednotlivých síťových prvků, které jsou předmětem realizace. Na závěr je proveden návrh vhodného rozšíření či zabezpečení sítě do budoucna a cenová rozvaha celého provedení.

## **I. TEORETICKÁ ČÁST**

# 1 DATOVÉ SÍTĚ A JEJICH PROSTŘEDKY

## 1.1 Datová síť

Datové neboli počítačové sítě se za posledních několik desítek let velmi rozšířily a byly nuceny se velmi rychle vyvíjet. Bylo nezbytné udržet krok se stále se zvyšujícími nároky uživatelů, kteří chtějí sdílet velké množství dat, aplikací a zařízení [1].

Pro zajištění komunikace mezi jednotlivými uživateli jsou v datových sítích používány tyto prostředky:

- Přenosová média (metalické kabely, optické kabely, vzduch).
- Přepínače (*switch*).
- Směrovače (*router*).
- Firewall.
- Síťové protokoly [2].

Dělení počítačových sítí:

- Homogenní
  - Stejná hardwarová platforma.
  - U jednotlivých koncových prvků stejný operační systém.
  - Používá se stejný přenosový protokol.
- Nehomogenní
  - Různá hardwarová platforma.
  - U jednotlivých koncových prvků různé operační systémy.
  - Jsou používány různé přenosové protokoly [2].
- Klient – server
  - Většina komunikace probíhá mezi klientem a serverem.
  - Server zprostředkovává komunikaci mezi klienty.
- Rovný s rovným (*peer-to-peer*)
  - Každý počítač může pracovat jako klient i jako jednoduchý server [2].

Počítačová síť tedy umožňuje komunikaci uživatelům podle určitých pravidel, za účelem sdílení společných zdrojů [3].

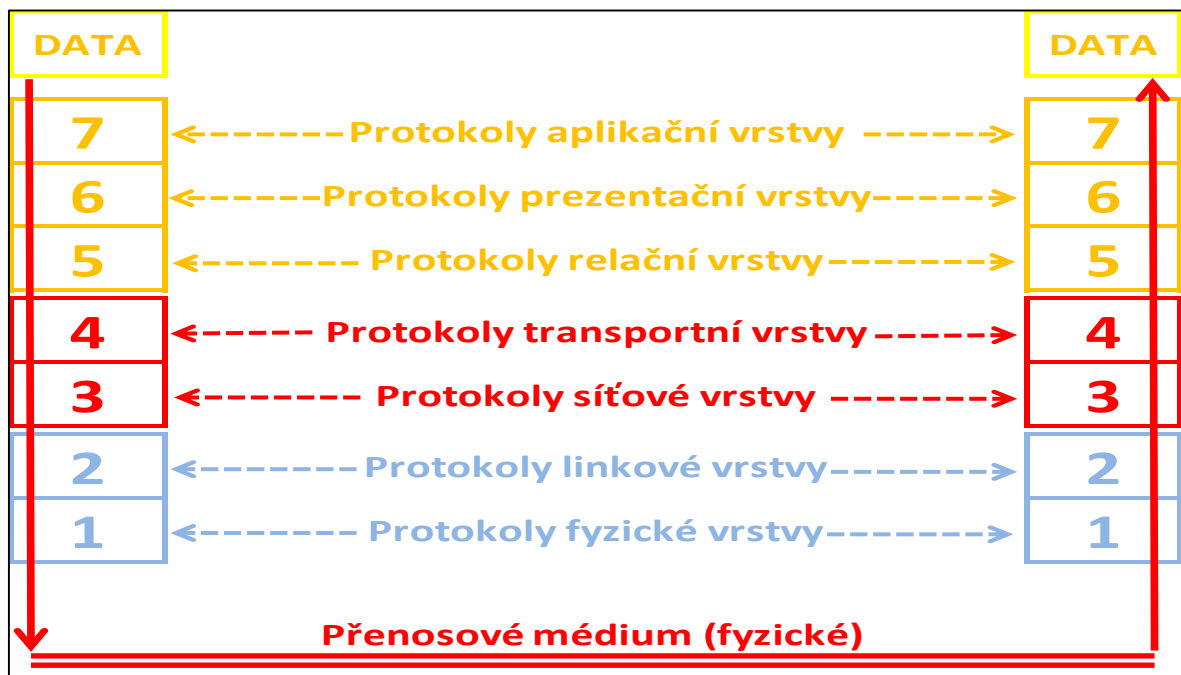
## 1.2 Síťové protokoly

Síťový protokol umožňuje výměnu dat prostřednictvím počítačové sítě za určitých pravidel. Komunikační zařízení se musejí shodovat ve společné sadě pravidel, tedy musí se shodnout na společném síťovém protokolu [2], [4].

Protokol může definovat:

- Kdy zpráva začíná a kdy končí.
- Maximální dobu, která může uplynout, než je zpráva přijata jednou ze stran.
- Druh přenosového média.
- Jak se zachovat, pokud dojde k poškození dat.

Jednotlivé síťové protokoly jsou přiřazeny k různým vrstvám modelu *ISO/OSI* (*Open Systems Interconnection/ Open Systems Interconnection*) nebo *TCP/IP* (*Transmission Control Protocol/Internet Protocol*). Ve vrstvě modelu *OSI* je přiřazena řada protokolů, jež plní funkce dané vrstvy. Je zde využívána takzvaná horizontální komunikace, kdy jednotlivé protokoly komunikují s protokoly sousedních vrstev pomocí hlaviček, popřípadě zápatí datových celků *PDU* (*Protocol Data Unit*) [5].



Obr. 1. Vrstvy modelu OSI [2]

Referenční model *OSI* umožňuje přenos dat mezi různorodými hostitelskými systémy. Tedy zajišťuje komunikaci mezi unixovými systémy a počítači s jiným operačním systémem [1].

Model *OSI* je množina zásad, podle nichž mohou vývojáři aplikací vytvářet a implementovat aplikace pracující v síti. Také definuje schéma pro vytváření a implementaci síťových standardů, zařízení a schémat propojování sítí [1].

Celý model *OSI* má sedm vrstev, které jsou dále rozděleny do dvou skupin. Tři nejvyšší vrstvy definují, jak aplikace na koncových stanicích mohou komunikovat s uživateli a také vzájemně mezi sebou. Spodní čtyři vrstvy pak popisují způsob přenosu dat od jednoho koncového zařízení do druhého [1].

### 1.2.1 Vrstvy referenčního modelu *OSI* a dané síťové protokoly:

- 1) **Aplikační vrstva** – poskytuje aplikačním procesům přístup je komunikačnímu systému a tím zajišťuje jejich vzájemnou spolupráci. Služby poskytované aplikační vrstvou může být zařazen přenos zpráv, identifikace komunikačních parametrů, ověření připravenosti komunikačního partnera, dohoda o způsobu ochrany zpráv, synchronizace spolupracujících aplikací a další [3].
  - **SMTP (Simple Mail Transfer Protocol)** – tento protokol je určený pro přenos zpráv elektronické pošty a zajišťuje doručení zprávy prostřednictvím přímé komunikace mezi odesílatelem a adresátem. Do poštovní schránky adresáta je doručena odeslaná zpráva a k té může adresát přistupovat prostřednictvím protokolů *IMAP (Internet Message Access Protocol)* nebo *POP3 (Post Office Protocol)* [5].
  - **FTP (File Transfer Protocol)** – protokol používaný pro přenos souborů. *FTP* je jeden z nejstarších protokolů a využívá porty 21 a 20. V protokolu je použit model klient – server [4], [5].
- 2) **Prezentační vrstva** – šestá vrstva modelu *OSI* zajišťuje transparentní přenos zpráv mezi koncovými uživateli a zabývá se strukturou přenášení zprávy. Úkolem šesté vrstvy je zajistit takovou reprezentaci informace, kterou jednotlivé aplikační entity používají při komunikaci nebo se na ni odvolávají. Hlavní účel je reprezentovat přenášené zprávy daným aplikacím jednotným způsobem [3].

- **TLS (Transport Layer Security)** – jeden s protokolů zajišťující kryptografii při komunikaci Internetem. Jeho nástupcem je protokol *SSL (Secure Sockets Layer)* [3].
- 3) **Relační vrstva** – tato vrstva je odpovědná za ustavení, správu a ukončení relací mezi entitami prezentační vrstvy. Zajišťuje také řízení dialogu mezi oběma zařízeními neboli uzly. Řídí komunikaci mezi systémy prostřednictvím následujících interakcí:
- Jednosměrné.
  - Obousměrně střídavé.
  - Obousměrně současné [3].
- 4) **Transportní vrstva** – vrstva nazývaná také jako přenosová, která segmentuje data do datového proudu a poté je zpětně sestavuje. Tato vrstva jednoznačně identifikuje veškeré relační entity tak, že jím přiřadí transportní adresu. Transportní spojení poskytuje duplexní přenos mezi dvojicí transportních adres. Je možné vytvoření více transportních spojení mezi jednou dvojicí transportních adres a tyto spojení jsou ve svých činnostech nezávislé [1], [3].
- **TCP (Transmission Control Protocol)** – je spojově orientovaný protokol, který zajistí spojení mezi dvěma aplikacemi. Základní jednotkou *TCP* je segment, který je vložen do *IP* datagramu. Vyznačuje se spolehlivým doručováním [4].
  - **UDP (User Datagram Protocol)** – tento protokol neposkytuje žádné záruky doručení. *UDP* nenavazuje spojení jako *TCP* protokol, pouze *UDP* datagram je přiřazen k *IP* datagramu [9].
- 5) **Síťová vrstva** – třetí vrstva referenčního modelu *OSI* má na starosti adresování zařízení, sleduje umístění zařízení v síti a stanovuje nejvhodnější způsob dopravy dat. Tedy síťová vrstva musí zajišťovat i provoz mezi zařízeními, která k ní nejsou připojena lokálně. Zařízeními třetí vrstvy jsou směrovače a některé přepínače, které zajišťují služby směrování v datové síti [1].
- **IPv4 (Internet Protocol version 4)** – datově orientovaný protokol používaný v sítích s přepojováním paketů. Jedná se o protokol spravující data bez záruky a negarantuje ani doručení, zachování pořadí a ani vyloučení duplicity [3].

- **ICMP (Internet Control Message Protocol)** – umožňuje směrovačům posílat chybové a řídicí zprávy ostatním směrovačům i počítačům, je součástí *IP* [2].
- 6) **Linková vrstva** – neboli spojová vrstva umožňuje síťové vrstvě řídit propojení datových okruhů ve fyzické vrstvě. Linková vrstva se pomocí hardwarové *MAC (Media Access Control)* adresy postará o to, aby se zprávy dostaly ke správnému zařízení v síti *LAN*, a převádí zprávy ze síťové vrstvy do jednotlivých bitů k vysílání ve fyzické vrstvě. Tato vrstva formátuje pakety do částí, které se nazývají datové rámce a k min doplňuje upravenou hlavičku s hardwarovou zdrojovou a cílovou adresou [1].
- **ETHERNET** – jedná se o souhrn topologií pro lokální počítačové sítě většinou standardizovaných jako *IEEE 802.3 (Institute of Electrical and Electronics Engineers)*, jež používají kabely s kroucenou dvoulinkou a optické kabely pro komunikaci s přenosovými rychlostmi od 10 Mbit/s po 100 Gbit/s [3].
- 7) **Fyzická vrstva** – tato vrstva zajišťuje odesílání a přijímání bitů. Fyzická vrstva komunikuje přímo s různými typy komunikačních médií, která pak reprezentují bitové hodnoty. První vrstva referenčního modelu *OSI* specifikuje elektrické, mechanické, procedurální a funkční požadavky na aktivaci, udržení a deaktivaci fyzické linky mezi koncovými systémy. Příklad *ETHERNETU* na fyzické vrstvě:
- **100BASE-TX** – pro přenos je využívána kroucená dvojlinka Cat 5 a přenosová rychlost je 100 Mbit/s. Poloduplex - jen jedním párem v jednom směru 100 Mb/s, plný duplex - oběma páry najednou, ale párem vždy jednosměrně 100 Mb/s [2].

### 1.2.2 Protokol *NTP*

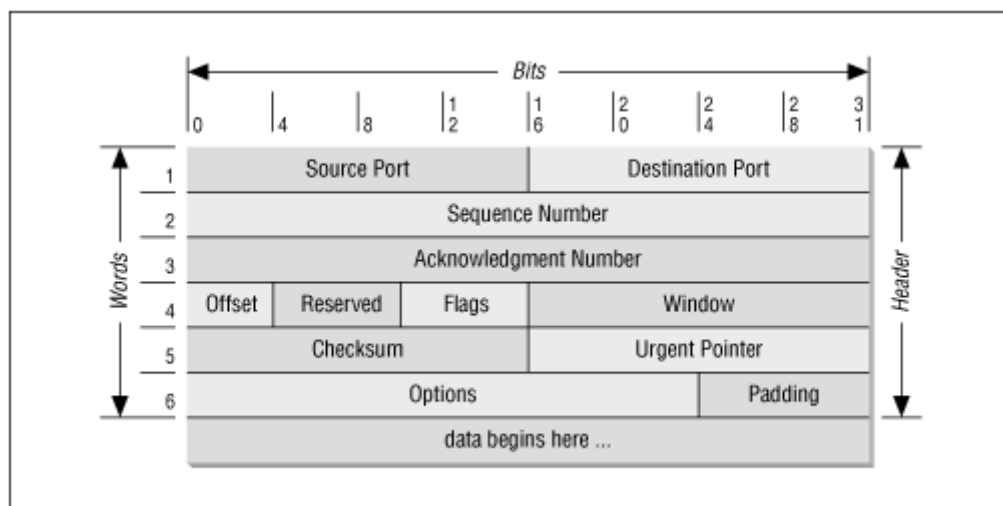
Protokol *NTP (Network Time Protokol)* slouží k synchronizaci systémového času síťových prvků, serverů či koncových prvků [4], [6]. Je součástí sedmé aplikační vrstvy síťové architektury *OSI*.

*NTP* je jeden z nejstarších doposud používaných *TCP/IP* protokolů. Funguje na architektuře klient-server, kdy klient (PC, server, přepínač, směrovač) vyšle jeden či několik dotazů několika *NTP* serverům a ty mu v odpovědi pošlou svůj přesný čas. Klient

nejprve z odpovědi vyloučí servery se zřejmě nesmyslným časem a poté ponechá skupinu serverů s největším společným průnikem. V podnikových sítích využívajících architekturu *AD (Active Directory)* se většinou používá jeden *NTP* server, a to doménový kontrolér [7].

### 1.2.3 Protokol TCP

Protokol *TCP (Transmission Control Protocol)* od aplikací získává datové bloky, které rozdělí na menší části tak zvané segmenty. Každá tato část neboli segment je očíslována a zařazena tak, aby jednotlivé části mohly být opět uspořádány cílovým zásobníkem protokolu *TCP*. Zásobník se řídí požadavky dané aplikace. Zásobník protokolu *TCP* vyčká na potvrzení přijetí segmentů. Pokud dojde k nějakým ztrátám při přenosu, tak opakuje přenos nepotvrzených segmentů [8]. Před tím, než dojde k samotnému přenosu dat, zásobník kontaktuje příjemce k navázání spojení. Tato vazba se definuje jako transportní spoj. Jedná se tedy o spojovanou komunikaci [8].



Obr. 2. Formát segmentu TCP [9]

Protokol *TCP* se vyznačuje spolehlivostí, přesností, je spojovaný a plně duplexní. Ale jsou pro něj typické i velké nároky na kapacitu sítě, což je zapříčiněno také jeho složitostí. Je nejpoužívanějším protokolem v sadě protokolů *TCP/IP* na transportní vrstvě [3].

#### 1.2.4 Protokol DHCP

Protokol *DHCP* (*Dynamic Host Configuration Protocol*) zjednodušuje přiřazování a správu počítačů připojených k síti *TCP/IP*. Protokol *DHCP* automaticky přiřazuje *IP* adresy pro počítače a jiná zařízení v síti z fondu dostupných adres [1].

Nakonfigurovaný server *DHCP* poskytuje databázi dostupných *IP* adres a mohou být nastavovány možnosti konfigurace pro klienty včetně adres serverů *DNS* (*Domain Name System*), adres brány a masky [1].

*DHCP* klient vyšle broadcastem *DHCP Discover* paket na něž odpoví *DHCP* server paketem *DHCP Offer* s nabídkou *IP* adresy. To umožňuje automatické přiřazení adresy *IP* spolu s maskou podsítě a dalšími informacemi. Adresa *IP* je přidělena každému klientovi na omezenou dobu. Tento proces se označuje jako zápůjčka. Zápůjčky mohou být čas od času obnoveny, což zajišťuje relaci bez přerušování. Zápůjčky jsou obnovovány po uplynutí zhruba poloviny jejich délky a je-li obnovení úspěšné, zůstává adresa *IP* přiřazena klientovi. Pokud není úspěšné, vrátí se adresa *IP* do fondu adres a je k dispozici pro jiného uživatele [4].

Klient, který odesílá zprávy *DHCP Discover* požádá o přidělení *IP* adresy, odesílá všesměrové vysílání na vrstvách 2 a 3 *TCP/IP* modelu. Všesměrové vysílání na vrstvě 2 obsahuje výhradně hexadecimální znaky F. Cílová *MAC* adresa tedy je: FF:FF:FF:FF:FF:FF. Všesměrové vysílání na vrstvě 3 má cílovou adresu 255.255.255.255, což znamená všechny sítě a všechny hostitele. Protokol *DHCP* je nespojovaný. Používá tedy protokol *UDP* (*User Datagram Protocol*) na transportní vrstvě, která se také označuje jako hostitelská vrstva [1].

#### 1.2.5 Protokol OSPF

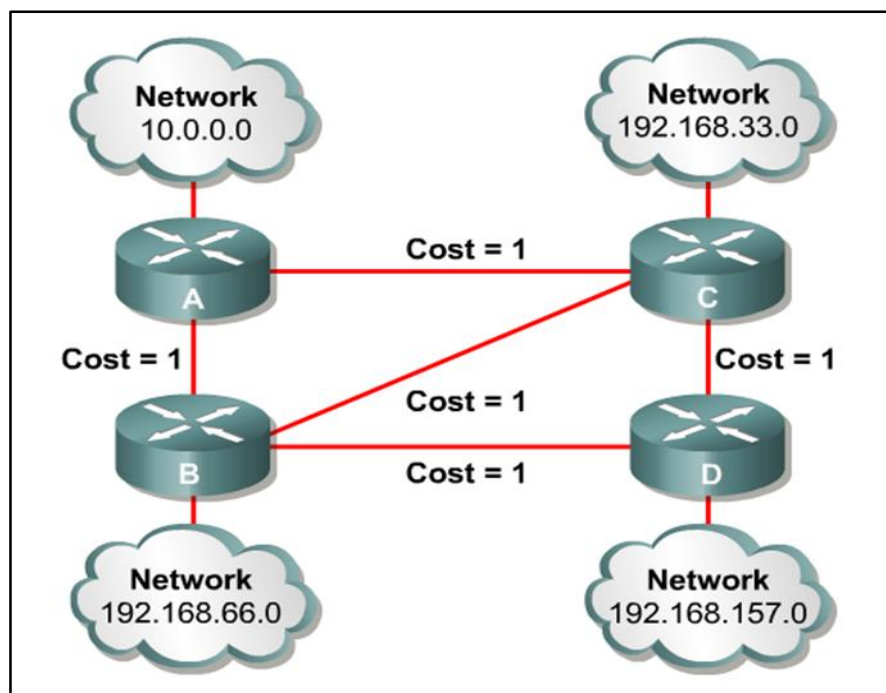
Protokol *OSPF* (*Open Shortest Path First*) je směrovací protokol otevřeného standardu, který implementuje mnoho dodavatelů síťových zařízení včetně společnosti Cisco. Používá se v případech, kdy ne všechny směrovače jsou od stejného výrobce. Protokol *OSPF* využívá takzvanou redistribuci tras [1].

