

# **Návrh inovace a zrychlení počítačové sítě na U5 na bázi zařízení firmy Cisco**

Modernization of the computer network at U5 based on Cisco devices

Bc. Martin Orlich

---

Diplomová práce  
2012



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

\*\*\* nescannované zadání str. 1 \*\*\*

\*\*\* nescannované zadání str. 2 \*\*\*

## ABSTRAKT

Táto práca sa zaoberá návrhom modernizácie počítačovej siete budovy U5, Univerzity Tomáše Bati ve Zlíně. Tento návrh spočíva v inovácií kľúčových prvkov počítačovej siete a jej zrýchlení tak, aby počítačová sieť vyhovovala požiadavkám, ktoré na ňu budú v budúcnosti kladené.

Práca je rozdelená do niekoľko častí, pričom prvá časť popisuje technológie, ktorých popis je pre túto prácu kľúčový. V tejto časti nie sú uvedené všetky kľúčové technológie, nakoľko ich popis som spracoval v svojej bakalárskej práci, ktorá sa zaoberala technológiou prepínania a prepínačov u lokálnych počítačových sietí. Ďalšia časť práce sa zaoberá analýzou súčasného stavu počítačovej siete na FAI UTB.

Práca zároveň obsahuje návrh riešení podľa jednotlivých požiadavkou na počítačovú sieť FAI UTB. V tejto časti je zároveň popísaná práca v simulačnom prostredí Packet Tracer, ktorej výsledkom je vytvorenie konfigurácií, pre jednotlivé aktívne prvky počítačovej siete. Posledná časť práca sa zaoberá ekonomickou analýzou, ktorej cieľom je zhrnutie potrebných nákladov na navrhovanú modernizáciu počítačovej siete na U5.

Klíčová slova: U5, LAN, Cisco, modernizace, Packet Tracer

## **ABSTRACT**

The purpose of the thesis is to design an upgrade of the computer network at U5, Tomas Bata University in Zlín. This new upgrade involves modernization of the key computer network elements and its acceleration, so that computer network will meet future demands.

The thesis is divided into several sections; the first section describes technologies, which are essential for this work. In this section, they are not listed all essential technologies, because their description was mentioned in my bachelor thesis, which is about the technology of switching and switches for local area networks. Next section of this thesis analyzes current state of computer network at FAI UTB.

The thesis contains design solutions according to individual requirements for the computer network at FAI UTB. In this part is also described work in the simulation environment Packet Tracer, which results are developed configuration files for the individual active components of the computer network. The last section of the thesis considers economical analysis, which results in summarization of the costs for the designed upgrade of the computer network at U5.

Keywords: U5, LAN, Cisco, modernization, Packet Tracer

Ďakujem Ing. Miroslavovi Matýskovi, Ph.D. za možnosť spracovania tejto témy, Ing. Petrovi Vojtekovi za odborné konzultácie a rodine za podporu pri písaní tejto práce, ako i pri celom štúdiu na FAI UTB.

*„I would love to believe that when I die I will live again, that some thinking, feeling, remembering part of me will continue. But much as I want to believe that, and despite the ancient and worldwide cultural traditions that assert an afterlife, I know of nothing to suggest that it is more than wishful thinking.*

*The world is so exquisite with so much love and moral depth, that there is no reason to deceive ourselves with pretty stories for which there's little good evidence. Far better it seems to me, in our vulnerability, is to look death in the eye and to be grateful every day for the brief but magnificent opportunity that life provides. “*

*Carl Sagan*

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>11</b>
<b>I TEORETICKÁ ČASŤ</b> .....	<b>12</b>
<b>1 ŠTRUKTUROVANÁ KABELÁŽ</b> .....	<b>13</b>
1.1 HISTÓRIA ŠTRUKTÚROVANEJ KABELÁŽE .....	13
1.2 POPIS ŠTRUKTÚROVANEJ KABELÁŽE.....	14
1.3 PRVKY ŠTRUKTÚROVANEJ KABELÁŽE .....	16
1.3.1 Prepojovacie panely .....	17
1.3.2 Zásuvky .....	18
1.3.3 Prepojovacia kabeláž.....	18
1.3.4 Rozvodná skriňa.....	19
1.4 POPIS POUŽÍVANEJ KABELÁŽE .....	19
1.4.1 Metalická kabeláž.....	19
1.4.2 Optická kabeláž.....	22
1.4.3 Konektory pre metalickú kabeláž.....	24
1.4.4 Konektory pre optickú kabeláž .....	25
1.5 ŠTANDARDY OVPLYVŇUJÚCE ŠTRUKTÚROVANÚ KABELÁŽ.....	26
1.6 PROTOKOLY PRE FYZICKÉ MÉDIA .....	26
1.6.1 Protokoly pre metalickú kabeláž.....	27
1.6.2 Protokoly pre optickú kabeláž.....	27
1.7 PROTOKOL 10GBASET NA EXISTUJÚCEJ METALICKEJ KABELÁŽI.....	27
1.7.1 Špecifikácia požiadavkou káblových systémov pre 10GBaseT.....	28
<b>2 HIERARCHICKÝ SIEŤOVÝ MODEL</b> .....	<b>30</b>
2.1 FUNKCIE VRSTIEV HIERARCHICKÉHO SIEŤOVÉHO MODELU.....	30
2.2 VÝHODY HIERARCHICKÉHO SIEŤOVÉHO MODELU .....	31
<b>3 TECHNOLÓGIA CISCO ETHERCHANNEL</b> .....	<b>33</b>
3.1 VÝHODY CISCO ETHERCHANNEL.....	34
3.2 KOMPONENTY CISCO ETHERCHANNEL .....	35
3.3 MOŽNOSTI KONFIGURÁCIE ETHERCHANNEL .....	36
3.4 PRINCÍP FUNGOVANIA ETHERCHANNEL .....	36
3.4.1 Vyrovnávanie záťaže.....	38
3.4.2 Port Aggregation Protocol.....	38
3.5 LINK AGGREGATION CONTROL PROTOCOL .....	39
3.6 NIC TEAMING IEEE 802.3AD .....	39
<b>4 VOICE OVER IP</b> .....	<b>41</b>
4.1 VÝHODY PAKETOVEJ TELEFÓNIE .....	41
4.2 KOMPONENTY VOIP.....	42
4.2.1 Signalizácia .....	42
4.2.2 Databázové služby .....	43

4.2.3	Riadenie doručovania.....	43
4.2.4	Kódek.....	44
4.3	VOIP PROTOKOLY.....	44
4.4	DOSTUPNOST VOIP SLUŽBY.....	46
4.5	PROTOKOLY RTP A RTCP.....	47
4.5.1	Aplikácia RTP a RTCP.....	49
4.5.2	Kompresia RTP hlavičky.....	49
4.6	VOIP SIEŤOVÁ ARCHITEKTÚRA.....	50
4.6.1	Centralizovaná architektúra.....	50
4.6.2	Distribuovaná architektúra.....	52
4.6.3	Distribuovaná architektúra založená H.323.....	52
4.6.4	SIP Distribuovaná sieťová architektúra.....	54
4.6.5	Porovnanie sieťových architektúr.....	56
<b>5</b>	<b>ANALÝZA POČÍTAČOVEJ SIETE NA U5.....</b>	<b>58</b>
5.1	ANALÝZA CHRBTICOVEJ SIETE UTB VE ZLÍNĚ.....	58
5.2	ANALÝZA ROZVODOV NA U5.....	59
5.3	ANALÝZA AKTÍVNYCH PRVKOV SIETE.....	60
5.4	ANALÝZA BEZDRÔTOVEJ SIETE NA U5.....	63
5.4.1	Bezdrôtová sieť eduroam.....	63
5.5	ANALÝZA LOGICKÉHO ZAPOJENIA SIETE.....	64
5.6	IP TELEFÓNIA.....	66
<b>II</b>	<b>PRAKTICKÁ ČASŤ.....</b>	<b>67</b>
<b>6</b>	<b>NÁVRH MODERNIZÁCIE POČÍTAČOVEJ SIETE NA U5.....</b>	<b>68</b>
6.1	POŽIADAVKY NA MODERNIZÁCIU.....	68
6.2	NAVRHOVANÉ ZMENY.....	69
6.2.1	Prechodná modernizácia.....	69
6.2.2	Variant finálnej modernizácie č.1.....	74
6.2.3	Variant finálnej modernizácie č.2.....	79
6.3	NÁVRH LOGICKEJ ŠTRUKTÚRY.....	80
6.4	BEZDRÔTOVÁ SIEŤ.....	82
6.5	SPANNING TREE PROTOCOL A JEHO VYLEPŠENIA.....	83
6.6	SMEROVANIE MEDZI VLAN SIEŤAMI.....	84
6.7	PROTOKOL VTP A VTP PRUNING.....	84
6.8	PROTOKOLY TYPU FIRST-HOP REDUNDANCY.....	85
6.9	ZABEZPEČENIE PORTOV.....	86
6.10	RIEŠENIE VOIP.....	86
<b>7</b>	<b>SIMULÁČNÉ ZAPOJENIE NAVRHOVANEJ SIETE.....</b>	<b>88</b>

7.1	SIMULAČNÉ ZAPOJENIE .....	88
7.2	PREPOJENIE SIEŤOVÝCH PRVKOV .....	90
7.3	ZÁKLADNÉ NASTAVENIA .....	90
7.4	NASTAVENIA VLAN SIETÍ A PROTOKOLU VTP .....	92
7.4.1	Nastavenie VLAN sietí .....	92
7.4.2	Nastavenia protokolu VTP .....	94
7.4.3	Nastavenie režimov na portoch .....	95
7.4.4	VTP Pruning .....	95
7.5	SPANNING TREE PROTOCOL .....	96
7.6	ETHERCHANNEL .....	97
7.7	SMEROVANIE MEDZI VLAN SIETAMI .....	98
7.8	DHCP A DNS SERVERI .....	98
7.9	VoIP A BEZDRÔTOVÉ ZARIADENIA .....	100
7.10	NASTAVENIE PRÍSTUPOVÝCH PORTOV A BEZPEČNOSŤ .....	101
7.10.1	Nastavenie prístupových portov .....	101
7.10.2	Bezpečnostné funkcie .....	102
7.11	PROTOKOL HSRP .....	104
7.12	KONFIGURAČNÉ SÚBORY .....	105
<b>8</b>	<b>EKONOMICKÉ ZHODNOTENIE NÁVRHOV .....</b>	<b>106</b>
	<b>ZÁVER .....</b>	<b>108</b>
	<b>CONCLUSION .....</b>	<b>109</b>
	<b>ZOZNAM POUŽITEJ LITERATÚRY .....</b>	<b>110</b>
	<b>ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK .....</b>	<b>112</b>
	<b>ZOZNAM OBRÁZKOV .....</b>	<b>116</b>
	<b>ZOZNAM TABULIEK .....</b>	<b>118</b>
	<b>ZOZNAM PRÍLOH .....</b>	<b>119</b>

## ÚVOD

Počítačové siete sa stali natoľko bežnou súčasťou našich životov, že si ich prítomnosť mnohokrát ani neuvedomujeme. To, že naša obľúbená web stránka sa načíta okamžite, alebo že odoslanie a prijatie emailu je záležitosťou okamihu vďačíme práve správne navrhutej a fungujúcej počítačovej sieti.

Počítačová sieť Fakulty aplikovanej informatiky Univerzity Tomáše Bati ve Zlíně sa nachádza v budove U5. Táto počítačová sieť je pomocou optického káblu pripojená k ďalšej sieťovej infraštruktúre na U1. Štruktúra počítačovej siete sa od svojho vzniku nemenila. Realizované projekty, ktoré sa týkali počítačovej siete menili hlavne aktívne komponenty siete, pričom sa zlepšovala najmä jej funkčnosť, správa a bezpečnosť.

Masívnym rozvojom nových sieťových služieb vzniká potreba, aby počítačová sieť na U5 bola pripravená na ďalší svoj ďalší rozvoj. Stavbou vedecko-výskumného ICT parku vzniká možnosť, kedy možno navrhnuť sieť tak, aby vyhovovala budúcim požiadavkám, ktoré na ňu budú v budúcnosti kladené.

Cieľom tejto práce je vytvorenie návrhu, ktorý by realizoval modernizáciu počítačovej siete na U5 a zároveň zohľadňoval i ekonomickú stránku takéhoto projektu. Navrhované riešenie by malo navrhnuť modernizáciu ako po fyzickej tak i logickej štruktúre počítačovej siete na U5.

## TEORETICKÁ ČASŤ

## 1 ŠTRUKTUROVANÁ KABELÁŽ

Požiadavka na bezproblémový chod počítačovej siete sa nezaobíde bez kvalitnej fyzickej infraštruktúry. Je všeobecne známe, že významné množstvo problémov zlyhania siete je spôsobených vďaka problémom v kabeláži. Jedným zo spôsobov ako dosiahnuť bezproblémový chod počítačovej siete je použitie univerzálneho normovaného systému a kvalitných prvkov infraštruktúry.

Štruktúrovaná kabeláž je univerzálny systém, ktorý podporuje prenos ako analógových tak i digitálnych signálov. Prípojné body sa inštalujú tam kde sú potreba, ale i tam kde sa predpokladá ich budúca potreba. Pre vytvorenie štruktúry používa káble založené na krútenej dvojlinke a optických kábloch. Z dôvodu morálnej i technickej životnosti je potrebné, aby použitá kabeláž bola dobre dimenzovaná i pre budúce potreby organizácie.

### 1.1 História štruktúrovanej kabeláže

So vznikom prvých počítačových sietí vzniká i potreba na univerzálny systém prepojovania jednotlivých zariadení, nakoľko prví výrobcovia používali vlastné technológie a komponenty, ktoré boli navzájom nekompatibilné. Táto potreba zahŕňala zjednotenie elektrických a fyzických vlastností káblov a prepojovacieho hardwaru.

Na začiatku 90-tých rokov spoluprácou ANSI (American National Standards), TIA (Telecommunications Industry Association) a EIA (Electronic Industries Alliance) vzniká systém pre jednotnú kabeláž, ktorý je postavený na riešení americkej telekomunikačnej spoločnosti AT&T. Tá používala pre prenos dát vlastné už existujúce telefónne rozvody v administratívnych budovách. Tieto rozvody mali hviezdicovú topológiu a ako prenosové médium bola použitá krútená dvojlinka. Ako výsledok spolupráce týchto štandardizačných organizácií vzniká norma pre štruktúrovanú kabeláž, označovaná ako ANSI/TIA/EIA 568 *Commercial Building Telecommunication Cabling Standard* pričom definuje prenosové požiadavky pre kabeláž kategórie 3, 4 a 5. V roku 1995 vyšla aktualizácia tejto normy, označovaná ako ANSI/TIA/EIA 568A a zároveň aj jej medzinárodná obdoba vo forme normy ISO/IEC 11801 *Generic Customer Premises Cabling Standard*, štandardizačných organizácií ISO (International Organization for Standardization) a IEC (International Electrotechnical Commission). Rozvojom prenosových protokolov, ktoré umožňujú rýchlejšie prenosi, sú tieto normy pravidelne aktualizované. Aktualizácie definujú nové parametre, ktoré musia komponenty spĺňať, aby bolo možné dosiahnuť požiadavky nových

protokolov. Zároveň tieto štandardy boli doplnené o nové merané alebo počítané parametre ako napríklad PSNEXT (Power Sum NEXT), PSACR (Power Sum ACR), PSELFEXT (Power Sum ELFEXT), *Delay Skew* atd [1].

## 1.2 Popis štruktúrovanej kabeláže

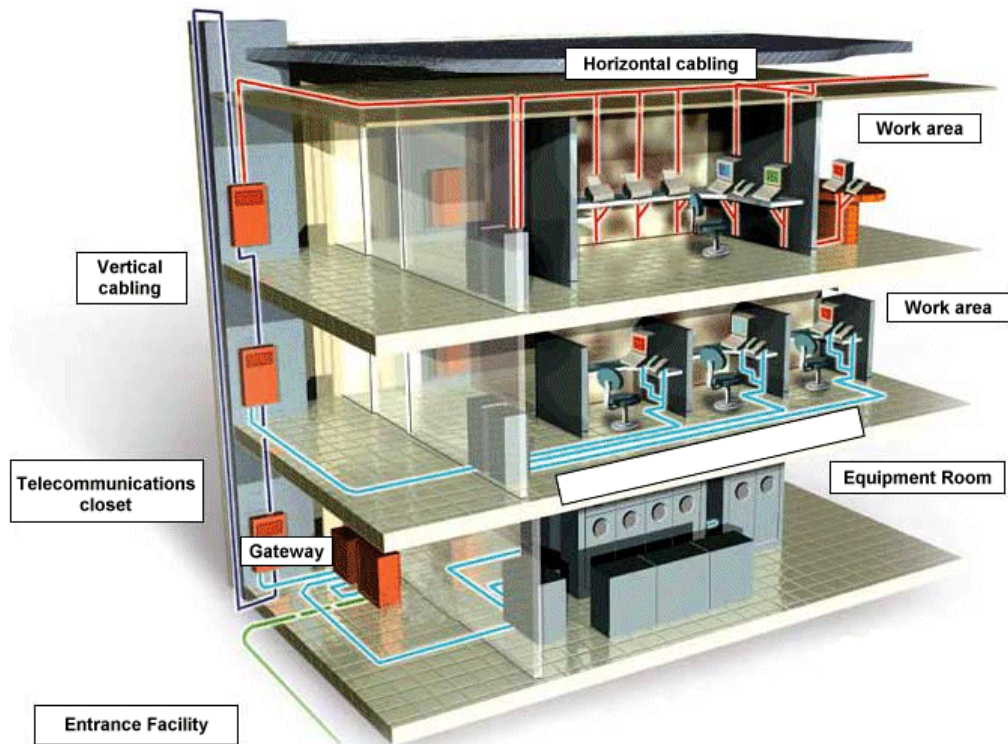
Štruktúrovaná kabeláž definuje použitie všeobecnej telekomunikačnej elektroinštalácie pre komerčné budovy pričom zahŕňa kabeláž, konektory a príslušenstvo použité pre pripojenie lokálnej počítačovej siete a zariadení telefónneho systému v rámci budovy. Charakteristickým rysom štruktúrovanej kabeláže je rozdelenie celej kabeláže do dvoch úrovní, horizontálnej a vertikálnej (tzv. *backbone*). Štandardy následne definujú typ použitého média, topológiu, ukončovacie a pripojovacie body a administratívu, ktorá má byť použitá.

Výhodou štruktúrovanej kabeláže je jej univerzálnosť a bezpečnosť. Ak sa preruší jeden kábel, má to vplyv iba na činnosť tej stanice, ktorá je pripojená daným káblu, pričom na činnosť ostatných staníc táto porucha vplyv nemá. Nevýhodou je vyššia celková dĺžka káblu a nutnosť budovania káblových tras s väčším prierezom.

Na obrázku č.1 je zobrazené klasické zapojenie podľa doporučenia TIA/EIA-586-A. Toto zapojenie je rozdelené do šiestich častí.

**Horizontálna kabeláž** je všetka kabeláž, ktorá sa nachádza medzi telekomunikačnou zásuvkou (*telecommunication outlet*) v pracovnej oblasti (*working area*) a horizontálnym prepojovačom (*patch panel*) v rozvodnej telekomunikačnej skrini (*wiring closet*). Ako už z názvu je zrejmé, je zvyčajne zapojená horizontálne v lištách na stene, stropoch, alebo v podlahe budovy pričom neprekračuje poschodie na ktorom je inštalovaná. Maximálna povolená vzdialenosť medzi rozvodnými skriňami a zásuvkami je 90 metrov, bez ohľadu na typ kábla. Ďalších 6 metrov je povolených pre prepojovacie káble (*patch cables*) v rozvodnej skrini a v pracovnej oblasti, ale celková dĺžka týchto prepojovacích káblov nesmie presiahnuť 10 metrov. Horizontálne káble by mali byť 4-párový 100  $\Omega$  UTP (Unshielded Twisted Pair) kábel (najnovšie štandardy špecifikujú kategórie 5E ako minimum), dvoj vlákňový mnohovidový 62.5/125  $\mu\text{m}$  optický kábel, alebo 50/125  $\mu\text{m}$  mnohovidový optický kábel.

**Vertikálna kabeláž** je zapojená cez podlažia budovy (cez stúpačky) alebo skrz areál a podstate ide o rozvodné skrine, vstupné zariadenia, vybavenie miestností a budov, vrátane kabeláže, ukončenie káblov, pomocné a hlavné pripojenia. Chrbticová kabeláž je inštalovaná medzi rozvodnými skriňami, vybavením miestností, vstupným vybavením na rovnakom podlaží, medzi poschodiami alebo budovami. Štandardy špecifikujú hierarchickú topológiu pre chrbticovú kabeláž v ktorej je všetka kabeláž šírená z centrálného bodu nazývaného *main distribution frame* (zvyčajne rozvodná skriňa). Každá rozvodná skriňa alebo vstupné zariadenia je priamo prepojené k *main distribution frame*, alebo cez pomocné prepojenie (*intermediate distribution frame*). Limity pre túto kabeláž závisia od použitého typu kabeláže a zariadení ktoré prepojuje (krútená dvojlinka je limitovaná na 90 metrov) [8].



Obr. 1. Model štruktúrovanej kabeláže.<sup>1</sup>

**Pracovná oblasť** (*work area*) sú priestory budovy, v ktorej pracovníci využívajú telekomunikačné zariadenia. Toto zahŕňa všetku kabeláž medzi komunikačnými

<sup>1</sup> - Obrázok použitý z [8].

zásuvkami a koncovými zariadeniami, ako sú napr. telefóny, pracovné stanice a tlačiarne, vrátane zásuviek samotných. Káblový systém je navrhnutý tak aby bol flexibilným, ale stále vyžaduje určitú mieru manažmentu. Všetky prvky štruktúrovanej kabeláže v pracovnej oblasti musia byť jednotnej normy (T568A alebo T568B), z dôvodu vyhnutia sa problémom s prekríženými párami. Štandard T568B je viac používanější pre dátové aplikácie. Tento štandard ďalej určuje dve zásuvky na každý vývod – jeden pre telefóniu a druhá pre dáta.

**Telekomunikačné rozvodne** (*wiring closets*) sú uzavretá oblasť, napr. miestnosť alebo skriňa, určená pre umiestnenie telekomunikačného vybavenia, distribučných rámov (*distribution frames*) a ukončenia káblov. Inými slovami, všetok hardware ktorý je vyžadovaný pre pripojenie horizontálne kabeláže k vertikálnej. V tejto časti môžu byť umiestnené i prídavné zariadenia, ako napr. dátové servery. Každá budova musí mať najmenej jednu rozvodňu, pričom norma odporúča jednu rozvodňu pre každé poschodie. Normovaná veľkosť rozvodne je tiež doporučená, v závislosti na oblasti služieb. Musí obsahovať dostatočne veľa priestoru pre služby personálu pre výkon údržby ako i pre požadovaný hardware. Osvetlenie, napájacie zdroje a environmentálne podmienky by mali tiež spĺňať nároky určené v štandarde.

**Miestnosť zariadení** (*equipment room*) je miesto budovy, kde sú umiestnené všetky telekomunikačné systémy ako PBX (Private Branch eXchange), servery, hlavné prepínače apod. a zároveň mechanické ukončenie systému telekomunikačnej kabeláže. Môže mať podobu samostatnej miestnosti, alebo rozvodnej skrine. Poskytuje ukončovací bod pre vertikálnu kabeláž. Pri veľkej rozlohe, každá budova môže mať vlastnú miestnosť zariadení, pričom ostatné sú miestnosti sú pripojené k jednej centrálnej, ktorá prepojuje celú štruktúrovanú kabeláž do jedného celku.

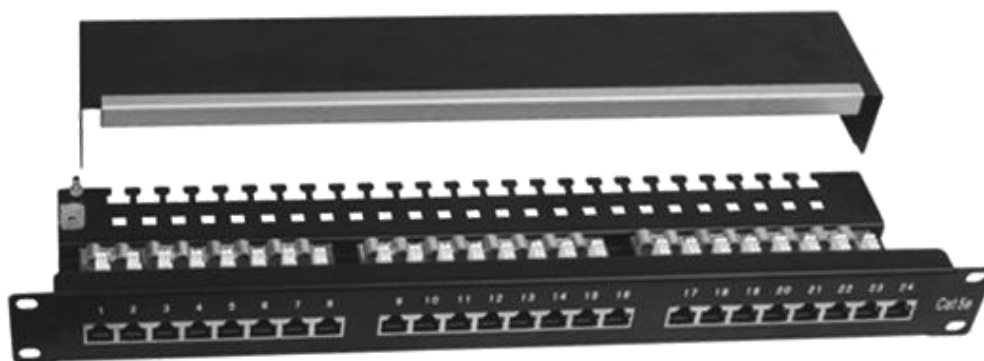
**Vstupné zariadenia** (*entrance facility*) obsahuje vstup telekomunikačnej služby do budovy a tiež môže obsahovať areálové chrbticové spojenie. Často obsahuje vymedzujúci bod (*network demarcation point*), čo je prepojenie na miestnej ústredni operátora telekomunikačných zariadení [8].

### 1.3 Prvky štruktúrovanej kabeláže

K účelu výstavby štruktúrovanej kabeláže sa používajú pasívne prvky, ktoré tvoria prepojovacie panely, zásuvky, rozvodné skrine, kabeláž a jej príslušné konektory.

### 1.3.1 Prepojovacie panely

Prepojovacie panely (*patch panels*) tvoria základný prvok štruktúrovanej kabeláže. Sú to zariadenia ktoré slúžia ako centrálné ukončenie všetkých káblov horizontálnej kabeláže. Zvyčajne bývajú inštalované v normovanej 19“ rozvodnej skrini, alebo rámoch, prípadne môžu byť inštalované i na stenu objektu.



Obr. 2. 19“ Patch panel s 24 portami RJ45.<sup>2</sup>

Samotný prepojovací panel sa skladá v podstate z dvoch častí, časť pre ukončenie horizontálnej kabeláže a portov, ktoré slúžia pre pripojenie zariadení. Tieto porty sú zvyčajne zakončené normovaným konektorom RJ45 a slúžia pre pripojenie najmä aktívnych prvkov. Časť pre pripojenie k horizontálnym rozvodom je riešená zárezovým konektorom, ktorý býva vybavený farebným kódom tak aby odpovedal farebnému kódu káblu. Panely používané najmä pre pripojenie telefónnych ústrední môžu používať i špeciálne konektory, ktoré umožňujú zapojovať jednotlivé páry kábelu oddelene (panel typ 110 alebo IDC). Panely sú dostupné v netienenom alebo tienenom prevedení. Ak ide o tienový panel, je tienenie prepojené s kostrou rozvodnej skrine, ktorá je uzemnená [2].

---

<sup>2</sup> - Obrázok použitý z FOCUS TECHNOLOGY CO., Ltd. *Made-in-China* [online]. 2012 [cit. 2012-03-23]. Dostupné z: <http://www.made-in-china.com/showroom/linkee/product-detaildoUJGazrvThX/China-24-Ports-Cat-5e-Shielded-Patch-Panel-LK-PP22-.html>

### 1.3.2 Zásuvky

Zásuvky sú ukončením horizontálnej kabeláže v pracovnej oblasti a slúžia pre pripojenie koncových zariadení. Vo svojej podstate ide o zmenšenú verziu prepojovacieho panelu ktorá je inštalovaná na steny. Každé pracovisko by malo mať minimálne dve pripojovacie miesta – čiže dve zásuvky jednoduché alebo jednu dvojité. Jedna sa potom väčšinou používa pre dáta a druhá pre telefón. V prípade dvojitej zásuvky, je dobrým zvykom aby zásuvka bola označená jedným číslom a konektory rozlíšené písmenami A a B. Tak ako i prepojovacie paneli sú zásuvky dostupné v tienenom i netienenom prevedení. Pri použití tienených zásuviek, alebo prepojovacích panelov je potrebné, aby bola i na opačnej strane boli použité tienené prvky [2].



Obr. 3. Príklad vyhotovenia zásuvky RJ45.<sup>3</sup>

### 1.3.3 Prepojovacia kabeláž

Prepojovací kábel (*patch cable*) slúži na prepojenie zásuvky a koncového zariadenia, alebo na prepojenie prepojovacieho panelu s aktívnym prvkom siete. Tieto káble sú na obidvoch koncoch osadené normovanými konektormi RJ45. Vyhotovenie prepojovacích káblov je metalická kabeláž, ktorá je popísaná v ďalšej časti.

V prípade, že prepojované zariadenia sú rovnakého typu, napr. PC + PC, je potreba aby jeden prepojovací kábel bol križený [2].

---

<sup>3</sup> - Obrázok použitý z [2].

### 1.3.4 Rozvodná skriňa

Rozvodná skriňa je normovaná skriňa, ktorá je určená pre montáž komunikačných rozvodných zariadení a aktívnych prvkov siete. Norma definuje niekoľko základných rozmerov, ktoré umožňujú kompatibilitu u pomerne širokej škále produktov. Základným rozmerom je rozteč montážnych rámov o veľkosti 19". Druhým normovaným rozmerom je rozteč medzi otvormi pre matice umiestnené na montážnych rámoch. Výška rozvodnej skrine sa uvádza v jednotkách U. Jednotka U (*Rack Unit*) má veľkosť zhruba 4,46 cm. Pre rozvodné skrine sa udomácnil názov *rack* [2].



Obr. 4. Príklady vyhotovenia 19“ rozvodných skriň.<sup>4</sup>

## 1.4 Popis používanej kabeláže

### 1.4.1 Metalická kabeláž

**Metalická** kabeláž je súčasnosti najpoužívanjšie riešenie pre horizontálnu kabeláž. Kábel je tvorený štyrmi párami krúteného drôtu (tzv. TP - Twisted Pair). Každý pár má farebné označenie definované podľa normy TIA/EIA-586-A. Páry sú od seba odlíšené farbami (modrá, zelená, oranžová a hnedá), pričom druhý drôt v páre je odlíšený pomocou bielej farby. Dôvodom pre toto farebné odlíšenie je uľahčenie inštalácie rozvodov pri osadzovaní

---

<sup>4</sup> - Obrázok použitý z [2].

zásuvek a prepojovacích panelov. Norma zároveň určuje krútenie (tzv. *twisting*) káblu. Táto metóda zlepšuje elektrické vlastností káblu, pričom sa zvyšuje odolnosť proti interferenciám s vonkajšími vplyvmi. Toto krútenie minimalizuje takzvané prieniky (z aj. *Cross-talk*) medzi párami a zároveň sa znižuje interakcia medzi dvojlinkou a jej okolím. Toto krútenie párov vytvára tzv. vlastné tienenie v kábli. Pri toku elektrického prúdu vo vodiči sa okolo vodiča vytvára elektromagnetické pole. Ak sú dva vodiče, ktoré sú súčasťou rovnakého elektrického okruhu dostatočne blízko seba, ich elektromagnetické polia pôsobia proti sebe a tým sa vzájomne potlačia.

Metalická kabeláž je vyrábaná v niekoľkých variantoch, ktoré sa odlišujú tienením a impedanciou. Tienenie tvorí ochranu pred signálmi z vonkajšieho prostredia, ale tiež i vyžarovanie do okolia, najmä pri vysokých rýchlostiach kde je frekvencia prenosu vyššia. Tienenie môže byť vyhotovené pomocou kovovej fólie, alebo ako opletenie kovovými drôtikmi.

- **UTP (Unshielded Twisted Pair)** – je najobvyčajnejším variantom krútenej dvojlinky. Káble tohto typu sú bez tienenia a pričom kábel pozostáva iba zo štyroch párov a vonkajšieho plášťa. Impedancia káblu je 100 Ω.
- **ScTP (Screened Twisted Pair)** – káble označované ako ScTP prípadne FTP (Foiled Twisted Pair) sú jednou z tienených variant krútenej dvojlinky. Toto tienenie je spoločné pre všetky páry a nachádza sa pod plastovým plášťom kábla. Samotné páry dvojlinky sú netienené. Impedancia káblu je opäť 100 Ω.
- **STP (Shielded Twisted Pair)** – tieto káble sú tiež tienenou variantom krútenej dvojlinky, pričom tienenie sa nachádza u každého páru kábla. Celý kábel tienový nie je. Impedancia káblu je 150Ω.
- **ScSTP (Screened Twisted Pair)** – sú kombináciou káblov ScTP a STP. Tienené sú ako samotné páry, tak i celý kábel. Impedancia u káblov ktoré sú označované ako ScSTP majú impedanciu 100 Ω.

