

# **Inovace sítě v Jazykové škole Lingua**

Inovation of the computer network in Language School Lingua

Michael Galia

---

Bakalářská práce  
2012



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2011/2012

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Michael GALIA**  
Osobní číslo: **A09218**  
Studijní program: **B 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Inovace sítě v Jazykové škole Lingua**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Proveďte analýzu současného stavu počítačové sítě v Jazykové škole Lingua.
3. Vypracujte návrh inovace počítačové sítě v Jazykové škole Lingua na bázi zařízení od firmy Cisco.
4. Navrhněte konfigurační soubory pro všechny aktivní prvky Cisco.
5. Sestavte finanční návrh řešení.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské 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. HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5. aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-802-5131-763.
3. KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-802-5122-365.
4. ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.
5. LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.

Vedoucí bakalářské práce:

**Ing. Miroslav Matýsek, Ph.D.**

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

**24. února 2012**

Termín odevzdání bakalářské práce:

**25. května 2012**

Ve Zlíně dne 24. února 2012



L.S.

  
prof. Ing. Vladimír Vašek, CSc.  
děkan

  
doc. Mgr. Milan Adámek, Ph.D.  
ředitel ústavu

## ABSTRAKT

Práce se zaměřuje na inovaci počítačové sítě na Jazykové škole Lingua pomocí aktivních prvků od společnosti Cisco. První část práce popisuje základní principy fungování počítačové sítě. Zaměřuje se především na popis principů, podle kterých síť pracuje a také popisuje základní vlastnosti pasivních a aktivních prvků. Druhá část se zabývá úpravou plánů počítačové sítě a následně popisuje všechny pasivní a aktivní prvky použité v návrhu. Práce obsahuje také konfigurační příkazy pro aktivní prvky společnosti Cisco.

Klíčová slova: Počítačová síť, Cisco, LAN, Wi-Fi, Switch, Router, Access Point

## ABSTRACT

The work focus on innovation of the computer network in Language School Lingua with active components from Cisco company. Theoretical part describes of working the computer network. I focus on describe a principles, according to which the computer network works and I am also describing basic properties of passive and active components. Practical part deals with modification of plan the computer network and then I am describing all passive and active components used in design. Work also contain a configuration command for active components by Cisco company

Keywords: Computer network, Cisco, LAN, Wi-Fi, Switch, Router, Access Point

Poděkování:

Děkuji vedoucímu Ing. Miroslavu Matýskovi, Ph.D. za pomoc při zpracovávání bakalářské práce. Také bych chtěl poděkovat firmě Kyklop spol. s r.o. za poskytnutí materiálů a ceníků, které mi velmi pomohly v této práci.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 POPIS POČÍTAČOVÝCH SÍTÍ</b> .....	<b>11</b>
1.1 LOKÁLNÍ SÍŤ.....	11
1.2 TOPOLOGIE POČÍTAČOVÉ SÍŤE .....	11
1.2.1 Hvězdicová topologie.....	11
1.2.2 Stromová topologie .....	12
1.3 SÍŤE TYPU KLIENT - SERVER .....	13
1.4 PŘÍSTUPOVÉ METODY .....	13
1.4.1 CSMA/CD.....	13
1.4.2 CSMA/CA.....	13
1.5 BEZDRÁTOVÉ SÍŤE.....	14
1.5.1 Propojení bezdrátových prvků .....	15
1.5.2 Způsoby zabezpečení Wi-Fi.....	16
<b>2 PASIVNÍ PRVKY SÍŤE</b> .....	<b>19</b>
2.1 KABELÁŽ POČÍTAČOVÉ SÍŤE .....	19
2.1.1 Metalické kabely .....	19
2.1.2 Optické kabely .....	20
2.2 PATCH PANEL .....	23
2.3 KONCOVÉ ZÁSUVKY .....	24
2.4 ROZVODNÉ SKŘÍŇ.....	25
2.5 PROPOJOVACÍ KABELY .....	25
<b>3 AKTIVNÍ PRVKY SÍŤE</b> .....	<b>26</b>
3.1 SWITCH .....	26
3.1.1 Zjišťování adresy.....	26
3.1.2 Rozhodování o předávání a filtrování .....	26
3.1.3 Předcházení smyčkám .....	27
3.1.4 Spanning Tree Protocol.....	27
3.1.5 Zabezpečení portů .....	30
3.2 ROUTER.....	31
3.3 ACCESS POINT.....	31
3.4 SÍŤOVÁ KARTA .....	32
<b>4 VLAN</b> .....	<b>33</b>
4.1 DĚLENÍ SÍŤI VLAN .....	33
4.1.1 Statické síť VLAN .....	33
4.1.2 Dynamické síť VLAN.....	33
4.2 IDENTIFIKACE SÍŤI VLAN .....	34
4.2.1 Přístupové porty .....	34
4.2.2 Trunkové porty.....	34

4.3	ZNAČKOVÁNÍ RÁMCŮ .....	34
4.4	METODY IDENTIFIKACE VLAN .....	35
4.4.1	Inter-Switch Link .....	35
4.4.2	IEEE 802.Q .....	35
4.5	INTER-VLAN ROUTING .....	35
4.6	PROTOKOL VTP .....	36
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>38</b>
<b>5</b>	<b>ANALÝZA SOUČASNÉHO STAVU.....</b>	<b>39</b>
5.1	POŽADAVKY NA SÍŤ .....	39
5.2	PŮVODNÍ DOKUMENTACE .....	39
5.3	DOKUMENTACE AKTUÁLNÍHO STAVU .....	40
<b>6</b>	<b>NÁVRH ŘEŠENÍ POČÍTAČOVÉ SÍTĚ .....</b>	<b>42</b>
6.1	SCHÉMA ZAPOJENÍ SÍTĚ .....	43
<b>7</b>	<b>VÝBĚR PASIVNÍCH PRVKŮ .....</b>	<b>44</b>
7.1	KROUCENÁ DVOULINKA CAT6 .....	44
7.2	PARAPETNÍ ŽLAB MALPRO EIP 110x60.....	44
7.3	ZÁSUVKA PRO UTP SOLARIX SX9-6-UTP-WH.....	45
7.4	KEYSTONE SOLARIX CAT6 UTP .....	45
7.5	PODLAHOVÁ KRABICE LEGRAND 89606 .....	45
7.6	PATCH PANEL SOLARIX 24 PORTŮ UTP 1U, CAT6 .....	46
7.7	RACK TRITÓN 60x80, 45U .....	46
<b>8</b>	<b>VÝBĚR AKTIVNÍCH PRVKŮ .....</b>	<b>48</b>
8.1	ROUTER CISCO 2901/K9 .....	48
8.2	SWITCH CISCO SG 200-26.....	48
8.3	ACCESS POINT LINKSYS EA2700 .....	49
8.4	UPS EATON 5PX 2200i RT2U .....	50
<b>9</b>	<b>NASTAVENÍ AKTIVNÍCH PRVKŮ.....</b>	<b>51</b>
9.1	NASTAVENÍ SWITCHE S1 .....	51
9.2	NASTAVENÍ ROUTRU R1 .....	53
9.3	NASTAVENÍ AP .....	54
<b>10</b>	<b>CENOVÝ ROZPOČET PROJEKTU .....</b>	<b>56</b>
	<b>ZÁVĚR .....</b>	<b>57</b>
	<b>CONCLUSION .....</b>	<b>58</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>59</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>61</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>63</b>
	<b>SEZNAM TABULEK.....</b>	<b>64</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>65</b>

## ÚVOD

Tato práce má za cíl inovaci počítačové sítě v jazykové škole Lingua. S tím však souvisí i pochopení základních principů fungování sítě a všech jejích aktivních prvků a také ideální rozmístění pasivních prvků jako jsou koncové zásuvky, nebo umístění kabelového vedení.

Současná síť je poměrně nová, ale při její realizaci byli k dispozici pouze plány, které se neustále měnili, a tudíž nevznikla síť, která je schopná pojmout další uživatele, popřípadě jsou některé prvky umístěny naprosto chaoticky a nesmyslně. Chci tedy ukázat, že správně připravené plány jsou schopny tomuto zabránit a také zabezpečit další růst sítě.

Síť nemá velký počet koncových uživatelů, je zde však předpoklad dalšího růstu. Uživatelé budou síť využívat nejen na připojení k Internetu, ale i na spouštění programů ze serveru a tudíž je nutné síť dostatečně naddimenzovat.

Práce je rozdělena na dvě části. V první části je popsáno základní rozdělení počítačové sítě, používané principy při provozu sítí, pasivní prvky a funkce jednotlivých aktivních prvků. Popisuji přístupové metody na síť, kabely využívané při realizaci sítě a další pasivní prvky. Především se však zaměřuji na principy fungování a technologie jednotlivých aktivních prvků, jako switch, router a access point.

V druhé části je popsán současný stav a porovnávám různé verze výkresové dokumentace a to původní plány, plány odpovídající skutečnému stavu a můj návrh sítě. V této části se dále zaměřuji na výběr vhodných pasivních prvků a způsob jejich instalace. Dále vybírám vhodné aktivní prvky a to především s ohledem na projektovanou rychlost sítě a spolehlivost daných zařízení. Nakonec uvádím konfigurační soubory aktivních prvků od firmy Cisco a cenový rozpočet projektu.

## **I. TEORETICKÁ ČÁST**

# 1 POPIS POČÍTAČOVÝCH SÍTÍ

## 1.1 Lokální síť

*„Jsou to počítačové sítě, kde spolu komunikuje několik stanic zpravidla na sdíleném médiu. V rámci jedné LAN (Local Area Network) se používá stejný linkový protokol. Geografický rozsah LAN je omezen. Pro zvětšení tohoto rozsahu lze na fyzické vrstvě využívat opakovač. Opakovače naslouchají na svých síťových rozhraních a automaticky veškerou komunikaci opakují na ostatní svá síťová rozhraní.“ [3]*

Hlavní použití je v domácnostech, kancelářích, anebo v rámci jedné budovy. V rámci této sítě mohou být propojeny i stovky počítačů a dalších zařízení. Rychlosti sítě se pohybují od 10Mb/s až po 10Gb/s. Nejpoužívanější technologie LAN jsou v současné době Ethernet a Wi-Fi.

## 1.2 Topologie počítačové sítě

Topologie určuje, jak jsou koncové stanice propojeny, jak budou mezi sebou komunikovat a jakou technologii k tomu použijí. Topologii dělíme na logickou a fyzickou.

**Logická topologie** nám popisuje, jak koncové zařízení přistupují na síť, aby mohla poslat data. Využíváme zde převážně dvě metody:

- Broadcast – stanice čeká, až bude na vedení volno
- Token – stanice čeká, až dostane právo vysílat

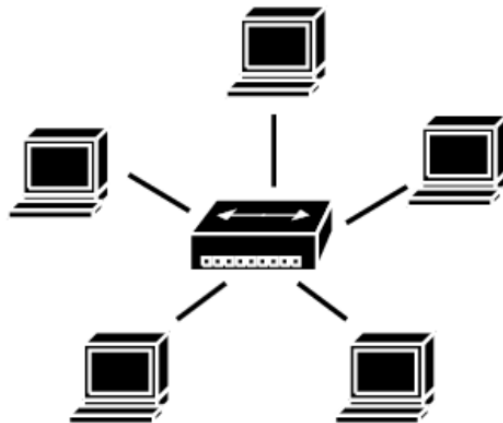
**Fyzická topologie** nám udává, jak jsou mezi sebou stanice propojeny a jestli používáme kabelové vedení, anebo bezdrátovou technologii.

### 1.2.1 Hvězdicová topologie

Každý počítač v síti je připojen kabelem, nejčastěji kroucenou linkou, do jednoho centrálního bodu. Dnes jsou tyto centrální body především switche, v dřívějších dobách se používaly huby. Tato topologie je dnes nejčastěji používané zapojení při návrhu nové sítě. Výhodou této sítě jsou:

- Při přerušení jednoho vedení, bude nedostupná pouze jedna stanice
- Na jednom vedení je připojen pouze jeden počítač, který má dané vedení pouze pro sebe
- Snadné úprava sítě podle budoucích požadavků

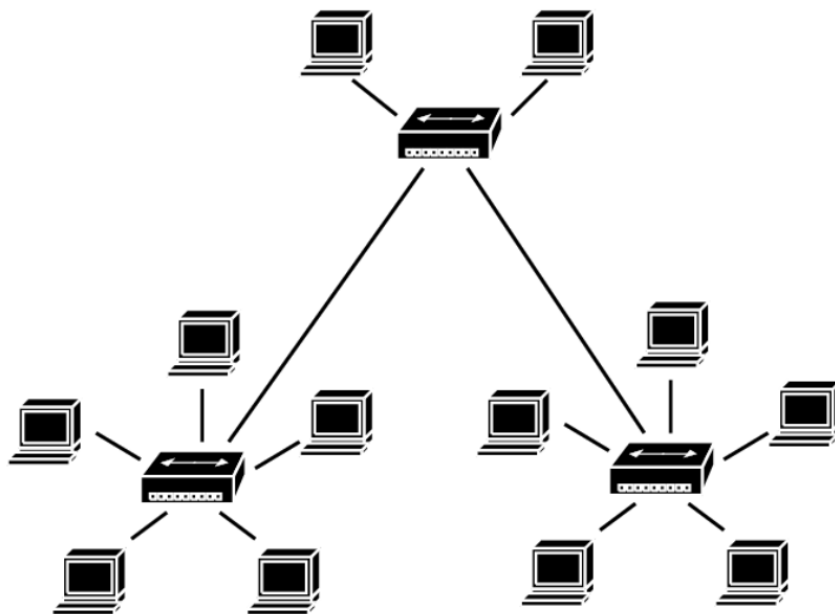
Nevýhodou je především délka použité kabeláže a nutnost mít centrální prvek .



Obr. 1. Hvězdicová topologie. [6]

### 1.2.2 Stromová topologie

Tato topologie vychází z hvězdicové topologie, která je rozšířena o další centrální body. Na původní centrální bod připojíme další, který tak rozšíří síť na velkou vzdálenost bez použití velkého množství kabeláže. Každý centrální prvek zde může reprezentovat různé správní jednotky, anebo různé budovy. Výhoda spočívá v tom, že pokud přestane fungovat jeden centrální prvek, zbytek sítě může fungovat bez problémů dál.