Fungování protokolu *OSPF* je založeno na Dijkstrově algoritmu. Všechny uzly v síti mají úplnou informaci o jednotlivých spojích a mohou si vypočítat optimální cesty. Protokol *OSPF* konverguje velmi rychle a podporuje více tras se stejnými náklady do jednoho cíle [1].

**OSPF poskytuje tyto funkce:**

- Skládá se z oblastí a autonomních systémů.
- Minimalizuje provoz aktualizace směrování.
- Umožňuje škálovatelnost.
- Má neomezený počet přeskoků.
- Je implementován více společnostmi (otevřený standart) [1].

Protokol *OSPF* je první protokol se stavem linky.



Obr. 3. OSPF [10]

Na obrázku (Obr. 3) lze vidět, že ze směrovače A do směrovače D vedou dvě rovnocenné cesty, proto jsou obě ve směrovací tabulce na obrázku (Obr. 4). Když si směrovač A vybere cestu ke směrovači D přes směrovač C a ta se přeruší (zácpa, porucha), protokol *LSA (Link State Advertisements)* to rozpozná a začne používat cestu přes směrovač B [10].

Router	Destination	Next Hop	Cost
A	192.168.66.0	B	1
A	192.168.33.0	C	1
A	192.168.157.0	B	2
A	192.168.157.0	C	2
B	10.0.0.0	A	1
B	192.168.33.0	C	1
B	192.168.157.0	D	1
C	10.0.0.0	A	1
C	185.134.0.0	B	1
C	192.168.157.0	D	1
D	10.0.0.0	B	2
D	10.0.0.0	C	2
D	192.168.66.0	B	1
D	192.168.33.0	C	1

Obr. 4. Směrovací tabulka OSPF [10]

Každý směrovač v rámci oblasti spočítá nejlepší (nejkratší) trasu do každé sítě ve stejné oblasti. Tento výpočet je založen na datech shromážděných v topologické databázi a na algoritmu, který se označuje jako „algoritmus nejkratší cesty“ neboli *SPF (Shortest Path First)*. Každý směrovač v oblasti si vytváří strom podobný rodokmenu, ve kterém je příslušný směrovač umístěn v kořeni a všechny ostatní sítě jsou uspořádány podél větví a listů tohoto stromu. Jedná se o strom nejkratší cesty pomocí, kterého směrovač vkládá trasy do směrovací tabulky. Strom obsahuje pouze sítě nacházející se ve stejné oblasti [1].

Protokol *OSPF* používá metriku označovanou jako *náklady*. Náklady souvisejí s každým výstupním rozhraním, které je součástí stromu nejkratších cest. Náklady na celou cestu jsou dány součtem nákladů výstupních rozhraní podél celé cesty. Hodnotu nákladů lze podle standardu *RFC 2338* zvolit libovolně. Společnost Cisco implementovala vlastní metodu výpočtu nákladů všech rozhraní s podporou protokolu *OSPF*. Cisco používá rovnici  $108/\text{šířka pásma}$ . Šířka pásma odpovídá konfigurované šířce pásma rozhraní. Tedy dle tohoto pravidla má rozhraní Fast Ethernet s rychlostí 100 Mb/s výchozí náklady *OSPF* 1. Tyto náklady lze upravit ručně příkazem `ip ospf cost [1]`.

#### Klíčové pojmy protokolu *OSPF*:

- **Linka** – rozhraní sítě nebo směrovače, které je přiřazeno k dané síti.
- **ID směrovače** – *IP* adresa sloužící k jeho identifikaci.
- **Soused** – označuje dva nebo více směrovačů, jež mají rozhraní ve stejné síti.

- **Přilehlost** – vztah mezi dvěma směrovači *OSPF* dovoluje přímou výměnu aktualizací tras.
- **Protokol Hello** – protokol *OSPF* Hello zajišťuje dynamické zjišťování sousedů a udržuje mezi nimi vztahy.
- **Databáze sousedství** – obsahuje seznam všech směrovačů, pro které byly zjištěny pakety Hello.
- **Topologická databáze** – zde se nachází údaje o všech paketech *LSA* (*Link State Advertisement*), který byly pro oblast přijaty.
- **Paket LSA** – datový paket protokolu *OSPF*, který obsahuje informace a stavu linky a směrování, jež jsou sdíleny mezi směrovači *OSPF*.
- **Oblasti OSPF** – sdružuje spojitou množinu sítí a směrovačů. Všechny směrovače ve stejné oblasti sdílejí společné *ID* oblasti. Vzhledem k tomu, že směrovač může být současně členem více oblastí, tak *ID* oblasti je ke konkrétnímu rozhraní směrovače. Všechny směrovače v rámci stejné oblasti mají stejnou tabulku topologie [1].

### 1.2.6 Protokol VTP

*VTP* (*VLAN Trunking Protokol*) je Cisco proprietární síťový protokol. Základním úkolem protokolu *VTP* je správa všech konfigurovaných sítí *VLAN* v rámci přepínané datové sítě a služba konzistence v celé síti. Protokol *VTP* umožňuje přidávat a odebírat sítě *VLAN* a měnit jejich názvy. Příslušné informace pak šíří všem ostatním přepínačům v doméně *VTP* [1].

Seznam některých užitečných funkcí, které protokol *VTP* poskytuje:

- Konzistentní konfigurace sítí *VLAN* přes všechny přepínače v síti.
- Přesné sledování a monitoring sítí *VLAN*.
- Dynamické oznamování přidanych sítí *VLAN* všem přepínačům v doméně *VTP*.
- Přidání sítí *VLAN* technologií Plug-and-Play [1].

Nejdříve je nutné vytvořit v rámci domény *VTP* server. Všechny servery, které mají sdílet informace sítí *VLAN*, musí používat stejný název domény a přepínače mohou být v konkrétním okamžiku pouze v jediné doméně.

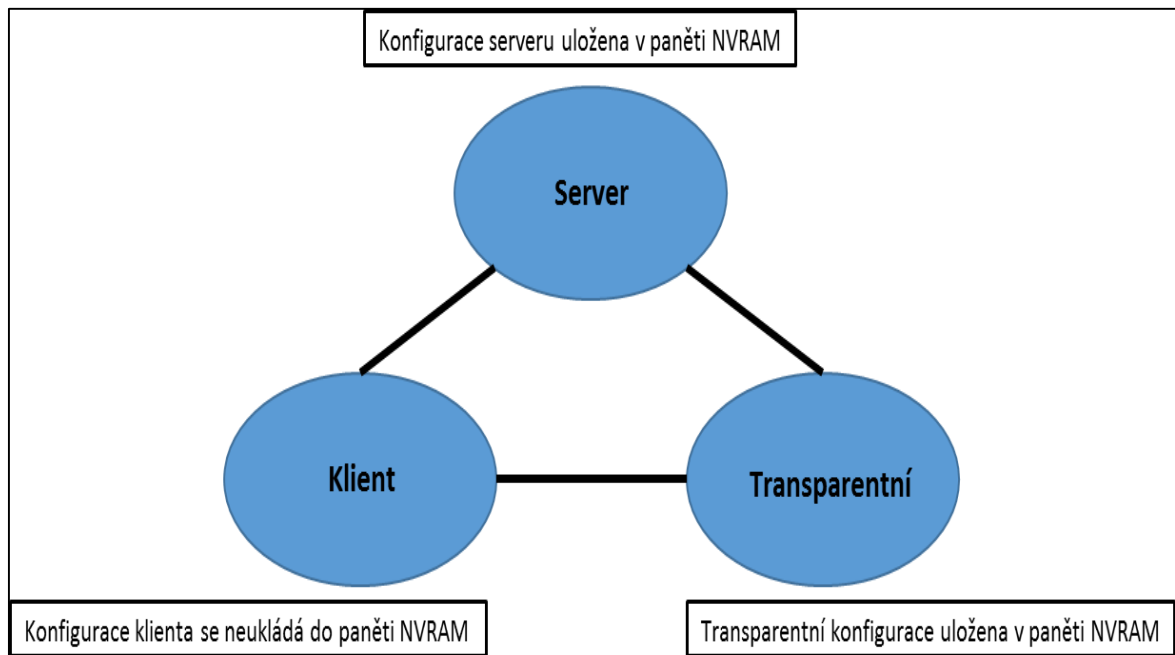
Přepínače propagují informace domény *VTP* pro správu a také číslo revize konfigurace a všechny známé sítě *VLAN* s případnými konkrétními parametry. K dispozici je také takzvaný *transparentní režim VTP*. V tomto režimu je možné přepínače nakonfigurovat tak, aby předávaly informace protokolu *VTP* přes trunkové porty, ale nepřijímaly aktualizace informací, ani neaktualizovaly své databáze *VTP* [1].

Přepínače detekují všechny přidávané *VLAN* na základě oznámení *VTP*. Poté na svých trunkových portech připraví k odeslání informaci o nově definované síti *VLAN*. Informace se odesílají jako čísla revizí, která jsou tvořena číslem oznámeným zvýšeným o jednotku. Kdykoli přepínač zjistí vyšší číslo revize, může z toho odvodit, že informace je aktuálnější, takže pomocí nových údajů přepíše obsah stávající databáze [1].

### **Režimy činnosti VTP:**

1. **Server:** Jedná se o výchozí režim všech přepínačů Cisco. V každé doméně *VTP* musí být alespoň jeden server, který šíří informace sítí *VLAN* v rámci dané domény. Přepínač se musí nacházet v serverovém režimu, aby mohl vytvářet, přidávat a odstraňovat sítě *VLAN* v doméně *VTP*. Informace *VTP* je nutné měnit v serverovém režimu. Libovolná změna provedená v serverovém režimu přepínače je oznámena do celé domény *VTP* [1].
2. **Klient:** Klientské režimy přepínače přijímají informace ze serveru *VTP*, ale zároveň odesílají a přijímají aktualizace. Z tohoto hlediska se chovají jako servery *VTP*. Rozdíl spočívá v tom, že neumožňují vytvářet, měnit či odstraňovat sítě *VLAN*. Do nové sítě *VLAN* navíc nelze přidat žádné porty klientského přepínače dříve, než novou síť *VLAN* odeslanému přepínači oznámí server *VTP* [1].
3. **Transparentní:** Přepínače v transparentním režimu se neúčastní domény *VTP* ani nesdílejí databázi sítí *VLAN*, ale předávají oznámení protokolu *VTP* pomocí konfigurovaných trunkových portů. Mohou vyvířet, upravovat a odstraňovat sítě *VLAN*, protože udržují svou vlastní databázi, kterou však neposkytují jiným přepínačům [1].

Protokol *VTP* umožňuje šetřit šířku pásma díky redukci množství paketů všesměrového, vícesměrového a jednosměrového vysílání. Tato operace se označuje jako *redukce*. Přepínače s redukcí protokolu *VTP* odesílají všesměrová vysílání pouze na trunkové linky, které příslušné informace vyžadují.



Obr. 5. Režimy protokolu VTP [1]

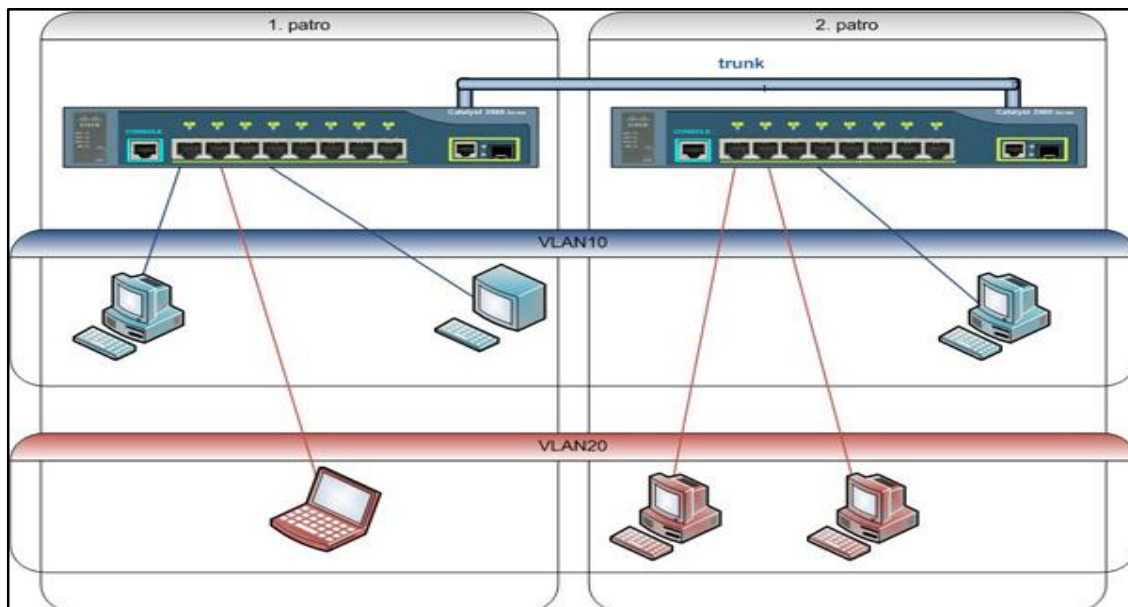
### 1.3 Síť VLAN

Virtuální síť slouží k logickému rozdělení sítě, které jsou nezávislé na fyzickém uspořádání. Je tedy možné segmentovat síť na menší sítě uvnitř fyzické struktury původní sítě. Zde jsou důležité porty, které jsou označovány jako trunk, což znamená, že tento port je zařazen do více VLAN [11]. Pokud je vytvořena virtuální síť, je možnost v rámci přepínané datové sítě vrstvy 2 vytvořit menší všesměrové domény tak, že různé porty přepínače jsou přiřazeny k různým dílčím sítím. Síť VLAN je považována za vlastní podsít' nebo všesměrovou doménu. Tedy rámce vysílané do sítě jsou přepínány pouze mezi porty, které jsou logicky seskupeny do stejné sítě VLAN [1].

#### Výhody VLAN:

- **Snížení broadcastů** – vytvořením více broadcastových domén bylo docíleno snížení provozu a tedy zvýšení výkonu sítě.
- **Zvýšení zabezpečení** – oddělení komunikace do samostatných VLAN.
- **Oddělení speciálního provozu** – použití i IP telefonie, kdy k jednomu portu je přiřazena speciální VLAN a VLAN pro přístup do běžné sítě. V IP telefonu se tato

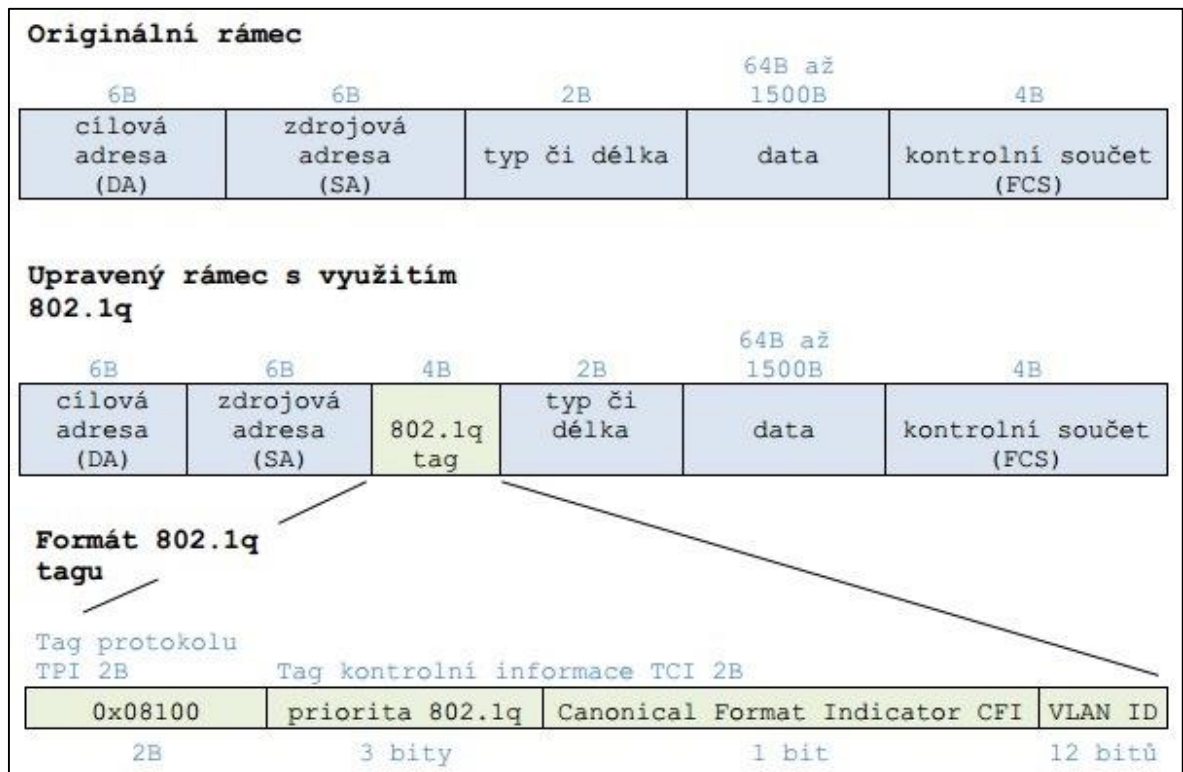
komunikace rozdělí a následně tedy *VLAN* pro *IP* telefonii pak neovlivňuje běžný provoz [11].



Obr. 6. VLAN [11]

### 1.3.1 IEEE 802.1q

Standart *IEEE* 802.1q umožňuje rozdělení fyzické ethernetové sítě do více logických virtuálních sítí. *Trunking protokol* či *dot1q* je založen na principu tak zvaného tagování. *IEEE* 802.1q vloží do záhlaví každého přenášeného rámce 4 oktetové informace; neboli vloží informaci, do jaké virtuální sítě daný rámec patří. Jak je uvedeno na (obr. 7), vezme se původní rámec a jeho hlavička se rozšíří o 4 Bitovou informaci, ve které je v prvním oktetu uvedena neměnná hodnota 0x8100, která určuje, že se jedná o protokol 802.1q . Jako další v pořadí je uvedena priorita dle 802.1q, dále informace, zda je *MAC* adresa v kanonickém tvaru a poslední je uvedeno *ID* virtuální sítě [11].