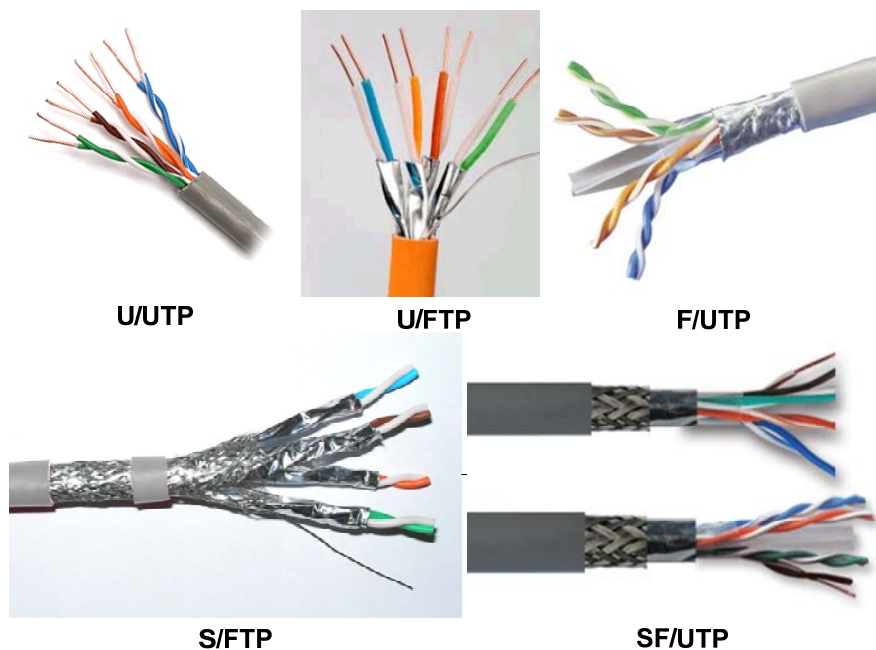
Z dôvodu nejednoznačnosti označenia u rôznych výrobcov, bola vydaná aktualizácia normy ISO/IEC 11801, ktorá definuje použitie nových názvov pre typy kabeláže. Toto nové označenie zobrazuje tabuľka č.1. Princíp označovania káblov rozložený na dve časti, pričom prvá časť na ľavo od znaku „/“, označuje tienenie kábla a druhá potom tienenie páru.

Tab. 1. Označovanie káblov podľa ISO/IEC 11801.

Staré označenie	Nové označenie	Tienenie kábla	Tienenie párov
UTP	U/UTP	-	-
STP	U/FTP	-	Fólia
FTP	F/UTP	Fólia	-
S-STP	S/FTP	Opletenie	Fólia
S-FTP	SF/UTP	Fólia, Opletenie	-

Spolu s typom káblu, existuje niekoľko kategórií krútenej dvojlinky. Tieto kategórie určujú parametre a použitie krútenej dvojlinky. V súčasnosti najvyššia kategória je č. 7, ktorej parametre sú vhodné i pre najnáročnejšie aplikácie ako napríklad 10GBase-T Ethernet.

Z dôvodu rozsiahlosti tabuľky kategórií TP káblov je tabuľka umiestnená ako príloha č.1 na CD-ROM.



Obr. 5. Typy káblov TP podľa ISO/IEC 11801.

### 1.4.2 Optická kabeláž

Súčasnosti optická kabeláž dominuje najmä u vertikálnej kabeláže, i keď u náročnejších alebo špecifických aplikáciách sa môže vyskytovať i v horizontálnych rozvodoch. Pre potreby štruktúrovanej kabeláže sa používajú existujúce dva typy optických vlákien, jednovidové (*singlemode*) a mnohovidové (*multimode*).

Medzi jednoznačné výhody optickej kabeláže v porovnaní s metalickou kabelážou je dosah optickej technológie, pretože už i TP káble kategórie CAT6 podporujú vysoko rýchlostné protokoly, ako napr. 10 Gbps Ethernet, ale len do 100 m. V závislosti na štandarde (napr. 100Base-FX alebo 1000Base-SX) je možné mnohovidové optické vlákna používať do vzdialenosti 2 km, pričom cena je o niečo vyššia ako u metalickej kabeláže. Výhodou jednovidových vlákien je vysoký dosah technológie (až niekoľko desiatok kilometrov), a schopnosť podporovať extrémne rýchle protokoly ako napr. 40GBASE-LR4, čím sa stávajú najviac vhodné pre chrbticové spoje. Ich nevýhodou je vyššia cena oproti mnohovidovým vláknám.

Dôležitým faktorom optickej kabeláže je útlm signálu, ktorý je spôsobený 2 spôsobmi a to, dĺžkou káblu a počtom spojov. Faktor útlmu je dôležitý najmä z toho dôvodu, z bez problémovej prevádzky vysokorýchlostných protokolov, pretože rôzne protokoly majú definovaný iný maximálny útlm signálu. Obecne tieto útlmy možno odhadnúť na základe pravidiel, že každý:

- 1km káblu má útlm 1 až 2 dB.
- Spoj 0,5 až 2 dB.

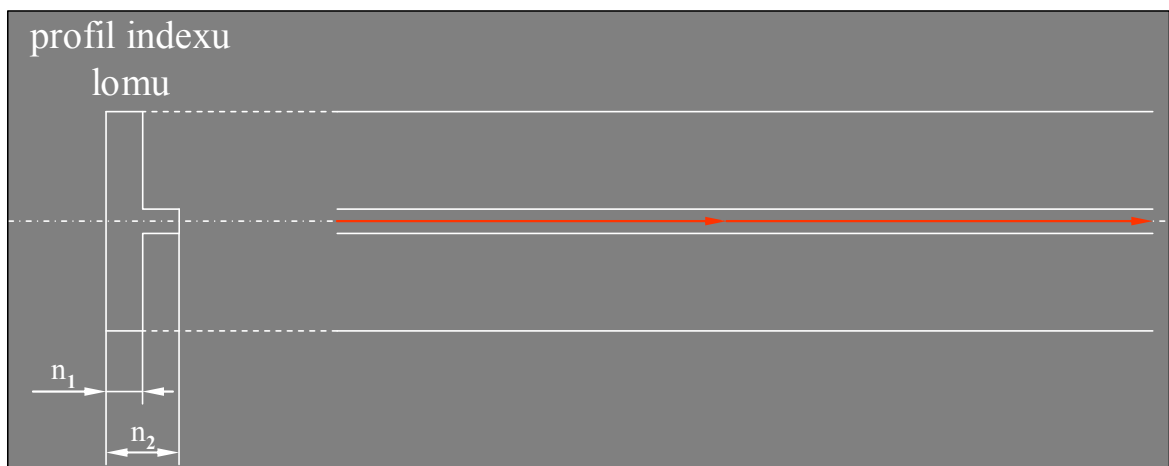
Vlákno optického káblu má dva základné parametre, priemer jadra a priemer plášťa, ktoré sú uvedené ako číslo pri popise kábla. Toto číslo je uvádzané v [ $\mu\text{m}$ ]. U mnohovidových vlákien sa používajú dva typy, 50/125  $\mu\text{m}$  (štandardizované ITU-T<sup>5</sup> podľa G.651) a 62,5/125  $\mu\text{m}$ . Jednovidové vlákna sa používajú o priemeroch 9/125  $\mu\text{m}$  (definované štandardami G.652, G.653, G.655 a G. 657).

---

<sup>5</sup> - International Telecommunication Union, sektor Telekomunikácie

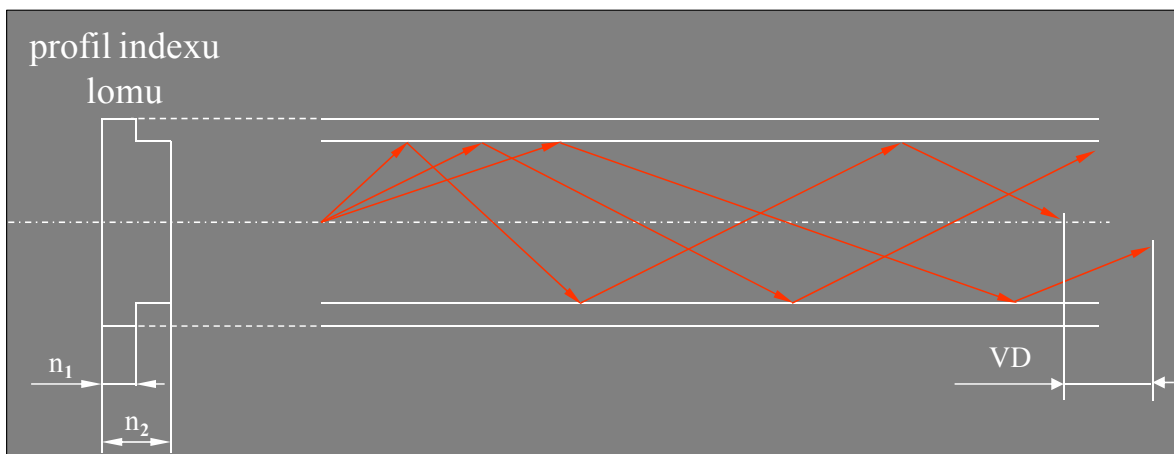
Rozdiel medzi mnohovidovými a jednovidovými vláknami je počet svetelných lúčov tzv. vidov. U mnohovidových vlákien sa prenáša pomerne väčšie množstvo lúčov, pričom u jednovidových sa prenáša iba jeden. Vidy u mnohovidových vlákien môžu prekonať vzdialenosť za rôzny čas, čo môže viesť k rušeniu na strane prijímača. Mnohovidové vlákna sú náchylnejšie disperziu, deformáciu signálu čo má za následok väčší útlm signálu. Z tohto obmedzenia plynie, že mnohovidové vlákna sú vhodnejšie pre menšie vzdialenosti. U jednovidových vlákien dochádza chromatickej a polarizačnej disperzií.

Optické vlákna možno ďalej rozdeliť na vlákna so skokovým indexom lomu (*step index*) a s postupnou zmenou indexu lomu (*graded index*), pričom vlákna s postupnou zmenou indexu lomu sa používajú iba pre mnohovidové vlákna.



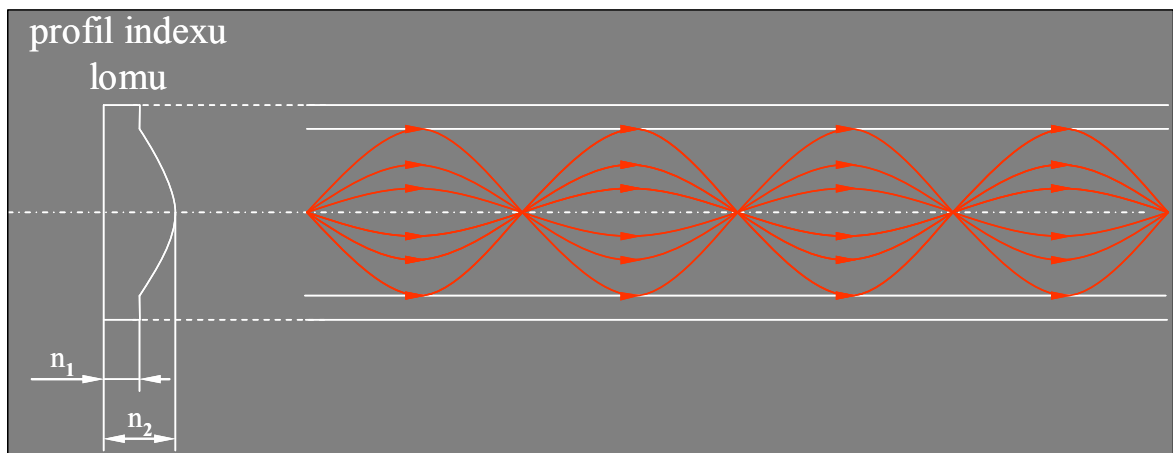
Obr. 6. Jednovidové optické vlákno.

Optické káble, ktoré majú vlákno so **skokovou zmenou indexom lomu** sa používajú pre obe varianty optických vlákien, ale z fyzických vlastností mnohovidových vlákien je tento typ používanější u jednovidových optických vlákien.



Obr. 7. Mnohovidové optické vlákno so skokovou zmenou indexu lomu.

Vlákna s **postupnou zmenou indexu lomu** sú zložené veľkého množstva vrstiev, ktoré sa líšia indexom lomu svetla. Tieto vrstvy spôsobujú, že lúč sa neodráža iba od plášťa, ale každá vrstva spôsobuje plynulejší ohyb lúču, ako je zobrazené na obrázku č.8. Toto spôsobuje lepšie vedenie lúču, menšiu disperziu a celkovo tieto vlákna majú menší útlm. Preto sú používanjšou alternatívou pre mnohovidové vlákna.



Obr. 8. Mnohovidové optické vlákno s postupnou zmenou indexu lomu.

### 1.4.3 Konektory pre metalickú kabeláž

V súčasnosti sa pre metalickú kabeláž sa používa výhradne konektor RJ45. Tento konektor používajú ako aktívne (prepínače, smerovače atď.), tak i pasívne prvky (prepojovacie panely, káble, zásuvky atď.).



Obr. 9. Tienený konektor RJ45.<sup>6</sup>

Tak ako kabeláž, tak i konektory RJ45 sú k dispozícií v tienenej variante. Túto variantu je nutné použiť ak inštalovaná kabeláž je tiež v tienenej variante, pričom tienenie káblu je potreba na jednom mieste uzemniť.

#### 1.4.4 Konektory pre optickú kabeláž

Konektory pre optického vlákna umožňujú spájanie/rozpájanie optického kábla, tam kde je to vyžadované. Konektor mechanicky zaručuje dvojicu vlákien, tak aby bol možný prechod svetla. Kým u metalickej kabeláže je typ konektoru stabilný, u optických káblov sa konektory vyvíjajú spolu s rýchlostnými požiadavkami, a zároveň aby bol spoj vlákien čo najhladší.

Medzi ďalšie vlastnosti, ktoré by mali konektory spĺňať patria:

- Malé vstupné a výstupné straty.
- Jednoduchú inštaláciu.
- Nízka cena.
- Spoľahlivosť.

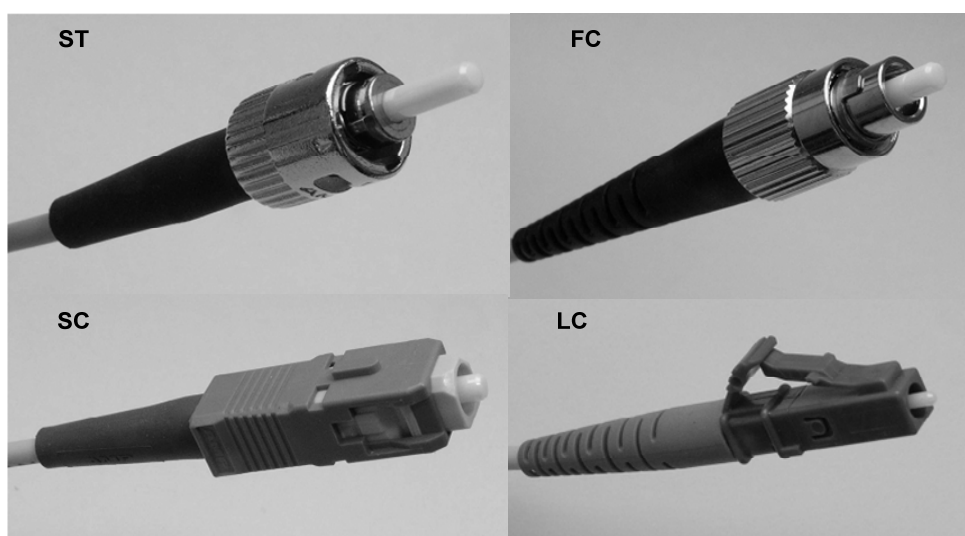
V súčasnosti existuje veľké množstvo konektorov pre optické vlákna, pričom sú navzájom nekompatibilné. Medzi v súčasnosti najpoužívanejšie typy konektorov patria:

- **ST:** Autorom tohto konektoru je spoločnosť AT&T a častým konektorom pre LAN (Local Area Network) siete. Používa bajonetový úchyt a má 2,5 mm zväčša keramickú fertulu – „kolík“ pre uchytenie vlákna. Medzi jeho výhody patrí cena a jednoduchosť.
- **SC:** Konektor štandardizovaný v norme TIA-568-A, v súčasnosti rozšírený konektor pre LAN. Pre siete WAN (Wide Area Network) sa používa s APC (Angle Point Contact). Výhodou je rýchla inštalácia, vlastnosti a cena týchto konektorov.

---

<sup>6</sup> - Obrázok použitý z <http://j.b5z.net/i/u/2060977/i/rj45shielded.jpg>

- **FC:** Prvý najpoužívanejší typ konektoru pre jednomódové optické káble. Má šróbovaciu konštrukciu. V súčasnosti je nahrádzaný konektormi typu SC a LC. Častejšie sa používa u meracích prístrojoch.
- **LC:** Miniaturný konektor s výbornými parametrami, vhodný pre rôzne aplikácie ako napr. LAN, WAN, *Fibre Channel*. Často používaný pre jednomódové optické vlákna. Používa sa v aktívnych prvkoch [1], [9].



Obr. 10. Optické konektory.

Obrázok zobrazujúci komplexný prehľad konektorov pre optické vlákna je umiestnený ako príloha č.11 na CD-ROM. Obrázok je prevzatý z [13].

## 1.5 Štandardy ovplyvňujúce štruktúrovanú kabeláž

Štruktúrovaná kabeláž je komplexný systém, ktorý by bez štandardizačných orgánov nevedel fungovať. V súčasnosti tieto orgány sa zaoberajú predovšetkým normami a štandardami, ktoré sa týkajú návrhom systému štruktúrovanej kabeláže, parametrami komponentov a ich inštaláciu, testovanie alebo inými vlastnosťami.

Z dôvodu veľkého počtu základných štandardov, ktoré sa zaoberajú štruktúrovanou kabelážou, je táto sekcia premiestnená na CD-ROM ako príloha ako č.12.

## 1.6 Protokoly pre fyzické média

V súčasnosti IEEE označuje protokoly pre Ethernet na základe použitého média. Prvé číslo označuje rýchlosť daného protokolu. *Base* označuje, že protokol používa vysielanie

v základnom pásme. Písmeno následne označuje použité médium. V prípade TP káblov, ak existuje viacero protokolov o rovnakej rýchlosti, sú tieto protokoly rozlíšené písmenom, prípadne číslom za typom média. Napr. 100Base-TX, označuje protokol pre krútenú dvojlinku, ktorého rýchlosť je 100 Mbps v základnom pásme.

### 1.6.1 Protokoly pre metalickú kabeláž

Tab. 2. Štandardy pre metalickú kabeláž.

Protokol	Médium	Vzdialenosť	Poznámky
10Base-T	Cat-3 (2 páry)	100 m	LatisNet, Návrh 802.3i; 1987.
100Base-T	Cat-5 (2 páry)	100 m	-
1000Base-T	Cat-5 (4 páry)	100 m	Doporučená Cat-5E
10GBase-CX4	Cat-5E	15 m	IEEE 802.3ap
10GBASE-T	Cat-6 netienená	55 m	IEEE 802.3an
10GBASE-T	Cat-6 tienená	100 m	IEEE 802.3an
10GBASE-T	Cat-6A	100 m	IEEE 802.3an
10GBASE-T	Cat-7	100 m	IEEE 802.3an

### 1.6.2 Protokoly pre optickú kabeláž

Z dôvodu rozsiahlosti je tabuľka štandardov pre optickú kabeláž umiestnená ako príloha č.2 na CD-ROM.

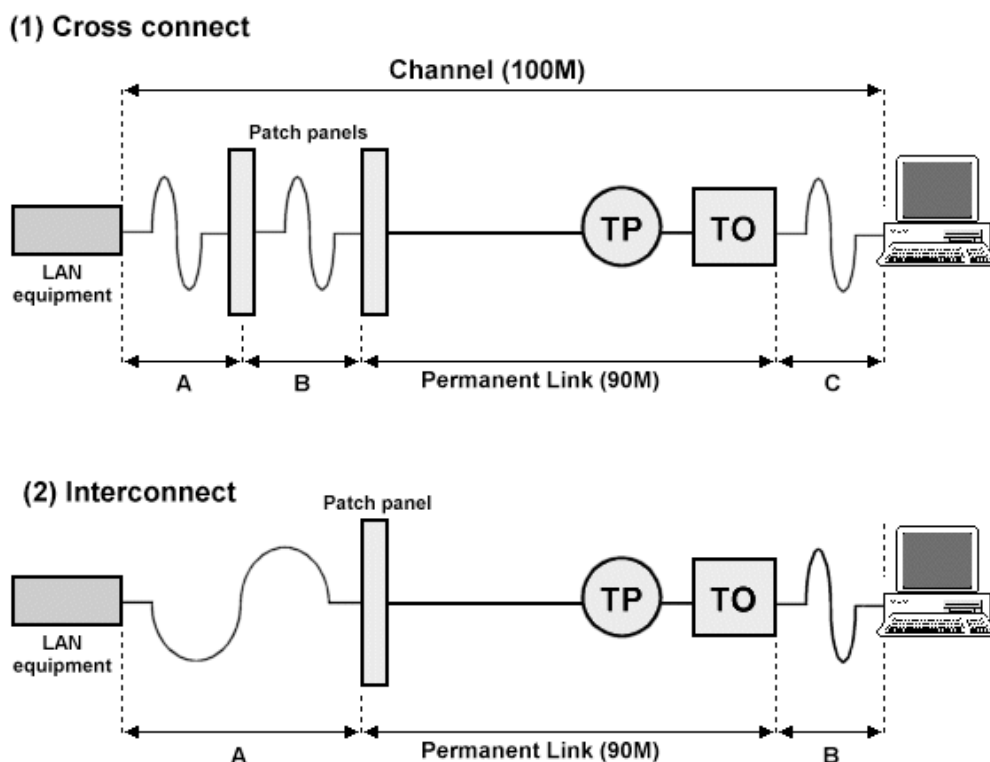
## 1.7 Protokol 10GBaseT na existujúcej metalickej kabeláži

Možnosť prevádzkovať protokol 10GBaseT na súčasnej kabeláži kategórie 5E a 6 sa zaoberá dokument s označením ANSI/TIA/EIA TSB 155. Testovaním vyplynulo, že napr. kabeláže kategórie 5E nebudú protokol 10GBaseT podporovať a UTP kategórie 6 je možné prevádzkovať rýchlosť 10 Gbps len do vzdialenosť do 55 m. U tienenej kategórie 6 je možné dosahovať väčších vzdialeností než u netienenej verzie, ale pre bezproblémovú

prevádzku 10GBaseT protokolu je vhodnejšie u nových inštalácií použiť buď prvky kategórie 6A alebo kategórie 7, ktoré vznikli práve z dôvodu plnej podpory protokolu 10GBaseT. Faktorom, ktorý ktorí obmedzuje dĺžku segmentu u kategórie 6, je *Alien Crosstalk* (tzv. cudzie prieniky). Tieto prieniky vznikajú medzi párami v kábli [1].

### 1.7.1 Špecifikácia požiadavkou káblových systémov pre 10GBaseT

Pre plnohodnotnú prevádzku protokolu 10GBaseT bola definovaná „nová“ kategória 6, ktorá má špecifikovanú šírku pásma až do 500 MHz – to je dvojnásobok oproti bežnej kategórie 6. Označenie tejto kategórie je CAT6A – tzv. „Augmented Category 6“. U tejto kategórie je možné prevádzkovať 10GBaseT na dĺžkach a všetkých typoch kabeláže (tzv. UTP i STP), ako i na linkách typu *Permanent Link*, tak na *Channel*. Zároveň bola definovaná i nová kategória 7, čím vznikla CAT7A ktorá má šírku pásma 1000 MHz oproti súčasným 600 MHz [1].



Obr. 11. Linka typu Channel a Permanent link.<sup>7</sup>

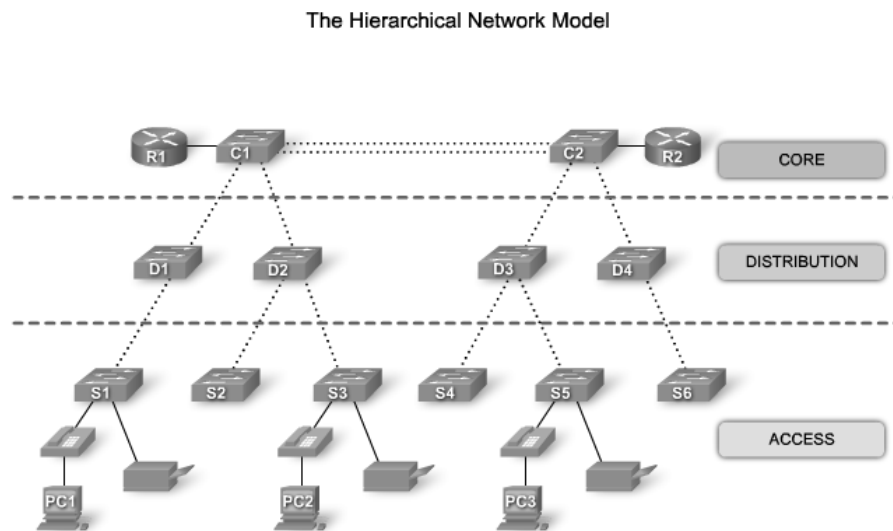
<sup>7</sup> - Obrázok použitý z [8].

Obrázok č.11 zobrazuje rozdiel medzi linkou typu *Channel* a *Permanent link*. Linka označovaná ako *Permanent link* je kabeláž medzi zásuvkou prepojovacím panelom. Pre tento typ linky je povolená maximálna dĺžka 90 m. Linka typu *Channel* je všetka kabeláž, ktorá vedie od počítača, až k sieťovému prvku, pričom celková dĺžka nesmie presiahnuť 100 m [8].

## 2 HIERARCHICKÝ SIEŤOVÝ MODEL

Ďalším faktorom, ktorý ovplyvňuje výkon počítačovej siete, je sieťový model. Správny výber tohto modelu ovplyvňuje nielen výkon počítačovej siete, ale i faktory ako je rozšíriteľnosť, bezpečnosť alebo spravovateľnosť.

Pre potreby modernej, vysokovýkonnej siete je najvhodnejšie použiť hierarchický sieťový model, ktorý využíva výhody návrhu štruktúrovanej kabeláže. Tento model rozdeľuje sieť do 3 vrstiev, prístupovú, distribučnú a chrbticovú. Každá vrstva je definovaná špecifickými funkciami, ktoré definujú jej úlohu v sieťovom modeli.



Obr. 12. Hierarchický sieťový model.<sup>8</sup>

### 2.1 Funkcie vrstiev hierarchického sieťového modelu

Hlavnou funkciou **prístupovej vrstvy** je poskytovať prístup koncovým zariadeniam do siete. S touto funkciou je priamo spojená i funkcia kontroly prístupu týchto zariadení, prípadne riadenie ich komunikácie smerom k iným častiam siete. Na tejto vrstve môže byť definovaná logická štruktúra siete pomocou virtuálnych sietí VLAN (Virtual LAN). Takto logicky rozdelená sieť je ľahšie kontrolovateľná z pohľadu prístupu, ktoré koncové zariadenie môže v sieti komunikovať a s ktorými zariadeniami. Ako je z obrázku č.11

<sup>8</sup> - Obrázok použitý [3].

vidieť, medzi zariadenia, ktoré sa nachádzajú na prístupovej vrstve, patria prepínače a bezdrôtové prístupové body, ktoré poskytujú bod pripojenia do siete pre koncové zariadenia. Medzi koncové zariadenia patria, počítače, telefóny, tlačiarne a podobne.

Cieľom **distribučnej vrstvy** je zber dát z prepínačov na prístupovej vrstve a ich preposlanie prvkom na chrbticovej vrstve, ktorá ich odošle na miesto určenia. Funkciou distribučnej vrstvy je vymedzenie *broadcast* domény a riadenie sieťovej prevádzky. Toto riadenie sieťovej prevádzky zároveň je súčasťou logického členenia pomocou sietí VLAN, kedy prvky distribučnej vrstvy slúžia ako riadiace body. Medzi zariadenia, ktoré môžeme nájsť na distribučnej vrstve, patria sú smerovače a výkonné prepínače, ktoré sú schopné vykonávať funkcie na sieťovej vrstve.

Ako vyplýva z predchádzajúcich odstavcov, cieľom **chrbticovej vrstvy** je vysokorýchlostné doručenie dát na miesto určenia. Chrbticová vrstva tvorí hlavnú kostru siete, ktorá je dôležitá pre dostupnosť medzi zariadeniami distribučnej vrstvy. Spolu s týmito funkciami súvisí i ďalšia, sprostredkovanie prístupu do iných sietí, ako napr. Internet. Z týchto dôvodov je zrejmé, aby zariadenia pracujúce na chrbticovej vrstve boli vysokovýkonné zariadenia, ktorých atribúty sú vysoký výkon, dostupnosť a dostatok systémových zdrojov. Medzi takéto zariadenia patria *hi-end* smerovače a prepínače. V určitých prípadoch, kedy štruktúra siete nie je natoľko rozvinutá, môžu chrbticová a distribučná vrstva splynúť do jednej vrstvy, čím sa vytvorí tzv. zlúčený hierarchický sieťový model [3].

## 2.2 Výhody hierarchického sieťového modelu

Medzi jednoznačné výhody hierarchického modelu spočíva v jeho modularite. Táto modularita umožňuje ľahkú rozšíriteľnosť siete, pretože prvky siete sa môžu kopírovať podľa potreby rozširovania siete.

Základom znakom vysokovýkonnej siete je dostupnosť, v zmysle fungujúcej komunikácie. Táto dostupnosť sa dosahuje implementovaním redundancie. Táto redundancia týka ako aktívnych (záložné prepínače), tak i pasívnych (záložné sieťové prepojenia) sieťových prvkov.

Hlavnou výhodou hierarchického sieťového modelu je vyšší výkon oproti iným sieťovým modelom. Správnou implementáciou tohto modelu je možné prevádzkovať konvergovanú

sieť, ktorá zahŕňa okrem dátovej i hlasovú a video prevádzku. Táto implementácia zahŕňa analýzu siete a budúcich potrieb, vhodný výber aktívnych prvkov siete a ich vhodná konfigurácia.

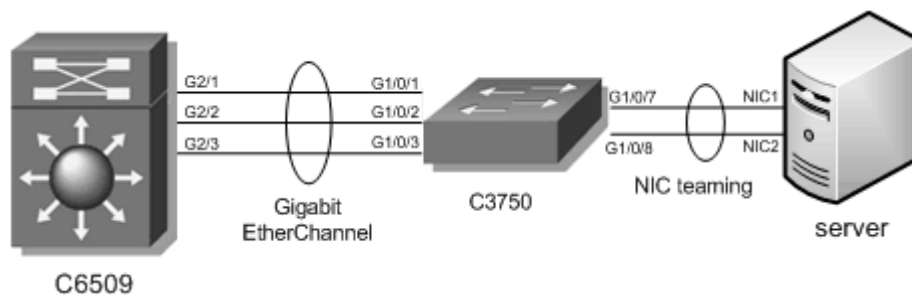
Hierarchický model má pri správnej konfigurácii i vyššie zabezpečenie siete. Prepínače prístupovej vrstvy môžu byť nakonfigurované pravidlami, ktoré umožňujú riadiť komunikáciu koncových zariadení, alebo či sa môže dané zariadenie do siete pripojiť. Implementovaním ďalších pravidiel na prvkoch distribučnej vrstvy je možné riadiť sieťové protokoly tak, aby sa minimalizovali riziká s nimi spojené.

Spravovanie siete, ktorá používa hierarchický sieťový model, je oproti iným sieťovým modelom jednoduchšia. Výhodou oproti iným modelom je jeho rozdelenie do vrstiev. Každá vrstva poskytuje špecifické funkcie, ktoré zdieľajú všetky zariadenia na danej vrstve. So zmenou niektorého nastavenia na jednom prvku, je možné len kopírovať toto nastavenie na ostatné zariadenia v danej vrstve. Pridanie novej inštancie sieťového zariadenia do siete je tiež jednoduchšie, pretože konfigurácie na jednej vrstve sa líšia len malými zmenami. Konzistencia medzi zariadeniami na každej vrstve dovoľuje rýchlu obnovu a jednoduchšie hľadanie chýb [3].

### 3 TECHNOLOGIA CISCO ETHERCHANNEL

Spolu s rozsiahlym nasadzovaním *Ethernet*-u a prepínačov sa zároveň rozšírili aplikácie, ktoré sú náročné na šírku pásma (*bandwidth*). Komunikačný model každý s každým, týchto aplikácií ako napr. video (*streaming, on demand*), interaktívna komunikácia, alebo nástroje pre vzájomnú spoluprácu, volajú po rozšírení šírky pásma ako u chrbtice, tak i na a koncoch siete. Zároveň kriticky dôležité aplikácie, pre svoj chod vyžadujú stabilné sieťové pripojenie s určitými vlastnosťami. So širokým nasadzovaním rýchlych prepínaných Ethernet liniek v rámci siete, užívatelia majú možnosť agregovať ich existujúce zdroje, alebo zvýšiť rýchlosť liniek a kľúčových prvkov siete pre zvýšenie výkonu chrbticovej siete.

K účelu agregácie liniek je možné použiť proprietárnu technológiu EtherChannel od spoločnosti Cisco. Táto technológia bola v roku 2000 s istými obmedzeniami uvoľnená a prijatá ako otvorený štandard IEEE 802.3ad. Pôvodná technológia EtherChannel bola pôvodne vyvinutá začiatkom 90.tych rokov spoločnosťou Kalpana, pričom v roku 1994 bola odkúpená spoločnosťou Cisco.