Obr. 2. Stromová topologie. [6]

### 1.3 Síť typu klient - server

Základem tohoto řešení je soustředit všechny data do jediného místa v síti. Toto místo pak můžeme důkladně zabezpečit a nabízet služby síťovým stanicím. Na server jsou v síti kladeny velké nároky, protože musí obsluhovat velké množství stanic v co nejkratším čase a taky musí být velmi spolehlivý. Tyto požadavky kladou velké nároky na HW (hardware) a SW (software) serveru. V tomto však spočívá i hlavní nevýhoda tohoto řešení, tj. musí být nakoupen speciální HW a SW splňující dané požadavky.

### 1.4 Přístupové metody

Přístupové metody popisují, jak zabezpečit, aby v daný čas vysílala na vedení pouze jedna stanice. Při vysílání dvou stanic na jednom vedení by došlo k vzájemnému rušení, které by znemožnilo přenos dat.

#### 1.4.1 CSMA/CD

Pokud potřebuje hostitel poslat data na síť, tak začne naslouchat provozu na síti, jestli zde probíhá komunikace. Pokud komunikace probíhá, počká, až skončí a začne vysílat vlastní data. Nadále však naslouchá provozu na síti a ujišťuje se, že nezačala vysílat jiná stanice. Může se však stát, že dvě stanice začnou vysílat v přesně stejný čas. Pokud stanice zjistí, že signál není její, okamžitě přeruší své vysílání a začne vysílat šumový signál. Šumový signál upozorní ostatní zařízení v síti, že nastala kolize na vedení a vyzve je ke spuštění speciálního algoritmu tzv. backoff. Tento algoritmus způsobí náhodné zpoždění, po kterém zařízení opět začne naslouchat provozu na síti. Může se teoreticky stát, že se nám nikdy nepodaří odeslat data, protože buď budeme neustále čekat a naslouchat provozu na síti a nebo backoff algoritmus na dané stanici skončí pokaždé později než na jiných. Výhodou je jednoduchost tohoto řešení. Nevýhodou je, že při přibývajícím počtu, se zvyšuje i pravděpodobnost kolizí a tím se přenos stává méně efektivní. Podle společnosti Cisco, je poloviční duplex, oproti plnému duplexu, efektivní pouze na 30 až 40%. Teoreticky by měla být efektivita 50%. [5]

#### 1.4.2 CSMA/CA

Druhá metoda je používána u standardu 802.11 tj. u bezdrátových sítí. U těchto sítí, se totiž velmi problematicky detekují kolizní stavy. *„Jde o to, že stanice sice může detekovat volné přenosové médium ve svém okolí, ale to ještě nutně neznamená, že*

*přenosové médium je volné i v okolí přijímací stanice. V tom samém okamžiku se totiž může o komunikaci s přístupovým bodem pokoušet jiná stanice, která není v dosahu první stanice, a tedy ani obě stanice nemohou vědět o tom, kdy která z nich vysílá.*“ [4]

Pro komunikaci je použit mechanismus předcházení kolizím spolu s kladným pozorováním. To znamená, že stanice naslouchá a pokud je médium volné, počká ještě určitý čas a teprve pak začne vysílat. Přijímací stanice zkontroluje CRC (Cyclic Redundancy Check) kontrolní součet přijatého paketu a odešle potvrzení ACK (Acknowledgement). Přijetí potvrzovacího paketu znamená pro odesílající stanici, že nedošlo ke kolizi. Pokud stanice paket ACK nedostane, opakuje vysílání. Aby se snížila pravděpodobnost kolizí vznikající právě tím, že se stanice nemohou slyšet, definuje standard virtuální naslouchací mechanismus. Stanice, která chce vysílat, vyšle nejdříve řídicí paket RTS (Request to Send) obsahující kromě zdroje a cíle i trvání následujícího přenosu. Cílová stanice odpovídá paketem CTS (Clear to Send) obsahující dobu trvání následujícího přenosu. Stanice, která slyší pakety RTS, anebo CTS, si nastaví indikátor virtuálního naslouchání NAV (Network Allocation Vector) na dobu trvání přenosu oznámenou v paketu. Po tuto dobu bude stanice brát médium jako používané, obsazené. [4]

Tím se riziko kolizí minimalizuje na dobu vysílání RTS paketu, protože paket CTS již distribuuje cílová stanice, která by měla mít dosah ke všem stanicím v síti, a z hodnoty CTS mohou již určit dobu obsazenosti přenosového média.

*„Tento mechanismus je ovšem efektivní pouze pro delší pakety, a tak standard rovněž umožňuje přenos bez použití mechanismu RTS/CTS, a to volbou RTS Threshold na stanici. Také multicast a broadcast zpráva nejsou potvrzovány.*“ [4]

## 1.5 Bezdrátové sítě

Signál se přenáší elektromagnetickým vlněním, kterým nahradíme metalické nebo optické kabely. Elektromagnetické vlny mají různou vlnovou délku. Pro bezdrátové sítě jsou k dispozici frekvence 2,4GHz a 5GHz. Pásmo 2,4GHz je zcela volně použitelné pásmo, ale využívají ho i jiné technologie jako Bluetooth, bezdrátové periferie, anebo třeba mikrovlnná trouba. Pásmo 2,4GHz je dále rozděleno na 14 kanálů. Střed prvního kanálu začíná na frekvenci 2,412GHz a po krocích 0,005GHz končí čtrnáctým kanálem na frekvenci 2,484GHz. V různých geografických územích můžeme použít jen určité kanály. [2], [4]

Tab. 1. Používané kanály v různých zemích. [3]

Země	Kanál
USA a Kanad	1-11 (2,412-2,462GHz)
Evropa	1-13 (2,412-2,472GHz)
Francie	10-13 (2,457-2,472GHz)
Španělsko	10-11 (2,457 -2,462GHz)
Japonsko	1-14 (2,484GHz)

V České Republice tedy máme k dispozici 13 kanálů, avšak každý kanál má frekvenční rozsah 22 MHz a odstupy mezi kanály jsou pouze 5 MHz. Z toho vyplývá, že máme k dispozici pouze tři nepřekrývající se kanály (kanál 1, kanál 6 a kanál 11). Pokud chceme tedy používat dva přístupové body, měli bychom zvolit kanály tak, aby se navzájem nepřekrývali.

Další možností je použití technologie Wi-Fi v pásmu 5 GHz tj. standart 802.11a. U tohoto pásma nehrozí rušení technologií Bluetooth a bezdrátovými periferiemi a celkově je toto pásmo méně zarušené než frekvence 2,4 GHz. U této frekvence máme k dispozici 11 nepřekrývaných kanálů, a pokud změním lineární polarizaci antén, dostaneme 22 nepřekrývaných kanálů, které pro většinu aplikací plně vyhovují. V dnešní době se však nejvíce prosazuje standard 802.11n. Tento standard vychází z předchozích standardů 802.11 a využívá obě dvě frekvence a navíc technologii MIMO (Multiple-input multiple-output), jenž zvyšuje datovou propustnost. Tato zařízení mohou mít až osm antén, v praxi však mají většinou pouze čtyři a dvě mohou sloužit jako vysílací a dvě jako přijímací. [3]

### 1.5.1 Propojení bezdrátových prvků

Bezdrátové prvky mohou komunikovat mezi sebou:

- **Ad hoc mód**

Je to přímé spojení několika zařízení, maximálně však pěti. Zařízení mezi sebou komunikují na stejné úrovni a celkově se tato síť podobá sítím peer-to-peer. Pro tento typ spojení nepotřebujeme žádný dodatečný hardware a lze ho též velmi rychle nainstalovat. Nevýhodou pak je, že zařízení musí být v dosahu ostatních a tudíž není možné tuto síť použít u větších prostor. Z uvedeného vyplývá, že tato síť je vhodná pouze pro jednoduché sdílení souborů, popřípadě internetu, ovšem s velmi malým dosahem. [3]

- **Infrastrukturní mód**

Zde je jako centrální prvek umístěn přístupový bod, takzvaný Access Point. Tento pracuje jako server, přes něhož probíhá veškerá komunikace mezi všemi bezdrátovými zařízeními. Veškerá komunikace musí tedy směřovat do přístupového bodu a tím je znemožněno vytváření Ad hoc sítí, které představují bezpečnostní riziko. Centrální prvek nám též umožní efektivní filtrování, nastavení efektivního zabezpečení a celkový dohled nad bezdrátovou sítí. [3]

### 1.5.2 Způsoby zabezpečení Wi-Fi

Při využití Wi-Fi technologie, bychom měli zaručit její bezpečnost a to z toho důvodu, aby se nikdo nepovoláný nedostal do naší sítě. Existuje několik způsobů zabezpečení:

- **WEP**

Zabezpečení WEP (Wired Equivalent Privacy) je způsob zabezpečení Wi-Fi, který je však v dnešní době již zastaralý. WEP používá symetrickou šifru, která používá pro šifrování i dešifrování stejný klíč, který je stejný pro všechny uživatele. Toto šifrování se může provádět klíčem o délce 64, 128 a 152 bitů. 24 bitů však tvoří inicializační vektor, který je v hlavičce paketu a efektivní délka klíče je o těchto 24 bitů kratší. WEP používá jako šifrovací algoritmus RC4, která k šifrování používá spojení náhodných znaků s textem pomocí funkce XOR. Dešifrování pak probíhá v opačném směru. Tento způsob zabezpečení byl prolomen v roce 2001 a dnes trvá jeho prolomení několik minut.

- **WEP s dynamickým klíčem**

U tohoto zabezpečení se inicializační vektory mění po předem nastaveném čase. Pro útočníka se sice může prolomit do sítě, má do ní však přístup pouze do doby, než se inicializační vektor změní a poté musí hledat klíč znovu. Toto zabezpečení je již spolehlivější, přesto se však používají pokročilejší technologie.

- **WPA – Personal**

Zabezpečení WPA – Personal (Wi-Fi Protected access) používá protokol TKIP (Temporary Key Integrity Protokol), jenž zajišťuje dynamickou změnu klíčů. Protokol je 128 bitový klíč, který obsahuje 48 bitový inicializační vektor. Heslo musí obsahovat 8 znaků, maximálně však 63 a je pro všechny uživatele stejné. Prolomení tohoto zabezpečení spočívá ve slovníkovém útoku, anebo v prolomení TKIP, které trvá asi minutu. Toto

můžeme vyřešit použitím šifrování AES (Advanced Encryption Standard), na které není v dnešní době známý úspěšný útok. Je zpětně kompatibilní s WEP.

- **WPA – Enterprise**

U tohoto zabezpečení se nevyužívá sdíleného hesla, ale ověřování každého uživatele na RADIUS (Remote Authentication Dial In User Service) serveru. Uživatel se tedy spojí s AP (Access Point) s využitím příslušné identifikace. AP pošle dotaz na RADIUS server, který projde svoji databází a určí, jestli uživatel dostane přístup do sítě. Toto zabezpečení se z důvodu použití serveru, který musí být neustále v provozu, využívá spíše ve firemním prostředí. Existuje několik typů autentizace:

- **LEAP** – Metoda společnosti Cisco, u které se využívají dynamické WEP klíče a ověřování mezi RADIUS serverem a AP. Po každém úspěšném ověření, získá uživatel nový WEP klíč.
- **EAP – TLS** – Vyžaduje privátní klíč uživatele, který může být uložen na tokenu, nebo třeba na čipové kartě. Pro průnik do sítě musí být tedy fyzicky odcizen tento klíč.
- **EAP – MD5** – Nepodporuje dynamickou změnu klíče. Autentizaci provádí pouze EAP (Extensible Authentication Protocol) server.
- **EAP – PSK** – Pro autentizaci používá PSK (Pre-Shared Key). Při úspěšném přihlášení se vytvoří zabezpečený komunikační kanál.
- **EAP – TLS** – Autentizace probíhá pomocí certifikátů vydaných certifikační autoritou.
- **EAP – TTLS** – Certifikát využívá pouze server pro autentizaci vůči uživateli a ten používá heslo.
- **EAP – IKEv2** – Využívá tři metody ověření a pro uživatele a EAP server mohou být tyto metody různé.
  - Asymetrické klíče
  - Hesla
  - Symetrické klíče
- **PEAP** – Umožňuje zapouzdření protokolu EAP s šifrováním a autentizovaným TLS.

V dnešní době se nejvíce používají techniky PEAP a EAP-TTLS

- **WAP2**

Metoda je šifrována pomocí algoritmu CCMP, jenž používá šifru AES. Integrita dat se kontroluje pomocí CBC-MAC (Cipher Block Chaining Message Authentication Code), jenž znemožní podvrhnutí paketů. Tato metoda se opět dělí na Personal a Enterprise. [7]

## 2 PASIVNÍ PRVKY SÍTĚ

### 2.1 Kabeláž počítačové sítě

V počítačových sítích používáme zejména následující tři typy přenosového média:

- Metalické kabely – přenáší se elektrické signály.
- Optické kabely – přenáší se optické signály.
- Vzduch – šíření pomocí elektromagnetických vln.

#### 2.1.1 Metalické kabely

Nejčastějším použitím metalických kabelů je kroucená dvoulinka, která je odvozena od telefonního kabelu. Skládá se z 8 samostatně izolovaných vodičů, které jsou uspořádány do čtyř párů a barevně označeny.

*„Elektrický signál, který je vodiči přenášen, je náchylný na rušení, jenž vzniká vzájemným působením vodičů. U kroucené dvoulinky spočívá ochrana proti vzájemnému rušení v „kroucení“. Oba vodiče tvořící jeden pár jsou navzájem zkrouceny, pravidelně střídají svou vzájemnou polohu. Také páry jsou navzájem překrouceny. Tím se minimalizuje ovlivňování jednoho vodiče druhým a vzájemné vlivy vodičových párů.“ [2]*

Kabely dělíme podle stínění na:

- **UTP** – nestíněný kabel
- **STP** – stíněný kabel – stíněný je každý pár uvnitř kabelu.
- **ScTP** – stíněný kabel – stíněný je pouze plášť kabelu.

#### **Kategorie kroucených dvoulinek:**

**Kategorie 1:** Určena pro hlasové a poplašné systémy. Není určena pro přenos dat. Šířka pásma je 100 kHz.

**Kategorie 2:** Určená pro hlasový telefon a připojení k němým terminálům IBM pro centrální počítače a minipočítače. Šířka pásma je max. 4 MHz.

**Kategorie 3:** Použití pro hlasový telefon, síť Ethernet do rychlosti 10 MB/s (10Base-T), síť token ring 4 MB/s, 100Base-T4. Šířka pásma je až 16 MHz.