Obr. 7. Formát Tagu 802.1q [11]

### 1.3.2 Statické síť VLAN

Statické síť VLAN představují nejčastější způsob vytváření sítí VLAN. Statické síť VLAN jsou nejbezpečnější. Tato bezpečnost pramení z toho, že každý port přepínače, který je přiřazen k síti VLAN, toto přiřazení portu zachová trvale, dokud nejsou ručně změněny. Statické síť VLAN se snadno konfiguruje a spravuje a fungují velmi dobře v síťovém prostředí, kde je nutné kontrolovat pohyb uživatelů v rámci sítě [1].

### 1.3.3 Dynamické síť VLAN

Oproti statickým sítím VLAN určují dynamické síť VLAN přiřazení uzlu k síti VLAN automaticky. Port je zařazen do příslušné VLAN dle zdrojové MAC adresy. V tomto případě tedy musí existovat tabulka se seznamem MAC adres pro všechna zařízení s informací, do které VLAN má být přiřazeno. Pokud se tedy síťový prvek do jiného portu na přepínači připojí dynamicky, je tomuto portu přiřazena VLAN dle MAC adresy.

Cisco tuto problematiku řeší pomocí VMPS (VLAN Membership Policy Server), kdy je nutná přítomnost speciálního serveru, který spravuje tabulky MAC adres [11]. Pomocí

služby *VMPS* lze nastavit databázi *MAC* adres, které se použijí při dynamickém adresování sítě *VLAN*. Databáze *VMPS* automaticky mapuje *MAC* adresy na síť *VLAN* [1].

#### 1.3.4 Identifikace sítě *VLAN*

Porty přepínače jsou výhradní rozhraní vrstvy 2, která jsou přidružena k fyzickému portu. Port přepínače může patřit pouze k jediné síti *VLAN*, jedná-li se o přístupový port, nebo ke všem sítím *VLAN*, pokud se jedná o trunkový port. Port je možné konfigurovat ručně jako přístupový nebo trunkový, nebo je možné aktivovat na jednotlivých portech protokol *DTP* (*Dynamic Trunking Protokol*). Protokol *DTP* následně vyjednává s portem na druhém konci linky [1].

**Přístupové porty** (*access port*): patří do jediné sítě *VLAN* a přenáší pouze provoz této sítě. Provoz se přijímá a odesílá v nativním formátu bez jakéhokoliv značkování sítě *VLAN*. Jakákoliv data doručená na přístupový port se považují za data, která patří síti *VLAN* přiřazené k portu [1].

**Trunkové porty**: termín *trunkový port* byl inspirován mezinárodními telefonními linkami, které současně přepínají více telefonických hovorů. Tedy trunkový port dokáže současně přenášet více sítí *VLAN* [1].

### 1.4 Přepínání

Přepínané sítě se využívají především z důvodu, že nedochází ke ztrátě šířky pásma kvůli kolizím se sdíleným médii. Proto je možné docílit velikosti kolizní domény rovno jedné a poskytnout sdílenou šířku pásma. Podporují vyhrazené připojení a virtuální sítě. V dnešní době přepínače zajišťují již mnoho funkcí směrovačů, nicméně je nemohou zcela nahradit. Proto se umisťují mezi hostitele a páteřní síť. Provoz řídí na základě zdrojové a cílové *MAC* adresy na linkové neboli spojové vrstvě. Oproti rozbočovači je přepínač schopen přečíst právě zdrojovou a cílovou *MAC* adresu každého rámce a zprávy přepíná mezi příslušné porty, ke kterým jsou *MAC* adresy mapovány. Neduplikuje se tedy provoz na všechny porty a výjimkou *multicastů* a *broadcastů*. Pokud přepínač přijme rámeček s neznámou cílovou nebo broadcastovou adresou pošle jej na všechny výstupní porty. Rámeček s *multicastovou* adresou lze použít pro správu koncových stanic s využitím protokolu *GMRP* (*GRAP Multicast Registration Protokol*).

Nejčastějším typem přepínání je přepínání procesorem, kdy se přerušuje činnost procesu a procesor zajistí prohledání tabulky *MAC* adres. Tabulku *MAC* adres si přepínač buduje

dynamicky. Nejdříve přepínač prozkoumá zdrojovou *MAC* adresu příchozího rámce a sdruží ji s portem, přes který rámec do přepínače dorazil [3].

#### Druhy přepínání:

- ***Store-and-forward*** – přijatý rámec je nejdříve přijat a uložen do bufferu, následně je určen výstupní port na základě cílové *MAC* adresy.
- ***Cut-through*** – po obdržení části hlavičky (s cílovou *MAC* adresou) je již určován výstupní port a následně je rámec ihned odeslán, a to i v případě že není ještě celý přijat.
- ***Fragment-free*** – kombinace přepínání *Store-and-forward* a *Cut-through* [7].

Veškeré přepínače od společnosti Cisco jsou vybaveny proprietárním protokolem *CDP* (*Cisco Discovery Protokol*), pomocí něhož je mapováno nejbližší okolí. Protokol pracuje na druhé vrstvě *TCP/IP* modelu a je závislý na protokolech vyšší vrstvy. Tento protokol používá multicastovou *MAC* adresu 0100.0ccc.ccc mezi síťovými prvky Cisco a dále se nerozesílá. Prostřednictvím tohoto protokolu přímo sousedící síťové prvky sdílejí informace o *MAC* adrese, *IP* adrese, typu zařízení, verze *IOS* a další [7].

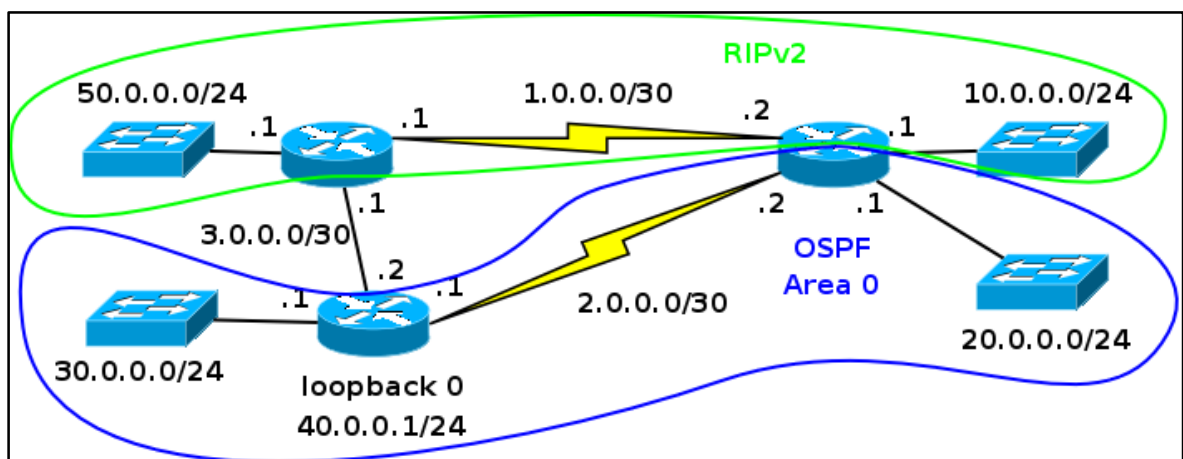
## 1.5 Směrování

Směrovače pracují na třetí tedy na síťové vrstvě *TCP/IP* modelu a zacházejí se síťovými adresami. Hlavním úkolem směrovače je zjištění nejvýhodnější cesty v síti a vnitřní přepínání paketů. Používají se směrovací tabulky na základě logického uspořádání sítě. Ve výchozím nastavení oproti přepínači blokuje směrovač pakety se všeobecnou (broadcast) adresou. Provádí fragmentaci paketů dle nastavení *MTU* (*Maximum Transmission Unit*), fyzickou adresaci a zapouzdření rámce. Cílová adresa se při cestě sítí *IP* datagramu nemění, ale hardwarová se mění při každém přeskočení na hodnotu fyzické adresy následujícího směrovače. Stejný princip je použit u zdrojové *IP* adresy a fyzické zdrojové adresy. Směrování se dělí na statické a dynamické. U statického se cesta konfiguruje ručně a není zde možnost využít alternativních cest. Má ovšem přednost před dynamickým směrováním, pokud není konfigurací priority tato přednost změněna [7].

Směrovače pro svou práci využívají směrovací protokoly, jejichž úkolem je zjišťovat nejlepší cestu k cílové logické adrese dle určitého algoritmu. Snahou směrovacího protokolu je tedy vybírat optimalizovanou cestu k cíli na základě metriky. Nejčastěji používané metriky

jsou počet skoků, délka cesty, šířka pásma, propustnost, cena, maximální délka *MTU* a další.

Rozlišují se vnitřní a vnější směrovací protokoly. Vnitřní zajišťují směrování uvnitř autonomního systému a vnější mezi těmito systémy. Autonomní systém se v *IP* sítích označuje číslem s délkou 16 bitů tedy celkem  $2^{16}$  neopakujících se čísel. Podmínkou vnějších směrovacích protokolů je číselný údaj autonomního systému. Co se týká algoritmu směrování, nejčastěji se používá algoritmus vektorů vzdáleností, algoritmus stavu liny a algoritmy hybridního směrování. Je možné, že se využije více směrovacích protokolů, což může znamenat problém, a proto se používá komunikace s redistribucí směrovacích informací. Redistribuce se používá většinou při manuální konfiguraci na jednotlivých hraničních zařízeních. Ovšem k redistribuci z jednoho směrovacího protokolu do druhého, může dojít pouze u cest, které jsou ve směrovací tabulce [7].



Obr. 8. Redistribuce směrovacích protokolů [12]

Informace se mohou redistribuovat podmíněně pomocí směrovacích map a metriky cest se mezi jednotlivými protokoly přepočítávají. Na obrázku (Obr. 8) je vizualizována redistribuce mezi směrovacími procesy *OSPF* a *RIP* (*Routing Information Protocol*) a to ve směru *OSPF* do *RIP* [7].

## 1.6 Přenosová média

Otázka přenosových médií používaných v počítačových sítích je velmi obsáhlá a zahrnuje nejrůznější druhy médií od koaxiálních kabelů až po optická vlákna. Praktická část práce je

zaměřena na implementaci síťových prvků, které jsou vzájemně propojeny, čili využívají přenos signálu prostřednictvím kroucené dvojlinky a optických kabelů. Proto se tato část věnuje právě těmto přenosovým mediím [7].

Přenosové médium je fyzické médium, kterým jsou přenášena data, hlasový signál či jiné typy signálů. Mezi tyto media patří:

- Metalický kabel.
- Optický kabel.
- Vzduch [3].

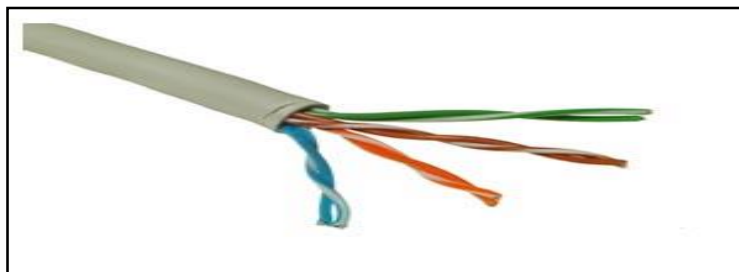
Přenosové médium zprostředkovává přenos signálu na první tedy na fyzické vrstvě *TCP/IP* modelu a přenáší signál na bity a bity na signál. Zprostředkovává komunikaci mezi jednotlivými prvky a jejich rozhraním síťové infrastruktury [7].

### 1.6.1 Kroucená dvojlinka

Jedná se o metalický kabel, který je označován jako *TP (Twisted Pair)*. Je to symetrické přenosové médium. Signál je přenášen jako rozdíl napětí mezi dvěma vodiči. Dva vodiče jsou vždy kolem sebe vzájemně obtočeny, čímž jsou minimalizovány ztráty způsobené kapacitním odporem a *EMI (Elektromagnetická Indukce)* [7].

Pomocí kroucené dvojlinky lze přenášet data až do rychlosti 10 Gb/s. Vyrábí se tři základní typy:

- *UTP (Unshielded Twisted Pair)* – jedná se o nestíněnou variantu.
- *ScTP (Screened Twisted Pair)* – společné stínění pro všechny vodiče.
- *STP (Shielded Twisted Pair)* – samostatné stínění každého páru.



Obr. 9. Příklad UTP kabelu [2]

Kroucená dvojlinka se skládá z těchto částí:

- **Vodič** – vyroben většinou z mědi a páry jsou vždy vzájemně okolo sebe obtočeny. Pro Ethernet 10 Mb/s-100 Mb/s se používají dva páry oproti Ethernetu 1 Gb/s – 10 Gb/s či PoE, kde jsou použity čtyři páry.
- **Stínění** – je použito pouze u *STP* a *ScTP*, kde je splétané nebo fóliové stínění kolem všech párů.
- **Plášť** – vnější kryt vnitřních vodičů, který může být vyroben z PVC či teflonu a zajišťuje prvotní stínění vodičů [2].

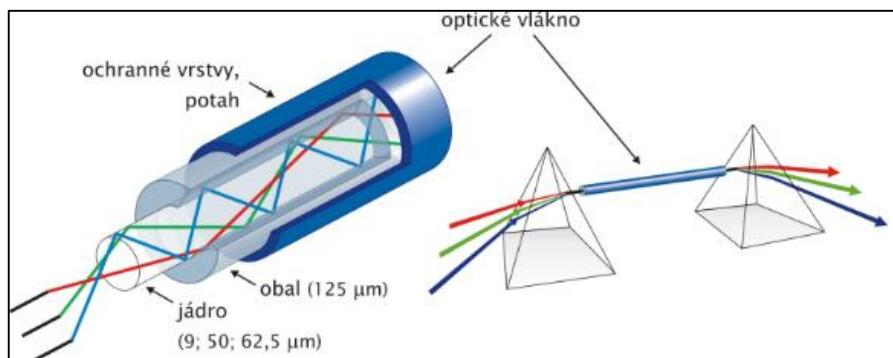
Level	Šířka pásma
1	přenos hlasu do 1 Mb/s, PTSN, ISDN, zvonek
2	ŠP 1,5 MHz, 4 Mb/s Token Ring
3	ŠP 16 MHz, 10 Mb/s Ethernet
4	ŠP 20 MHz, 16 Mb/s Token Ring
5	ŠP 100 MHz, data do 100 Mb/s Ethernet, 155 Mb/s ATM
5E	ŠP 100 MHz, 1 Gb/s Ethernet
6	ŠP 250 MHz, 10 Gb/s Ethernet s problémy
6A	ŠP 500 MHz, vyvinut pro 10 Gb/s Ethernet
7	ŠP 600 MHz, data do 10 Gb/s Ethernet

Obr. 10. Level – Kroucená dvojlinka [2]

Kroucená dvojlinka je jednoduchá na instalaci a umožňuje velmi snadné propojení jednotlivých prvků počítačové sítě. Ovšem je zde omezena přímá vzdálenost mezi jednotlivými prvky, a to do 100 metrů [2].

### 1.6.2 Optický kabel

Optický kabel se skládá z čirého skleněného nebo čirého plastického jádra, které nese světelné impulsy. Jádro je obklopeno zrcadlovou vrstvou, která se nazývá obalový plášť. Okolo tohoto pláště je vrstva plastického distančního proužku. Poté následuje ochranná vrstva tvořena tkanými kevlarovými vlákny, všechny části jsou v jeden celek sloučeny vnější vrstvou teflonu nebo PVC (Polyvinylchlorid) [4].



Obr. 11. Optické vlákno [13]

Optický kabel je naprosto odlišným typem kabelu, než je koaxiální kabel či kroucená dvojlinka. Důvodem je to, že místo signálu ve formě elektrického napětí přes měděné vodiče používá optický kabel světelné impulsy (fotony), které přenáší binární signály generované síťovými prvky prostřednictvím skleněných nebo plastických vláken.

Vzhledem k tomu, že optický kabel k přenosu signálu používá světlo místo elektřiny, je odolný vůči elektromagnetickým vlivům stejně jako přeslechům a je méně vystaven útlumu (tendence oslabování signálu při cestě linkou) než měděné kabely. Některé optické kabely mohou překlenout vzdálenost až 120 kilometrů bez znatelného snížení úrovně signálu. Pokud tuto skutečnost porovnáme s kroucenou dvojlinkou, pro kterou se sníží úroveň signálu až na nečitelnost po 100 metrech, je optický kabel nejlepší volbou, je-li potřeba nainstalovat kabel, který má překlenout dlouhé vzdálenosti. Další výhodou je, že kabely s optickými vlákny jsou mnohem bezpečnější než měděné kabely, protože pokud se k němu někdo připojí, je ovlivněna normální komunikace přes tento propoj [4].

U optických vláken se definuje takzvaný Index lomu, který je vymezen jako podíl rychlosti světla ve vakuu k rychlosti světla v materiálu. Dle vzorce  $n = c/v$ .

<b>Médium</b>	<b>Index lomu n</b>
Vakuum	1.0000
Vzduch	1.0003
Voda	1.33
Plášť světlovodu	1.46
Jádru	1.48

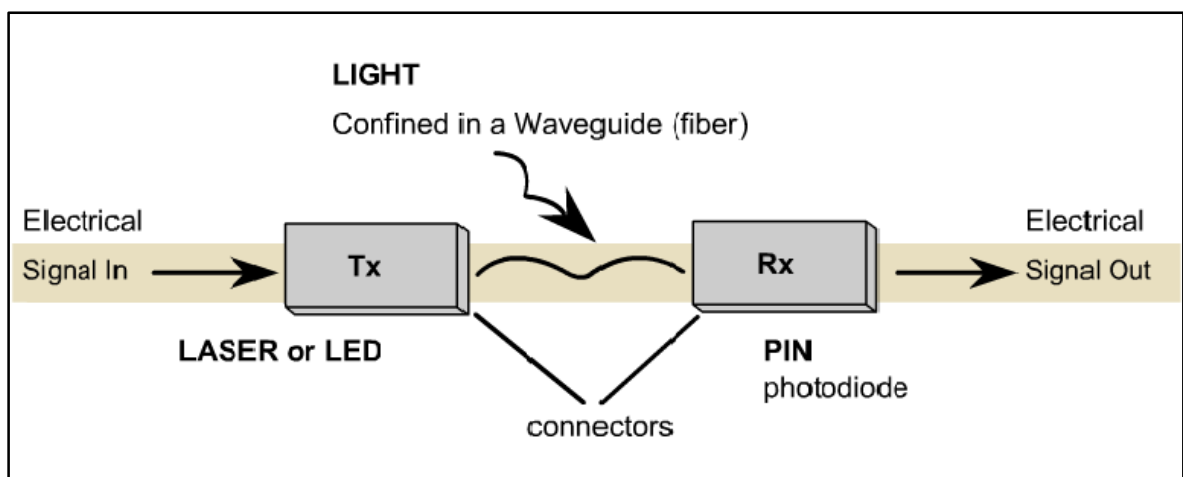
Obr. 12. Index lomu dle média [2]

Převod elektrického signálu na světlo zajišťuje **Vysílač (Tx)** a v opačné fázi tedy převod světla na elektrický signál zajišťuje **Příjímač (Rx)**.