Obr. 13. Agregácia liniek.<sup>9</sup>

Technológia Cisco EtherChannel (ďalej už len EtherChannel) je postavená na štandarde 802.3 plne duplexného *Ethernet*-u, pričom poskytuje spoľahlivé, vysoko-rýchlostné riešenie pre chrbticové sieťové spoje. EtherChannel dovoľuje zlúčiť až 8 fyzických Ethernet liniek do jednej logickej Ethernet linky. Toto prepojenie je možné použiť ako u aktívnych sieťových prvkov, tak i u serverov, ktoré sú vybavené sieťovými kartami podporujúcimi túto technológiu. I u náročných situáciách, EtherChannel pomáha

<sup>9</sup> -Obrázok použitý z [11].

agregovať celkovú prevádzku a udržuje preťaženie na minime, zatiaľ čo poskytuje odolné riešenie [10].

### 3.1 Výhody Cisco EtherChannel

- **Postavený na štandardoch** – EtherChannel je postavený na štandardoch IEEE 802.3 zoskupovaním viacerých, plne duplexných *point-to-point* liniek dokopy.
- **Rozličné platformy** – Výhodou tejto technológie je flexibilita a jej možnosť použiť ju hocikde v sieti, ktorá má problémy so stabilným preťažením tzv. *bottleneck*.
- **Flexibilný nárast šírky pásma** – EtherChannel poskytuje agregáciu v násobkoch 100 Mbps, 1 Gbps, alebo 10 Gbps v závislosti na rýchlosti agregovaných liniek.
- **Vyrovňavanie záťaže (Load Balancing)** – Nakoľko EtherChannel pozostáva z niekoľkých ethernet liniek je schopný u týchto liniek distribuovať sieťovú prevádzku rovnomerne. Toto poskytuje vyšší výkon a využitie paralelných, inak redundantných liniek.
- **Odolnosť a rýchla konvergencia** – Pri zlyhaní niektorej linky, EtherChannel poskytuje automatickú obnovu, presmerovaním prevádzky medzi zostávajúce linky. Pri zlyhaní linky je prevádzka presmerovaná na ostatné linky v priebehu menej než jedna sekunda. Takáto konvergencia je transparentná pre koncových užívateľov, pričom nedochádza k vypršaniu časovačov u sieťových protokolov a tým pádom, relácie nie sú narušené.
- **Jednoduchý manažment** – EtherChannel využíva skúsenosti spoločnosti Cisco s riešením problémov a údržbou Ethernet sietí. Pre správu a riešenie problémov je možné používať aplikácie ako napr. CiscoWorks, alebo aplikácie tretích strán, ktoré dokážu pracovať s EtherChannel.
- **Transparentnosť k sieťovým aplikáciám** – EtherChannel nevyžaduje žiadne zmeny u sieťových aplikácií. Pri použití EtherChannel, prepínače a smerovače poskytujú vyrovňavanie záťaže transparentne sieťovým užívateľom. Pre podporu EtherChannel u serverov a sieťových kariet, je potreba špeciálnych ovládačov aby dokázali spracovávať prevádzku z viacerých rozhraní.

- **Kompatibilita s Cisco IOS® Softwarom** – Prepojenia sú plne kompatibilné s Cisco IOS (Internetwork Operating System) VLAN a smerovacími technológiami. Zaistená je tiež podpora *trunk* protokolov, ktoré môžu prenášať viaceré siete VLAN medzi linkami v kanáli, tak i smerovacie protokoly ako napríklad HSRP (Hot Standby Router Protocol).
- **Kompatibilita s CWDM konvertormi** – Implementácia EtherChannel a CWDM (Coarse Wavelength Division Multiplexing) umožňuje zvýšiť šírku pásma liniek bez nutnosti investovať do novej optickej kabeláže. Toto spojenie umožňuje agregovanú prevádzku kanálu multiplexovať do jedného optického vlákna [10].

### 3.2 Komponenty Cisco EtherChannel

EtherChannel je *trunk* technológia umožňujúca zdieľanie záťaže na viacerých linkách, ktoré pôvodne boli určené ako redundantné.

Táto technológia pozostáva z nasledujúcich kľúčových komponentov:

- **Ethernetové linky** – EtherChannel prepojenie môže pozostávať až z 8 liniek, ktoré zdieľať sieťovú prevádzku, pričom je možné dosiahnuť až 80 Gbps pri použití 10-Gigabitových Ethernet liniek. Takáto linka môže prepojovať LAN prepínače, smerovače, servery alebo klientov. Pretože vyrovňovanie záťaže je priamo integrované v architektúre Cisco Catalyst, nedochádza k degradácii výkonu po pridaní liniek do kanálu a tým je dosahovaná vyššia priepustnosť a nižšia latencia. Ďalšou výhodou je, že poskytuje pružnosť liniek v rámci kanálu – ak zlyhá linka, sieťová prevádzka je okamžite smerovaná na ostatné linky v kanále.
- **Redundancia** – Výhodou EtherChannel je, že nie je nutné použiť 802.1D STP (Spanning Tree Protocol) pre údržbu stavu topológie v rámci kanálu. Namiesto toho používa protokoly typu *peer-to-peer*, ktoré poskytujú automatickú konfiguráciu a konvergenciu paralelných liniek. Tento prístup umožňuje EtherChannel používať funkcie pre zotavenie siete bez pridania komplexnosti, alebo vytvorením nekompatibility pri použití zariadení od tretích strán alebo pomocou softwaru.
- **Manažment** – Konfigurovať EtherChannel je možné jednoducho pomocou CLI (Command Line Interface) alebo pomocou SNMP (Simple Network Management

Protocol) aplikácií ako napr. CiscoWorks. CiscoWorks v sieťovom prostredí s prepínačmi graficky zobrazuje EtherChannel prepojenia medzi zariadeniami, zbiera štatistiky pre individuálne linky v rámci kanálu a tiež i agregovanú pre celý kanál. Hlavnou výhodou EtherChannel je schopnosť detegovať, ohlásiť a zabrániť nesprávnemu spárovaniu rozhraní v rámci kanálu. Kontrola konzistencie je vykonaná pred aktiváciou kanála, čo pomáha zaistiť sieťovú integritu [10].

### 3.3 Možnosti konfigurácie EtherChannel

EtherChannel je možné konfigurovať ručne, alebo automaticky pomocou konfiguračných protokolov. Medzi tieto protokoly patrí proprietárny Cisco protokol PAgP (Port Aggregation Protocol) alebo protokol LACP (Link Aggregation Control Protocol), ktorý je súčasťou štandardu IEEE 802.3ad. Tieto protokoly sa používajú pre automatickú vyjednanie a vytvoreniu EtherChannelu medzi prepínačmi a smerovačmi. U agregácie liniek smerom k serverom sa táto technológia označuje ako NIC *Teaming* (Network Interface Card), prípadne NIC *Bonding* [11].

### 3.4 Princíp fungovania EtherChannel

Ako bolo spomenuté vyššie, EtherChannel slúži k agregácii liniek, pričom podmienkou pri zlučovaní je, že porty musia byť zhodne nastavené – rovnaký typ, rýchlosť, príslušnosť k rovnakým VLAN sieťam, alebo *trunk* mód s rovnakými parametrami. Pri agregácii pomocou PAgP protokolu môžeme použiť až 8 fyzických rozhraní. Pri použití protokolu LACP je možné použiť až 16 rozhraní, pričom ale iba 8 z nich je aktívnych, ostatné sú móde *Stand-By*.

V závislosti na verzii operačného systému, prípadne modelovej rady prepínača je možné vytvoriť rôzny počet (skupín) EtherChannel kanálov. U modelovej rady Catalyst 6500/6000 je možné vytvoriť až 64 EtherChannel kanálov. V minulosti, u tejto technológie bola podmienka, aby všetky porty jednej strany skupiny sa nachádzali na jednom prepínači. Dnes je možné, aby zúčastnené porty boli súčasťou jedného *stacku* [11].

Vytvorením EtherChannel kanálu sa vytvorí jeden **virtuálny port**, s ktorým pracujú všetky ostatné technológie. Príkladom môže byť protokol STP, ktorý skupinu portov vidí ako jeden port a preto nedochádza k blokovaniu redundantných liniek.

EtherChannel redukuje binárnu časť adres v rámci na numerickú, ktorá potom rozhoduje ktorou linkou v kanáli budú rámce distribuované. Distribúcia rámcov v EtherChannel používa proprietárny Cisco *hash* algoritmus. Tento algoritmus je deterministický, čiže ak sa použijú rovnaké adresy a relačné informácie, bude použitý rovnaký port v kanály. Táto metóda zabraňuje aby pakety prišli mimo poradia.

*Hash* algoritmus, ktorý je použitý v EtherChannel, počíta hodnoty v rozsahu od 0 do 7. Táto hodnota následne určuje konkrétny port, ktorý je zvolený. Nastavenie portu zahŕňa masku, ktorá značí, ktoré hodnoty port prijme pre prenos dát. S maximálnym počtom portov v jednom EtherChannel, čo je 8 portov, každý port prijme len jednu hodnotu. V prípade, že do EtherChannel sú zapojené 4 porty, tak každý port prijme iba 2 hodnoty, a tak ďalej. Tabuľka č.5 zobrazuje, koľko port prijme hodnôt pri danom počte portov [5].

Tab. 3. Rozloženie počtu hodnôt.

Počet portov v EtherChannel	Rozloženie zát'aže
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

**Poznámka:** Tabuľka č.3 zobrazuje iba počet hodnôt, ktoré vypočíta *hash* algoritmus a koľko ich port prijme. Nie je možné určiť port, ktorý použije daný tok, ale je možné len ovplyvniť rozloženie zát'aže pomocou metódy distribúcie rámcov, ktorej výsledkom je väčšia rozdielnosť.

Z tabuľky č.3 je vidieť, že pre dosiahnutie ideálneho rozloženia zát'aže, i s použitím náhodných adres, je možné iba pri použití 2, 4 alebo 8 portoch na kanál [5].

### 3.4.1 Vyrovnávanie zát'aže

Vyrovnávanie zát'aže je priamo integrované v operačnom systéme prepínačov a smerovačov spoločnosti Cisco. Použitý algoritmus sa odlišuje medzi platformami jednotlivých zariadení, pričom rozhodovanie je založené buď na zdrojových alebo cieľových MAC (Media Access Control), IP (Internet Protocol) adresách, alebo na číslach portov TCP (Transmission Control Protocol) a UDP (User Datagram Protocol) protokolov. U protokolu typu TCP je snaha, aby rámce z jednej TCP relácie boli odosielané cez rovnakú linku, inak by mohlo dôjsť k doručení mimo poradia a ďalším problémom u virtuálneho portu. Prichádzajúce dáta sa združujú zo všetkých rozhraní do virtuálneho portu EtherChannel [5].

Tabuľka zobrazujúca jednotlivé algoritmy pre jednotlivé platformy je z dôvodu veľkosti umiestnená ako príloha č.3.

### 3.4.2 Port Aggregation Protocol

PAGP je proprietárny protokol spoločnosti Cisco a je podporovaný, iba na Cisco prepínačoch. PAGP podporuje vytvorenie EtherChannelu iba z rozhraní na jednom prepínači (nie v rámci *stacku*). Cieľ PAGP protokolu je automatického vytvorenia EtherChannel. PAGP pakety sú zasielané medzi EtherChannel *ready* portami podľa poradia za účelom vytvorenia kanálu.

PAGP môže pracovať buď v aktívnom režime, kedy sa aktívne snaží vyjednať vytvorenie EtherChannelu. Tento režim sa označuje ako **Desirable**. U pasívneho režimu sa EtherChannel označovaného ako **Auto**, sa začne vyjednávať, iba ak príde požiadavka z druhej strany – sám nikdy nezačne vyjednávanie. Toto automatické vytvorenie EtherChannel kanálu má niekoľko obmedzení:

- PAGP nevytvorí zväzok na portoch, ktoré sú konfigurované dynamickými VLAN sieťami. PAGP vyžaduje, aby všetky porty v kanáli patri do rovnakej VLAN siete, alebo boli nakonfigurované do *trunk* linky. Ak zväzok už existuje a VLAN sieť na porte je zmenená, všetky porty v zväzku sú modifikované, tak aby sedeli s danou VLAN sieťou.

- PAgP nevytvorí zväzok zo skupinu portov, ktoré pracujú rozdielnymi rýchlosťami alebo pri inom nastavení duplexu. Ak sa rýchlosť alebo duplex zmenia u už existujúce zväzku, PAgP zmení rýchlosti a duplex na všetkých portoch v zväzku.
- Režimy PAgP sú **OFF**, **Auto**, **Desirable** a **On**. Iba kombinácia Auto-Desirable, Desirable-Desirable a On-On môžu sformovať kanál. Ak zariadenie (napr. smerovač) na opačnej strane nepodporuje PAgP, tak PAgP musí byť nastavené na možnosť On [5], [11].

### 3.5 Link Aggregation Control Protocol

LACP je štandardizovaný protokol, ktorý slúži k rovnakému účelu ako proprietárny PAgP protokol. Ide o súčasť štandardu IEEE 802.3ad. Výhodou tohto štandardizovaného riešenia je že vytvorí agregáciu na prepínači automaticky, a zároveň použiť agregáciu liniek u prepínačov, ktoré nepodporujú technológiu EtherChannel.

U IEEE 802.3ad, LACP protokol automaticky povie prepínači, ktoré porty by mali byť agregované. Keď je 802.3ad agregácia nakonfigurovaná, sú LACP dátové jednotky vymenené medzi serverom a prepínačom. LACP dá vedieť prepínaču, ktoré adaptéry sú konfigurované v agregácií a mali by byť považované za jeden, bez ďalšieho zásahu užívateľa.

LACP podobne ako PAgP má dva módy **Active** a **Passive**. V móde **Active** sa protokol sám snaží vyjednať agregáciu, pričom sám odosiela pakety pre vyjednanie spojenia. Naproti tomu režim **Passive** funguje podobne ako režim Auto u PAgP, čiže vyjednávanie agregácie začne až keď je vyzvaný [12].

### 3.6 NIC Teaming IEEE 802.3ad

NIC (Network Interface Card) Teaming je termín pre agregáciu sieťových kariet. Ide o technológiu, ktorá umožňuje spojiť 2 alebo viac fyzických NIC do jedného logického (virtuálneho) sieťového adaptéru, ktorý sa označuje ako **bond** (zväzok). K tomuto účelu zväčša využíva štandard IEEE 802.3ad.

K tomuto účelu je buď potreba natívna podpora zo strany operačného systému, alebo ovládač sieťovej karty s podporou *bonding*.

NIC Teaming môže fungovať i s obyčajným prepínačom, ktorý nepodporuje agregáciu liniek. U takéhoto prípadu, je potrebné konfigurovať agregáciu iba na strane serveru a uplatňuje sa primárne pre odchádzajúcu (*outgoing*) prevádzku.

Sieťové adaptéry môžu byť zapojené i do rôznych prepínačov a môžu mať i inú rýchlosť a duplex. Vytvorením teamu podľa 802.3ad sa vytvorí jedno virtuálne rozhranie, ktoré získa MAC adresu od jedného z fyzických adaptérov a môžeme mu nastaviť jednu alebo viac IP adries. Pri použití niektorého režimu nezávislom na prepínači, tak všetky fyzické porty (v rámci virtuálneho) používajú svoju vlastnú MAC adresu.

Pri nastavovaní NIC *Teaming* je tiež možnosť nastaviť zároveň i mód *teaming*, prípadne metódu fungovania:

- **Adapter Fault Tolerance**, kedy je jeden adaptér aktívny a ostatné sú v režime *Stand-by* (prepnú sa v prípade výpadku). Tento mód sa nenastavuje na strane prepínača.
- **Switch Fault Tolerance** podporuje dve linky pripojené do 2 rôznych prepínačov, jedna je aktívna a druhá *Stand-by*. Tento mód sa nenastavuje na strane prepínača.
- **Adaptive Load Balancing** odchádzajúca prevádzka je vyvažovaná cez všetky adaptéry, zároveň poskytuje *fault tolerance*, môže vykonávať *load balancing* i na prichádzajúcej prevádzke. Tento mód sa nenastavuje na strane prepínača.
- **Static Link Aggregation** je použitie manuálneho EtherChannelu, kedy je na prepínači nastavený mód On.
- **Dynamic Link Aggregation** využíva LACP protokol podľa IEEE 802.3ad [11].

## 4 VOICE OVER IP

VoIP (Voice over IP) je spoločný názov pre rodinu technológií, metodológií, komunikačných protokolov a prenosových techník určený pre doručovanie hlasovej komunikácie, prípadne multimediálnych relácií pomocou IP protokolu.

Základom tejto technológie je vzrastajúca efektivita paketových sietí a schopnosť štatisticky multiplexovať hlasovú prevádzku s dátovými paketmi. Toto umožňuje organizáciám maximalizovať návratnosť nákladov (ROI – Return of Investments) do sieťovej infraštruktúry pre dáta.

V klasickom riešení je hlasová a dátová sieť oddelená a tým pádom sa nemôžu navzájom ovplyvňovať. U konvergovaného riešenia, je nevyhnutné vybrať také protokoly, ktoré sú schopné riadiť hlasové hovory a zabezpečiť, aby dátové prúdy negatívne neovplyvňovali tie, ktoré nesú hlasové dáta.

### 4.1 Výhody paketovej telefónie

Medzi výhody paketovej telefónie oproti telefónii pomocou prepínaných okruhov patria:

- **Vyššia efektivita šírky pásma a zariadení** – Paketová telefónia zdieľa šírku pásma medzi viacerými logickými spojeniami a prideluje ju podľa objemu z existujúcich hlasových prepínačov.
- **Nižšie náklady na prenos telefónnej siete** – Paketová telefónia štatisticky multiplexuje hlasovú prevádzku medzi dátovú. Táto konsolidácia predstavuje značné ušetrzenie kapitálu a prevádzkových nákladov.
- **Konsolidácia nákladov na hlasovú a dátovú sieť** – Hlasové siete sú zmenené tak, aby mohli využívať architektúru prepínaných paketov, pre vytvorenie jednotnej komunikačnej siete s bežným prepínaním a vysielačím systémom.
- **Vyššia návratnosť u nových služieb** – Paketová telefónia umožňuje integrovať služby, ako napr. vysielenie kvalitného zvuku, zjednotené posielanie správ, alebo reálny prenos hlasu spolu s dátovou spoluprácou. Tieto služby zvyšujú zamestnaneckú produktivitu a zisk, oproti základným hlasovým službám. Zároveň umožňujú spoločnostiam a poskytovateľom sa odlíšiť od konkurencie a zlepšiť si tak pozíciu na trhu.

- **Vyššie inovácie v službách** – Zjednotená komunikácia používa IP infraštruktúru ku konsolidácii komunikačných metód, ktoré pred tým boli nezávislé, ako napr. fax, hlasová schránka, email, pevná linka, mobilná telefónia a Web.
- **Prístup nových komunikačných zariadení** – IP telefóniu môžu používať zariadenia, ktoré nie sú určené pre TDM (Time Division Multiplex) infraštruktúru, napr. počítače, bezdrôtové zariadenia, úžitkové spotrebiče, PDA (Personal Digital Assistant) zariadenia, alebo televízny *set-top* box. Prístup týchto zariadení umožňuje spoločnostiam a poskytovateľom služieb zvýšiť objem komunikácie, ponuku služieb a tým zvýšiť počet zákazníkov. Toto umožňuje spoločnostiam predávať nové zariadenia, ako napr. videotelefóny, multimediálne terminály a pokročilé IP telefónov.
- **Pružná cenová štruktúra** – Sieťová šírka pásma je dynamicky alokovaná, tým pádom používanie siete nemusí byť merané v minútach, alebo vo vzdialenosti. Dynamické alokovanie umožňuje poskytovateľom služieb zasiahnúť potreby zákazníkov, čo umožňuje vyšší profit [7].

## 4.2 Komponenty VoIP

U tradičnej PSTN (Public Switched Telephone Network) telefónnej siete všetky elementy, ktoré sú potrebné pre hovor sa pre koncového používateľa javia transparentne. Migráciou na VoIP vyžaduje povedomie o týchto elementoch, pochopenie protokolov a komponentov, ktoré poskytujú rovnakú funkcionálnosť v IP sieti.

### 4.2.1 Signalizácia

Signalizácia je vlastnosť, pri ktorej sa generujú a vymieňajú kontrolné informácie pre vytvorenie, monitorovanie a ukončenie spojenia medzi dvoma koncovými bodmi. Hlasová signalizácia vyžaduje schopnosť poskytovať kontrolnú, adresnú a upozorňovaciu funkciu medzi uzlami. PSTN používa SS7 (Signaling System 7) signalizáciu, pre prenos riadiacich správ pomocou samostatnej (z aj. *out-of-band*) signalizačnej siete. VoIP má na výber niekoľko možností signalizácie, vrátane H.323, SIP (Session Initiation Protocol), Megaco/H.248 a MGCP (Media Gateway Control Protocol). Niektoré VoIP brány sú tiež schopné používať SS7 signalizáciu priamo do PSTN siete.

Signalizačné protokoly sú klasifikované buď ako *peer-to-peer* alebo *client/server*. SIP a H.323 sú príklady *peer-to-peer* signalizačných protokolov, kde koncové zariadenia alebo brány obsahujú schopnosti iniciovať a ukončiť hovory a interpretovať kontrolné správy. Megaco/H.248 a MGCP sú príklady *client/server* protokolov, kde koncové body alebo brány neobsahujú vlastnosti pre riadenie hovorov, ale posielajú alebo prijímajú upozornenia na udalosti servery, bežne označovaného ako *call agent*. Napr. keď MGCP brána deteguje, že telefón bol zdvihnutý, brána nevie automaticky poskytnúť vyzváňací tón. Brána odošle upozornenie na udalosť *call agent*, pričom mu povie, že telefón bol detegovaný v stave zdvihnutý. *Call Agent* potom upozorní bránu aby poskytovala oznamovací tón.

#### 4.2.2 Databázové služby

Prístup k službám ako napr. čísla ako 158, 112 alebo ID volajúceho vyžaduje schopnosť opýtať sa databázy, ako má byť prichádzajúci hovor rozoznaný, alebo aké informácie sú o ňom dostupné. Databázové služby zahrnujú prístup k fakturačným informáciám, meno volajúceho, bezplatné služby (čísla ako 112) atď. Poskytovatelia VoIP môžu rozlišovať ich služby poskytnutím prístupu k rozličným databázam. Napr. zjednodušiť prístup k faxu pre mobilných používateľov, tým že poskytovateľ môže vytvoriť službu, ktorá konvertuje fax na email. Ďalším príkladom môže byť, poskytovanie služby na oznamovanie hovoru. Hlasová správa je umiestnená do hlasovej schránky, pričom táto služba upozorní užívateľa v špecifický čas, alebo udalosť.

#### 4.2.3 Riadenie doručovania

Nosné kanály sú kanály, ktoré nesú hlasové hovory. Správny dohľad týchto kanálov vyžaduje, aby signalizácia, pre spojenie a ukončenie hovoru, prešla medzi koncovými zariadeniami. Správna signalizácia zaisťuje, že kanál je alokovaný pre daný hovor a že kanál bude správne uvoľnený, keď niektorá strana ukončí hovor. Tieto spojovacie a ukončovacie správy sú prenášané pomocou SS7 v rámci PSTN siete, a SIP, H.323, Megaco/H.248, alebo MGCP v rámci IP siete.

#### 4.2.4 Kódek

Kódek poskytuje kódovanie a dekódovanie stavov medzi analógovými a digitálnymi zariadeniami. Každý kódek definuje metódu kódovania hlasu, kompresného mechanizmu, ktorý je použitý pre konverziu hlasu. PSTN používa TDM pre prenos každého hovoru. Každý hlasový kanál používa 64 kbps šírky pásma a používa G.711 kódek pre konverziu medzi analógovou zložkou na TDM hlasový prúd. G.711 vytvára 64 kbps digitalizovaný hlasový prúd. U návrhu VoIP, kódek často komprimuje hlas pod 64 kbps hlasový prúd, čo umožňuje vyššiu efektivitu sieťových zdrojov. Najrozšírenejším kódek u WAN sietí je G.729, ktorý komprimuje hlasový prúd iba na 8 kbps [7].

### 4.3 VoIP protokoly

VoIP používa rôzne protokoly, pre zostavenie a ukončenie hovoru, posielanie informácií počas hovoru. Nasledujúci zoznam zobrazuje hlavné VoIP protokoly:

- **H.323** – Je štandardizovaný protokol ITU, pre interaktívnu komunikáciu. Pôvodne navrhovaný pre multimédia v *connectionless* prostredí, ako napr. LAN. Štandard H.323 zahrnuje ďalšie štandardy, ktoré definujú všetky aspekty synchronizovaného hlasu, videa a dátovej prevádzky a zároveň definuje *end-to-end* signalizáciu.
- **MGCP** – Tento protokol je špecifikovaný v RFC 2705, pričom MGCP definuje protokoly pre riadenie VoIP brán, ktoré sú pripojené k externým riadiacim hlasovým zariadeniam, označované ako *call agent*. MGCP poskytuje signalizáciu pre lacnejšie koncové zariadenia, ako napr. brány, ktoré nemusia mať implementovaný plný hlasový a signalizačný protokol ako napr. H.323. Príkladom môže byť udalosť zdvihnutia slúchadla na hlasovom porte brány, hlasový port ohlási udalosť *call agent*. Tento *call agent* potom oznámi danému zariadeniu aby poskytoval službu, ako napr. signalizáciu vytáčania.
- **Megaco/H.248** – Protokol je výsledkom spojenia snáh IETF (Internet Engineering Task Force) a ITU, pričom je založený na MGCP štandarde. Megaco definuje jednu riadiacu bránu, ktorá pracuje s viacerými bránovými aplikáciami vrátane PSTN brány, ATM (Asynchronous Transfer Mode), analógové rozhrania, servery a iné. Megaco poskytuje plnú správu pre riadenie hovorov a implementuje úroveň hovorov, ako napr. prenos, konferencia, presmerovania a podržanie. Klasická

operácia protokolu Megaco je vo svojej podstate veľmi podobná MGCP protokolu. Avšak Megaco poskytuje vyššiu flexibilitu, širšiu podporu aplikácií a brán.

- **Session Initiation Protocol (SIP)** – Obširny protokol, ktorý špecifikuje príkazy a odpovede pre vytvorenie a ukončenie hovorov. SIP tiež špecifikuje funkcie ako bezpečnosť, proxy a transportné služby (TCP a UDP). SIP a jeho partnerské protokoly SAP (Session Announcement Protocol) a SDP (Session Description Protocol) môže poskytovať oznámenia a informácie o *multicast* reláciách užívateľovi na sieti. SIP definuje *end-to-end* telefonickú signalizáciu medzi zariadeniami. SIP je textový protokol, ktorý využíva mnoho elementov HTTP (Hyper Transfer Text Protocol), použitím rovnakého transakčného modelu (*request* a *response*) a podobnými hlavičkami a kódom odpovede. Taktiež prijal modifikovanú formu URL (Uniform Resource Locator) adresnú schému používanú v rámci emailu, ktorá je založená na SMTP protokole (Simple Mail Transfer Protocol).
- **Real-Time Transport Protocol (RTP)** je IETF štandardizovaný protokol pre *stream* médií. RTP nesie hlasové dáta v *payload* časti skrz sieť. RTP poskytuje sekvenčné čísla a časové známky pre spracovanie v poradí hlasových paketov. Mimo hlasových paketov, RTP môže niesť streamované video pakety.
- **RTP Control Protocol (RTCP)** poskytuje *out-of-band* kontrolné informácie pre RTP prúd. Každý RTP prúd má odpovedajúci RTCP prúd, ktorý oznamuje štatistiky o hovore. RTCP je použitý pre oznamovanie QoS (Quality of Service) [7].

Úspešná integrácia *connection-oriented* hlasovej prevádzky v *connectionless* IP sieti, vyžaduje vylepšenie signalizačného *stack*. Určitým spôsobom, užívateľský hlasový protokol musí urobiť *connectionless* sieť tak aby vyzerala viac *connection-oriented* skrz sekvenčné čísla. Tabuľka č.4 poskytuje príklady ako rozličné VoIP komponenty a protokoly sú rozdelené v sedem vrstvovom OSI modeli.

Tab. 4. OSI model a VoIP komponenty a protokoly.

Vrstva v OSI modeli	VoIP komponent a protokol
Aplikačná	IP Komunikátor, CallManager a ľudská reč
Prezentačná	Kódek
Relačná	H.323, SIP, MGCP a Megaco
Transportná	RTP a UDP (médiá); TCP and UDP (signalizácia)
Sieťová	IP
Linková	Hociktorá linková technológia, ktorá podporuje prenos IP paketov. Napr. Frame Relay, ATM, Ethernet, Point-to-Point Protocol (PPP), Multilink PPP (MLP), a High-Level Data Link Control (HDLC).
Fyzická	Hociktorá technológia, ktorá podporuje prenos rámcov z linkovej vrstvy alebo buniek určených protokolom linkovej vrstvy. Napr. UTP, T1, E1, ISDN BRI a ISDN PRI.

#### 4.4 Dostupnosť VoIP služby

U tradičných telefónnych sietí má hlasová služba garantované oneskorenie, ktoré vzniká prechodom cez sieť. Pretože šírka pásma je garantovaná TDM prostredím, nedochádza tu k variabilnému oneskoreniu, tzv. *jitter*. Implementácia VoIP do dátovej siete, ale vyžaduje také sieťové prostredie pre hlasové služby, aby vznikalo malé oneskorenie (*delay*), minimálny *jitter*, a minimálna strata paketov. Požiadavky na šírku pásma musia byť správne vypočítané na základe použitého kódeku a počte súbežných spojení. Technológia QoS je základným kameňom pre minimalizáciu *jitter* efektu a stratu hlasových paketov.

Pre dosiahnutie 99,999% dostupnosť ako pri PSTN sieti, je potreba IP sieť navrhnuť s redundanciou a ochrannými mechanizmami proti zlyhaniu. Zároveň, dobrou praxou je vytvoriť bezpečnostné pravidlá, ktoré zaručia stabilitu siete a bezpečnosť hlasového prúdu [7].

Tab. 5. Riešenia pre implementáciu VoIP.

Problém	Riešenie
<b>Latencia</b>	Zvýšenie šírky pásma. Voľba iného kódeku. Fragmentácia dátových paketov. Nastavenie priority pre hlasové pakety.
<b>Jitter</b>	Použitie zásobníkov, ktoré vyrovnávajú <i>jitter</i> efekt.
<b>Šírka pásma</b>	Vypočítanie požiadavkou na šírku pásma, zahrnutie hlasových, riadiacich a normálnych dát.
<b>Strata paketov</b>	Návrh siete, ktorý bude minimalizovať preťaženie. Nastavenie priority pre hlasové pakety. Zníženie priority pre dáta, ktoré majú vyššiu prioritu než hlasové.
<b>Spoľahlivosť</b>	Zavedenie redundancie pre: <ul style="list-style-type: none"> <li>• Hardware.</li> <li>• Linky.</li> <li>• Napájanie – UPS (Uninterruptible Power Supply).</li> </ul> Vykonávanie proaktívneho sieťového manažmentu.
<b>Bezpečnosť</b>	Zabezpečením nasledujúcich komponentov: <ul style="list-style-type: none"> <li>• Sieťová infraštruktúra.</li> <li>• Systémy spracúvajúce hovory.</li> <li>• Koncové body.</li> <li>• Aplikácie.</li> </ul>

#### 4.5 Protokoly RTP a RTCP

Protokol RTP poskytuje *end-to-end* transportnú funkcie určené pre aplikácie prenášajúce dáta (*payload*) v reálnom čase, ako napr. audio a video. Tieto funkcie zahŕňajú identifikáciu dát, sekvencovanie, časové známkovanie a sledovanie doručenia.

RTP je nad UDP a využíva jeho služby ako napr. multiplexovanie a kontrolný súčet. Hoci sa RTP často používa pre *unicast* relácie, pôvodne bol navrhnutý pre relácie typu *multicast*. Okrem úlohy odosielateľa a príjemcu, RTP tiež definuje úlohy *translator* a *mixer* pre podporu *multicast* požiadaviek.

RTP je základnou komponentov VoIP. RTP hlavička obsahuje časovú známku a sekvenčné číslo, ktoré umožňujú prijímaciemu zariadeniu uložiť a odstrániť *jitter* a latenciu zosynchronizovaním paketov a vytvorením neprerušeneho prúdu mediálnych dát. RTP používa sekvenčné čísla pre správne zoradenie paketov, avšak RTP nežiada znovu o vyslanie paketov pri ich strate. Smerovače s podporou hlasových služieb môžu použiť algoritmus ukrytia straty paketu (*loss-concealment*), pre vytvorenie približných dát v stratených paketoch. Kým tento prístup minimalizuje dopad výpadku, alebo straty jedného paketu, u viac za sebou vygenerovaných hlasových paketov je výsledkom slabá kvalita hovoru.

Kým RTP streamuje daný multimedialny obsah, RTCP monitoruje kvalitu distribúcie dát a poskytuje kontrolné informácie.

