

# Vytvoření laboratorních úloh pro kurz Cisco CCNA R@S Základy směrování a přepínání

Břetislav Sobek

---

Bakalářská práce  
2015

 Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

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

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Břetislav Sobek**  
Osobní číslo: **A11055**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Informační a řídicí technologie**  
Forma studia: **prezenční**

Téma práce: **Vytvoření laboratorních úloh pro kurz Cisco CCNA R@S Základy směrování a přepínání**

Téma anglicky: **Creating Laboratory Tasks for the Cisco CCNA R@S Routing and Switching Essentials Course**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Vytvořte laboratorní úlohy pro volitelný předmět Cisco CCNA R@S Základy směrování a přepínání.
3. Navrhněte vzorová řešení pro vypracované úlohy, včetně konfigurací aktivních prvků Cisco.
4. Navržené úlohy ověřte v Cisco výukovém systému Packet Tracer.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. KUROSE, James F a Keith W ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.
2. LAMMLE, Todd a Keith W ROSS. CCNA: výukový průvodce přípravou na zkoušku 640-802. 1. vyd. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.
3. EMPSON, Scott. CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. 1. vyd. Brno: Computer Press, 2009, 336 s. ISBN 978-80-251-2286-0.
4. HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce: autorizovaný výukový průvodce. 5. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-80-251-3176-3.
5. LAMMLE, Todd. CCNA: routing and switching: study guide. 1. vyd. Wiley-Blackwell, 2013, 1176 s. ISBN 11-187-4961-8.

Vedoucí bakalářské práce:

**Ing. Miroslav Matýsek, Ph.D.**

Ústav počítačových a komunikačních systémů


Datum zadání bakalářské práce:

**6. března 2015**

Termín odevzdání bakalářské práce:

**22. května 2015**

Ve Zlíně dne 6. března 2015



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



prof. Ing. Vladimír Vašek, CSc.  
*ředitel ústavu*

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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 20. 5. 2015 .....



.....  
podpis diplomanta

## **ABSTRAKT**

Práce se zaměřuje na počítačové sítě v rozsahu kurzu Cisco CCNA R@S Základy směrování a přepínání. V práci jsou popsány základní věci týkající se přepínaných sítí, základů směrování a směrovací protokol OSPF. Dále se zabývá Access control listy a síťovými službami NAT a DHCP. Je zde rozebrán operační systém IOS, který běží na Cisco zařízeních.

Klíčová slova: počítačové sítě, přepínání, směrování, IOS, Cisco

## **ABSTRACT**

This thesis focuses on the topic of computer networks in the extent of the course Cisco CCNA R@S Routing and Switching Essentials. There are described essentials regarding switched networks, basics of a routing and a routing protocol OSPF in this thesis. Moreover there are written about Access control lists, NAT and DHCP. IOS, which runs in Cisco devices, is also described in this thesis.

Keywords: computer networks, switching, routing, IOS, Cisco

Poděkování:

Děkuji vedoucímu Ing. Miroslavu Matýskovi, Ph.D. za pomoc při zpracovávání bakalářské práce. Děkuji také Ing. Petru Skovajsovi za zapůjčení přepínačů Cisco a svým rodičům za podporu při studiu.

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

**OBSAH**

<b>ÚVOD</b> .....	<b>12</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>13</b>
<b>1 ÚVOD DO PŘEPÍNANÝCH SÍTÍ</b> .....	<b>14</b>
1.1 KONVERGOVANÉ SÍTĚ .....	14
1.2 TŘÍVRSTVÝ HIERARCHICKÝ MODEL .....	14
1.2.1 PŘÍSTUPOVÁ VRSTVA .....	14
1.2.2 DISTRIBUČNÍ VRSTVA.....	15
1.2.3 VRSTVA JÁDRA.....	15
1.2.4 VÝHODY HIERARCHICKÉ MODELU .....	15
1.2.5 KRITÉRIA PRO VÝBĚR PŘEPÍNAČŮ.....	15
1.3 PŘEPÍNÁNÍ RÁMCŮ .....	16
1.3.1 METODA STORE-AND-FORWARD .....	16
1.3.2 METODA CUT-THROUGH .....	17
1.4 DOMÉNY .....	17
1.4.1 KOLIZNÍ DOMÉNA.....	17
1.4.2 BROADCASTOVÁ DOMÉNA.....	18
<b>2 ZÁKLADY PŘEPÍNÁNÍ A KONFIGURACE PŘEPÍNAČŮ</b> .....	<b>19</b>
2.1 STRUKTURA PAMĚTÍ ZAŘÍZENÍ CISCO .....	19
2.2 KONFIGURAČNÍ MÓDY ZAŘÍZENÍ CISCO .....	19
2.3 ZÁKLADNÍ BOOTOVACÍ SEKVENCE PŘEPÍNAČE .....	19
2.4 STAVOVÉ DIODY NA PŘEPÍNAČI.....	20
2.5 VZDÁLENÝ PŘÍSTUP PŘES TELNET .....	21
2.6 NASTAVENÍ PORTŮ NA PŘEPÍNAČI .....	22
2.6.1 JEDNOSMĚRNÁ A OBOUSMĚRNÁ KOMUNIKACE.....	22
2.6.2 RYCHLOST PORTU .....	22
2.6.3 AUTO-MDIX .....	22
2.7 OVĚŘOVÁNÍ NASTAVENÍ ZAŘÍZENÍ CISCO .....	22
2.8 ŘEŠENÍ PROBLÉMŮ NA FYZICKÉ A LINKOVÉ VRSTVĚ .....	24
2.9 VZDÁLENÝ PŘÍSTUP PŘES SSH .....	25
2.10 BEZPEČNOST PŘEPÍNAČŮ .....	26
2.10.1 TYPY BEZPEČNOSTNÍCH DĚR A ÚTOKŮ .....	26
2.10.2 OBRANA PROTI ÚTOKŮM .....	26
2.10.3 PORT SECURITY .....	27
<b>3 VLAN</b> .....	<b>28</b>
3.1 TYPY VLAN .....	28

3.1.1	DATOVÁ VLAN .....	28
3.1.2	VÝCHOZÍ VLAN .....	29
3.1.3	NATIVNÍ VLAN .....	29
3.1.4	VLAN PRO SPRÁVU .....	29
3.1.5	VLAN PRO VOIP .....	29
3.2	TRUNK A OZNAČOVÁNÍ RÁMCŮ .....	29
3.2.1	OZNAČOVÁNÍ RÁMCŮ POMOCÍ 802.1Q .....	30
3.3	KONFIGURACE VLAN .....	31
3.3.1	VYTVOŘENÍ VLAN .....	31
3.3.2	PŘÍŘAZENÍ PORTU DO SPRÁVNÉHO MÓDU .....	31
3.3.3	OVĚŘENÍ NASTAVENÍ VLAN SÍTÍ .....	32
3.4	DTP .....	33
3.5	BEZPEČNOST VLAN SÍTÍ .....	34
3.5.1	FALEŠNÝ PŘEPÍNAČ .....	34
3.5.2	FALEŠNÝ TAG .....	34
<b>4</b>	<b>ÚVOD DO SMĚROVANÝCH SÍTÍ .....</b>	<b>35</b>
4.1	SMĚROVÁNÍ .....	35
4.2	SMĚROVAČ A PŘIPOJENÍ .....	36
4.3	DOKUMENTACE SÍTĚ .....	36
4.4	ZÁKLADNÍ KONFIGURACE SMĚROVAČE .....	36
4.5	DTE, DCE A CLOCK RATE .....	38
4.6	LOOPBACK PORT .....	38
4.7	OVĚŘENÍ KONFIGURACE PORTŮ .....	39
4.8	URČENÍ NEJLEPŠÍ CESTY V SÍTÍ .....	39
4.9	VYVAŽOVÁNÍ ZÁTĚŽE .....	39
4.10	ADMINISTRATIVNÍ VZDÁLENOST .....	40
4.11	TYPY NAUČENÍ CEST K SÍTÍM .....	40
4.11.1	PŘÍMO PŘIPOJENÉ CESTY .....	40
4.11.2	STATICKE SMĚROVÁNÍ .....	40
4.11.3	DYNAMICKÉ SMĚROVACÍ PROTOKOLY .....	40
4.12	VÝCHOZÍ CESTA .....	41
<b>5</b>	<b>INTER-VLAN SMĚROVÁNÍ .....</b>	<b>42</b>
5.1	TYPY INTER-VLAN SMĚROVÁNÍ .....	42
5.1.1	ZASTARALÉ INTER-VLAN SMĚROVÁNÍ .....	42
5.1.2	ROUTER-ON-A-STICK .....	42
5.1.3	SMĚROVÁNÍ POMOCÍ L3 PŘEPÍNAČE .....	43
5.2	KONFIGURACE ROUTER-ON-A-STICK .....	43
<b>6</b>	<b>STATICKE SMĚROVÁNÍ .....</b>	<b>45</b>
6.1	TYPY STATICKE CEST .....	45