**Vysílač (Tx)** – převádí elektrický signál na světelný a vysílá jej do vlákna. Při převodu elektrického signálu z metalického vedení je provedena změna kódování, které jej upraví na vhodný tvar pro přenos přes optické vlákno. Vysílač obsahuje zdroj světla v podobě laserové diody nebo *LED (Light Emitting Diode)* [2].

**Příjímač (Rx)** je složen z:

- **Fotodetektoru** – převádí optický signál na elektrické impulsy.
- **Zesilovače** – zesiluje signál a převádí jej do tvaru připraveného pro zpracování.
- **Procesoru** – reprodukuje původní signál = změna kódování [2].



Obr. 13. Převod signálu [2]

Optické kabely se liší ve svých rozměrech, složení a vlnových délkách světla. Je zde malý útlum, tudíž světelný signál podléhá malému odporu a informace je možné přenášet rychlostí až 50 Gb/s na jedné vlnové délce [2].

Optická vlákna se dělí:

- **Jednovidové (*single mode*)** – jádro je velmi tenké a světlo může postupovat jen jednou cestou. Zdrojem světla je laserová dioda a disponuje malým útlumem.
- **Mnohovidové (*multi mode*)** – jádro je širší a světelný paprsek má více prostoru a v jádru může probíhat, více cestami. Zdrojem světla je *LED*. Vidová disperze je veličina zkreslení signálu z důvodu rušení více vodiči, které optický kabel

obsahuje. Udává se v ns/km a představuje rozdíl mezi nejrychlejším a nejpomalejším světelným průběhem [2].

## **II. PRAKTICKÁ ČÁST**

## 2 IMPLEMENTACE SÍŤOVÝCH PRVKŮ

Tato část je věnována samotné implementaci síťových prvků Cisco do již fungující sítě nadnárodní společnosti. Před samotnou implementací byl nejprve proveden audit současného stavu a na základě zjištěných výsledků z prvotní revize byl vypracován návrh řešení Cisco síťových prvků a plán postupu jejich implementace.

Navazující částí bylo zhodnocení implementace, a to i s výčtem nákladů na ni použitých. Na závěr práce byl vypracován návrh postupu možného rozšíření do budoucna o realizaci záložních datových cest a možnosti správy všech prvků z jednoho místa.

Požadavkem vedení společnosti bylo vytvoření stabilní síťové infrastruktury, která bude postavena na stabilním *HW (hardware)* a bude plně kompatibilní se sítěmi, které jsou funkční v ostatních evropských pobočkách.

### 2.1 Audit současného stavu

Předmětem auditu byla analýza veškerých částí, které souvisí s požadavky vedení společnosti na implementaci nového síťového modelu. Důraz byl kladen především na správné vyhodnocení současného stavu sítě. Ve fázi doporučení bylo přihlédnuto k možnostem dalšího rozšiřování.

#### **Postup auditu byl stanoven dle zavedených procesů:**

- Sběr dat.
- Analýza dat.
- Vyhodnocení a doporučení..

#### **2.1.1 Sběr dat**

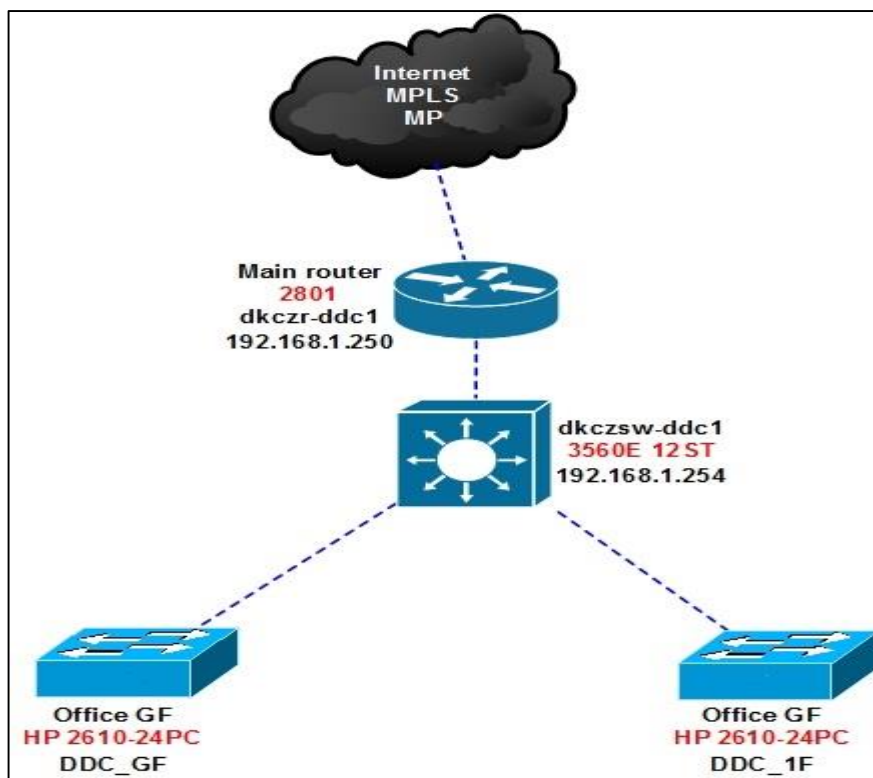
Sběr dat byl prováděn fyzickou kontrolou veškerých zařízení souvisejících s danou problematikou. Pro kompletní sběr dat byla nutná komunikace s *IT* oddělením v Belgii a získání nákrešů stávající sítě od společnosti, která prováděla kompletní výstavbu továrny.

- Typy hlavních síťových prvků a jejich počet viz tabulka (Tab.1).

Tab. 1. Typy síťových prvků a optické kabeláže

HW	počet	poznámka
<b>HP 2610</b>	4	Umístěny v kancelářích v přízemí a prvním podlaží propojení do serverovny metalickými rozvody
<b>Cisco 3560</b>	1	Umístěn v serverovně jako hlavní switch - je v majetku poskytovatele internetového připojení
<b>Cisco 2801</b>	1	Router zajišuje připojení k dodavateli VPN není možné zjistit jeho konfiguraci - je v majetku poskytovatele Internetového připojení
<b>optická kabeláž</b>	2	Rozvod multimode 8vl 50/125 propojení serverovny a dvěma racky umístěných v prostřední části haly
<b>optická kabeláž</b>	2	Rozvod singlemode 24vl 9/125 propojení serverovny a dvěma racky umístěných v nejzašší části haly
<b>optická kabeláž</b>	1	Rozvod singlemode 24vl 9/125 propojení hlavní serverovny a serverovny v cca 600 metru vzdálené budově

- Současné rozložení sítě - pro tuto část bylo použito grafického znázornění rozložení síťových prvků, obrázek (Obr. 14). Veškerá komunikace je staticky směrována z přepínače 3560 na IP směrovače Cisco 2801 192.168.1.250. Nastavení směrovače Cisco 2801 nebylo nutné analyzovat z důvodu změny dodavatele *MPLS VPN* linky.



Obr. 14. Stávající rozložení sítě

- Optická vizualizace prostor, ve kterých bude nutné připojit uživatele do podnikové sítě – již při výstavbě továrny proběhla instalace strukturované kabeláže specializovanou firmou. V obou hlavních kancelářích byly instalovány rozvaděče, které byly propojeny s hlavní serverovnou metalickou kabeláží. Druhá budova společnosti byla vybavena sekundární serverovnou, která byla s hlavní serverovnou propojena optickou kabeláží typu SM 24vl 9/125. Optická kabeláž byla svedena do optické vany, která je umístěna v rozvaděči.

V prostorách výrobní haly byly umístěny čtyři rozvaděče, do nichž ústila optická kabeláž, která byla v rozvaděči zakončena do optické vany. Dva rozvaděče uprostřed haly byly s hlavní serverovnou propojeny optickou kabeláží typu MM 8vl 50/125 a dva rozvaděče v nejbližší části haly byly s hlavní serverovnou propojeny optickou kabeláží typu SM 24vl 9/125.

Důvod, proč byly použity různé druhy optické kabeláže, byl ten, že realizace instalace optické kabeláže typu SM 24vl 9/125 byla prováděna o zhruba rok později než instalace optické kabeláže typu MM 8vl 50/125.

- Sběr požadavků centrály v Belgii pro VPN propojení sítě společnosti. V této části bylo nezbytné zjistit, jaké požadavky musí být splněny:
  - Povolení rozsahu *VLAN*.
  - Jaký provider bude zajišťovat *MPLS VPN* a zajistí propojení lokální podnikové sítě do jedné virtuální sítě.
  - *DNS* a *PROXY* server bude pod správou belgické strany

Bylo také nutné provést měření optické kabeláže, což bylo provedeno prostřednictvím firmy, která se na tyto aktivity specializuje. Veškerá měření byla provedena s kladným výsledkem, jehož část je uvedena na obrázku (Obr. 15).

Vana A - Umístena v hlavní serverovně (první shora)				Referenční Hodnota [dBm]				3,5			
Vana B - Umístena v budově OTC 902				<b>Hodnocení : Splněny všechny limity</b>							
Vana C - Umístena v hlavní serverovně (druhá odshora)											
Vana D - Umístena v hlavní serverovně (třetí odshora)											
Vana E - Umístena v nové budované hale (první od vchodu)											
Vana F - Umístena v nové budované hale (druhá od vchodu)											
<b>Delka trasy [m] 572</b>				<b>Delka trasy [m] 220</b>				<b>Delka trasy [m] 232</b>			
		Útlum				Útlum				Útlum	
viákno	A→B [dB]	B→A [dB]		viákno	C→F [dB]	F→C [dB]		viákno	D→E [dB]	E→D [dB]	
1	0,51	0,28		1	0,18	0,41		1	0,52	0,97	
2	0,45	0,47		2	0,4	0,51		2	0,46	0,51	
3	0,51	0,74		3	0,46	0,42		3	0,65	0,52	
4	0,43	0,50		4	0,93	1,05		4	0,84	0,46	
5	0,76	0,32		5	0,31	0,38		5	0,77	0,57	
6	0,60	0,07		6	0,38	0,47		6	0,82	0,73	
7	1,07	0,70		7	0,3	0,7		7	0,44	0,91	
8	0,79	0,50		8	0,59	0,36		8	0,27	0,76	
9	0,95	0,22		9	0,2	0,45		9	0,45	0,65	
10	0,76	0,27		10	0,38	0,1		10	0,43	0,53	
11	0,76	0,43		11	0,66	0,53		11	0,83	0,9	
12	0,54	0,58		12	0,16	0,56		12	0,24	0,73	
13	0,59	0,13		13	0,35	0,41		13	0,67	0,54	
14	1,33	0,80		14	0,52	0,46		14	0,24	0,85	
15	1,24	1,63		15	0,93	1,04		15	0,48	0,52	
16	0,65	0,26		16	0,97	0,36		16	0,74	0,56	
17	0,72	0,25		17	1,14	0,72		17	0,39	0,44	
18	0,35	0,68		18	0,55	0,3		18	1,02	0,83	
19	0,64	0,33		19	0,55	0,46		19	1	0,57	
20	0,85	0,63		20	0,63	0,62		20	0,53	0,4	
21	0,59	0,51		21	0,52	0,38		21	0,69	1,27	
22	0,51	0,12		22	0,67	0,62		22	0,5	0,77	
23	0,40	0,61		23	0,59	0,38		23	0,45	0,63	
24	0,85	0,30		24	0,38	0,61		24	0,55	0,49	

Obr. 15. Část z výsledku kontroly optické kabeláže

### 2.1.2 Analýza dat a vyhodnocení

Pro analýzu byly použity veškeré informace získané v první části auditu. Nejprve byl proveden rozbor stávajících síťových prvků, které firma vlastní, pak byl zjišťován stav datové struktury. Také bylo provedeno nastudování plánů budov a vedení kabeláže, které je nezbytné pro plánování dalších postupů.

Ze získaných dat bylo zřejmé, že zasíťování továrny a připojení druhé haly bylo na velmi dobré úrovni, nicméně nebylo kompletně dořešeno propojení prostřednictvím jednotlivých síťových prvků.

Doposud byly propojeny pouze dvě kanceláře, kde byly použity přepínače HP 2610 a ty byly propojeny s přepínačem Cisco 3560 v hlavní serverovně prostřednictvím metalické kabeláže CAT 5e. Tento přepínač je ve vlastnictví dodavatele stávající virtuální linky.

Jako zásadní problém byla vyhodnocena nekompletnost propojení veškerých destinací v rámci továrny. Dále byla spatřena potřeba v použití různých síťových prvků od různých výrobců, což by bylo problematické pro další rozšíření do budoucna. Nebyla zde řešena naprosto vůbec problematika TRUNK portů či možnost nastavení *port-security*, což

výrazně mohlo ovlivnit bezpečnost paketů procházejících skrze podnikovou síť. Také nebylo aplikováno rozdělení sítě do *VLAN*, což by v dohledné době znamenalo řešení problému s nedostatkem *IP* adres pro pracovní stanice či jiné síťové prvky.

Čili stávající řešení síťové infrastruktury bylo dostačující pouze v omezeném množství, tedy nedostačovalo nárokům středně velké nadnárodní společnosti, kde je důležitá dostupnost dat a jejich bezpečný tok.

Je však nutné podotknout, že společnost si problém uvědomovala a věděla, že stávající řešení bylo pouze dočasné. Proto z těchto důvodů byla v akčním plánu zahrnuta implementace kompletní infrastruktury, tedy celková obměna stávajících síťových prvků.

### 2.1.3 Doporučení

V souvislosti s předchozím bodem auditu bylo nezbytné navrhnout implementaci síťových prvků, které budou plně odpovídat novým trendům, budou kompatibilní s použitou strukturovanou kabeláží a vzájemně mezi sebou. Z důvodu potřeby propojení sítě podniku se sítí centrály v Belgii byla nezbytná komunikace s belgickou stranou.

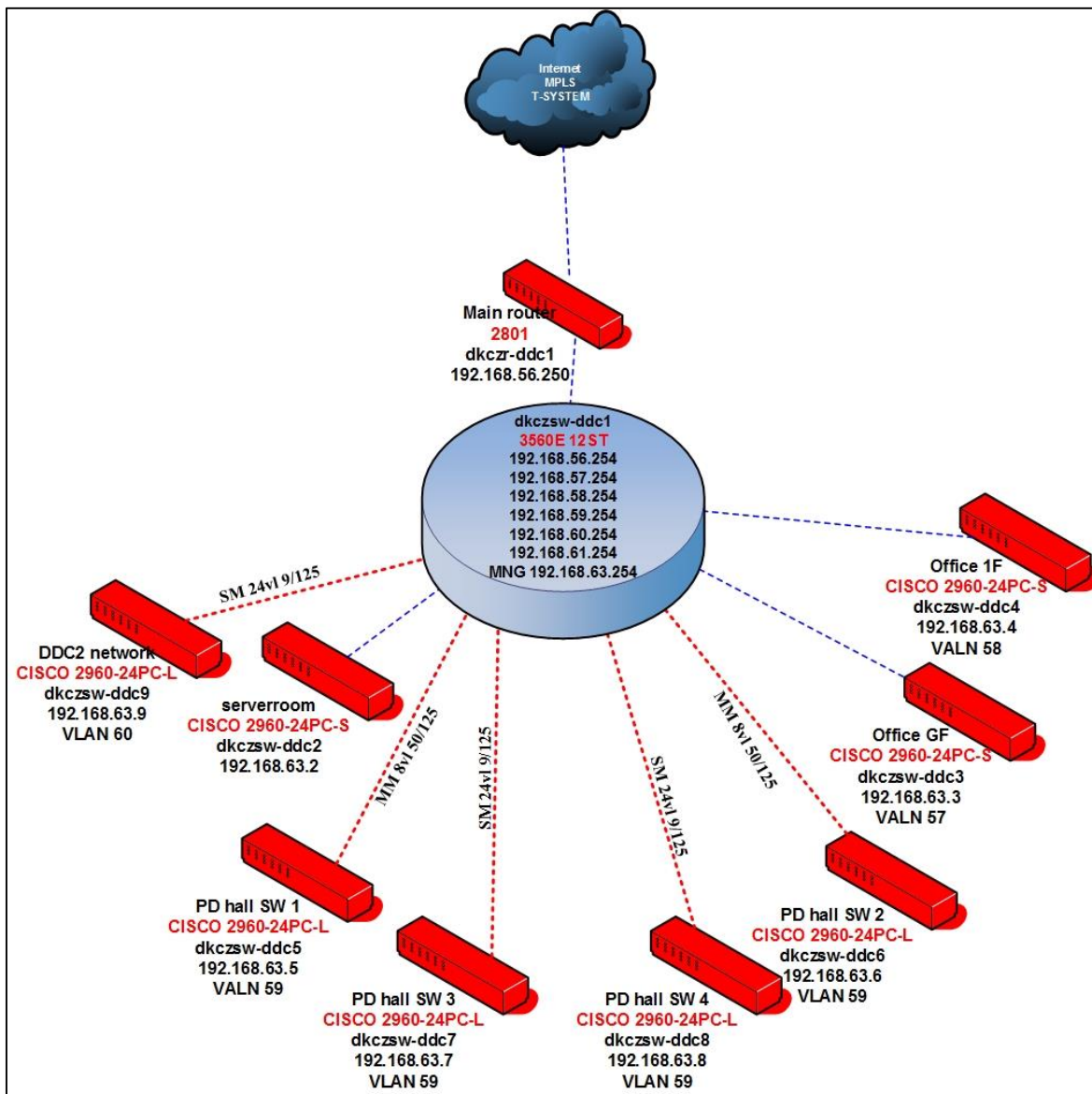
Bylo nutné připojení další haly, kde je umístěn rozvaděč, do nějž ústí optický kabel SM 24vl 9/125. V hlavní budově v části produkční haly jsou další čtyři rozvaděče, z nichž dva z nich jsou propojeny s hlavní serverovnou prostřednictvím optického kabelu typu MM 8vl 50/125 a poslední dva propojeny s hlavní serverovnou pomocí optického kabelu SM 24vl 9/125. Důvod použití odlišné kabeláže byl ten, že první dva rozvaděče byly se serverovnou propojeny v první fázi výstavby. Dva zbývající rozvaděče a druhá budova byly připojeny až později ve fázi rozšiřování továrny. Nicméně to nezpůsobilo problémy, pouze bylo nutné pro fázi implementace zvolit vhodné *HW* komponenty.

Závěrem tohoto bodu bylo potřeba zdůraznit, že bylo doporučeno vyřadit ze stávající sítě síťové prvky HP 2610 a nahradit je Cisco přepínači z důvodu vzájemné kompatibility, zejména použitím Cisco proprietárního protokolu *VPT*. Následně místa s vyústěním optické kabeláže, tedy 4 x výrobní hala a 1 x druhá budova, bylo také nezbytné nainstalovat Cisco přepínače a prostřednictvím stávající optické kabeláže propojit s hlavní serverovnou. Ostatní síťové prvky jako přepínač Cisco Catalyst 3560 a směrovač Cisco 2801 bylo navrženo vrátit dodavateli virtuální linky. Poté bylo naplánováno pořídit nový L3 přepínač s podporou pro optické kabely a vlastní Cisco router 2801.