RTCP poskytuje nasledujúce informácie o sieťových podmienkach:

- Mechanizmus pre účastníkov, ktorý sú zahrnutý v RTP relácií, pre výmenu informácií o monitorovaní a riadení relácie. RTCP monitoruje kvalitu elementy ako napr. počet paketov, ich stratu, oneskorenie a *jitter* medzi jednotlivými paketmi. RTCP vysiela pakety ako percentuálny podiel šírky pásma danej relácie, o špecifickej intenzite, najmenej každých 5 sekúnd.
- Časová známka NTP (Network Time Protocol) protokolu je založená na synchronizovaných hodinách. RTP časová známka je náhodne generovaná a založená na vzorkovaní dátových paketov. RTCP používa obe informácie NTP a RTP protokolov.
- Pridelením UDP portu hlasovému prúdu je RTP typicky priradené párne číslo portu, a RTCP ďalší nepárny port. Každý hovor má priradené 4 porty – RTP + RTCP vo vysielačom smere a RTP + RTCP v smere pre príjem [7].

#### 4.5.1 Aplikácia RTP a RTCP

Hlasové pakety vyslané po sieti môžu ísť k cieľu jednou, prípadne viacerými cestami. Každá cesta pritom môže mať rozdielnu dĺžku a rýchlosť, čo môže viesť k tomu, že pakety môžu doraziť do cieľa mimo poradia.

K eliminácii tohto nežiaduceho efektu, RTP značí pakety časovou známku a sekvenčným číslom. Vďaka tomu, na cieľovej stanici, RTP môže zoradiť pakety a poslať ich DSP (Digital Signal Processor) procesoru na ich reprodukciu v poradí takom, akom boli odoslané.

Počas trvania každej RTP relácie, sa generujú RTCP *report* pakety najmenej každých 5 sekúnd. V prípade zlých sieťových podmienok sa hovor môže ukončiť z dôvodu vysokého počtu stratených paketov. Analýzou RTCP paketov je možné zistiť informácie ako napr. počet paketov, počet oktetov, počet stratených paketov alebo *jitter*, ktoré môžu pomôcť odhaliť prečo bol hovor zrušený.

#### 4.5.2 Kompresia RTP hlavičky

RTP pracuje na transportnej vrstve (podľa modelu ISO OSI), pričom je zapuzdrený do UDP segmentu a potom do IP paketu. Súčtom hlavičiek IP, UDP a RTP protokolov vzniká 40 bajtov *overhead*. Avšak pôvodná implementácia G.729 protokolu a určuje, aby hlasové dáta (*payload*) boli iba 20 bajtov, čo je polovica veľkosti riadiacich dát v hlavičkách.

Spoločnosť Cisco využíva funkciu nazvanú RTP *Header Compression* (cRTP), ktorá redukuje 40 bajtovú hlavičku iba na 2 až 4 bajty.



Obr. 14. Kompresia RTP hlavičky.<sup>10</sup>

<sup>10</sup> - Obrázok použitý z [7].

V princípe táto technológia nekomprimuje hlavičku ale len využíva fakt, že väčšina informácií obsiahnutých v IP, UDP a RTP hlavičkách sa počas hovoru nemení. Ide o informácie ako napr. zdrojové a cieľové IP adresy, čísla UDP portov alebo typ dát v RTP. Preto namiesto týchto nadbytočných informácií v každom pakete, cRTP umožňuje aby smerovače na každom konci linky uchovali tieto informácie v *cache* pamäti a posielali v hlavičke iba informácie ako sú UDP kontrolný súčet a *Context ID* relácie, ktorý identifikuje RTP reláciu, ktorej dané pakety patria [7].

## 4.6 VoIP Sieťová architektúra

Jednou z výhod VoIP technológie je možnosť voľby sieťovej architektúry, ktorá môže byť centralizovaná alebo distribuovaná. Táto flexibilita umožňuje organizáciám budovať siete tak aby mali jednoduchý manažment a aby inovácie mali požadovaný efekt.

### 4.6.1 Centralizovaná architektúra

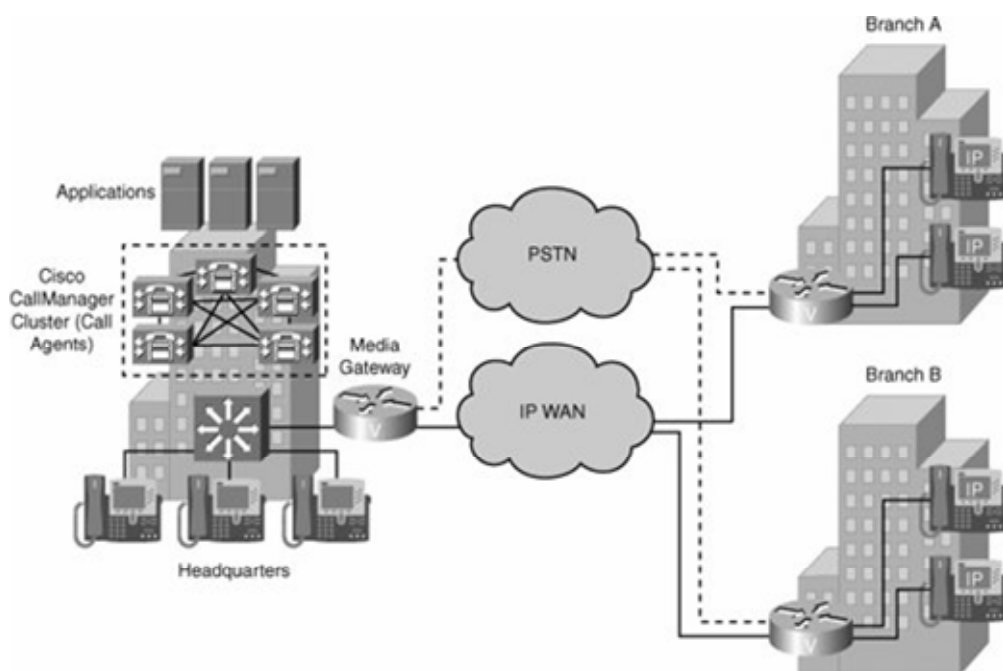
Obrázok č.15 zobrazuje nasadenie centralizovanej architektúry spracovania hovoru s *cluster* Cisco CallManager, ktorý vystupuje ako *call agent* v centrálnom sídle a IP WAN s QoS pravidlami v pripojených sídlach. Vzdialené pobočky sa spoliehajú na Cisco CallManager *cluster* pre spracovanie ich hovorov, ale majú tiež lokálne smerovače s podporou hlasových služieb, ktoré slúžia ako hlasová brána. Každá pobočka je tiež pripojená k lokálnej PSTN sieti.

Tento typ architektúry pozostáva z nasledujúcich komponentov:

- **Central gateway controller** (*Call Agent*) – Pracuje s prepínacou logikou a riadi hovory pre všetky pobočky. Tento radič zahrnuje centralizovanú konfiguráciu, a tiež správu riadenia hovorov. Pridaní funkcionality sa aktualizuje iba tento radič.
- **Média brána** (*Media Gateway*) – Poskytuje fyzické prepojenie medzi telefónnou sieťou, individuálnymi koncovými bodmi a IP sieťou. Média brány komunikujú s *call agent* pre upozornenie na udalosť, pre určenie akcie. Po výmene riadiacich dát hovoru brána smeruje vysiela audio alebo média hovoru.
- **IP WAN** – nesie ako riadiacu signalizáciu, tak i samotné hlasové dáta hovoru medzi centrálnym sídlom a pobočkami. QoS konfigurácia je nevyhnutná pre správne funkciu. Pre minimalizovanie šírky pásma použitú pre hlasový prúd

prechádzajúci cez WAN sieť je pre kompresiu hlasu používaný kódok G.729. Ten komprimuje hlas na 8 kbps na hovor oproti 64 kbps u tradičnej telefónie.

Typické použitie centralizovanej architektúry je príklad väčšej organizácie s niekoľkými menšími pobočkami. Jednotlivé pobočky sú pripojené cez WAN sieť s aplikovanými QoS pravidlami, pričom nevyžadujú všetky funkcie a funkcionality pri výpadku WAN. U tejto architektúry sa používajú prevažne MGCP alebo Megaco/H.248 signalizačné protokoly, pre riadenie brán a koncových bodov.



Obr. 15. Centralizovaná VoIP architektúra.<sup>11</sup>

Jedinou nevýhodou implementácie centralizovanej architektúry je, zlyhanie WAN spojenia medzi pobočkou a centrálou, v ktorej sa nachádza Cisco CallManager, pretože tým pádom nie je možné aby boli spracované hovory. Jedným z riešení je implementácia redundantných WAN liniek medzi pobočkou a centrálou. Riešením je použitie SRST (Survivable Remote Site Telephony) prístupu, ktorý poskytuje dostupnosť hlasových služieb. SRST obsahuje skupinu schopností spracovania hovoru v rámci brány pobočky.

<sup>11</sup> - Obrázok použitý z [7].

Táto funkcia umožňuje pobočkám pokračovať a poskytovať hlasovú konektivitu i v prípade zlyhania linky [7].

#### 4.6.2 Distribuovaná architektúra

Organizácie s pobočkami prepojenými pomocou WAN siete je možné zvoliť distribuovanú architektúru, čím každé sídlo je nezávislé pri spracovávaní hovorov. Každá pobočka, alebo sídlo spoločnosti má vlastný *call agent*, ktorý je pripojený k IP WAN, ktorá prenáša hlasovú prevádzku medzi distribuovanými pracoviskami. IP WAN ale nenesie žiadne riadiacu signalizáciu spojenú s hovormi. PSTN sieť potom slúži ako záloha spojenia v prípade, zlyhania WAN spojenia, alebo pri nedostatku šírky pásma.

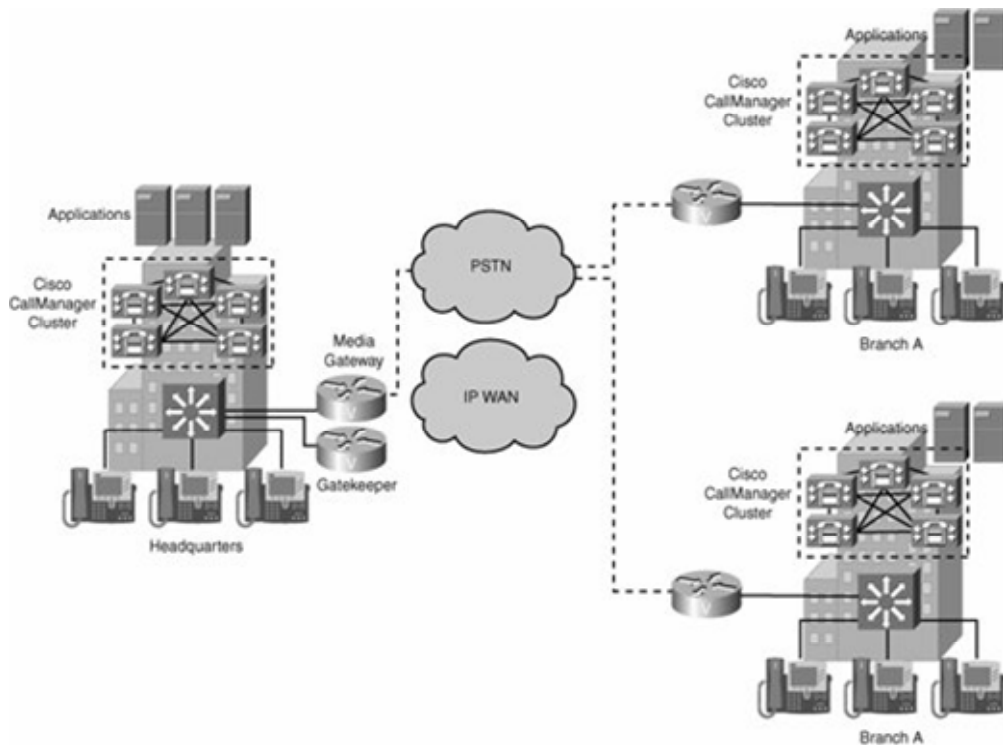
Pre distribuovanú architektúru sa používajú prevažne protokoly H.323 a SIP, pričom podľa použitého protokolu sa architektúra mierne odlišuje. Tieto protokoly obsahujú funkcie pre komunikáciu medzi koncovými bodmi a zariadeniami na riadenie hovorov. Ide o funkcie pri spracovávaní hovoru vrátane:

- Stav hovoru.
- Funkcie hovorov.
- Smerovanie hovorov.
- Doručovanie.
- Účtovanie.

#### 4.6.3 Distribuovaná architektúra založená H.323

Každé sídlo u distribuovanej architektúry používajúcej H.323 môže zahŕňať:

- Vlastný *call processing agent*.
- Pôvodnú PBX s VoIP bránou.
- Centralizované miesto pre spracovanie hovorov a pobočky.



Obr. 16. Distribuovaná architektúra na báze H.323.<sup>12</sup>

Na obr. č.16 je zobrazená distribuovaná architektúra na bázy signalizačného protokolu H.323, pričom každá pobočka má vlastného *call agent cluster*. Takýto prístup pozostáva:

- Cez IP WAN sa neprenáša žiadna signalizácia.
- Transparentné použitie PSTN siete v prípade nedostupnosti IP WAN.
- Iba jeden typ kódeku pre IP WAN.

U distribuovanej architektúry sú ako koncové body označované zariadenia, ktoré sú schopné iniciovať a ukončiť H.323 hovor. U sieti s protokolom H.323 sa riadiace zariadenie nazýva *gatekeeper*. U veľkých sietí sa niektoré riadiace zariadenie môžu označovať ako *directory gatekeeper*, pričom takéto zariadenia poskytujú súhrn viacerých *gatekeepers*.

WAN architektúra s distribuovaným spracovaním hovoru pozostáva z nasledujúcich komponentov:

---

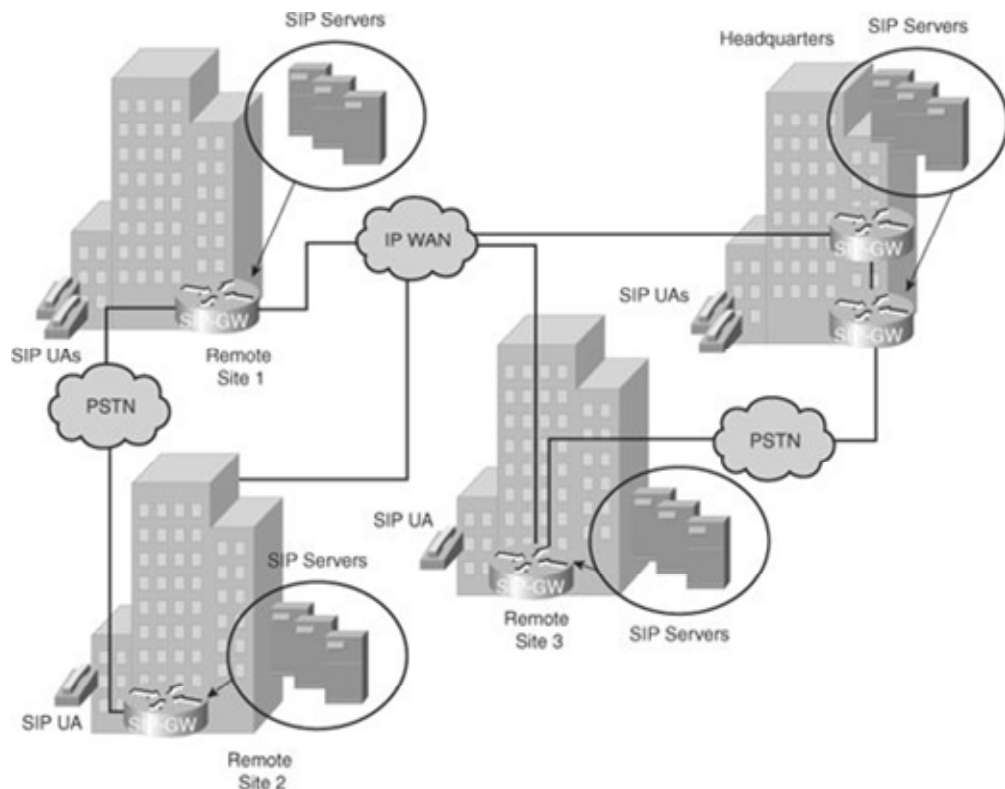
<sup>12</sup> - Obrázok použitý z [7].

- **Média brána** (Media gateway) – Služi rovnako ako u centralizovanej architektúry. Zároveň prekladajú hlasovú signalizáciu medzi PSTN alebo lokálnymi koncovými bodmi. Média brána musí obsahovať nástroje na vykonávanie funkcií spojené s H.323. Média brána komunikuje s *gatekeeper* pre určenie adresy hovoru a CAC (Call Admission Control).
- **Gatekeeper** – Je zariadenie, ktoré poskytuje CAC a E.164 rozlíšenie čísiel. Zároveň poskytuje *dial plan resolution*, ktorý vylepšuje rozšíriteľnosť H.323 siete. Bez *gatekeeper* každá brána musí byť nakonfigurovaná, kde sú ostatné telefóny umiestnené. *Gatekeeper* poskytuje centrálnu skladisko telefónnych čísiel a brán spojených s týmito číslami. Pri použití *gatekeeper* v sieti je proces učenia sa dynamicky, pretože všetky zúčastnené brány sa registrujú s *gatekeeper* a upozornia ho v prípade dostupnosti nového telefónu.
- **IP WAN** – Riadiaca signalizácia a samotný prenos hlasu všetkých vnútorných hovorov a hovorov mimo, ktoré majú ísť cez PSTN zostáva v rámci sídla (siete) [7].

#### 4.6.4 SIP Distribuovaná sieťová architektúra

Sieť na báze protokolu SIP pozostáva z niekoľkých komponentov, ktoré zobrazuje obrázok č.17:

- **SIP User Agent** – Koncové zariadenie v sieti, ktoré môže začať, alebo ukončiť SIP reláciu. Toto zariadenie môže byť telefón s podporou SIP, SIP PC klient (tzv. *softphone*) alebo SIP brána.
- **SIP Proxy Server** – Zariadenie na riadenie hovorov, ktoré poskytuje služby ako smerovanie SIP správ medzi SIP *User Agent*-mi.
- **SIP Redirect Server** – Zariadenie, ktoré poskytuje smerovacie informácie *User Agent* na vyžiadanie, pričom sa poskytuje URI (Uniform Resource Identifier) alebo cieľový UAS (User Agent Server).
- **SIP Registrar Server** – Zariadenie, ktoré ukladá logickú polohu *user agent* v rámci domény, alebo subdomény. SIP *Registrar Server* ukladá polohu *user agent* a dynamicky aktualizuje jeho dáta cez REGISTER správy.



Obr. 17. Distribuovaná SIP architektúra.<sup>13</sup>

SIP dodatočne poskytuje tieto funkcie:

- **Určenie polohy cieľového koncového bodu** – SIP poskytuje rozoznanie adres, mapovanie mien a presmerovanie hovorov.
- **Určenie mediálnych schopností koncového bodu** – Pomocou SDP protokol SIP rozlišuje „najnižšiu úroveň“ dostupných služieb medzi koncovými bodmi. Konferencie sú vytvorené na základe mediálnych schopností, ktoré podporujú všetkými koncovými bodmi.
- **Určuje dostupnosť cieľových koncových bodov** – Ak spojenie nemôže byť dokončené, pretože cieľový koncový bod je nedostupný, SIP určí či volaná strana práve telefonuje, alebo neodpovedá v stanovenom počte zvonení. SIP potom vráti správu, ktorá značí, prečo cieľový koncový bod bol nedostupný.

<sup>13</sup> - Obrázok použitý z [7].

- **Vytvorenie relácie medzi zahajujúcim a koncovým bodom** – Ak spojenie môže byť dokončené, SIP vytvorí reláciu medzi koncovými bodmi. SIP tiež podporuje medzi hovorové zmeny, ako napr. pridanie ďalšieho koncového bodu do konferencie, alebo zmena mediálnych vlastností alebo kódeku.
- **Spracováva prenos a ukončenie hovoru** – SIP podporuje prenos hovorov z jedného koncového bodu na iný. Počas hovoru SIP vytvorí reláciu medzi príjemcom a novým koncovým bodom určeným prenášajúcou stranou. SIP potom ukončí reláciu medzi pôvodnými stranami. Na konci hovoru, ukončí všetky relácie medzi všetkými stranami.

SIP ako protokol distribuovanej architektúry umožňuje spoločnostiam budovať rozsiahle siete, ktoré sú dobre rozšíriteľné, odolné a dimenzované na náročnú prevádzku. Protokol SIP poskytuje mechanizmy pre prepojovanie s inými VoIP sieťami a pre pridanie inteligencie a nových funkcií, či už koncovým bodom, alebo SIP *proxy* alebo *redirect* serverom [7].

#### 4.6.5 Porovnanie sieťových architektúr

Či už centralizovaný alebo distribuovaný model, oba majú výhody i nevýhody. Funkcie, ktoré sú považované ako výhoda u jedného modelu, môžu byť nevýhodou pre druhý. Hlavné rozdiely medzi týmito modelmi sú:

- **Konfigurácia** – Model centralizovaného riadenia hovorov poskytuje nadradenú konfiguráciu a údržbu *dial plan* a databázy koncových bodov. Tento model má jednoduchšie uvedenie nových funkcií a doplnkových služieb. Centralizovaný model tiež poskytuje vhodné umiestnenie pre zber a šírenie záznamov o detailoch hovoru. Distribuovaný model vyžaduje distribuovanú administráciu, konfiguráciu a manažment koncových bodov. Tento prístup komplikuje administráciu *dial plan*. Tento model naopak zjednodušuje nasadenie dodatočných koncových bodov, kým pridanie nových funkcií a dodatočných služieb je ťažšie implementovať.
- **Bezpečnosť** – Centralizovaný model vyžaduje aby koncové body boli známe centrálnej autorite. Takýto prístup redukuje bezpečnostné obavy, pričom autonómia koncových bodov u distribuovaného ich zase zvyšuje.

- **Spolehlivost** – Centralizovaný model má dva zranitelné body: jeden prvok zlyhania a súťaženie o prostriedky. To kladie vysoké nároky na dostupnosť dátovej siete, sieť WAN, tak aby zároveň bola odolná voči chybám. U distribuovaného modelu je minimalizovaná závislosť na zdieľanom komponente a sieťových zdrojoch. Zároveň redukuje riziká spojené s jedným bodom zlyhania súťaže o sieťové prostriedky.
- **Efektivita** – Nevýhodou je u centralizovaného modelu, nie je plne využitá schopnosť smerovať u koncových bodov. Interakcia medzi *call agent* a koncovými bodmi spotrebúva šírku pásma. U distribuovaného modelu je plne využitá možnosť smerovať hovory na koncových bodoch.

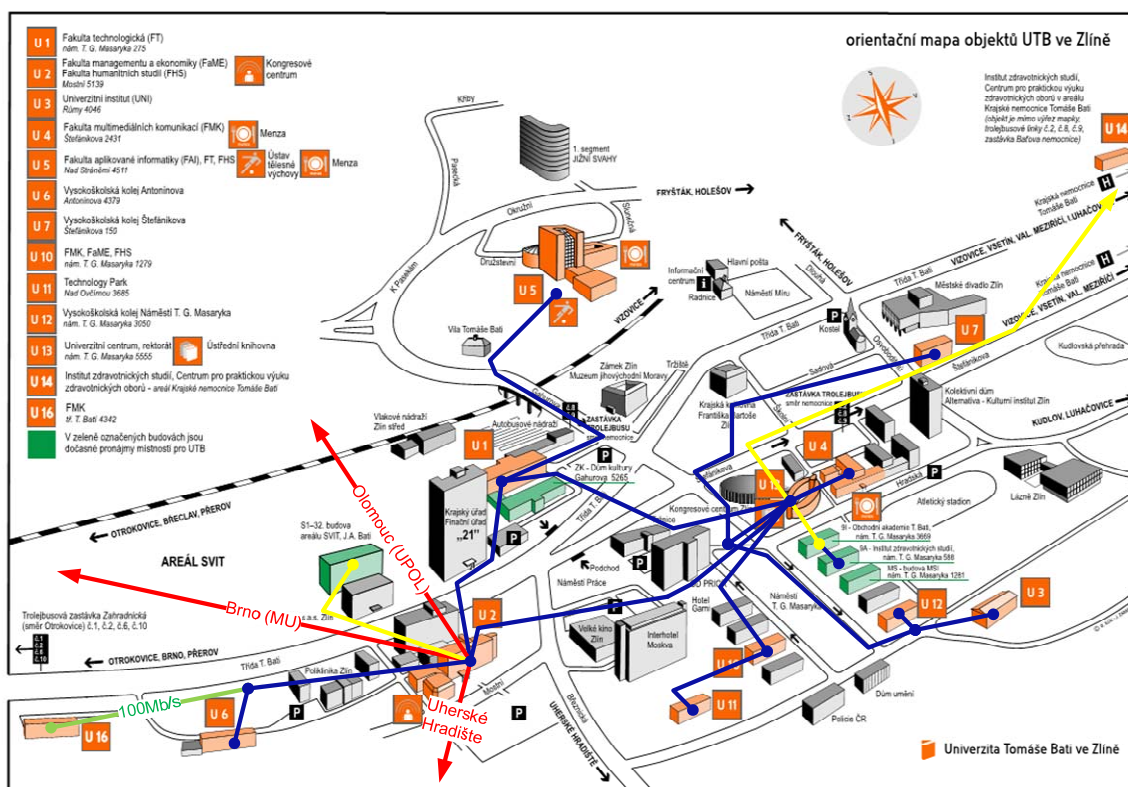
Nakoľko centralizovaný model je viac náchylný na výpadok WAN siete, musí tento návrh implementovať mechanizmy zabezpečujúce dostupnosť a manažment pre vyrovnávanie záťaže. Distribuovaná implementácia riadenia hovoru pomocou protokolov H.323 a SIP sa z dôvodu rozšíriteľnosti zväčša nasadzujú s bežným riadením komponentov, čo dáva koncovým bodom mnoho výhod centralizovaného riadenia. Toto však nesie nevýhody centralizovaného modelu [7].

## 5 ANALÝZA POČÍTAČOVEJ SIETE NA U5

**Pozn.:** Z dôvodu politiky informačnej bezpečnosti sú niektoré údaje pozmenené!

### 5.1 Analýza chrbticovej siete UTB ve Zlíně

Počítačová sieť FAI UTB nachádzajúca sa v budove U5 je pripojená k chrbtvej časti siete pomocou optickej kabeláže. Táto chrbticová sieť spája jednotlivé počítačové siete, ktoré sa nachádzajú v jednotlivých budovách univerzity a tiež i detašované pracoviská nachádzajúce sa v Uherském Hradišti, alebo v Prostějově. Detašované pracovisko v Prostějově používa prenajatú linku z Brna o rýchlosti 100 Mbps, pričom je virtuálnym tunelom prepojená s UTB ve Zlíně. Z tohto dôvodu používa i logickú štruktúru siete ako na UTB.



Obr. 18. Chrbticová optická sieť UTB ve Zlíně.

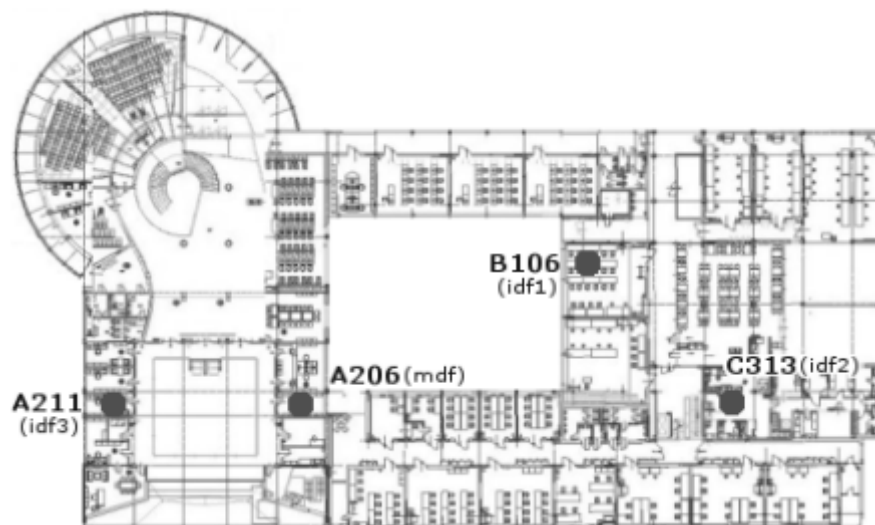
Obrázok č.18 zobrazuje chrbticovú optickú sieť UTB. Modrou farbou je vyznačená optická kabeláž, ktorá je vo vlastníctve UTB. Rýchlosť takýchto prepojení je 1 Gbps. Trasa medzi U6 a U16, ktorá je vyznačená zelenou farbou, je tiež vo vlastníctve UTB, ale jej rýchlosť je len 100 Mbps. Táto trasa je realizovaná mnohovidovými optickými vláknami. Trasy

vyznačené žltou farbou, označujú prenajaté linky od lokálnych poskytovateľov internetu, ktorý zabezpečujú konektivitu pre nové budovy univerzity. Červenou farbou sú označené linky prepojujú UTB s ostatnými univerzitnými počítačovými sieťami v Brne, Olomouci alebo v Uherském Hradišti.

Počítačová sieť budovy U5 je pripojená k uzlu nachádzajúceho sa v budove U1. Toto prepojenie je realizované pomocou optickej kabeláže, pričom spoj je realizovaný pomocou 72 optických vlákien (48x jednovidových, 24x mnohovidových). V súčasnosti je použitý ale len jeden pár jednovidových vlákien, vďaka čomu je zabezpečená 1 Gbps *full duplex* konektivita. Z tohto spoja následne pokračuje optická kabeláž do budovy rektorátu U13, kde je pripojená k hlavnému L3 prepínaču Cisco 6509. Ide o modulárny prepínač s podporou prepínania na viacerých vrstvách a primárne pre UTB slúži ako smerovač. Zároveň obsahuje i *Firewall* modul, ktorý zabezpečuje počítačovú sieť. Tento centrálny prvok je zároveň pripojený k sieti spoločnosti Cesnet z.s.p.o., ktorá zabezpečuje internetové pripojenie pre univerzitu. Toto pripojenie je realizované 10 Gbps optickým prepojením, pričom je ukončené v smerovači Cisco 7609, odkiaľ ďalej ide do miest Brno a Olomouc 10 Gbps optickou linkou založenou na DWDM (Dense Wavelength Division Multiplexing) multiplexe.

## 5.2 Analýza rozvodov na U5

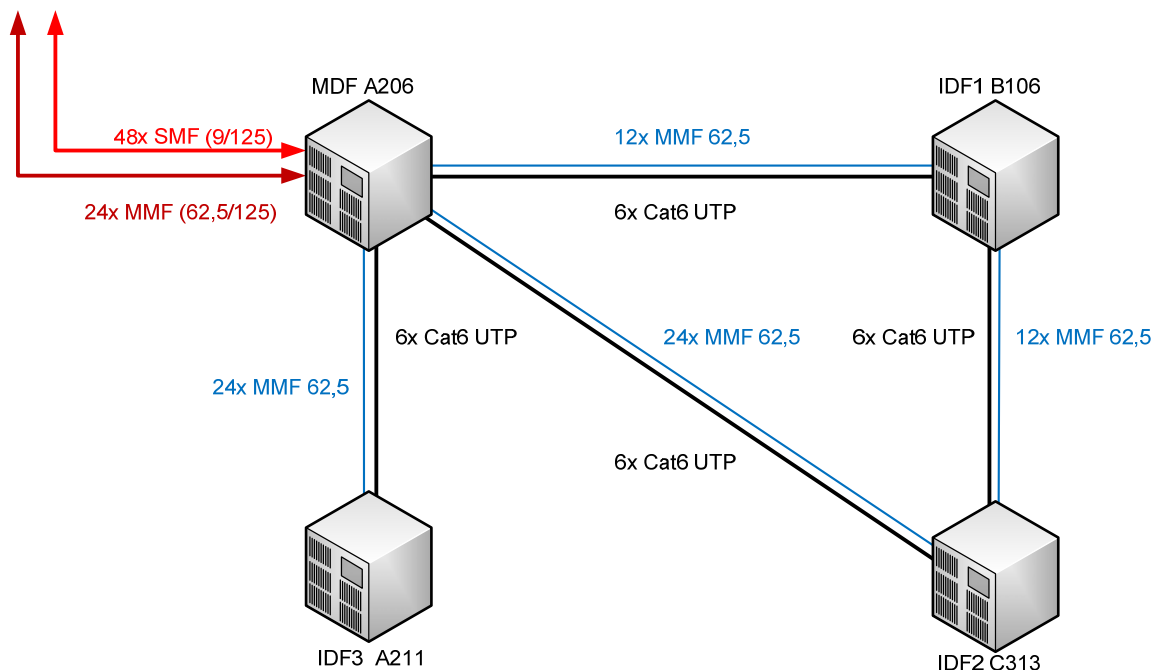
Súčasná podoba počítačovej siete na U5 používa 4 rozvodne, pričom dve sa nachádzajú v časti 51, a zvyšné 2 sú umiestnené po jednej v častiach U52 a U53.