6.1.1	STANDARTNÍ STATICKÁ CESTA.....	45
6.1.2	VÝCHOZÍ STATICKÁ CESTA.....	45
6.1.3	SOUHRNNÁ STATICKÁ CESTA .....	45
6.1.4	ZÁLOŽNÍ STATICKÁ CESTA .....	45
6.2	KONFIGURACE IPV4 STATICKÝCH CEST.....	46
6.3	KONFIGURACE IPV6 STATICKÝCH CEST.....	46
6.4	TYPY SMĚROVÁNÍ.....	47
6.4.1	CLASSFUL SMĚROVÁNÍ.....	47
6.4.2	CLASSLESS SMĚROVÁNÍ .....	47
6.5	VLSM.....	47
<b>7</b>	<b>DYNAMICKÉ SMĚROVÁNÍ.....</b>	<b>48</b>
7.1	ZJIŠŤOVÁNÍ CEST .....	48
7.1.1	POČÁTEČNÍ ZJIŠŤOVÁNÍ.....	48
7.1.2	VÝMĚNA SMĚROVACÍCH INFORMACÍ MEZI SMĚROVAČI.....	48
7.1.3	KONVERGENCE .....	48
7.2	TYPY SMĚROVACÍCH PROTOKOLŮ .....	48
7.2.1	INTERNÍ A EXTERNÍ SMĚROVACÍ PROTOKOLY.....	48
7.2.2	VEKTOROVÉ A LINK-STATE SMĚROVACÍ PROTOKOLY.....	49
7.2.3	CLASSFUL A CLASSLESS SMĚROVACÍ PROTOKOLY .....	49
7.3	METRIKA.....	51
7.4	RIP A RIPNG.....	51
7.5	KONFIGURACE RIP .....	52
<b>8</b>	<b>OSPF.....</b>	<b>54</b>
8.1	OSPF OBLASTI .....	54
8.2	STAVY OSPF.....	55
8.3	DR A BDR .....	55
8.4	ID SMĚROVAČE .....	56
8.5	METRIKA OSPF .....	56
8.6	KONFIGURACE OSPF.....	57
<b>9</b>	<b>ACCESS CONTROL LISTY .....</b>	<b>59</b>
9.1	FUNGOVÁNÍ ACL .....	59
9.2	PRAVIDLA PRO POUŽITÍ ACL .....	59
9.3	STANDARTNÍ ČÍSLOVANÉ ACL.....	59
9.4	ROZŠÍŘENÉ ČÍSLOVANÉ ACL .....	60
9.5	POJMENOVANÉ ACL .....	60
<b>10</b>	<b>DHCP.....</b>	<b>62</b>
10.1	PRŮBĚH PŘIDĚLOVÁNÍ S DHCP .....	62

10.1.1	DHCP DISCOVER.....	62
10.1.2	DHCP OFFER.....	62
10.1.3	DHCP REQUEST.....	62
10.1.4	DHCP PACK.....	62
10.2	KONFIGURACE DHCP.....	62
<b>11</b>	<b>NETWORK ADDRESS TRANSLATION.....</b>	<b>64</b>
11.1	PŘEKLAD NAT.....	64
11.2	TYPY NAT PŘEKLADU.....	65
11.2.1	STATICKÝ PŘEKLAD.....	65
11.2.2	DYNAMICKÝ PŘEKLAD.....	65
11.2.3	PORT ADDRESS TRANSLATION.....	65
11.3	KONFIGURACE NAT A PAT.....	66
<b>II</b>	<b>PRAKTICKÁ ČÁST.....</b>	<b>67</b>
<b>12</b>	<b>PROVEDENÍ PRAKTICKÉ ČÁSTI.....</b>	<b>68</b>
12.1	ZADÁNÍ ÚLOHY.....	68
12.2	ŘEŠENÍ ÚLOHY.....	68
12.3	PROVEDENÍ KONFIGURACE.....	68
12.4	DOPORUČENÍ PRO KONFIGUROVÁNÍ ÚLOH.....	68
<b>13</b>	<b>ÚLOHA 1 – ZÁKLADNÍ NASTAVENÍ.....</b>	<b>69</b>
13.1	ZADÁNÍ.....	69
13.2	ŘEŠENÍ.....	70
<b>14</b>	<b>ÚLOHA 2 – VZDÁLENÝ PŘÍSTUP, NASTAVENÍ PORTŮ A BEZPEČNOST</b>	<b>73</b>
14.1	ZADÁNÍ.....	73
14.2	ŘEŠENÍ.....	74
<b>15</b>	<b>ÚLOHA 3 – NASTAVENÍ VLAN.....</b>	<b>77</b>
15.1	ZADÁNÍ.....	77
15.2	ŘEŠENÍ.....	78
<b>16</b>	<b>ÚLOHA 4 – NASTAVOVÁNÍ PORTŮ SMĚROVAČE.....</b>	<b>82</b>
16.1	ZADÁNÍ.....	82
16.2	ŘEŠENÍ.....	82
<b>17</b>	<b>ÚLOHA 5 – INTER-VLAN SMĚROVÁNÍ.....</b>	<b>84</b>
17.1	ZADÁNÍ.....	84
17.2	ŘEŠENÍ.....	84
<b>18</b>	<b>ÚLOHA 6 – STATICKE SMĚROVÁNÍ.....</b>	<b>86</b>
18.1	ZADÁNÍ.....	86
18.2	ŘEŠENÍ.....	86
<b>19</b>	<b>ÚLOHA 7 – KONFIGURACE RIPV2.....</b>	<b>89</b>
19.1	ZADÁNÍ.....	89
19.2	ŘEŠENÍ.....	90
<b>20</b>	<b>ÚLOHA 8 – KONFIGURACE OSPFV2.....</b>	<b>92</b>

---

20.1	ZADÁNÍ.....	92
20.2	ŘEŠENÍ.....	93
<b>21</b>	<b>ÚLOHA 9 – ACL LISTY .....</b>	<b>95</b>
21.1	ZADÁNÍ.....	95
21.2	ŘEŠENÍ.....	95
<b>22</b>	<b>ÚLOHA 10 – DHCP .....</b>	<b>97</b>
22.1	ZADÁNÍ.....	97
22.2	ŘEŠENÍ.....	97
<b>23</b>	<b>ÚLOHA 11 – NAT .....</b>	<b>99</b>
23.1	ZADÁNÍ.....	99
23.2	ŘEŠENÍ.....	99
	<b>ZÁVĚR .....</b>	<b>101</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>102</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>103</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>106</b>
	<b>SEZNAM TABULEK.....</b>	<b>108</b>
	<b>SEZNAM PŘÍLOH NA CD .....</b>	<b>109</b>

## ÚVOD

V dnešním světě jsou počítačové sítě velmi důležité. Rychlost přenosu informace je dnes důležitější než kdy dříve. Počítačové sítě slouží k propojování lidí a datových center na celém světě. Potřeba komunikace s různými subjekty na trhu je dnes klíčová pro úspěch. Jednotlivé podniky používají sítě k propojení svých zaměstnanců a sdílení informací mezi sebou. Díky přístupu většiny zaměstnanců k informacím firmy může i řadový zaměstnanec přijít na něco, na co by úzká skupina nepřišla. Dále také dochází k úspoře času a papíru, což zajišťuje lepší životní prostředí. Dnes jednatel ve firmě už nemusí čekat, až k němu dorazí prodejní čísla z pobočky, ale má je přímo a ihned před sebou a to díky počítačovým sítím.