**Kategorie 4:** Použití pro síť Token Ring s rychlostí 16 MB/s. Šířka pásma je až 20 MHz.

**Kategorie 5:** Použití pro 100Base-TX, Sonet, ATM. Šířka pásma až 100 MHz. Lze využít i pro standart 1000Base-T, pokud vyhoví dodatečným testovacím parametrům v TIA/EIA TSB-95

**Kategorie 5e:** Dodržují se u ní přísnější parametry a tak může být použita pro síť 1000Base-T. Šířka pásma je 125 MHz

**Kategorie 6:** Použití pro síť 1000 Base-TX a šířka pásma je 250 MHz. V současné době je jedna z nejpoužívanějších kabeláží. Tato kategorie lze též použít pro 10GBase-T, avšak v pouze omezené délce 30m a to podle standardu TIA-155-A. Oproti jiným typů kabeláže zde přibyl dělicí plastový kříž, který od sebe odděluje jednotlivé páry

**Kategorie 6a:** Použití pro síť 10GBase-T. Tato kabeláž se využije především v páteřních spojích a všude tam, kde potřebujeme přenášet velké množství dat. Šířka pásma je 500 MHz. U této kategorie se využívá stínění jednotlivých párů i celého kabelu

**Kategorie 7:** Použití pro síť 1000Base-TX. Šířka pásma 600 MHz. Používá konektory GC45 a TERA [1], [2]

Pro síť Ethernet se tedy hodí kategorie kabeláže 3 a poté kategorie 5 a více. V dnešní době se však s kategorií 3 setkáme pouze u starých rozvodů a do nových rozvodů se nepoužívá. Dnes se stále nejvíce používá kabeláž kategorie 5e a 6, které jsou cenově dostupné a nabízejí vysoké přenosové rychlosti.

#### **Pravidla práce s metalickými kabely:**

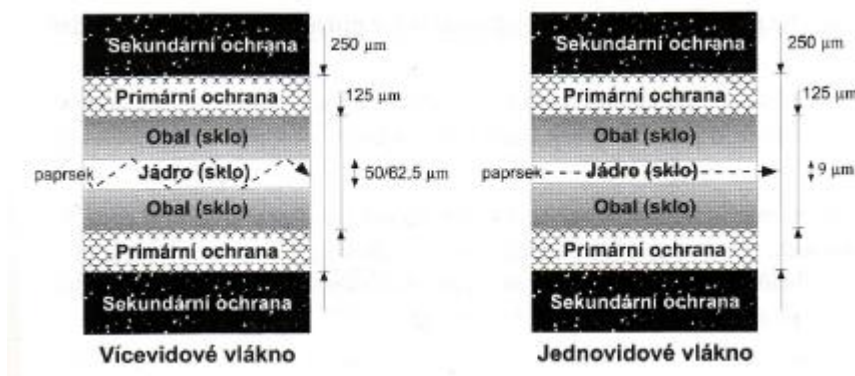
- Neohýbat kabel o více jak 90°
- Nevyvíjet na kabely v tahu sílu více jak 10kg
- Nedělat smyčky
- Nelámat kabel
- Poloměr ohybu musí odpovídat minimálně 6x průměru
- Kabel nevypínat
- Při konektorování nemít delší odizolovanou část jak 13mm

#### **2.1.2 Optické kabely**

*„Optická vlákna jsou tvořena dvěma vrstvami skla. Jeden typ je použit pro jádro vlákna a jiný typ skla pro obal vlákna. V jádře vlákna je veden optický paprsek, který se postupně odráží od rozhraní mezi dvěma druhy skla. Sklo má nízký optický odpor pouze*

pro tři vlnové délky světla: 850nm, 1300nm a 1500nm, proto se vždy k buzení optického signálu používá jedna z těchto vlnových délek. Optické vlákno je vždy simplexní spoj, tj. na jedné straně je vysílač a na druhé přijímač. Pro duplexní spoje (což potřebujeme téměř vždy) je nutná dvojice vláken – pro každý směr jedno vlákno.

Optická vlákna jsou nejprve obalena tzv. primární ochranou, která zajišťuje pružnost vlákna. Bez primární ochrany je vlákno velice křehké. Sekundární ochrana pak zvyšuje ochranu vlákna. S odstraněnou sekundární ochranou se již setkáváme u optických propojovacích kabelů. S optickými kabely, které mají odstraněnou sekundární ochranu, se v běžných firemních podmínkách obtížně pracuje. V této sféře jsou populární vlákna s tzv. těsnou sekundární ochranou (průměr  $900\mu\text{m} = 0,9\text{mm}$ ), která integruje primární i sekundární ochranu. Takové kabely jsou o něco dražší (proto se nehodí na propojování velkých vzdáleností), ale na druhou stranu je možné na tyto kabely svépomocí nasazovat optické konektory.“ [3]



Obr. 3. Optické vlákno. [3]

Optické kabely dělíme na:

**Mnohovidové:** Průměr jádra je  $50\mu\text{m}$ . Má horší optické vlastnosti, index lomu není všude stejný, dochází u něj k lomům vedeného paprsku. Vyslaný světelný signál se rozpadne na několik vidů. Tyto vidy mohou dorazit na konec vlákna za různě dlouhou dobu, což může způsobit zkreslení signálu. I když tyto kabely mají horší optické vlastnosti, tak optické trasy z nich složené levnější. K tomu přispívá i to, že jako zdroj světla používáme místo laseru levnější LED (Light-Emitting Diode) diody. Pro své horší vlastnosti se tento typ kabelů používá pro kratší vzdálenosti. Řádově jde však o stovky metrů, což pro většinu sítí LAN postačuje a proto se setkáváme většinou právě s tímto typem. Používají se pro rychlosti do 10 Gbit/s.

**Jednovidové:** Průměr jádra  $9\mu\text{m}$ . V tomto typu kabelu je index lomu mezi jádrem a pláštěm optického vlákna velmi malý a po celé délce konstantní. Kabelem prochází pouze jeden vid bez lomů a ohybů. Tento typ kabelů má lepší optické vlastnosti a s tím související přenosovou kapacitu a schopnost přenést signál na větší vzdálenost než mnohovidové kabely. Tyto kabely jsou však dražší, protože potřebují kvalitní zdroj světla – laser, takže se používají spíše na páteřních spojích telekomunikačních firem a v LAN se používají jen výjimečně. Lze dosáhnout rychlostí v řádu Tbit/s a to na vzdálenost desítek kilometrů. [3]

**Koncovky:** optické kabely jsou zakončeny normovanou koncovkou. Používají se především dva typy zakončení:

- Kulatý konektor ST
- Hranatý konektor SC



Obr. 4. Optické konektory. [9]

#### **Pravidla práce s optickým kabelem:**

Je důležité dodržovat několik základních pravidel:

- Kritickým místem optického vlákna je koncovka a její ferule. Ferulí prochází světelné impulsy, a pokud by došlo k jejímu znečištění, tak dojde k výraznému útlumu světelného signálu. Proto je feruli nutné opatřit krytkou. Pokud je ferule vysunuta ze zdířky, je nutné na ni nasadit kryt a nedotýkat se jí prsty
- Optické vlákna jsou velmi tenká a tak s nimi musíme zacházet velmi opatrně

- Při ohybu blízcímu se 90° může vzniknout špatný odraz optického signálu, což způsobí jeho útlum. Stejné problémy vzniknou i při stlačení vlákna. Oběma těmito případy se musíme vyhnout [3]

### **Spojování optických kabelů:**

Jestliže chceme spojit optický kabel s primární ochranou, musíme použít továrně připravené optické konektory nasazené na kusu optického vlákna. Tomuto se říká pig tail. Tento pig tail se následně navaří na připravený optický kabel.

Svaření dvou optických kabelů je velmi náročné. Při jednoduchém svaření by se sklovina obou vláken slila dohromady a vznikla by tak nepropustná překážka pro světelný signál. Vlákná se musí svařit tak, aby takový svár nevznikl. Pro správný svár však potřebujeme specializované vybavení.

Proto se snažíme svařování vyhnout za použití vlákna s těsnou sekundární ochranou. To nám umožní na konec vlákna nasadit optické konektory, pomocí kterých vlákna spojíme. Konec spojovaného vlákna musí být odborně ošetřen, protože pokud bychom ho zakrátili v ruce, dojde k roztříštění konce a spoj by nebyl možný. Na lámání používáme speciální nástroj, kterým tříštění omezíme. Konce se následně musí zabrousit a zkontrolovat mikroskopem, jestli byly všechny praskliny odstraněny. Následně se pomocí optického konektoru spojí dvě optické vlákna. Jádra vláken musí být tímto konektorem přitlačena k sobě, aby mohl světelný signál přejít z jednoho vlákna do druhého. [3]

## **2.2 Patch panel**

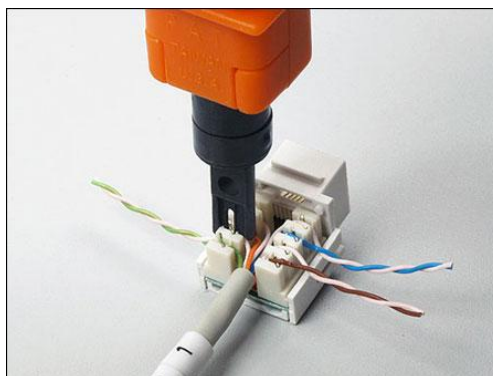
Jsou to propojovací pole pro ukončení horizontálních rozvodů. Panel může být připevněn na zeď, ale častěji bývá umístěn v rozvaděčové skříni. Má příslušné množství portů, a každý se dále dělí na další dvě části. Jedna slouží pro ukončení horizontální kabeláže a druhá pro připojení zařízení. Část pro horizontální rozvod je zakončena pomocí zářezových konektorů, které jsou pro snadnější instalaci označeny barevným kódem. Druhá část je opatřena konektorem RJ45. Je-li panel stíněný, musí být stínění spojené s kostrou rozvaděče a tento je uzemněn. [8]



Obr. 5. Patch panel. [10]

### 2.3 Koncové zásuvky

Zajišťuje ukončení kabeláže v pracovní oblasti, kde je umístěna podle požadavků, tj. na zdi, ve zdi, ve žlabu, nebo zapuštěné v zemi. Pro každou pracovní stanici by měla být minimálně dvě přípojná místa. Jedno je použito pro přenos dat a druhé se může použít pro telefon. Používáme proto dvě jednoduché zásuvky vedle sebe, anebo jednu dvojitou. Dvojitá zásuvka se pak označuje číslem a písmeny A a B. Zásuvka je ukončena konektorem RJ45 a v některých případech jsou zásuvky opatřeny krytkou, která zabrání pronikání nečistot, pokud do ní není připojen žádný kabel. Instalace kabelů se provádí narážáním kabelů speciálním nástrojem přímo v zásuvce, anebo použijeme zásuvky, které jsou uzpůsobeny pro keystoney. To jsou koncovky, do kterých se kabel buď naráží, popřípadě u dražších systémů se používají samo prořezávací. Takto připravené konektory se poté pouze umístí do zásuvky. Tento systém má výhodu ve snadnější manipulaci s kabelem a u samo prořezávacích keystoneů odpadá i požadavek na speciální nářezací nástroj.



Obr. 6. Narážecí nástroj. [11]

## 2.4 Rozvodné skříň

Rozvodná skříň, neboli rack, má několik standardizovaných rozměrů pro snadnější montáž aktivních i pasivních prvků. Nejdůležitějším rozměrem je rozteč montážních rámců o velikosti 19". Druhým základním rozměrem je rozteč mezi otvory pro matice umístěných na montážních rámech. Tento rozměr je udáván v jednotkách U a odpovídá 44,45mm. Rozvodné skříň se vyrábějí v mnoha provedeních, např.:

- Jednoduchý nebo dvojitý stojan bez opláštění
- Uzavřená skříň postavená na zem
- Uzavřená skříň pro zavěšení na zeď
- Použitým materiálem pro dveře
- Vnější půdorysem
- Výškou

Do rozvodných skříní můžeme kromě aktivních a pasivních prvků sítě umístit i servery a diskové pole. [8]

## 2.5 Propojovací kabely

Používají se v místě rozvádění panelů, tak i u pracovních stanic. Standardně jsou kabely osazeny na obou koncích konektory RJ-45. Pro spojování koncových stanic s aktivními prvky se používají kabely průchozí. Při použití speciálních panelů, jsou propojovací kabely voleny podle daného účelu zapojení. Jde-li například o propojení speciálního panelu s aktivním prvkem, na jednom konci bude speciální konektor a na druhém bude konektor RJ-45. Pro propojení dvou koncových uzlů, anebo aktivních prvků stejného logického typu, je třeba použít optický kabel. [8]

## 3 AKTIVNÍ PRVKY SÍTĚ

### 3.1 Switch

Je to aktivní síťový prvek, který propojuje jednotlivé části sítě. Switch rozděljuje velké kolizní domény na menší. Kolizní doména znamená, že dvě nebo více zařízení sdílí stejnou šířku pásma. Jelikož každý port switchce vytváří svou vlastní kolizní doménu, lze tak vytvořit mnohem lepší lokální síť. Pokud je síť se switchy navržena správně, vede to k přehledné a odolné síti. Rychlost switchce spočívá v tom, že neztrácí čas analýzou informací hlaviček síťové vrstvy, jako routery, ale kontrolují pouze hardwarovou adresu rámců a podle nich se rozhodují, zda rámec předají dál, hromadně rozešlou nebo zahodí. Switch tedy přijme paket, ten prozkoumá na druhé vrstvě modelu OSI (Open Systems Interconnection), načte rámec zapouzdřený v paketu a podle MAC (Media Access Control) adresy odešle na příslušný port. Oproti routeru tedy nezasahuje do paketu, tím se zvyšuje rychlost a odolnost proti chybám. Pokud použijeme přepínání na druhé vrstvě pro připojení pracovních skupin i segmentaci sítě, vytvoříme tak plošší návrh s více síťovými segmenty, než u směrování. [5]

