

UNIVERZITA PARDUBICE  
Fakulta elektrotechniky a informatiky

Technologie Spanning Tree Protocolu na platformě MikroTik

Martin Matušina

Bakalářská práce  
2014

Univerzita Pardubice  
Fakulta elektrotechniky a informatiky  
Akademický rok: 2013/2014

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin Matušina**  
Osobní číslo: **I10131**  
Studijní program: **B2646 Informační technologie**  
Studijní obor: **Informační technologie**  
Název tématu: **Technologie Spanning Tree Protocolu na platformě Mikrotik**  
Zadávající katedra: **Katedra informačních technologií**

### Z á s a d y p r o v y p r a c o v á n í :

Cílem práce je ověřit Spanning Tree Protocol na platformě Mikrotik a porovnat jej se zařízením Cisco. V teoretické části autor popíše možnost vzniku smyček na L2 vrstvě a řešení tohoto problému pomocí SPT dle normy IEEE 802.1d včetně RSTP. V praktické části autor navrhne topologie postihující řešení smyček v síti na L2 vrstvě na zařízeních Mikrotik a Cisco včetně příkladů jak každá technologie přistupuje k řešení výpadků linek. V závěrečném hodnocení provede výsledné zhodnocení jednotlivých technologií STP a RSTP.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

LAMMLE, Todd. CCNA: Cisco certified network associate fast pass. 3rd ed.

Indianapolis: Wiley Publishing, 2007, xxix, 467 s. ISBN 978-0-470-18571-1.

PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z: Cisco certified network associate fast pass. 2. aktualiz. vyd. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.


Vedoucí bakalářské práce:

Ing. Soňa Neradová

Katedra softwarových technologií

Datum zadání bakalářské práce: 20. prosince 2013

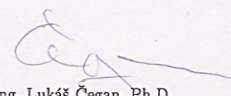
Termín odevzdání bakalářské práce: 9. května 2014



prof. Ing. Simeon Karamazov, Dr.  
děkan



L.S.



Ing. Lukáš Čegan, Ph.D.  
vedoucí katedry

V Pardubicích dne 31. března 2014



## **Prohlášení autora**

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 6. 5. 2014

Martin Matušina

## **Poděkování**

Chtěl bych poděkovat paní.

Tímto bych chtěl vyjádřit své poděkováním paní inženýrce Soně Neradové, pod kterou tato práce vznikla. Zároveň bych jí chtěl poděkovat za poskytnuté materiály a konstruktivní připomínky, které vedly k vypracování této práce. V druhé řadě bych chtěl poděkovat své rodině, která mě po dobu studií morálně ale i finančně podporovala.

## **Anotace**

Cílem práce je ověřit Spanning Tree Protocol na platformě MikroTik a porovnat jej se zařízením Cisco. V teoretické části autor popíše možnost vzniku smyček na L2 vrstvě a řešení tohoto problému pomocí SPT dle normy IEEE 802.1d včetně RSTP. V praktické části autor navrhne topologie postihující řešení smyček v síti na L2 vrstvě na zařízeních MikroTik a Cisco včetně příkladů, jak každá technologie přistupuje k řešení výpadků linek. V závěrečném hodnocení provede výsledné zhodnocení jednotlivých technologií STP a RSTP.

## **Klíčová slova**

Síťová topologie, vznik a řešení smyček

## **Title**

Spanning Tree Protocol on Mikrotik platform.

## **Annotation**

Main goal of bachelor's thesis is to verify how Spanning Tree Protocol works on MikroTik and compare its functionality on Cisco devices. In theoretical part author is going to describe how loops are created on L2 layer and solution of this problem using SPT according IEEE 802.1d including RSTP.

In practical part, author is going to create a topology which is dealing with cycles in second layer on MikroTik and Cisco devices, including examples, how each technology deal with malfunctions. At the end of the bachelor's author will conduct an evaluation of each technologies.

## **Keywords**

Network topology, solving network loops

## Obsah

<b>Seznam zkratek .....</b>	<b>8</b>
<b>Seznam obrázků .....</b>	<b>9</b>
<b>Seznam tabulek .....</b>	<b>9</b>
<b>Úvod .....</b>	<b>10</b>
<b>1 Počítačové sítě .....</b>	<b>11</b>
1.1 WAN .....	11
1.2 MAN .....	11
1.3 LAN .....	12
<b>2 Síťové topologie.....</b>	<b>13</b>
2.1 Fully Connected topology – Plně propojená topologie .....	14
2.2 Bus topology – Sběrníková topologie .....	14
2.3 Ring topology - Kruhová topologie .....	15
2.4 Star topology – Hvězdicová topologie.....	16
2.5 Tree topology – Stromová topologie .....	16
2.6 Hybrid topology – Hybridní topologie .....	17
<b>3 Referenční model ISO/OSI .....</b>	<b>17</b>
3.1 Physical layer - Fyzická vrstva .....	18
3.2 Link layer - Spojová vrstva.....	18
3.3 Network layer - Síťová vrstva - dokument .....	19
3.4 Transport layer - Transportní vrstva .....	19
3.5 Session layer - Relační vrstva .....	19
3.6 Presentation layer - Prezentační vrstva .....	19
3.7 Application layer - Aplikační vrstva.....	20
<b>4 Komponenty v síti .....</b>	<b>20</b>
4.1 Přenosová media .....	20
4.1.1 Optické kabely .....	20
4.1.2 Metalické kabely .....	21
4.1.3 Bezdrátový přenos .....	22
4.2 Propojovací zařízení .....	22
<b>5 Spanning Tree Protocol.....</b>	<b>25</b>
5.1 Redundance v síti.....	25
5.2 Problémy spojené s výskytem smyček .....	26



5.3	Popis technologie STP .....	26
5.4	BPDU .....	27
5.5	Volba root bridge .....	28
5.6	ST Algoritmus - Spanning Tree Algorithm .....	28
5.7	Stavy portů .....	31
5.8	STP detekce změny topologie.....	31
5.9	Varianty STP.....	31
<b>6</b>	<b>Představení platformy MikroTik .....</b>	<b>32</b>
6.1	Možnosti konfigurace RouterBoardu.....	32
6.2	První zapnutí routeru .....	33
6.3	Představení aplikace WinBox .....	33
<b>7</b>	<b>Konfigurace STP na platformě MikroTik.....</b>	<b>35</b>
7.1	Doplňující konfigurace WLAN .....	37
7.2	Konfigurace portů .....	38
7.3	Nastavení DHCP pro bezdrátovou síť .....	41
7.4	Alternativní konfigurace MikroTik s užitím WebFig.....	47
<b>8</b>	<b>Konfigurace STP na platformě Cisco .....</b>	<b>47</b>
8.1	Ukázka konfigurace S1 .....	48
	<b>Závěr .....</b>	<b>51</b>

## Seznam zkratek

AP	Access point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BPDU	Bridge Protocol Data Units
CLI	Command Line Interface - Příkazový řádek
DHCP	Dynamic Host Configuration Protocol
DP	Designated Port (pověřený port)
FTP	File Transfer Protocol
IP	Internet Protokol
ISO	International Organization for Standardization
ISP	Internet Service Provider
L2	Layer 2 (jedna z vrstev OSI normy)
L3	Layer 3
LAN	Local Area Network
MAC	Media access control address
MAN	Metropolita Area Network
NDP	Non-designated Port (nepověřený port)
OSI	Open Systems Interconnection
PVST	Per VLAN Spanning Tree
Rapid PVST	Rapid Per VLAN Spanning Tree
RB	RouterBoard
RP	Root Port (kořenový port)
RSTP	Rapid Spanning tree
SMTP	Simple Mail Transfer Protocol
STA	Spanning Tree Algorithm
STP	Spanning Tree Protocol
TCA	Topology Change Notification Acknowledgment (Potvrzení o změně topologie)
TCN	Topology Change Notification (Notifikace o změně topologie)
TTL	Time to live
UTF	Unicode Transformation Format
UTP	Unshielded Twisted Pair (nestíněná kroucená dvojlinka)
WAN	Wide Area network
WLAN	Wireless Local Area Network

## Seznam obrázků

Obrázek 1 - Ukázka sítí WAN, MAN a LAN.....	13
Obrázek 2 – Příklady topologií. (1) .....	14
Obrázek 3 – Topologie zapojení do kruhu.....	15
Obrázek 4 - Kruhová topologie, selhání prvků.....	16
Obrázek 5 - Stromová síť.....	17
Obrázek 6 - ilustrace OSI vrstev .....	18
Obrázek 7 - Rozdělení BPDU rámce .....	27
Obrázek 8 - Modelové zapojení centrálního prvku jako root bridge .....	30
Obrázek 9 - spouštěcí okno aplikace WinBox.....	33
Obrázek 10 - Hlavní nabídka WinBox .....	34
Obrázek 11 – Modelovaná topologie sítě .....	35
Obrázek 12 - Rychlé nastavení základních vlastností .....	36
Obrázek 13 - Interface - WLAN, nastavení bezdrátové sítě.....	37
Obrázek 14 - Konfigurace zabezpečení WLAN .....	38
Obrázek 15 – Vytvoření a nastavení nového bridge.....	39
Obrázek 16 - Bridge - Ports - výpis všech přidávaných portů.....	39
Obrázek 17 - Interface list obsahující veškeré porty .....	40
Obrázek 18 - Address list.....	41
Obrázek 19 - Nastavení rozsahu IP adres .....	42
Obrázek 20 - Nastavení DHCP Serveru .....	43
Obrázek 21 - konfigurace DHCP serveru .....	44
Obrázek 22 - výpis informací o síťovém adaptéru .....	44
Obrázek 23 - příkaz ping na koncové zařízení se zapnutým STP .....	45
Obrázek 24 - přepnutí bridge2 do stavu RSTP .....	46
Obrázek 25 - ping na koncové zařízení s přepnutím na RSTP .....	46
Obrázek 26 - Ukázka konfigurace v WebFigu .....	47
Obrázek 27 - Řešená síťová topologie Cisco.....	48

## Seznam tabulek

Tabulka 1 - dělení přenosových médií (9),(10) .....	22
---	----

## Úvod

Ačkoliv běžný uživatel internetu nemusí o síťové topologii a struktuře internetu vůbec nic vědět a je mu povětšinou lhostejné, jak se k němu dostávají data o webové stránce, vyjadřuje svojí vysokou nespokojenost, jestliže vyžádaná data nezíská v daném čase nebo ještě hůře, nezíská je vůbec. Připojení k internetu je ovlivněno jak vlastním zařízením, tak i některými aktivními síťovými prvky. Za jeho připojení uživatelů k internetu, odpovídá několik aktivních síťových prvků. Ať už hovoříme o počátečním směrovači, přepínači či serveru, na kterém jsou dostupné informace. Mezi počáteční a cílovou destinací je veliké množství různých prvků, které spojují tyto dva body, přes které putuje datový požadavek.

V moderních sítích je nutné řešit situaci, kdy je nějaký prvek nedostupný. Důvody pro nedostupnost prvku mohou být různé. Závada na přenosové soustavě či přímo na uzlu. Pro zajištění bezproblémového síťového provozu je obvyklé vytvářet zálohy v podobě redundantních spojů. Tyto spoje jsou využity, pokud jeden z prvků selže či nefunguje správně.

Aby bylo možné vytvářet záložní spoje, je nutné zavádět postupy, které předchází a zabraňují vytvoření smyček v síti. Právě smyčky, jsou častým neduhem vzniku duplicitních spojů, které dále vytvářejí nestabilitu sítě. Jedním z postupů, jak předcházet problémům je odstraňování smyček pomocí Spanning Tree Protocolu.

Řešení redundancí pomocí Spanning Tree Protocolu na jiných jak Cisco zařízeních není věnována příliš velká pozornost. Proto vznikla tato bakalářská práce, která si klade za cíl, porovnat nastavování STP pro platformu MikroTik a dále tuto problematiku přiblížit široké veřejnosti.

## 1 Počítačové sítě

Počítačové sítě vznikaly od poloviny dvacátého století. Prvním důvodem byla nutnost propojení jednotlivých sálových počítačů tak, aby bylo možné sdílení souborů a zasílání interních zpráv. V šedesátých letech byla tato snaha rozšířena o to, aby se využilo co nejvíce výpočetní kapacity mainframu.

Dalším z důvodů bylo vzdálené připojování terminálu, který tak získával přístup k datům, periferiím, ale také výpočetní kapacitě, což umožňovalo efektivnější využití procesoru sálového počítače.

Pro tyto účely byly sálové počítače propojovány do hvězdicové topologie, převážně využívající již existující telefonní přenosovou soustavu.

Všechny níže uvedené typy používají určité sady protokolů. Jasně definované protokoly fungující jako univerzální sada pravidel pro nakládání s přenášenými daty zaručují, že přenesená data nebudou znehodnocena a to bez ohledu na to, jaké protokoly byly použity pro přenos dat.

### 1.1 WAN

Wide Area Network je rozlehlá komunikační síť, která svým rozsahem pokrývá několiknásobně větší zeměpisnou plochu než LAN. Obvykle jsou tak označovány sítě, které překračují hranice měst, států či kontinentů. WAN spojuje jednotlivé LAN sítě do jednotné a navenek ucelené sítě, také nazývané Internetem. Aby bylo možné přenášet data na veliké vzdálenosti, tak technologie, která je použita ke spojování jednotlivých prvků ve WAN se odlišuje od technologií v LAN.

Některé WAN sítě jsou soukromé, jelikož mohou tvořit globální interní firemní systém, či jen spojovat jednotlivá datová centra, rozmístěná na různých lokacích. Jedním z příkladů může být i interní systém společnosti Vodafone nebo E.ON. Mnoho z nich je však budováno jako ISP (Internet Service Provider), které umožňuje připojení LAN do sítě internetu, aby bylo umožněno koncovému uživateli připojit se k síťovým prostředkům.

### 1.2 MAN

Metropolitní nebo také městskou můžeme označovat síť, která je rozmístěná v rozsahu města v řádu několika čtverečních kilometrů. Je velice podobná LAN, avšak ke vzájemnému spojení

jednotlivých prvků jsou využívány i veřejné komunikační sítě. Umožňují tak rozšíření LAN. Jedním z příkladů může být třeba i Pražská akademická počítačová síť PASNET.

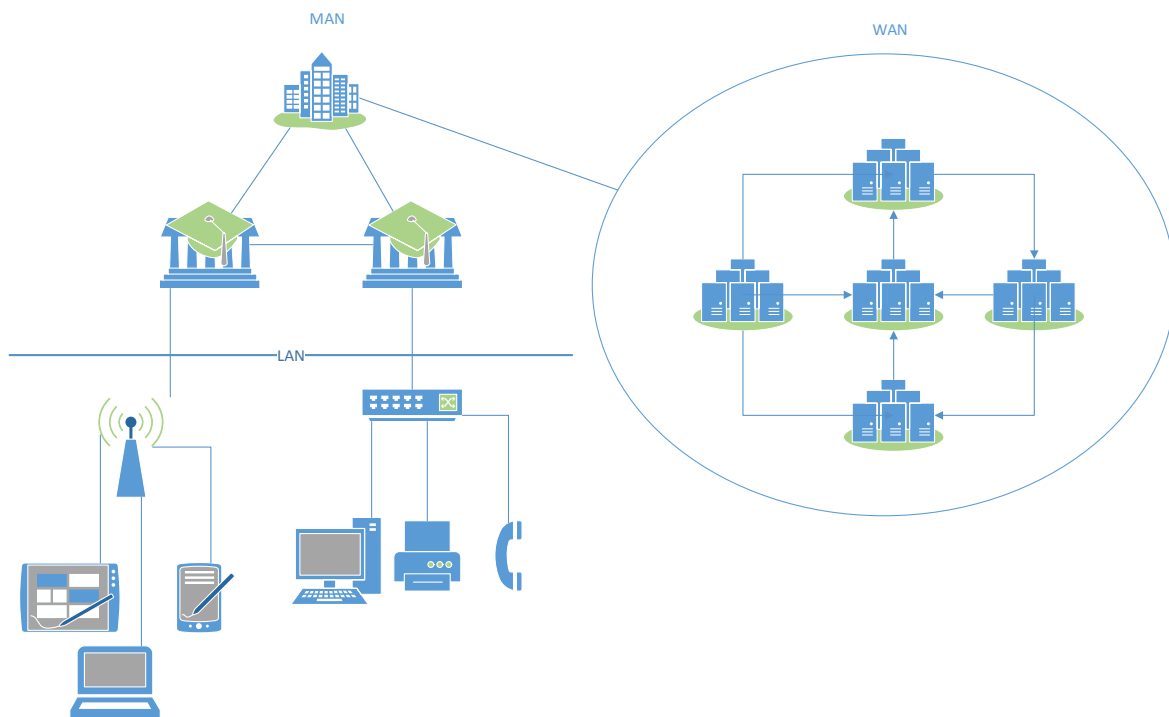
### 1.3 LAN

Lokální počítačová síť je ve většině případů budovou, rozkládající se maximálně na několika stovkách metrů čtverečních. Může se jednat o rodinný dům, malou firmu, školu nebo továrnu. Síť je obvykle zajišťována správcem sítě, který se stará o bezproblémový chod. Na rozsáhlejších místech, která vyžadují nepřetržitou funkčnost, je síť spravována hned několika síťovými administrátory, kteří však musí vzájemně plánovat a koordinovat svoji činnost.

Nasazení lokálních sítí umožňuje sdílení společných dat, které je nutné pro chod aplikace. To jsou například interní komunikace, sdílení tiskáren, případně NASu, jako zařízení pro zálohování a úložiště dat.

LAN je tvořena zpravidla z osobních počítačů propojených síťovými kabely a potřebnými síťovými prvky. Dříve používané koaxiální kabely byly již dávno nahrazeny kroucenou dvojlinkou (UTP) nebo místy i optickým kabelem. Výjimkou však ani nejsou často nasazované bezdrátové sítě, ať už z důvodu obtížné dostupnosti kabelu nebo jednoduššímu šíření sítě a internetu.

Následující obrázek č. 1 zachycuje všechny typy sítí. Síť WAN s mainframy, tvořící jakousi páteř sítě. Následně MAN, je příkladem sítě meziuniverzitní, kdy každá fakulta vlastní ještě svou síť lokální s různými síťovými prvky. (switche, AP).