Kvalitní počítačová síť je stěžejní pro úspěch v dnešní době. Kvalitní počítačovou síť je třeba vybudovat z kvalitních síťových zařízení. Těmito zařízeními jsou přepínače a směrovače firmy Cisco. Kromě kvalitního zařízení je třeba tyto zařízení správně nastavit, aby zaručovaly vysokou propustnost a bezpečnost. Pro tento úkol je třeba mít kvalitního administrátora, který je schopen tato zařízení efektivně nakonfigurovat.

Tato práce je rozdělena do dvou částí, teoretické a praktické. V teoretické části jsou popsány technologie a služby počítačových sítí. Mezi ně patří přepínání a směrování. Specifičtěji směrovací protokoly RIPv2 a OSPFv2, VLAN sítě, služby počítačových sítí jako DHCP, NAT a ACL listy pro zabezpečení sítě. V každé kapitole jsou uvedeny příkazy pro konfiguraci jednotlivých technologií a služeb počítačových sítí.

V praktické části je popsáno, jak bylo postupováno při tvorbě této části. Praktická část se skládá z 11 praktických úloh pro program Cisco Packet tracer pro simulaci počítačových infrastruktur. Každá úloha se skládá se zadání a řešení, a to jak v provedení v programu Word tak i v Packet traceru. Jednotlivé úlohy jsou přiloženy jako přílohy k této práci.

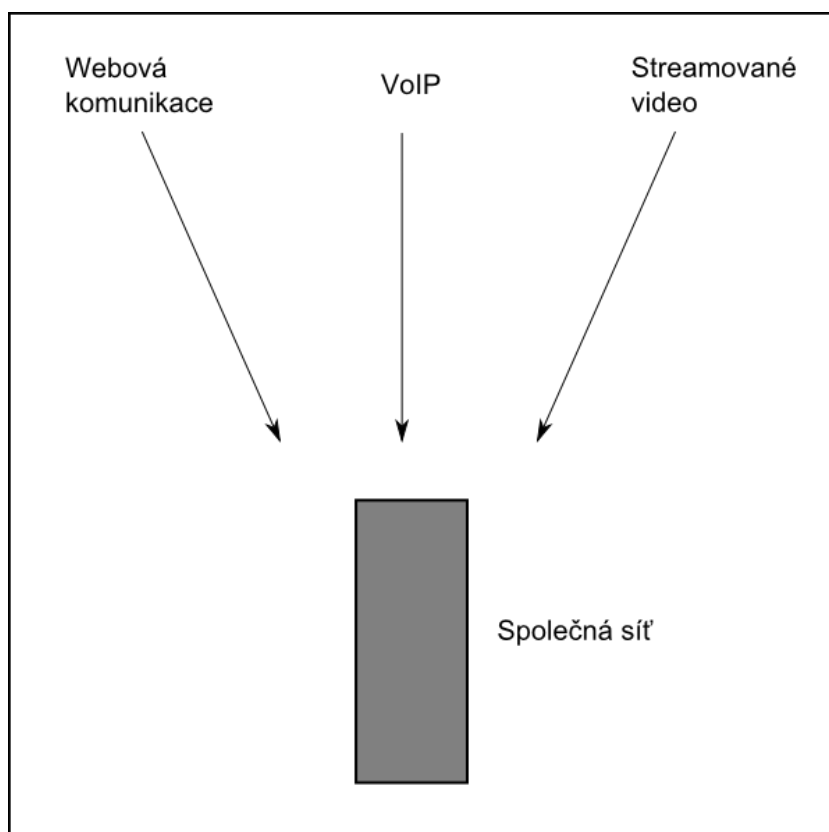
Cílem této práce je studentům CCNA akademie poskytnout potřebnou teorii v českém jazyce, jelikož samotná akademie je v jazyce anglickém. Dále je také cílem poskytnout 11 praktických úloh korespondující s kapitolami v kurzu Cisco CCNA R@S Routing and Switching Essentials.

## **I. TEORETICKÁ ČÁST**

# 1 ÚVOD DO PŘEPÍNANÝCH SÍTÍ

## 1.1 Konvergované sítě

Dnes jsou konvergované sítě základním kamenem počítačových sítí. Konvergovaná síť je síť, která umí přenést webovou komunikaci, VoIP (Voice over IP) i streamované video přes jednu paketovou síť. Již není potřeba mít zvlášť síť pro telefonii a internetový provoz [1].



Obr. 1. Konvergované sítě.

## 1.2 Třívrstvý hierarchický model

Model přepínané sítě se skládá ze tří vrstev, přístupové vrstvy, distribuční vrstvy a vrstvy jádra. Každá vrstva zastává jiné funkce [2].

### 1.2.1 Přístupová vrstva

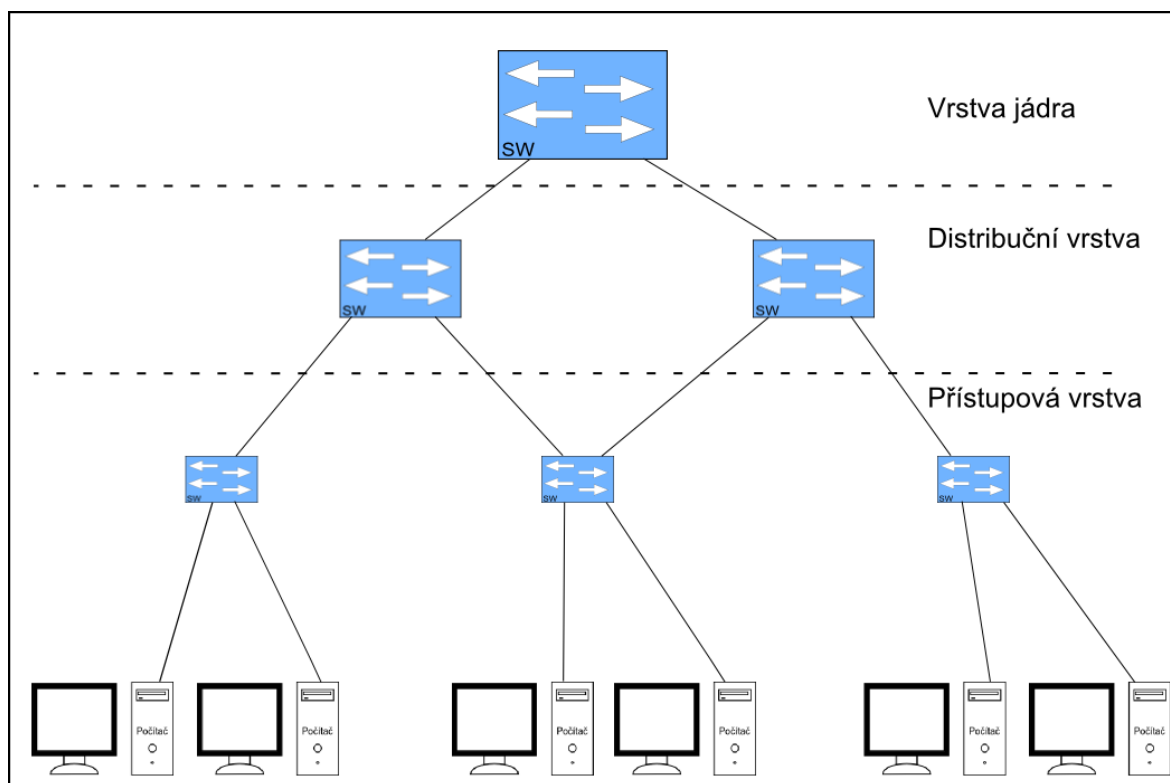
Tato vrstva poskytuje přístup pro uživatele, je to bod, kde data opouští síť a jsou posílána hostům v síti. Na této vrstvě jsou porty přiřazovány do jednotlivých VLAN (Virtual Local Area Network) sítí.