#### 3.1.1 Zjišťování adresy

Switchce si pamatují zdrojovou MAC adresu každého přijatého rámce na portu a tuto adresu ukládají do databáze MAC adres, která se označuje jako tabulka předávání a filtrování. Po prvním zapnutí je tato tabulka prázdná. Pokud zařízení přijme rámec na portu, umístí switchce zdrojovou adresu rámce do tabulky. Takto udržuje informace o připojených zařízeních. Po přijetí rámce je v tabulce adres pouze jeden záznam, a to zařízení, které rámec vyslalo, a tak musí switch zaplavit síť tímto rámcem kromě zdrojového portu. Jestliže zařízení na tento rámec odpoví, switch načte zdrojovou adresu rámce a uloží ji do tabulky. V tabulce se tedy nacházejí již dva záznamy a tak mohou tyto dvě zařízení navázat dvoubodové spojení a switch již nemusí zaplavovat síť rámci a vyšle rámec pouze na daný port. [5]

#### 3.1.2 Rozhodování o předávání a filtrování

Když je na port switchce doručen rámec, je cílová MAC adresa porovnána s uloženými adresami v tabulce pro předávání a filtrování. Pokud je cílová adresa známa a uložena v tabulce, je rámec odeslán pouze na správné výstupní rozhraní. Tento způsob,

který se označuje jako filtrování rámců, šetří šířku pásma v jiných síťových segmentech. Jestliže se však cílová MAC adresa nenachází v tabulce, je rámec hromadně rozeslán ze všech aktivních portů, kromě portu ze kterého byl přijat. Pokud zařízení na rámec odpoví, je tabulka s MAC adresami aktualizována. Když switch přijme od hostitele, anebo serveru všesměrové vysílání, tak switch ve výchozím nastavení rozešle hromadně tento rámec na všechny aktivní porty, kromě portu zdrojového. Switch totiž tvoří menší kolizní domény, ale standardně tvoří jednu velkou všesměrovou doménu. [5]

### 3.1.3 Předcházení smyčkám

Redundantní spojení switchů je výhodné, jelikož souží jako prevence kompletního výpadku sítě v případě, že jedno spojení přestane fungovat. Tyto redundantní spoje mohou být velmi užitečné, ale bývají též zdrojem problémů. Důvod těchto problémů spočívá v tom, že rámce mohou být hromadně odeslány po všech redundantních spojích současně, což má za následek síťové smyčky a další potíže jako například: všesměrové bouře, u kterých se neustále rozesílají všesměrová vysílání po celé síti, příjem více kopií rámce, daný rámec může totiž dorazit současně z odlišných segmentů, cyklická aktualizace MAC tabulky, switch může přijmout rámec z více linek a tak se přepínač může dostat do cyklu neustálých aktualizací tabulky a rámec tak nikdy nemusí předat, generování vícenásobných smyček, mohou se objevit smyčky v rámci jiných smyček. Toto spolu s všesměrovou bouří může znemožnit přeposílání rámců. Tyto situace jsou velmi nebezpečné, a proto používáme STP (Spanning Tree Protocol), který umí tyto situace napravit anebo jim úplně předejít. [5]

### 3.1.4 Spanning Tree Protocol

Hlavním úkolem protokolu STP je předejít síťovým smyčkám na druhé vrstvě. Protokol sleduje síť a vyhledává všechny linky. Přitom vypnutí všech redundantních smyček zajišťuje, aby se nevyskytly žádné smyčky. Protokol STP pomocí algoritmu kostry grafu, STA, nejprve vytvoří topologickou databázi a poté vyhledá a zlikviduje redundantní linky. Pokud je protokol STP aktivní, jsou rámce předávány pouze po nejlepších spojích, které tento protokol vybere. Vypnutí redundantních linek zajišťuje protokol STP tak, že nejdříve zvolí kořenový most, který předává přes všechny porty a slouží jako referenční bod pro všechna ostatní zařízení v doméně STP. Jakmile se všechny switche shodnou na tom, který z nich bude fungovat jako kořenový most, musí všechny najít svůj kořenový port. Každá linka mezi dvěma switchi musí mít pouze jeden určený port, který poskytuje

největší šířku pásma ke kořenovému switchi. Na cestě ke kořenovému switchi se můžou nacházet další switche, to znamená, že cesta není vždy nejkratší, ale volí se ta nejrychlejší. U kořenového switchu, jsou všechny porty určenými porty, protože samotný kořen má ke kořeni nejkratší možnou vzdálenost. Hned jak se určí kořenové a určené porty, jsou všechny ostatní porty uvedeny do stavu blokování, aby se přerušily smyčky přepínání. [5]

U switchů s technologií STP máme několik principů a technologií, které bychom měli znát:

- **Výběr kořenového switchce**

Hodnota ID switchu slouží k volbě kořenového switchu a výběru kořenového portu pro každé zbývající zařízení. Hodnota ID má 8 bajtů a obsahuje prioritu i MAC adresu zařízení. Výchozí priorita zařízení používajících STP protokol ve verzi IEEE je 32768. Pokud chceme určit kořenový most, musíme zkombinovat priority všech mostů a jejich MAC adresami. Pokud mají dva switche stejnou prioritu, rozhodne o nejnižším ID jejich MAC adresa. Princip je následující. Pokud mají dva switche stejnou výchozí prioritu, použije se místo priority MAC adresa. Nejvyšší prioritu podle MAC adresy dostane ten switch, který má hodnotu MAC adresy nejnižší. Hodnotu ID lze změnit ručně, aby automaticky převzal roli kořenového mostu. Tato možnost zajišťuje, že ve velkých sítích budou zvoleny optimální trasy. Změna priority se provádí v konfiguračním režimu příkazem:

```
spanning-tree vlan1 priority 0-61440.
```

Při prioritě 0 bude switch vždy kořenovým mostem. Priorita se také nastavuje v násobcích 4096. Pokud chceme, aby switch sloužil jako kořenový most ve všech sítích VLAN (Virtual Local Area Network), musíme prioritu nastavit každé síti zvlášť. Nastavení priority u jednoho přepínače na 0 u všech VLAN by však nebylo vhodné.

Při výchozím nastavení se datové jednotky protokolu STP odesílají každé dvě sekundy ze všech aktivních portů switchu. [5]

- **Stavy portů protokolu STP**

Porty switchu se mohou nacházet v pěti stavech:

1. **Blokování:** blokový port nepředává rámce a pouze naslouchá datovým jednotkám protokolu STP. Stav blokování zabraňuje vzniku smyček. Ve stavu blokování jsou po zapnutí všechny porty

2. **Naslouchání:** port naslouchá datovým jednotkám protokolu STP, aby před předáním rámců zjistil, že se v síti neobjeví žádné smyčky. Port v tomto stavu je připraven k předání datových rámců bez zaplnění tabulky MAC adresami
3. **Zjišťování:** port naslouchá datovým jednotkám STP a zjišťuje všechny trasy v síti. Port ve stavu zjišťování plní tabulku MAC adresami, ale nepředává datové rámce. Zpoždění předávání je doba přechodu portu mezi režimem naslouchání a režimem zjišťování. Ve výchozím nastavení je tato doba nastavena na 15 sekund
4. **Předávání:** port přijímá a odesílá všechny datové rámce na přemostěném portu. Jestliže je port na konci stavu zjišťování určeným nebo kořenovým portem, přejde do stavu předávání
5. **Zakázáno:** port v zakázaném stavu se neúčastní na předávání rámců ani na fungování STP. Port v tomto stavu není funkční

Porty switchů se nejčastěji nacházejí ve stavech blokování a předávání. U stavu předávání bylo zjištěno, že má nejnižší náklady na trasu ke kořenovému mostu. Pokud se však změní uspořádání sítě, přejdou porty do režimů naslouchání a zjišťování. Jestliže však switch zjistí, že blokový port by měl být z důvodu změny topologie nastaven jako určený nebo kořenový, přejde do režimu zjišťování a kontroluje všechny přijaté datové jednotky protokolu STP, aby zajistil, že po přechodu portu do režimu předávání nevznikne žádná smyčka. [5]

- **Konvergence STP**

Ke konvergenci dojde v okamžiku, kdy všechny porty switche přejdou do režimu předávání nebo blokování. Pokud není konvergence dokončena, tak se nepředávají žádné data. Aby bylo možné data opět předávat, je zapotřebí všechna zařízení aktualizovat. Pokud tedy probíhá konvergence protokolu STP, tak se zastaví veškerý přenos uživatelských dat. Aby byla zajištěna komunikace mezi uživateli, musí být síť fyzicky navržena tak, aby mohl protokol STP velmi rychle konvergovat. Konvergence tedy zjišťuje, že všechna zařízení mají stejnou databázi, toto ale trvá nějaký čas. Přejed z režimu blokování do režimu předávání trvá obvykle 50 sekund a výchozí časovače není vhodné měnit. Jestliže vytvoříme hierarchický návrh switchů, lze nastavit jádro sítě jako kořen protokolu STP. Toto zajistí rychlou a účinnou konvergenci. Při restartu zařízení mohou nastat s dobou konvergence potíže s časovým limitem operací u hostitelů a serverů. Toto lze vyřešit zakázáním protokolu STP pomocí funkce PortFast. [5]

- **PortFast**

Pokud je ke switchi připojen server, anebo mu podobné zařízení, a jsme si naprosto jisti, že vypnutí protokolu STP nezpůsobí smyčku, můžeme na daných portech využít funkce portfast. Tato funkce zajistí, že port nestráví 50 sekund, při kterých by čekal na konvergenci. [5]

- **UplinkFast**

Příkaz společnosti Cisco, který zkracuje čas konvergence v případě selhání linky. Tento příkaz lze uplatnit v přepínaném prostředí, kde má switch alespoň jeden alternativní, nebo záložní kořenový port. Tato funkce se doporučuje aktivovat pouze u switchů s blokovánými porty a na přístupové vrstvě. Díky této funkci, umí switch najít alternativní trasu ke kořenovému mostu před výpadkem primárního spojení. Port tedy nečeká standardních 50 sekund. Není však vhodné tuto funkci zapínat, jestliže neznáme topologii alternativní trasy ke kořeni.[5]

- **BackboneFast**

Tato funkce se používá k urychlení konvergence v případě selhání linky, která není připojena k switchi. Pokud switch s touto funkcí přijme nekvalitní datovou jednotku protokolu STP (nekvalitní jednotka, je taková, která uvádí stejný switch pro kořenový i určený most) a vyvodí z toho, že došlo k výpadku linky na trase ke kořeni. Tato funkce umožní zkrátit konvergenci protokolu STP o 20 sekund z výchozích 50. [5]

### 3.1.5 Zabezpečení portů

Pokud chceme, aby si nikdo nepřipojil zařízení k portu switche, anebo si nepřidal u své stanice další switch, nebo přístupový bod můžeme nastavit, aby se zastavilo automatické přidávání MAC adres. Máme několik možností:

- **Přiřadit jednu MAC adresu danému portu:** vybereme daný port a zadáme příkaz: `switchport port-security mac-address MAC_adresa`
- **Možnost připojení pouze jedné MAC adresy na jeden port:** při nastavení 1 MAC adresy na port, se při pokusu připojit druhé zařízení port vypne a musí být znovu zapnut příkazem `shutdown` a `no shutdown`, po vybrání portu zadáme:  
`switchport port-security maximum 1`  
`switchport port-security violation shutdown`

- **Automatické nastavení MAC adres pro daný port:** MAC adresa zařízení na portu se uloží jako statická a záznam zůstane v platnosti po předem definovanou dobu. Příkaz zní:

```
switchport port-security mac-address sticky
```

```
switchport port-security maximum 1
```

```
switchport port-security violation shutdown
```

Zamezení koncovým uživatelům připojení dalších zařízení je velmi důležité, protože při připojení například vlastního přístupového Wi-Fi bodu vzniká v síti bezpečnostní díra, kterou může využít útočník, který se chce do sítě dostat. [5]

## 3.2 Router

Tento prvek, tvoří většinou jádro datové sítě, jež spojuje více sítí dohromady. Směrování probíhá na 3. Vrstvě modelu ISO/OSI, tj. podle IP (Internet Protocol) adres.

Router však musí splňovat i další podmínky:

- Zajištění chodu 24 hodin denně 7 dní v týdnu
- Zajištění integrity dat video a hlasových služeb. K tomu využívá funkce QoS (Quality of Service), ta zajistí, že pakety těchto služeb budou zpracovávány přednostně a nedojde tak ke zpoždění, které je u těchto služeb velmi nežádoucí
- Chránění vnitřní sítě, např. použitím firewallu

Router je koncipován jako zařízení pro nepřetržitý provoz a proto se pro tento účel nehodí obyčejné PC, které by šlo použít jako router s příslušným SW, ale používají se specifické komponenty, které zajistí nepřetržitý provoz s minimem poruch. Na routeru se nachází několik druhů rozhraní. Základní jsou LAN a WAN (Wide Area Network). LAN rozhraní slouží pro propojení vnitřní sítě a jsou to většinou konektory Ethernet a FastEthernet, kdežto WAN rozhraní pro připojení vnější sítě jsou většinou přes sériové rozhraní. Na routeru se nachází i obslužné porty jako console port, který umožní připojení PC (Personal Computer), přeš něhož bude router programovat a auxiliary port, jenž se hodí na připojení modemu. [12]

## 3.3 Access Point

Je to zařízení, které zprostředkovává komunikaci mezi drátovou sítí a bezdrátovými zařízeními. Převádí tedy pakety TCP/IP ze standartu 802.11 určeného pro Wi-Fi sítě na

802.3 určeného pro kabelové sítě. AP má velmi velké možnosti nastavení. V jeho nastavení volíme typ zabezpečení, použité frekvence, kanály, automatické přiřazování adres. AP mohou pracovat v následujících módech BSS (Basic Service Set), to v případě, že se jedná o samostatné AP, nebo ESS (Extended Service Set), máme-li AP více a chceme-li, aby mohl uživatel mezi těmito AP bez omezení přecházet.

### 3.4 Síťová karta

Karta zprostředkovává komunikaci mezi PC a sítí podle daných síťových standardů jako jsou typ kabeláže, typ použitého protokolu a přístupová metoda. V dnešní době většinou už bývají síťové karty integrovány v základních deskách. Občas však může síťová karta scházet, anebo potřebuje více NIC. Pak můžeme tuto kartu připojit v zásadě pomocí dvou sběrnic: [2]

**PCI:** Je to starší typ sběrnice a na dnešních deskách se již přestává objevovat. Je 32 bitová a pracuje na frekvenci 33 MHz

**PCI Express:** Je to dnes nejpoužívanější standard, používá sériový přenos dat a vyrábí se v několika variantách. Tyto varianty se od sebe liší počtem použitých vodičů. U normálních PC se používá nejpomalejší varianta PCIe x1, u severů pak PCIe x4 a PCIe x8

**PCMCIA:** Toto rozhraní se používá především u notebooků a umožňuje připojení externí karty. U levnějších notebooků se však toto rozhraní nemusí nacházet.