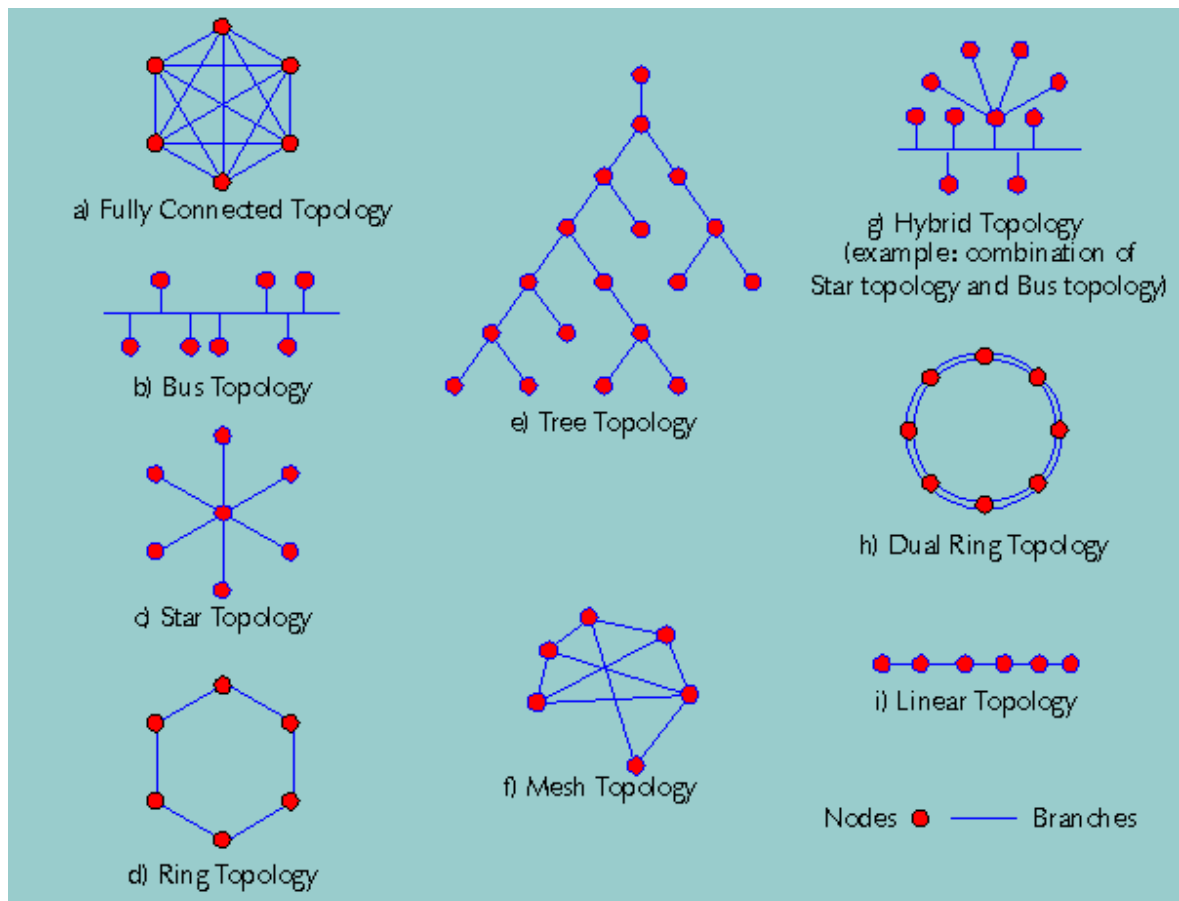
Obrázek 1 - Ukázka sítí WAN, MAN a LAN

## 2 Síťové topologie

Sběrnice, hvězda, kruh pro jediný segment sítě a při propojování segmentu se stává složitější – segment nebo smyčka.

Topologie je specifické fyzické reálné uspořádání prvků v síti. Například dvě sítě jsou stejné, jestliže mají stejnou konfiguraci. Ačkoliv skutečné zapojení jednotlivých prvků do sítě se může lišit vzdáleností mezi jednotlivými uzly nebo přenosovou rychlostí.

Příklady topologií jsou zobrazeny na obrázku č. 2.



Obrázek 2 – Příklady topologií. (1)

## 2.1 Fully Connected topology – Plně propojená topologie

Tato topologie znamená, že jsou všechny prvky zapojeny tak, že existuje přímá cesta k hledanému bodu, tzv. každý s každým. Porucha jakéhokoliv prvku nenaruší fungování celé sítě.

## 2.2 Bus topology – Sběrníková topologie

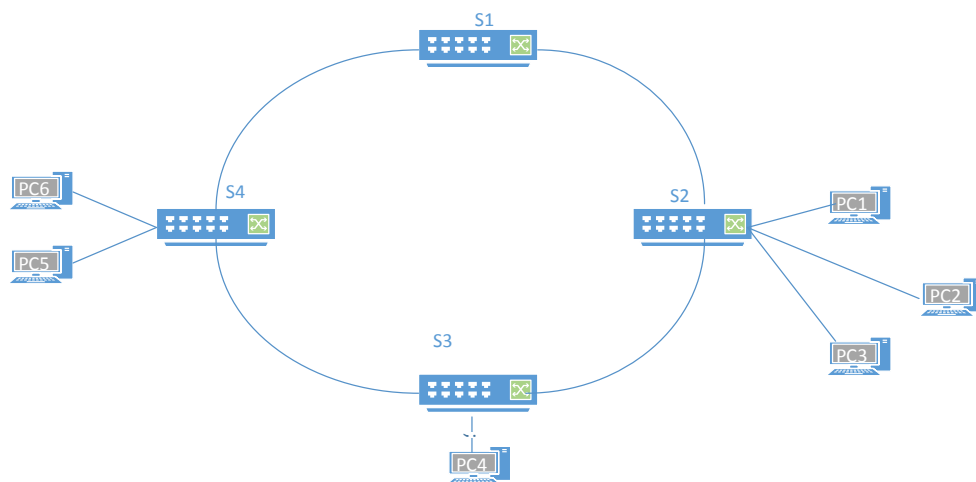
Jedná se o připojení, kde všechny prvky (stanice) jsou spojeny jedinou sdílenou linkou. Sběrníková topologie je dříve asi nejpoužívanější metodou zapojení. Jako přenosové médium byl používán koaxiální kabel, který však zajišťoval nízkou přenosovou rychlost. Hlavní nevýhodou tohoto typu zapojení jsou obvyklé kolize, kdy stanice neví, kdo a kdy bude vysílat. Při poruše sběrnice dojde k zasažení všech připojených uživatelů. Výhodou však jsou nízké pořizovací náklady a snadné všesměrové vysílání. (2)



## 2.3 Ring topology - Kruhová topologie

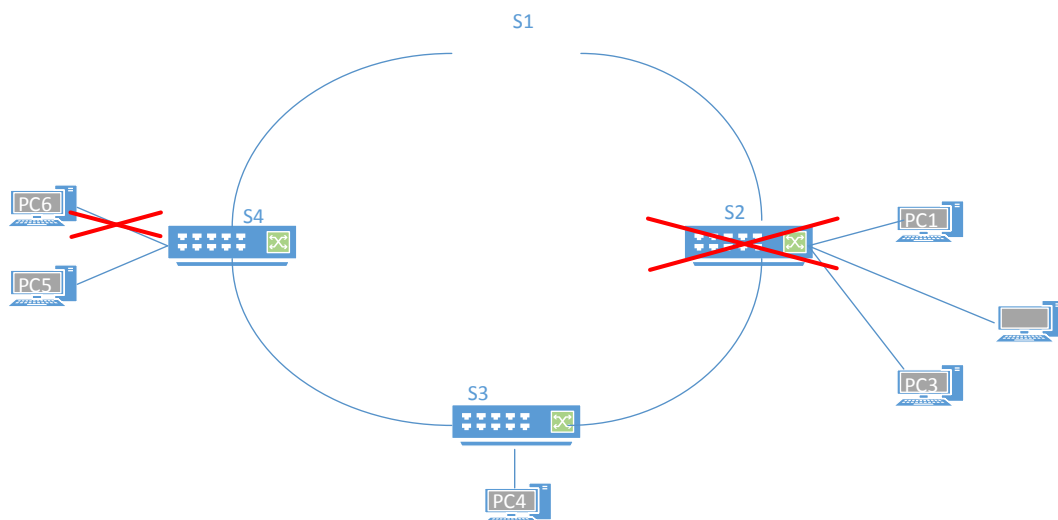
V lokální síti (LAN), kdy přepínače tvoří pomyslnou kružnici, je možné přenášet data jedním směrem, tato vlastnost sice zabraňuje vzniku smyček a přestože má několik výhod má i své nedostatky jako je nutnost projítí dat přes všechny zapojené prvky.

Na přiloženém obrázku vidíme ilustrační síť zapojenou do kruhové topologie. Nachází se zde čtyři propojené přepínače (Switch) a nějaké koncové zařízení.



**Obrázek 3 – Topologie zapojení do kruhu**

Informace v této síti na obrázku č. 3 se mohou posílat po směru hodinových ručiček nebo proti nim, nikdy však zároveň. Zprvu se může zdát, že se jedná o redundantní topologii, kdy je vždy nějakým způsobem možné se dostat z jedné strany na druhou. Jestliže, ale dojde k selhání přepínacího prvku S2, jak je vyobrazeno na obr. č. 4, nebude nijak možné přistoupit na koncová zařízení PC1 - 3 a fungování celé sítě bude ohroženo.



**Obrázek 4 - Kruhová topologie, selhání prvků**

Stejný případ nastane, když dojde k poruše spoje mezi přepínačem a konečným zařízením. Síť zcela redundantní není a může zde dojít k přerušení komunikace. Výhodou uvedeného zapojení je malý počet spojů a možnost snadného rozšiřování. (2)

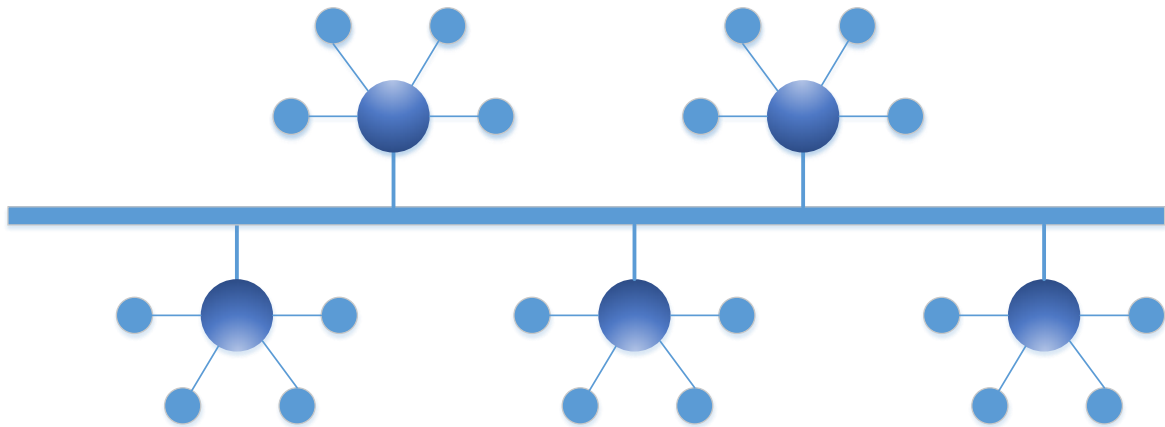
## 2.4 Star topology – Hvězdicová topologie

Toto je dnes asi nejčastěji užívané zapojení, jehož myšlenka spočívá ve vytvoření jakéhosi centrálního prvku, který všechny ostatní spojuje. Dříve se mohlo jednat o aktivní rozbočovač tzv. hub, který byl nahrazen směrovači.

Při poruše centrálního zařízení opět dojde k poruše a ztráty připojení všech připojených zařízení, ale výpadek koncového zařízení, nijak neovlivňuje chod celé sítě.

## 2.5 Tree topology – Stromová topologie

Stromová topologie sítě je ideální, když jsou pracovní stanice umístěny ve skupinách, přičemž každá skupina zabírá relativně malou oblast. Příkladem je univerzitní kampus, ve kterém každá budova má svou vlastní síť zapojenou do hvězdy a všechny centrální počítače jsou propojeny do systému školní sítě. Pak je snadné přidat nebo odebrat stanici z hvězdy. Celé hvězdy mohou být přidávány i odebírány ze sběrnice, obrázek č. 5.



**Obrázek 5 - Stromová síť**

Pokud sběrnice má nízké ztráty nebo je vybavena opakovači může být tato technologie použita také v široké síti WAN. Nevýhodou však zůstává, že dojde-li k výpadku uzlu, dojde také k odpojení dále připojených zařízení a ochromení fungování části sítě. Ostatní uzly a zařízení v síti však budou fungovat zcela normálně.

## **2.6 Hybrid topology - Hybridní topologie**

Hybridní topologie je počítačová síť, která využívá kombinace dvou a více topologií takovým způsobem, že výsledná síť nepřipomíná jednu ze standardních topologií používaných v počítačových sítích. Příkladem hybridní topologie může být hvězdicová a sběrnicová topologie nebo kruhová a hvězdicová síť. Použití hybridní topologie, umožňuje kombinování těch nejlepších částí ze standardních topologií.

## **3 Referenční model ISO/OSI**

V osmdesátých letech dvacátého století byl vypracován komunikační model International Standards Organization / Open System Interconnection Standard (Mezinárodní organizace pro normalizaci / propojení otevřených systémů), který měl standardizovat komunikaci v síti nezávisle na výrobcích.

Ve vrstvené architektuře se vzniklé zprávy vždy předávají nejnižší vrstvě, která zprávě nerozumí, ale má za úkol její doručení. Jelikož jsou vrstvy na sobě nezávislé, při změně protokolu na jedné z nich se změny nedotknou dalších vrstev.

Výsledkem těchto snah je sedmivrstvá architektura, která nestanovuje konkrétní protokoly, ale pouze vymezuje funkce. Jelikož nebyla jasně stanovená pravidla, vznikly problémy

s kompatibilitou jednotlivých verzí, které ústily k pomalému vývoji a zavádění standardů. Proto se OSI v praxi neprosadilo a zůstalo pouze jako obecný model. (3)

Některé funkce jsou obecné nebo případně doplněné další vrstvou, proto je možné je potkat v několika vrstvách. Například fragmentace dat nebo detekování a opravování chyb.



Obrázek 6 - ilustrace OSI vrstev

### 3.1 Physical layer - Fyzická vrstva

Tato vrstva specifikuje fyzickou komunikaci, aktivuje a udržuje a deaktivuje fyzické spojení s koncovým systémem. Spojení může být dvoubodové nebo vícebodové s podporou half<sup>1</sup> nebo full duplex<sup>2</sup>. Stanovuje způsob, jakým bude přenášen proud dat.

Hlavní funkce: navázání a uzavření spojení, oznamování chybových stavů spojové vrstvě, řazení značek, fyzický přenos bitů v zadaném pořadí. (4)

Zařízení pracující na fyzické vrstvě: hub, repeater.

### 3.2 Link layer - Spojová vrstva

Spojová vrstva vytváří, udržuje a ruší spojení mezi síťovými entitami.

Umožňuje kontrolu integrity dat, kterou provádí pomocí kontrolního součtu. V případě potřeby je vrstva schopna opravit chyby v přenosu. Adresace na spojové vrstvě funguje pomocí fyzických adres (MAC). Řadí data z fyzické vrstvy do logických celků (rámců).

Je reprezentovaná síťovou kartou. Vrstva typicky využívaná switchem a bridgem.

<sup>1</sup> Half duplex – komunikace oběma směry, ale pouze v daném okamžiku jen jedním směrem

<sup>2</sup> Full duplex – komunikace v obou směrech současně

### **3.3 Network layer - Síťová vrstva - dokument**

Odpovídá za doručování paketů<sup>3</sup> do protilehlé síťové vrstvy, při ztrátě paketu je síťová vrstva schopná vytvořit report o nedoručení zprávy. Jednou z vlastností síťové vrstvy je schopnost překlenout rozdílné chování jiných síťových technologií spojové i bez spojové. Zajišťuje přepravování paketů přes jednu nebo několik vzájemně propojených sítí. Vrstva, na které pracují routery, které jsou schopny směřovat pakety do jiných sítí s použitím IP. S pomocí protokolu ARP, provádí převod logické IP adresy na fyzickou adresu síťové karty. Další z vlastností je řízení síťového provozu. (5)

### **3.4 Transport layer - Transportní vrstva**

Na transportní vrstvě dochází opětovnému složení zprávy, zároveň zajišťuje předávání přejatých zpráv a jejich doručení do běžících procesů na daném zařízení.

Vrstva postavená mezi uživatele a síťovou infrastrukturou, vytvářející, udržující a ukončování transportních spojení. Zajišťuje výměnu dat mezi aplikacemi, schopná fragmentovat krátké zprávy do delších a naopak delší defragmentovat do menších celků. Oznamování chybových a neopravitelných stavů vyšším vrstvám. Kvalita služeb poskytovaných na relační vrstvě je závislá na požadavcích, při vytváření spojení, kdy se může klást důraz na dodržení maximální zpoždění či minimální propustnosti, po celou dobu trvání spojení.

### **3.5 Session layer - Relační vrstva**

Relační vrstva zajišťuje výměnu dat mezi aplikacemi. Stará se o udržování připojení (relace) a o korektní ukončení spojení, pakliže relace už není dále potřeba. Umožňuje pozdržení zpráv, kdy již odeslaná zpráva se doručí až po pokynu od odesílatele. Řízení dialogu (duplex, half-duplex).

### **3.6 Presentation layer - Prezentační vrstva**

Vznášení požadavku na relační vrstvu o vytvoření a zrušení relace. Řeší strukturu přenášených dat, jak je reprezentovat a jak je přenášet do aplikační vrstvy. Smyslem funkce je sjednocení způsobu prezentace přenášené zprávy pro aplikaci. Používá šifrování a kompresi dat. Používání textového kódování ASCII a UTF, kódování grafických dat JPEG a další.