### 1.2.2 Distribuční vrstva

Tato vrstva slouží jako spojovací bod mezi přístupovou a vrstvou jádra. Zajišťuje směrování mezi jednotlivými VLAN sítěmi a kontrolu síťového provozu pomocí access control listů. K této vrstvě mohou být připojeny vzdálené pobočky přes síť WAN (Wide Area Network) či veřejnou síť Internet.

### 1.2.3 Vrstva jádra

Tato vrstva se stará o propojení jednotlivých distribučních vrstev, které mohou být umístěny v jednotlivých budovách firmy. Smyslem této vrstvy je co nejrychleji přepínat pakety a zajistit tak rychlou komunikaci mezi jednotlivými částmi směrované počítačové sítě. Tato vrstva sítě je připojena k veřejné síti Internet.



Obr. 2. Hierarchický model sítě.

### 1.2.4 Výhody hierarchického modelu

Rozšiřitelnost, která umožňuje dále zvětšovat síť. Odolnost a nadbytečnost, která zajišťuje lepší robustnost sítě a vylepšená bezpečnost sítě.

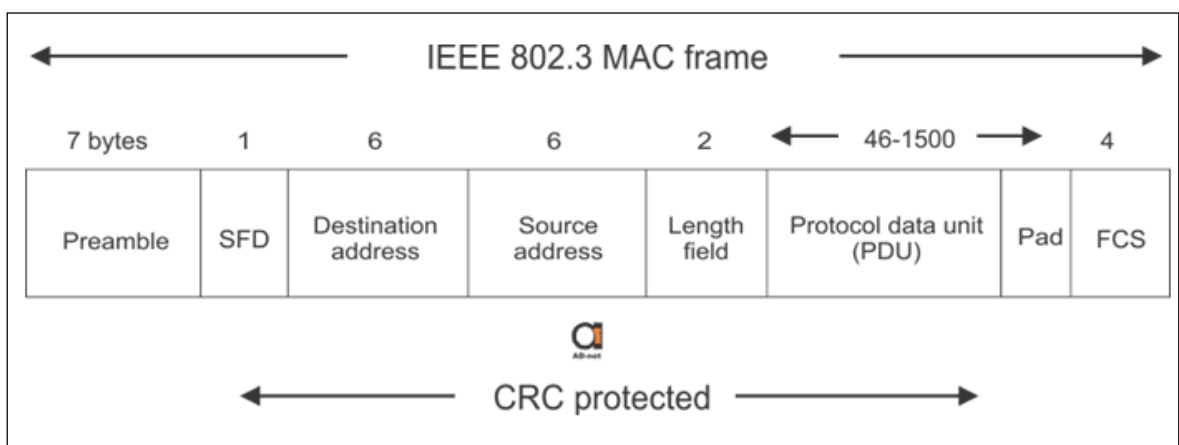
### 1.2.5 Kritéria pro výběr přepínačů

- Cena – Rozhodující faktor, odvíjí se od počtu portů, jejich rychlosti a nabízených funkcí.

- Rozšiřitelnost – Pevná konfigurace přepínače či možnost přidávání modulů.
- Přítomnost PoE (Power over Ethernet) – Přítomnost PoE portů, které nabízejí napájení přes kroucenou dvojlinku [4].

### 1.3 Přepínání rámců

Existují dvě metody na přepínání rámců Store-and-forward a Cut-through. K přepnutí (přeposlání rámce) ze vstupního portu na výstupní je třeba cílová MAC (Media Access Control) adresa, která určuje, na jaký port bude rámeček předán podle CAM (Content Addressable Memory) tabulky. V CAM tabulce je uloženo přiřazení MAC:port, kde se nachází daný host s danou MAC adresou.



Obr. 3. Ethernet rámeček.

- Preamble, SFD – Indikuje začátek rámce.
- Destination address – Cílová MAC adresa.
- Source address – Zdrojová MAC adresa.
- Length field – Délka celého rámce.
- PDU (Protocol Data Unit) – Vlastní náklad rámce (paket).
- FCS (Frame Check Sequence) – Kontrolní součet.

#### 1.3.1 Metoda Store-and-forward

Je metoda, při které je celý rámeček uložen ve vyrovnávací paměti přepínače, je zkontrolován jeho FCS pro nechybovost rámce a rámeček je následně přeposlán na odchozí port na základě údajů v CAM tabulce.

Rámce, které neprojdou kontrolním součtem, jsou vyřazeny. Při příchodu do přepínače jsou uloženy do vyrovnávací paměti, při odchodu jsou poslány do vyrovnávací paměti odchozího portu. To zajišťuje vyrovnávání rozdílů rychlostí mezi linkami. Například rychlá příchozí linka 1 Gb/s a pomalejší odchozí 100 Mb/s

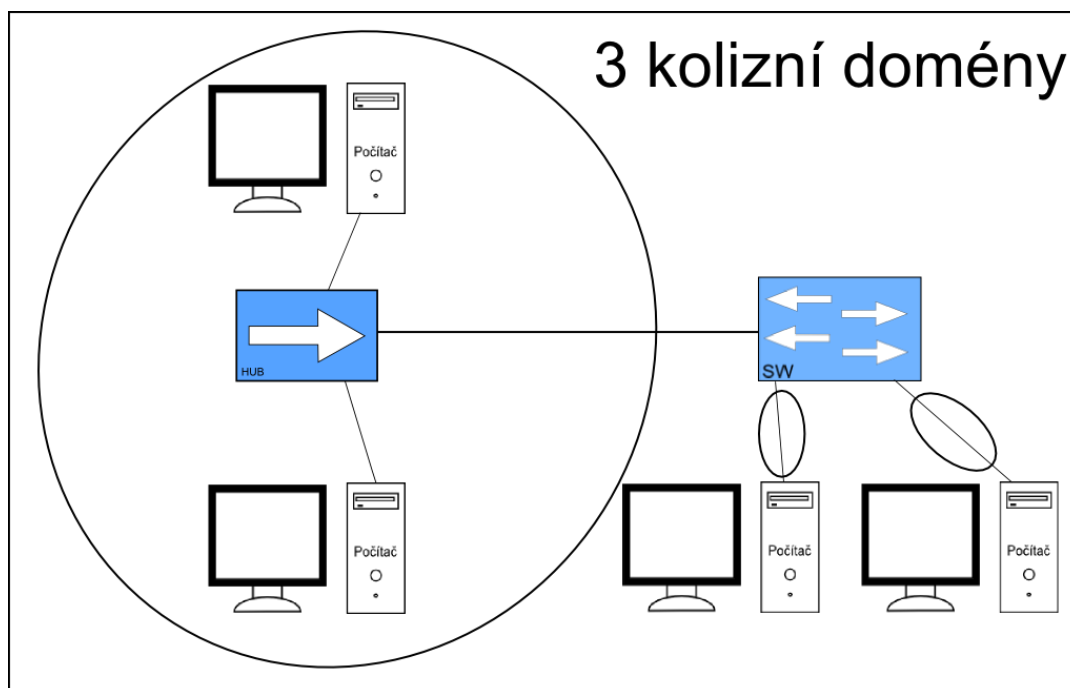
### 1.3.2 Metoda Cut-through

Je metoda při, které se nečeká, až je rámec celý přijat přepínačem. Po přijetí cílové MAC adresy se údaj vyhledá v CAM tabulce a rámec se začne přeposílat k cílovému hostu. Přepínače u této metody nekontroluje FCS, proto mohou být přeposlány vadné rámce.