Také bylo vyhodnoceno jako vhodné rozdělit jednotlivé lokality do virtuálních sítí pro jejich jednodušší správu, jak je popsáno níže. *VLAN* 56 – 60,61,63 byly vybrány dle požadavků z belgické centrály s tím, že rozčlenění bylo možné zvolit dle našeho uvážení. Jako nejlepší bylo vyhodnoceno rozdělení dle pracovišť s tím, že byl vzat v úvahu počet uživatelů.

Rozdělení virtuálních sítí:

- *VLAN* 56 – 192.168.56.0/24
  - Určena pro užití *IT* oddělení – použita na hlavním směrovači na portu Fa0/1, na který se posílá veškerá komunikace mimo interní síť z hlavního L3 přepínače.
- *VLAN* 57 – 192.168.57.0/24
  - Určena pro velkou kancelář v přízemí (*PC* a ostatní síťové prvky).
- *VLAN* 58 – 192.168.58.0/24
  - Určena pro velkou kancelář v prvním patře (*PC* a ostatní síťové prvky).
- *VLAN* 59 – 192.168.59.0/24
  - Určena pro výrobní halu.
- *VLAN* 60 – 192.168.60.0/24
  - Tato *VLAN* byla vyčleněna pro druhou výrobní halu.
- *VLAN* 61 – 192.168.61.0/24
  - Vyhrazena pro *IP* telefonii, která byla plánována jako budoucí náhrada stávající technologie.
- *VLAN* 63 – 192.168.63.0/24
  - Určena výhradně pro vzdálenou správu Cisco síťových prvků, z důvodu bezpečnosti nesmí být použita pro jiná síťová zařízení.



Obr. 16. Návrh sítě

V popisu chyběla virtuální síť 62. Pro tuto síť zatím nebyl oficiálně schválen účel jejího využití. Proto v tomto přehledu nebyla uvedena, ale s největší pravděpodobností by měla být použita pro účely výrobní linky, jež bude využívat systém *MES (Manufacturing Execution Systems)*.

### 3 IMPLEMENTACE

Tato kapitola se věnuje samotné implementaci navrženého řešení v předchozí kapitole, která byla popsána v poslední fázi auditu stávající sítě. Samozřejmě bylo nutné vše prodiskutovat s vedením společnosti a centrálou v Belgii. Návrh volby typů síťových prvků a jejich konfigurace musel projít procesem schválení.

Veškeré síťové prvky byly vybrány dle jejich vhodnosti pro danou činnost, ale také dle ceny, což se odvíjelo od rozpočtu, který firma vyčlenila pro tuto realizaci. Rozpočet činil 650 000 korun s tím, že jeho překročení nebude akceptováno.

V jednotlivých kapitolách byl popsán postup konfigurace, v každé z nich byly také uvedeny potřebné části z příkazů *show run* nebo *show vlan* nebo *show interfaces status*. Součástí přílohy této práce jsou výstupy ze souboru *config.text*

#### 3.1 Hlavní přepínač Cisco Catalyst 3750X

Jako hlavní přepínač byl od společnosti Cisco zvolen model Catalyst 3750X 12 Port GE SFP. Jedná se o přepínač řady L3, který pracuje i na třetí vrstvě *TCP/IP* modelu. Tedy pracuje jak s *MAC* adresami, tak i s *IP* adresami. Typ s 12 *SFP* porty byl zvolen z důvodu různého typu přenosového média použitého pro propojení jednotlivých bodů firemní sítě. Jednotlivé *SFP* porty jsou osazeny Gigabit *SFP* moduly pro optické kabely (typu jedno-vidové a více-vidové osazené) *LC* konektory a 1000BASE-T moduly pro *UTP* kabely osazené konektorem *RJ-45*.

Tab. 2. Osazení modulů na jednotlivých portech přepínače

PORT	1	2	3	4	5	6
<b>SFP modul</b>	GLC-SX-MM	GLC-SX-MM	GLC-SX-MM	GLC-LH-SM	GLC-LH-SM	GLC-LH-SM
<b>konektor</b>	LC	LC	LC	LC	LC	LC
PORT	7	8	9	10	11	12
<b>SFP modul</b>	GLC-T	GLC-T	GLC-T	GLC-T	GLC-T	GLC-T
<b>konektor</b>	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45

Tento síťový prvek je umístěn v serverovně, kde ústí jak optické kabely, tak i metalické kabely z hlavních bodů v továrně a jednotlivých kancelářích.

### 3.1.1 Konfigurace zabezpečení přepínače Catalyst 3750X

Konfigurace hlavního přepínače byla rozdělena do jednotlivých částí a byla prováděna za pomoci Cisco konzolového kabelu osazeným konektorem RJ-45 a RS323.



Obr. 17. Cisco konzolový kabel [14]

Pro konfiguraci všech síťových prvků byl zvolen software s názvem PUTTY, který umožňuje spojení s prvkem prostřednictvím sériové linky, *TELNET* (*Telecommunication Network*) či *SSH*. Nicméně první konfigurace musela být vždy provedena prostřednictvím sériové linky. Síťový prvek při prvním spuštění byl v továrním nastavení a bylo tedy nutné ho nejdříve nakonfigurovat, aby jeho správa mohla být prováděna prostřednictvím *TELNET* či *SSH*.

Konfigurace zabezpečení hlavního přepínače bylo nastavení hesla do privilegovaného módu přepínače.

#### **Příkaz:**

```
Switch#configure terminal  
Switch(config)#enable secret heslo
```

Výše uvedeným příkazem bylo vytvořeno heslo „heslo“, které bylo uloženo prostřednictvím hashe MD5. Tento příkaz bylo možné provést v konfiguračním módu. Nakonfigurovaný způsob zabezpečení byl základní, proto bylo vhodné ještě provést zabezpečení přístupu přímo přes konzoli.

**Příkazy:**

```
Switch#conf t
Switch(config)#line console 0
Switch(config-line)#password heslo
Switch(config-line)#login
```

Nicméně při této konfiguraci nebylo zašifrováno heslo a bylo nutné spustit službu pro kryptování hesel pomocí příkazu `service password-encryption` v konfiguračním módu přepínače.

```
Switch(config)# service password-encryption
```

Pro vzdálenou konfiguraci prostřednictvím protokolu *TELNET* bylo nutné nastavit *VTY* (*Virtual Terminal*). Nastavení bylo podobné jako konfigurace konzole, pouze bylo nutné přepnutí do konfigurace *VTY*.

```
Switch#conf t
Switch(config)#line vty 0 15
Switch(config-line)#password heslo
Switch(config-line)#login
```

Příkazem `show run` byla prověřena provedená nastavení a pokud bylo vše funkční, tak bylo nutné spuštěnou konfiguraci nakopírovat do startup konfigurace příkazem `copy running-config startup-config`.

Samozřejmě bylo možné nastavení více lokálních uživatelů nebo napojení na *RADIUS* (*Remote Authentication Dial In User Service*) server pro ověřování uživatelů, ale vzhledem k tomu, že správu všech síťových prvků bude provádět pouze jeden administrátor, tak tato konfigurace nyní nebyla nutná.

**3.1.2 Nastavení NTP, logování a hostname**

Pro správné nastavení data a času hlavního přepínače bylo nejvhodnější zvolit synchronizaci s *NTP* server. V rámci sítě společnosti byl *NTP* server, jehož hlavní funkce byla *AD* (*Active Directory*) controller, s nímž se synchronizovaly veškeré počítače ve firmě. Správný datum a čas byl velmi důležitý pro správnou časovou osu při kontrole logů přepínače.

Nejprve bylo třeba zvolit časovou zónu a následně nastavení *IP NTP* serveru. Níže uvedené příkazy bylo nutné provést v konfiguračním módu přepínače.

```
Switch(config)#clock timezone GMT 1
Switch(config)#ntp server 192.168.57.198
```

Také byla možná manuální konfigurace data a času přepínače pomocí příkazu `clock set`. Což by ale mohlo způsobit problém, pokud by došlo k restartu přepínače, tak by se nastavení data a času nemělo, kde synchronizovat a tyto hodnoty by tedy nebyly aktuální.

Aby se logy a debugy zobrazovaly s aktuálním datem a časem, bylo vhodné změnit výchozí nastavení těmito příkazy:

```
Switch(config)#service timestamps debug datetime msec
Switch(config)#service timestamps log datetime msec
```

Pokud by se toto nastavení neprovedlo, tak by logované informace měly časovou hodnotu, která byla generována od startu přepínače.

V tuto chvíli bylo již vhodné si změnit *hostname* přepínače na jméno, jež je uvedeno v návrhu implementace. Bylo to nezbytné, aby administrátor měl přehled, který přepínač konfiguruje.

```
Switch(config)#hostname dkczsw-ddc1
dkczsw-ddc1(config)#
```

Nyní bylo zřejmé, že administrátor konfiguruje přepínač `ddc1`.

### 3.1.3 Konfigurace VLAN a protokolu VTP

Způsob rozdělení sítě do *VLAN* bylo popsáno v části Doporučení. Bylo zde uvedeno určité logické rozdělení sítě pro její jednodušší správu. Vytváření *VLAN* bylo možné realizovat pouze v konfiguračním módu přepínače. Následujícími příkazy byly vytvořeny jednotlivé *VLAN*y na hlavním přepínači. Na obrázku (Obr. 18) byl uveden výpis dostupných *VLAN* pomocí příkazu `show vlan brief`:

```
dkczsw-ddc1#conf t
dkczsw-ddc1(config)#vlan 56
dkczsw-ddc1(config-vlan)#vlan 57
```

```
dkczsw-ddc1 (config-vlan) #vlan 58
dkczsw-ddc1 (config-vlan) #vlan 59
dkczsw-ddc1 (config-vlan) #vlan 60
dkczsw-ddc1 (config-vlan) #vlan 61
dkczsw-ddc1 (config-vlan) #vlan 63
dkczsw-ddc1 (config-vlan) #exit
dkczsw-ddc1 (config) #exit
dkczsw-ddc1#wr
dkczsw-ddc1#show vlan brief
```

```
dkczsw-ddc1>show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
56	VLAN0056	active	
57	VLAN0057	active	
58	VLAN0058	active	
59	VLAN0059	active	
60	VLAN0060	active	
61	VLAN0061	active	
63	VLAN0063	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Obr. 18. Výpis VLAN

Příkaz `wr` je zkrácená verze příkazu `copy running-config startup-config` pro uložení konfigurace do *NRAM* (*Non Volatile Random Access Memory*) paměti přepínače.

Vzhledem k tomu, že se jednalo o hlavní L3 přepínač, který by měl zajišťovat přepínání mezi *VLAN*ami, bylo nutné pro každou *VLAN*u nastavit *IP* adresu a masku. Tuto *IP* adresu by měly mít nastaveny koncové síťové prvky jako výchozí bránu pro přechod z jedné *VLAN*y do druhé. Následující příkazy sloužily pro vizualizaci nastavení *IP* adres pro

jednotlivé *VLANy* a závěrem výpis příkazem `show interface vlan` informací o nastavení nad danou *VLANou*.

```
dkczsw-ddc1(config)#interface vlan 56
dkczsw-ddc1(config-if)#ip address 192.168.56.254
255.255.255.0
dkczsw-ddc1(config-if)#interface vlan 57
dkczsw-ddc1(config-if)#ip address 192.168.57.254
255.255.255.0
dkczsw-ddc1(config-if)#interface vlan 58
dkczsw-ddc1(config-if)#ip address 192.168.58.254
255.255.255.0
dkczsw-ddc1(config-if)#interface vlan 59
dkczsw-ddc1(config-if)#ip address 192.168.59.254
255.255.255.0
dkczsw-ddc1(config-if)#interface vlan 60
dkczsw-ddc1(config-if)#ip address 192.168.60.254
255.255.255.0
dkczsw-ddc1(config-if)#interface vlan 61
dkczsw-ddc1(config-if)#ip address 192.168.61.254
255.255.255.0
dkczsw-ddc1(config-if)#interface vlan 63
dkczsw-ddc1(config-if)#ip address 192.168.63.254
255.255.255.0
```

```
dkczsw-ddc1#show interfaces vlan 56
Vlan56 is up, line protocol is up
  Hardware is CPU Interface, address is 00d0.bc54.b94a (bia 00d0.bc54.b94a)
  Internet address is 192.168.56.254/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1682 packets input, 530955 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    563859 packets output, 0 bytes, 0 underruns
    0 output errors, 23 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Obr. 19. Nastavení IP na VLAN 56

Všechny tyto VLANy by měly být posléze vytvářeny i na ostatních přepínačích, a to automaticky po konfiguraci VTP protokolu. Tento proprietární Cisco protokol bylo ovšem nutné nejprve nakonfigurovat na přepínači, který byl v síti jako VTP server.

```
dkczsw-ddc1(config)#vtp domain daikin.co.jp
Changing VTP domain name from NULL to daikin.co.jp
dkczsw-ddc1(config)#vtp mode server
Device mode already VTP SERVER.
dkczsw-ddc1(config)#vtp password ddcz
Setting device VLAN database password to ddcz
```

Výše uvedenými příkazy byla vytvořena VTP doména, nastavení přepínače do módu server a heslo do VTP domény.

Nastavení bylo možné ověřit příkazem `show vtp status`, jak je uvedeno na obrázku (Obr. 19).

```
dkczsw-ddc1#show vtp status
VTP Version           : 2
Configuration Revision : 1
Maximum VLANs supported locally : 255
Number of existing VLANs : 13
VTP Operating Mode    : Server
VTP Domain Name       : daikin.co.jp
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation  : Disabled
MDS digest            : 0x1B 0x84 0xC1 0xB4 0x42 0x77 0xD5 0xDD
```

Obr. 20. Nastavení VTP protokolu

Zde bylo nutné upozornit na číslo revize konfigurace. Tato hodnota se zvyšovala o jedničku při každém přidání či odebrání virtuální sítě. Do VTP domény nesměl být připojen síťový prvek s vyšším číslem konfigurace. Mohlo by to způsobit přepsání VLAN na všech prvcích v rámci dané VTP domény.

### 3.1.4 Konfigurace portů

Po konfiguraci VLAN bylo možné nastavit porty a k jednotlivým portům přiřadit virtuální síť. Aby bylo možné port přiřadit do více virtuálních sítí, bylo nutné jej nastavit jako trunkový. Také bylo potřebné nastavit typ zapouzdření v síti VLAN. Nejvíce bylo používáno standardní *dot1q*, tedy zapouzdření dle IEEE 802.1q. Typ zapouzdření *dot1q* byl aplikován také z důvodu, že řada přepínačů 2960, která byla užita v další části konfigurace této práce, jiný typ zapouzdření nepodporovala [1].

Vzhledem k tomu, že všechny porty byly nakonfigurovány stejně (měly stejné zapouzdření a stejný počet virtuálních sítí), byla konfigurace provedena pro všechny porty najednou.

```
dkczsw-ddc1#configure terminal
dkczsw-ddc1(config)#interface range GigabitEthernet 0/1-12
dkczsw-ddc1(config-if-range)#switchport trunk encapsulation
dot1q
dkczsw-ddc1(config-if-range)#switchport mode trunk
dkczsw-ddc1(config-if-range)#switchport trunk allowed vlan
56-61,63
```

```
dkczsw-ddc1#sh interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gi0/1	on	802.1q	trunking	1
Gi0/2	on	802.1q	trunking	1
Gi0/3	on	802.1q	trunking	1
Gi0/4	on	802.1q	trunking	1
Gi0/5	on	802.1q	trunking	1
Gi0/6	on	802.1q	trunking	1
Gi0/7	on	802.1q	trunking	1
Gi0/8	on	802.1q	trunking	1
Gi0/9	on	802.1q	trunking	1
Gi0/10	on	802.1q	trunking	1
Gi0/11	on	802.1q	trunking	1
Gi0/12	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Gi0/1	56-61,63
Gi0/2	56-61,63
Gi0/3	56-61,63
Gi0/4	56-61,63
Gi0/5	56-61,63
Gi0/6	56-61,63
Gi0/7	56-61,63
Gi0/8	56-61,63
Gi0/9	56-61,63
Gi0/10	56-61,63
Gi0/11	56-61,63
Gi0/12	56-61,63

Obr. 21. Trunk porty

Na obrázku (Obr. 21) byl zobrazen výpis všech aktivních trunk portů. Zde byla důležitá informace o zapouzdření, a o tom jaké virtuální sítě byly přiřazeny k jednotlivým portům.

### 3.1.5 Nastavení směrování

L3 síťové prvky jsou vhodné, protože umožňují nastavení základního směrování. Tato skutečnost byla v daný okamžik velmi důležitá, a to z důvodu přenosu síťového provozu mezi jednotlivými virtuálními sítěmi. Nastavení bylo provedeno v konfiguračním módu přepínače pomocí jednoho příkazu.

```
dkczsw-ddc1(config)#ip routing
```

```
dkczsw-ddc1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.56.0/24 is directly connected, Vlan56
C    192.168.57.0/24 is directly connected, Vlan57
C    192.168.58.0/24 is directly connected, Vlan58
C    192.168.59.0/24 is directly connected, Vlan59
C    192.168.60.0/24 is directly connected, Vlan60
C    192.168.61.0/24 is directly connected, Vlan61
C    192.168.63.0/24 is directly connected, Vlan63
```

Obr. 22. Přepínání VLAN

Na obrázku (Obr. 22) byl zobrazen výpis příkazu `show ip route`. Zde bylo evidentní, že bylo vytvořeno směrování mezi virtuálními sítěmi. Jenomže pokud by do přepínače přišel paket s jinou informací, než je v směrovací tabulce, tak by byl v ten okamžik zahozen. Například když by byl zadán dotaz na nějakou `www` stránku, která byla mimo naši síť. Proto bylo nutné vše ostatní, co patří mimo naši síť, přeposlat na další síťový prvek. Tento prvek byl většinou směrovač a ten zajistil další přenos paketu. *IP* adresa našeho směrovače byla `192.168.56.250` a bylo nutné na tuto adresu zaslat ostatní pakety.

Další zápis do směrovací tabulky směrovače byl následující:

```
dkczsw-ddc1(config)#ip route 0.0.0.0 0.0.0.0 192.168.56.250
```

Tento příkaz zabezpečil, aby vše, co nepatří do námi stanovených virtuálních sítí, bylo posláno na síťový prvek `192.168.56.250`. Ve směrovací tabulce tím přibyl další záznam se statickým směrováním tak, jak je uvedeno na obrázku (obr. 23).

```
C    192.168.63.0/24 is directly connected, Vlan63
C    192.168.61.0/24 is directly connected, Vlan61
C    192.168.60.0/24 is directly connected, Vlan60
C    192.168.59.0/24 is directly connected, Vlan59
C    192.168.58.0/24 is directly connected, Vlan58
C    192.168.57.0/24 is directly connected, Vlan57
C    192.168.56.0/24 is directly connected, Vlan56
S*  0.0.0.0/0 [1/0] via 192.168.56.250
```

Obr. 23. Statické směrování

Statické směrování bylo možné nastavit až při po konfiguraci přepínače. Ale pokud by byla *IP* adresa pevně stanovena, nebyl by problém jej nastavit již ve fázi implementace.

### 3.1.6 Konfigurace *DHCP* protokolu

Protokol *DHCP* byl implementován z důvodu usnadnění práce administrátora sítě, kdy u pracovních stanic uživatelů nebylo nutné pracně nastavovat *IP* adresu, masku, bránu a *DNS* (*Domain Name System*). Bylo možné *DHCP* server nastavit na některém ze serveru na platformě Windows či Linux, ale co se týče operačního systému Windows, vše je vázáno vždy na licence. Spuštění *DHCP* serveru ve Windows by bylo velmi finančně nákladné.

Při použití L3 přepínače bylo vhodné spuštění *DHCP* služby přímo na daném přepínači. Pomocí následujících příkazů byl vytvořen *DHCP* pool a provedeno další nastavení [15]:

- Přidělení brány.
- Nastavení *IP* adres, které se nebudou přidělovat jednotlivým klientům.
- Identifikace *DNS* serverů, které se budou přidělovat.
- Nastavení maximální délky zapůjčení *IP* adresy.