Obr. 19. Rozloženie rozvodní na U5.

Obrázok č.19 zobrazuje rozmiestnenie jednotlivých rozvodní na U5. Hlavná rozvodňa je označená ako MDF (Main Distribution Frame) a nachádza sa v miestnosti A206. Rozvodne označené ako IDF (Intermediate Distribution Frame) sú prepojené s hlavnou rozvodňou, pričom rozvodne IDF1 a IDF2 sú zároveň prepojené i navzájom. V hlavnej rozvodni sú zároveň ukončené optické káble, pripojujúce lokálnu počítačovú sieť na U5 do chrbticovej časti siete. Medzi rozvodňami sú natiiahnuté mnohovidové optické vlákna a i metalická kabeláž. Celá metalická kabeláž, ako i všetky pasívne prvky pre prepojovanie sú vo vyhotovení kategórie 6.

Obrázok č.20 zobrazuje ako sú prepojené jednotlivé rozvodne. Jednotlivé rozvodne sú prepojené ako metalickými káblami Cat-6 typu UTP, tak i optickými káblami. V súčasnosti sú aktívne prvky siete prepojené len jedným metalickým káblom, pričom je dosiahnutá 1 Gbps rýchlosť v režime plného duplexu.



Obr. 20. Prepojenie jednotlivých rozvodní.

### 5.3 Analýza aktívnych prvkov siete

Jednotlivé aktívne prvky sú umiestnené v jednotlivých rozvodniach, pričom v hlavnej MDF rozvodni je umiestnený chrbticový prepínač, ktorý pripojuje počítačovú sieť na U5 s chrbticovou sieťou UTB. Štruktúra aktívnych prvkov na U5 je usporiadaná do hierarchického sieťového modelu, pričom v každej rozvodni sú umiestnené prepínače

prístupovej a distribučnej vrstvy. Prepínače distribučnej vrstvy sú následne prepojené s hlavným prepínačom, ktorý sa nachádza v hlavnej rozvodni na A206.

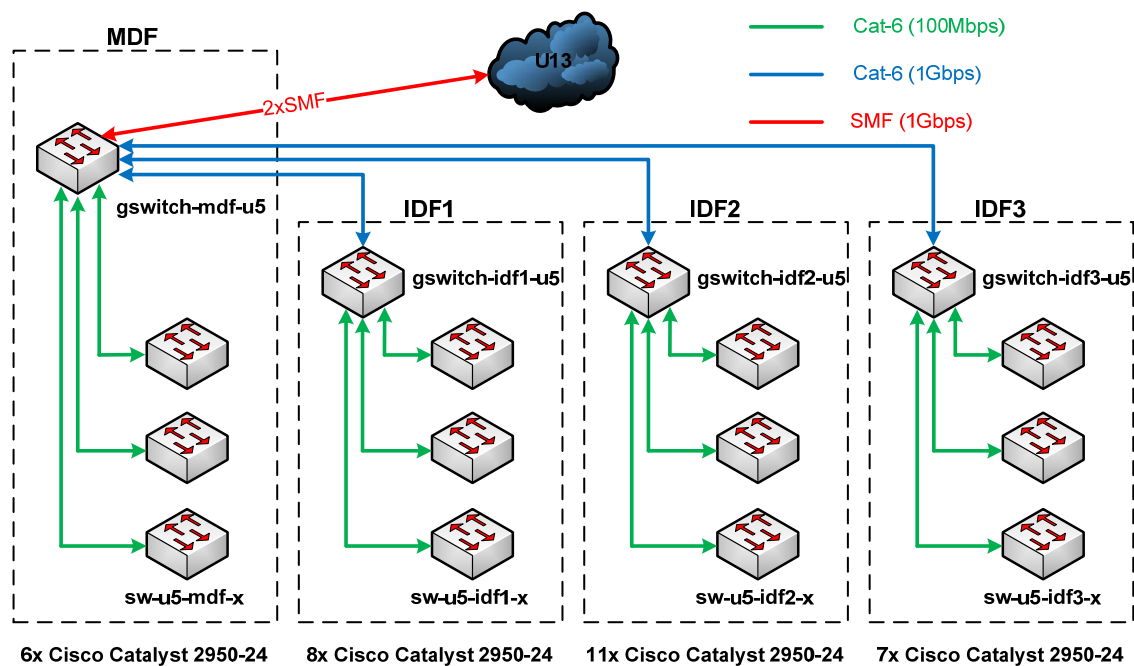
V každej rozvodni je použitý distribučný prepínač Cisco Catalyst 3560G-48PS. Ide o prepínač o veľkosti 1U, s pevnou fyzickou konfiguráciou portov. Tento prepínač obsahuje 48x 10/100/1000 Mbps portov s podporou PoE (Power over Ethernet) a 4x 1 Gbps SFP (Small Form-Factor Pluggable) porty. Tieto prepínače sú pomenované ako:

- **gswitch-u5-mdf**,
- **gswitch-u5-idf1**,
- **gswitch-u5-idf2**,
- **gswitch-u5-idf3**.

Prepínač označený ako **gswitch-u5-mdf** zároveň slúži ako hlavný prepínač ktorý prepojuje ostatné distribučné prepínače umiestnené v jednotlivých rozvodniach. Pomocou SFP portov je k tomuto prepínaču pripojená optická linka, ktorá spojuje sieť s hlavným prepínačom na U13. Prepojenie optickej linky a hlavného prepínača je pomocou LC konektorov.

Prepínače pracujúce na distribučnej vrstve slúžia k pripojeniu prepínačov z prístupovej vrstvy a v určitých prípadoch i k samotnému pripojovaniu zariadení, ako sú prístupové body, serveri a podobne.

Ako prepínače prístupovej vrstvy sú použité zariadenia Cisco Catalyst 2950-24, ktoré majú 24x 10/100 Mbps portov. V súčasnosti je použitých 32 takýchto prepínačov pre pripojenie jednotlivých koncových zariadení. Každý prepínač slúži k pripojeniu 23 koncových zariadení, pretože posledný 24. port je použitý ako *uplink* pre pripojenie prepínača k distribučnému prepínaču v rozvodni. Tieto prepínače sú pomenované na základe rozvodne, v ktorej sa nachádzajú a poradového čísla v rozvodni. Príkladom môže byť 3. prepínač nachádzajúci sa v rozvodni IDF1. Prepínač bude teda mať meno v tvare: **sw-u5-idf1-3**.



Obr. 21. Logická topológia aktívnych prvkov siete na U5.

Obrázok č. 21 zobrazuje topológiu aktívnych prvkov na U5. Prepínače prístupovej vrstvy sú pripojené k prepínačom na distribučnej vrstve. Toto prepojenie je zobrazené zelenou farbou. Fyzicky je toto prepojenie realizované metalickou kabelážou Cat-6, pričom rýchlosť takejto linky je iba 100 Mbps. Distribučné prepínače sú prepojené s hlavným prepínačom znova UTP káblom Cat-6, ale operačná rýchlosť je 1 Gbps.

Tab. 6. Obsadenie jednotlivých rozvodní.

Rozvodňa	Počet prepínačov	Počet portov	Počet dostupných portov pre koncové zariadenia
MDF	6	144	138
IDF1	8	192	184
IDF2	11	264	253
IDF3	7	168	161
Celkovo	32	768	736

Kabeláž a zároveň všetky pasívne prvky použité pre pripojenie jednotlivých koncových zariadení k prepínačom na prístupovej vrstve je realizovaná prvkami kategórie 6, pričom

kabeláž je vo vyhotovení UTP. Koncové zariadenia sú pripojené 100M s *full duplex* linkou. Nevýhodou tohto zapojenia, že všetky koncové zariadenia zdieľajú jednu 100 Mbps *uplink* linku.

## 5.4 Analýza bezdrôtovej siete na U5

Bezdrôtové prístupové body sú v rozvodni pripojené k distribučným prepínačom v jednotlivých rozvodniach metalickou kabelážou kategórie 6. Tieto prístupové body sú súčasťou prístupovej vrstvy, nakoľko poskytujú bezdrôtové pripojenie do počítačovej siete na U5 pre koncové zariadenia, ktoré podporujú technológiu WIFI (Wireless Fidelity). V súčasnosti sa oficiálne na FAI UTB prevádzkuje len bezdrôtová sieť **eduroam**, ale pri skenovaní prostredia je možné nájsť ďalšie neoficiálne bezdrôtové siete. Tieto siete výsledkom pripojenia domácich bezdrôtových smerovačov do siete. Prevádzkou takýchto neoficiálnych sietí môžu pri nesprávnom nastavení alebo manipulácií spôsobovať problémy, ako napr. rušenie na kanáli siete eduroam, alebo posielanie DHCP správ, ktoré pridelujú nastavenia zariadeniam.

### 5.4.1 Bezdrôtová sieť eduroam

V súčasnosti je na U5 rozmiestnených 12 prístupových bodov spoločnosti Cisco. Ide o prístupové body 6x **Aironet 1242AG** a 6x **Aironet 1231**. Päť z týchto 12 prístupových bodov je umiestnených na prízemí a prvom podlaží, 2x na druhom podlaží, 3x na treťom podlaží a po jednom na šiestom a ôsmom podlaží výškovej budovy U5.



Cisco Aironet 1242G



Cisco Aironet 1231

Obr. 22. Typy bezdrôtových prístupových bodov na U5.

Obrázky zobrazujúce fyzické rozmiestnenie jednotlivých prístupových bodov bezdrôtovej siete eduroam spolu s vysielajúcimi kanálmi sú umiestnené ako príloha pod číslom 4, 5, 6, 7 a 8.

## 5.5 Analýza logického zapojenia siete

Počítačová sieť na U5 je rozdelená pomocou VLAN technológie na niekoľko logických častí, pričom každá takáto logická časť – VLAN sieť má vlastný adresný priestor. Výhodou takéhoto delenia je zmenšenie *broadcast* domény a logické rozdelenie jednotlivých sieťových tokov od seba. Nakoľko sú ale tieto jednotlivé siete oddelené použitím rozdielnych VLAN identifikátorov a adresných priestorov, je potreba aby dáta, putujúce z jednej VLAN siete do druhej, boli presmerované smerovačom. Ten sa ale nachádza na U13 budovy rektorátu. Tento smerovač je centrálny smerovací prvok siete, ktorý pripája všetky siete a smeruje ich požiadavky, pričom ide o smerovač Cisco 6509 ktorý je prepojený so sieťou Cesnetu.

Tab. 7. Tabuľka VLAN sietí na U5.

Číslo VLAN	Označenie	Rozsah IP adres
50	Management	10.5.5.0/24
51	U5 Zamestnanci	10.5.16.0/22
52	Učebne, študovne	10.5.160.0/22
54	Zamestnanci_Old	199.187.98.0/24 199.131.98.128/25 199.131.99.128/27
55	Zamestnanci/Servery	199.187.49.0/26
59	U5-WIFI-EDU-ROAM	10.5.140.0/23

Toto rozdelenie VLAN sietí je distribuované na všetky prepínače UTB pomocou protokolu VTP (VLAN Trunking Protocol). Zoznam týchto VLAN sietí je udržiavaný na hlavnom smerovači, pričom z pohľadu protokolu VTP je smerovač v režime server a ostatné prepínače v režime klient. Nevýhodou tohto riešenia je všetky VLAN v zozname sú

distribúované na klientske prepínače. To môže predstavovať problém, najmä pre prístupové prepínače, ktoré majú obmedzený počet VLAN, ktoré môžu uchovať. Napr. prístupový prepínač Cisco Catalyst 2950-24 pri najnovšej verzii (verzia 12.1(22)EA 14) operačného systému podporuje 128 VLAN sietí.

Tabuľka č.7 zobrazuje VLAN siete, ktoré sa používajú v počítačovej sieti na U5. Sieť VLAN s číslom 50 sa používa pre manažment aktívnych sieťových prvkov. Sieť s č. 51 je použitá pre zamestnancov U5. Sieť č.52 je vyhradená pre učebne a študovne na U5. Siete číslo 54 a 55 používajú verejný rozsah adries a sú použité predovšetkým pre niektorých učiteľov (z Technologickej fakulty) a servery nachádzajúce sa na U5. Siete vždy ako *default gateway* používajú prvú možnú adresu z rozsahu.

Tab. 8. Ostatné VLAN siete na U5.

Ostatné VLAN siete na U5	
82	MENZY
641	TELEPHONE-CENTRAL
642	MAR
644	PRINT-SERVICES
645	DVP
648	ACCESS-SYS
664	MONET

Tabuľka č.8 zobrazuje ďalšie VLAN siete, ktoré sa používajú na U5. Ide o také siete, ktoré sa používajú na celej univerzite, alebo sú súčasťou väčšieho bloku adries a sieťový tok potrebuje byť oddelený.

Použitím len jedného centrálného smerovača je zrejma ďalšia nevýhoda a to, že všetka prevádzka, ktorá potrebuje prebiehať medzi jednotlivými VLAN sieťami musí byť odoslaná na tento centrálny smerovač, ktorý presmeruje dáta do danej VLAN siete. Zároveň sa cez túto *trunk* linku šíria *broadcast* rámce, ktoré by mal byť mali ostať na U5 a nezaťažovať tak túto linku a centrálny smerovač.

## 5.6 IP Telefónia

V súčasnosti UTB okrem niektorých budov používa IP telefóniu. Ide o budovy U1, U2, U3, U4, U5 a U10. Táto IP telefónia je založená na riešení od spoločnosti Siemens, ktorá používa svoj vlastný proprietárny protokol HFA (HiPath Feature Access), ktorý zabezpečuje riadiacu signalizáciu i správu hovorov.

Kľúčový prvok IP telefónie tvorí ústredňa HiPath 4000 od spoločnosti Siemens. Tá je na U13 pripojená do LAN siete. Vo svojej podstate je to server so špecializovaným softwarom u ktorého sa registrujú jednotlivé IP telefóny. Zároveň táto ústredňa poskytuje presmerovanie medzi jednotlivými IP, analógovými a digitálnymi telefónmi pomocou ďalšej digitálnej ústredne. IP a digitálne ústredne sú medzi sebou prepojené, čím sa zabezpečí konektivita medzi telefónmi pripojenými rozdielnymi ústredňami. IP telefóny sú tiež použité od spoločnosti Siemens, modelová rada OpenStage.

## **PRAKTICKÁ ČASŤ**

## 6 NÁVRH MODERNIZÁCIE POČÍTAČOVEJ SIETE NA U5

Počítačová sieť na U5 od svojho vzniku prešla niekoľkými zmenami, pričom sa menili, alebo pridávali najmä aktívne prvky siete, tak aby sieť vyhovovala požiadavkám či už na fungovanie, správu, alebo potrebám jej užívateľov.

V súčasnosti počítačová sieť na U5 je v štádiu kedy ešte vyhovuje požiadavkám, ktoré sú na ňu kladené, ale s postupom času a príchodom nových služieb sa sieť ocitne vo fáze, kedy už jej výkon nemusí postačovať. Z tohto dôvodu je potrebné, aby sieť mala plán, ktorý bude určovať fázy modernizácie tak, aby zohľadňoval požiadavky výkonu ako i ekonomickej realizateľnosti, takéhoto plánu. Stavbou nového vedecko-výskumného ICT parku v blízkosti U5, ponúka nové možnosti pri návrhu modernizácie počítačovej siete na U5. Toto vedecko-výskumné centrum bude okrem iných projektov zamerané i na *Grid Computing* a *Cloud Computing*, pričom tieto projekty sa vyznačujú vysokou sieťovou aktivitou. Z tohto dôvodu je potrebné, aby navrhovaná sieťová infraštruktúra počítala i s touto alternatívou.

### 6.1 Požiadavky na modernizáciu

Pre budúce fungovanie počítačovej siete boli definované nové požiadavky, ktoré sa zameriavajú najmä na zvýšenie výkonu a efektivity, ktoré sú kritické pri nasadzovaní budúcich služieb v počítačovej sieti. Ide o:

- **Zvýšenie priepustnosti** – Jednou zo základných požiadaviek pri modernizácii je zvýšenie dátovej priepustnosti. Toto môže byť dosiahnuté technológiami, ako napr. agregáciou liniek, alebo inštalovaním nových zariadení, ktoré podporujú rýchle protokoly ako napr. 10 Gbps Ethernet. Medzi nové rýchlostné požiadavky na sieť patria zvýšenie rýchlosti u distribučnej časti siete na U5 na 10 Gbps, zvýšenie rýchlosti linky, ktorá pripojuje sieť na U5 k chrbticovej sieti na 10 Gbps a zvýšenie prístupovej rýchlosti na 1 Gbps pre koncové zariadenia.
- **Zvýšenie efektivity fungovania** – Základom bezproblémového fungovania siete nie je len samotná sieťová infraštruktúra, ale tiež i použitý logický model. Aby výkon siete bol využívaný na plno, je potrebné, aby boli nasadené také technológie, ktoré uľahčia správu, znížia, alebo odstránia nedostatky, zvýšia efektivitu pri používaní a podobne. Medzi jednotlivé požiadavky patrí odstránenie parazitnej

prevádzky, navrhnutie novej logickej štruktúry siete a nasadenie takých technológií, ktoré zlepšia funkčnosť a jednoduchosť siete.

- **Zvýšenie zabezpečenia a dostupnosti** – Navrhované riešenie by zároveň malo byť odolné proti výpadku určitého komponentu tak aby neboli narušené procesy a bola zaručená dostupnosť. Modernizácia by tiež mala zvyšovať bezpečnosť siete.
- **Zvedenie moderných technológií** – Medzi ďalšie požiadavky je zavedenie technológií ako napríklad PoE, ktoré umožnia nasadiť IP telefóniu bez potreby použitia napájacieho adaptéru. Navrhované riešenie by zároveň malo zahrňovať integráciu IP telefónie, ktorá už na niektorých budovách UTB existuje.

## 6.2 Navrhované zmeny

Navrhovanú modernizáciu možno rozdeliť na dva rovnocenné návrhy. Je to z toho dôvodu, že stavbou ICT centra v blízkosti U5, vzniká možnosť zjednotenia počítačovej siete ICT parku so sieťou na U5 a ušetriť časť nákladov nákupom iných aktívnych sieťových prvkov, alebo pridať také zariadenia, ktoré budú zabezpečovať lepšiu funkčnosť počítačovej siete. Zároveň obe varianty modernizácie musia byť rozdelené do viacerých fáz, nakoľko jednorázová realizácia nie je v súčasnosti ekonomicky reálna. Taktiež u takejto modernizácie by bolo veľmi náročné zachovať kontinuitu interných procesov na fakulte. Z tohto dôvodu v nasledujúcej časti, bude uvedená prechodná modernizácia, ktorej cieľ je pripraviť podmienky pre navrhovaný úplný prechod. Táto prechodná modernizácia je základom pre obe varianty navrhovanej modernizácie.

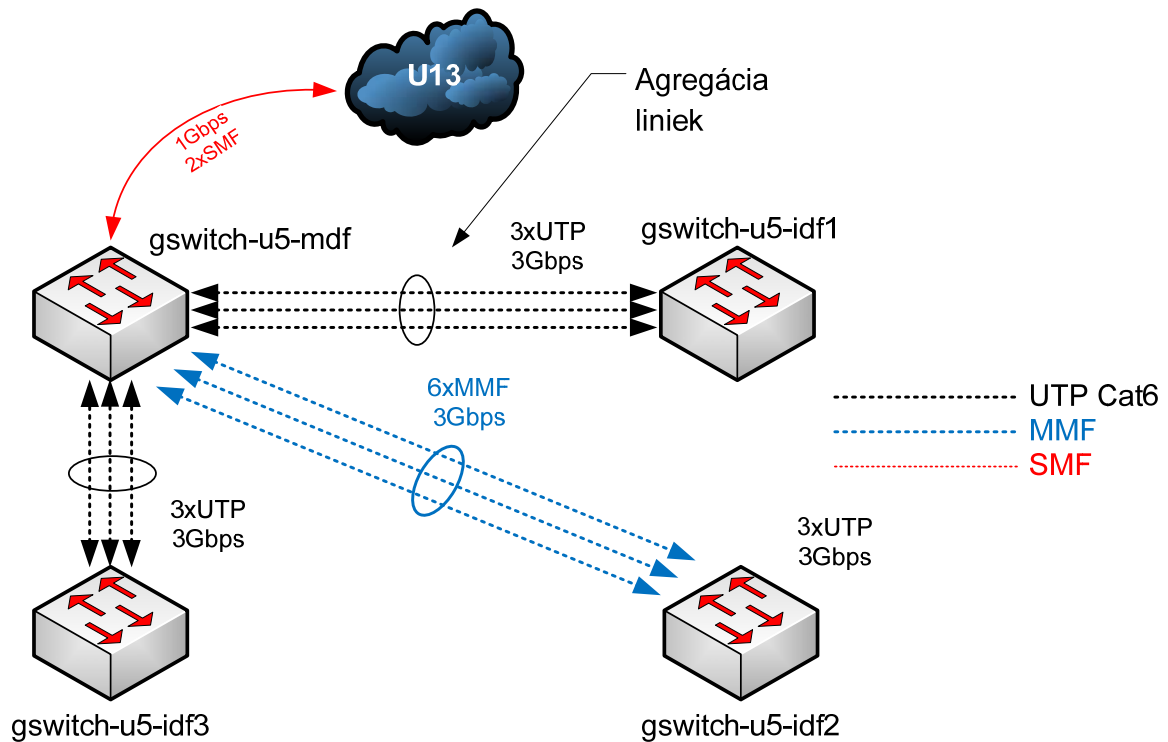
### 6.2.1 Prechodná modernizácia

Navrhovaná prechodná modernizácia využíva štandardný hierarchický model. Pričom z pohľadu U5 ide plnohodnotný model.

Súčasný stav počítačovej siete na U5 umožňuje čiastočné zvýšenie priepustnosti pomocou agregácie liniek. K tomuto účelu je výhodné použiť proprietárnu technológiu EtherChannel, nakoľko všetky prepínače nachádzajúce sa na U5 sú od spoločnosti Cisco.

Navrhovaná modernizácia bude využívať okrem stávajúcich zariadení i kabeláž. Táto agregácia liniek bude zvyšovať priepustnosť medzi distribučnými prepínačmi nachádzajúcich sa v rozvodniach IDF a hlavným prepínačom v MDF rozvodni.

Navrhované riešenie už raz bolo v prostredí U5 neúspešne inštalované. Chybou bola nekonzistentná inštalácia kabeláže a nedodržanie noriem pri použitej kabeláži, nakoľko použitá metalická kabeláž medzi hlavnou rozvodňou MDF a rozvodňou IDF2 je o niečo dlhšia než určuje štandard. Toto spôsobilo problémy pri použití technológie EtherChannel, nakoľko táto technológia je dimenzovaná na štandardnú dĺžku kabeláže.



Obr. 23. Možnosti agregácie liniek na U5.

Z vyššie spomenutých problémov, preto navrhované riešenie využíva ako metalickú, tak i existujúcu optickú kabeláž. Táto optická kabeláž bude použitá medzi prepínačmi **gswitch-u5-idf2** a **gswitch-u5-mdf**. Ostatné prepínače sú prepojené metalickou kabelážou.

Optické prepojenie využíva SFP *uplink* porty na distribučných prepínačoch v jednotlivých rozvodniach. Každý distribučný prepínač Cisco 3560G-48PS obsahuje 4 SFP porty. U hlavného prepínača v rozvodni MDF je tento jeden port použitý pre pripojenie siete na U5 k chrbticovej optickej sieti UTB. Na prepojenie medzi **gswitch-u5-mdf** a **gswitch-u5-idf2** zostávajú tri SFP porty, ktoré je možné použiť a pomocou technológie EtherChannel logicky spojiť a získať tak priepustnosť 3 Gbps *full duplex*. K tomuto účelu je potreba použiť 6 mnohovidových vlákien, aby vznikla daná priepustnosť. Ostatné prepínače sú prepojené metalickou kabelážou. Počet liniek zapojených do agregácie závisí od toho koľko je dostupných portov na prepínačoch pre vytvorenie agregácie a vytvárania linky.

Navrhovaná agregácia medzi distribučnými prepínačmi a hlavným prepínačom využíva je realizovaná pomocou 3x UTP káblu. Agregovaním týchto liniek sa zvýši šírka pásma na 3 Gbps. Navrhovaná modernizácia je zobrazená na obrázku č.23. Agregovaním liniek sa zvýši najmä dátová priepustnosť u prevádzky, ktorá zostáva v jednej VLAN. Ďalšou čiastočnou výhodou je zavedenie „skrytej“ redundancie pomocou paralelných liniek. Pri výpadku jednej linky v rámci agregovaného kanálu bude prevádzka presmerovaná na ostatné.

Kým táto navrhovaná modernizácia zvyšuje najmä priepustnosť chrbticovej časti siete na U5 jej hlavný problém zostáva nevyriešený. Ide tzv. *bottleneck* problém linky, ktorá pripojuje sieť na U5 k chrbticovej časti siete na U13.

Zvýšením priepustnosti medzi distribučnými prepínačmi a hlavným prepínačom sa zvýši priepustnosť najmä u prevádzky, ktorá zostáva v rovnakej VLAN sieti. Nakoľko pomer prevádzky, ktorá zostáva v tej istej VLAN sieti, oproti prevádzke, ktorá je smerovaná von na hlavný prepínač, je výrazný v prospech k odchádzajúcej. Toto predstavuje problém, pretože hlavný prepínač nevláda tak rýchlo odosielať rámce, a preto musí uchovávať prijaté rámce, ktoré majú byť odoslané na hlavný L3 prepínač na U13.

Riešením tohto problému je v zrýchlení linky, ktorá pripojuje počítačovú sieť na U5 k chrbticovej sieti na 10 Gbps. Problémom je, že súčasný hlavný prepínač na U5 neumožňuje nasadenie takejto technológie. Z tohto dôvodu je potreba ho nahradiť za taký prepínač, ktorý umožní navrhovanú modernizáciu.

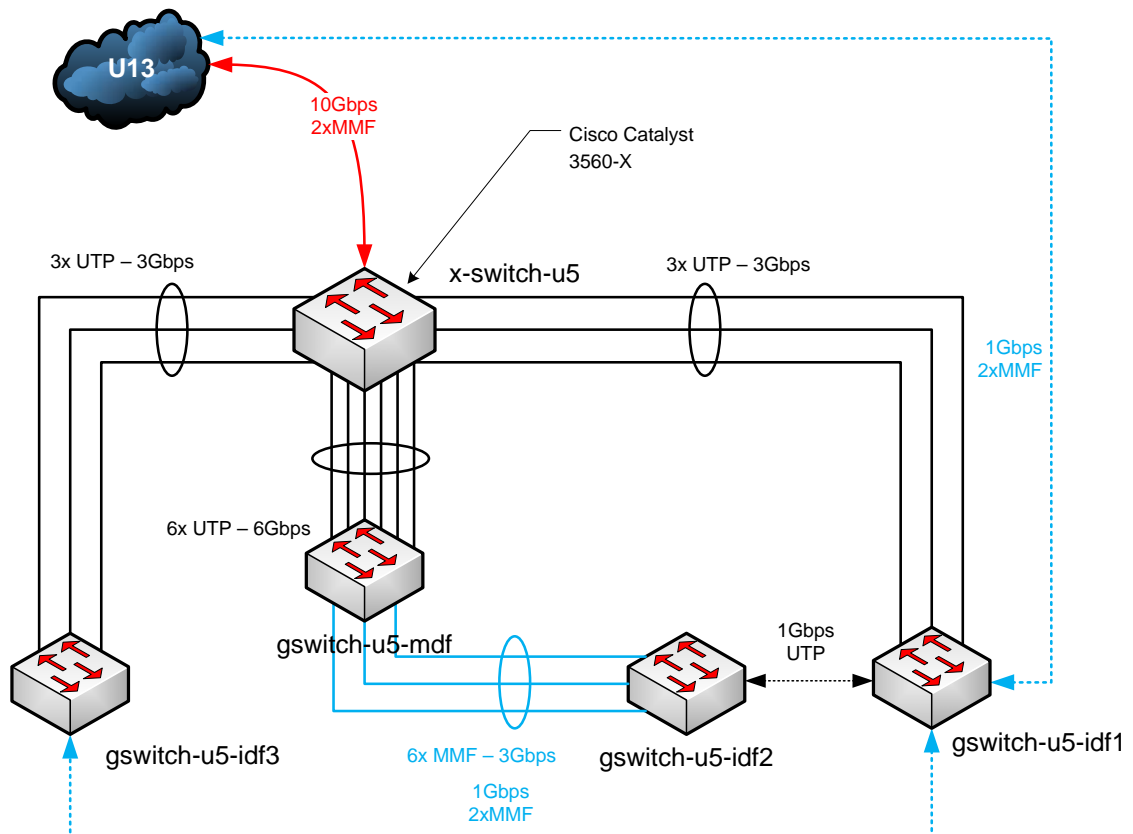
Pri výbere prepínača treba prihliadať najmä na jeho budúce využitie. Preto by mal spĺňať nasledujúce požiadavky. Ide najmä o podporu 10 Gbps protokolu po optickej kabeláži, nakoľko inštalovaná metalická kabeláž nie je vhodná na nasadenie takéhoto protokolu. Ďalšou požiadavkou je výkon takéhoto prepínača, aby jeho vnútorná priepustnosť dokázala obslúžiť dané množstvo rámcov a netvoril sa nové úzke miesto v komunikácií. Ďalším faktorom, ktoré ovplyvňuje výber prepínača je počet portov a jeho ďalšie funkcie, ako napr. L3 funkcie.

Nakoľko definované požiadavky určujú, aby distribučné prepínače v jednotlivých rozvodniach boli pripojené k hlavnému pomocou 10 Gbps protokolu. Toto nie je realizovateľné bez investície do nových distribučných prepínačov, ktoré budú podporovať takýto protokol. Tento stav sa dá preklenúť zaobstaraním nového prepínača, ktorý bude

podporovať 10 Gbps protokol, pričom sa využije navrhovaná agregácia liniek. Tento typ prepínača bude vo finálnej navrhovanej modernizácii slúžiť ako distribučný prepínač.

Pre túto navrhovanú modernizáciu je vhodné použiť Cisco prepínač rady Catalyst 3560-X. Konkrétne je použitý model **WS-C3560X-24T-S**, ktorého operačný systém podporuje základné IP služby. Nakoľko tento prepínač i po prechodnej fáze bude slúžiť iba ako agregátor prístupových prepínačov, nie je potrebné aby obsahoval funkcionality PoE a taký počet portov ako prístupové prepínače. Navrhovaný prepínač obsahuje 24x 10/100/1000 Mbps portov, pričom 10 Gbps konektivita je zabezpečená pomocou voliteľného sieťového modulu **C3KX-NM-10G**, ktorý má 2x SFP+ a 2xSFP *uplink* porty. V danej fáze modernizácie bude tento prepínač slúžiť ako prepínač, ktorý vykonáva smerovanie medzi VLAN sieťami a tým pádom rozdeľuje *broadcast* doménu. SFP/SFP+ porty neslúžia pre priame pripojenie optického, prípadne metalického kábla, ale pre pripojenie príslušného modulu, ktorý zabezpečuje komunikáciu. Pre zabezpečenie 10 Gbps konektivity pomocou jednovládneho vlákna je potrebné použiť **Cisco SFP-10G-LR** SFP+ modul. Tento modul dokáže zabezpečiť 10 Gbps komunikáciu na vzdialenosť až 10 km.

Produktová dokumentácia prepínača Cisco Catalyst 3560-X je umiestená ako príloha č.13 na CD-ROM.



Obr. 24. Navrhovaná prechodná modernizácia.

Obrázok č.24 zobrazuje prechodnú modernizáciu. Hlavný prepínač (na obr. označený x-switch-u5 a ďalej už len hlavný prepínač) slúži ako koncentrátor liniek z jednotlivých distribučných prepínačov. Distribučný prepínač z rozvodne IDF2 je pripojený k distribučnému prepínaču v rozvodni MDF, nakoľko hlavný prepínač obsahuje iba 2x SFP porty. Ostatné distribučné prepínače sú pripojené k hlavnému prepínaču pomocou UTP. Počet prepojení na obrázku označuje reálny počet agregovaných prepojení. Z dôvodu zvýšenia dostupnosti počítačovej siete na U5, navrhovaná modernizácia počíta so zavedením čiastočnej redundancie. Tá na obrázku č.24 je zobrazená ako prerušovaná čiara. Táto redundancia počíta s výpadkom hlavného prepínača. V prípade výpadku optickej linky, ktorá pripojuje U5 k chrbticovej optickej sieti, ale sieť ostatne izolovaná. Výpadkom niektorého distribučného prepínača bude obmedzená konektivita len tých prístupových prepínačov, ktoré sú pripojené k danému prepínaču. Nakoľko implementácia zvýšenia dostupnosti medzi prístupovými a distribučnými prepínačmi v tejto fáze nie je možné realizovať, pretože nie je dostatočný počet UTP káblov medzi rozvodňami, ktoré by mohli prepojiť prístupové prepínače z jednej rozvodne do distribučného prepínača druhej rozvodne.