---

<sup>3</sup> Paket - je blok informací přenášený v síti

### **3.7 Application layer - Aplikační vrstva**

Aplikační vrstva je koncový výstup pro uživatele, což znamená, že do aplikační a jako jediné vrstvy může zasahovat i uživatel, ne jako v předchozích případech, kdy je vše prováděno technickými prostředky. Domlouvá mechanické zabezpečení zprávy a synchronizaci aplikací. Vrstva určuje, jak mají být data posílána z a do aplikačních programů.

„Aplikační vrstvu může použít jakéhokoliv software, který je schopen využívat síťový přenos. Schopnost použití protokolů pro přenášení souborů (FTP), použití elektronické pošty (SMTP). Umožňuje identifikaci komunikujících a jejich verifikaci.“ (6)

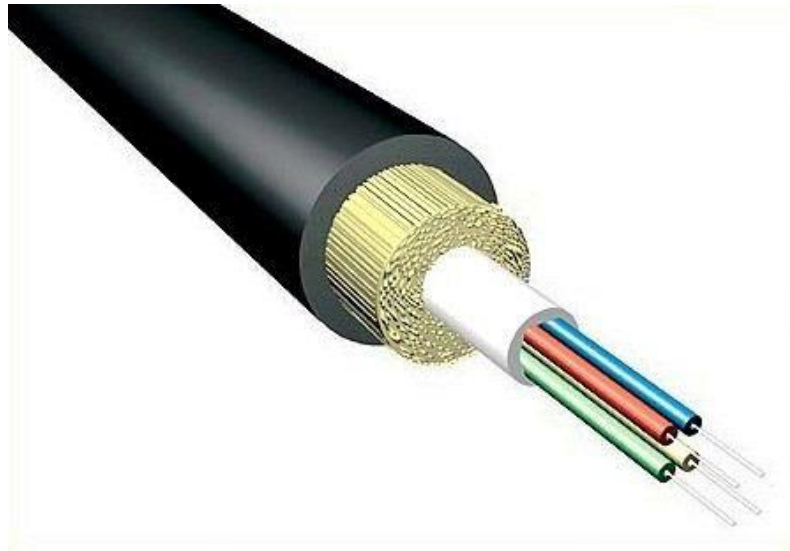
## **4 Komponenty v síti**

### **4.1 Přenosová media**

Pro vybrání správného propojovacího média, je nutné zvážit několik prvků. Prvním požadavkem je vzdálenost jednotlivých propojovaných prvků, odolnost proti rušení a na konec požadovaná rychlost. Zbývající požadavky už nemusí být tak důležité, nicméně jako další je třeba zvážit i pořizovací cenu média a jeho instalace.

#### **4.1.1 Optické kabely**

Nejnovějším přenosovým médiem, k přenosu informací je využíván světelný paprsek. Dříve byl využíván hlavně a skoro výlučně v páteřních sítích nebo velikých uzlech. Případně na místech, kde nesmělo dojít ke ztrátě informací následkem elektrického nebo magnetického rušení. Částečným důvodem pro nepoužívání optických kabelů nebyla jen cena, ale také horší manipulace a instalace. V dnešní době došlo k rozmachu optického kabelu, kdy na mnoha místech byl metalický kabel ponechán pouze jako náhradní médium v případě selhání optického kabelu obrázek č. 7.



**Obrázek č. 7 - Ilustrace optického kabelu (7)**

Optické kabely se dělí podle místa použití - venkovní, vnitřní, univerzální, speciální

Typu – multimode (do vzdálenosti 2 km), singlemode (vzdálenosti vyšší jak 2 km)

#### **Výhody optického kabelu:**

- přenos dat na větší vzdálenosti díky nízkému útlumu
- větší šířka pásma a vyšší rychlost – užití v páteřních spojích
- odolnost vůči elektrickému i magnetickému rušení
- nevyzařuje žádnou energii do svého okolí, a proto je odolnější i vůči odposlechu
- nepodléhá časové degradaci jako metalický kabel

#### **4.1.2 Metalické kabely**

Kroucená dvojlinka nahradila v devadesátých letech minulého století vytvořený koaxiální kabel, který sloužil jako dominantní přenosové médium. Důvodů pro ustoupení od koaxiálního kabelu bylo několik, ale tím nejdůležitějším byla již nedostačující přenosová rychlost, dosahující pouhých 10 Mbit/s. S metalickým kabelem a kroucenou dvojlinkou se přešlo ze sběrníkové na hvězdicovou topologii, která umožňuje strukturovanou kabeláž.

Kroucená dvojlinka je tvořena dvěma páry vodičů, které jsou pravidelně krouceny tak, aby se zlepšily elektrické vlastnosti kabelu. Kroucením kabelu je zajištěno snížení příjmu

elektromagnetického záření z okolí, ale i jeho vysílání, vyzařování potom neohrožuje ani jiné zařízení ani lidské zdraví.

„Dva vodiče, kterými je souběžně přenášen signál, se chovají jako anténa, která vyzařuje do svého okolí elektromagnetické vlny. V některých případech může být vyzařování nestíněné kroucené dvojlinky (UTP) stále příliš vysoké a tak je využíváno stíněné kroucené dvojlinky.“ (8)

**Tabulka 1 - dělení přenosových médií (9),(10)**

	forma přenášení signálu	Kategorie	standard	frekvence (GHz)	dosah	teoretická rychlost	
Bezdrátový přenos	elektromagnetické vlnění		802.11a	5	120m	1-2 Mbit/s	
				3.7	5000m	6-54 Mbit/s	
			802.11b	2.4	140m	1-11 Mbit/s	
			802.11g	2.4	140m	6-54 Mbit/s	
			802.11n	2.4, 5	250m	600 Mbit/s	
			802.11ac	5		433-1300 Mbit/s	
	802.11ad	60			až 6.8 Gb/s		
Optický kabel	světelné pulzy ve skleněném vlákne	multimode			2km	100 Mbit/s	
					600m	1 Gb/s	
		singlemode			300m	10 Gb/s	
					10km	100 Mbit/s	
Měděný kabel (UTP)	elektrické pulzy	Cat5	100BASE-TX		100m	100	Mbit/s
		Cat5e	1000Base-T		100m	1000	Mbit/s
		Cat6	10GBASE-T		55-100m	10	Gb/s

#### 4.1.3 Bezdrátový přenos

Bezdrátová lokální síť (WLAN), je síť v malé nebo omezené fyzické lokalitě, jako skupina lokálních sítí pod kontrolou jednoho administrativního prvku.

#### 4.2 Propojovací zařízení

Propojování sítí je zajišťováno několika prvky, některé z těchto prvků fungují na jiných fyzických vrstvách a tak i jinak s procházejícími daty pracují.

- **Gateway - Brána**



Zařízení, které bylo nahrazeno směrovačem, sloužilo jako místo, kde se potkávali dvě a více sítí pracujících na jiných protokolech. Aby tato konverze fungovala, pracuje brána na aplikační vrstvě, kde dokáže chápat strukturu přenášených dat a může tak správně interpretovat obsah. Příkladem může být posílání emailových zpráv ze sítě do sítě, kdy se zpráva může lišit v kódování zprávy nebo hlavičce.(11)

**default gateway** funguje jako výchozí brána do vnější sítě, v dnešní době je takto označován směrovač umožňující přístup do sítě internet.

- **Bridge - Most**

Zařízení pracující na linkové vrstvě, je tak schopné rozlišit, jaká data přijalo a do jakého segmentu sítě jsou data určena. Most data přijme, zpracuje a rozhodne, zda data patří do jeho segmentu sítě nebo jestli je potřeba je dále přeposlat na jiný směrovač. Díky této vlastnosti je bridge schopný redukovat provoz na síti, protože data, která nejsou určena do jeho sítě, nejsou dále přeposílána na všechny porty tak, jak to je u hubu. Jednotlivé sítě a uzly jsou objevovány právě při příchodu rámce na most, který je schopen naučit se celou topologii sítě.

- **Repeater - Opakovač**

Jelikož u kroucené dvojlinky dochází k útlumu signálu, činí maximální dosah kabelu 100 m. Pokud tedy bylo nutné, aby signál byl dopraven na delší vzdálenost, bylo nutné vytvořit aktivní síťový prvek pracující na fyzické vrstvě, jehož hlavní úlohou je regenerace a zesilování signálu. Je tak možné zvětšit dosah bez obavy o ztrátu dat. (11)

- **Switch - Přepínač**

Hlavní výhodou na rozdíl od hubu, který byl switchem nahrazen, bylo mimo jiné i to, že byl schopen využívat kompletní šířku pásma na všech portech, čehož hub, který šířku pásma na všech portech dělil, nebyl schopný. Switch je schopný lépe zvládat různé rychlosti sítě, takže dvě rychlejší zařízení komunikující 100BaseT<sup>4</sup>, mohou

---

<sup>4</sup> 100Base-T - Jako přenosové vodič je použita stíněná nebo nestíněná dvojlinka kategorie minimálně Cat5. Je to varianta vhodná pro starší rozvody strukturované kabeláže. (12)

spolu komunikovat vyšší rychlostí, i když zároveň musí komunikovat s pomalejšími zařízeními 10Base-T<sup>5</sup>. (13)

Ethernetové switche byly běžně používány v domácích sítích, než byly nahrazeny stále populárnějšími routery.

Tradiční switche podporují až rychlost 1Gbps, ale vysoce výkonné přepínače v datových centrech obecně podporují rychlosti do až 10 GB. Vysoce výkonné síťové přepínače jsou ještě široce používány v podnikových sítích a datových centrech. Různé modely mají různé počty portů a tak v klasických spotřebních přepínačích můžeme nalézt pouze od 4 do 8 portů na rozdíl od již zmíněných firemních, podporujících 32-128 přípojek.

- **Hub - Rozbočovač**

Rozbočovač funguje podobně jako repeater, je to propojovací zařízení, které aktualizuje a zesiluje signál, kterým následně zaplavuje všechny své porty, kromě portu, ze kterého byl signál obdržen. Obvykle jako centrální prvek ostatních zařízení, připojených kabelem do hvězdicové topologie. Nevýhodou hubu je právě neustálé rozesílání dat na všechny porty, kdy případný odposlech sítě je poměrně jednoduchý, jelikož všechny stanice v síti přijímají veškerá data procházející přes hub. Udržuje také veliké množství kolizních domén.

**Kolizní doména** – je část sítě, ve které je skupina zařízení připojena do stejné sítě a je připojena přes sdílené médium. V této části může dojít ke kolizi z důvodu současného vysílání několika zařízení najednou. Z části byl tento problém eliminován vznikem kroucené dvojlinky, kde je možné vytvářet jen dvojbodové spoje bez odboček. Problém byl finálně dořešen nahrazením hubů - switchem, kdy pro každé rozhraní vytváří switch vlastní kolizní doménu. (14)

- **Router - Směrovač**

„Jeho hlavní úlohou je směrování, tedy nalezení optimální cesty, ale stejně jako bridge má i router za úkol spojovat jednotlivé segmenty sítě. Na rozdíl od něj však pracuje na síťové vrstvě. Router tak už není v síťové topologii transparentní a jednotlivé

---

<sup>5</sup> 10Base-T – Používá jako přenosové médium kroucný dvoudrát s rychlostí 10 Mbit/s minimálně Cat3.

stanice o existenci směrovače ví. Směrovač uchovává routovací tabulku, která obsahuje nejlepší cesty“. (15)

Pokud datový paket přijde z jedné z linek, router přečte informace o adrese v paketu k určení jeho konečného určení. Potom s použitím informací ve své směrovací tabulce směruje paket do další sítě, kam náleží.

V domácnostech nebo malých firmách najdeme jednoduché routery, které mají za úkol přeposílat data, jako jsou webové stránky nebo maily, mezi jednotlivými počítači a internetem. Ve větších firmách, je nutné provozovat o něco sofistikovanější zařízení, které zvládají více požadavků v kratším čase, případně zvládnou spojení optickým kabelem na páteřní síť. (16)

## 5 Spanning Tree Protocol

### 5.1 Redundance v síti

Pojem v síťové terminologii určuje a definuje schopnost, kdy se síť musí přizpůsobit situaci, ve které došlo k nějaké závadě na vedení, tak aby byla schopna dále fungovat. Fungující počítačová síť je dnes nezbytná pro práci skoro v každé firmě. Je jasné, že není možné, aby došlo ke ztrátě spojení mezi bankami a burzami, kde probíhá neustálá komunikace. Nejde však pouze o ztráty finanční, ale i o ztráty na lidském životě, třeba při přerušení komunikace mezi pilotem letadla a řídicí věží, jestliže by některý mezičlánek přestal fungovat. Proto začaly na síti vznikat záložní spoje mezi aktivními prvky (switchem a routerem), pro případ, že by došlo k nějaké neočekávané situaci, jako je selhání celého prvku nebo jen závady na vedení.

S redundantním propojováním, ale došlo ke vzniku cyklů, již na druhé síťové vrstvě. V rozsáhlé síti není nemožné, že by nedošlo, k chybě lidského faktoru a tak i místo připojení dvou switchů, může dojít připojení stejného zařízení dvakrát. U velikých rozvodných a páteřních mnoha portových switchů může dojít ke zmíněné chybě, která se špatně odstraňuje.

## 5.2 Problémy spojené s výskytem smyček

Jelikož rámec nedisponuje ničím jako je TTL<sup>6</sup> u paketu na třetí vrstvě, může se stát, že rámec koluje v síti nekonečně dlouho nebo tak dlouho, než je síť zahlcena. Z principu switchu, který funguje tak, že přijatý rámec vezme a odešle na všechny své porty, kromě toho, z něhož rámec obdržel. Největším problémem takovéto sítě jsou broadcastové bouře, které jsou schopné zahltit přepínače.

K posílání do všech segmentů na L2 vrstvě se používají multicastové a broadcastové vysílání. Broadcastové vysílání je vysílání, které je určeno všem "naslouchajícím", na takové vysílání reaguje každá síťová karta nebo zařízení. Multicastové vysílání je určeno pro skupinu hostitelů. V případě, že je v síti smyčka, broadcastový provoz zamoří síť tak, že nezbyde žádné místo pro přenos dat z aplikací. (17)

Může dojít také k nestabilitě tabulky MAC adres, kdy stejná zpráva přijde na více portů přepínače, který mění neustále místo, odkud si myslí, že byla zpráva vyslána. (18)

## 5.3 Popis technologie STP

Spanning Tree protokol definovaný normou IEEE 802.1d běží na druhé síťové vrstvě, a to na stejné jako přepínače a mosty. Hlavním cílem je zajistit, že se nebudou vytvářet smyčky, které vznikají redundantním zapojením.

Aby bylo možné zajistit požadovanou redundanci a zároveň bylo zabráněno vzniku cyklů, definuje STP strom, který obsahuje veškeré přepínače v síti. STP přepíná určité redundantní spoje do stavu standby (blokovaný) a další cesty nechává ve stavu forwarding (přeposílající). Pokud port, který byl ve stavu forwarding, přestane být k dispozici, STP změní konfiguraci sítě a přesměruje datové cesty prostřednictvím aktivace příslušné záložní cesty, která byla doposud v blokovaném režimu.

Blokovaný spoj nepřenáší data, ale zprávy BPDU, které obsahují informace o portech, adresách, cenách a zajišťuje, že data skončí tam, kde bylo zamýšleno.

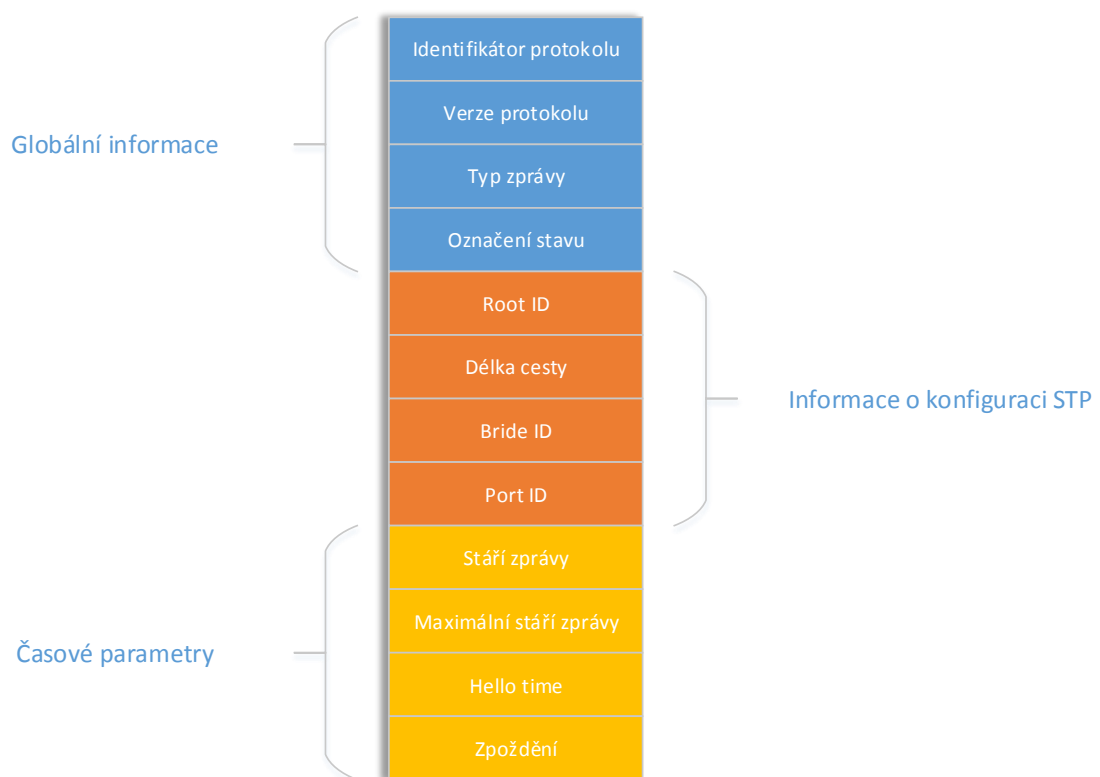
BPDU zprávy jsou předávány přes mosty pro detekci smyček v síti. V případě výpadku nebo nedostupnosti existující cesty, přepočítá STP cestu tak, aby vypadlé spojení bylo nahrazeno za jiné a byla obnovena funkčnost sítě.