## 1.4 Domény

### 1.4.1 Kolizní doména

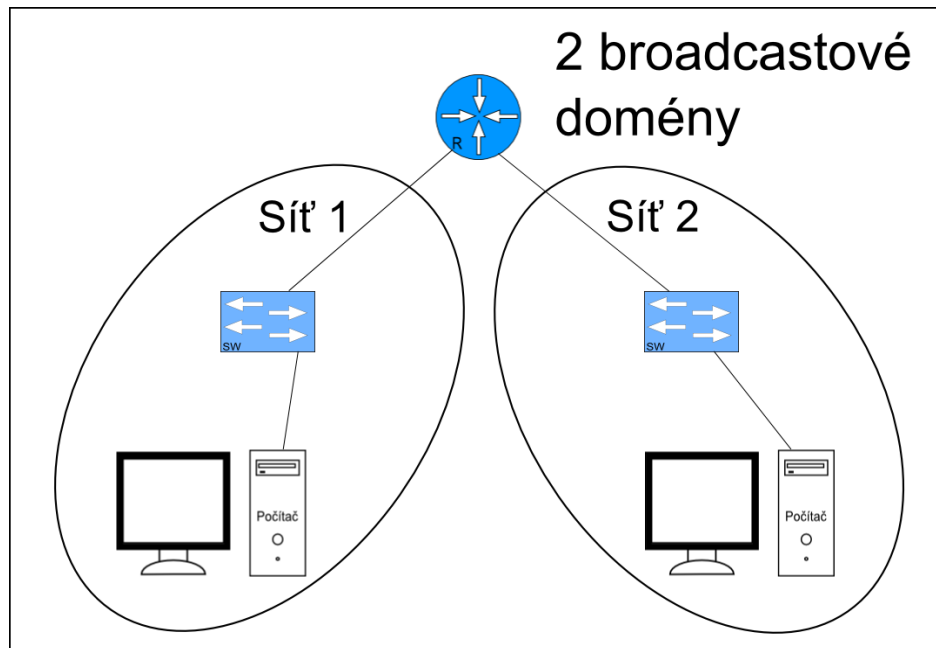
Je část sítě, ve které může dojít ke kolizi. Tato část sítě je sdílena více síťovými zařízeními, které jsou umístěny ve stejné části sítě. Zařízení v této části sítě naslouchají na přenosovém médiu a čekají, až bude prázdné, aby mohli vysílat. Hub je síťové zařízení, které nedělí kolizní doménu a pracuje na první vrstvě modelu ISO/OSI (ISO's Open Systems Interconnect). Hub pouze přepoše bity z příchozího portu na všechny ostatní. Přepínač je síťové zařízení, které dělí kolizní doménu a pracuje na druhé vrstvě modelu ISO/OSI. Přepínač, tedy umožňuje hostům svobodně vysílat. Příchozí rámec je přeposlán (přepnut) pouze k danému hostu, pro kterého je rámec určen. Nedochozí k zahlcování sítě zbytečným přepínáním rámců na porty, pro které rámce nejsou určeny.



Obr. 4. Kolizní doména.

### 1.4.2 Broadcastová doména

Je část sítě, ve které jsou všichni hosti schopni přijímat broadcastové vysílání. Přepínače filtrují rámce na základě MAC adresy, nicméně nefiltrují broadcastové rámce. Pro tento účel slouží v síti zařízení zvané směrovač. Směrovač je zařízení, které nepřeposílá broadcastové rámce. Směrovač dělí broadcastovou i kolizní doménu.



Obr. 5. Broadcastová doména.

## 2 ZÁKLADY PŘEPÍNÁNÍ A KONFIGURACE PŘEPÍNAČŮ

K přepínači či směrovači se lze připojit lokálně skrz konzolový port či vzdáleně přes telnet či SSH (Secure SHell). Jak se připojit k přepínači pomocí konzolového portu je popsáno v praktické úloze 1.

### 2.1 Struktura paměti zařízení Cisco

- ROM (Read Only Memory ) – Zde je uložen zavaděč.
- RAM (Random Access Memory) – Zde je načten právě běžící IOS a také running-config.
- FLASH – Zde jsou uloženy soubory včetně IOS obrazu.
- NVRAM – Zde je uloženo startup-config.

### 2.2 Konfigurační módy zařízení Cisco

*Tab. 1. Konfigurační módy zařízení Cisco.*

User Exec	Privileged Exec	Global conf. mode	Interface mode, lines mode
switch>	switch#	switch(config)#	switch(config-if)# switch(config-line)# router(config-router)#

- **User Exec** – Mód, ve kterém jdou zobrazovat informace o zařízeních Cisco.
- **Privileged Exec** – Mód, ve kterém je více možností pro zobrazování různých informací o zařízeních Cisco.
- **Global conf. Mode** – Mód, ve kterém lze upravovat globální nastavení na zařízeních Cisco.
- **Ostatní módy** – Interface mode, line mode atd... módy, ve kterých se nastavují parametry jednotlivých součástí zařízení Cisco. Například nastavení portů, linek pro vzdálený přístup apod [2].

### 2.3 Základní bootovací sekvence přepínače

Po zapnutí přepínače do elektrické sítě se spustí test POST (Power On Self Test), který provádí kontrolu hardwaru přepínače. Tento program je uložen v paměti ROM. Následně je spuštěn zavaděč, který je také uložen v paměti ROM. Tento zavaděč provede inicializaci procesoru, jeho registrů a paměti FLASH ve které je uložen obraz operačního systému IOS (Internetwork Operating System). Zavaděč nakonec načte tento operační systém do RAM podle cesty k obrazu tohoto operačního systému [5].

Příkazy týkající se bootování:

**prepinac(config)# BOOT SYSTEM flash:/název obrazu operačního systému**

Nastavení cesty k obrazu IOS.

**prepinac# SHOW BOOT**

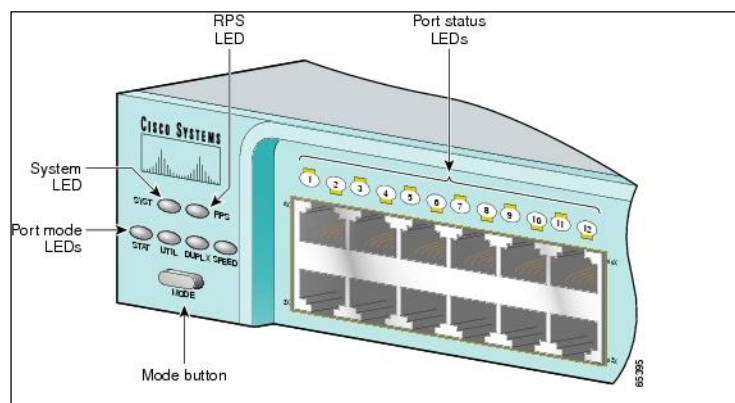
**prepinac# SHOW BOOTVAR**

Ověření cesty k obrazu IOS.

## 2.4 Stavové diody na přepínači

Na přední liště přepínače jsou Stavové diody, které ukazují stav portů na přepínači. Je zde přepínací tlačítko MODE, kterým je možno mezi těmito stavy přepínat. Diody nad porty pak ukazují zvolenou informaci. Tyto diody se liší podle přepínače. V tomto příkladu je použit přepínač Cisco 2950.