Navrhovaná redundancia zavádza optické prepojenie medzi distribučnými prepínači v rozvodniach IDF3 a IDF1, ďalej prepojenie pomocou UTP káblu medzi IDF1 a IDF2. Hlavné redundantné spojenie ide z rozvodne IDF1 odkiaľ pokračuje do rozvodne MDF, kde pomocou *patch* panela je vytvorené spojenie medzi U5 a U13. Toto spojenie však musí byť tiež zapojené na U13. Rýchlosť takéhoto spojenia je 1 Gbps, pričom primárny cieľ je udržať konektivitu do doby opravy.

Kompletná schéma zobrazujúca návrh prechodnej modernizácie je umiestnená ako príloha č.14 na CD-ROM.

Táto navrhovaná schéma modernizácie zároveň počíta i s pripojením počítačovej siete ICT výskumného centra pričom, pričom je potrebné vybudovať optické spojenie medzi U5 a ICT centrom. Takéto spojenie vyžaduje aby optický kábel medzi U5 a ICT centrom obsahoval minimálne 2xMMF optické vlákna. Na schéme je táto trasa vyznačená prerušovanou zelenou čiarou. K účelu pripojenia je vyhradený druhý SFP+ port na hlavnom prepínači, ktorý zabezpečí 10 Gbps konektivitu. Pre zabezpečenie 10 Gbps prenosu pomocou mnohovidového vlákna je potrebné použiť **SFP-10G-LRM** modul. Ten umožňuje komunikáciu až na 220 m pre 62,5  $\mu\text{m}$  vlákno alebo 300 metrov pre 50  $\mu\text{m}$  MMF.

### 6.2.2 Variant finálnej modernizácie č.1

Kompletná schéma zobrazujúca návrh prechodnej modernizácie je umiestnená ako príloha č.15 na CD-ROM.

Tento variant modernizácie je rozšírením prechodnej modernizácie, pričom predpokladá vytvorenie optického prepojenia medzi budovou U5 a výskumným ICT centrom v blízkosti U5. K tomuto účelu bude potrebné aby optický kábel obsahoval minimálne 2x jednovidové a 8x mnohovidových optických vlákien. Pár jednovidových optických káblov pripojuje chrbticový L3 prepínač umiestnený v budove ICT centra s chrbticovou optickou sieťou. Toto prepojenie vznikne prepojením na optických *patch* paneloch na U5, v ktorých sú ukončené jednotlivé optické káble. Mnohovidové vlákna slúžia pre pripojenie distribučných prepínačov. Tento variant počíta s umiestneným chrbticového prepínača vo vedecko-výskumnom parku.

Nakoľko pripravované projekty v ICT parku a zavedenie VoIP s centralizovanou architektúrou, vyžadujú vysokú dostupnosť siete. I keď prechodná modernizácia zvyšovala

dostupnosť pre koncové zariadenia zavádza redundanciu v podobe prepojení medzi distribučnými prepínačmi, hlavný problém pri budovaní vysoko dostupného riešenia zostal nevyriešený, nakoľko modernizácia neponúka riešenie pri výpadku optickej linky medzi U5 a U13. Z tohto dôvodu sa pri budovaní nového ICT centra ponúka možnosť uzatvoriť obojstrannú zmluvu s niektorým lokálnym zlínskym ISP o použití ich existujúcej optickej linky v prípade výpadku hlavnej optickej linky U5/ICT. V tomto prípade by bol chrbticový prepínač pripojený k optickej sieti daného ISP. Tým sa zároveň zvýši zabezpečenie i pre ISP v prípade prerušenia jeho primárnej optickej trasy.

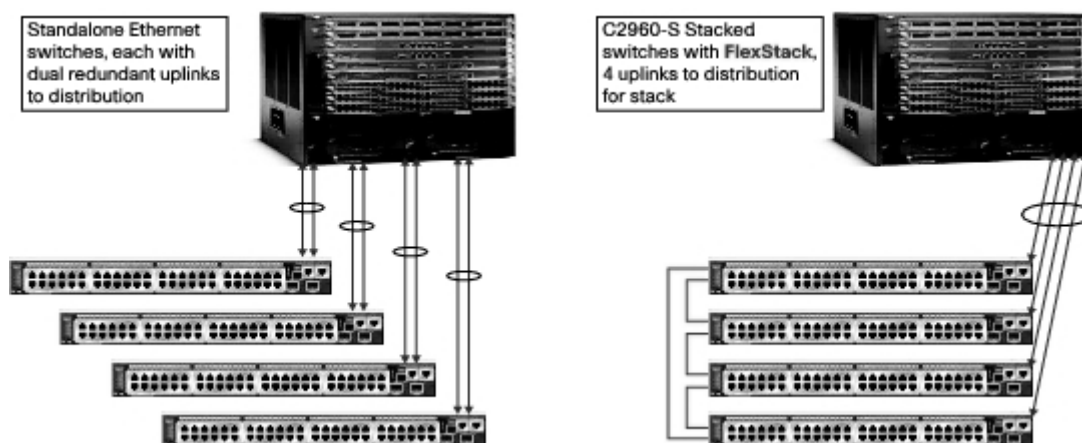
Chrbticový prepínač bol na základe nárokov zvolený prepínač rady **Nexus**, nakoľko z mnohých pripravovaných výskumných projektov ICT centra budú aplikácie *Grid Computing* a *Cloud Computing*, ktoré sú veľmi aktívne na generovanie sieťovej prevádzky a tým pádom správny výber sieťových komponentov je kľúčový pre ich nasadenie. Prepínače rady Nexus sa vyznačujú modulárnym vyhotovením a okrem vysokého výkonu, tak i redundantnými a *hot-swappable* komponentmi (napr. vetráky chladičov, alebo napájacie zdroje) a sú určené pre náročné aplikácie, ako napríklad prepínače pre dátové centrá, agregáciu, chrbticové nasadenie pre podniky a podobne náročné sieťové aplikácie. Výhodou tohto prepínača je jeho modularita, pričom práve prispôsobenie prepínača môže byť kľúčové pri nasadzovaní nových aplikácií a projektov.

Hlavný prepínač na obrázku č.24 označený ako **x-switch-u5** v tejto variante slúži ako distribučný prepínač. Ostatné distribučné prepínače sú v princípe modularity hierarchického modelu nahradené rovnakým modelom, čiže WS-C3560X-24T-S, a s rovnakým sieťovým modulom, ktorý zabezpečí 10 Gbps konektivitu. Tieto distribučné prepínače sú pripojené k chrbticovému prepínaču pomocou štyroch párov mnohovidových vlákien pre zabezpečenie 10 Gbps *full duplex* konektivity.

Pre zrýchlenie prístupovej vrstvy na 1Gbps je potrebné vymeniť všetky prístupové prepínače. Okrem toho, že súčasné prepínače nepodporujú 1 Gbps protokol, tak neobsahujú ani funkciu PoE, ktorá je kľúčová pre nasadenie technológie VoIP, nakoľko pri vhodnom nastavení by sa dali použiť ako prístupové prepínače pre IP telefóniu. Z tohto dôvodu je potrebné ich vymeniť za prepínače rady Catalyst 2960-S. Konkrétne model **WS-C2960S-48LPS-L**, ktorý ponúka 48x 10/100/1000 Mbps portov a tiež 4x 1 Gbps SFP porty. Pre komunikáciu pomocou SFP portov rýchlosťou 1 Gbps je potrebné použiť Cisco **GLC-LH-SM** pre MMF vlákna.

Celý prepínač dokáže zabezpečiť 370 W pre funkcionality PoE+, pričom tento výkon je možno progresívne distribuovať medzi porty. Pri pomere portov 1:1 (napájané/nenapájané) dokáže zabezpečiť až 15,4 W na jeden port. To je dostatočný počet výkon i pre zariadenia triedy č.3 [16].

Ďalšou výhodou tohto typu prepínača je možnosť nasadenia technológie **FlexStack**. Ide o *hot-swappable* modul, pomocou ktorého možno prepojiť až 4 prepínače podporujúce technológiu FlexStack do jedného logického celku nazývaného *stack*. Výhodou takéhoto prepojenia je správa takýchto zariadení, pretože prepínače prepojené do *stack*-u sa tvária ako jeden prepínač. Zároveň spolu so zabudovanou redundanciou v rámci *stack*-u sa zvýši dostupnosť. Toto prepojenie tiež podporuje technológie ako EtherChannel, SPAN (Switch Port Analyzer) a FlexLink. Technológia FlexStack ponúka až 20 Gbps priepustnosť (1 spojenie ponúka 10 Gbps *full duplex*), vďaka čomu sa táto technológia nestane úzkym miestom v komunikácii, a okrem zjednodušenej správy sa zrýchli doručovanie dát medzi prepínačmi v rámci rovnakej VLAN siete. Ďalšou výhodou je menší počet použitých *uplink* spojení, ako je zobrazené na obrázku č.24. Prepínače v rámci jedného *stack*-u zdieľajú použité *uplink* linky a zároveň použitím agregácie možno dosiahnuť požadované prenosy a redundanciu.



Obr. 25. Porovnanie FlexStack klasického riešenia.<sup>14</sup>

Túto výhodu je možné použiť pri tvorbe redundantných spojení, čím sa zvýši dostupnosť v sieti. Táto redundancia zabezpečí dostupnosť pre prístupové prepínače v prípade

<sup>14</sup> - Obrázok použitý z [14].

výpadku distribučního prepínača v danej rozvodni. Redundantné spojenia sa nachádzajú medzi rozvodňami IDF3 – MDF a IDF1 – IDF2. Redundancia je zabezpečená pomocou existujúcej UTP kabeláže, pričom jednotlivé prepínače v *stack*-u možno prepojiť menším počtom káblov a ušetriť tak porty na prepínači. Nakoľko prepínače Catalyst 3560G neumožňujú prepojenie do *stack*-u je potrebné, aby bol každý prepínač prepojený so susedným distribučným prepínačom.

Navrhovaná schéma zapojenia redundancie a prepínačov do *stack*-u je umiestnená ako príloha č.20 na CD-ROM. Daná schéma zobrazuje zapojenie pre navrhovaný počet prepínačov, ktorý je zobrazený v tabuľke č.9.

Pre navrhovaný počet prepínačov je medzi rozvodňami IDF3 a MDF možné použiť všetkých šesť UTP káblov. Jeden pár bude slúžiť pre vytvorenie redundantných spojení medzi prepínačmi Catalyst 3560G-48PS a distribučnými Catalyst 3560-X, nakoľko ich nie je možné umiestniť do *stack*-u. Ďalšie 2 páry pomocou agregácie je možné použiť prepojením *stack*-ov a jednotlivých distribučných prepínačov. Tým vznikne medzi prístupovými prepínačmi v *stack*-u a distribučným prepínačom 2 Gbps redundantné spojenie. Nakoľko technológia FlexStack podporuje až 4 prepínače, u týchto rozvodní je ešte možné pridať prepínač do *stack*-u bez toho aby bolo potreba vytvoriť nové redundantné spojenie. Zároveň pri rozsiahlejšom rozširovaní je vhodné nakombinovať počty prepínačov do *stack*-ov a zmeniť počet prepojení, prípadne tiež použiť SFP porty na distribučných prepínačoch.

Tab. 9. Navrhovaný počet prepínačov.

Rozvodňa	Počet prepínačov	Počet portov pre:		
		Celkový	Uplink	Koncové zariadenia
MDF	4	192	7	185
IDF1	5	240	7	233
IDF2	6	288	9	279
IDF3	4	192	7	185

Nakoľko v rozvodniach IDF1 a IDF2 sa nachádza viac prístupových prepínačov je potrebné pre budúce rozširovanie vhodne nakombinovať umiestnenie prepínačov do *stack*-ov, z dôvodu obmedzeného počtu dostupných UTP káblov. Z tohto dôvodu nie je možné zaviesť agregáciu pre redundantné spojenia, čím by sa zvýšila priepustnosť linky v prípade výpadku distribučného prepínača.

Nakoľko súčasné distribučné prepínače Catalyst 3560G-48PS vyhovujú požiadavkám pre navrhované prístupové prepínače, budú tieto prepínače použité v navrhovanej modernizácii, čím sa ušetrí náklady. Tieto prepínače poskytujú obsahujú funkcionality PoE a majú preposielací výkon 32 Gbps a tým nebudú problémom pri nasadzovaní VoIP. Ich jedinou nevýhodou je, že neponúkajú možnosť prepojenia do *stack*-u.

Prístupové prepínače budú okrem pripojovania koncových zariadení ako PC, tlačiarne a podobne, slúžiť i k pripojovaniu bezdrôtových prístupových bodov, ktoré v pôvodnej konfigurácii boli pripojené k distribučným prepínačom, nakoľko iba tie podporovali technológiu PoE. Okrem týchto zariadení technológiu PoE (prípadne PoE+) budú využívať najmä VoIP telefóny.

Každý z navrhovaných prístupových prepínačov obsahuje 48 portov, čím dokáže nahradiť pôvodné dva. Navrhovanou modernizáciou sa zníži počet prepínačov, čím sa ušetrí miesto v rozvodni a zároveň sa zjednoduší správa, zníži spotreba elektrickej energie. Pri použití prepínačov s 48 portami sa navyše ušetrí jeden port pre *uplink*. Počet prístupových prepínačov bude závisieť od počtu pripojených VoIP telefónov, bezdrôtových prístupových bodov, prípadne ďalších zariadení, ktoré možno pripojiť do siete a môžu využívať technológiu PoE. Tabuľka č.9 zobrazuje počet potrebných prepínačov, ktoré pokryjú súčasné potreby koncových zariadení. Tabuľka nezahŕňa nasadenie technológie VoIP, ktorej potreby sú individuálne. Implementácia VoIP z pohľadu prístupových prepínačov nepredstavuje väčší problém, nakoľko modularita sieťového modelu umožňuje aplikovať nastavenia plošne a podľa potrieb.

Produktovú dokumentáciu k sérii prepínačov Catalyst 2960 je umiestnená na CD-ROM ako príloha č.17. Produktová dokumentácia k sérii prepínačov Catalyst 3560 je umiestnená na CD-ROM ako príloha č.18.

### 6.2.3 Variant finálnej modernizácie č.2

Kompletná schéma zobrazujúca návrh prechodnej modernizácie je umiestnená ako príloha č.16 na CD-ROM.

Tento návrh modernizácie sa od predchádzajúceho návrhu odlišuje najmä umiestneným a funkciou chrbticového prepínača. Nakoľko v predchádzajúcej variante, modulárny prepínač Nexus, okrem chrbticovej funkcie slúži ako distribučný/chrbticový agregátor, tak zároveň môže byť i vo funkcií prístupového prepínača pre náročné aplikácie. Vhodným umiestneným rozvodne v budove môže slúžiť i ako prístupový prepínač pre veľké množstvo portov. Jeho funkcia závisí najmä od použitých modulov.

Variant č.2 uvažuje chrbticový prepínač umiestnený na U5. Jeho funkcia je najmä ako chrbticový koncentrátor z distribučných prepínačov, pričom v navrhovanej konfigurácii slúži zároveň tiež ako distribučný/chrbticový prepínač pre prístupové prepínače v rozvodni MDF. Zároveň tiež pripojuje distribučné prepínače výskumného ICT centra, pričom záloha spojenia siete môže byť pripojená k niektorému distribučnému prepínaču v ICT centre, prípadne priamo k chrbticovému prepínaču na U5. Pre pripojenie ICT centra k hlavnému prepínaču na U5 je potrebné vybudovať optické spojenie, ktoré bude obsahovať minimálne 6x mnohovidové vlákna, pre pripojenie distribučného/chrbticového prepínača a pre zálohu konektivity siete. Pre každý ďalší distribučný prepínač sú potrebné ďalšie dve vlákna pre vytvorenie duplexnej prevádzky.

K tomuto účelu bude použitý agregáčny prepínač Cisco Catalyst 4500-X, konkrétne model **WS-C4500X-16SFP+**. Ide 1U prepínač s fixnou konfiguráciou a voliteľným rozširujúcim sieťovým modulom, pričom navrhovaný prepínač obsahuje 16x portov SFP+, ktoré podporujú 1/10 Gbps Ethernet, nakoľko sa nepredpokladá väčšie rozširovanie siete. Pre zachovanie dostupnosti tento prepínač obsahuje redundantné *hot-swappable* chladiace vetráky a napájacie zdroje.

Produktová dokumentácia k sérii prepínačov Catalyst 4500-X je umiestnená ako príloha č.19 na CD-ROM.

Distribučné a prístupové prepínače sú volené rovnako ako v prípade navrhovanej modernizácie č.1, čiže modeli Catalyst 3560-X pre distribučnú a Catalyst 2960-S pre prístupovú vrstvu. Počet prístupových prepínačov zostáva rovnaký ako v prípade varianty

č.1, ktorá je zobrazená v tabuľke č.9. Schéma návrhu zapojenia redundancie a prepínačov do *stack*-ov je umiestnený ako príloha č.21, ktorá je umiestnená na CD-ROM.

### 6.3 Návrh logickej štruktúry

Nakoľko logický návrh v súčasnosti nie je úplne ideálny, pretože zbytočne používa veľké rozsahy neverejných IP adries, čo v prípade operačného systému Windows nie je ideálny stav, nakoľko táto platforma produkuje veľké množstvo *broadcast* prevádzky. Ďalším faktom je že sa stále používajú i verejné IP adresy, čo nie je ideálny stav, najmä z pohľadu bezpečnosti.

Z tohto dôvodu je potrebné navrhnuť novú logickú štruktúru, ktorá bude lepšie vyhovovať požiadavkám, ako sú napríklad veľkosť rozsahu IP adries a *broadcast* domény, správa a rozšíriteľnosť siete a zároveň bude kladený dôraz na bezpečnosť.

Pri logickom návrhu siete, by VLAN sieť nemala prekračovať rozsah rozvodne. V minulosti bolo tiež dobrým zvykom aby každý prepínač mal vlastnú VLAN sieť, ale použitím IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) and 802.1s MSTP (Multiple Instance Spanning Tree Protocol) sa toto už nemusí dodržiavať, nakoľko tieto protokoly umožňujú výrazne rýchlejšiu konvergenciu STP. Ďalším faktorom pri návrhu VLAN je rozsah adries. Nakoľko niektoré platformy generujú periodicky veľké množstvo *broadcast* prevádzky, je z tohto dôvodu dobré obmedziť jeho dosah. Preto by každá VLAN sieť mala mať maximálne rozsah 512 zariadení, čo odpovedá 2 podsietiam typu C [15].

Tab. 10. Navrhované logické rozdelenie.

Č. VLAN siete	Názov VLAN	Adresný rozsah	Adresa východzej brány	Adresa Broadcast
50	Management	10.5.0.0/24	10.5.0.1	10.5.0.255
51	MDF-1	10.5.1.0/24	10.5.2.1	10.5.2.255
52	MDF-2	10.5.2.0/24	10.5.3.1	10.5.3.255
53	IDF1-1	10.5.3.0/24	10.5.4.1	10.5.4.255
54	IDF1-2	10.5.4.0/24	10.5.5.1	10.5.5.255
55	IDF2-1	10.5.5.0/24	10.5.6.1	10.5.6.255
56	IDF2-2	10.5.6.0/24	10.5.7.1	10.5.7.255
57	IDF3-1	10.5.7.0/24	10.5.8.1	10.5.8.255
58	IDF3-2	10.5.8.0/24	10.5.9.1	10.5.9.255
59	WIFI-EDU-ROAM-1	10.5.9.0/24	10.5.10.1	10.5.10.255
60	SERVER-VLAN	10.5.10.0/24	10.5.11.1	10.5.11.255
61	Voice-1	10.5.11.0/24	10.5.12.1	10.5.12.255
62	Voice-2	10.5.12.0/24	10.5.13.1	10.5.13.255

Účelu logickej štruktúry bude použitý neverejný rozsah IP adries **10.5.0.0/16**, ktorý bude rozčlenený na jednotlivé menšie podsiete. Základom pre delenie bude fyzické umiestnenie prepínačov podľa rozvodní na U5.

Samotný rozsah je rozdelený podľa fyzickej štruktúry na jednotlivé podsiete, so sieťovou maskou o veľkosti 24 bitov. Tým sa dosiahne lepšie rozdelenie *broadcast* prevádzky. To zároveň umožní začleniť menej zariadení do jednej VLAN siete a tiež v prípade ďalšieho rozširovania, je tu dostatok adries pre nové zariadenia.

Tabuľka č.10 zobrazuje logické rozdelenie siete. Sieť VLAN s číslom 50 bude ako v pôvodnom návrhu slúžiť pre správu aktívnych prvkov siete, ako sú prepínače

a bezdrôtové prístupové body. Ďalej sú tu zobrazené jednotlivé VLAN siete podľa jednotlivých rozvodní, pričom každá rozvodňa má vyhradené 2 VLAN siete. Dve VLAN siete sú tiež vyhradené pre bezdrôtovú sieť **eduroam**. Pre VoIP technológiu sú vyhradené VLAN siete s č.61 a 62.

#### 6.4 Bezdrôtová sieť

Pre účely modernizácie bezdrôtovej siete **eduroam**, bol vytvorený dotazník, ktorého cieľom bolo zozbierať údaje o používaní tejto siete medzi študentmi. Dotazník s otázkami je umiestnený ako príloha č.9, ktorá je umiestnená na CD-ROM.

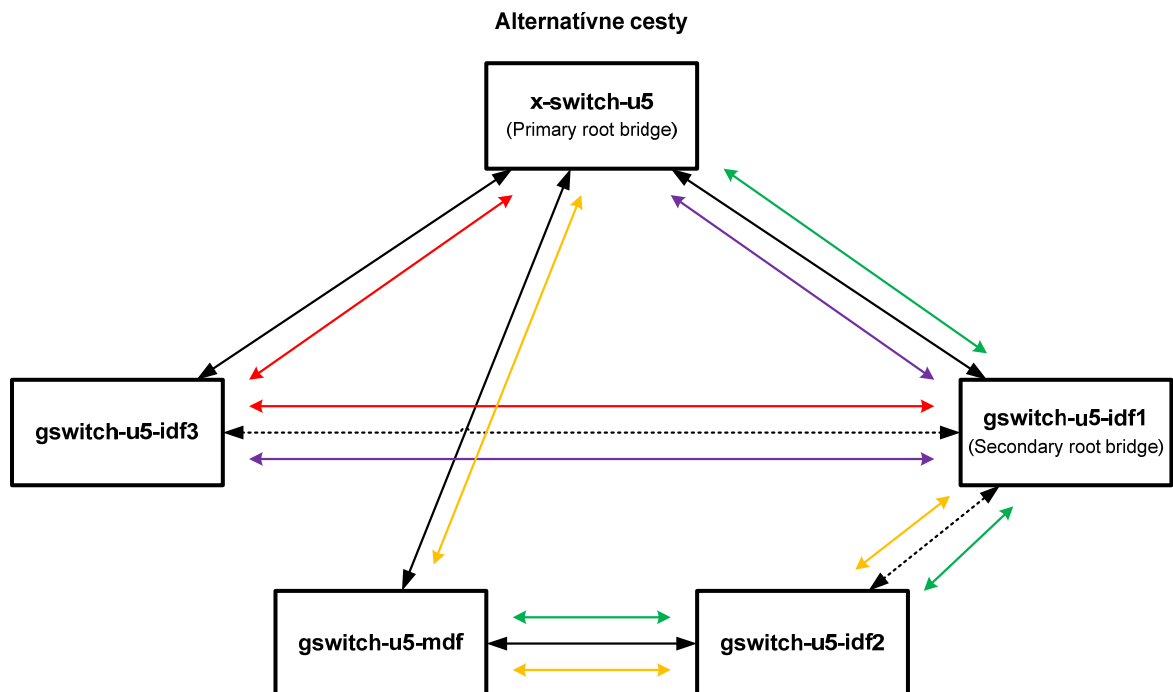
Výsledky ukazujú, že medzi študentmi je používanie tejto bezdrôtovej siete obľúbené, nakoľko 70% (70 zo 100 študentov) opýtaných používa túto bezdrôtovú sieť. Zároveň až 65% z používajúcich študentov vie o možnosti použitia súčasného účtu pre pripojenie k sieti eduroam v ČR alebo EU. Skoro polovica opýtaných študentov uviedla spokojnosť s dostupnosťou siete. Z druhej polovice opýtaných, len 14 uviedla nedostupnosť a to najmä v prednáškových miestnostiach. Až 60% opýtaných má však problémy s touto sieťou. Tie sa týkajú najmä spotrebou viac prihlasovacích pokusov, samovoľnom odpájaní, alebo problémy s prihlasovaním. Notebook pre pripojenie používa 89% a dominuje operačný systém Windows 7 a zároveň až 47% používa mobilný telefón (*smartphone*), alebo *tablet*, pričom dominuje operačná systém Android. Z výsledkov dotazníku vyplýva, že rozšírenie siete o ďalšie prístupové body, skôr by používatelia privítali lepšiu funkčnosť siete.

Problémy týkajúce sa pripojenia by mohol vyriešiť prvok na riadenie bezdrôtových sietí. Ide o zariadenie nazývané *Wireless Controller*, pričom pre účel U5 a technologického parku by mal byť použitý model **AIR-CT2504-25-K9**, z produktovej rady Cisco 2500 *series wireless controller*. Ten dokáže koordinovať až 15 prístupových bodov, čo je dostatočný počet i pre v prípade ďalšieho rozširovania. Zároveň obsahuje ďalšie funkcie, ktoré uľahčujú nasadenie a používanie bezdrôtových sietí spolu s pevnou. V prípade, že by tento počet v budúcnosti nestačil, je možné dokúpiť ďalšie licencie na ďalšie prístupové body.

Produktová dokumentácia k produktovej rade Cisco 2500 *Wireless Controller* je umiestnená na CD-ROM ako príloha č.25.

## 6.5 Spanning Tree Protocol a jeho vylepšenia

Tým, že jednotlivé návrhy modernizácie zvyšujú dostupnosť siete zavadením redundantných liniek, je potrebné v sieti používať STP protokol, ktorý zabraňuje vzniku slučiek na linkovej vrstve. Nakoľko všetky navrhované zariadenia sú od spoločnosti Cisco je vhodné použiť Rapid PVST+ (Rapid per-VLAN spanning tree protocol) protokol, čo je proprietárne vylepšenie štandardizovaného IEEE 802.1D RSTP protokolu. Tento protokol umožňuje rýchlejšiu konvergenciu cez viacero VLAN sietí.



Obr. 26. Alternatívne cesty u prechodnej modernizácie.

Obrázok č. 26 zobrazuje alternatívne cesty pri výpadku linky medzi hlavným a niektorým distribučným prepínačom. To aká cesta sa vyberie záleží ako sa prepočíta trasa k hlavnému prepínaču.

U variant modernizácie 1 a 2 protokol STP protokol slúži najmä na blokovanie liniek, ktoré spájajú prístupové prepínače so susedným distribučným prepínačom. U finálnych variant je s spolu STP protokolom možné použiť technológiu FlexLink, ktorá je podporovaná na navrhovaných prepínačoch. Táto technológia poskytuje L2 (linkovú) redundanciu a oproti STP protokolom má táto technológia rýchlejšiu konvergenciu (do 100 ms). Pri konfigurácii portu technológiou FlexLink je na porte vypnutý STP protokol, pričom nastavovaný port nesmie byť nastavovaný funkciami STP a zabezpečením portov.

FlexLink tvorí pár liniek, pričom redundantná linka je nastavená do režimu *stand-by*. V prípade výpadku primárnej linky, prevezme činnosť záložná a po obnovení primárnej linky prejde opäť do blokujúceho stavu [17].

## 6.6 Smerovanie medzi VLAN sieťami

Navrhované modernizácie používajú ako chrbticové prvky prepínače, ktoré umožňujú funkcie sieťovej vrstvy. Tým pádom je možné opustiť súčasné riešenie, kedy smerovanie medzi jednotlivými VLAN sieťami je vykonávané na centrálnom prepínači na U13 a smerovať prevádzku medzi VLAN sieťami na U5. Tým sa kompletne oddelí prevádzka z U5 a na centrálny prvok budú smerované pakety, ktoré majú ísť mimo sieť na U5. Týmto sa zlepši využívanie šírky pásma, nakoľko sa odstráni parazitná prevádzka. Použitím takýchto prvkov zároveň umožní použiť novú logickú štruktúru a jej prípadné neskoršie úpravy.

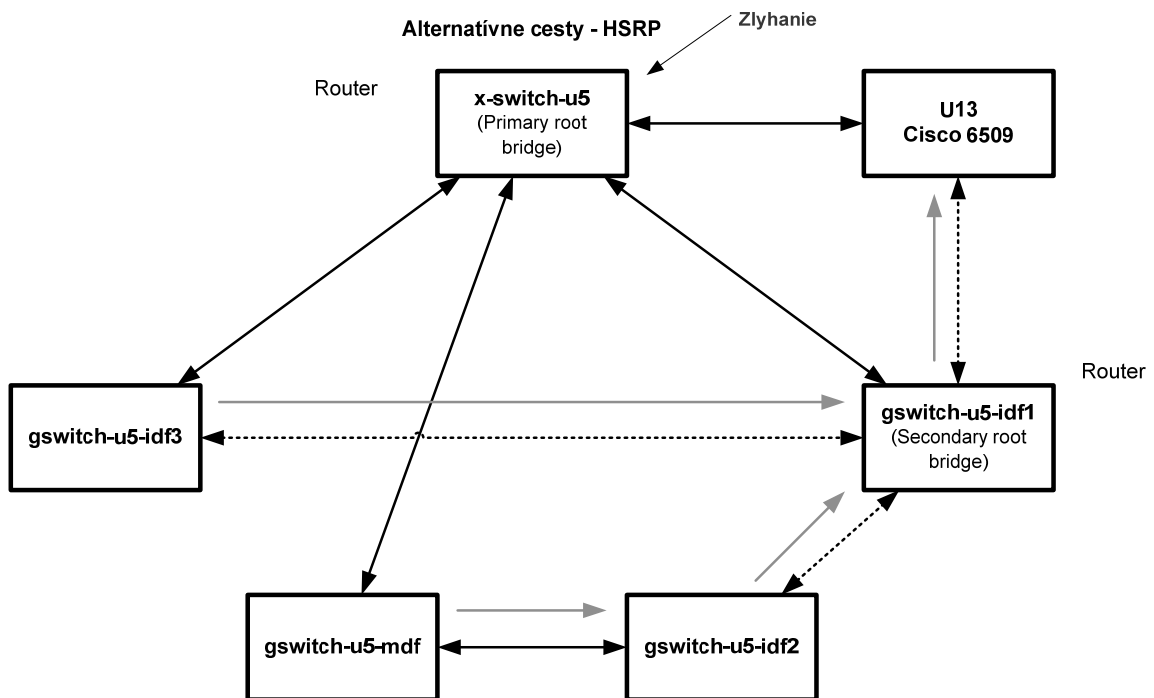
## 6.7 Protokol VTP a VTP pruning

Spolu s novým logickým členením siete na VLAN siete funkciou smerovania medzi nimi, by chrbticový prvok mal zastávať funkciu servera pre VTP protokol. Tým nie je potrebné držať zoznam VLAN sietí pre U5 na centrálnom prvku, pretože tento hlavný prepínač sa stane serverom pre VTP doménu. Tým dôjde k lepšiemu logickému členeniu siete pomocou VTP domény a zároveň sa odstráni prevádzka z linky medzi U5 a U13 pri aktualizácií zoznamu VLAN sietí. Ostatné prepínače sú v režime *client*, na ktoré prijímajú informácie zo servera.

Jednotlivé prepínače sú prepojené linkami v režime *trunk*. Tieto linky natívne prenášajú prevádzku zo všetkých VLAN sietí. To pri aktívnejšej *broadcast* prevádzke môže spôsobovať degradáciu efektivity šírky pásma. Z tohto dôvodu by prepínača mohli používať VTP funkcionality *pruning*, ktorá redukuje zbytočnú hromadnú prevádzku ako napr. *broadcast*, *multicast*, neznáme (*unknown*), alebo hromadné *unicast* pakety. VTP obmedzuje hromadnú prevádzku na tých *trunk* linkách, ktoré prevádzka musí použiť pre prístup na dané sieťové zariadenia. Táto funkcionality môže výraznejšie zvýšiť priepustnosť najmä u prístupových prepínačoch, ktoré používajú málo VLAN sietí.

## 6.8 Protokoly typu First-Hop Redundancy

Nakoľko pri budovaní siete s vysokou dostupnosťou, treba počítať tiež s výpadkom hlavného prvku, prípadne linky, ktorá spojuje lokálnu sieť s inými sieťami, pretože inak sieť ostatne odrezaná. Navrhované modernizácie počítajú s možnosťou takejto situácie a zavádzajú alternatívnu cestu. Pre správnu funkciu je ale potrebné ochrániť použitú *default gateway*. K tomuto účelu je potrebné nastaviť 2 alebo viac smerovačov (prípadne zariadení s funkciami sieťovej vrstvy) pre poskytovanie zálohy za túto adresu. K tomuto účelu sa používajú protokoly typu *First-Hop Redundancy*. Medzi tieto protokoly patrí i proprietárny Cisco protokol HSRP (Hot Standby Router Protocol), ktorý podporujú o všetky navrhované prvky.