---

<sup>6</sup> TTL – číslo omezující počet průchodů přes prvky a tak omezuje platnost zprávy v síti

## 5.4 BPDU

Pro interní komunikaci mezi přepínači jsou využívány BPDU zprávy. Přestože blokové porty nejsou schopny zpracovávat data, BPDU zprávy však ano. Při prvním zapnutí se vyšle konfigurační BPDU a následně při každé změně už topologie nebo nastavení STP se zašle TCN BPDU jehož příjem je potvrzen Topology Change Notification Acknowledgment (TCA). Jelikož STP pracuje na druhé síťové vrstvě, směrují se BPDU zprávy podle MAC adresy portu. Jestliže rámec BPDU dojde na zařízení, pro které není určeno, rámec není dále přeposílán, ale je zahozen. Rámce jsou pak odesílány na společnou multicastovou adresu 01:80:C2:00:00:00.



Obrázek 7 - Rozdělení BPDU rámce

Ve třetí části BPDU rámce se nachází časové parametry, které je nutné splnit proto, aby se mohlo přejít z blokového stavu do forwarding, obrázek č. 7.

- **Hello time** – označuje, jak často jsou rozepisovány BPDU rámce. Defaultně 2s s možností nastavit až na 10 s.
- **Zpoždění - Forward delay** – určuje, jak dlouho se čeká na zprávu, tedy jak dlouho má port zůstat ve stavu listening nebo learning. Defaultně 15 s, ale možné nastavit čekání až do 30 s.

- **Maximální stáří zprávy - Maximum age** – stanovuje maximální stáří BPDU zprávy, které je uchované na přepínači.

## 5.5 Volba root bridge

Předtím než začneme konfigurovat STP, je dobré si vybrat kořenový přepínač. Nemusí se jednat o ten nejlepší, ale je lepší vybrat nejvíce centralizovaný switch v síti. Switche v páteřních sítích, bývají často voleny za root bridge, jelikož tyto přepínače nejsou běžně propojeny ke koncovým stanicím a tak pohyby a změny v sítích neovlivňují chody těchto páteřních přepínačů. Aby bylo možné určit, který switch bude fungovat jako root bridge, je nutné změnit bridge priority. Každý přepínač má nastavenou nějakou vlastní prioritu a v případě, že nebyla administrátorem upravena, disponuje defaultní.

Jakmile se potkají dvě defaultní priority, dojde ke změně chování při rozhodování, který ze zařízení bude nastaven jako root bridge. V takové situaci se rozhoduje na základě fyzické adresy zařízení. Rozhodování na základě MAC adresy není ideální, jelikož problém, který ze switchů bude zvolen za root bridge je sice vyřešen, ale výsledná hodnota není předvídatelná a při přidání nového switchu může způsobit změnu root bridge.

Při zapnutí přepínačů se každý přepínač považuje jako root bridge a jakmile dojde k připojení nebo aktivování linek mezi přepínači, je vyslán BPDU rámec s oznámením nového kořenového mostu. Přepínač, který obdrží rámec, porovná, zda jeho Bridge ID je vyšší než obdržené root ID. V případě, že se opravdu jedná o vyšší číslo, uzná sousední přepínač jako kořenový a aktualizuje svoje BPDU, i když se vůbec nemusí jednat o skutečně nejnižší prioritu switchu zapojeného do sítě. V opačném případě, jestliže bude obdrženo číslo vyšší, pak sousední přepínač uznán jako root bridge nebude.

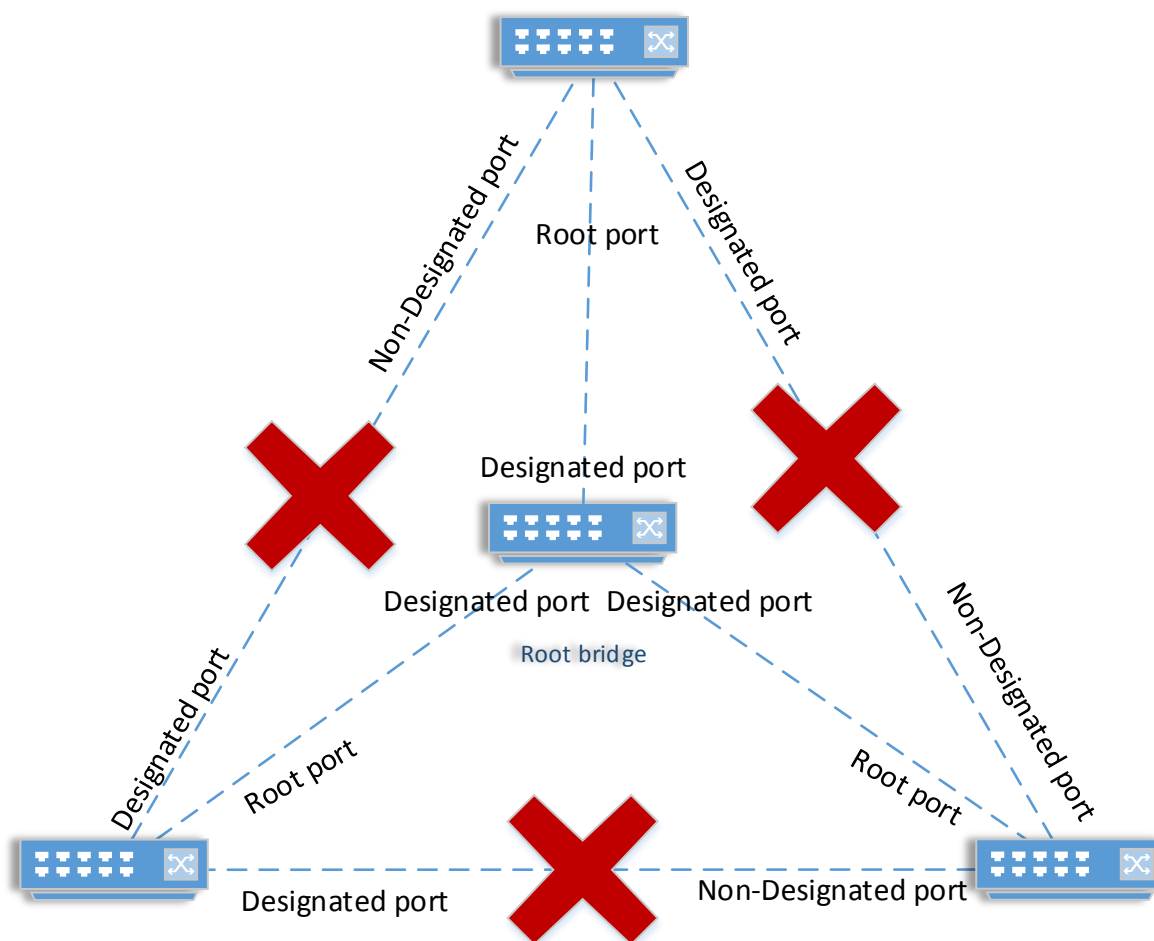
## 5.6 ST Algoritmus - Spanning Tree Algorithm

Jakmile je zvolen root bridge, začne algoritmus počítat nejlepší cesty od každého switchu ke kořenovému mostu. Činí tak na základě počítání nejkratší cesty, kde se zaznamenává každý průchod přes jednotlivé porty na cestě. Jestliže algoritmus narazí na existenci několika cest ke stejnému cíli, vybere si tu nejkratší. Po skončení počítání cest, přidělí algoritmus jednotlivým portům jejich funkci.

Všechna ostatní rozhodnutí v síti, jako je to, který port zablokovat a který port přepnout do režimu přeposílání, jsou činěna z perspektivy root bridge.

- Funkce jednotlivých portů:
- **Designated port** – jsou porty na kterých je povoleno přenášet data. V každém segmentu může být pouze jeden takový nebo jeden root port, všechny zbývající jsou branné jako záložní a musí být označeny jako NDP.
- **Non-Designated port** – je alternativní, zablokovaný port schopný přijímat pouze BPDU rámce, využíváný pro přerušování cyklů. Neobsahuje nejkratší cestu ke kořenovému přepínači.
- **Root port** – na switchi se může jednat o pouze jedinou cestu. Jde o cestu, která je nejlepší nebo nejkratší k root bridgi
- **Disabled port** – je vypnutý nebo odpojený port. (19)

Během činnosti STP algoritmu, je veškerý provoz na síti kromě BPDU rámců pozastaven, do té doby dokud nedojde k plné konvergenci na síti.



**Obrázek 8 - Modelové zapojení centrálního prvku jako root bridge**

Na obrázku č. 8 bylo vytvořené modelové schéma, kde jako kořenový prvek byl zvolen switch umístěný do středu topologie. Z root bridge vychází tři linky, jelikož všechny tři linky, jsou přímo připojeny na kořenový prvek, stanou se z těchto portů pověřené porty pro zbývajících switchů. Root porty a designated porty jsou přepnuty do režimu forwarding a porty, které nejsou ani kořenové nebo pověřené jsou označeny jako blokované. V takové chvíli dojde ke konvergenci sítě, jelikož se už nemůže stát, že by v síti vznikla smyčka.

Kdyby z jakéhokoliv důvodu blokováný port přestal dostávat BPDU aktualizace, které jsou v defaultním nastavení zasílány po 20 s, začal by se proces, který by odblokoval port a přepnul by ho na forwarding. Mnohokrát STA selže jen proto, že se BPDU v síti ztratí a není doručeno, což způsobí přepínání portu do stavu forwarding.



Některé ze situací, kdy ztráta BPDU rámce způsobí, že blokový port se přepne do forwarding může být porušený paket, softwarová chyba, špatně nastavené STP, nesoulad v nastavení duplexu (full, half duplex).

## 5.7 Stavy portů

Ke konvergenci počítačové sítě dojde, jakmile jsou všechny porty přepnuté buď do stavu blokový nebo přeposílající. Po startu nebo zapojení linky by mohlo dojít k vytvoření smyčky, proto musí každý port projít všemi stavy, než dojde k finální konvergenci. Mezi každým přechodem je určitý časový interval, což znamená, že při úpravě síťové topologie nějakou dobu trvá, než se síť přizpůsobí a bude schopná plné funkčnosti. Při zaznamenání změny topologie, je port automaticky přepnut na naslouchání.

- **Blokující - Blocking** – schopný zpracovávat BPDU zprávy, ale nic nevysílá.
- **Naslouchací - Listening** – posílá a přijímá BPDU.
- **Přeposílající - Forwarding** – plně fungující port, který dokáže zpracovat jak uživatelské zprávy, ale je schopen je i dále předávat. Pracuje s BPDU.
- **Vypnutý** – port, který nebyl správcem sítě zapnut.

## 5.8 STP detekce změny topologie

Jakmile dojde ke změně topologie, v důsledku výpadku linky nebo závady na aktivním prvku, detekuje připojený switch problém a zašle upozornění kořenovému mostu, který přijatou informaci o nedostupnosti prvku rozešle do sítě. Pro upozornění na změnu v topologii se využívá BPDU TCN. Switch, který zaznamenal nedostupnost jiného prvku, odešle TCN na svůj root port. Po obdržení TCN zprávy kořenovým prvkem, je zaslána informace, kterou si prvky postupně mezi sebou předávají, dokud nedorazí informace o změně topologie do celé sítě.

## 5.9 Varianty STP

Od zavedení a standardizování STP uběhlo několik let a tak klasické STP začalo být vylepšováno a postupně nahrazováno jeho variantami.

**Per-VLAN Spanning Tree (PVST)** udržuje Spanning tree pro každou konfigurovanou VLAN v síti. Vzhledem k tomu, PVST se chová ke každé VLAN jako k samostatné síti, má schopnost vyvažovat provoz na druhé vrstvě tak, že předává některé VLAN po jedné lince jiné VLAN na jiné, aniž by došlo k vzniku smyčky.

**Rapid Spanning Tree Protocol (RSTP)** zaveden normou IEEE 802.1w, funguje jako vylepšený standart 802.1d. Většina parametrů zůstala nezměněna, takže přechod z STP na RSTP je poměrně rychlý a snadný. RSTP může dosáhnout mnohem rychlejší konvergence ve správně nakonfigurované síti, někdy v řádu několika stovek milisekund.

**Rapid PVST** zavádí pro každou VLAN RSTP, zaveden s příchodem normy IEEE 802.1w. Schopný komunikovat i s přepínači, které pracují na starém STP protokolu. (20)

## 6 Představení platformy MikroTik

V roce 1995 byla v Lotyšsku založena společnost MikroTik, jejímž cílem bylo navrhování routerů a ISP systémů. V roce 2002 navázala na svoje úspěchy zahájením výroby RouterBOARD s vlastním RouterOS. MikroTik OS

Díky zkušenostem získaným při vývoji si společnost MikroTik uvědomovala potenciál vzniku nového prostředí pro konfiguraci routerů. Proto se v roce 1997 rozhodla vytvořit vlastní systém tzv. RouterOS, který je v různých modifikacích dnešní doby používán.[MIKROTIK. *About us*. 2013. Dostupné z: <http://www.mikrotik.com/aboutus>]

]

Jeho obliba i u koncových zákazníků je poměrně logická. Systém je postavený na linuxové distribuci, který je možný konfigurovat přes několik rozhraní. Jedná se o systém robustní, rychlý, ale hlavně přehledný. Je možné použít GUI pro nakonfigurování základní sítě, není třeba znát množství příkazů, ale stačí si „naklikat“ co je potřeba. Pro konfiguraci v GUI je možné použít WinBox nebo WebFig. RouterBOARD je však možné připojit přes konzoli.

### 6.1 Možnosti konfigurace RouterBoardu

Nejvíce využívanou vlastností je samozřejmě směrování. Další z možností je omezení šířky pásma, vytvoření bezdrátového přístupového bodu, ověřování klientů či možnost skriptování. Užitečné je také instalování jednotlivých modulů, které rozšiřují vlastnosti MikroTiku.

Příkladem takových modulů může být Calea, která je povinná v USA, za účelem sledování a logování síťového provozu.

## 6.2 První zapnutí routeru

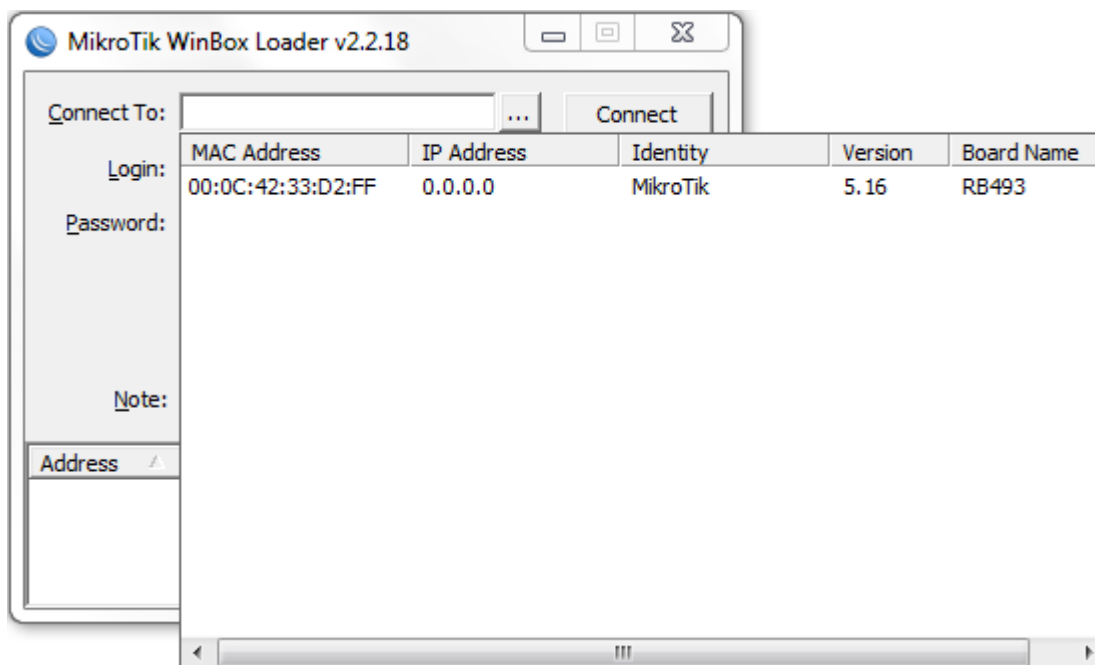
Jak již bylo zmíněno, existuje několik cest, jak se připojit k novému zařízení. K takovému zařízení můžeme přistoupit, pomocí CLI (konzole) přes Telnet, SSH nebo sériový kabel. Přístup je možný pomocí grafického rozhraní v prohlížeči tzv. WebFig nebo můžeme použít aplikaci přímo k tomu určenou, to je WinBox.