```
dkczsw-ddc1(config)#ip dhcp pool vlan57
```

```
dkczsw-ddc1(dhcp-config)#network 192.168.57.0 255.255.255.0
```

```
dkczsw-ddc1(dhcp-config)#default-router 192.168.57.254
```

```
dkczsw-ddc1(dhcp-config)#dns-server 192.168.204.78
```

```
192.168.204.79
```

```
dkczsw-ddc1(dhcp-config)#lease 2
```

```
dkczsw-ddc1(config)#ip dhcp pool vlan58
```

```
dkczsw-ddc1(dhcp-config)#network 192.168.58.0 255.255.255.0
```

```
dkczsw-ddc1(dhcp-config)#default-router 192.168.58.254
```

```
dkczsw-ddc1(dhcp-config)#dns-server 192.168.204.78
```

```
192.168.204.79
```

```
dkczsw-ddc1(dhcp-config)#lease 2
```

```
dkczsw-ddc1(config)#ip dhcp pool vlan59
```

```
dkczsw-ddc1(dhcp-config)#network 192.168.59.0 255.255.255.0
```

```
dkczsw-ddc1 (dhcp-config) #default-router 192.168.59.254
dkczsw-ddc1 (dhcp-config) #dns-server 192.168.204.78
192.168.204.79
dkczsw-ddc1 (dhcp-config) #lease 2
dkczsw-ddc1 (config) #ip dhcp pool vlan60
dkczsw-ddc1 (dhcp-config) #network 192.168.60.0 255.255.255.0
dkczsw-ddc1 (dhcp-config) #default-router 192.168.60.254
dkczsw-ddc1 (dhcp-config) #dns-server 192.168.204.78
192.168.204.79
dkczsw-ddc1 (dhcp-config) #lease 2
dkczsw-ddc1 (dhcp-config) #exit
dkczsw-ddc1 (config) #ip dhcp excluded-address 192.168.57.1
192.168.57.50
dkczsw-ddc1 (config) #ip dhcp excluded-address 192.168.58.1
192.168.58.50
dkczsw-ddc1 (config) #ip dhcp excluded-address 192.168.59.1
192.168.59.50
dkczsw-ddc1 (config) #ip dhcp excluded-address 192.168.60.1
192.168.60.50
```

**Nastavení DHCP po spuštění příkazu `show run` vypadalo následovně:**

```
ip dhcp excluded-address 192.168.57.1 192.168.57.50
ip dhcp excluded-address 192.168.58.1 192.168.58.50
ip dhcp excluded-address 192.168.59.1 192.168.59.50
ip dhcp excluded-address 192.168.60.1 192.168.60.50
!
ip dhcp pool vlan57
    network 192.168.57.0 255.255.255.0
    default-router 192.168.57.254
```

```
dns-server 192.168.204.78 192.168.204.79
lease 2
ip dhcp pool vlan58
network 192.168.58.0 255.255.255.0
default-router 192.168.58.254
dns-server 192.168.204.78 192.168.204.79
lease 2
ip dhcp pool vlan59
network 192.168.59.0 255.255.255.0
default-router 192.168.59.254
dns-server 192.168.204.78 192.168.204.79
lease 2
ip dhcp pool vlan60
network 192.168.60.0 255.255.255.0
default-router 192.168.60.254
dns-server 192.168.204.78 192.168.204.79
lease 2
```

Nastavení nebylo provedeno u virtuálních sítí 56, 61 a 63:

- *VLAN 56* byla určena pro páteřní směrovače, kde *DHCP* služba nebyla vhodná a standardně se nevyžívala.
- *VLAN 61* byla určena pro telefonní ústřednu, kde bylo nezbytné definovat přesně *IP* telekomunikačního zařízení.
- *VLAN 63* byla používán pouze Cisco síťovými prvky, kde dynamické přidělování *IP* adres nebylo využitelné pro jejich správu. Bylo nutné, aby každý prvek měl nastavenou statickou *IP* adresu pro jeho snadnější správu a identifikaci v rámci sítě.

Škála *IP* adres, které by nebyly přidělovány v rozsahu xxx.xxx.xxx.1 – xxx.xxx.xxx.50, byla zvolena záměrně. V určitých situacích nebylo u některých síťových zařízení vhodné využívat dynamické přidělování, a to z důvodu nutnosti komunikovat v síti stále stejnou *IP*

adresou. Těmito prvky v našem případě byly: servery, tiskárny, čtecí zařízení na výrobních linkách a některé pracovní stanice.

## 3.2 Konfigurace přepínačů Cisco Catalyst 2960s

Tato část byla věnována konfiguraci ostatních přepínačů, které byly umístěny v koncových bodech kanceláří a výrobní haly. Jednalo se o osm přepínačů Catalyst 2960s, jejichž konfigurace byla téměř identická. Za odlišnost bylo považováno například přiřazení jednotlivých portů do virtuálních sítí. Důvodem bylo přidělení určité oblasti na jednotlivé virtuální síť.

Z důvodu podobné konfigurace jako u Catalyst 3750 zde byly popsány pouze části, které byly odlišné. Například zabezpečení, *NTP* či logování.

### 3.2.1 Konfigurace VTP

Hlavní přepínač Catalyst 3750 byl z hlediska protokolu *VTP* nakonfigurován jako server. To znamená, že ostatní přepínače, u kterých bylo předpokládáno využití *VTP*, bylo nutné nakonfigurovat jako klienta a přiřadit je do stejné *VTP* domény se stejným heslem.

Celá konfigurace byla velmi podobná jen s rozdílem části `vtp mode`. Zbývajících osm přepínačů Catalyst 2960 bylo nastaveno do režimu klient. Na daných přepínačích se nesměly vytvářet žádné virtuální sítě, aby nenastala situace, ve které by dané přepínače měly vyšší číslo revize. Mohlo by totiž dojít k přepsání virtuálních sítí na serveru. To by bylo možné považovat jako nevýhodu protokolu *VTP*. Nicméně byl tento protokol hodnocen jako velmi užitečný a schopný usnadnit administrátorům práci.

Konfigurace protokolu *VTP* je prováděna opět v konfiguračním módu přepínače:

```
Switch#conf t
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp domain daikin.co.jp
Changing VTP domain name from NULL to daikin.co.jp
Switch(config)#vtp password ddcz
Setting device VLAN database password to ddcz
```

Aby *VTP* protokol byl funkční, bylo nezbytné porty prostřednictvím, kterých jsou přepínače propojeny, nastavit jako trunk. Pouze v modu trunk bylo možné přenést přes port více jak jednu virtuální síť. Z obrázku (Obr. 24) je zřejmé, že i když byl *VTP* protokol správně nastaven, tak seznam virtuálních sítí na přepínači stále zůstal ve výchozím stavu [17].

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Gi0/1, Gi0/2, Gi0/3, Gi0/4 Gi0/5, Gi0/6, Gi0/7, Gi0/8 Gi0/9, Gi0/10, Gi0/11, Gi0/12 Gi0/13, Gi0/14, Gi0/15, Gi0/16 Gi0/17, Gi0/18, Gi0/19, Gi0/20 Gi0/21, Gi0/22, Gi0/23, Gi0/24 Gi1/1, Gi1/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Obr. 24. *VTP bez Trunk portu*

V tuto chvíli byl *VTP* protokol nefunkční a bylo tedy třeba nakonfigurovat port prostřednictvím, kterého by přepínač byl propojen s hlavním přepínačem Catalyst 3750.

```
Switch(config)#interface Gi 0/1
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/2, Gi0/3, Gi0/4, Gi0/5 Gi0/6, Gi0/7, Gi0/8, Gi0/9 Gi0/10, Gi0/11, Gi0/12, Gi0/13 Gi0/14, Gi0/15, Gi0/16, Gi0/17 Gi0/18, Gi0/19, Gi0/20, Gi0/21 Gi0/22, Gi0/23, Gi0/24, Gi1/1 Gi1/2
56	VLAN0056	active	
57	VLAN0057	active	
58	VLAN0058	active	
59	VLAN0059	active	
60	VLAN0060	active	
61	VLAN0061	active	
63	VLAN0063	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Obr. 25. Funkční VTP

Na obrázku (Obr. 25) je patrné, že po nastavení daného portu jako trunk došlo k synchronizaci nastavení virtuálních sítí za pomoci protokolu *VTP*. Nastavení trunkového portu bylo možné ověřit příkazem `show interfaces trunk`, jehož výpis byl uveden v obrázku (Obr. 26).

```
Switch#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gi0/1	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Gi0/1	1-1005			
Port	Vlans allowed and active in management domain			
Gi0/1	1,56,57,58,59,60,61,63			
Port	Vlans in spanning tree forwarding state and not pruned			
Gi0/1	1,56,57,58,59,60,61,63			

Obr. 26. VLANy na trunkovém portu

Trunk port sdílel tedy potřebné virtuální sítě dle nastavení na hlavním přepínači Catalyst 3750.

### 3.2.2 Konfigurace portů

Jednotlivé porty daného přepínače musely být přiřazeny dle využití do dané virtuální sítě. Vzhledem k tomu, že každý přepínač by měl mít rozdílně přiřazené virtuální sítě k jednotlivým portům, byl proveden příklad nastavení na přepínači dkcsw-ddc2. Ostatní přepínače a jejich virtuální sítě přiřazené k jednotlivým portům byly uvedeny v tabulce (Tab. 3).

```
dkcsw-ddc2(config)#interface range Gi0/2 - 22
dkcsw-ddc2(config-if-range)#switchport mode access
dkcsw-ddc2(config-if-range)#switchport access vlan 57
dkcsw-ddc2(config)#interface range Gi0/23 - 24
dkcsw-ddc2(config-if-range)#switchport mode access
dkcsw-ddc2(config-if-range)#switchport access vlan 61
```

Porty číslo 2 až 22 byly přiřazeny k virtuální síti z důvodu umístění tohoto přepínače v hlavní serverovně, který by měl sloužit pro připojení serverů do podnikové sítě. Následně porty 23 až 24 byly primárně připraveny pro *VOIP (Voice over Internet Protocol)* telefonii a případné testování *VOIP* telefonů

Port 1 byl již nastaven jako trunk, aby bylo možné přenášet víc virtuálních sítí mezi daným a hlavním přepínačem Catalyst 3750.

Tab. 3. Ostatní přepínače přiřazující porty do VLAN

	Trunk port	Port VLAN 57	Port VLAN 58	Port VLAN 59	Port VLAN 60	Port VLAN 61
dkcsw-ddc2	1	2 - 22				23 - 24
dkcsw-ddc3	1	2 - 20	21			22 - 24
dkcsw-ddc4	1		2 - 21			22 - 24
dkcsw-ddc5	25 SFP			1 - 21		22 - 24
dkcsw-ddc6	25 SFP			1 - 21		22 - 24
dkcsw-ddc7	25 SFP			1 - 21		22 - 24
dkcsw-ddc8	25 SFP			1 - 21		22 - 24
dkcsw-ddc9	25 SFP		21		1 - 20	22 - 24

V tabulce (Tab. 3) bylo uvedeno rozdělení portů a k nim přiřazených virtuálních sítí. Do virtuálních sítí 56 a 63 nebyly přiřazeny žádné porty. Důvodem bylo to, že tyto virtuální sítě byly určeny pouze pro administraci a komunikaci se směrovačem.

### 3.2.3 Vzdálená správa

Veškeré přepínače je nutné vzdáleně spravovat prostřednictvím služby *TELNET* nebo *SSH*. Aby se administrátor těchto přepínačů nemusel stále fyzicky připojovat prostřednictvím konzolového portu, je nutné nastavit nad jednu z virtuálních sítí *IP* adresu. Prostřednictvím této *IP* adresy pak bude možné provádět vzdálenou administraci.

```
dkczsw-ddc2(config)#interface vlan 63
dkczsw-ddc2(config-if)#description >>MANAGEMENT<<
dkczsw-ddc2(config-if)#ip address 192.168.63.2 255.255.255.0
dkczsw-ddc2(config-if)#exit
dkczsw-ddc2(config)#ip default-gateway 192.168.63.254
```

Popis výše uvedených příkazů:

- `interface vlan 63` : přechod do konfiguračního módu dané virtuální sítě,
- `description >>MANAGEMENT<<` : popis dané virtuální sítě,
- `ip address` : nastavení *IP* adresy pro tuto virtuální síť prostřednictvím, které je možné tento přepínač spravovat za pomoci služby *TELNET*,
- `ip default-gateway` : nastavení *IP* adresy brány, na kterou měla být zasílána komunikace z jiných virtuálních sítí.

```

dkczsw-ddc2#show interfaces vlan 63
Vlan63 is up, line protocol is up
  Hardware is EtherSVI, address is 04da.d2d9.b541 (bia 04da.d2d9.b541)
  Description: >>MANAGEMENT<<
  Internet address is 192.168.63.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 3 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    194967 packets input, 14883085 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    126970 packets output, 11326029 bytes, 0 underruns
    0 output errors, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out

```

*Obr. 27. Informace o virtuální síti 63*

Na obrázku (Obr. 27) byl zobrazen výpis příkazu `show interface` virtuální sítě 63. Byly zde podrobné informace dané virtuální sítě a bylo zde zřejmé předchozí nastavení. Také bylo možné vyčíst informace o přijatých a odeslaných paketech.

IP adresy virtuální sítě 63 na ostatních přepínačích byly chronologicky přiděleny dle jména daného přepínače, jak bylo uvedeno v tabulce (Tab. 4).

*Tab. 4. IP daných přepínačů*

	IP VLAN 63
<b>dkczsw-ddc2</b>	192.168.63.2 /24
<b>dkczsw-ddc3</b>	192.168.63.3 /24
<b>dkczsw-ddc4</b>	192.168.63.4 /24
<b>dkczsw-ddc5</b>	192.168.63.5 /24
<b>dkczsw-ddc6</b>	192.168.63.6 /24
<b>dkczsw-ddc7</b>	192.168.63.7 /24
<b>dkczsw-ddc8</b>	192.168.63.8 /24
<b>dkczsw-ddc9</b>	192.168.63.9 /24

### 3.3 Konfigurace směrovače Cisco 2801

Konfigurace směrovače Cisco 2801 byla provedena rozdělením do tří fází. Nejprve bylo provedeno nastavení zabezpečení a *NTP*, následně byla realizována konfigurace portů a v neposlední řadě nastavení a otestování směrovacího protokolu *OSPF*.



Obr. 28. Cisco 2801

Na obrázku (Obr. 28) bylo vyobrazeno autentické znázornění daného směrovače, kde jsou použity dva gigabitové porty RJ-45. Ostatní rozšiřující sloty nebyly osazeny žádným rozhraním.

#### 3.3.1 Zabezpečení, *NTP* a změna názvu směrovače

Konfigurace výše uvedených bodů byla shodná s konfigurací přepínače Catalyst 3750, proto je níže uveden pouze postup konfigurace. Pojmenování tohoto směrovače bylo zvoleno dle předchozí syntaxe.

```
Router(config)#hostname dkczr-ddc1
dkczr-ddc1(config)#enable secret heslo
dkczr-ddc1(config)#line console 0
dkczr-ddc1(config-line)#password heslo
dkczr-ddc1(config-line)#login
dkczr-ddc1(config-line)#line vty 0 4
dkczr-ddc1(config-line)#password heslo
dkczr-ddc1(config-line)#login
dkczr-ddc1(config-line)#exit
```

```
dkcزر-ddc1 (config) # service password-encryption
dkcزر-ddc1 (config) # clock timezone GMT 1
dkcزر-ddc1 (config) # ntp server 192.168.57.198
dkcزر-ddc1 (config) # service timestamps debug datetime msec
dkcزر-ddc1 (config) # service timestamps log datetime msec
```

Oproti konfiguraci přepínačů v části nastavení *VTY (Virtual terminal line)* byla provedena minoritní změna. Na místo povolení maximálního počtu spojení přes *TELNET*, byla hodnota omezena pouze na nejvíce 5 spojení. Důvodem bylo zabezpečení konfigurace tak, aby nebylo možné provést připojení více jak pěti současných spojení.

### 3.3.2 Konfigurace portů

Oba porty (interface) 0/0 a 0/1 podporovaly gigabitový přenos dat. Port 0/0 byl nastaven na adresy vnitřní sítě a port 0/1 pro komunikaci společnosti s centrálou v Belgii. Na přepínači bylo již nastaveno statické směrování 0.0.0.0 0.0.0.0 192.168.56.250. Tento typ statického směrování zabezpečil přeoslání paketů, které nenáležely do naší sítě, na *IP* adresu 192.168.56.250. Jako příklad bylo možné uvést situaci, kdy byla do webového prohlížeče zapsána *IP* adresa 172.10.10.15, přičemž L3 přepínač Catalyst 3750 packet zaslal na *IP* adresu 192.168.56.250. *IP* adresa 192.168.56.250 byla přidělena směrovači, který zná cesty do jiných sítí.

#### Konfigurace portu 0/0:

```
dkcزر-ddc1 (config) # interface Gi 0/0
dkcزر-ddc1 (config-if) # ip address 192.168.56.250 255.255.248.0
dkcزر-ddc1 (config-if) # no shutdown
```

Z výše uvedené konfigurace bylo zřejmé, že na portu 0/0 byla nastavena *IP* adresa 192.168.56.250 s délkou síťového prefixu /21. Aby bylo možné portu přenášet více *IP* adres, ale zároveň, aby bylo aplikované určité bezpečnostní omezení, bylo provedeno takzvané „vymaskování“. Jinými slovy, byl povolen pouze určitý rozsah *IP* adres, které mohly portem procházet.

Popis:

- Adresa sítě 192.168.56.0 /21.

- Použitelné *IP* adresy 192.168.56.1 – 192.168.63.254.
- Broadcast 192.168.63.255.

Z rozsahu použitelných sítí bylo zřejmé, že se jednalo o námi použité virtuální sítě v rámci naší vnitřní infrastruktury.

Test komunikace směrem k směrovači a od směrovače k uživatelským stanicím byl proveden prostřednictvím příkazu *ping*, který využívá *ICMP (Internet Control Message Protocol)* protokol.