Obr. 27. Použitie HSRP protokolu v prechodnej modernizácii.

HSRP smeruje IP prevádzku bez spoliehania sa na jeden smerovač. HSRP umožňuje aby skupina rozhraní smerovača pracovala spoločne a vyzerala ako jeden smerovač, alebo *default gateway* pre užívateľov v LAN. Smerovače zahrnuté v HSRP protokole poskytujú virtuálnu MAC a IP adresu, ktorá je nakonfigurovaná na smerovačoch, ako adresu virtuálneho smerovača. Jeden zo zúčastnených smerovačov je určený ako aktívny ostatné sú v režime *stand-by*. V prípade výpadku linky, alebo smerovača, úlohu preberá prvok v režime *stand-by*.

V prípade prechodnej modernizácie je k účelu druhého smerovača použitý distribučný prepínač **gswitch-u5-idf1**. Vo finálnych variantoch bude ako záložná cesta slúžiť prenajatá optická trasa niektorého lokálneho poskytovateľa. HSRP protokol potom bude aktivovaný na hlavnom chrbticovom prvku, medzi dvoma rozhraniami, ktoré pripojujú sieť k chrbticovej sieti.

## 6.9 Zabezpečenie portov

Prístupové prepínače tvoria prístupový bod do siete. Nakoľko porty na prístupových prepínačoch nevyužívajú žiadne zabezpečenie, predstavuje toto bezpečnostnú medzeru. Zavedením prísnych prístupových pravidiel, ale vznikne veľa práce pri administrácii siete. Povolením viacerých MAC adries na port, ale opäť predstavuje bezpečnostné riziko, ktoré môže byť zneužitú. Z tohto dôvodu zavedenie zabezpečenia portov musí byť v súlade s celkovou bezpečnostnou politikou na U5. Počítače by mali obsahovať všetky potrebné programy k výučbe, tak aby žiaci nemali potrebu pripájať svoje zariadenia do siete pomocou štruktúrovanej kabeláže, ale len pomocou bezdrôtovej siete eduroam.

Zabezpečenie portov by malo povoľovať iba 1 MAC adresu a používať nastavenie **Restrict**, pri ktorom sa prístupový port nevypne pri narušení. Toto nastavenie spôsobí, že iba prevádzka na povolenej MAC adrese je ďalej posielaná po sieti. Zároveň sa generuje SNMP *Trap* správa, zaznamenáva sa správa do *SysLog* a zvýši sa počítadlo narušenia (tzv. *violation counter*). Toto umožní spätnú kontrolu toho, kto narušil bezpečnostné pravidlá.

## 6.10 Riešenie VoIP

Riešenie VoIP telefónie pre budovu U5 bude využívať stávajúce riešenie tejto technológie, ktoré už je úspešne implementované. Je to jednak z dôvodu, že UTB nie je až tak veľký subjekt a tiež i po ekonomickej stránke, nakoľko by bolo neefektívne nasadzovať na každej fakulte VoIP ústredňu. Z toho plynie, že použitá architektúra používa centralizovaný model, pričom správa hovorov a telefónov sa deje v VoIP ústredni, ktorá je umiestnená na U13.

Pri implementácii takéhoto riešenia je dobrým pravidlom aby koncové zariadenia boli od rovnakého výrobcu. I keď VoIP ústredňa HiPath 4000 umožňuje používať štandardizovaný SIP protokol, z dôvodu lepšej správy a funkčnosti, koncové zariadenia by mali schopné používať protokol HFA, ktorý je momentálne nasadený. Z tohto dôvodu by telefóny mali

byť z modelovej rady OpenStage od spoločnosti Siemens. Táto modelová rada ponúka až 8 rôznych modelov, líšiacich sa vybavením a funkciami, pričom protokol HFA podporujú modeli OpenStage 20, 40, 60 a 80. Napájanie týchto telefónov bude prostredníctvom funkcionality PoE, ktorá je podporovaná na navrhovaných prístupových prepínačoch.

Pre úspešné implementovanie VoIP do siete je potrebné na všetkých prvkoch nastaviť QoS pravidlá, ktoré budú uprednostňovať hlasovú prevádzku.

Produktová dokumentácia k modelovej rade telefónov OpenStage je umiestnená ako príloha č.24 na CD-ROM.

## 7 SIMULÁČNÉ ZAPOJENIE NAVRHOVANEJ SIETE

Pre účel vytvorenia konfiguračných súborov pre jednotlivé aktívne prvky je použité simulačné prostredie Packet Tracer. Ide o software spoločnosti Cisco primárne určený pre tréning a výučbu pre kurz CCNA (Cisco Certified Network Associate), pričom je možné využívať i pre jednoduchšie sieťové simulácie. Tento simulátor ale neobsahuje všetky funkcie a príkazy reálneho operačného systému, ktorý je použitý v navrhovaných zariadeniach, preto tieto konfiguračné súbory bude treba pred nasadením upraviť a doplniť o chýbajúce funkcie. Z tohto dôvodu sú tu uvedené i príkazy, ktoré nie sú súčasťou simulátoru, ale pomocou ktorých sa dosiahne požadovaný efekt.

**Pozn.:** Konfiguračné súbory boli vytvorené vo verzií: Cisco Packet Tracer 5.3.3.0019.

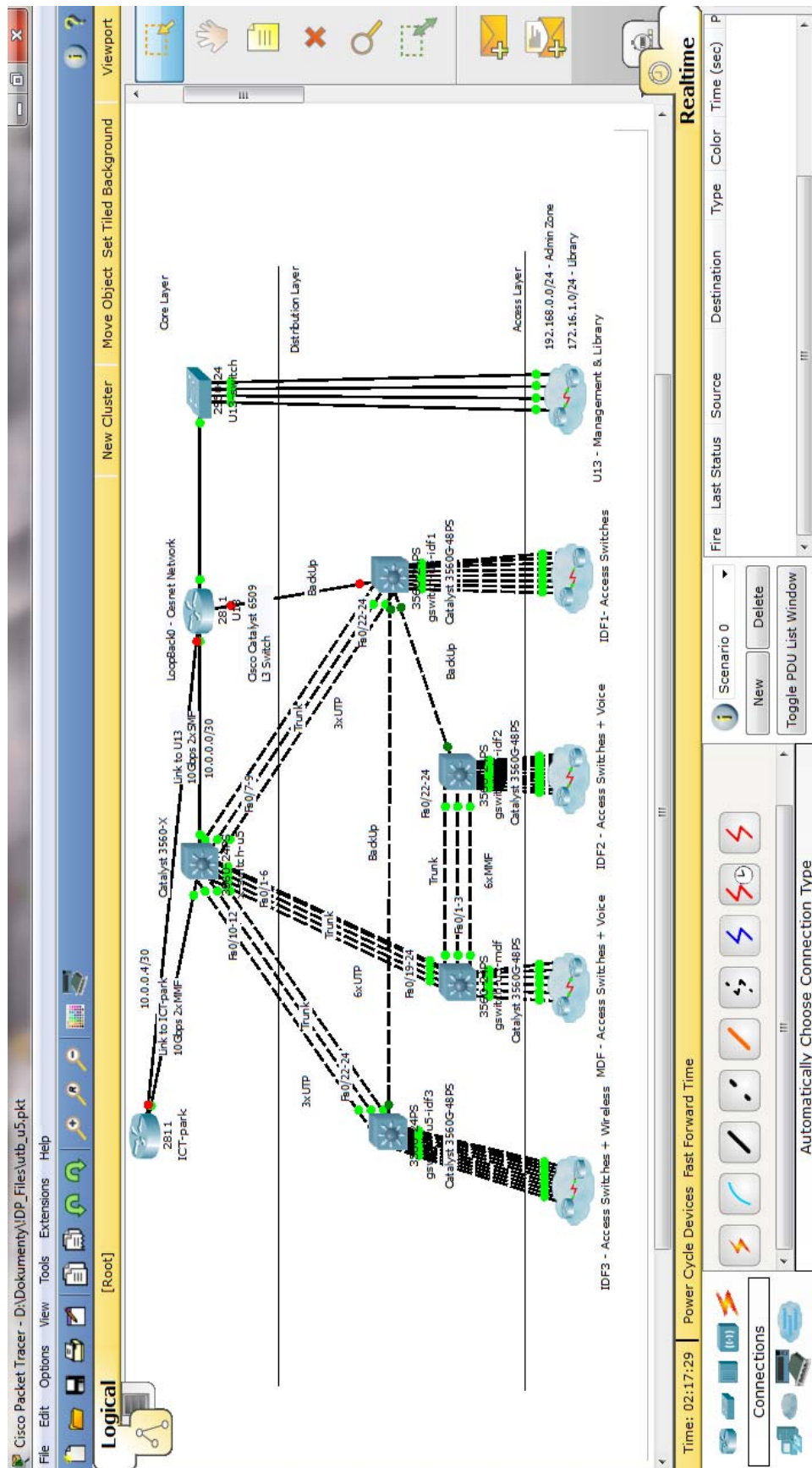
### 7.1 Simulačné zapojenie

Pre simuláciu bola vybratá schéma prechodnej modernizácie, nakoľko táto modernizácia môže byť realizovaná v blízkej dobe použitím minimálnych nákladov. Zároveň navrhované typy prepínačov možno najjednoduchšie simulovať.

Nakoľko simulačné prostredie neobsahuje všetky typy použitých zariadení, boli pre tvorbu simulácie použité zaradenia:

- Smerovač 2811 – ako prepínač s úplnými L3 funkciami.
- Prepínač 3560-24PS ako prepínač so základnými L3 funkciami.
- Prepínač 2950-24 – základný prepínač s L2 funkciami.

Obrázok č.26 zobrazuje simulačné zapojenie v programe Packet Tracer. Prístupové prepínače sú umiestnené do logických *cluster*-ov, nakoľko ich v danom počte spolu s koncovými zariadeniami nie je možné zobrazit'.



Obr. 28. Simulačné zapojenie v Packet Tracer.

## 7.2 Prepojenie siet'ových prvkov

Nakoľko simulačné zariadenia neobsahujú taký počet a typ portov, ako navrhované zariadenia, sú všetky prepojenia simulované pomocou metalickej kabeláže. Toto bude mať najzásadnejší vplyv na finálne konfiguračné súbory.

Prepínače boli prepájané spôsobom ako v súčasnom stave, čiže posledný port slúži ako *uplink* a kým prvé porty sú určené pre pripojovanie zariadení. Prehľad priradenia jednotlivých portov na chrbticovom a distribučných prepínačov je umiestnený ako príloha č.23 na CD-ROM.

Všetky linky, ktoré prepojujú prepínače, sú nastavené do režimu *trunk*. Ostatné porty na prístupových prepínačoch sú nastavené do prístupového režimu pre konkrétnu VLAN sieť. Tieto nastavenia boli vykonané až po vykonaní základných nastavení a po nastavení prepínačov o VLAN siete a protokol VTP. Z tohto dôvodu príkazy sú uvedené až po týchto nastaveniach.

## 7.3 Základné nastavenia

U každého zaradenia boli vykonané základné nastavenia. Medzi tieto nastavenia patrí:

- Nastavenie mena zariadenia.
- Šifrované heslo do exekutívneho režimu.<sup>15</sup>
- Zakázaný preklad doménového mena na IP adresu.
- Šifrovanie hesla pre prístup cez konzolový port alebo virtuálny terminál.
- Prihlasovacia správa s textom: UNAUTHORIZED ACCESS PROHIBITED
- Nastavenie konzoly a virtuálnych terminálov
  - Nastavenie prihlasovania a hesla.
  - Nastavenie kurzoru na nový riadok.
  - Opustenie exekutívneho režimu po 5 minútach nečinnosti.

---

<sup>15</sup> - **Pozn.:** Všetky heslá obsiahnuté v konfiguráciách sú volené ako: **UTB**

**Príklad zobrazenia vykonaných nastavení:**

```
Current configuration : 1345 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname x-switch-u5
!
enable secret 5 $1$mERr$tHssSYxniaK0Pojon/oe30
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
banner login ^CUNAUTHORIZED ACCESS PROHIBITED^C
banner motd ^CUNAUTHORIZED ACCESS PROHIBITED^C
!
line con 0
exec-timeout 5 0
password 7 0814786C
logging synchronous
login
line vty 0 4
```

```
exec-timeout 5 0
password 7 0814786C
logging synchronous
login
!
```

**Pozn.:** Riadok č.10 zobrazuje zašifrované heslo do exekutívneho režimu. Toto heslo používa šifrovanie typu 5. Heslá pre prístup cez konzolový port (riadky č. 27 a 32) alebo virtuálny terminál sú šifrované pomocou šifry typu 7. Tieto šifry sú oproti typu 5 ľahšie rozlúšiteľné.

Príkazy, ktoré majú vplyv na funkciu konzolového portu alebo virtuálneho terminálu sa zadávajú v konfiguračnom režime pre dané pripojenie.

#### **Príkaz pre nastavenie hesla do exekutívneho režimu:**

```
x-switch-u5(config)#enable secret UTB
```

Natívne, heslá pre prístup cez konzolový port a virtuálny terminál, nie sú šifrované a treba šifrovanie treba aktivovať.

#### **Príkaz pre aktiváciu šifrovania hesla:**

```
x-switch-u5(config)#service password-encryption
```

Ostatné príkazy pre základnú konfiguráciu sú vo forme v akej sú zobrazené v príklade základnej konfigurácie.

## **7.4 Nastavenia VLAN sietí a protokolu VTP**

### **7.4.1 Nastavenie VLAN sietí**

Pre správu zariadení na každom prepínači bolo vytvorené virtuálne VLAN rozhranie, ktorému bola priradená IP adresa na základe tabuľky č.11.

Kompletné priradenie IP adries použité v simulácii je umiestnené ako príloha č.22 na CD-ROM.

Tab. 11. Tabuľka rozdelenia siete určenej pre manažment zariadení.

Adresa/Rozsah adres	Význam
10.5.0.0	IP Adresa siete
10.5.0.1	Adresa rozhrania prepínača: <b>x-switch-u5</b>
10.5.0.2 – 10.50.15	Rezerva
10.5.0.16	Adresa rozhrania prepínača: <b>gswitch-5-mdf</b>
10.5.0.17	Adresa rozhrania prepínača: <b>gswitch-5-idf1</b>
10.5.0.18	Adresa rozhrania prepínača: <b>gswitch-5-idf2</b>
10.5.0.19	Adresa rozhrania prepínača: <b>gswitch-5-idf3</b>
10.5.0.20 – 10.5.0.31	Rezerva
10.5.0.32 – 10.5.0.47	Adresy vyhradené pre prístupové prepínače v rozvodni MDF
10.5.0.48 – 10.5.0.63	Adresy vyhradené pre prístupové prepínače v rozvodni IDF1
10.5.0.64 – 10.5.0.79	Adresy vyhradené pre prístupové prepínače v rozvodni IDF2
10.5.0.80 – 10.5.0.95	Adresy vyhradené pre prístupové prepínače v rozvodni IDF3
10.5.0.96 – 10.5.0.254	Rezerva
10.5.0.255	IP adresa pre <i>broadcast</i> siete

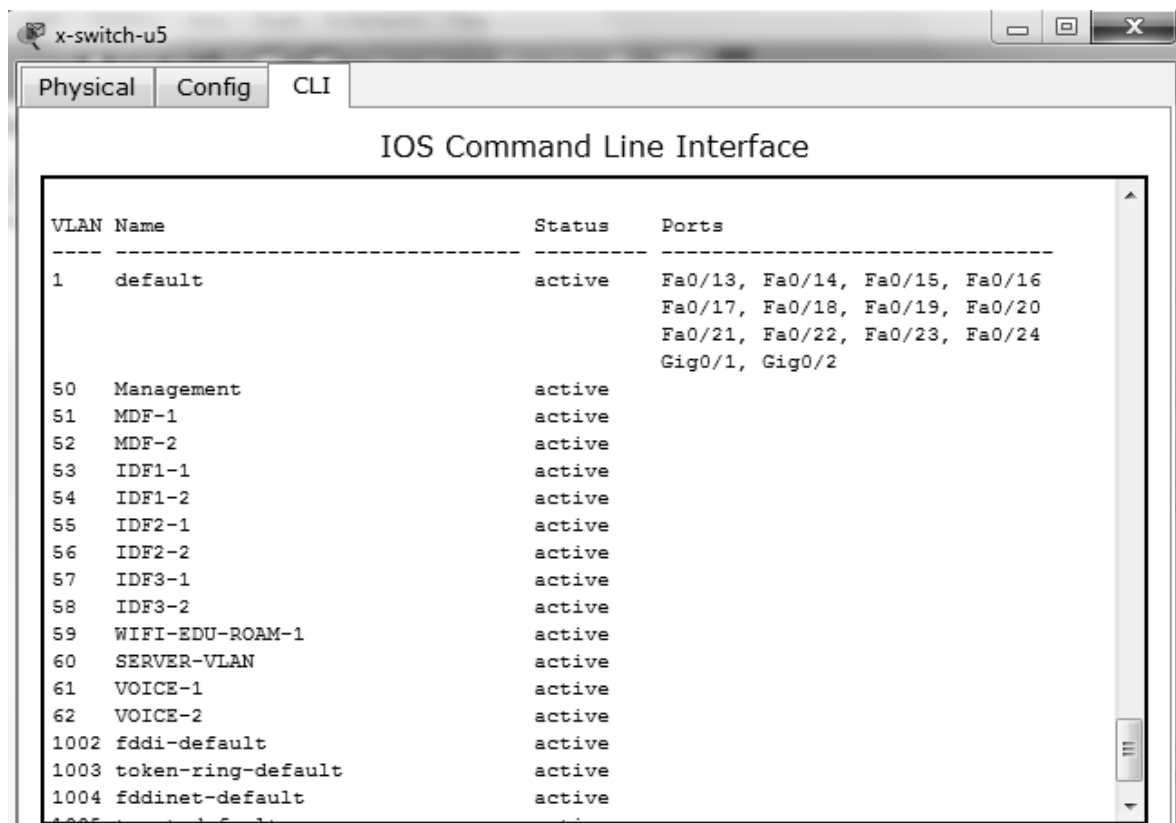
### Príkazy pre vytvorenie a nastavenie virtuálneho rozhrania pre manažment na prepínači:

```
x-switch-u5(config)#interface vlan 50
x-switch-u5(config-if)#ip address 10.5.0.1 255.255.255.0
```

**Pozn.:** Toto rozhranie je na prepínači aktivované až po vytvorení VLAN siete.

### Príkazy pre vytvorenie VLAN siete:

```
x-switch-u5(config)#vlan 50
x-switch-u5(config-vlan)#name Management
```



VLAN Name	Status	Ports
1 default	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
50 Management	active	
51 MDF-1	active	
52 MDF-2	active	
53 IDF1-1	active	
54 IDF1-2	active	
55 IDF2-1	active	
56 IDF2-2	active	
57 IDF3-1	active	
58 IDF3-2	active	
59 WIFI-EDU-ROAM-1	active	
60 SERVER-VLAN	active	
61 VOICE-1	active	
62 VOICE-2	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	

Obr. 29. Výstup príkazu Show vlan brief.

Obrázok č.29 zobrazuje výstup príkazu *show vlan brief* po vytvorení a pomenovaní všetkých VLAN sietí.

#### 7.4.2 Nastavenia protokolu VTP

Hlavný prepínač označený ako **x-switch-u5** bude slúžiť ako správca VTP domény. Tento prepínač je nastavený do režimu **server**. Ostatné prepínače sú nastavené do režimu **klient**, v ktorom iba preberajú nastavenia zo servera. V simulácii bolo ako názov VTP domény zvolené: **UTB-U5**. Všetky prepínače v danej doméne používajú verziu VTP protokolu č.2. Pre riadenie VTP domény sú všetky zúčastnené prepínače, ktoré majú prebrať VTP nastavenia nastavené heslom – **UTB**.

#### Príkazy pre nastavenie protokolu VTP:

```
x-switch-u5(config)#vtp mode server
x-switch-u5(config)#vtp domain UTB-U5
x-switch-u5(config)#vtp password UTB
x-switch-u5(config)#vtp version 2
```

Po nastavení VTP protokolu boli na hlavnom prepínači vytvorené a nastavené VLAN siete podľa tabuľky č.10.

### 7.4.3 Nastavenie režimov na portoch

Pomocou nasledujúcich príkazov boli na prístupových prepínačoch porty nastavené do prístupového režimu. Ide o hromadný príklad pomocou ktorého sa nastaví 23 portom na prepínači do prístupového režimu pre VLAN 51.

#### Príklad nastavenia portov do prístupového režimu:

```
sw-u5-mdf-1(config)#interface range fastethernet 0/1-23
sw-u5-mdf-1(config-if-range)#switchport mode ccess
sw-u5-mdf-1(config-if-range)#switchport ccess vlan 51
```

#### Príklad nastavenia portov do režimu trunk:

```
x-switch-u5(config)#interface fastethernet 0/24
x-switch-u5(config-if)#switchport trunk encapsulation dot1q
x-switch-u5(config-if)#switchport mode trunk
```

Príklad zobrazuje príkazy pre nastavenie *uplink* linky do režimu *trunk*. Pred tým než je určený režim, je potrebné určiť prepínaču, aby používal štandardizované zapuzdrenie definované štandardom IEEE 802.1Q. Po vykonaní tohto nastavenia môže byť určený režim linky na *trunk*.

Pri definovaní *trunk-u*, je zároveň potrebné určiť tzv. *Native VLAN*. Ide o VLAN sieť, ktorá nepoužíva žiadne dodatočné informácie. Ako *Native VLAN* bola ponechaná VLAN sieť č.1. Táto VLAN sieť nemá aktivované VLAN rozhranie a zároveň na všetkých *trunk* linkách nie je povolená.

### 7.4.4 VTP Pruning

Nakoľko Packet Tracer neobsahuje funkcionality VTP *Pruning*, v simulácií bola použité manuálne orezanie VLAN siete na *trunk* linkách. Toto obmedzenie bolo použité najmä u *trunk* liniek prístupových prepínačov, nakoľko tie používajú len VLAN siete č. 50, pre správu prepínača, 61 a 62 pre hlasovú prevádzku a jednu VLAN sieť pre dáta, podľa umiestnenia v rozvodni. *Trunk* linky medzi distribučnými a hlavným prepínačom bol

ponechaný rozsah VLAN sietí 50-62, nakoľko pri orezaní by linky neprenášali prevádzku z ostatných sietí pri výpadku hlavnej linky smerom k hlavnému prepínaču.

#### Príklad manuálneho orezania pre prístupový prepínač v rozvodni MDF:

```
sw-u5-mdf-1(config)#interface fastethernet 0/24
sw-u5-mdf-1(config-if)#switchport trunk allowed vlan 50,51,61,62
```

#### Aktivácia VTP Pruning na reálnom prepínači:

```
switch(config)#vtp pruning
switch(config-if)#switchport trunk pruning vlan remove vlanlist
switch(config-if)#switchport trunk pruning vlan add vlanlist
```

S automatickým nastavením, ale môže vzniknúť riziko, že na *trunk*-och môžu byť odrezané také VLAN siete, ktoré istých prípadoch sú žiaduce, pretože predvolene sú všetky VLAN siete označené ako *eligible for pruning* (vhodné na odrezanie). K tomu aby neboli odstránené všetky slúži, druhý zobrazený príkaz. Tretí príkaz opäť pridá VLAN sieť do zoznamu odrezateľných VLAN sietí.

## 7.5 Spanning Tree Protocol

Prepínače majú predvolene nastavený ako STP protokol nastavený PVST. Ten má ale pomalú konvergenciu siete. Z tohto dôvodu bol na každom prepínači nastavený protokol Rapid PVST+. Zároveň v sieti boli určené prepínače, ktoré budú zastávať funkciu *root bridge*. Ide o hlavný prepínač **x-switch-u5**, ktorý je nastavený ako primárny prepínač pre túto funkciu a prepínač **gswitch-u5-idf1**, nastavený ako sekundárny *root bridge*. Ten prevezme úlohu *root bridge* v prípade zlyhania primárne určeného prepínača.

#### Príkaz pre nastavenie Rapid PVST+ protokolu:

```
x-switch-u5(config)#spanning-tree mode rapid-pvst
```

#### Príkaz pre nastavenie pre funkciu root bridge:

```
x-switch-u5(config)#spanning-tree vlan 50-62 root primary
gswitch-u5-idf1(config)#spanning-tree vlan 50-62 root secondary
```

## 7.6 EtherChannel

Po nakonfigurovaní prepínačov boli *uplink* linky smerom k hlavnému prepínaču spojené do logického kanálu pomocou technológie agregácie liniek. K účelu vytvorenia kanálu bol použitý protokol PagP.

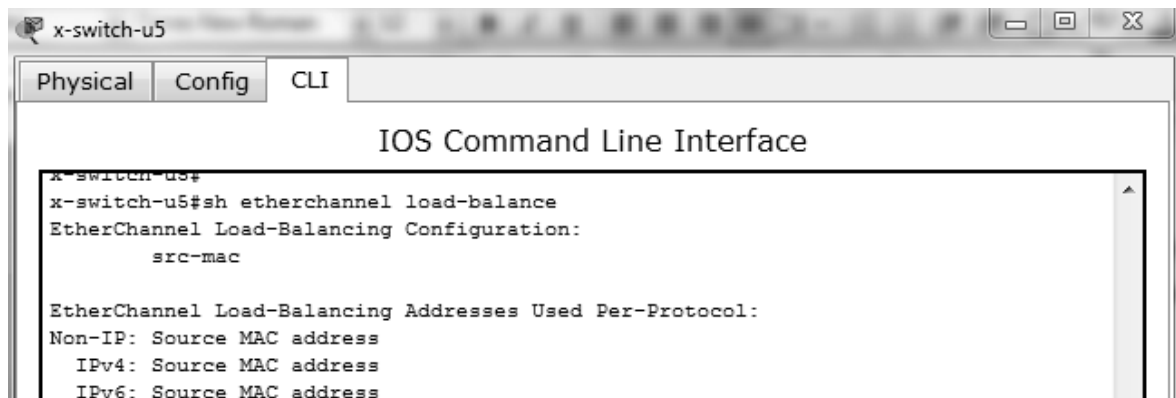
### Príklad pre nastavenie EtherChannel:

```
x-switch-u5(config)#interface range fastethernet 0/1-6
x-switch-u5(config-if-range)#channel-group 1 mode desirable
gswitch-u5-mdf(config)# interface range fastethernet 0/19-24
gswitch-u5-mdf(config-if-range)#channel-group 1 mode desirable
```

Zároveň, je možné nastaviť algoritmus rozloženia záťaže. Ten bol v simulácií ponechaný na svojej predvolenej hodnote: **src-mac**. Overenie použitého algoritmu zobrazuje obrázok č.30.

### Príkaz pre konfiguráciu algoritmu:

```
x-switch-u5(config)#port-channel load-balance ?
dst-ip          Dst IP Addr
dst-mac         Dst Mac Addr
src-dst-ip      Src XOR Dst IP Addr
src-dst-mac     Src XOR Dst Mac Addr
src-ip          Src IP Addr
src-mac         Src Mac Addr
x-switch-u5(config)#port-channel load-balance src-mac
```



Obr. 30. Výstup príkazu *show etherchannel load-balance*.

## 7.7 Smerovanie medzi VLAN siet'ami

Pre nastavenie hlavného prepínača do úlohy smerovača medzi VLAN siet'ami, bolo potrebné u neho aktivovať smerovacie služby.

### Aktivácia smerovania na prepínači:

```
x-switch-u5(config)#ip routing
```

Zároveň každú VLAN sieť boli na hlavnom prepínači vytvorené virtuálne rozhrania, rovnako ako v prípade VLAN pre správu zariadení. IP adresy boli opäť použité podľa tabuľky č.10.

Ďalším krokom bolo zabezpečenie konektivity so smerovačom na U13. K tomuto účelu bolo použité rozhranie fa0/24. Tomuto rozhraniu bolo potrebné definovať, že sa má správať ako rozhranie na sieťovej vrstve. Na prepojenie prepínača s hlavným smerovačom U13 bol použitý rozsah 10.0.0.0/30 IP adries. Pre hlavný prepínač na U5 bola priradená druhá adresa z tohto rozsahu.

### Príkazy pre aktiváciu funkcií sieťovej vrstvy na prepínači:

```
x-switch-u5(config)#interface fastethernet 0/24
x-switch-u5(config-if)#no switchport
x-switch-u5(config-if)#ip address 10.0.0.2 255.255.255.252
x-switch-u5(config-if)#no shutdown
```

Po nadefinovaní rozhrania bola vytvorená predvolená cesta, ktorá bude pakety s cieľovou adresou mimo definované siete smerovať na U13.

### Príkaz pre nastavenie predvolenej cesty:

```
x-switch-u5(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0/24
```

## 7.8 DHCP a DNS serveri

V simulácií sa okrem koncových počítačov nachádzajú serveri, ktorý poskytujú služby DHCP, DNS a http servera. Porty na prístupovom prepínači pre tieto serveri sú určené pre VLAN 60.

DHCP

Service  On  Off

Pool Name: SERVER-VLAN

Default Gateway: 10.5.10.1

DNS Server: 0.0.0.0

Start IP Address: 10 5 10 2

Subnet Mask: 255 255 255 0

Maximum number of Users: 253

TFTP Server: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Number	TFTP Sever
MDF-2	10.5.2.1	10.5.10.3	10.5.2.2	255.255.255.0	253	0.0.0.0
IDF1-1	10.5.3.1	10.5.10.3	10.5.3.2	255.255.255.0	253	0.0.0.0
IDF1-2	10.5.4.1	10.5.10.3	10.5.4.2	255.255.255.0	253	0.0.0.0
IDF2-1	10.5.5.1	10.5.10.3	10.5.5.2	255.255.255.0	253	0.0.0.0
IDF2-2	10.5.6.1	10.5.10.3	10.5.6.2	255.255.255.0	253	0.0.0.0
IDF3-1	10.5.7.1	10.5.10.3	10.5.7.2	255.255.255.0	253	0.0.0.0
IDF3-2	10.5.8.1	10.5.10.3	10.5.8.2	255.255.255.0	253	0.0.0.0
WIFI-EDU-ROAM-1	10.5.9.1	10.5.10.3	10.5.9.2	255.255.255.0	253	0.0.0.0
Voice-1	10.5.11.1	10.5.10.3	10.5.11.10	255.255.255.0	246	10.5.11.2
Voice-2	10.0.0.1	10.5.10.3	10.5.12.2	255.255.255.0	253	10.0.0.1
MDF-1	10.5.1.1	10.5.10.3	10.5.1.2	255.255.255.0	253	0.0.0.0

Obr. 31. Nastavenie DHCP serveru.

Obrázok č.31 zobrazuje nastavenie rozsahov na DHCP serveri. Pre správnu funkciu DHCP servera pri priradovaní IP adries koncovým staniciam bolo potrebné na centrálnom prepínači zapnúť funkciu, ktorá umožňuje preposlať *broadcast* požiadavku na DHCP server, pretože DHCP server a koncové stanice sa nachádzajú v rozdielnych VLAN sieťach. Týmto sa z prepínača stane DHCP *Relay Agent*. Túto funkciu treba zapnúť pre každé virtuálne VLAN rozhranie na prepínači.

### Príkaz pre nastavenie preposielania špecifického *broadcast*:

```
x-switch-u5(config)#interface range VLAN 51-62
x-switch-u5(config-if-range)#ip helper-address 10.5.10.2
```

IP adresa v druhom príkaze patrí DHCP serveru.

DNS

DNS Service  On  Off

Resource Records

Name:  Type: A Record

Address:

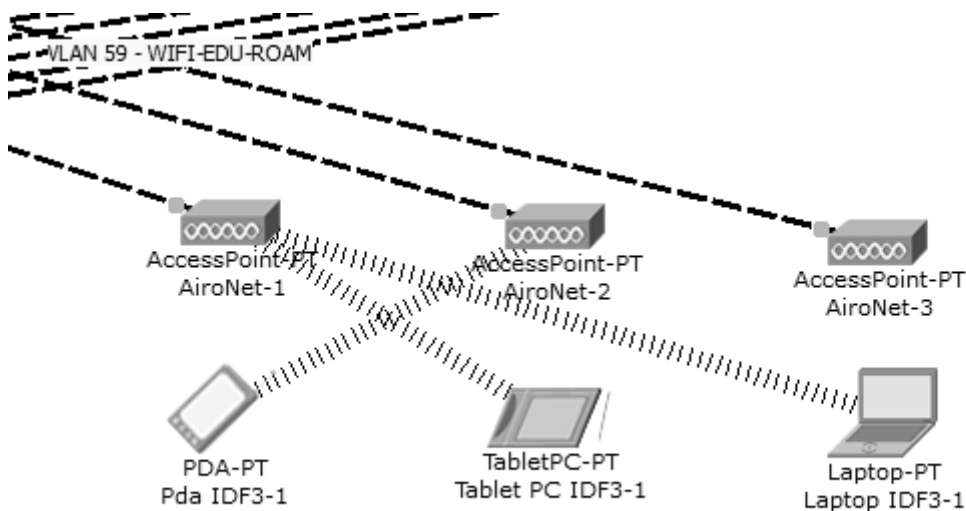
No.	Name	Type	Details
1	google	CNAME	www.google.com
2	google.com	CNAME	www.google.com
3	www.google.com	A Record	18.18.18.2
4	www.vyuka.fai.utb.cz	A Record	10.5.10.4

Obr. 32. Nastavenie DNS servera.