„Každý router má ve výchozím nastavení na prvním portu nastavenou adresu 192.168.88.1/24. Tedy při připojování používáme adresu 192.168.88.1:9999.“(22)

„Nekonfigurovaný MikroTik, používá jako uživatelské jméno: **Admin** a heslo zůstává nevyplněno.“ (23)

## 6.3 Představení aplikace WinBox

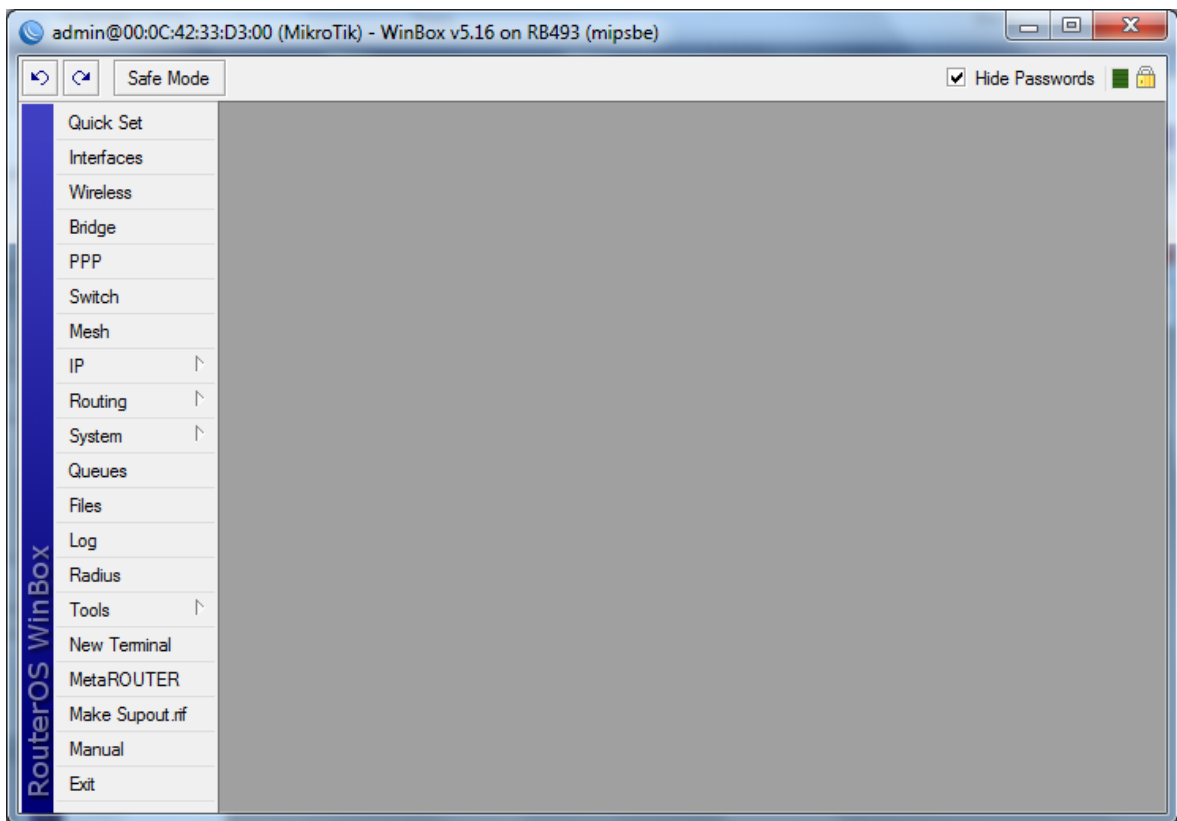
WinBox slouží jako aplikace, která je schopna se připojit na RouterBoard s užitím MAC nebo IP adresy.



Obrázek 9 - spouštěcí okno aplikace WinBox

Jestliže je zařízení poprvé spouštěno a není známa ani IP nebo MAC adresa, je zde možnost kliknout na tři tečky, které zobrazí podokno obsahující výpis připojených zařízení. Po kliknutí na MAC adresu a potvrzením stisknutím tlačítka *Connect*, dojde k připojení.

Jakmile dojde k úspěšnému připojení, otevře se nové okno, odkud je již dále možné konfigurovat jednotlivé požadované vlastnosti.



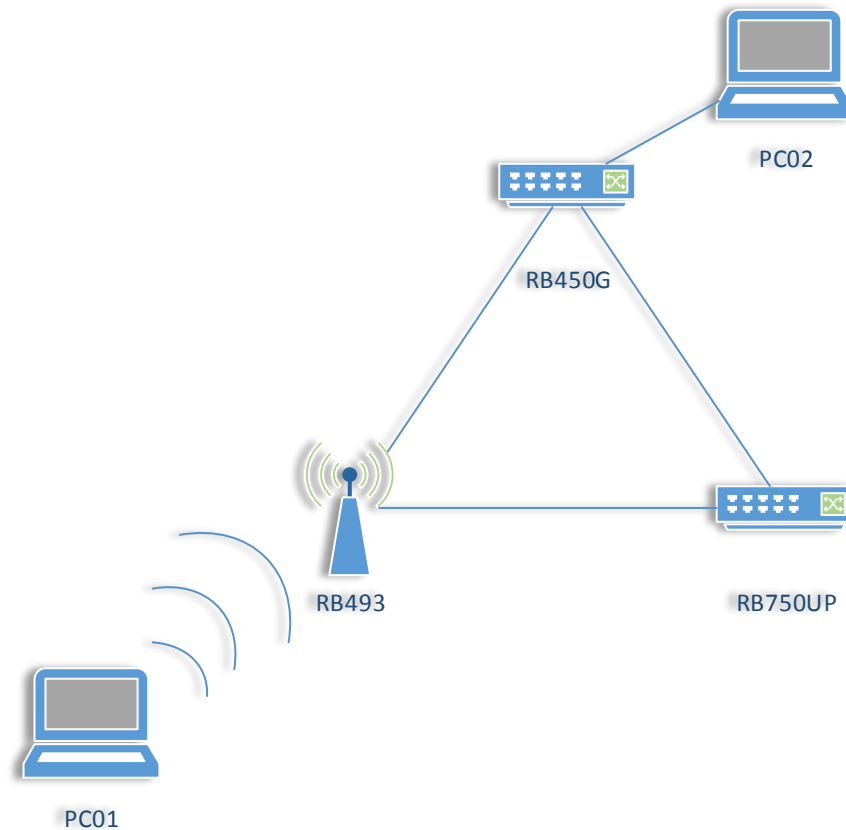
**Obrázek 10 - Hlavní nabídka WinBox**

V horní liště jsou vypsané informace o zařízení obrázek č. 10. Jméno připojeného uživatele - admin, fyzická nebo IP adresa, ID routeru (MikroTik) a verze instalovaného RouterOS 5.16. Posledním prvkem v horní liště je typ RouterBoardu v tomto případě RB493.

Dále je vidět konfigurační menu, tlačítka pro možnost vrácení se o krok zpátky i postup dopředu.

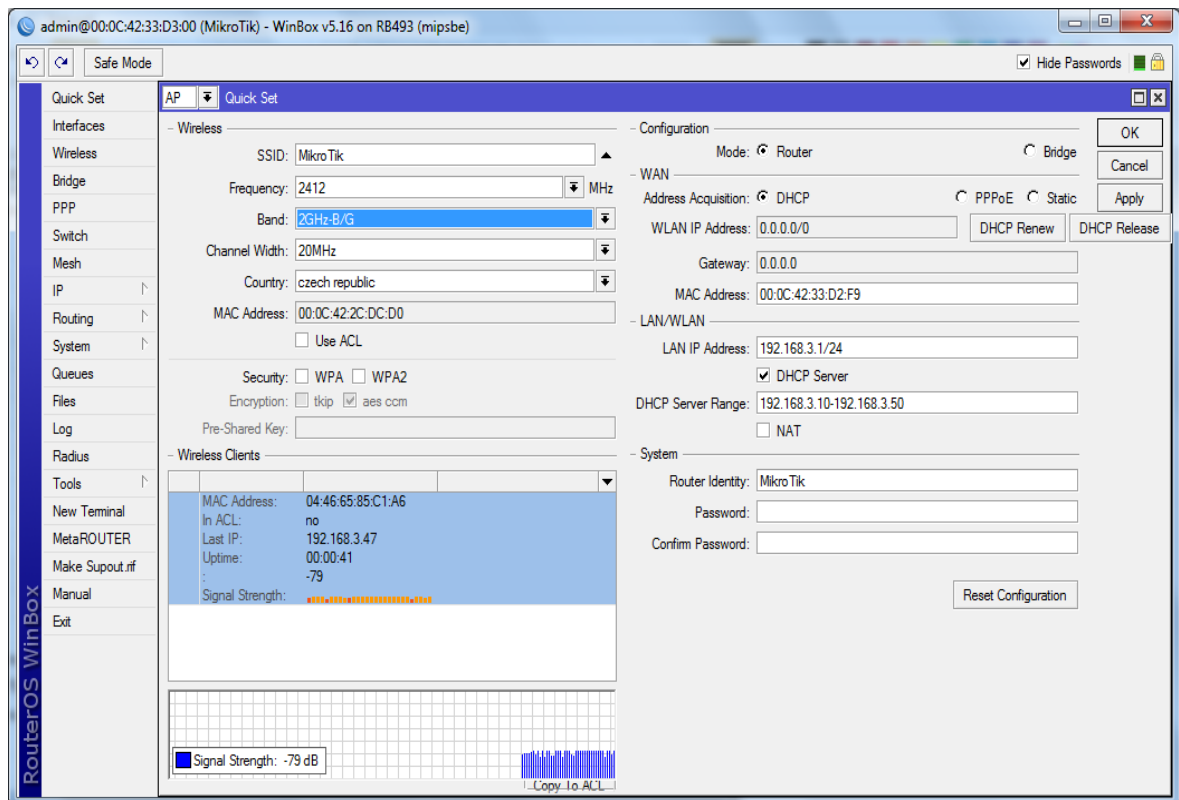
## 7 Konfigurace STP na platformě MikroTik

V první chvíli je důležité se rozhodnout, jak daná topologie sítě bude vypadat. Jelikož měl autor k dispozici tři RouterBoardy, zvolil jejich propojení do trojúhelníku. Autor si dal za cíl práce, vytvořit jeden RB, který bude sloužit jako AP a vysílat bezdrátovou síť, na které je zapojeno jedno z koncových zařízení. Zbývající zařízení, byly propojeny do smyčky a k jednomu z nich bylo připojeno druhé koncové zařízení.



Obrázek 11 – Modelovaná topologie sítě

V tomto momentu, kdy bylo rozhodnuto o výsledné podobě topologie, obrázek č. 11, jednotlivé prvky byly propojeny a bylo rozhodnuto o konfiguraci přes WinBox,



Obrázek 12 - Rychlé nastavení základních vlastností

Na obrázku č. 12 je základní nastavení bezdrátové sítě:

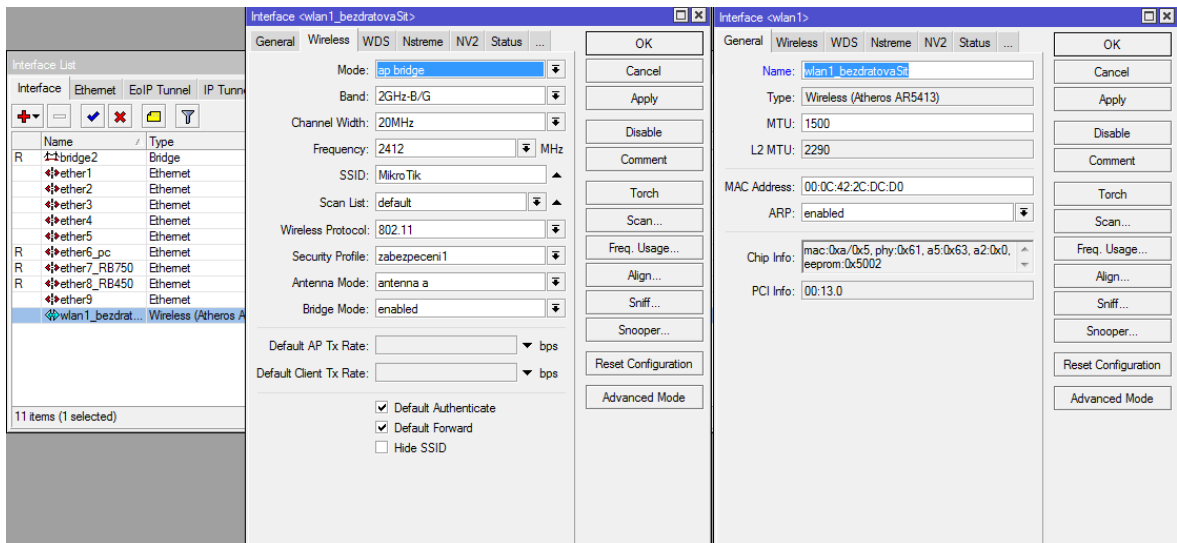
**SSID** – název sítě

**Band** – pásmo, na kterém je síť vysílána

**LAN/WAN** - fyzická adresa RB

**DHCP Server Range** – nastavení rozsahu, který bude použit při rozdávání adres DHCP.

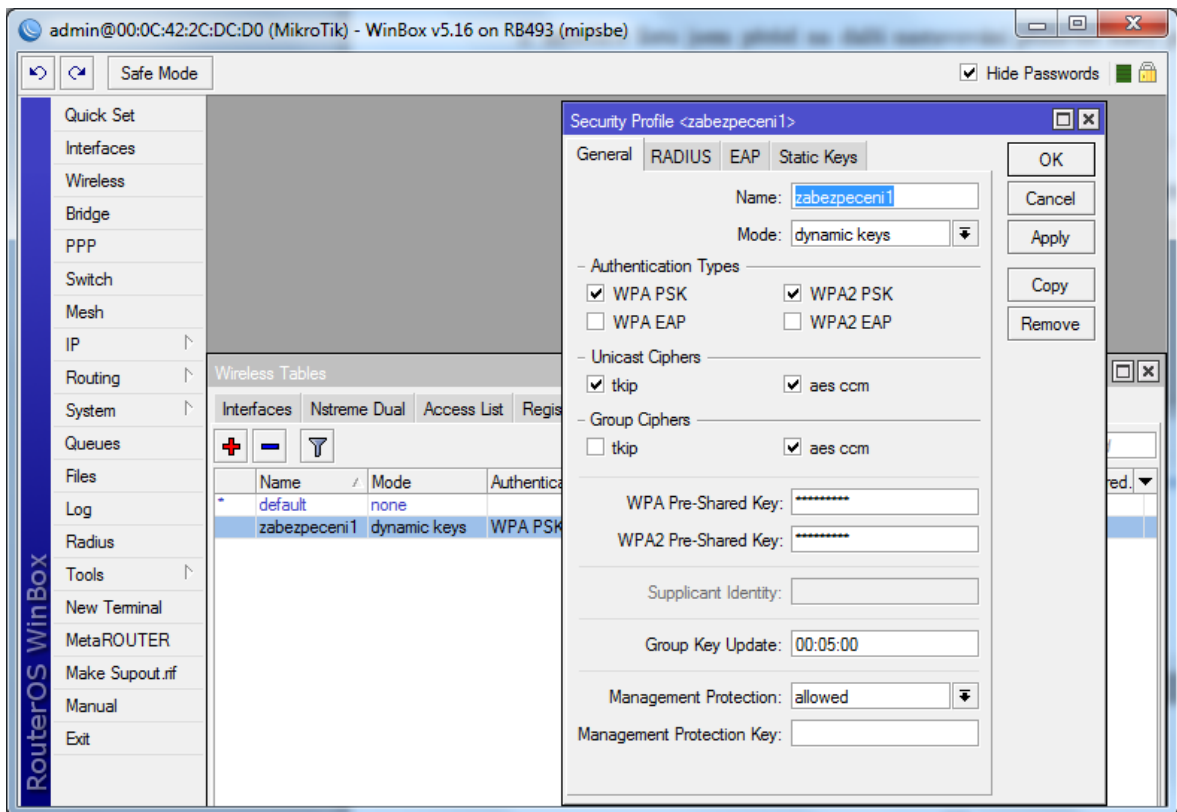
## 7.1 Doplnující konfigurace WLAN



Obrázek 13 - Interface - WLAN, nastavení bezdrátové sítě

Z interface listu autor přešel na další nastavování přídatné karty pro bezdrátový přenos. Kde doplnil jméno pro rozhraní a nastavil security profil, obrázek č. 13 a 14.

Vlastní nastavení security profile bylo provedeno po rozkliknutí Wireless - Security Profiles



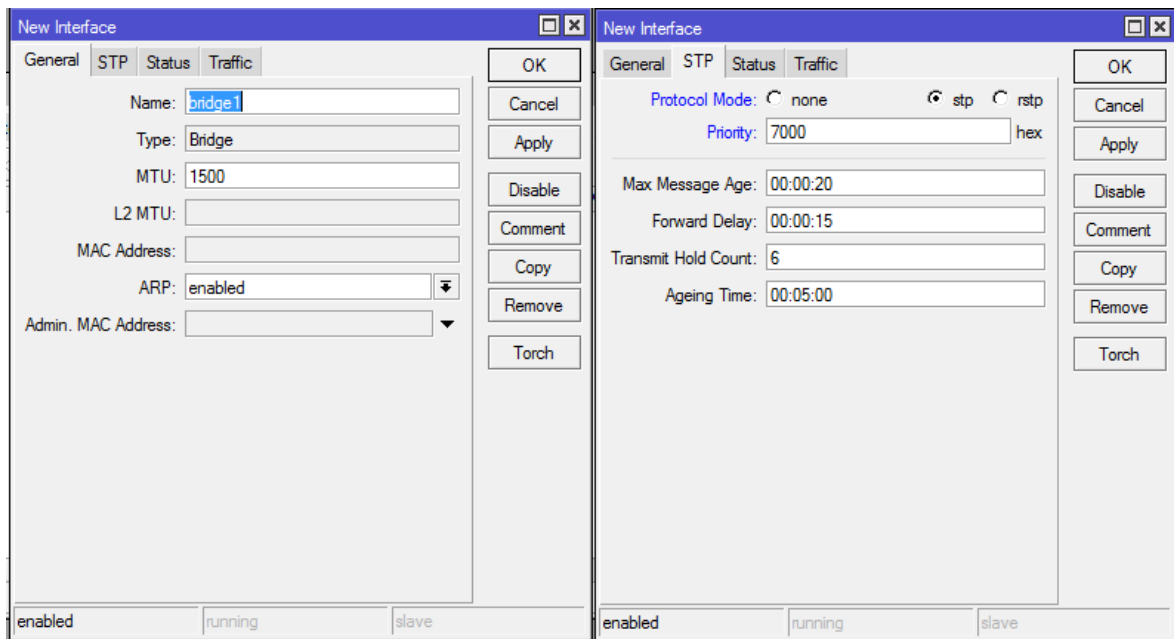
Obrázek 14 - Konfigurace zabezpečení WLAN

Tím byla nastavena bezdrátová síť a bylo možné přejít na konfiguraci jednotlivých portů.