- SYST – Zobrazuje stav přepínače. Pokud tato dioda nesvítí, systém není zapojen do elektrické sítě. Pokud je zelená, přepínač pracuje správně. Pokud je oranžová, přepínač nepracuje správně.
- STAT – Zobrazuje stav portů na přepínači. Pokud dioda nad portem nesvítí, není připojen kabel. Pokud svítí stále zeleně, na port je připojen kabel. Pokud problikává zeleně, port přijímá a odesílá rámce. Pokud je dioda oranžová, port nepřepíná rámce. Například z důvodu STP (Spanning-Tree Protocol) a zamezení smyčky.
- UTIL – Zobrazuje využití propustnosti portu.
- DUPLX – Zobrazuje zdali jsou porty v half-duplex nebo ve full-duplex módu. Pokud dioda nad portem nesvítí, port pracuje v half-duplex. Pokud dioda svítí zeleně, port pracuje ve full-duplex módu.
- SPEED – Zobrazuje jakou propustnost má port. Pokud nesvítí, port běží rychlostí 10 Mb/s. Pokud svítí stále zeleně, port běží rychlostí 100 Mb/s. Pokud bliká zeleně, port běží rychlostí 1000 Mb/s [7].



Obr. 6. Přední panel přepínače Cisco 2950 [7].

## 2.5 Vzdálený přístup přes Telnet

Tento přístup je používán tehdy, když je třeba se na přepínač přihlásit vzdáleně z lokální či vzdálené sítě. Jelikož přepínač je zařízení pracující na L2 a pro vzdálený přístup je třeba IP (Internet Protocol) adresa a maska podsítě, je třeba nakonfigurovat SVI (Switch Virtual Interface), které slouží, jako virtuální port na který je možno se vzdáleně přihlásit. SVI jsou svázány s VLAN sítěmi, což je logická LAN. VLAN síť je virtuální LAN do které je možno přiřazovat porty přepínače. Tyto porty se pak tváří, že jsou součástí této VLAN sítě i přesto, že jsou tyto porty fyzicky umístěny na jiných přepínačích. VLAN 1 je výchozí VLAN síť pro správu přepínače. Ve výchozím nastavení jsou všechny porty přiřazeny do VLAN 1. Z bezpečnostních důvodů je však lepší pro VLAN síť určenou pro správu použít jinou VLAN než 1.

Pro konfiguraci vzdáleného přístupu bude zde použito VLAN 1, jelikož ta je již na přepínači vytvořena a také je k ní přiřazen alespoň 1 port. Připojení je realizováno pomocí protokolu telnet. Pro vzdálený přístup je nutno vytvořit VLAN síť a této VLAN síti přiřadit alespoň jeden port. Následně je třeba pro vzdálený přístup nakonfigurovat SVI, kterému je přiřazena IP adresa a maska. Také je nutno nakonfigurovat heslo pro privilegovaný mód, heslo pro vty lines a zvolit metodu vzdáleného přístupu.

Příkazy pro konfiguraci telnetu:

```
prepinac(config)# INTERFACE VLAN číslo vlanu  
prepinac(config-if)# IP ADDRESS ip_adresa maska
```

Vytvoření SVI pro VLAN.

```
prepinac(config)# LINE VTY 0 15  
prepinac(config-line)# PASSWORD heslo  
prepinac(config-line)# TRANSPORT INPUT TELNET  
prepinac(config-line)# LOGIN
```

Konfigurace vty lines, heslo, typ vzdáleného přístupu a autorizace heslem.

```
prepinac(config)# IP DEFAULT-GATEWAY ip_adresa
```

Konfigurace výchozí brány pro přístup ze vzdálené sítě.

## 2.6 Nastavení portů na přepínači

Každému portu je možno změnit určité parametry, které ovlivňují jeho vlastnosti.

### 2.6.1 Jednosměrná a obousměrná komunikace

Half-duplex – Přijímací a odesílací kanál je stejný.

Full-duplex – Je zde samostatný vysílací a přijímací kanál. Data mohou proudit obousměrně zároveň. Nedochozí zde ke kolizím.

```
prepinac(config-if)# DUPLEX {FULL/HALF}
```

Konfigurace *FULL* nebo *HALF* duplex režimu.

### 2.6.2 Rychlost portu

```
prepinac(config-if)# SPEED {10/100/1000/AUTO}
```

Nastavení rychlosti portu, kde *10* je 10 Mb/s, *100* je 100 Mb/s, *1000* je 1000 Mb/s a *AUTO* je automatická detekce.

### 2.6.3 Auto-MDIX

Pokud je třeba propojit přepínač s přepínačem či počítač se směrovačem je nutno použít křížený kabel. S vlastností auto-mdix, ale toto již není třeba. Tento příkaz umožňuje použít jakýkoliv kabel na propojení a zařízení se přizpůsobí:

Auto-MDIX lze nastavit:

```
prepinac(config-if)# MDIX AUTO
```

*AUTO* značí automatickou detekci.

```
prepinac# SHOW CONTROLLERS ETHERNET-CONTROLLER port  
PHY / Auto-MDIX
```

Ověření nastavení MDIX.

## 2.7 Ověřování nastavení zařízení Cisco

Zařízení Cisco nám nabízí mnoho příkazů, které lze použít pro ověření nastavení zařízení Cisco, prohlédnutí si statistik provozu či příkazy, kterými je možno zkoumat co právě zařízení Cisco dělá.

**prepinac# SHOW INTERFACES { port / nic }**

Příkaz pro ověření nastavení na druhé linkové vrstvě včetně statistik o přenosu dat. Při zadání portu se zobrazí informace pouze pro daný port, při zadání ničeho se zobrazí všechny porty.

**prepinac# SHOW STARTUP-CONFIG**

Zobrazí aktuální startup-config.

**prepinac# SHOW RUNNING-CONFIG**

Zobrazí aktuální running-config.

**prepinac# SHOW FLASH**

Zobrazí obsah paměti flash.

**prepinac# SHOW VERSION**

Zobrazí informace o zařízení, aktuální použitý IOS a jiné.

**prepinac# SHOW HISTORY**

Zobrazí poslední zadané příkazy.

**prepinac# SHOW IP INTEFACE *port***

Zobrazí informace o portu pro třetí síťovou vrstvu.

**prepinac# SHOW MAC-ADDRESS-TABLE**

**prepinac# SHOW MAC ADDRESS-TABLE**

Zobrazí MAC tabulku [3].

## 2.8 Řešení problémů na fyzické a linkové vrstvě

Při řešení problémů se sítíovou infrastrukturou je důležité rozpoznat na které vrstvě je problém, který je hledán. Nejdříve je zde uveden výstup z přepínače:

```
AccessSW#show interfaces fastEthernet 0/1
FastEthernet0/1 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 000f.23ef.2ec1 (bia 000f.23ef.2ec1)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 100BaseTX
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    11629 packets input, 932864 bytes, 0 no buffer
    Received 9147 broadcasts (8795 multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 8795 multicast, 0 pause input
    0 input packets with dribble condition detected
  8946 packets output, 801999 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

Obr. 7. Výstup z přepínače.

Tento výstup byl získán pomocí příkazu **SHOW INTERFACES { port / nic }**. Zobrazuje informace o první a druhé sítíové vrstvě. Z prvního řádku je možno vyčíst zdali je problém na první vrstvě *FastEthernet0/1 is down*. Například špatný kabel. Pokud je problém na druhé sítíové vrstvě, ve výpisu je *FastEthernet0/1 up, line protocol is down*. Například nenastavený clock rate u směrovače či špatné rychlosti a duplex na koncích kabelu. Pokud je ve výpisu *FastEthernet0/1 is administratively down, line protocol is down*, znamená to, že port je administrativně vypnut pomocí příkazu **SHUTDOWN**. Pokud je zde *FastEthernet0/1 up, line protocol is up* problém s komunikací se nevyskytuje na fyzické ani linkové vrstvě.

Ve výpisu lze také vidět statistiku přepnutých rámců. Některé z nich zde budou uvedeny a vysvětleny:

- Runts – Rámce, které byly menší než minimální velikost 64 B.
- Giants – Rámce, větší než 1518 B.
- No buffer – Pokud toto číslo stoupá, znamená to, že vyrovnávací paměť na portech je plná.

- Input Errors – Celkový součet všech špatně přijatých, vadných a jiných nějakým způsobem nevyhovujících rámců.
- CRC (Cyclic Redundancy Check) – Rámce, u kterých nesouhlasil CRC.
- Frame – Pokud jsou přijmuty vadné rámce, nekompletní či dojde ke kolizi, toto číslo se inkrementuje.
- Packet Outputs – Celkový počet úspěšně přeposlaných paketů [5].

## 2.9 Vzdálený přístup přes SSH

Vzdálené připojení přes telnet je nešifrované a je tedy možné heslo odchytil pomocí snifovacího software WireShark. To je důvod proč používat SSH, které je šifrované.

Pro vygenerování šifrovacího klíče je třeba nastavit hostname přepínače a doménové jméno.

Nastavení SSH:

```
prepinac(config)# IP DOMAIN-NAME doménové_jméno
```

Nastavení doménového jména.