**USB:** V dnešní době jedno z nejpoužívanějších rozhraní pro připojení periférií. Umožňuje rychlé připojení a odpojení daného zařízení.

Další užitečnou vlastností síťových karet je funkce Wake-On, která nám umožní spustit počítač příkazem přes síť. Tuto funkci též musí podporovat základní deska. Počítač tedy čeká v uspaném stavu na signál pro probuzení. Tato funkce bývá integrována do většiny programů pro správu sítě. [2]

## 4 VLAN

Síť VLAN je logické seskupení síťových uživatelů a prostředků s připojením k administrativně definovaným portům switche. Máme tak možnost pomocí switche vytvořit menší všesměrové domény a to tím, že přiřadíme různé porty switche k různým sítím VLAN. Síť VLAN se považuje za vlastní podsíť, nebo všesměrovou doménu. Rámce vysílané do sítě jsou přepínány pouze porty, které jsou logicky přiřazeny do stejné sítě VLAN. Pokud však chceme, aby mohli uživatelé komunikovat mezi různými VLAN, budeme v síti potřebovat router. Sítě VLAN mají následující výhody:

- **Správa uživatelů:** přidávání, odebrání, přesuny a změny sítí lze snadno provést konfigurací portu do příslušné VLAN
- **Lepší zabezpečení:** uživatelé, kteří vyžadují vysokou úroveň zabezpečení mohou být přesunuti do vlastní VLAN, aby s nimi nemohli uživatelé vně sítě komunikovat
- **Logické seskupení:** síť VLAN nezávisí na geografickém umístění, ale pouze na logickém seskupení
- **Bezpečnost:** velké zlepšení bezpečnosti sítě
- **Omezení provozu:** zvyšují počet všesměrových domén a omezují jejich velikost

### 4.1 Dělení sítí VLAN

Pokud správce systému přiřazuje síť VLAN portům switche ručně, označujeme takové síť jako statické. Tato metoda je však náročnější na čas a tak se u větších sítí používají dynamické síť VLAN. Zde se VLAN uživateli přiřadí automaticky. [5]

#### 4.1.1 Statické síť VLAN

Je to nejčastější způsob vytváření VLAN a to z toho důvodu, že je tento způsob nejbezpečnější, protože port je trvale přiřazen do dané VLAN dokud ho správce ručně nezmění. Velmi dobře se též kontroluje pohyb uživatelů v rámci sítě a správce sítě má nad tímto absolutní kontrolu.

#### 4.1.2 Dynamické síť VLAN

Zde se hostitelé k sítím VLAN přiřazují automaticky a to například podle MAC adres, použitých protokolech a užívaných programech. Pokud by jsme měli MAC adresy zadány v centrální aplikaci pro správu VLAN a připojili bychom novou stanici k nepřidělenému portu switche, tak databáze pro správu VLAN vyhledá MAC adresu

zařízení a nakonfiguruje daný port do správné VLAN. Switch tedy při pohybu uživatelů automaticky určí danou VLAN do které patří a daný port poté nakonfiguruje. Tato metoda však vyžaduje značné množství práce při prvotní naplnění databáze MAC adres. [5]

## 4.2 Identifikace sítí VLAN

Port switche může patřit pouze jediné síti VLAN, jde-li o přístupový port, anebo ke všem sítím VLAN, pokud jde o trunkový port. Port lze tedy nastavit jako přístupový, nebo jako trunkový. Můžeme však aktivovat protokol DTP (Dynamic Trunking Protocol), který nastaví režim portu vyjednáváním s portem na druhém konci linky.

### 4.2.1 Přístupové porty

Patří pouze do jediné VLAN a přenáší jen provoz této sítě. Provoz je přijímán a odeslán v nativním formátu, bez jakéhokoliv značkování sítě VLAN. Doručená data na tento port se považují za data, která patří do dané sítě. Pokud však port přijme označený paket např. 802.1Q bude takový paket zahozen. Přístupový port totiž nekontroluje zdrojovou adresu a tak lze značkováný provoz přijímat pouze na trunkových portech.

Žádná zařízení připojené k tomuto portu nemají přehled o svém členství ve VLAN a předpokládá, že je součástí stejné všesměrové domény, nezná širší kontext a tak nerozumí fyzické topologii. [5]

### 4.2.2 Trunkové porty

Je to dvoubodové spojení mezi switchi, switchem a routem nebo serverem a switchem, která přenáší provoz více sítí VLAN současně. Tento port se tedy může zapojit do více sítí VLAN zároveň. Server tak například můžeme nastavit do dvou samostatných všesměrových domén současně a tím nám odpadne router pro přístup uživatelů na tento server. Při připojení switchů pomocí trunkového portu pak umožníme komunikaci uživatelů ve stejných VLAN, ale zapojených na jiných switchích. [5]

## 4.3 Značkování rámců

Při propojení více switchů a jejich VLAN musí být možnost sledovat všechny uživatele a rámce při jejich přenosu v přepínané síti a sítích VLAN. K tomuto využíváme značkování rámců. Tato metoda přiřazuje každému rámci jedinečnou uživatelsky definovanou hodnotu ID. Switch při doručení rámce nejdříve zjistí ID sítě VLAN a poté

informací z filtrovací tabulky určí, co s rámcem dále provede. Jakmile dosáhne tento rámeček cílového přístupového portu odpovídajícího ID sítě VLAN, je ID sítě VLAN odstraněno. Toto zajistí, aby cílové zařízení nemuselo rozumět identifikátorům VLAN.

Trunkové porty však mohou pracovat se značkami i bez nich. Trunkovému portu je totiž přiřazen výchozí identifikátor portu sítě VLAN, ve kterém se bude přenášet veškerý provoz bez značek. Tato síť je označena jako nativní VLAN a ve výchozím stavu má označení VLAN 1. Předpokládá se tedy, že rámeček bez značky patří do sítě VLAN 1 a může komunikovat pouze v této VLAN. Ostatní data pro další VLAN však již musí být označena, jinak by skončila ve VLAN 1. [5]

## 4.4 Metody identifikace VLAN

Identifikace umožňuje sledovat všechny rámce při průchodu sítí. Switche zjišťují, jaké rámce patří do které sítě VLAN. Máme k dispozici tyto metody:

### 4.4.1 Inter-Switch Link

Dovoluje explicitně značkovat síť VLAN do rámce Ethernet. Toto umožňuje multiplexování sítí VLAN v trunkové lince pomocí externí metody zapouzdření, díky čemuž dokáže switch identifikovat příslušnost rámce k VLAN po trunkové lince. Je-li Inter-Switch Link aktivní, lze propojit více switchů a zachovat informace sítí VLAN při přenosu po trunkových linkách. Inter-Switch Link pracuje tak, že na druhé vrstvě zapouzdřuje datový rámeček s novou hlavičkou a kontrolním součtem CRC. Jedná se o Cisco technologii. [5]

### 4.4.2 IEEE 802.Q

Je to standardní metoda značkování rámců a značkování probíhá pomocí vkládání pole do rámců, jenž identifikují VLAN. Princip je následující. Nejprve určíme port, jenž se bude používat jako trunkový. Poté přiřadíme portům konkrétní ID sítě VLAN. Porty, které následně patří do stejné trunkové linky, vytvářejí skupiny v rámci této sítě VLAN.

## 4.5 Inter-VLAN Routing

Pokud máme vytvořené síť VLAN a chceme mezi nimi komunikovat, musíme použít zařízení, které pracuje na 3. vrstvě modelu ISO/OSI a je tedy schopné pracovat s IP adresami. Použít tedy můžeme router, anebo switch pracující na 3. vrstvě.

Také máme dva způsoby fyzického zapojení:

- Pro každou VLAN použít vlastní port – Toto zapojení má výhodu v tom, že celá šířka pásma je vyhrazena pouze pro jednu VLAN. Pro propojení switchu a routeru se používá access mode. Nevýhodou je však cena takového řešení. Jestliže máme rozsáhlejší síť, potřebovali bychom desítky portů a další kabeláže
- Jeden port pro všechny VLAN – Pro zapojení používá trunkový port, který umožní komunikaci všech VLAN sítí přes jediný kabel. Z toho plynou výhody i nevýhody. Výhodou je menší množství kabeláže a cena zařízení, které nepotřebují takové množství portů. Nevýhodou je pak to, že všechny VLAN se musí podělit o danou šířku pásma a tak zde může vzniknout hrdlo, které bude brzdit provoz

## 4.6 Protokol VTP

Tento protokol byl vytvořen pro lepší správu sítí VLAN a jednodušší přidávání a odstraňování dalších VLAN sítí. Informace o změně VLAN se rozšíří všem switchům v doméně VTP (VLAN Trunking Protocol).

Základem tohoto protokolu je server VTP. Servery VTP však mohou sdílet informace pouze na doméně se stejným názvem a switchu mohou být v daném okamžiku pouze v jedné doméně. Pokud jsou však všechny switchy v jedné VLAN, není tento protokol potřebný.

Switchy detekují nové VLAN podle informací z protokolu VTP. Následně na trunkových portech připraví informace o nové síti VLAN. Aktualizace se posílají jako čísla revizí a tato jsou tvořena číslem oznámení navýšeným o jednotku. Pokud switch zjistí, že se číslo revize zvýšilo, odvodí z toho, že jsou k dispozici novější informace a přepíše tak stávající obsah databáze VTP. [5]

Máme následující 3 režimy činnosti v doméně VTP:

**Server:** V každé doméně musí být minimálně jeden server, jenž šíří informace o sítích VLAN pro danou doménu. Switch se musí také nacházet v serverovém režimu a to proto, aby byl schopný měnit informace o sítích VLAN v doméně STP. Jakákoliv změna v serverovém režimu VTP je rozeslána do celé domény. Všechny konfigurace sítí VLAN jsou uloženy v NVRAM (Non-volatile random-access memory).

**Klient:** V tomto režimu přijímají informace ze severů, ale zároveň přijímají i odesílají aktualizace, chovají se tedy podobně jako servery, ale neumožňují spravovat síť VLAN. Nelze ani přidat nové porty dřív, než novou síť VLAN oznámí server v aktualizaci. Informace o VLAN se v tomto režim neukládají do NVRAM a tak v případě resetu, jsou všechny informace o VLAN odstraněny

**Transparentní:** V tomto režimu se switch neúčastní domény VTP a nesdílejí databázi VLAN. Mohou však předávat aktualizace přes trunkové porty. Vytváření a upravování VLAN je zcela v jejich kompetenci, protože mají svou vlastní databázi a tu neposkytují ostatním switchům. V zásadě slouží pro přijetí databáze vzdálenějšího switche od VTP serveru prostřednictvím právě tohoto switche, který informaci pouze předává.

## **II. PRAKTICKÁ ČÁST**

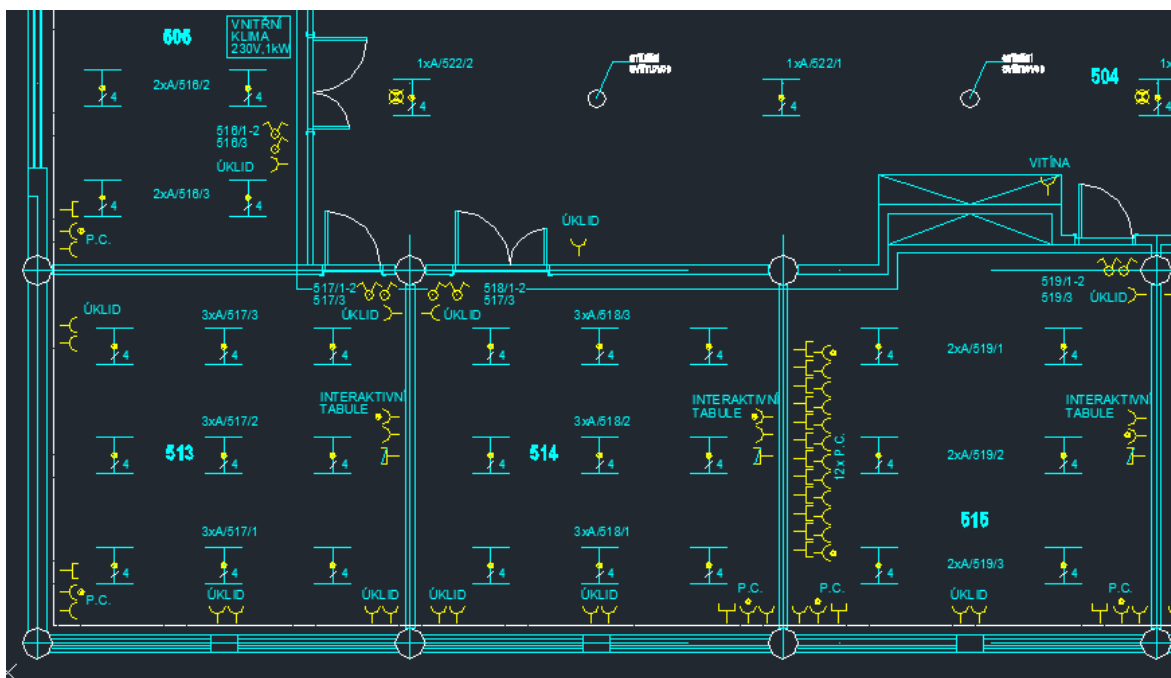
## 5 ANALÝZA SOUČASNÉHO STAVU

### 5.1 Požadavky na síť

Síť musí být schopna přenášet velké objemy dat, protože na pracovních stanicích se budou spouštět výukové programy ze serveru. Nejprve je počítáno s jednou počítačovou učebnou v místnosti 515 a později i v místnosti 507. Další počítače budou používat učitelé a to v kabinetech a učebnách 506, 507, 513-515. Tyto budou sloužit především pro komunikaci s interaktivní tabulí. Nachází se zde též síťová tiskárna a v místnosti 505 malá knihovna, ve které jsou umístěny 4 počítače pro studenty. Síť je pak doplněna o Wi-Fi pro větší komfort studentů a učitelů.

### 5.2 Původní dokumentace

Projektová dokumentace současného stavu je absolutně nevyhovující. Z velké části dokumentace neodpovídá skutečnosti. Původní plány se nacházejí v příloze I. Jako ukázkou zde uvádím výřez daných plánů.