## 7.2 Konfigurace portů

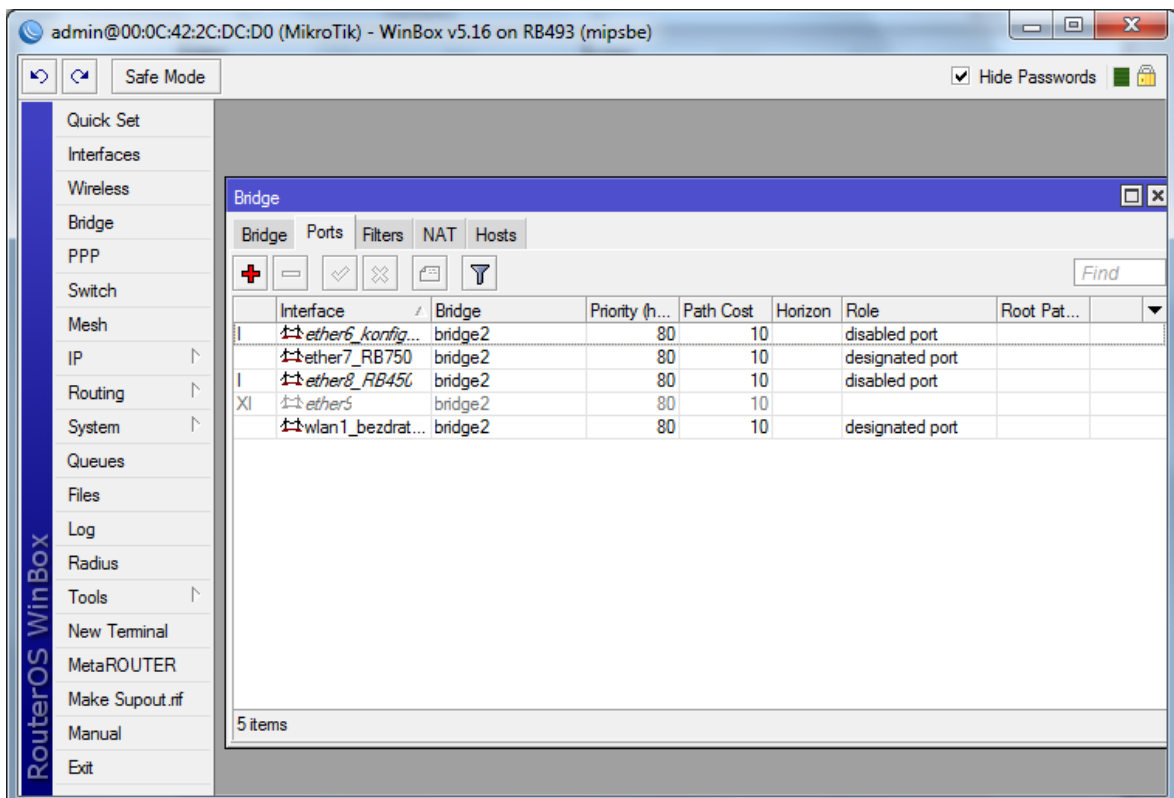
Další postup byl do karty bridge, kde byl vytvořen nový most a zvoleno nastavení STP a s možností byla změněna priorita přepínače tak, aby RB493 byl nastaven jako root bridge. Proto byla snížena priorita z defaultní hodnoty 8000.





Obrázek 15 – Vytvoření a nastavení nového bridge

Následující konfigurace zobrazená na obrázku č. 16 vedla na podkartu Ports, kde byly přidány požadované porty do ucelené sítě tak, aby mezi sebou mohly komunikovat.



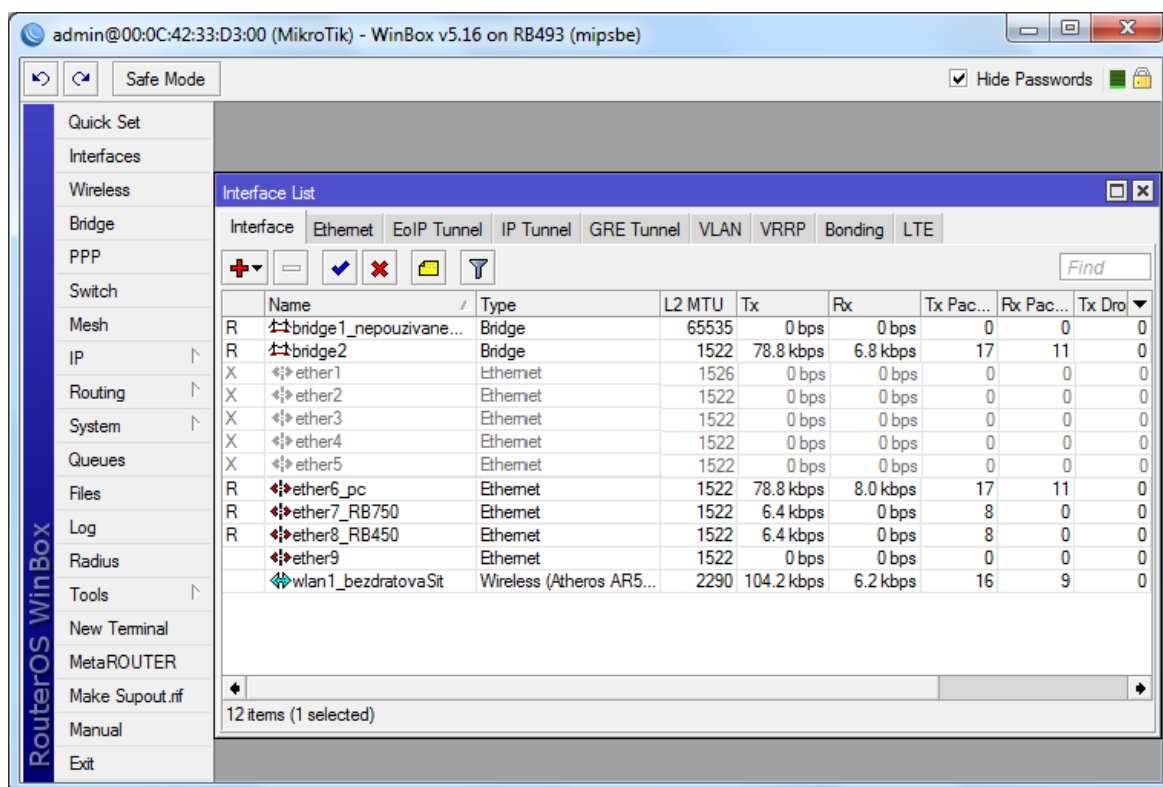
Obrázek 16 - Bridge - Ports - výpis všech přidanych portů

V tomto okamžiku na je již možné vidět role jednotlivých portů.

**Disabled** – port odpojený

**Designated** – port pověřený přenosem dat

Důvodem proč je Ethernet5 šedivý, je ten, že je zablokovaný. Port je v současnosti zakázán, ale nakonfigurován a přidán do bridge. Pokud v budoucnu vznikne potřeba přidat nové zařízení, pak jediné, co bude třeba udělat je aktivovat rozhraní. Potom bude portu, stejně jako ostatním, přidělena jeho role a řádek v okně bude aktivní.



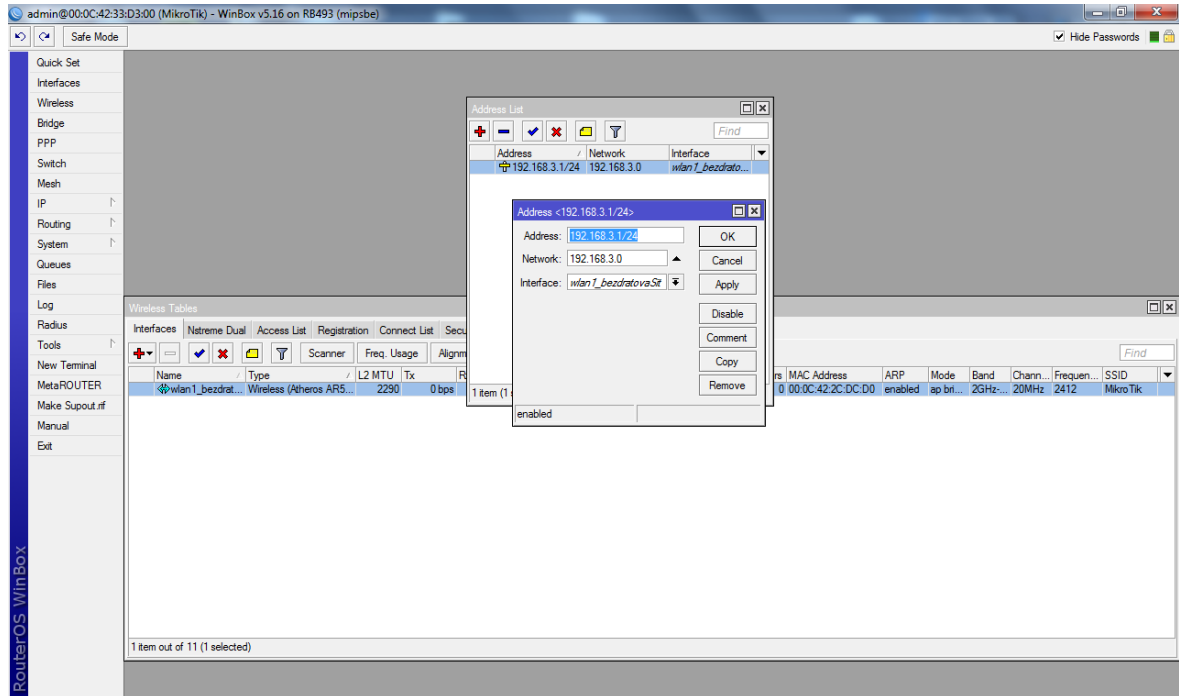
Obrázek 17 - Interface list obsahující veškeré porty

Na obrázku č. 17 je možné vidět veškeré porty, kterými RB493 disponuje. Šedé porty opět ukazují zakázané porty.

V tomto okamžiku, je již síť i STP protokol nastaven a plně funkční.

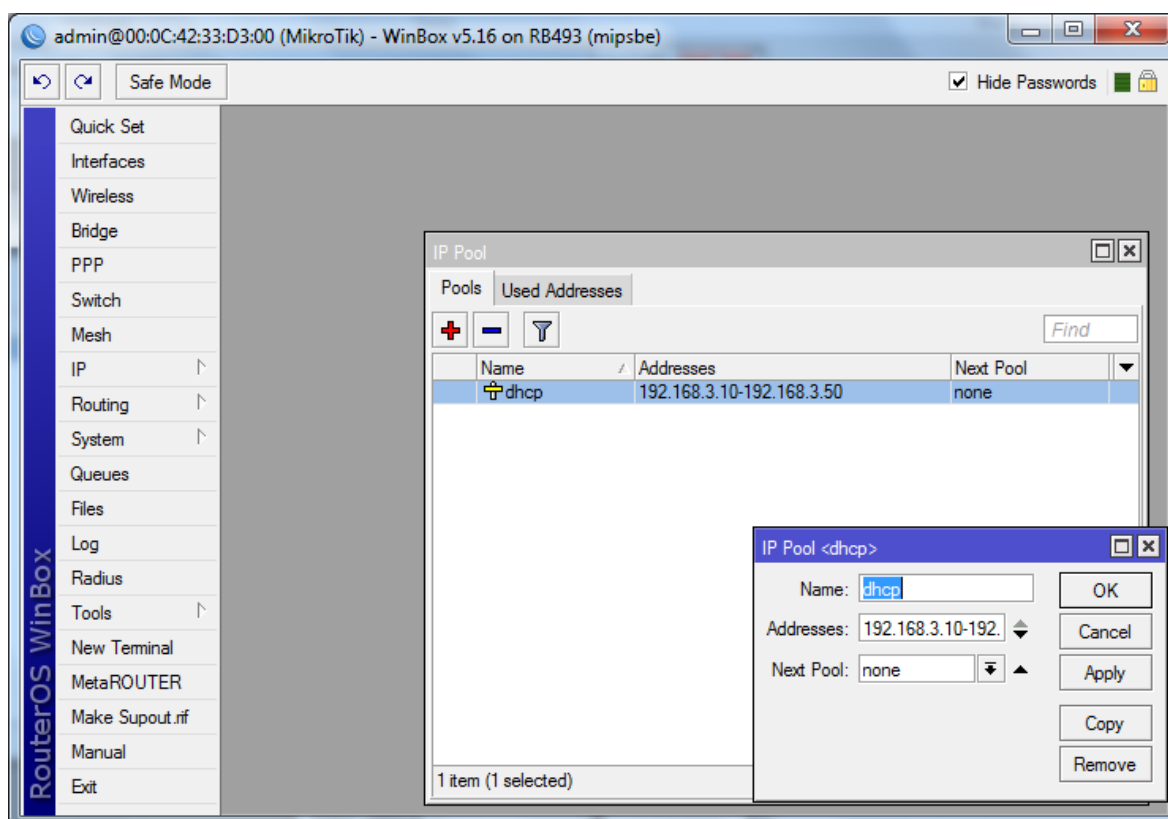
### 7.3 Nastavení DHCP pro bezdrátovou síť

V současné chvíli máme již vytvořenou síť a jediné co zůstává k nakonfigurování je DHCP server, aby bylo možné připojit bezdrátově počítač a dokončit síťové zapojení.



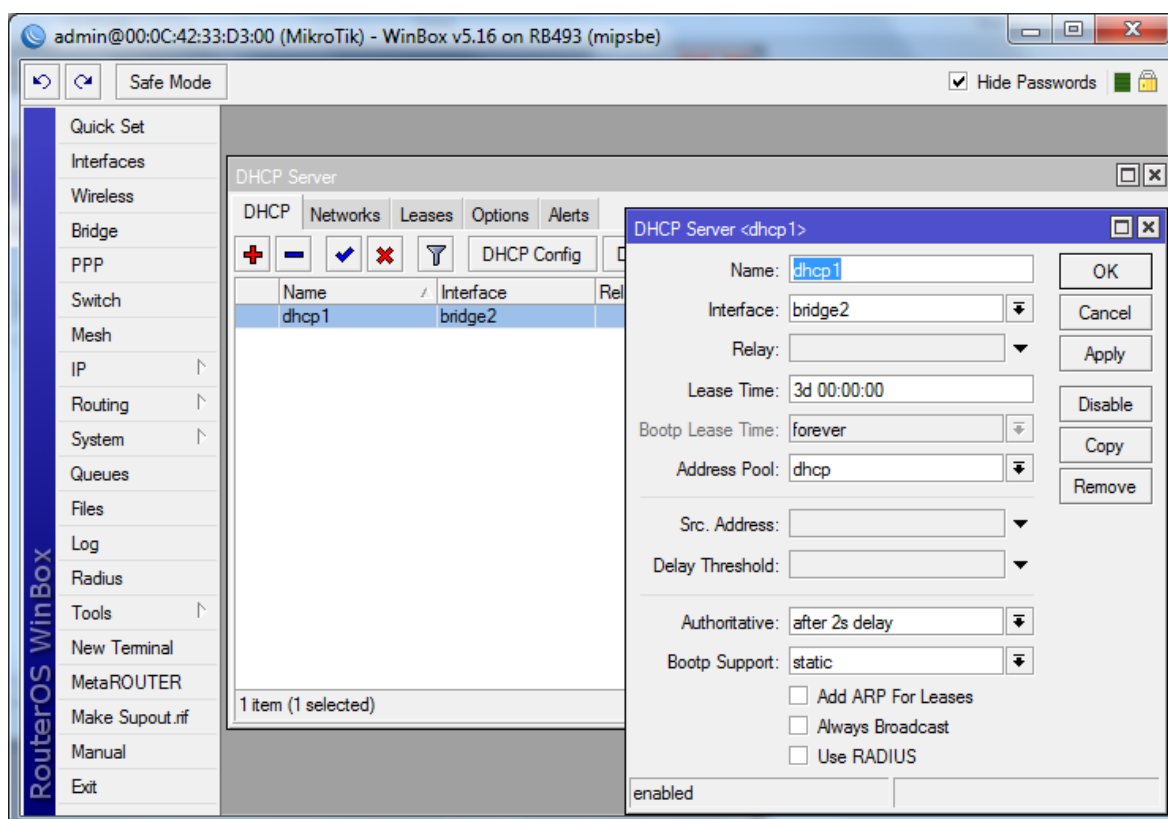
Obrázek 18 - Address list

Pro ten účel je třeba otevřít IP - Address List a nastavit adresu sítě a přiřadit k požadovanému interface, obrázek č. 18.



Obrázek 19 - Nastavení rozsahu IP adres

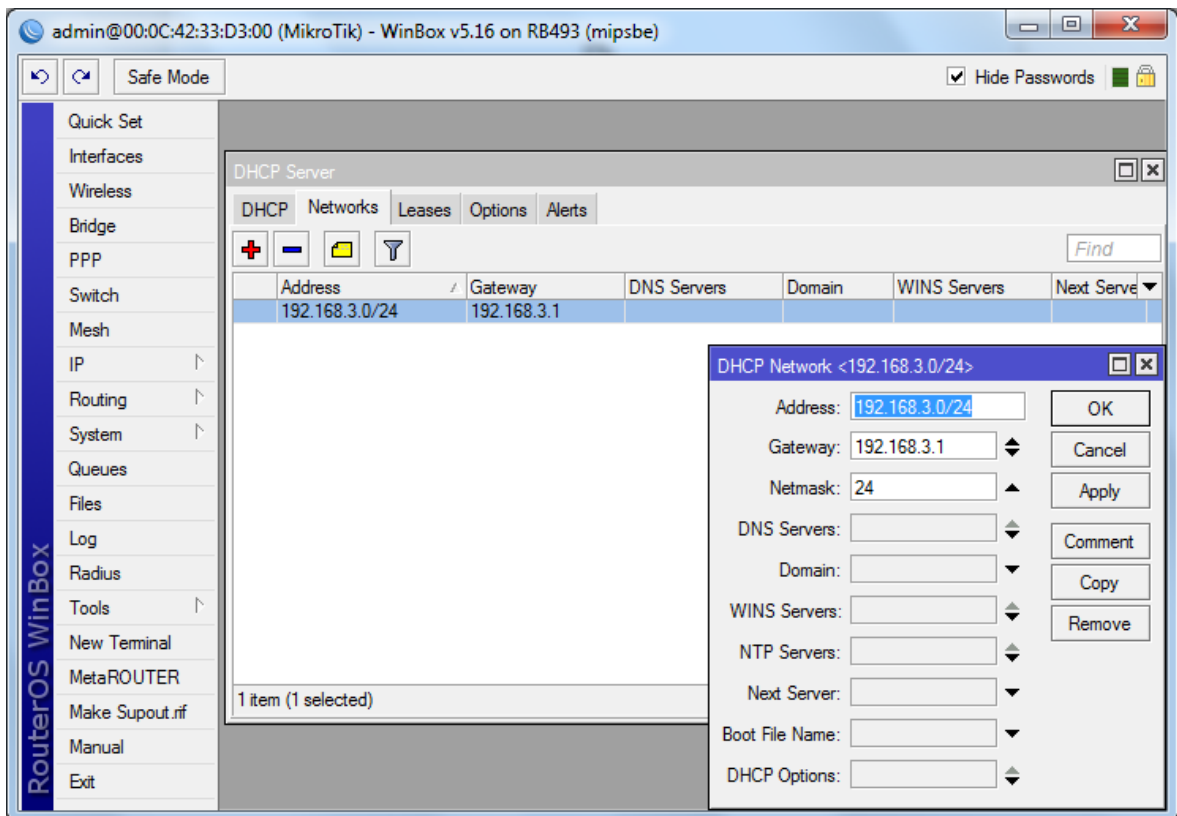
Ilustrační obrázek č. 19 znázorňuje přechod do karty IP – Pool, kde je možné nastavit jméno rozsahu a přiřadit rozsah adres, které budou přiřazovány připojeným zařízením.