```
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::203:E4FF:FE6D:B20C
IP Address.....: 192.168.57.51
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.57.254

PC>ping 192.168.56.250

Pinging 192.168.56.250 with 32 bytes of data:

Reply from 192.168.56.250: bytes=32 time=0ms TTL=254
Reply from 192.168.56.250: bytes=32 time=0ms TTL=254
Reply from 192.168.56.250: bytes=32 time=0ms TTL=254
Reply from 192.168.56.250: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.56.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Obr. 29. Test komunikace směrem k přepínači

```
dkcyr-ddcl>ping 192.168.57.51

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.57.51, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms
```

Obr. 30. Test komunikace směrem k uživateli

V případě požadavku zaslání paket z vnitřní sítě z *IP* adresy 192.168.55.10, je paket zaslán L3 přepínačem Catalyst 3750 na *IP* 192.168.56.250 a tam je zmíněný paket zahozen, protože není v rozsahu použitelných *IP* adres. Identická situace nastane v případě požadavku z vnější sítě do naší na *IP* 192.168.55.10.

Poslední část nastavení `no shutdown` označovala aktivaci portu. Ta byla nutná, protože všechny porty směrovačů byly neaktivní, i když byly propojeny s protějším portem, který byl aktivní. U přepínačů jsou defaultně všechny porty ve stavu `no shutdown`.

### **Konfigurace portu 0/1 pro VPN komunikaci:**

```
dkcyr-ddc1(config)#interface Gi 0/1
dkcyr-ddc1(config-if)#ip address 85.93.126.107
255.255.255.248
dkcyr-ddc1(config-if)#no shutdown
```

Adresní rozsah 85.93.126.105 – 110 byl přidělen dodavatelem a správcem *VPN (Virtual Private Network)* linky. V tomto konkrétním případě byla použita *IP* adresa s délkou síťového prefixu 29, tak aby dodavatel mohl přidělovat své veřejné *IP* adresy po menších blocích.

### **3.3.3 Konfigurace protokolu *OSPF***

Konfigurace směrovacího protokolu *OSPF* spočívala ve vytvoření procesu *ID* a čísla oblasti na daných směrovačích. Proces *ID* mohl na směrovačích nabývat odlišných hodnot, ale čísla oblasti se musela shodovat.

Pro případ této práce je nastavení *OSPF* poměrně jednoduché, a to z důvodu, že veškerá komunikace (mimo směrem ven) do Internetu byla směrována přes firewall, jež je umístěn v belgické centrále. Tudíž správa tohoto bezpečnostního prvku v síti byla pod správou *IT* oddělení v Belgii. Naším úkolem bylo zabezpečit, aby jakýkoliv síťový prvek v rámci naší vnitřní sítě, jež by používal jinou virtuální síť, nemohl zasílat své pakety mimo tuto síť. Tento problém již byl vyřešen zvolením délky síťového prefixu /21 na portu `Gi 0/0` přepínače `dkcyr-ddc1`.

V daný okamžik bylo nezbytné zajistit, aby síť společnosti mohla komunikovat se síťovými prvky (servery, počítače, přepínače, atd.) v belgické centrále. Následně po konzultaci s *IT* oddělením v Belgii, byl zvolen směrovací protokol *OSPF*. Důvodem pro jeho použití byl fakt, že se jedná především o otevřený standart a v sítích rozsahu této společnosti. Je jeden z nejvíce používaných [16].

**Postup konfigurace OSPF na směrovači dkczr-ddc1:**

Nejprve bylo nutné vytvoření *ID OSPF* procesu na směrovači, což bylo možné provést pouze v konfiguračním módu.

```
dkczr-ddc1#conf t
```

```
dkczr-ddc1(config)#router ospf 56
```

```
dkczr-ddc1(config-router)#
```

*ID* procesu protokolu *OSPF* bylo zvoleno 56, protože bylo požadováno směrování z portu 0/0, kde je zvolena *VLAN* 56.

Následně bylo nutné nakonfigurovat sítě, které byly použity na rozhraních daného přepínače. V tomto případě to byly tedy dva záznamy protokolu *OSPF*. *IP* Adresy sítí se zadávaly společně se zástupnou maskou. Na závěr bylo zadáno číslo oblasti 200. Hodnota byla přidělena *IT* oddělením v Belgii a důvod použití hodnoty 200 byl následující. Směrovače, které spolu chtěly komunikovat, musely mít zadané stejné číslo oblasti. Na směrovači v Belgii bylo již více takovýchto oblastí a na směrovači české pobočky definovali právě hodnotou 200.

```
dkczr-ddc1(config-router)#network 192.168.0.0 0.0.255.255  
area 200
```

```
dkczr-ddc1(config-router)#network 85.93.126.0 0.0.0.255 area  
200
```

Dalším příkazem byla nastavena *syslog* zpráva, kterou odesílá směrovač o změně stavu mezi sousedy *OSPF*. Tato operace je vždy ve výchozím stavu zapnuta, ale bez prefixu *detail*. Odesílá tedy pouze informace o uvedení linky do provozu a o jejím vyřazení z provozu.

```
dkczr-ddc1(config-router)#log-adjacency-changes detail
```

Na níže uvedeném obrázku (Obr. 31) byly uvedeny podrobné informace o doručení zprávy „Hello“ na rozhraní směrovače v Belgii a byla zde uvedena i časová hodnota a *IP* adresa. Tyto informace byly zapisovány do systémového logu směrovače.

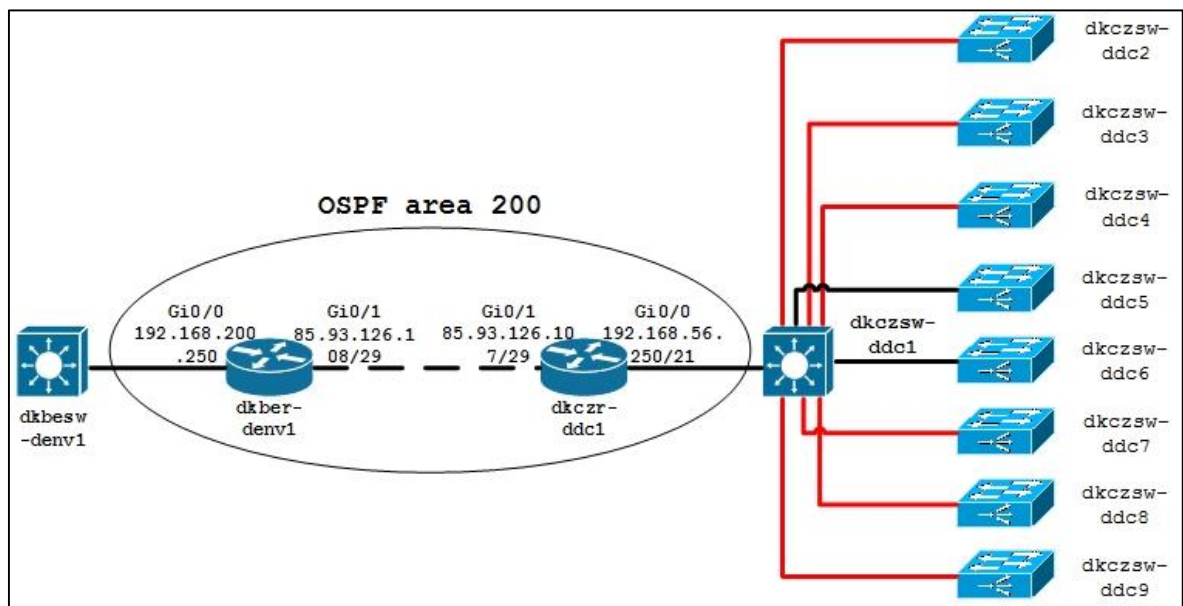
```

dkczr-ddc1(config-router)#log-adjacency-changes detail
dkczr-ddc1(config-router)#
*II 02, 14:20:18.2020: 14:20:18: %OSPF-5-ADJCHG: Process 56, Nbr 192.168.200.250
on GigabitEthernet0/1 from DOWN to INIT, Received Hello
*II 02, 14:20:18.2020: 14:20:18: %OSPF-5-ADJCHG: Process 56, Nbr 192.168.200.250
on GigabitEthernet0/1 from INIT to 2WAY, 2-Way Received
*II 02, 14:20:18.2020: 14:20:18: %OSPF-5-ADJCHG: Process 56, Nbr 192.168.200.250
on GigabitEthernet0/1 from 2WAY to EXSTART, AdjOK?
*II 02, 14:20:18.2020: 14:20:18: %OSPF-5-ADJCHG: Process 56, Nbr 192.168.200.250
on GigabitEthernet0/1 from EXSTART to EXCHANGE, Negotiation Done
*II 02, 14:20:18.2020: 14:20:18: %OSPF-5-ADJCHG: Process 56, Nbr 192.168.200.250
on GigabitEthernet0/1 from EXCHANGE to FULL, Exchange Done
*II 02, 14:20:18.2020: 14:20:18: %OSPF-5-ADJCHG: Process 56, Nbr 192.168.200.250
on GigabitEthernet0/1 from LOADING to FULL, Loading Done

```

Obr. 31. SYSLOG protokolu OSPF

Na obrázku (Obr. 32) bylo graficky znázorněno propojení naší sítě se směrovačem v belgické centrále. Pro úplnost byly uvedeny popisy portů daných přepínačů v *OSPF* lokalitě s *ID* 200.



Obr. 32. OSPF lokalita 200

Pro kontrolu funkce protokolu *OSPF* bylo možné na směrovači použít různé varianty příkazu *show*. Pro naši kontrolu by bylo dostačující použít tyto příkazy:

1. *show ip route* – příkaz, který zobrazí kompletní směrovací tabulku IP daného směrovače. Z posledního řádku výpisu je zřejmé směrování prostřednictvím protokolu *OSPF* s náklady na linku.

```

Gateway of last resort is not set

      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       85.93.126.104/29 is directly connected, GigabitEthernet0/1
L       85.93.126.107/32 is directly connected, GigabitEthernet0/1
C       192.168.56.0/21 is directly connected, GigabitEthernet0/0
        192.168.56.0/32 is subnetted, 1 subnets
L       192.168.56.250/32 is directly connected, GigabitEthernet0/0
O       192.168.200.0/21 [110/2] via 85.93.126.108, 08:14:10, GigabitEthernet0/1

```

Obr. 33. Směrovací tabulka

2. show ip ospf neighbor detail – vypisuje detailní seznam sousedů *OSPF* a jejich stav.

```

dkczr-ddcl#show ip ospf neighbor detail
Neighbor 192.168.200.250, interface address 85.93.126.108
  In the area 200 via interface GigabitEthernet0/1
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 85.93.126.108 BDR is 85.93.126.107
  Options is 0x00
  Dead timer due in 00:00:33
  Neighbor is up for 08:21:59
  Index 1/1, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum is 0 msec

```

Obr. 34. Informace o sousedním směrovači

3. show ip ospf database – pomocí posledního příkazu bylo možné získat výpis obsahu databáze *OSPF*.

```

dkczr-ddcl#show ip ospf database
      OSPF Router with ID (192.168.56.250) (Process ID 56)

      Router Link States (Area 200)

Link ID          ADV Router      Age             Seq#            Checksum Link count
192.168.56.250  192.168.56.250  1796           0x80000017     0x009a85  2
192.168.200.250 192.168.200.250 1397           0x80000014     0x00155b  2

      Net Link States (Area 200)

Link ID          ADV Router      Age             Seq#            Checksum
85.93.126.108   192.168.200.250 1397           0x80000011     0x006e76

```

Obr. 35. Obsah databáze *OSPF*

**Testování komunikace dle požadavků belgické strany:**

Pro testování komunikace mezi pobočkami byla ze strany belgické centrály určena *IP* adresa serveru 192.168.204.78, na kterou bylo požadováno zaslání *ICMP* paket pomocí příkazu `ping`. Tato část byla provedena ve všech virtuálních sítích vždy z jedné *IP* adresy. Následně byla vytvořena testovací virtuální síť *VLAN* 55, pro ověření funkčnosti povoleného rozsahu *IP* adres na portu `Gi0/0` přepínače `dkcزر-ddc1`.

```
Pinging 192.168.204.78 with 32 bytes of data:  
Reply from 192.168.204.78: bytes=32 time=1ms TTL=125  
Reply from 192.168.204.78: bytes=32 time=0ms TTL=125  
Reply from 192.168.204.78: bytes=32 time=0ms TTL=125  
Reply from 192.168.204.78: bytes=32 time=0ms TTL=125
```

*Obr. 36. Test komunikace z VLAN 58*

```
Pinging 192.168.204.78 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.
```

*Obr. 37. Test komunikace z VLAN 55*

Testováním bylo konstatováno, že komunikace byla funkční a bylo možné linku do belgické centrály plně využívat pro sdílení potřebných prostředků. Tímto byla část implementace oficiálně uzavřena a bylo nastaveno dvoutýdenní testovací období, v jehož rámci byly odstraňovány problémy, jež by mohly nastat, a to převážně při komunikaci směrem do Internetu. Nicméně tato problematika byla již pouze v kompetenci *IT* oddělení v Belgii, které zodpovídá za správu centrálního firewallu.

## 4 MOŽNOSTI DALŠÍHO ROZŠÍŘENÍ SÍTĚ

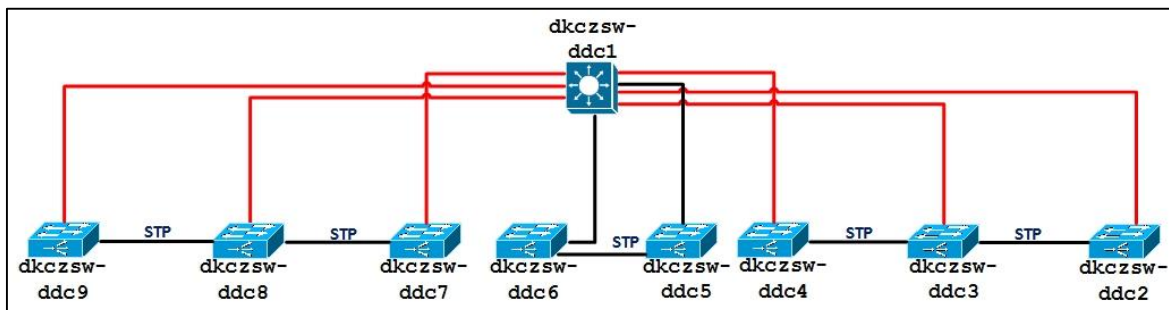
Vzhledem k tomu, že bylo nutné realizaci provést co nejdříve a za co nejnižších finančních nákladů, bylo nezbytné navrhnout možnosti dalšího rozšíření nebo většího zabezpečení sítě do budoucna. Hlavním aspektem byla co největší dostupnost sítě při výpadku jakéhokoliv ze síťových prvků. Při realizaci byla použita stávající infrastruktura, v níž nebylo zaimplementováno žádné zdvojení komunikačních tras.

Stávající datová síť byla realizována jako hvězda, kdy veškeré trasy byly propojeny přímo k hlavnímu přepínači Cisco Catalyst 3750. Pokud by došlo k přerušení kabelu v rámci spoje, tak by tato část sítě byla nedostupná.

Proto bylo vhodné mít záložní řešení, které by umožnilo získat čas na odstranění problému, nebo rozdělení komunikace různými směry, což se týkalo především komunikace vně společnosti.

### 4.1 Vnitřní síť

Jak již bylo řečeno, bylo nezbytné mít vhodně řešené komunikační spoje s hlavním přepínačem. Pokud by vedla k hlavnímu přepínači jen jedna cesta, tak by bylo účelné mít záložní trasu. Proto v rámci Cisco přepínačů bylo aktuální použít protokol *STP* (*Spanning Tree Protocol*). Pro jeho využití bylo však mezi přepínači nezbytné vytvořit smyčku. Tyto chtěné smyčky bylo možné aplikovat se spoluprací protokolu *STP*, který umožňoval zabránit propojení smyčkám v síti [17]. Na obrázku (Obr. 38) byl uveden příklad realizace stávající sítě za podpory protokolu *STP*.



Obr. 38. Návrh sítě s STP protokolem

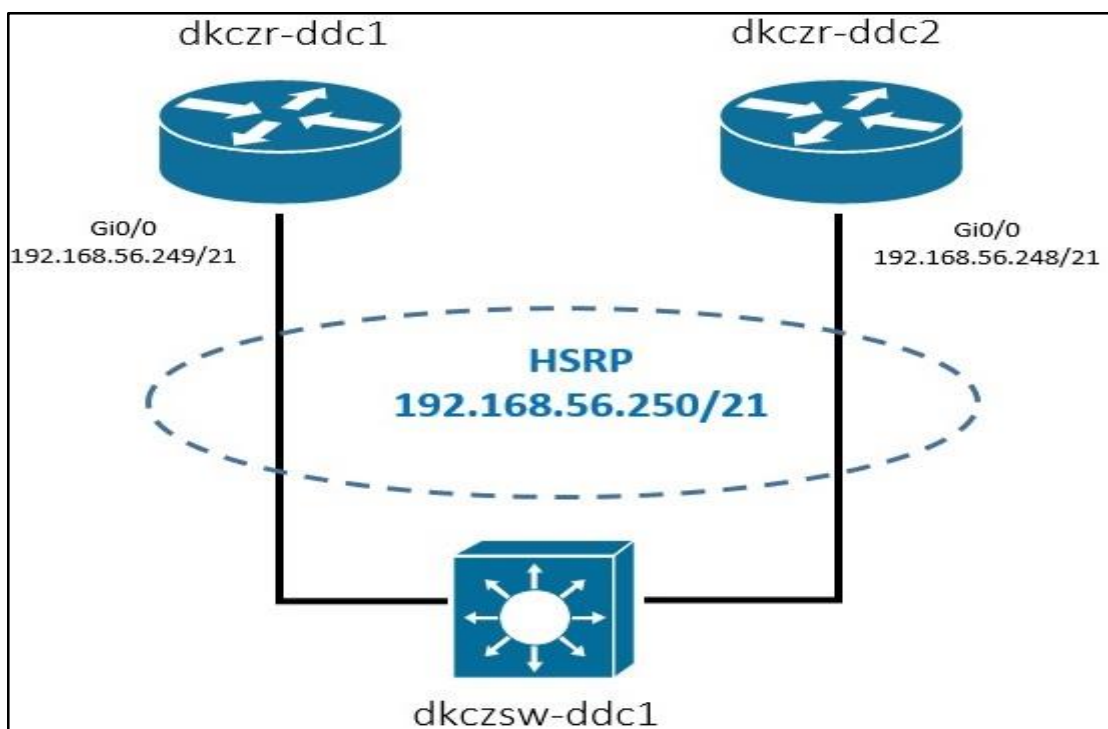
Z obrázku (Obr. 38) byla zřejmá nutnost vybudovat záložní trasy mezi přepínači. Tato změna by neměla být příliš nákladná vzhledem k tomu, že bylo možno použít klasické metalické vedení - kroucenou dvojlinkou.

Pro případ, že by došlo k výpadku komunikace mezi přepínačem `dkczsw-ddc1` a `dkczsw-ddc2`, tak by *SPT* protokol zjistil problém na hlavní trase a začal pakety posílat k přepínači `dkczsw-ddc1` přes `dkczsw-ddc3`.