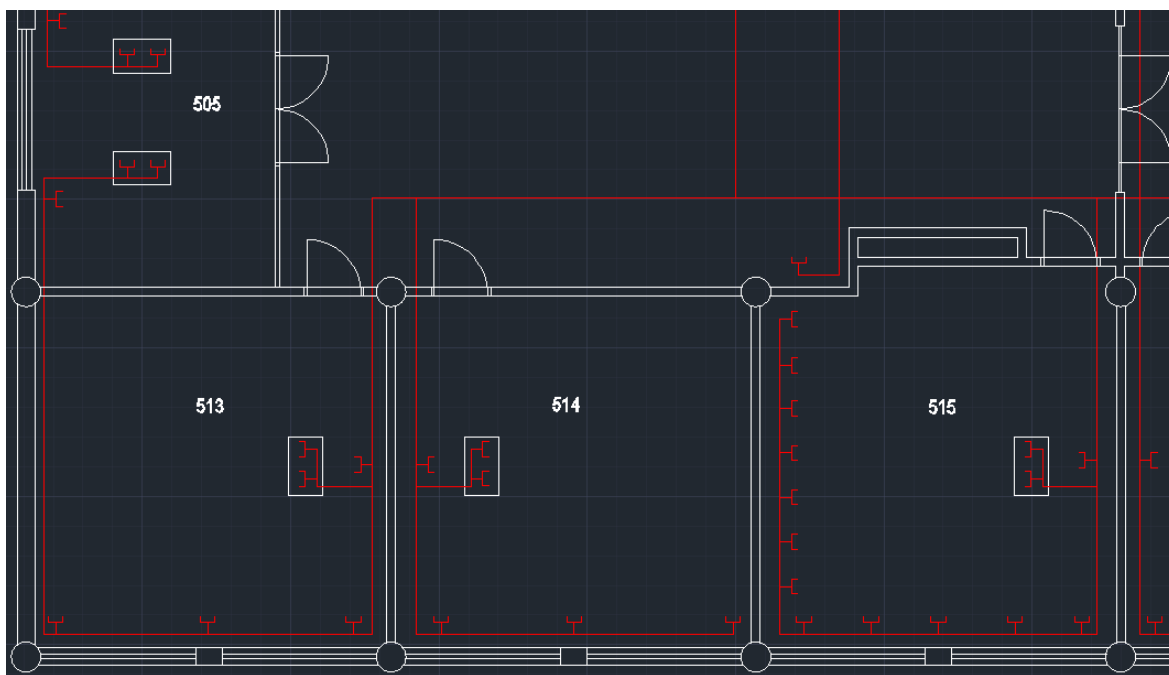


Obr. 7. Původní plány.

Hlavním problémem jsou použité barvy. Pokud se tyto plány vytisknou, budou zde žluté prvky mít po vytištění světle šedou barvu, které nejde téměř vůbec přečíst. Další problém představují špatně nakreslené stěny, kde jsou zbytečně umístěny osy sloupů a další nesouvisející čáry. Také zde není zakreslena kabeláž k jednotlivým prvkům. Není zde

též myšleno na učitelské počítače ve třídách, které budou komunikovat s interaktivní tabulí a ani s počítači v knihovně, které jsou umístěny uprostřed a ne u oken. Nepočítá se zde ani s možností počítačové učebny v místnosti 507. Celkově by v objektu mělo nahlížet 37 zásuvek UTP, ve skutečnosti je zde však 77 zásuvek. Tento rozdíl vznikl zasahováním do projektu při výstavbě.

### 5.3 Dokumentace aktuálního stavu



Obr. 8. Plány odpovídající skutečnosti.

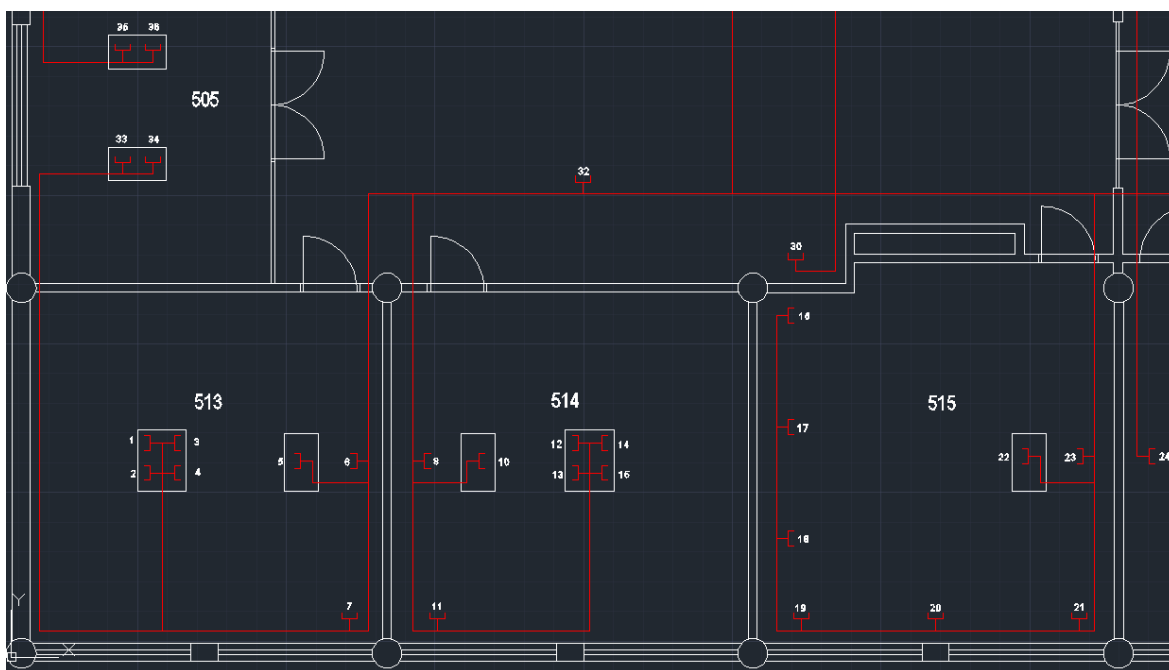
Opět zde uvádím výřez plánů, které teď ovšem odpovídají skutečnosti. Úplné plány se nacházejí v příloze II. Jak vidíme, plány jsou kresleny barvami, které po vytisknutí budou mít na papíře černou barvu. Také přibily podlahové krabice, které jsou umístěny v učebnách 505, 506, 507, 513, 514 a 515. V místnosti 505 jsou tyto podlahové krabice umístěny kvůli počítačům, které budou v prostoru. V ostatních místnostech budou sloužit pro připojení učitelského počítače do sítě. V místnosti 509 bylo realizováno 7 zásuvek, i když je zde místo maximálně pouze pro pár počítačů. Opět zde není počítáno s druhou počítačovou učebnou v místnosti 507, ani se sítí Wi-Fi. Celkově je zde umístěno mnoho zásuvek, které v budoucnu nebudou mít žádné využití.

Fyzicky je síť řešena pomocí UTP cat. 6, kde server je umístěn v místnosti 518. Odtud vede kabeláž na chodbu, a je vedena po celé délce chodby. Poté odbočuje do jednotlivých místností. V těchto místnostech je dovedena až téměř k oknům, kde je pomocí husích krků

přivedena do sádrokartonové příčky a odtud vede do parapetního žlabu, kde je následně kabeláž dovedena až na své místo. Díky dutým podlahám je instalace podlahových krabic jednoduchá. Stačí pouze na správné místo dovést kabeláž v ochranné trubce a vyříznout díru do podlahy.

## 6 NÁVRH ŘEŠENÍ POČÍTAČOVÉ SÍTĚ

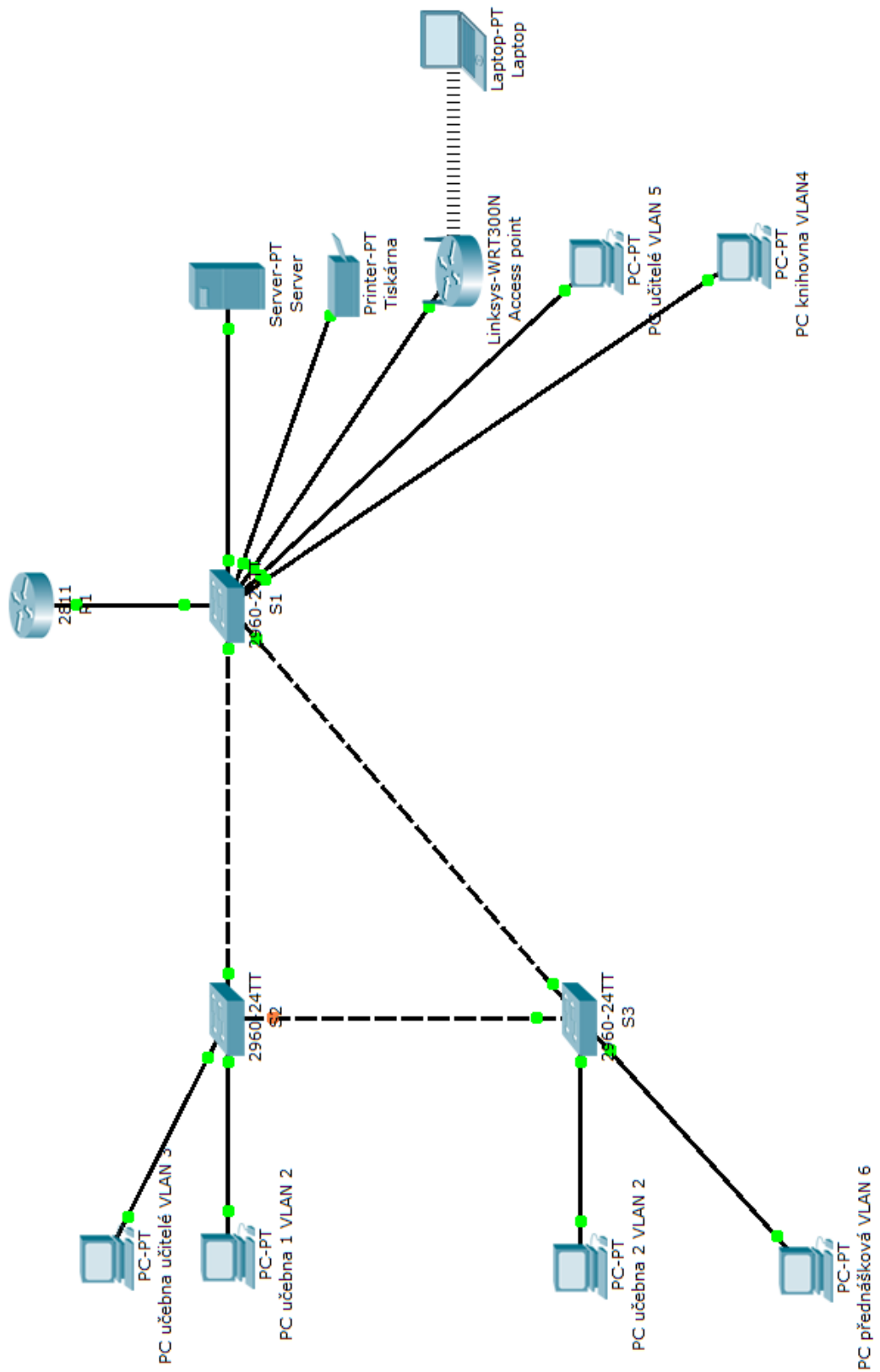
V návrhu jsem počítal s počítačovou učebnou v místnosti 507. Také jsem odstranil zásuvky v učebnách, které jsou umístěny pod okny, a nechal jsem pouze jednu rezervní. Ušetřené zásuvky jsem přesunul do podlahových krabic doprostřed místností, kde je v budoucnu lze použít pro vytvoření dalších počítačových učeben. Zredukoval jsem zásuvky v místnosti 509 na 2 a odstranil jsem zásuvky z učeben 508, 516 a 517, ve kterých jsem nechal pouze zásuvku pro možné připojení učitelského počítače. Také jsem zrušil zásuvky v čekárně a to z důvodu větší bezpečnosti sítě. Zrušil jsem též dvě zásuvky v místnosti 505 umístěné pod okny. Ve všech podlahových krabicích určených pro připojení učitelských PC, jsem nechal pouze jednu zásuvku. V místnosti 506, která bude sloužit jako přednášková a bude též pronajímána, jsem zvýšil počet zásuvek pomocí podlahových krabic. Také jsem umístil dvě zásuvky na chodbu do podhledu, které budou sloužit pro připojení AP. Zásuvky číslo 30 a 31 budou sloužit pro připojení tiskáren. Celkově je zde naprojektováno 70 zásuvek. Úplné plány jsou v příloze III.



Obr. 9. Návrh řešení PC sítě.

Serverová místnost je umístěna v místnosti číslo 518, která bude sloužit i jako sklad. Od skladu budou mít klíče jen předem vybraní lidé a tak bude zabezpečeno, že se k síťovým prvkům nedostanou nepovolané osoby.

### 6.1 Schéma zapojení sítě



Obr. 10. Schéma zapojení sítě.

## 7 VÝBĚR PASIVNÍCH PRVKŮ

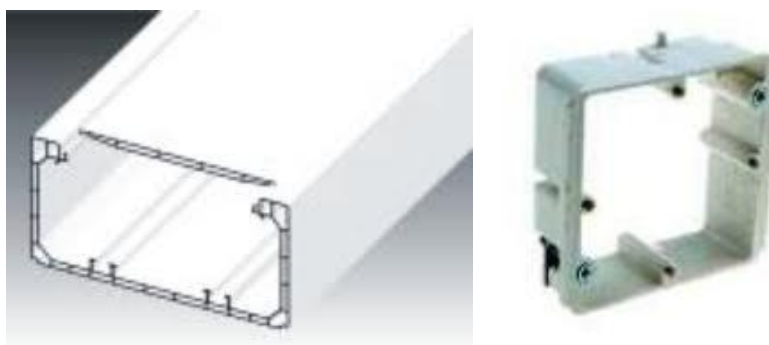
Prvky jsou vybrány tak, aby splňovali požadavky kladené na síť a to především na rychlost. Prvky jsou vybrány jen od ověřených výrobců.