Použitý DNS server slouží najmä na testovacie účely, pričom obsahuje záznam pre adresu `www.google.com`, ktorá odkazuje na IP adresu `loopback0` na prepínači označenom ako U13. Ďalej sa tu nachádza záznam pre http server, na ktorom beží testovacia stránka `www.vyuka.fai.utb.cz`.

## 7.9 VoIP a bezdrôtové zariadenia

Do simulácie zároveň boli zahrnuté bezdrôtové prístupové body a zariadenia. Tie sú umiestnené v *cluster-i* nazvanom IDF3 – Access Switches + Wireless.



Obr. 33. Simulácia bezdrôtovej siete eduroam.

Prístupové body sú pripojené k distribučnému prepínaču `gswitch-u5-idf3`, pričom porty, ktoré pripojujú tieto prístupové body sú v prístupovom režime pre VLAN č.59, ktorá je vyhradená pre sieť eduroam. Ako SSID (Service Set ID) bol zvolený názov: **eduroam**.

Technológia VoIP bola simulovaná pomocou Cisco Unified Communication Manager Express - UCME. Ide o IP-PBX implementovanú v Cisco IOS. Táto technológia je určená malým alebo podnikom pričom podporuje SCCP (Skinny Client Control Protocol) a SIP protokoly. Táto technológia bola aktivovaná na smerovači na U13 pre simuláciu centralizovaného modelu. Simulovaná telefónia používa SCCP protokol, ktorý používa port 2000.

### Príkazy použité pre nastavenie UCME:

```
U13(config)#telephony-service
U13(config-telephony)#max-dn 9
```

```
U13(config-telephony)#max-ephones 42
U13(config-telephony)#ip source-address 10.0.0.1 port 2000
U13(config)#ephone-dn 1
U13(config-ephone-dn)#number 8000
U13(config)#ephone-dn 2
U13(config-ephone-dn)#number 8001
...
U13(config)#ephone 1
U13(config-ephone)#button 1:1
```

Na to aby IP telefónom bola priradená IP adresa z rozsahu určeného pre hlasovú prevádzku bolo potrebné portu nastaviť hlasovú VLAN.

#### Príkaz pre nastavenie hlasovej VLAN siete:

```
sw-u5-idf2-1(config)#interface fastEthernet 0/1
sw-u5-idf2-1(config-if)#switchport voice vlan 62
```

## 7.10 Nastavenie prístupových portov a bezpečnosť

### 7.10.1 Nastavenie prístupových portov

Po pripojení všetkých koncových zariadení a oživení potrebných služieb boli na prístupových portoch zavedené funkcie ktoré zvyšujú funkčnosť a bezpečnosť siete. Na každom prístupovom porte bola použitá funkcionálna **PortFast**. Použitie tejto funkcie je vhodné iba pre prístupové porty, nakoľko po pripojení zariadenia, port prejde automaticky do preposielacieho stavu (*forwarding state*). Táto funkcionálna zlepšuje funkčnosť siete a pomáha napr. pri žiadosti o pridelenie IP adresy cez DHCP server.

V prípade, že by na port, kde je aktivovaná funkcionálna *portfast* bol pripojený ďalší prepínač, alebo iné než koncové zariadenie, by mohlo spôsobiť L2 slučku. Táto situácia nesmie nastať, nakoľko toto predstavuje veľké bezpečnostné riziko, ktoré by mohla znefunkčovať počítačovú sieť. Z tohto dôvodu je na portoch aktivovaná funkcia **BPDU Guard** (Bridge Protocol Data Unit). Tá spôsobí, že ak port, ktorý je nastavený **PortFast**, prijme BPDU správu ho vypne. Tým sa zabráni aby sa zmenila topológia STP protokolu. Funkcia BPDU *guard* nesmie byť aktivovaná na portoch, ktoré pripojujú IP telefón. Je to z dôvodu, že IP telefón má integrovaný v sebe prepínač, pomocou ktorého je možné

pripojiť PC. Týmto by pri aktivovaní funkcie BPDU *guard* bol port automaticky vypnutý, nakoľko prijme BPDU správu.

Spolu s týmito funkciami STP protokolu je na prístupových portoch nastavené zabezpečenie. Oproti predvolenému nastaveniu, kedy pri narušení pravidiel sa port vypne, bolo nastavené obmedzenie v podobe zakázanej komunikácie na danom porte, pre cudziu MAC adresu. Zoznam MAC adries bol získaný pomocou funkcionality *sticky*, ktorá dynamicky nájdené MAC adresy „prilepí“ do konfigurácie prepínača.

#### Príkazy pre konfiguráciu daných funkcionalít:

```
sw-u5-mdf-1(config)#interface range fastethernet 0/1-23
sw-u5-mdf-1(config-if-range)#spanning-tree portfast
sw-u5-mdf-1(config-if-range)#spanning-tree bpduguard enable
sw-u5-mdf-1(config-if-range)#switchport port-security
sw-u5-mdf-1(config-if-range)#switchport port-security mac-address sticky
sw-u5-mdf-1(config-if-range)#switchport port-security violation restrict
```

Príkaz č.4 aktivuje na prepínači zabezpečenie portov, ktoré predvolene je vypnuté. Príkaz č.5 aktivuje *sticky* režim. Príkazom č.6 sa zmení režim na *restrict*.

Predvolená hodnota u maximálne počtu adries je 1. U portov, ktoré pripojujú IP telefóny musia byť porty nastavené minimálne na hodnotu 2. Zároveň porty nesmú používať statické alebo *sticky* MAC adresy pre hlasovú VLAN sieť.

#### 7.10.2 Bezpečnostné funkcie

**DHCP snooping** je bezpečnostná funkcionalita, ktorá poskytuje zabezpečenie filtrovaní nedôveryhodných DHCP správ, tvorením a spravovaním DHCP *snooping binding* tabuľky. Nedôveryhodná správa je taká, ktorá je prijatá mimo sieť, alebo *firewall* a ktorá môže spôsobiť útok v rámci počítačovej siete.

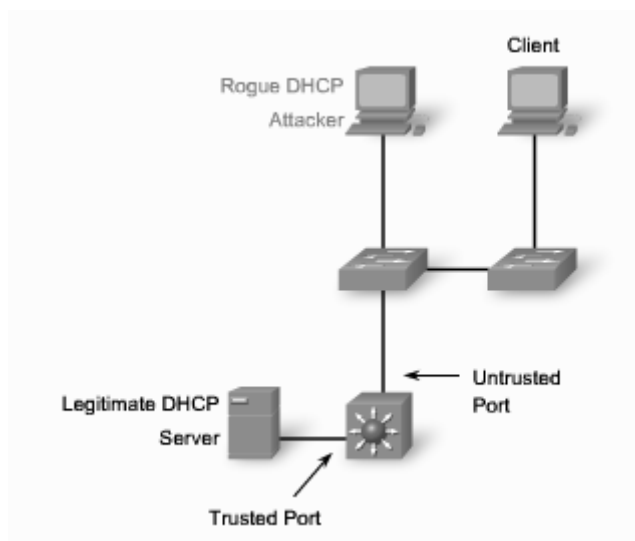
Nakoľko ale táto funkcia nie je podporovaná v programe Packet Tracer, ide o základný bezpečnostný prvok používaný v počítačových sieťach. Dôvodom používania môže byť ochrániť sieť pred útokmi, tak i pred neodborným zásahom do siete, napr. pripojením domáceho smerovača, ktorý bežne ponúka funkciu DHCP na svojich prepínacích portoch. To môže viesť infekcie siete zlými IP adresami, čo môže mať za následok nefunkčnosť služieb, alebo iné problémy.

**Príkazy pre konfiguráciu DHCP snooping:**

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan number [ number ]
Switch(config)#ip dhcp snooping information option
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate rate
```

Príkaz č.1 aktivuje funkciu DHCP *snooping* na prepínači. Príkaz č.2 aktivuje túto funkciu pre dané VLAN siete. Ďalší príkaz aktivuje vloženie tzv. **Option 82** dát.

Základom tejto bezpečnostnej funkcie je určiť, ktoré porty môžu odpovedať na DHCP požiadavky. Nedôveryhodné porty sú také, ktoré nie sú určené ako dôveryhodné. Nedôveryhodné porty môžu byť zdrojom iba DHCP požiadaviek. Príkaz číslo č.4 definuje dané rozhranie ako dôveryhodné. Príkaz č.5 definuje aký počet DHCP paketov za sekundu môže dané rozhranie prijať.



Obr. 34. Schéma použitia DHCP Snooping.<sup>16</sup>

**Prístupové zoznamy** (*Access Control Lists*) slúžia ako jednoduchý paketový *firewall*. Základom filtrácie paketov sa deje na základe zdrojových IP adries, na ktoré sa následne aplikujú dané pravidlá. V simulácii bol vytvorený zoznam, ktorý zamedzuje ostatným PC

<sup>16</sup> - Obrázok použitý z [3]

v sieti, aby kontaktovali IP adresy v Management VLAN. Toto právo bolo ponechané len Management PC, ktoré je pripojené cez prepínač na smerovač označený ako U13.

#### Použité príkazy:

```
x-switch-u5(config)#access-list 1 permit host 192.168.0.3
x-switch-u5(config)#access-list 1 permit 10.5.0.0 0.0.0.255
x-switch-u5(config)#access-list 1 deny any
```

### 7.11 Protokol HSRP

Protokol HSRP v Packet Traceri nie je podporovaný. Jeho implementácia do siete však zvyšuje dostupnosť v sieti pri výpadku hlavného prepínača, ktorý sprostredkuje smerovanie medzi VLAN sieťami. Pre tento účel je potrebné nastaviť prepínač **gswitch-u5-idf1**, ktorý bude spĺňať náhradného smerovača, rovnako ako hlavný prepínač, pričom je potrebné na ňom vytvoriť dané VLAN rozhrania a aktivovať funkciu smerovania.

Pre prípad simulácie by následne bolo potrebné upraviť IP adresy buď na DHCP serveri, alebo na hlavnom prepínači, na adresu virtuálneho smerovača.

#### Príklad nastavenia pre vytvorenie záložného prepínača pre smerovanie medzi VLAN sieťami:

```
x-switch-u5(config)#interface vlan 51
x-switch-u5(config-if)#ip address 10.5.1.2 255.255.255.0
x-switch-u5(config-if)#standby 1 ip 10.5.1.1
x-switch-u5(config-if)#standby priority 120
x-switch-u5(config-if)#standby 1 authentication UTB
gswitch-u5-idf1(config)interface vlan 51
gswitch-u5-idf1(config-if)#ip address 10.5.1.3 255.255.255.0
gswitch-u5-idf1(config-if)#standby 1 ip 10.5.1.1
gswitch-u5-idf1(config-if)#standby 1 authentication UTB
...
```

## 7.12 Konfiguračné súbory

Konfiguračné súbory sú umiestnené ako príloha CD-ROM. Ide o hlavný prepínač označený ako **x-switch-u5** (príloha č.26), distribučný prepínač **gswitch-u5-mdf** (príloha č.27) a po jednom prepínači z prístupovej vrstvy (príloha č.28, 29, 30 a 31).

Súbor so simuláciou je umiestnený ako príloha č.32 na CD-ROM.

## 8 EKONOMICKÉ ZHODNOTENIE NÁVRHOV

I keď v súčasnosti počítačová sieť vyhovuje nárokom, postupom času je jej modernizácia nevyhnutná. Nakoľko kompletná modernizácia nie je možná, či už z ekonomického pohľadu tak i časového, nakoľko i predkonfigurované komponenty treba dokonfigurovať a „doladiť“ na mieste, po zapojení s ostatnými komponentmi.

Z tohto dôvodu sa návrh prechodnej modernizácie javí ako optimálne riešenie nakoľko zavádza len jeden nový prepínač, ktorý celkovo zvýši priepustnosť v sieti a možnosť pripojiť sieť na U5 10 Gbps linkou. Pri tomto návrhu je použitá technológia agregácie liniek, ktorá umožní pripojiť distribučné prepínače k hlavnému pomocou súčasnej kabeláže, rýchlejšie. Ďalším ekonomickým aspektom je použitie len 1 optického modulu, ktorý zabezpečuje komunikáciu po optickom vlákne, nakoľko tieto moduly tvoria podstatnú časť nákladov pri nákupe nového prepínača. Nevýhodou tohto návrhu je, že nemodernizuje prístupovú vrstvu a ponecháva rýchlosť pre koncové stanice rovnakú aká je v súčasnom stave. Toto riešenie modernizácie predstavuje tzv. „za málo peňazí, veľa muziky“.

Navrhovaná modernizácia č.1 predpokladá hlavný prepínač v novom vedecko-výskumnom ICT centre. Ide o modulárny prepínač, ktorý poskytuje množstvo funkcií. Jeho vhodným umiestnením môže nahradiť veľké množstvo prepínačov, čím sa vyrovná jeho investícia oproti klasickému riešeniu viacerých prepínačov. Takýto prístup k riešeniu znižuje náklady, nakoľko prístupové prepínače možno pripojiť priamo k hlavnému prepínaču, čím odpadá použitie distribučných prepínačov. Pre pripojenie siete U5 k tomuto prepínaču je ale nutné vybudovať nové spojenie. Investícia do nových prístupových prepínačov nie je až tak veľká, nakoľko navrhované prístupové prepínače nahrádzajú súčasné 2. Zároveň návrh je pripravený na implementáciu VoIP technológie, nakoľko navrhnuté prepínače sú natívne určené pre aplikáciu zjednoteného komunikačného modelu. Nevýhodou tejto varianty je vyššia finančná náročnosť, nakoľko počíta s nahradením distribučných a prístupových prepínačov a zároveň potreba zaobstarania aspoň 8 optických modulov, ktoré zabezpečia komunikáciu po optických kábloch.

Na modernizáciu č.2 sa možno pozerať z 2 pohľadov, jeden je ako alternatíva k návrhu č.1 a druhý pohľad ako na ďalšie rozšírenie siete. Táto alternatíva uvažuje hlavný prepínač na U5. Oproti variante č.1, namiesto modulárneho prepínača používa fixný prepínač s podporou 10 Gbps prenosov. To sa prejaví na cene riešenia, nakoľko pri návrhu č.1 treba

zakúpiť prepínač s určitou veľkosťou šasi a obslužné modulu. Prepojenie s ICT centrom môže pripájať iba potrebný počet distribučných prepínačov. Riešenie chrbticového prvku na U5, bude vyžadovať investície do prístupový a distribučných prepínačov, ktoré v predchádzajúcom prípade zabezpečoval modulárny prepínač. V prípade, že tento návrh bude doplnením, tak sa zvýši dostupnosť kľúčových prvkov. Zároveň sa môžu použiť funkcie podporované hlavne na chrbticovej vrstve.

## ZÁVER

Hlavným cieľom tejto práce bolo navrhnúť riešenie modernizácie a zrýchlenie počítačovej siete na U5. Navrhované riešenie spočíva v modernizácii kľúčových prvkov a nasadení takých technológií, ktoré by umožnili danú modernizáciu.

V práci sa nachádzajú všetky body, ktoré boli určené zadaním tejto práce. Prvá časť práce sa zaoberá technológiami, ktoré sú použité v navrhovaných riešeniach a zároveň som ich neuviedol vo svojej bakalárskej práci. Na základe analýzy súčasného stavu počítačovej siete boli vypracované návrhy danej modernizácie. Budovanie vysoko-dostupnej počítačovej siete si vyžaduje hlboké znalosti problematiky a zároveň tiež praktické skúsenosti pri navrhovaní takýchto sietí. Z tohto dôvodu je možné sieť modernizovať rozličnými spôsobmi. Zároveň najväčším obmedzením pri návrhu siete je rozpočet učený na danú modernizáciu. I keď práca neuvažovala konkrétny rozpočet pre danú modernizáciu, uvedené návrhy počítajú s ekonomickou zložkou pri návrhoch modernizácie siete.

Okrem návrhov modernizácie, táto práca spočívala i vo vytvorení konfiguračných súborov. K tomuto účelu bolo použité simulačné prostredie Packet Tracer od spoločnosti Cisco. Nakoľko nejde o reálny simulátor počítačových sietí, neobsahuje všetky funkcie ako reálne zariadenia. Z tohto dôvodu v časti, ktorá sa zaoberala popisom simulácie sú uvedené i dodatočné príkazy, ktoré umožnia danú funkcionality. V závere práci sú zhrnuté jednotlivé navrhované modernizácie po ekonomickej stránke.

## CONCLUSION

The main goal of this thesis was to propose solution for modernization and acceleration of computer network at U5. The proposed solution is based on modernization of the key elements and on deployment of technologies which help to accomplish this task.

The thesis contains all the objectives, which were assigned for this paper. The first part describes technologies, which are used in proposed solutions and they were not mentioned in my bachelor thesis. Based on the analysis of the current state of computer networks have been developed that modernization proposals. Building of the high-available computer networks requires deep knowledge of the domain, together with practical experiences with designing of these networks. Therefore, the computer network can be upgraded in various ways. At the same time, the most restrictive limitation of designing computer network is given budget for modernization. Although that the thesis does not consider a specific budget for that modernization, the proposed solutions took economic point of view into account.

In the addition of proposal of the new designs, this thesis consisted in the creation of configuration files. For this purpose was used simulation environment Packet Tracer by Cisco. Since it is not real computer network simulation it does not contain all features like real equipment. Therefore, in the part which describes work in Packet Tracer, are mentioned commands which are not supported and provide given functionality. The last section summarize given proposals from economic point of view.

**ZOZNAM POUŽITEJ LITERATURY**

- [1] SOLARIX CABLING SYSTEM. *2008 Katalog produktů: Hvězdné řešení* [online]. 2008 [cit. 2012-01-29]. Dostupný z:  
[http://www.ped.muni.cz/wtech/03\\_studium/teps/Katalog\\_Solarix\\_2008.pdf](http://www.ped.muni.cz/wtech/03_studium/teps/Katalog_Solarix_2008.pdf)
- [2] Svět sítí. *Strukturované kabeláže* [online]. 2001 [cit. 2012-01-29]. Dostupný z: <http://www.svetsiti.cz/rubrika.asp?rid=17&tid=48>
- [3] CISCO SYSTEMS, Inc. *Curriculum Exploration – LAN Switching and Wireless* [online]. [cit. 2012-01-29]. Dostupný z: <http://cisco.netacad.net>
- [4] CISCO SYSTEMS, Inc. *EtherChannel* [online]. 2003 [cit. 2012-01-29]. Dostupný z:  
[http://www.cisco.com/en/US/tech/tk389/tk213/tsd\\_technology\\_support\\_protocol\\_home.html](http://www.cisco.com/en/US/tech/tk389/tk213/tsd_technology_support_protocol_home.html)
- [5] CISCO SYSTEMS, Inc. *Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches* [online]. 2007 [cit. 2012-01-29]. Dostupný z:  
[http://www.cisco.com/en/US/tech/tk389/tk213/technologies\\_tech\\_note09186a0080094714.shtml](http://www.cisco.com/en/US/tech/tk389/tk213/technologies_tech_note09186a0080094714.shtml)
- [6] CISCO SYSTEMS, Inc. *Internetworking Technology Handbook* [online]. 2012 [cit. 2012-01-29]. Dostupné z:  
[http://docwiki.cisco.com/wiki/Internetworking\\_Technology\\_Handbook](http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook)
- [7] WALLACE, Kevin. CISCO SYSTEMS, Inc. *Authorized Self-Study Guide Cisco Voice over IP (Cvoice)*. Indianapolis: Cisco Press, 2007. ISBN 1-58705-262-8.
- [8] TECHNOLOGYUK. *Computer Networks: Structured Cabling* [online]. 2001 – 2012 [cit. 2012-01-29]. Dostupné z:  
[http://www.technologyuk.net/telecommunications/networks/structured\\_cabling.shtml](http://www.technologyuk.net/telecommunications/networks/structured_cabling.shtml)
- [9] THE FIBER OPTIC ASSOCIATION. *Connector Identifier* [online]. Fallbrook, 2005-2010 [cit. 2012-03-06]. Dostupné z:  
<http://www.thefoa.org/tech/connID.htm>

- [10] CISCO SYSTEMS INC. *Cisco EtherChannel Technology: White Paper* [online]. 1992-2003 [cit. 2012-03-06]. Dostupné z: [http://www.cisco.com/en/US/tech/tk389/tk213/technologies\\_white\\_paper09186a0080092944.shtml](http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml)
- [11] BOUŠKA, Petr. *Cisco IOS 21: EtherChannel, Link Agregation, PagP, LACP, NIC Teaming* [online]. 08.06.2009, 01.07.2009 [cit. 2012-03-06]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-ios-21-etherchannel-link-agregation-pagp-lACP-nic-teaming/>
- [12] IBM. *Dokumentácia pre AIX: IEEE 802.3ad Link Aggregation configuration* [online]. 1989-2008 [cit. 2012-03-06]. Dostupné z: [http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.commadmn/doc/commadmndita/ieee8023ad\\_intro.htm](http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.commadmn/doc/commadmndita/ieee8023ad_intro.htm)
- [13] EMPRESA MEDIA, a.s. *Technologie přenosu dat přes optická vlákna: Konektory optických vláken* [online]. 22.1.2008 [cit. 2012-04-04]. Dostupné z: [http://pctuning.tyden.cz/hardware/site-a-internet/9994-technologie\\_prenosu\\_dat\\_pres\\_opticka\\_vlakna?start=3](http://pctuning.tyden.cz/hardware/site-a-internet/9994-technologie_prenosu_dat_pres_opticka_vlakna?start=3)
- [14] CISCO SYSTEMS, Inc. *Cisco Catalyst 2960-S FlexStack: Description, Usage, and Best Practices* [online]. 2012 [cit. 2012-04-24]. Dostupné z: [http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/white\\_paper\\_c11-578928.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/white_paper_c11-578928.html)
- [15] CISCO SYSTEMS, Inc. *Network Infrastructure: Layer 2 Access Design Recommendations* [online]. June 4, 2010 [cit. 2012-05-03]. Dostupné z: [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/srnd/7x/netstruc.html#wp1043655](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/netstruc.html#wp1043655)
- [16] POWER INTEGRATIONS. *What is Power over Ethernet (PoE)?: Classification Phase* [online]. 2012 [cit. 2012-05-12]. Dostupné z: <http://www.powerint.com/node/113>
- [17] CISCO SYSTEMS, Inc. *Flex Links* [online]. 2012 [cit. 2012-05-12]. Dostupné z: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/flexlink.html>

**ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK**

ACR	Attenuation-to-Crosstalk Ratio
ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
BPDU	Bridge Protocol Data Unit
CCNA	Cisco Certified Network Associate
CLI	Command Line Interface
CNAM	Calling Name
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CWDM	Coarse Wavelength Division Multiplexing
DSP	Digital Signaling Processor
DWDM	Dense Wavelength Division Multiplex
EIA	Electronic Industries Alliance
ELFEXT	The Equal-Level Far-End Crosstalk
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
HLDC	High-Level Data Link Control
http	Hyper Transfer Text Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IOS	Internetwork Operation System
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	ITU – Telecommunication Standardization Sector

---

LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MLP	Multi Link PPP
MMF	Multi Mode Fiber
MPLS	Multi Packet Label Switching
MSTP	Multiple Instance Spanning Tree Protocol
NIC	Network Interface Card
NTP	Network Time Protocol
PagP	Port Aggregation Protocol
PBX	Private Branch eXchange
PDA	Personal Digital Assistant
PoE	Power over Ethernet
PPP	Point to Point Protocol
PSACR	Power Sum ACR
PSELFEXT	Power Sum ELFEXT
PSNEXT	Power-Sum Near-End Cross Talk
PSTN	Public Switched Telephone Network
QoS	Quality of Service
ROI	Return of Investments
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTP	Real Time Protocol
SAP	Session Announcement Protocol

---

SCCP	Skinny Client Control Protocol
ScSTP	Screened Shielded Twisted Pair
ScTP	Screened Twisted Pair
SDP	Session Description Protocol
SFP	Small Form-Factor Pluggable
SIP	Session Initiation Protocol
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SRST	Survivable Remote Site Telephony
SS7	Signaling System 7
SSID	Service Set ID
STP	Shielded Twisted Pair
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TIA	Telecommunications Industry Association
TP	Twisted Pair
UAS	User Agent Server
UCME	Unified Communication Manager Express
UDP	User Datagram Service
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

---

UTP	Unshielded Twisted Pair
VLAN	Virtual LAN
VoIP	Voice over IP
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WIFI	Wireless Fidelity
WLAN	Wireless LAN

**ZOZNAM OBRÁZKOV**

Obr. 1. Model štruktúrovanej kabeláže.....	15
Obr. 2. 19“ Patch panel s 24 portami RJ45.....	17
Obr. 3. Príklad vyhotovenia zásuvky RJ45. ....	18
Obr. 4. Príklady vyhotovenia 19“ rozvodných skriň. ....	19
Obr. 5. Typy káblov TP podľa ISO/IEC 11801.....	21
Obr. 6. Jednovidové optické vlákno. ....	23
Obr. 7. Mnohovidové optické vlákno so skokovou zmenou indexu lomu. ....	24
Obr. 8. Mnohovidové optické vlákno s postupnou zmenou indexu lomu. ....	24
Obr. 9. Tienený konektor RJ45.....	25
Obr. 10. Optické konektory. ....	26
Obr. 11. Linka typu Channel a Permanent link. ....	28
Obr. 12. Hierarchický sieťový model. ....	30
Obr. 13. Agregácia liniek.....	33
Obr. 14. Kompresia RTP hlavičky.....	49
Obr. 15. Centralizovaná VoIP architektúra. ....	51
Obr. 16. Distribuovaná architektúra na báze H.323. ....	53
Obr. 17. Distribuovaná SIP architektúra.....	55
Obr. 18. Chrbticová optická sieť UTB ve Zlíně. ....	58
Obr. 19. Rozloženie rozvodní na U5. ....	59
Obr. 20. Prepojenie jednotlivých rozvodní.....	60
Obr. 21. Logická topológia aktívnych prvkov siete na U5.....	62
Obr. 22. Typy bezdrôtových prístupových bodov na U5. ....	63
Obr. 23. Možnosti agregácie liniek na U5.....	70
Obr. 24. Navrhovaná prechodná modernizácia. ....	73
Obr. 25. Porovnanie FlexStack klasického riešenia. ....	76
Obr. 26. Alternatívne cesty u prechodnej modernizácie.....	83
Obr. 27. Použitie HSRP protokolu v prechodnej modernizácií.....	85
Obr. 28. Simulačné zapojenie v Packet Tracer.....	89
Obr. 29. Výstup príkazu Show vlan brief. ....	94
Obr. 30. Výstup príkazu show etherchannel load-balance. ....	97
Obr. 31. Nastavenie DHCP serveru. ....	99

Obr. 32. Nastavenie DNS servera.....	99
Obr. 33. Simulácia bezdrôtovej siete eduroam.....	100
Obr. 34. Schéma použitia DHCP Snoofing. ....	103

**ZOZNAM TABULIEK**

Tab. 1. Označovanie káblov podľa ISO/IEC 11801. ....	21
Tab. 2. Štandardy pre metalickú kabeláž. ....	27
Tab. 3. Rozloženie počtu hodnôt. ....	37
Tab. 4. OSI model a VoIP komponenty a protokoly. ....	46
Tab. 5. Riešenia pre implementáciu VoIP. ....	47
Tab. 6. Obsadenie jednotlivých rozvodní. ....	62
Tab. 7. Tabuľka VLAN sietí na U5. ....	64
Tab. 8. Ostatné VLAN siete na U5. ....	65
Tab. 9. Navrhovaný počet prepínačov. ....	77
Tab. 10. Navrhované logické rozdelenie. ....	81
Tab. 11. Tabuľka rozdelenia siete určenej pre manažment zariadení. ....	93

**ZOZNAM PRÍLOH**

- P I Tabuľka kategórií TP káblov. CD-ROM:\01\_Tabuľka\_kategórií\_TP\_káblov.xls
- P II Tabuľka protokolov pre optickú kabeláž. CD-ROM:\02\_protokoly\_pre\_optickú\_kabeláž.xls
- P III Tabuľka algoritmov EtherChannel vyrovnávania záťaže pre jednotlivé platformy. CR-ROM:\03\_Prehľad\_algoritmov\_pre\_rôzne\_platformy.xls
- P IV Rozmiestnenie prístupových bodov bezdrôtovej siete eduroam. CD-ROM:\04\_U5\_1np.jpg
- P V Rozmiestnenie prístupových bodov bezdrôtovej siete eduroam. CD-ROM:\05\_U5\_2np.jpg
- P VI Rozmiestnenie prístupových bodov bezdrôtovej siete eduroam. CD-ROM:\06\_U5\_3np.jpg
- P VII Rozmiestnenie prístupových bodov bezdrôtovej siete eduroam. CD-ROM:\07\_U5\_6np.jpg
- P VIII Rozmiestnenie prístupových bodov bezdrôtovej siete eduroam. CD-ROM:\08\_U5\_8np.jpg
- P IX Dotazník prieskumu používania bezdrôtovej siete eduroam medzi študentmi U5. CR-ROM:\09\_dotazník\_študent.doc
- P X Otázky pre prieskum používania bezdrôtovej eduroam medzi učiteľmi na U5. CD-ROM:\10\_dotazník\_učiteľ.doc
- P XI Obrázok zobrazujúci prehľad konektorov pre optické vlákna. CD-ROM:\11\_optické\_konektori.jpg
- P XII Dokument obsahujúci základný prehľad štandardou zaoberajúcich sa štruktúrovanou kabelážou. CD-ROM:\12\_štandardy\_štrukturovanej\_kabeláže.doc
- P XIII Dokumentácia produktovej rady prepínačov Cisco Catalyst 3750-X a 3560-X. CD-ROM:\13\_catalyst\_3750-X\_3560-X.pdf

- P XIV Schéma zobrazujúca navrhovanú prechodnú modernizáciu. CD-ROM:\14\_návrh\_prechodnej\_modernizácie.pdf
- P XV Schéma zobrazujúca navrhovanú modernizáciu, variant č.1. CD-ROM:\15\_navrhovaná\_modernizácia\_1.pdf
- P XVI Schéma zobrazujúca navrhovanú modernizáciu, variant č.2. CD-ROM:\16\_navrhovaná\_modernizácia\_2.pdf
- P XVII Dokumentácia produktovej rady prepínačov Cisco Catalyst 2960. CD-ROM:\17\_catalyst\_2960.pdf
- P XVIII Dokumentácia produktovej rady prepínačov Cisco Catalyst 3560. CD-ROM:\18\_catalyst\_3560.pdf
- P XIX Dokumentácia produktovej rady prepínačov Cisco Catalyst 4500-X. CD-ROM:\19\_catalyst\_4500-X.pdf
- P XX Schéma návrhu zapojenia redundancie a prepínačov do stacku, variant č.1. CD-ROM:\20\_schema\_flexstack\_redundancia\_var1.pdf
- P XXI Schéma návrhu zapojenia redundancie a prepínačov do stacku, variant č.2. CD-ROM:\21\_schema\_flexstack\_redundancia\_var2.pdf
- P XXII Tabuľka IP adries prepínačov. CD-ROM:\22\_tabuľka\_ip\_adresy\_prepínače.xls
- P XXIII Tabuľka priradenia portov na jednotlivých prepínačoch. CD-ROM:\23\_tabuľka\_portov.xls
- P XXIV Produktová dokumentácia k telefónnej platforme OpenStage. CD-ROM:\24\_OpenStage-IP-Datasheet.pdf
- P XXV Produktová dokumentácia k produktovej rade Cisco 2500 Wireless Controller. CD-ROM:\25\_2500\_wireless\_controller.pdf
- P XXVI Konfiguračný súbor prepínača x-switch-u5. CD-ROM:\26\_x\_switch\_u5.txt
- P XXVII Konfiguračný súbor prepínača gswitch-u5-mdf. CD-ROM:\27\_gswitch\_u5\_mdf.txt
- P XXVIII Konfiguračný súbor prepínača sw-u5-mdf-1. CD-ROM:\28\_sw-u5-mdf-1.txt
- P XXIX Konfiguračný súbor prepínača sw-u5-idf1-1. CD-ROM:\29\_sw-u5-idf1-1.txt

- P XXX Konfiguračný súbor prepínača sw-u5-idf2-1. CD-ROM:\30\_sw-u5-idf2-1.txt
- P XXXI Konfiguračný súbor prepínača sw-u5-idf3-1. CD-ROM:\31\_sw-u5-idf3-1.txt
- P XXXII Súbor so simuláciou v programe Packet Tracer. CD-ROM:\32\_utb\_u5.pkt