## 4.2 VPN

Virtuální privátní síť zajišťuje propojení se sítí v belgické centrále. Výpadek této sítě, ať už ze strany dodavatele této linky nebo z naší strany výpadkem centrálního směrovače, by měl za následek kompletní odpojení veškeré komunikace mimo vnitřní virtuální síť. Bylo by tedy možné používat pouze interní síťová zařízení jako servery či tiskárny. Nicméně komunikace se servery v belgické centrále nebo do Internetu by nebyla možná.

Z těchto důvodů bylo účelné zabezpečit konektivitu i pro případ výpadku *VPN* nebo směrovače. Tuto problematiku v zásadě řeší proprietární protokol společnosti Cisco. Tímto protokolem je *HSRP* (*Hot Standby Routing Protocol*), který se zabývá právě problematikou výpadku dle konfigurace přepínače nebo směrovače. Varianta návrhu sítě s implementovaným *HSRP* protokolem je na obrázku (Obr. 39).



Obr. 39. HSRP protokol

Z takového nastavení by však vyplývala nutnost pořízení dalšího směrovače, který by sloužil jako záložní. Pro tyto směrovače by se vytvořila identická virtuální *IP* adresa a jeden z nich by vykonával primární funkci v závislosti na nastavené prioritě. Sekundární směrovač by pouze vyčkával a v případě výpadku primárního směrovače, by převzal směrovací protokoly a stal by se primárním.

Pro maximální využití *HSRP* protokolu by bylo zapotřebí, aby každý směrovač byl připojen na odlišnou *VPN* linku.

Připojení směrovačů do *VPN*:

- *dkczr-ddc1* – připojení do *VPN* prostřednictvím optické kabeláže společností Maxprogres,
- *dkczr-ddc2* - připojení do *VPN* prostřednictvím mikrovln v pásmu 10 GHz společností GTS Novera (nyní T-Mobile).

V tomto případě bylo nutné poukázat na to, že by došlo k nárůstu měsíčních nákladů na platby za *VPN*. Nicméně sekundární linka by mohla z hlediska kapacity být na nižší hodnotě než primární. Proto by mělo být reálné nárůst měsíčních nákladů zredukovat na přijatelnou hodnotu.

## 5 ROZPOČET PROJEKTU

Pro konkrétní případ projektu byly zpracovány investiční rozpočty. Při zadávání zakázek je obvyklé porovnávat minimálně dvě cenové nabídky. Pro kompletnost byly připraveny tři nabídky. Všechny tři byly identicky rozděleny do tří hlavních částí: na hlavní prvky, které jsou nezbytné k realizaci, dále média, která slouží k propojení hlavních prvků a třetí nedílnou součástí každé cenové nabídky byla i cena za implementaci, tedy za službu vlastního připojení síťových prvků a odzkoušení jejich funkčnosti.

V tabulce (Tab. 5) je cenová nabídka zpracovaná společností Autocont.

Tab. 5. Cenová nabídka od dodavatelské firmy Autocont

Název	Popis	Počet	Cena (bez DPH)
<b>Hlavní prvky:</b>			
Cisco Catalyst 3750-X	L3 přepínač 12 x SFP porty	1	164.534,- Kč
Cisco 2801-V3PN/K9	Hlavní směrovač	1	71.800,- Kč
Cisco Catalyst 2 960X-24TD-L	L2 přepínač 24 x port + 2 x SFP	8	305.456,- Kč
Cisco GLC-SX-MMD, 1000BASE-SX SFP	SFP modul pro MM optické vlákno	3	25.068,- Kč
Cisco GLC-LH-SMD, 1000BASE-SX SFP	SFP modul pro SM optické vlákno	3	24.690,- Kč
Cisco GLC-T, 1000BASE-T SFP	SFP modul pro UTP	6	25.692,- Kč
<b>Média:</b>			
Patch kabel UTP 1 m	Propojovací kabel 2x RJ-45	10	500,- Kč
Patch kabel UTP 2 m	Propojovací kabel 2x RJ-45	10	578,- Kč
LC-SC 09/125 - 1m SM	Optický patch kabel duplex	5	695,- Kč
LC-SC 50/125 - 1m MM	Optický patch kabel duplex	5	680,- Kč
<b>Implementace:</b>		1	40.000,- Kč
<b>Cena celkem</b>			<b>659.693,- Kč</b>

V tabulce (Tab. 6) je cenová nabídka společnosti Markit.Eu a v následné tabulce (Tab. 7) společnosti KDDI.

Tab. 6. Cenová nabídka od dodavatelské firmy Markit.Eu

Název	Popis	Počet	Cena (bez DPH)
<b>Hlavní prvky:</b>			
Cisco Catalyst 3750-X	L3 přepínač 12 x SFP porty	1	175.568,- Kč
Cisco 2801-V3PN/K9	Hlavní směrovač	1	68.260,- Kč
Cisco Catalyst 2960X-24TD-L	L2 přepínač 24 x port + 2 x SFP	8	308.400,- Kč
Cisco GLC-SX-MMD, 1000BASE-SX SFP	SFP modul pro MM optické vlákno	3	24.560,- Kč
Cisco GLC-LH-SMD, 1000BASE-SX SFP	SFP modul pro SM optické vlákno	3	28.530,- Kč
Cisco GLC-T, 1000BASE-T SFP	SFP modul pro UTP	6	30.389,- Kč
<b>Média:</b>			
Patch kabel UTP 1 m	Propojovací kabel 2x RJ-45	10	548,- Kč
Patch kabel UTP 2 m	Propojovací kabel 2x RJ-45	10	536,- Kč
LC-SC 09/125 - 1m SM	Optický patch kabel duplex	5	616,- Kč
LC-SC 50/125 - 1m MM	Optický patch kabel duplex	5	730,- Kč
<b>Implementace</b>		<b>1</b>	<b>55.000,- Kč</b>
<b>Cena celkem</b>			<b>693.137,- Kč</b>

Tab. 7. Cenová nabídka od dodavatelské firmy KDDI

Název	Popis	Počet	Cena (bez DPH)
<b>Hlavní prvky:</b>			
Cisco Catalyst 3750-X	L3 přepínač 12 x SFP porty	1	183.500,- Kč
Cisco 2801-V3PN/K9	Hlavní směrovač	1	75.300,- Kč
Cisco Catalyst 2960X-24TD-L	L2 přepínač 24 x port + 2 x SFP	8	315.300,- Kč
Cisco GLC-SX-MMD, 1000BASE-SX SFP	SFP modul pro MM optické vlákno	3	23.600,- Kč
Cisco GLC-LH-SMD, 1000BASE-SX SFP	SFP modul pro SM optické vlákno	3	26.820,- Kč
Cisco GLC-T, 1000BASE-T SFP	SFP modul pro UTP	6	28.560,- Kč
<b>Média:</b>			
Patch kabel UTP 1 m	Propojovací kabel 2x RJ-45	10	493,- Kč
Patch kabel UTP 2 m	Propojovací kabel 2x RJ-45	10	520,- Kč
LC-SC 09/125 - 1m SM	Optický patch kabel duplex	5	680,- Kč
LC-SC 50/125 - 1m MM	Optický patch kabel duplex	5	630,- Kč
<b>Implementace</b>		1	55.000,- Kč
<b>Cena celkem</b>			<b>710.403,- Kč</b>

Při jednoduchém porovnání cenových nabídek byla nejnižší nabídka společnosti Autocont, a to i včetně implementace. Kromě ceny bylo vhodné zohlednit také zkušenosti s danými společnostmi. V minulosti byly již *IT* zakázky zadávány společnosti Autocont a vždy bylo jednání s touto společností bezproblémové. Nejenom díky jejímu přímému zastoupení v lokaci společnosti, ve které k implementaci docházelo, ale také díky komunikačnímu jazyku, kterým je čeština.

Na rozdíl od toho společnost KDDI má zastoupení v Německu a vždy se komunikovalo v japonštině či angličtině, což přináší určité komplikace. Se společností Markit.Eu prozatím nedošlo ke spolupráci, a proto bylo obtížné její kvalitu poskytovaných služeb hodnotit.

Na tento projekt byl pro tento hospodářský rok vyhrazen rozpočet ve výši 650.000,- Kč a z toho důvodu bylo přistoupeno k variantě nákupu jednotlivých prvků od společnosti Autocont a implementaci svými vlastními silami.

## ZÁVĚR

V rámci práce byla provedena implementace síťových prvků Cisco do středně velké nadnárodní společnosti. Stěžejním úkolem byla samotná realizace včetně konfigurace jednotlivých síťových prvků.

Samozřejmostí takovéto implementace bylo provedení auditu stávajícího řešení a následné vyhodnocení podpořené návrhem nového uspořádání na základě informací získaných při rozboru situace. Proto byla první část praktického oddílu práce věnována právě auditu, jenž je členěn do tří částí. V prvním segmentu bylo popsáno získávání potřebných informací k dané problematice, následně byla provedena analýza a vyhodnocení získaných informací. Poslední část auditu byla věnována doporučení, tedy návrhu řešení realizace síťové infrastruktury, která byla vhodná pro danou společnost.

Následujícím bodem druhé části byla právě implementace daného konceptu, v níž byly použity síťové prvky společnosti Cisco. Jednalo se o směrovač řady 2801, přepínače řady 2960 a 3750x. Realizace se zabývala především konfigurací použitých síťových prvků a popisu jednotlivých fází nastavení. Veškeré konfigurační práce byly realizovány vlastními silami s částečnou podporou *IT* oddělení v belgické centrále. Tato výpomoc se týkala především části konfigurace směrovače, kdy bylo nutné prodiskutovat zvolení vhodného směrovacího protokolu a získáním adresního rozsahu od dodavatele *VPN* linky.

Část možnosti dalšího rozšíření sítě byla věnována návrhu na zlepšení realizovaného řešení, jež z časových a finančních důvodů nemohlo být provedeno. Soustředila se především na problematiku zabezpečení plné funkčnosti při přerušení linky v hlavních částech vnitřní sítě. Také je zde řešen možný plán zdvojení *VPN* linky, které by zabezpečilo plnou funkčnost při problému na hlavní trase do belgické centrály nebo při výpadku hlavního směrovače.

Závěr části implementace byl směřován k popisu tří cenových návrhů na pořízení síťových prvků a komponent potřebných pro propojení jednotlivých zařízení. U každého cenového návrhu bylo také na cenění prací v případě realizace jednotlivými dodavateli. Vzhledem k omezenému rozpočtu bylo ovšem nutné implementaci provést vlastními silami, kdy *IT* oddělení provedlo veškerou konfiguraci a otestování komunikace.

Práce vychází z praktických zkušeností s přípravou, realizací samotné implementace a se správou sítě daného podniku. Poznatky získané při tvorbě této práce by měly být přínosem pro společnost, jež čelí podobné problematice a potřebuje provést podobnou implementaci.

**SEZNAM POUŽITÉ LITERATURY**

- [1] LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.
- [2] MATÝSEK, Miroslav. 2014. Počítačové sítě: Učební prezentace UTB FAI UAI. Zlín.
- [3] PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]. Vyd. 2. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.
- [4] BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.
- [5] ŠPIČÁK, Ivo. Konfigurace sítě s napojením na externí úložiště. Zlín, 2013. Bakalářská práce. UTB ve Zlíně. Vedoucí práce doc.Ing.Martin Sysel, Ph.D.
- [6] PELIKÁN, Michal. Síťový protokol pro synchronizaci času NTP [online]. [cit. 2015-03-21]. Dostupné z: <http://uzitecne.mpelikan.com/ntp-synchronizace-cas-protokol.html>
- [7] LAMMLE, Todd. CCNA routing and switching: study guide : exams 100-101, 200-101, and 200-120. First edition. Indianapolis, Sybex, a Wiley Brand, [2013], 1 online zdroj (1178 pages). ISBN 978-1-118-74973-9.
- [8] BOUŠKA, Petr. TCP/IP - model, encapsulace, paket vs. rámeček. Samuraj-cz [online]. [cit. 2015-05-11]. Dostupné z: <http://www.samuraj-cz.com/clanek/tcpip-model-encapsulace-paketu-vs-ramec/>
- [9] TCP/IP Network Administration. Diablotin.com [online]. [cit. 2015-03-26]. Dostupné z: [http://www.diablotin.com/librairie/networking/tcpip/ch01\\_06.htm](http://www.diablotin.com/librairie/networking/tcpip/ch01_06.htm)
- [10] CISCO SYSTEM, INC. 2004. CCNA 3 Module 3 Single-Area OSPF.
- [11] VLAN - Virtual Local Area Network [online]. [cit. 2015-03-21]. Dostupné z: <http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/>
- [12] Optimalizace směrování [online]. [cit. 2015-03-21]. Dostupné z: [http://wh.cs.vsb.cz/mil051/index.php/Optimalizace\\_sm%C4%9Brov%C3%A1n%C3%AD](http://wh.cs.vsb.cz/mil051/index.php/Optimalizace_sm%C4%9Brov%C3%A1n%C3%AD)

- [13] P. Holub. Lambda služby. Zpravodaj ÚVT MU. ISSN 1212-0901, 2004, roč. XV, č. 2, s. 8-13.
- [14] Simple RJ45 DB9 Cisco console cable. Instructable [online]. [cit. 2015-05-12]. Dostupné z: <http://www.instructables.com/id/Simple-RJ45-DB9-Cisco-console-cable/>
- [15] CISCO. Catalyst 3750 Switch: Software Configuration Guide [online]. 2009 [cit. 2015-03-21]. Dostupné z: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122\\_5se/configuration/guide/3750scg.pdf](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122_5se/configuration/guide/3750scg.pdf).]
- [16] Cisco Routing 3 - OSPF - Open Shortest Path First [online]. [cit. 2015-03-21]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-routing-3-ospf-open-shortest-path-first/>
- [17] VELTE, Toby J a Anthony T VELTE. Síťové technologie Cisco: velký průvodce. Vyd. 1. Brno: Computer Press, 2003, 759 s., 16 s. obr. příl. Administrace. ISBN 80-7226-857-0.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

AD	Active Directory
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTP	Dynamic Trunking Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Elektromagnetická indukce
FTP	File Transfer Protocol
GMRP	GRAP Multicast Registration Protocol
HSRP	Hot Standby Routing Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
IPv4	Internet Protocol version 4
ISO/OSI	Open Systems Interconnection/ Open Systems Interconnection
LAN	Local Area Network
LED	Light Emitting Diode
LSA	Link State Advertisements
MAC	Media Access Control
MTU	Maximum Transmission Unit
NMS	Network Management Studio
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PC	Personal Computer
PDU	Protocol Data Unit
POP3	Post Office Protocol
PVC	Poly-vinyl-chlorid
RIP	Routing Information Protocol
ScTP	Screened Twisted Pair
SMTP	Simple Mail Transfer Protocol

---

SPF	Shortest Path First
SSL	Secure Sockets Layer
STP	Shielded Twisted Pair
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Telecommunication Network
TLS	Transport Layer Security
TP	Twisted Pair
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VLMS/CIDR	Valuable Length Subnet Mask/Classless Inter-Domain Routing
VMPS	VLAN Management Policy Server
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
VTY	Virtual terminal line

**SEZNAM OBRÁZKŮ**

<i>Obr. 1. Vrstvy modelu OSI [2]</i> .....	12
<i>Obr. 2. Formát segmentu TCP [9]</i> .....	16
<i>Obr. 3. OSPF [10]</i> .....	18
<i>Obr. 4. Směrovací tabulka OSPF [10]</i> .....	19
<i>Obr. 5. Režimy protokolu VTP [1]</i> .....	22
<i>Obr. 6. VLAN [11]</i> .....	23
<i>Obr. 7. Formát Tagu 802.1q [11]</i> .....	24
<i>Obr. 8. Redistribuce směrovacích protokolů [12]</i> .....	27
<i>Obr. 9. Příklad UTP kabelu [2]</i> .....	28
<i>Obr. 10. Level – Kroucená dvojlinka [2]</i> .....	29
<i>Obr. 11. Optické vlákno [13]</i> .....	30
<i>Obr. 12. Index lomu dle média [2]</i> .....	30
<i>Obr. 13. Převod signálu [2]</i> .....	31
<i>Obr. 14. Stávající rozložení sítě</i> .....	35
<i>Obr. 15. Část z výsledku kontroly optické kabeláže</i> .....	37
<i>Obr. 16. Návrh sítě</i> .....	40
<i>Obr. 17. Cisco konzolový kabel [14]</i> .....	42
<i>Obr. 18. Výpis VLAN</i> .....	45
<i>Obr. 19. Nastavení IP na VLAN 56</i> .....	47
<i>Obr. 20. Nastavení VTP protokolu</i> .....	48
<i>Obr. 21. Trunk porty</i> .....	49
<i>Obr. 22. Přepínání VLAN</i> .....	50
<i>Obr. 23. Statické směrování</i> .....	50
<i>Obr. 24. VTP bez Trunk portu</i> .....	55
<i>Obr. 25. Funkční VTP</i> .....	56
<i>Obr. 26. VLANy na trunkovém portu</i> .....	56
<i>Obr. 27. Informace o virtuální síti 63</i> .....	59
<i>Obr. 28. Cisco 2801</i> .....	60
<i>Obr. 29. Test komunikace směrem k přepínači</i> .....	62
<i>Obr. 30. Test komunikace směrem k uživateli</i> .....	62
<i>Obr. 31. SYSLOG protokolu OSPF</i> .....	65
<i>Obr. 32. OSPF lokalita 200</i> .....	65

---

<i>Obr. 33. Směrovací tabulka .....</i>	<i>66</i>
<i>Obr. 34. Informace o sousedním směrovači .....</i>	<i>66</i>
<i>Obr. 35. Obsah databáze OSPF .....</i>	<i>66</i>
<i>Obr. 36. Test komunikace z VLAN 58 .....</i>	<i>67</i>
<i>Obr. 37. Test komunikace z VLAN 55 .....</i>	<i>67</i>
<i>Obr. 38. Návrh sítě s STP protokolem .....</i>	<i>68</i>
<i>Obr. 39. HSRP protokol.....</i>	<i>69</i>

**SEZNAM TABULEK**

<i>Tab. 1. Typy síťových prvků a optické kabeláže .....</i>	<i>35</i>
<i>Tab. 2. Osazení modulů na jednotlivých portech přepínače.....</i>	<i>41</i>
<i>Tab. 3. Ostatní přepínače přiřazující porty do VLAN .....</i>	<i>57</i>
<i>Tab. 4. IP daných přepínačů.....</i>	<i>59</i>
<i>Tab. 5. Cenová nabídka od dodavatelské firmy Autocont .....</i>	<i>71</i>
<i>Tab. 6. Cenová nabídka od dodavatelské firmy Markit.Eu .....</i>	<i>72</i>
<i>Tab. 7. Cenová nabídka od dodavatelské firmy KDDI.....</i>	<i>73</i>

## SEZNAM PŘÍLOH

P I Záloha konfigurace přepínače Cisco Catalyst 3750.

Uloženo na DVD. Cesta: DVD\ Cisco Catalyst 3750\ dkczsw-ddc1-config

P II Záloha konfigurace směrovače Cisco Catalyst 2960.

Uloženo na DVD. Cesta: DVD\ Cisco Catalyst 2960\ dkczsw-ddc2-config

P III Záloha konfigurace směrovače Cisco 2801.

Uloženo na DVD. Cesta: DVD\ Cisco 2801\ dkczr-ddc1-config