### 7.1 Kroucená dvoulinka Cat6

Kroucená dvoulinka kategorie 6 je schopná fungovat v gigabitových sítích typu 1000 Base-TX. V dnešní době je to již nejpoužívanější druh kabeláže v nově budovaných rozvodech počítačové sítě. Je však zpětně kompatibilní a tak není problém připojit i starší zařízení. Pro dodržení rychlosti 1000 Base-TX nesmí horizontální kabeláž přesáhnout 90m. Pro rychlosti 10GBASE-T pak nesmí být celková délka kabeláže větší jak 30m. Pro rychlost 1Gb/s by šla též použít kabeláž kategorie 5e, ale jelikož cenový rozdíl mezi touto kategorií a kategorií 6 je minimální, rozhodl jsem se proto pro kategorii 6.

### 7.2 Parapetní žlab MALPRO EIP 110x60

Kabeláž bude vedena v těchto žlabech po celé budově. Musí být zvolen větší typ 110x60 a to proto, že v žlabu bude souběžně vedena i silnoproudá kabeláž od zásuvek. Silnoproudé kabely a slaboproudé kabely budou odděleny přepážkou. V místech určených projektem, kde budou umístěny zásuvky, se umístí instalační krabice, která umožní montáž zásuvky. Parapetní žlaby budou vedeny přímo pod parapety, kde budou do zdiva uchyceny pomocí hmoždinek o průměru 12mm a použitím příslušně velkého vrutu. Uchycení by mělo být prováděno přibližně po 1 metru a jak v horní tak i spodní části parapetu. V místech, kde parapetní žlab bude veden po sádrokartonové přičce, se pro uchycení použijí hmoždinky do sádrokartonu, tyto však mají menší nosnost a protože se musí kotvení provádět po 30-50 centimetrech. Pro finální úpravu se mezi stěnu a parapetní žlab aplikuje silikon, který zakryje i drobné nerovnosti stěn.



Obr. 11. Parapetní žlaby a instalační krabičky. [13]

### 7.3 Zásuvka pro UTP SOLARIX SX9-6-UTP-WH

Je to zásuvka určená pro 2 x RJ45 v kategorii 6 v nestíněné verzi a je určena pro instalaci na omítku případně pro parapetní žlaby. Zásuvka slouží pro ukončení horizontální kabeláže na straně uživatelů, do které se následně připojují uživatelské zařízení. V zásuvce je kabeláž ukončena pomocí keystoneů, které jsou při finální montáži pouze vsazeny do daných otvorů v zásuvce. Instalace pomocí keystoneů je efektivnější z toho důvodu, že keystoney se dají zapojovat snadněji než přímo v zásuvce. Toto šetří čas především při finální montáži. Zásuvka je též vybavena pozicí pro umístění popisku zásuvky, do kterého se pomocí štítkovače vytiskne příslušné číslo zásuvky.

### 7.4 Keystone SOLARIX CAT6 UTP

Keystoney slouží pro ukončení horizontální kabeláže a následné umístění do zásuvky popřípadě pro umístění do podlahové krabice. Kabeláž se v něm ukončí pomocí narážecího nástroje. Na keystoneu jsou též natisknuty způsoby zapojení, což opět zjednodušuje montáž.



Obr. 12. Keystone. [13]

### 7.5 Podlahová krabice LEGRAND 89606

Slouží k vytvoření pracovního místa tam, kde nejsou v dosahu přístupné zásuvky. Instalace je velmi jednoduchá. Pouze se vyřízne montážní otvor do podlahy podle pokynů výrobce a po srovnání podlahy anhydritovým potěrem se může krabice osadit na místo. V dvojitých střepech však musíme použité kabely chránit. K tomuto účelu použijeme zemní ohebnou trubku KOPOFLEX, která je dostatečně pevná a také nám oproti instalační ohebné trubce snáze umožní protažení dalších kabelů.



Obr. 13. Podlahová krabice. [13]

## 7.6 Patch panel SOLARIX 24 portů UTP 1U, CAT6

Patch panel nemá v sítích žádný vliv na jejich funkčnost. Jeho jedinou funkcí je propojení zásuvek s aktivními prvky v síti. Při použití patch panelu se zpřehlední a zefektivní údržba dané sítě, protože její správce dostane přehled o tom, který uživatel je připojený na jaký aktivní prvek. Kabel se připojí ze zadní části panelu a ve přední části jsou poté umístěny konektory RJ45, které umožní propojení s aktivními prvky. Vybraný patch panel má 24 portů pro UTP kategorie 6 a zabírá 1U v racku. Šlo by použít i 48 portové patch panely, tyto však vycházejí draž než dva patch panely s 24 porty.



Obr. 14. Patch panel. [13]

## 7.7 Rack Tritón 60x80, 45U

Je to rozvodná skříň, ve které jsou umístěny všechny důležité prvky, jako je router, switch, server, ale i například patch panel. Rack musí též obsahovat dostatečně prostoru pro všechny komponenty, případně i pro další růst sítě. Rack je opatřen skleněnými

předními dveřmi, které se dají uzamknout a znemožní tak přístup nepovolaným osobám k zařízením umístěným uvnitř. Z důvodu elektrické bezpečnosti, musí být rack uzemněn zelenožlutým kabelem o průměru 6mm, který je ukončen v rozvodné skříňce s jističí.



*Obr. 15. Rack .[13]*

## 8 VÝBĚR AKTIVNÍCH PRVKŮ

Na aktivní prvky jsou především kladeny nároky na rychlost a to z toho důvodu, že v síti se budou spouštět učební programy ze serveru na pracovních počítačích. Dalším kritériem je spolehlivost celého systému.

### 8.1 Router Cisco 2901/K9

Router od firmy Cisco má 2 porty RJ 45 podporující rychlosti až do 1Gb/s, jeden port pro konzoly, jeden pro AUX port a také má 9 rozšiřitelných slotů. V racku zabírá 1U. Router též podporuje řadu dalších technologií jako firewall, AAA (Authentication, Authorization and Accounting), SNMP (Simple Network Management Protocol) a mnoho dalších. Router bude v síti především směřovat provoz mezi sítěmi VLAN a také na něm bude zprovozněn firewall.

- Počet portů: 2
- Počet USB: 3
- Velikost v racku: 1U
- Počet rozšiřitelných slotů: 9
- Paměť: 512MB
- Maximum paměti: 2,5GB
- Operační systém: IOS



Obr. 16. Router Cisco 2901/K9. [14]

### 8.2 Switch Cisco SG 200-26

Je to 24 portový switch, s dvěma porty pro připojení dalších switchů a dvěma optickými moduly SFP. Switch zvládá rychlosti až 1Gb/s.

- Počet portů: 24
- Maximální přenosová rychlost: 52Gb/s
- Počet VLAN: 128

- Velikost tabulky adres: 8000
- Velikost paměti: 128MB
- Velikost v racku: 1U
- Podpora filtrování MAC adres: Ano



Obr. 17. Switch Cisco SG 200-26. [14]

### 8.3 Access point Linksys EA2700

Jedná se o Wi-Fi router pracující na frekvencích 2,4 a 5GHz a podporující základní Wi-Fi standardy.

- Pracovní frekvence: 2,4GHz, 5GHz
- Externí antény: Ne
- Rychlost Wi-Fi: 300Mb/s
- Wi-Fi standardy: 802.11a, 802.11b, 802.11g, 802.11n
- Šifrování: WEP, WPA, WPA2



Obr. 18. Linksys EA2700. [15]

#### 8.4 UPS Eaton 5PX 2200i RT2U

Je to nepřerušitelný zdroj energie, který zabezpečí nepřetržitou dodávku elektrické energie. Zabezpečuje tak zařízení proti výpadkům elektrické energie, popřípadě dokáže pokrýt možné výkyvy elektrické sítě.

- Kapacita: 2200VA
- Výkon: 1980W
- Počet zásuvek: 9
- Velikost v racku: 2U



*Obr. 19. UPS Eaton 5PX. [15]*

## 9 NASTAVENÍ AKTIVNÍCH PRVKŮ

Aktivní prvky byly programovány v programu Cisco Packet Tracer ve verzi 5.3.3.0019 konfigurace switchů 2 a 3 jsou uvedeny v přílohách. Simulace sítě je v příloze IV.

### 9.1 Nastavení switchu S1

```
Switch>enable //Zapne privilegovaný mód
Switch#configure terminal //Zapne konfigurační mód
Switch(config)#hostname S1 //Změní jméno switchu na S1
S1(config)#enable secret Heslo //Nastaví heslo do konfiguračního módu
S1(config)#ip default-gateway 192.168.99.1 //Nastavení výchozí brány
S1(config)#line console 0
S1(config-line)#password Heslo1 //Nastavení Hesla pro consoly
S1(config-line)#login //Aktivování loginu
S1(config-line)#line vty 0 15
S1(config-line)#password Heslo2 //Nastavení hesla pro vty
S1(config-line)#login //Aktivování loginu
S1(config-line)#exit
S1(config)#interface range fa0/1-24 //Výběr portů v rozsahu 1-24
S1(config-if-range)#shutdown //Vypnutí portů
S1(config)#interface range gi1/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#vtp mode server //Nastavení módu VTP
S1(config)#vtp domain Skola //Nastavené jména VTP
S1(config)#vtp password Lingua //Nastavení hesla VTP
S1(config)#interface range gi1/1-2
S1(config-if-range)#switchport mode trunk //Přiřazení trunkových portů
S1(config-if-range)#switchport trunk native vlan 99 //Přiřazení VLAN
S1(config-if-range)#no shutdown //Zapnutí portů
S1(config)#interface range fa0/1-3
S1(config-if-range)#switchport mode trunk //Přiřazení trunkových portů
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config)#vlan 2 //Vytvoření VLAN
S1(config-vlan)#name pc_ucebny //Pojmenování VLAN
S1(config-vlan)#vlan 3
S1(config-vlan)#name pc_ucebny_ucitele
```

```
SI(config-vlan)#vlan 4
SI(config-vlan)#name knihovna
SI(config-vlan)#vlan 5
SI(config-vlan)#name ucitele
SI(config-vlan)#vlan 6
SI(config-vlan)#name prednaskova
SI(config-vlan)#vlan 7
SI(config-vlan)#name wifi
SI(config-vlan)#vlan 99
SI(config-vlan)#name sprava
SI(config-vlan)#exit
SI(config)#interface vlan 99
SI(config-if)#ip address 192.168.99.2 255.255.255.0 //Přiřazení IP VLAN
SI(config-if)#no shutdown
SI(config-if)#exit
SI(config)#interface fa0/4
SI(config-if)#switchport mode access //Přiřazení módu access
SI(config-if)#switchport access vlan 7 //Přiřazení portu VLAN 7
SI(config-if)#no shutdown
SI(config-if)#interface range fa0/5-14
SI(config-if-range)#switchport mode access
SI(config-if-range)#switchport access vlan 5
SI(config-if-range)#interface fa0/14
SI(config-if)#no shutdown
SI(config-if)#interface range fa0/15-18
SI(config-if-range)#switchport mode access
SI(config-if-range)#switchport access vlan 4
SI(config-if-range)#interface fa0/18
SI(config-if)#no shutdown
S3(config-if)#exit
SI(config)#spanning-tree vlan 1 priority 4096 //Změna priority STP
SI(config)#spanning-tree vlan 2 priority 4096
SI(config)#spanning-tree vlan 3 priority 4096
SI(config)#spanning-tree vlan 4 priority 4096
SI(config)#spanning-tree vlan 5 priority 4096
SI(config)#spanning-tree vlan 6 priority 4096
SI(config)#spanning-tree vlan 7 priority 4096
SI(config)#spanning-tree vlan 99 priority 4096
SI(config)#int range fa0/5-18
SI(config-if-range)#switchport port-security //Zapnutí zabezpečení portů
```

```
SI(config-if-range)#switchport port-security maximum 1 //Nastavení maximálního počtu MAC adres
SI(config-if-range)#switchport port-security mac-address sticky //Způsob přiřazování MAC adres
SI(config-if-range)#switchport port-security violation shutdown //Vypnutí portu při porušení pravidel
SI(config-if-range)#end
SI#copy running-config startup-config //Uložení konfigurace
```

## 9.2 Nastavení routru R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#enable secret Heslo
R1(config)#line console 0
R1(config-line)#password Heslo1
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password Heslo2
R1(config-line)#login
R1(config-line)#exit
R1(config)#interface fa0/0
R1(config-if)#no shutdown
R1(config-if)#interface fa0/0.1 //Výběr subportu pro VLAN
R1(config-subif)#encapsulation dot1Q 1 //Výběr způsobu zapouzření
R1(config-subif)#ip address 192.168.1.1 255.255.255.0 //Nastavení IP adresy pro subport
R1(config-subif)#interface fa0/0.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#interface fa0/0.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#ip address 192.168.3.1 255.255.255.0
R1(config-subif)#int fa0/0.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#ip address 192.168.4.1 255.255.255.0
R1(config-subif)#int fa0/0.5
R1(config-subif)#encapsulation dot1Q 5
R1(config-subif)#ip address 192.168.5.1 255.255.255.0
R1(config-subif)#int fa0/0.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#ip address 192.168.6.1 255.255.255.0
```