**Obrázek 20 - Nastavení DHCP Serveru**

Takto je možné vytvořit nový DHCP server, pojmenovat a přiřadit jej na bridge, ve kterém jsou porty, pro které chceme, aby fungovalo přidělování adres. Nastaveno bylo již v předchozím kroku Address pool a konfigurace byla potvrzena, obrázek č. 20.

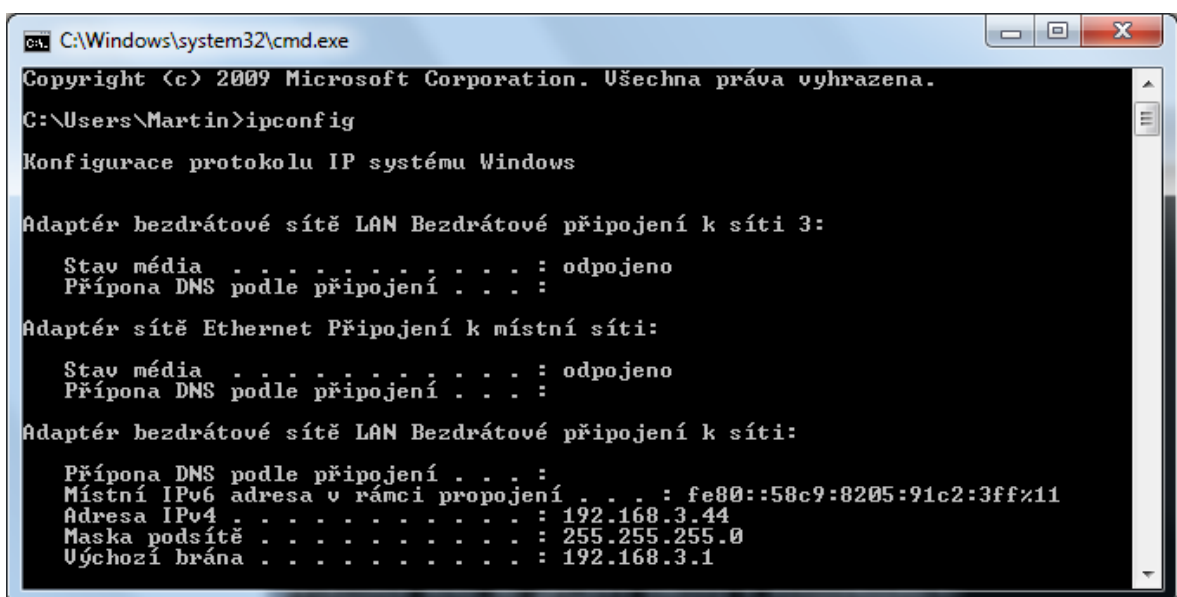
V případě, že nebylo použito rychlého nastavování (quick set), je ještě nutné přejít do karty Networks a nastavit adresu sítě a výchozí bránu, obrázek č. 21.



Obrázek 21 - konfigurace DHCP serveru

Jelikož konfigurace ostatních RB je stejná. Pouze se vynechává část, kde se nastavovala bezdrátová síť a DHCP server není již nutné konfiguraci dále uvádět.

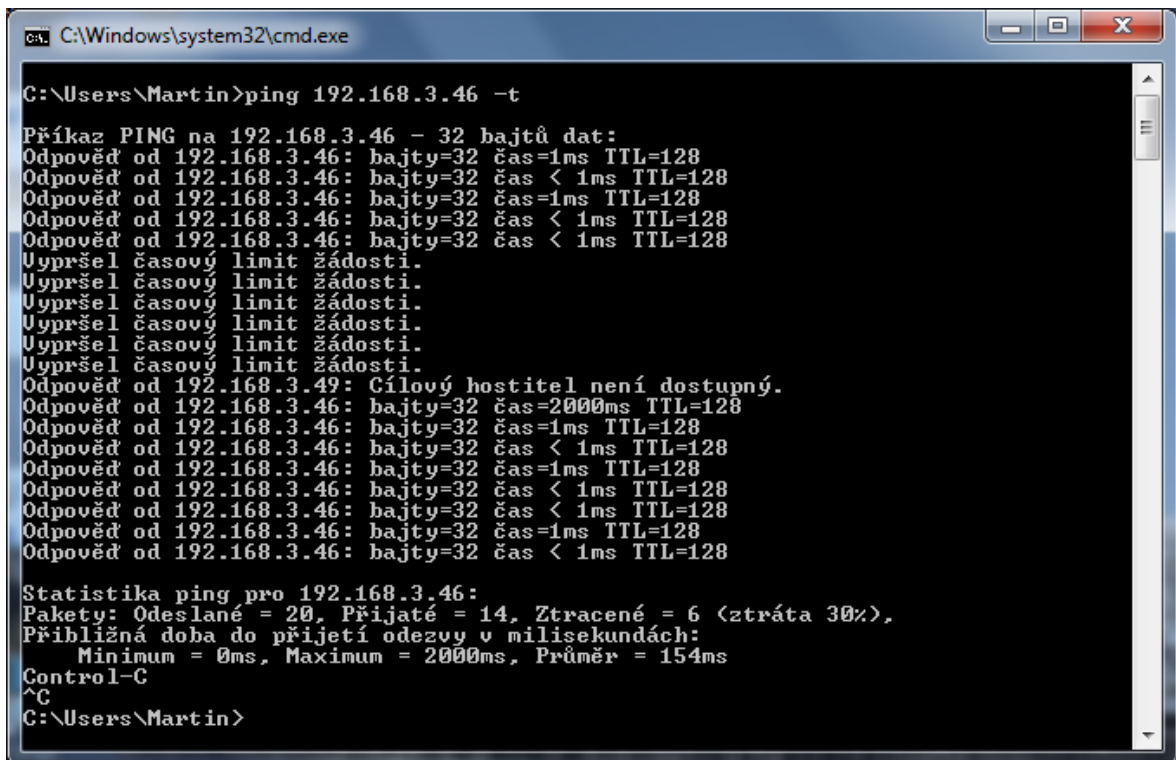
S takto nakonfigurovaným zařízením, by každé koncové zařízení mělo obdržet IP adresu z RB493 a tímto způsobem je možné pustit se do otestování funkčnosti zapojené sítě.



Obrázek 22 - výpis informací o síťovém adaptéru

Jak je na obrázku č. 22 vidět, bezdrátově připojený počítač obdržel IP adresu 192.168.3.44, jehož výchozí branou je 192.168.3.1. V takovéto chvíli je možné spustit ping na adresu druhého cílového zařízení a otestování, zda při přerušení jedné z linek dojde k přesměrování linek.

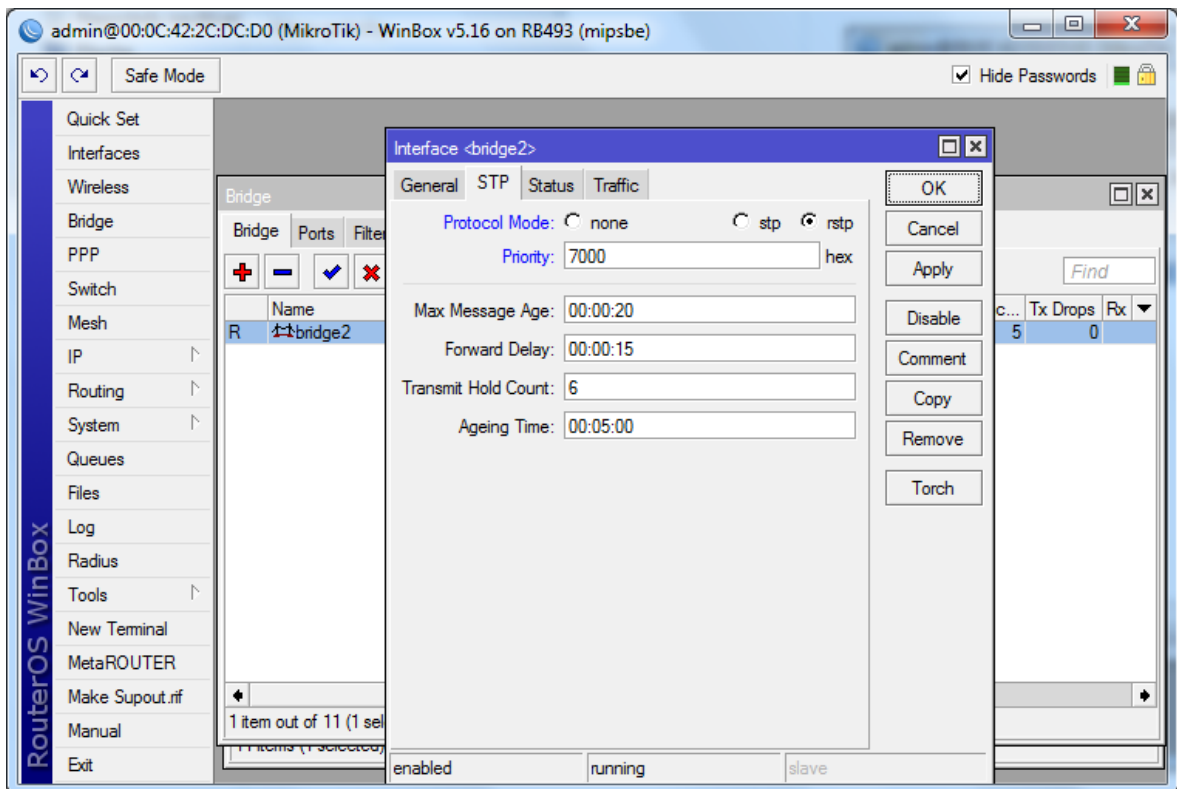
Následuje testování přerušení linky při plné konvergenci sítě, kdy došlo k přerušení jedné linky.



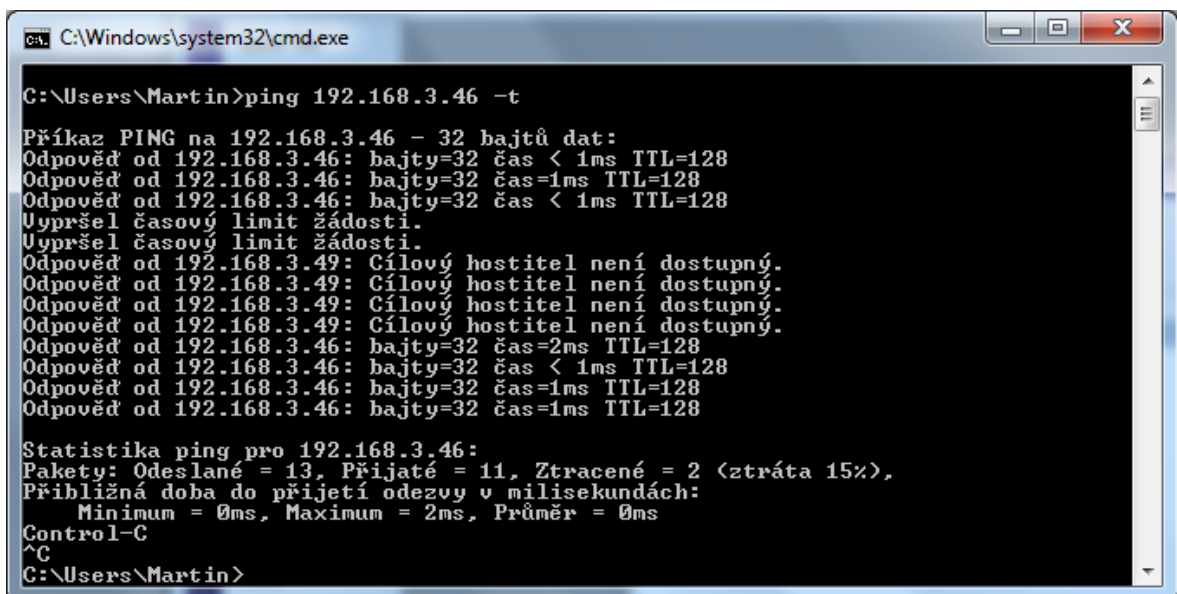
```
C:\Windows\system32\cmd.exe
C:\Users\Martin>ping 192.168.3.46 -t
Příkaz PING na 192.168.3.46 - 32 bajtů dat:
Odpověď od 192.168.3.46: bajty=32 čas=1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas=1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Uypršel časový limit žádosti.
Uypršel časový limit žádosti.
Uypršel časový limit žádosti.
Uypršel časový limit žádosti.
Uypršel časový limit žádosti.
Uypršel časový limit žádosti.
Odpověď od 192.168.3.49: Cílový hostitel není dostupný.
Odpověď od 192.168.3.46: bajty=32 čas=2000ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas=1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas=1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas=1ms TTL=128
Odpověď od 192.168.3.46: bajty=32 čas < 1ms TTL=128
Statistika ping pro 192.168.3.46:
Pakety: Odeslané = 20, Přijaté = 14, Ztracené = 6 (ztráta 30%),
Přibližná doba do přijetí odezvy v milisekundách:
Minimum = 0ms, Maximum = 2000ms, Průměr = 154ms
Control-C
^C
C:\Users\Martin>
```

Obrázek 23 - příkaz ping na koncové zařízení se zapnutým STP

Obrázek č. 23 demonstruje, jak prvně fungující síť, přestala přenášet data a začala přepočítávat topologii sítě. Výsledného přepočítání a plné konvergence dosáhla síť po sérii pokusů průměrně vždy kolem 32 s. Při přepnutí všech RB do režimu RSTP byla konvergence rychlejší a k opětovnému zprovoznění stačilo průměrně 22 s, zobrazují obrázky č. 24 a 25.



Obrázek 24 - přepnutí bridge2 do stavu RSTP



Obrázek 25 - ping na koncové zařízení s přepnutím na RSTP

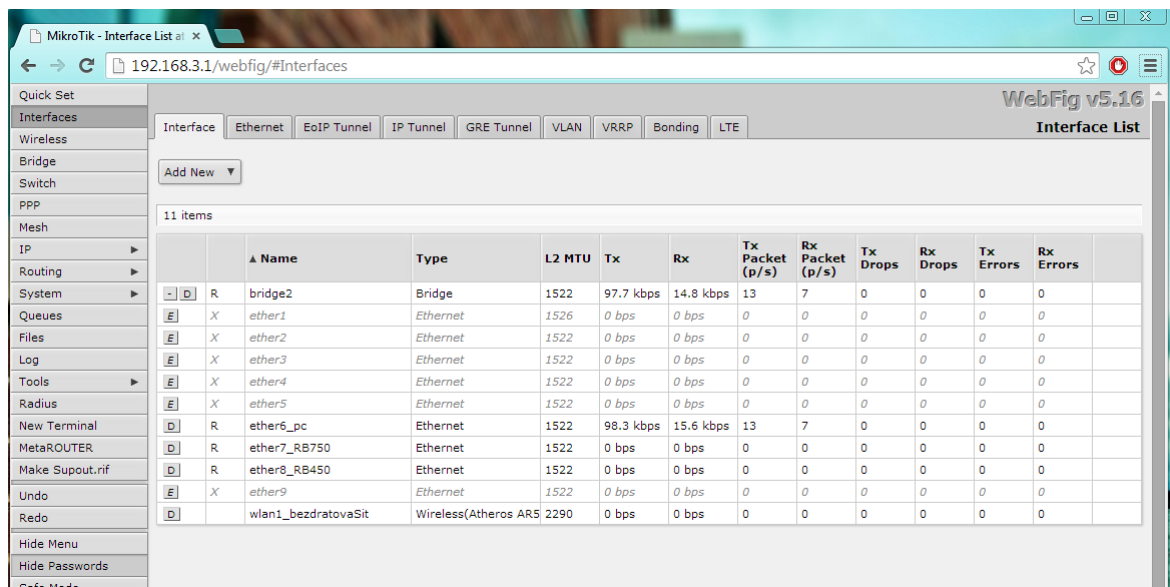


## 7.4 Alternativní konfigurace MikroTik s užitím WebFig

WebFig je webová alternativa, založená na RouterOS, která umožňuje monitorovat, konfigurovat a případně debugovat router. WebFig je navržen jako alternativa k WinBoxu a tak má velmi podobné prostředí. Obě varianty mají stejné možnosti k přístupu všem funkcím RouterOS.

WebFig je přístupný přímo z routeru, což znamená, že zde není potřeba instalovat žádný dodatečný software kromě webového prohlížeče.