```

R1(config-subif)#int fa0/0.7
R1(config-subif)#encapsulation dot1Q 7
R1(config-subif)#ip address 192.168.7.1 255.255.255.0
R1(config-subif)#int fa0/0.99
R1(config-subif)#encapsulation dot1Q 99 native
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#end
R1#copy running-config startup-config

```

### 9.3 Nastavení AP

The screenshot shows the 'Internet Setup' page of a Linksys WRT300N router. The 'Internet Connection type' is set to 'Static IP'. The IP address is 192.168.7.10, the subnet mask is 255.255.255.0, and the default gateway is 192.168.7.1. All DNS settings are set to 0.0.0.0.

Field	Value
Internet Connection type	Static IP
Internet IP Address:	192 . 168 . 7 . 10
Subnet Mask:	255 . 255 . 255 . 0
Default Gateway:	192 . 168 . 7 . 1
DNS 1:	0 . 0 . 0 . 0
DNS 2 (Optional):	0 . 0 . 0 . 0
DNS 3 (Optional):	0 . 0 . 0 . 0

Obr. 20. Nastavení IP adresy routeru.

The screenshot shows the 'Basic Wireless Settings' page of a Linksys WRT300N router. The network mode is 'Mixed', the SSID is 'Lingua', the radio band is 'Auto', the wide channel is 'Auto', and the standard channel is '11 - 2.462GHz'. The SSID broadcast is enabled.

Field	Value
Network Mode:	Mixed
Network Name (SSID):	Lingua
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	11 - 2.462GHz
SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Obr. 21. Nastavení jména a frekvence.

The screenshot shows the configuration interface for a Linksys WRT300N router. The page title is "Wireless-N Broadband Router WRT300N" and the firmware version is "v0.93.3". The navigation menu includes "Setup", "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", and "Status". The "Wireless Security" sub-menu is active, showing options for "Basic Wireless Settings", "Wireless Security", "Wireless MAC Filter", and "Advanced Wireless Settings".

The "Wireless Security" section is expanded, showing the following configuration options:

- Security Mode: WPA2 Enterprise
- Encryption: AES
- RADIUS Server: 192 . 168 . 99 . 5
- RADIUS Port: 1645
- Shared Secret: HesloAP
- Key Renewal: 3600 seconds

A "Help..." link is visible on the right side of the configuration area.

Obr. 22. Nastavení komunikace pro RADIUS server.

Nastavení AP bylo zvoleno po předchozím skenování prostor, při němž bylo zjištěno, že většina okolních AP pracuje na kanálu 6. Tudíž byl zvolen kanál 11 a pro druhé AP kanál 1.

## 10 CENOVÝ ROZPOČET PROJEKTU

Rozpočet byl sestavován podle aktuálních cen z velkoobchodů a u některých komponentů z maloobchodů.

Tab. 2. Rozpočet projektu.

Položka	Typ	Množství	Cena/ks	Celkem
<b>Router</b>	Cisco 2901/K9	1	15 121,25	15 121,25
<b>Switch</b>	Cisco SG 200-26	3	5 907,33	17 722,00
<b>Access point</b>	Linksys EA2700	2	1 582,50	3 165,00
<b>UPS</b>	Eaton 5PX 2200i RT2U	1	14 585,08	14 585,08
<b>Patch panel</b>	SOLARIX 24 portů UTP 1U, CAT6	6	1 179,17	7 075,00
<b>Rack</b>	Tritón 60x80, 45U	1	9 649,17	9 649,17
<b>Kroucená dvoulinka</b>	Cat6	6 000	7,67	46 000,00
<b>Parapetní žlab</b>	MALPRO EIP 110x60	40	375,83	15 033,33
<b>Instalační krabice</b>	MALPRO 5212	32	20,42	653,33
<b>Instalační krabice do příček</b>	SEZ-CZ KUP 68	10	16,75	167,50
<b>Zásuvka pro UTP</b>	SOLARIX SX9-6-UTP-WH	43	105,00	4 515,00
<b>Keystone</b>	SOLARIX CAT6 UTP	140	39,75	5 565,00
<b>Podlahová krabice</b>	LEGRAND 89606	11	1 161,96	12 781,54
<b>Chráníčka</b>	KOBOFLEX 50	50	14,17	708,33
<b>Trubka ohebná</b>	LPFLEX 32	150	10,00	1 500,00
<b>Elektroinstalační materiál</b>		1	4 200	4 200,00
<b>Práce</b>	Rozvod kabelů	320	180	57600,00
<b>Práce</b>	Zapojení sítě	32	240	7 680,00
<b>Práce</b>	Nastavení sítě	8	450	3 600,00
<b>Celkem bez DPH</b>				227 321,54
<b>Celkem s DPH</b>				272 785,85

V ceně jednotlivých komponent je zahrnuta i marže dodavatele.

## ZÁVĚR

Nejdůležitějším faktorem pro správný návrh počítačové sítě jsou v první řadě správně zpracované plány, které budou zohledňovat aktuální, ale hlavně i budoucí požadavky na danou počítačovou síť. Pokud jsou však plány zpracovány nekvalitně, a to jak z pohledu umístění pasivních prvků, tak i z pohledu špatného nakreslení plánů, budou se tyto plány během stavby neustále upravovat a může v návrhu vzniknout velké množství nelogičností, které si vynutí dodatečné náklady na síť.

Důležitou roli v návrhu sítě hraje i výběr pasivních prvků a to především kabeláže, která nám určí, jakou rychlost bude síť mít a jaké aktivní prvky musíme pro danou rychlost sítě zvolit. Cenový rozdíl mezi jednotlivými kategoriemi UTP není velký, ale velký rozdíl v ceně je poté v pasivních a aktivních prvcích sítě. Proto si při návrhu sítě musíme zjistit požadavky zadavatele, který musí jasně definovat, kolik je ochotný do sítě investovat a jaké by měla splňovat požadavky.

Při návrhu sítě také musíme brát v úvahu bezpečnost této sítě. Musíme dostatečně zabezpečit Wi-Fi síť, a to pokud možno přes RADIUS server, který nám zaručí téměř stoprocentní zabezpečení. Také ale musíme zabezpečit fyzickou síť, a to buď znemožněním připojení do sítě, anebo omezení jednotlivých uživatelů. K tomu nám poslouží aktivní prvky od firmy Cisco, které nabízejí pokročilé možnosti správy zabezpečení portů. K síťové bezpečnosti také přispívá i použití sítí VLAN. Při použití sítí VLAN však musí být kvalitně zpracován návrh sítě, aby koncoví uživatelé měli přístup k síťovým zdrojům. V rozsáhlejší síti se však správa stává velmi časově náročná. Aktivní prvky od firmy Cisco však mají k dispozici technologii VTP, která tuto správu značně zjednoduší.

Práce též obsahuje celkový cenový položkový rozpočet nákladů, které by musela Jazyková škola Lingua za tuto inovaci zaplatit.

## CONCLUSION

Right prepared plans are the most important factor for right computer network design. The plans will be consider actual and mainly the future requirements for this network. If the plans are poorly developed, both in terms of passive components and also both in terms of wrong plans drawn, these plans would be continually adjusted during construction and it may occur a large number of illogicalities in the design that cost more money.

A selection of passive components plays important role in network design, especially cabling, which will determine the speed that network will have and what active elements we need to choose for selected network speed. The price difference between different categories of UTP is not too big, but big difference in price is in the passive and active elements of the network. We need to identify customer requirements already in the design of the network, he must tell how much money is ready to invest into the network and what requirements should the network meet.

We need to considerate the network security in the design of the network as well. We have to secure Wi-Fi network through a RADIUS server if possible, which guarantees near-perfect security. We need to secure the physical network also, either by disabling the network connection, or limitation of individual users. Active components from Cisco will serve us well in this way. They offer advanced options in security management of ports. Using VLANs contributes to network security too. Network design must be well prepared when using VLAN, that end users would have access to the network resources. Network management becomes time consuming for administrators in a larger network, so the active elements of Cisco use the VTP technology, which greatly simplifies the administration.

The work also contains the total price itemized budget of costs that Lingua Language School would have to pay for this innovation.

**SEZNAM POUŽITÉ 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] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-802-5131-763.
- [3] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-802-5122-365.
- [4] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.
- [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] Přenosová média a metody jejich sdílení. Topologie sítí. [online]. [cit. 2012-05-13]. Dostupné z: <http://www.cs.vsb.cz/grygarek/PS/lect0304/ps1lect2.html>
- [7] Extensible Authentication Protocol. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-05-13].
- [8] *Strukturované kabeláže* [online]. 2001 [cit. 2012-05-13]. Dostupné z: <http://www.svetsiti.cz/rubrika.asp?rid=17&tid=48>
- [9] *Fiber Optic* [online]. 2012 [cit. 2012-05-13]. Dostupné z: <http://www.age.co.za/Products/Network/FiberCableConnectors/tabid/450/language/en-US/Default.aspx>
- [10] *Products* [online]. 2012 [cit. 2012-05-13]. Dostupné z: <http://www.indiamart.com/et-tech-pvtltd/products.html>
- [11] *Keystone Jacks* [online]. 2011 [cit. 2012-05-13]. Dostupné z: <http://www.hyperline.com/catalog/keystone/>
- [12] *Routing Protocols and Concepts* [online]. 2009 [cit. 2012-05-13]. Dostupné z: <http://cisco.netacad.net/cnams/course/CourseMaterial.jsp?>
- [13] *SÍTĚ / LAN* [online]. 2012 [cit. 2012-05-22]. Dostupné z: <http://www.adiglobal.cz/iiWWW/cz/produkty113.nsf/wp/index>

- [14] *Cisco Systems* [online]. 2012 [cit. 2012-05-13]. Dostupné z:  
<http://www.provantage.com/cisco-systems~880CSCO.htm>
- [15] *Síťové prvky* [online]. 2012 [cit. 2012-05-13]. Dostupné z:  
<http://www.czc.cz/sitove-prvky/produkty>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

AAA	Authentication, Authorization, and Accounting.
ACK	Acknowledgement.
AES	Advanced Encryption Standard.
AP	Access Point.
BSS	Basic Service Set.
CRS	Cyclic Redundancy Check.
CBC-MAC	Cipher Block Chaining Message Authentication Code
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection.
CTS	Clear to Send.
DTP	Dynamic Trunking Protocol.
EAP	Extensible Authentication Protocol.
ESS	Extended Service Set.
HW	Hardware.
IP	Internet Protocol.
LAN	Local Area Network.
LEAP	Lightweight Extensible Authentication Protocol.
LED	Light-Emitting Diode.
MAC	Media Access Control.
MIMO	Multiple-Input Multiple-Output.
NAV	Network Allocation Vector.
NVRAM	Non-Volatile Random-Access Memory.
OSI	Open Systems Interconnection.
PEAP	Protected Extensible Authentication Protocol.

---

PSK	Pre-Shared Key.
QOS	Quality of Service.
RADIUS	Remote Authentication Dial In User Service.
RST	Request to Send.
SNMP	Simple Network Management Protocol.
STP	Spanning Tree Protocol.
SW	Software.
TKIP	Temporary Key Integrity Protokol.
VLAN	Virtual Local Area Network.
VTP	VLAN Trunking Protocol.
WAN	Wide Area Network.
WEP	Wired Equivalent Privacy.
WPA	Wi-Fi Protected Access.
WPA2	Wi-Fi Protected Access II.

**SEZNAM OBRÁZKŮ**

<i>Obr. 1. Hvězdicová topologie.</i>	12
<i>Obr. 2. Stromová topologie.</i>	12
<i>Obr. 3. Optické vlákno.</i>	21
<i>Obr. 4. Optické konektory.</i>	22
<i>Obr. 5. Patch panel.</i>	24
<i>Obr. 6. Narážecí nástroj.</i>	24
<i>Obr. 7. Původní plány.</i>	39
<i>Obr. 8. Plány odpovídající skutečnosti.</i>	40
<i>Obr. 9. Návrh řešení PC sítě.</i>	42
<i>Obr. 10. Schéma zapojení sítě.</i>	43
<i>Obr. 11. Parapetní žlaby a instalační krabičky.</i>	44
<i>Obr. 12. Keystone.</i>	45
<i>Obr. 13. Podlahová krabice.</i>	46
<i>Obr. 14. Patch panel.</i>	46
<i>Obr. 15. Rack</i>	47
<i>Obr. 16. Router Cisco 2901/K9.</i>	48
<i>Obr. 17. Switch Cisco SG 200-26.</i>	49
<i>Obr. 18. Linksys EA2700.</i>	49
<i>Obr. 19. UPS Eaton 5PX.</i>	50
<i>Obr. 20. Nastavení IP adresy routeru.</i>	54
<i>Obr. 21. Nastavení jména a frekvence.</i>	54
<i>Obr. 22. Nastavení komunikace pro RADIUS server.</i>	55

**SEZNAM TABULEK**

<i>Tab. 1. Používané kanály v různých zemích. ....</i>	15
<i>Tab. 2. Rozpočet projektu. ....</i>	56

## SEZNAM PŘÍLOH

- P I: Původní plány jazykové školy – na CD
- P II: Plány odpovídající současnému stavu – na CD
- P III: Návrh plánů pro inovaci – na CD
- P IV: Simulace počítačové sítě – na CD
- P V: Konfigurační příkazy pro S2
- P VI: Konfigurační příkazy pro S3

## **PŘÍLOHA P V: KONFIGURAČNÍ PŘÍKAZY PRO S2**

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S2
S2(config)#enable secret Heslo
S2(config)#no ip domain-lookup
S2(config)#ip default-gateway 192.168.99.1
S2(config)#line console 0
S2(config-line)#password Heslo1
S2(config-line)#login
S2(config-line)#line vty 0 15
S2(config-line)#password Heslo2
S2(config-line)#login
S2(config-line)#exit
S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config)#interface range gi1/1-2
S2(config-if-range)#shutdown
S2(config-if-range)#exit
S2(config)#vtp mode client
S2(config)#vtp domain Skola
S2(config)#vtp password Lingua
S2(config)#interface range gi1/1-2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
S2#configure terminal
S2(config)#interface vlan 99
S2(config-if)#ip address 192.168.99.3 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#interface range fa0/1-11
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 2
S2(config-if-range)#interface fa0/11
S2(config-if)#no shutdown
S2(config-if)#int range fa0/12-21
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#switchport access vlan 3
S2(config-if)#int fa0/21
S2(config-if)#no shutdown
S3(config-if)#exit
S2(config)#interface range fa0/1-19
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security maximum 1
S2(config-if-range)#switchport port-security mac-address sticky
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if)#end
S2#copy running-config startup-config
```

## PŘÍLOHA P VI: KONFIGURAČNÍ PŘÍKAZY PRO S3

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S3
S3(config)#enable secret Heslo
S3(config)#no ip domain-lookup
S3(config)#ip default-gateway 192.168.99.1
S3(config)#line console 0
S3(config-line)#password Heslo1
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password Heslo2
S3(config-line)#login
S3(config-line)#exit
S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config)#interface range gi1/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit
S3(config)#vtp mode client
S3(config)#vtp domain Skola
S3(config)#vtp password Lingua
S3(config)#interface range gi1/1-2
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
S3#configure terminal
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.4 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#interface range fa0/1-11
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 2
S3(config-if-range)#interface fa0/11
S3(config-if)#no shutdown
S3(config-if)#interface range fa0/12-19
S3(config-if-range)#switchport mode access
```

```
S3(config-if-range)#switchport access vlan 6
S3(config-if-range)#interface fa0/19
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#interface range fa0/1-19
S3(config-if-range)#switchport port-security
S3(config-if-range)#switchport port-security maximum 1
S3(config-if-range)#switchport port-security mac-address sticky
S3(config-if-range)#switchport port-security violation shutdown
S3(config-if-range)#end
S3#copy running-config startup-config
```