„Jelikož je WebFig nezávislá platforma, může být router konfigurovaný z různých mobilních zařízení bez nutnosti instalovat jakýkoliv další program.“ (24)

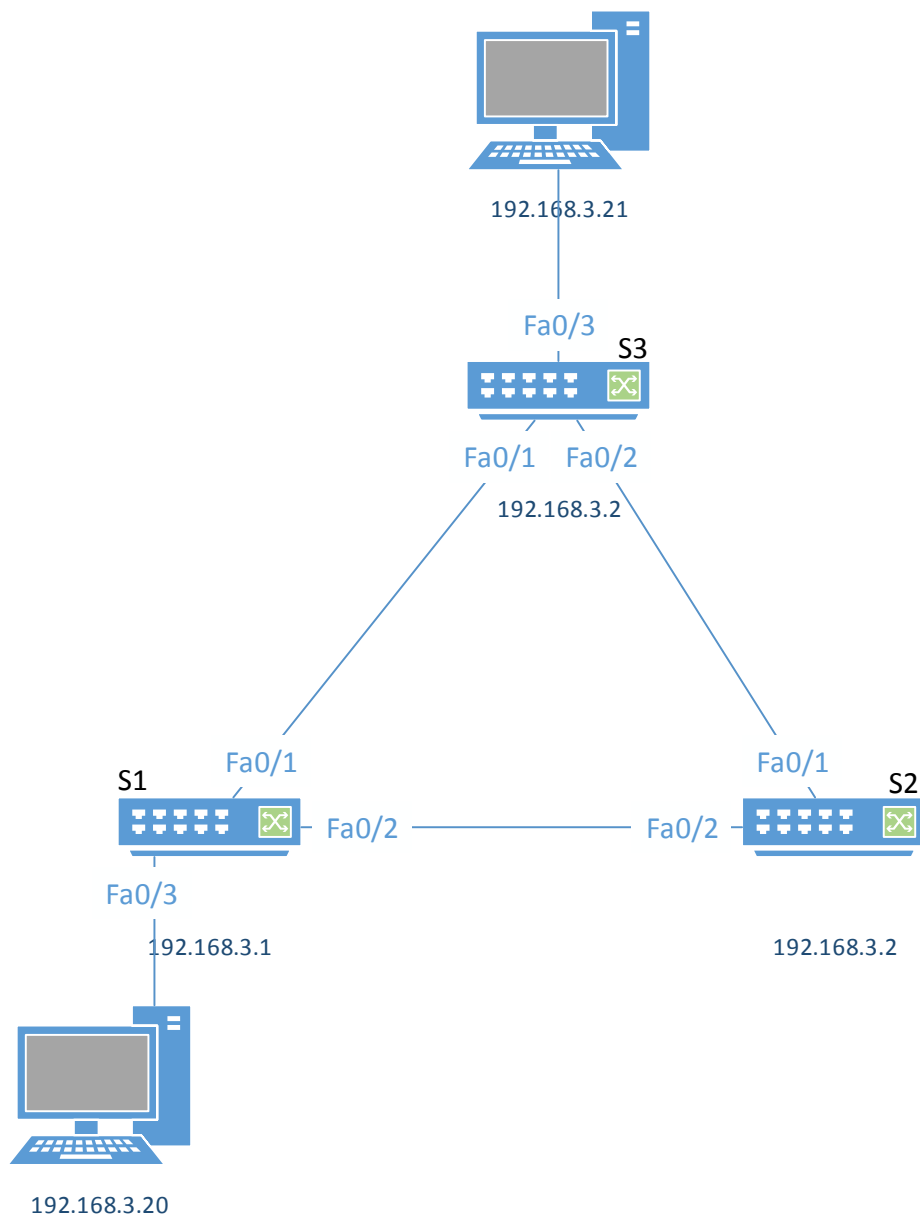


		▲ Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	Tx Drops	Rx Drops	Tx Errors	Rx Errors
	R	bridge2	Bridge	1522	97.7 kbps	14.8 kbps	13	7	0	0	0	0
	X	ether1	Ethernet	1526	0 bps	0 bps	0	0	0	0	0	0
	X	ether2	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	X	ether3	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	X	ether4	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	X	ether5	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	R	ether6_pc	Ethernet	1522	98.3 kbps	15.6 kbps	13	7	0	0	0	0
	R	ether7_RB750	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	R	ether8_RB450	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	X	ether9	Ethernet	1522	0 bps	0 bps	0	0	0	0	0	0
	D	wlan1_bezdratovaSit	Wireless(Atheros AR5	2290	0 bps	0 bps	0	0	0	0	0	0

Obrázek 26 - Ukázka konfigurace v WebFig

## 8 Konfigurace STP na platformě Cisco

Pro konfiguraci na Cisco zařízení byly použity tři 24 portové switche s FastEthernet 2 Gigabit Ethernety.



Obrázek 27 - Řešená síťová topologie Cisco

## 8.1 Ukázka konfigurace S1

```
Switch>enable // přepnutí do privilegovaného režimu
Switch#show ip interface brief // vypíše všechny aktivní porty instalované
na zařízení
```

Interface	IP-Address	OK?	Method	Status
Protocol				
Vlan1	unassigned	YES	unset	administratively down
down				
FastEthernet0/1	unassigned	YES	unset	up
FastEthernet0/2	unassigned	YES	unset	up
FastEthernet0/3	unassigned	YES	unset	up
FastEthernet0/4	unassigned	YES	unset	down
down				

```

FastEthernet0/5      unassigned      YES unset  down
down
FastEthernet0/6      unassigned      YES unset  down
down
FastEthernet0/7      unassigned      YES unset  down
down
FastEthernet0/8      unassigned      YES unset  down
down
FastEthernet0/9      unassigned      YES unset  down
down
FastEthernet0/10     unassigned      YES unset  down
down
FastEthernet0/11     unassigned      YES unset  down
down
FastEthernet0/12     unassigned      YES unset  down
down
FastEthernet0/13     unassigned      YES unset  down
down
FastEthernet0/14     unassigned      YES unset  down
down
FastEthernet0/15     unassigned      YES unset  down
down
FastEthernet0/16     unassigned      YES unset  down
down
FastEthernet0/17     unassigned      YES unset  down
down
FastEthernet0/18     unassigned      YES unset  down
down
FastEthernet0/19     unassigned      YES unset  down
down
FastEthernet0/20     unassigned      YES unset  down
down
FastEthernet0/21     unassigned      YES unset  down
down
FastEthernet0/22     unassigned      YES unset  down
down
FastEthernet0/23     unassigned      YES unset  down
down
FastEthernet0/24     unassigned      YES unset  down
down
GigabitEthernet0/1   unassigned      YES unset  down
down
GigabitEthernet0/2   unassigned      YES unset  down
down

```

```

Switch#conf terminal // přesunutí do konfiguračního rozhraní
Switch(config)#hostname S1 // změna názvu zařízení
S1(config)#no ip domain-lookup // při zadání chybného příkazu se nesnaží
switch překládat příkaz

```

```

S1(config)#int range fa0/1-24 // vstup do rozhraní všech FastEthernetových
portů
S1(config-if-range)#shutdown // vypnutí celého rozhraní
*Mar 1 00:08:43.667: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively down // od každého portu se obdrží potvrzení
o vypnutí

```

```

S1(config-if-range)#int range g0/1-2
S1(config-if-range)#shutdown

```

```

S1(config-if-range)#exit // vyskočení o úroveň nazpět

S1(config)#int fa0/3
S1(config-if)#switchport mode access
S1(config-if)#no shutdown

*Mar 1 00:10:26.578: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed
state to up
*Mar 1 00:10:27.585: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed state

S1(config-if)#int fa0/1
S1(config-if)#switchport mode trunk7 // přepnutí fa0/1 do trunk módu
S1(config-if)#no sh

S1(config-if)#int fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#no sh
*Mar 1 00:12:17.945: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to upint fa0C:2
*Mar 1 00:12:21.720: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed

S1(config-if)#int vlan1 // vytvoření kontrolní VLAN
S1(config-if)#ip address 192.168.3.1 255.255.255.0 // přidání adresy
kontrolní VLANy
S1(config-if)#no shutdown

```

### Zajištění, že S1 bude root bridgem:

```

S1(config)#spanning-tree vlan1 priority 16384 // nastaví prioritu switche
S1(config)#spanning-tree vlan 10 root primary // nastavení switche jako
root

```

```

S1#show spanning-tree // vypsání stavu

```

```

VLAN0001
  Spanning tree enabled protocol ieee
    Root ID      Priority      16384
               Address      0024.c3bb.1400
               This bridge is the root
               Hello Time   2 sec      Max Age 20 sec      Forward Delay 15 sec

    Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
               Address      0024.c3bb.1400
               Hello Time   2 sec      Max Age 20 sec      Forward Delay 15 sec
               Aging Time   15 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	-----	-----	-----	-----	-----
Fa0/3	Desg	FWD	19	128.6	P2p

Jakmile bylo provedené stejné nastavení, jen se správnými adresami na všech ostatních přepínačích, začala síť fungovat.

<sup>7</sup> Trunk – je označován takový port, který je zařazen do více VLAN

## Závěr

V práci byl poskytnut základní pohled na funkce zařízení MikroTik, které může levně, jednoduše a hlavně plnohodnotně nahradit konkurenční zařízení. Ačkoliv v práci byly používány zařízení obsahující pouhých 9 portů, i když MikroTik vyrábí více portové zařízení, které mohou být nasazeny i na síťových uzlech. Využití těchto zařízení je možné v ISP, firmách i v domácích sítích.

V práci byla představena konfigurace datové sítě a na ní technologie zabráňující smyčkám na L2 vrstvě, pomocí STP jak na zařízení MikroTik tak i zařízení firmy Cisco. Čas potřebný ke konvergenci sítě při použití STP, se lišil na těchto platformách pouze v řádu několika vteřin. Na rozdíl od Cisca, MikroTik podporuje STP a RSTP a další nadstavby jako je Rapid PVST není možné nastavit. Jelikož prvky firmy MikroTik nepodporují nové nadstavby přepínacích protokolů, není vhodné je volit jako páteční prvky u rozsáhlejších datových sítí. Na základě získaných zkušeností s prvky MikroTik se jeví jako vhodné pro vytvoření páteční sítě. Vhodné použití pro MikroTik RouterBOARD je jako inteligentních přístupových bodů.

Práce by mohla sloužit jako příručka pro ostatní uživatele MikroTik, poskytující základní údaje a představení funkcí. Zároveň ukazuje modelové příklady pro vytváření moderních sítí s použitím RouterBOARD. Ukazuje výhody jako je nízká cena, jednoduchá správa a konfigurace. Obsahuje informace pro správný a včasný zásah při poruchách. Je možné sledovat chování sítě, ať už s pomocí již předinstalovaných modulů nebo modulů rozšiřující funkce RouterBOARDu.

Přestože konfigurace MikroTiku je intuitivní a poměrně přehledná, je nutné mít jisté počáteční znalosti. Jako nevýhodou se může zdát být to, že běžný uživatel, na kterého jak se zdá bylo i cíleno, pro vytvoření domácí sítě raději zvolí zařízení, které připojí do „zásuvky“ a ono „nějak“ funguje. Proto myslím, že pro určitou skupinu lidí, disponuje MikroTik v základním nastavení příliš velkým množstvím funkcí, čímž se stává pro neznalého uživatele nepřehledným a tak i neatraktivním.

1. Příklady topologií. In: ATIS [obrázek]. Atis, [Online] 2014 [cit. 2014-04-14]. Dostupnost: <http://www.atis.org/glossary/definition.aspx?id=3516>
2. **PŘÍHODA, Petr.** PŘÍRODOVĚDECKÁ FAKULTA, Univerzita Palackého, Katedra Informatiky. *Počítačové sítě*. Olomouc, [Online] 2007. [cit. 2014-04-14] Dostupné z: [http://phoenix.inf.upol.cz/esf/ucebni/poc\\_site.pdf](http://phoenix.inf.upol.cz/esf/ucebni/poc_site.pdf)
3. **SATRAPA, Pavel.** PEDAGOGICKÁ FAKULTA A FAKULTY MECHATRONIKY, Technická univerzita v Liberci. *Architektura sítě, referenční model OSI, architektura internetových protokolů*. Liberec, [Online] 2014. [cit. 2014-04-14] Dostupné z: <http://www.nti.tul.cz/~satrapa/vyuka/site/prednaska02.pdf>
4. **GRYGAREK, Petr.** TECHNICKÁ UNIVERZITA V OSTRAVĚ, Fakulta elektrotechniky a informatiky. *Síťová architektura*. [Online] 2009. [cit. 2014-05-1] Dostupné z: <http://www.cs.vsb.cz/grygarek/PS/lect0304/ps1lect5.html>
5. **BOUŠKA, Petr.** *OSI model*. Fórum [www.samuraj-cz.com](http://www.samuraj-cz.com), články. [Online] 4.3.2007. [Citace: 2. 4 2014.] Dostupné z: <http://www.samuraj-cz.com/clanek/osi-model/>.
6. **PÁV, Miroslav, Jan SYŘÍNEK a Jana HOŠKOVÁ.** *CCNA Exploration - Základy sítí* [online]. Plzeň, 2011, 2011-10-10 [cit. 2014-04-11]. Registrační číslo projektu: CZ.1.07/1.1.12/01.0004. Dostupné z: [http://nidv.mysh.cz/data/resources/ccna\\_exploration\\_1\\_tisk\\_%5B9141179%5D.pdf](http://nidv.mysh.cz/data/resources/ccna_exploration_1_tisk_%5B9141179%5D.pdf)
7. Optický kabel. In: Lancomat [obrázek]. Lancomat, 2014 [cit. 2014-05-1]. Dostupnost: <http://www.lancomat.cz/ImageHandler.ashx?size=1&img=MTA1NWM1YWM4NzQ4ZDcwNC5qcGc=>
8. **PETERKA, Jiří.** FEL ČVUT. Kroucená dvoulinka. [Online] 2011. [cit. 2014-05-1] Dostupné z: <http://www.earchiv.cz/a93/a343c120.php3>
9. **SATRAPA, Pavel.** PEDAGOGICKÁ FAKULTA A FAKULTY MECHATRONIKY, Technická univerzita v Liberci. *Bezdrátové sítě IEEE 802.11*. Liberec, 2014. [Citace: 2. 4 2014] Dostupné z: <http://www.nti.tul.cz/~satrapa/vyuka/site/prednaska05.pdf>
10. **DANIELYAN, Edgar.** CISCO. *IEEE 802.11*. [Online] 2001. [cit. 2014-05-1] Dostupné z: [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_5-1/ieee.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_5-1/ieee.html)
11. **PETERKA, Jiří.** FEL ČVUT. *Router, Gateway*. [Online] 2011. [cit. 2014-04-7] Dostupné z: <http://www.earchiv.cz/a93/a343c120.php3>
12. **ODVÁRKA, Petr.** SVĚT SÍTÍ. *Ethernet* [online]. [Online] 2000 [cit. 2014-05-01]. Dostupné z: <http://www.svetsiti.cz/clanek.asp?cid=Ethernet-1992000>
13. **GLIDDEN, Matthew.** ATPM MAGAZINE. *How to become a network guru: Switches and Hubs*. [Online] 2011. [cit. 2014-05-01] Dostupné z: <http://www.atpm.com/7.10/networking-1.shtml>

14. **BOUŠKA, Petr.** *Ethernet - CSMA/CD, kolizní doména, duplex.* Fórum [www.samuraj-cz.com](http://www.samuraj-cz.com), články. [Online] 3.8.2007. [cit. 2014-04-03] Dostupné z: <http://www.samuraj-cz.com/clanek/ethernet-csmacd-kolizni-domena-duplex/>
15. **KOZIEROK, Charles.** *Overview Of Key Routing Protocol Concepts: Architectures, Protocol Types, Algorithms and Metrics* [online]. 2005 [cit. 2014-04-02]. Dostupné z: [http://www.tcpipguide.com/free/t\\_OverviewOfKeyRoutingProtocolConceptsArchitecturesP.htm](http://www.tcpipguide.com/free/t_OverviewOfKeyRoutingProtocolConceptsArchitecturesP.htm)
16. **GRYGAREK, Petr.** TECHNICKÁ UNIVERZITA V OSTRAVĚ, Fakulta elektrotechniky a informatiky. *Propojování sítí a směrování.* [Online] 2009. [cit. 2014-04-02] Dostupné z: [http://www.cs.vsb.cz/grygarek/PS/lect/propojovani\\_prvky.html](http://www.cs.vsb.cz/grygarek/PS/lect/propojovani_prvky.html)
17. **VÍT, Míchal a Petr ŠPRINGL.** VUT FAKULTA INFORMAČNÍCH TECHNOLOGIÍ. *CISCO Network Academy: Základy Přepínání CCNA1 - Modul 8.* Brno, [Online] 2007. [cit. 2014-04-02] Dostupné z: <http://netacad.fit.vutbr.cz/texty/ccna-moduly/ccna1-8.pdf>
18. **BOUŠKA, Petr.** *Cisco IOS 9 - Spanning Tree Protocol.* Fórum [www.samuraj-cz.com](http://www.samuraj-cz.com), články. [Online] 3.5.2009. [cit. 2014-04-07] Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/>
19. **CISCO.** *Understanding Rapid Spanning Tree Protocol (802.1w).* [Online] 2006. [cit. 2014-04-03] Dostupné z: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>
20. **CISCO.** *Cisco Nexus 5000 Series Switch CLI Software Configuration Guide: Configuring Rapid PVST.* San Jose, USA, [Online] 2012. [cit. 2014-05-01] Dostupné z: <http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/RPVSpanningTree.html#wp1205454>
21. **MIKROTIK.** *About us.* [Online] 2013. [cit. 2014-05-01] Dostupné z: <http://www.mikrotik.com/aboutus>
22. **MIKROTIK.** *WinBox.* [Online] 2014. [cit. 2014-05-01] Dostupné z: <http://wiki.mikrotik.com/wiki/Manual:Winbox>
23. **MIKROTIK.** *First time startup.* [Online] 2013. [cit. 2014-05-01] Dostupné z: [http://wiki.mikrotik.com/wiki/Manual:First\\_time\\_startup](http://wiki.mikrotik.com/wiki/Manual:First_time_startup)
24. **MIKROTIK.** *Webfig.* [Online] 2012. [cit. 2014-05-01] Dostupné z: <http://wiki.mikrotik.com/wiki/Manual:Webfig>
25. **LAMMLE, Todd.** *CCNA: Cisco certified network associate fast pass.* 3rd ed. Indianapolis: Wiley Publishing, 2007, xxix, 467 s. ISBN 978-0-470-18571-1