```
prepinac(config)# CRYPTO KEY GENERATE RSA
```

Vygenerování klíčového páru.

```
prepinac(config)# USERNAME uživ_jméno PASSWORD heslo
```

Pro vytvoření uživatelského účtu v lokální databázi na přepínači.

Příkazy potřebné pro nastavení vty lines:

```
prepinac(config-line)# TRANSPORT INPUT SSH
```

```
prepinac(config-line)# LOGIN LOCAL
```

*LOCAL* – heslo má být použito to, které je nakonfigurované v lokální databázi.

```
prepinac(config)# IP SSH VERSION 2
```

Příkaz pro upřesnění verze SSH [5].

Funkčnost SSH lze ověřit pomocí připojení přes program Putty, kde je zvoleno pomocí SSH.

Je možné také ověřit pomocí:

```
prepinac# SHOW SSH
```

```
prepinac# SHOW IP SSH
```

## 2.10 Bezpečnost přepínačů

### 2.10.1 Typy bezpečnostních děr a útoků

Zaplavování MAC tabulky – MAC tabulka v každém přepínači je omezené velikosti. Když je tato tabulka zaplavena rámci s falešnými MAC adresami nezbyde zde místo na hosty, kteří jsou oprávněnými uživateli v síti.

Využití všech IP adres od DHCP (Dynamic Host Configuration Protocol) serveru – DHCP server nabízí omezené množství IP adres, pokud se v síti objeví záškodník, začne posílat falešné DHCP požadavky za účelem vyplývání všech dostupných IP adres. Následně nezbyde žádná IP adresa pro oprávněné hosty.

Falešný DHCP server – Po provedení prvního zneužití DHCP serveru záškodník vytvoří svůj vlastní DHCP server a začne nabízet tyto služby oprávněným klientům.

Zneužití protokolu CDP (Cisco Discovery Protocol) – CDP je firemní protokol Cisca, který slouží k poskytování informací o sousedních zařízeních. Je nešifrovaný a ve výchozím nastavení je povolen. Záškodník může tyto rámce odchytil a zjistit z nich informace o sousedech. Může také poslat do sítě rámce s falešnými informacemi o sousedech.

Brute Force attack – Jedná se o útok, kdy záškodník zkouší všechny možné kombinace hesel, aby získal přístup k zařízení [8].

### 2.10.2 Obrana proti útokům

Proti útokům je možno se bránit:

```
prepinac(config-if)# SHUTDOWN
```

Vypnutí nepoužívaných portů.

Obrana před zneužitím DHCP:

**prepinac(config-if)# IP DHCP SNOOPING TRUST**

Po nastavení tohoto příkazu, bude pouze tento port posílat odpovědi na DHCP požadavky. Porty, které jsou untrusted mohou pouze posílat požadavky.

**prepinac(config-if)# IP DHCP SNOOPING LIMIT RATE** *počet\_povol  
ných\_dhcp\_zprāv\_za\_1\_s*

Tento příkaz říká, že přes daný port může být přeposláno jenom určitý počet DHCP zpráv.

### 2.10.3 Port security

Je vlastnost, která porty zabezpečuje před použitím falešné MAC adresy. Lze nastavit maximální počet povolených MAC adres na port. Lze také nastavit pouze jednu povolenou MAC adresu na port. Dále je možno nastavit co se stane po porušení těchto pravidel.

Nastavení port security:

**prepinac(config-if)# SWICHPORT PORT-SECURITY**

Aktivace vlastnosti port security.

**prepinac(config-if)# SWICHPORT PORT-SECURITY MAC-ADDRESS** *mac\_ad-  
resa*

Nastavení jedné povolené MAC adresy.

**prepinac(config-if)# SWICHPORT PORT-SECURITY MAXIMUM** *počet\_povo-  
lených\_MAC\_adres*

Nastavení limitu povolených MAC adres.

**prepinac(config-if)# SWICHPORT PORT-SECURITY VIOLATION**  
{*PROTECT/RESTRICT/SHUTDOWN*}

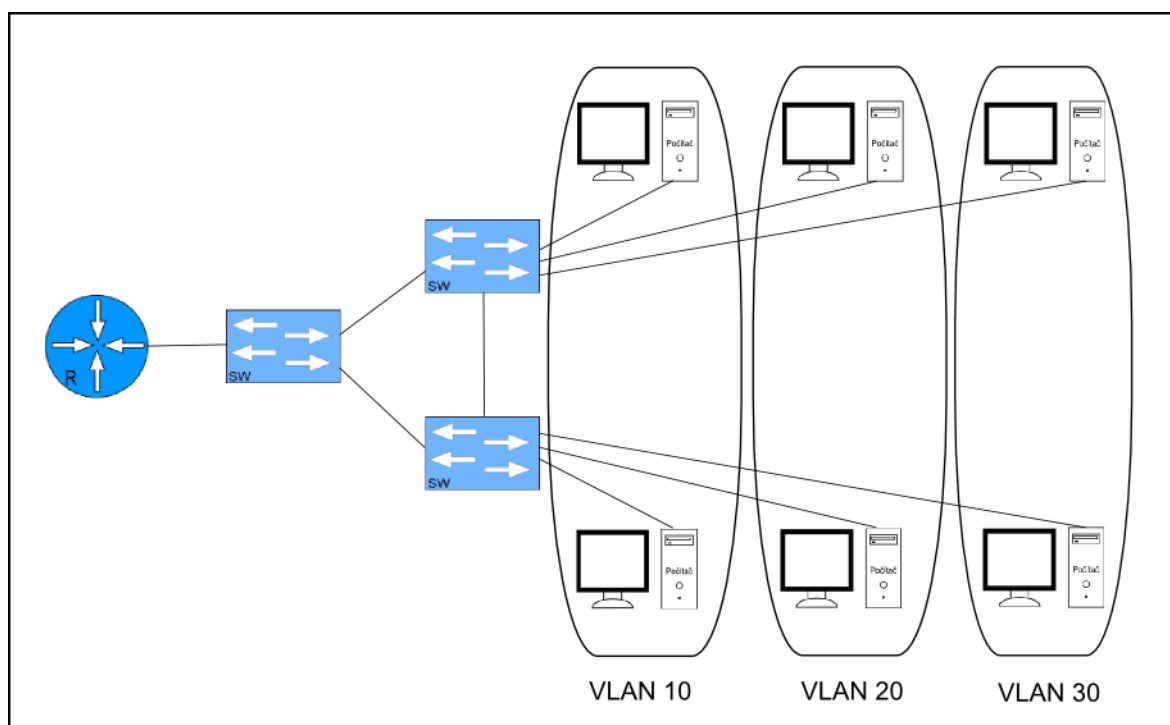
- *PROTECT* mód – Při porušení, může povolená MAC adresa stále vysílat.
- *RESTRICT* mód – Pomocí SNMP protokolu se pošle upozornění o porušení.
- *SHUTDOWN* mód – Při porušení se port vypne.

**prepinac# SHOW PORT-SECURITY INTERFACE** *port*

Pro ověření nastavení port security na daném portu [3].

### 3 VLAN

Virtuální lokální síť slouží pro separaci broadcastových domén a rozdělení hostů podle účelu podsítě. Umožňuje seskupovat počítače připojené na jeden či více přepínačů bez ohledu na to, kde jsou umístěny a do kterého přepínače jsou připojeny. Pokud jsou hosté součástí VLAN sítě, chovají se jako klasická síť LAN, která by byla připojená k jednomu přepínači a všechny počítače by byli součástí stejné LAN. Porty, na které jsou připojeni hosti, se nazývají access porty a porty, které přenášejí rámce z více VLAN sítí, jsou nazývány trunk porty. Trunk port každý rámec označí příslušným ID VLAN. Každá VLAN síť má svoji vlastní podsíť a vlastní rozsah IP adres, stejně jako LAN.



Obr. 8. VLAN síť.

#### 3.1 Typy VLAN

Existuje několik typů VLAN sítí podle jejich specifického účelu.

##### 3.1.1 Datová VLAN

Je typ VLAN sítě, která je určena pro přenos uživatelského obsahu. Do této VLAN sítě patří uživatelé.

### 3.1.2 Výchozí VLAN

Je výchozí VLAN síť do které patří všechny porty, pokud není nastaveno jinak. Každý port přepínače musí patřit do nějaké VLAN sítě. Její účel je také pro přenos řídicích informací protokolů jako CDP a VTP (VLAN Trunk Protocol). Tato VLAN síť nemůže být smazána ani přejmenována. Nedoporučuje se používat pro nic jiného než pro informace řídicích protokolů.

### 3.1.3 Nativní VLAN

Je typ VLAN sítě, který je přiřazen trunk portům. Její hlavní účel je přenášet rámce, které pocházejí od hostů, které nejsou členy žádné VLAN sítě a také rámce, které pocházejí ze zařízení, které nepodporují VLAN sítě. Rámce, které přicházejí od hostů, kteří jsou členy nativní VLAN sítě, od hostů bez podpory VLAN sítí a od hostů, kteří nejsou členy žádné VLAN sítě nejsou označeny při odchodu z trunk portu. Do všech ostatních rámců při odchodu z trunk portu je přidáno číslo VLAN sítě jako identifikátor. Ve výchozím nastavení je nativní VLAN síť výchozí VLAN sítí. Nedoporučuje se používat VLAN 1 jako nativní VLAN síť.

### 3.1.4 VLAN pro správu

Je VLAN síť, která se používá pro správu přepínačů. Aby bylo možné se vzdáleně přihlásit k přepínači přes telnet či SSH, je třeba konfigurovat SVI a k němu příslušnou IP adresu z podsítě která je asociována s VLAN sítí pro správu. VLAN síť pro správu může být jakákoliv VLAN síť. Je doporučeno nepoužívat VLAN 1 jako VLAN síť pro správu sítě.

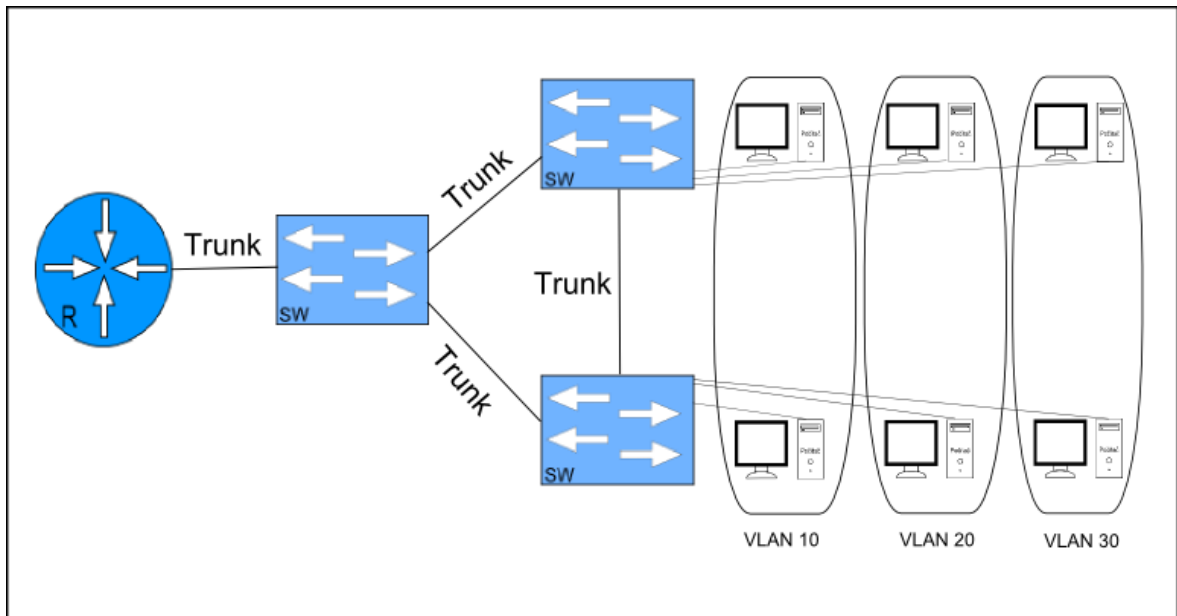
### 3.1.5 VLAN pro VoIP

Je specifická VLAN síť použita pro přenos VoIP komunikace. Pro tuto VLAN síť je nutné, aby splňovala požadavky na kvalitní přenos zvuku. Těmi jsou nízká odezva, směrování přes síť i když je ucpána, zajištění minimální velikosti vysílacího pásma a priority nad ostatními druhy provozu [8].

## 3.2 Trunk a označování rámců

VLAN Trunk je vlastnost portů, která se používá pro propojení portů přepínačů na místech, kde je třeba, aby spojení přenášelo data z více než jenom jedné VLAN sítě. Pro

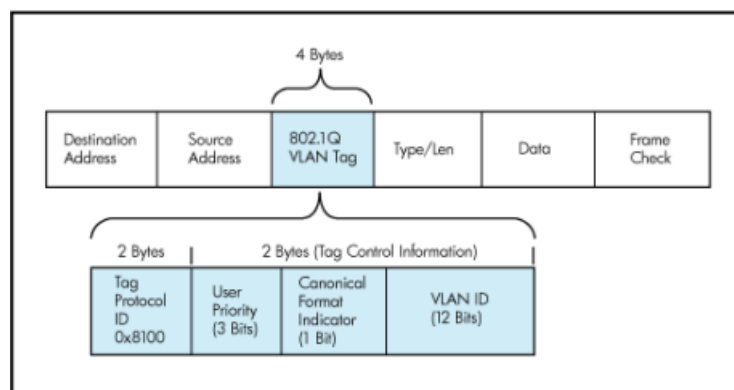
označování rámců, podle toho z jaké VLAN sítě pochází je použit protokol IEEE (Institute of Electrical and Electronics Engineers) 801.1Q. Tento protokol přidává do hlavičky rámce informace o tom do jaké VLAN sítě daný rámec patří. K tomuto označování dochází na trunk portech.



Obr. 9. Trunk spojení mezi zařízeními, které potřebují přenášet data z více než jedné VLAN sítě.

### 3.2.1 Označování rámců pomocí 802.1Q

Když přijde rámec z určité VLAN, než je odeslán k jinému přepínači je označen 4 B tagem, který říká do jaké VLAN sítě tento rámec patří, aby mohl být na cílovém přepínači přepnut do správné VLAN sítě. K označování dochází na trunk portech. Do trunku lze port přiřadit příkazem. Všechny rámce kromě těch, které pochází z nativní VLAN sítě a zařízení, které nepodporují tagování jsou označeny tímto tagem.



Obr. 10. 802.1Q rámec [9].

- Tag protocol ID – Identifikátor protokolu 802.1Q.
- User priority – Stanovuje prioritu rámce.
- Canonical Format Identifier – Nutné pro podporu Token Ringu.
- VLAN ID – Číslo VLAN do které rámec patří.

### 3.3 Konfigurace VLAN

Výchozí je VLAN 1. VLAN sítě dostupné v normálním rozsahu jsou od 1 do 1005. Rozšířený rozsah je od 1006 do 4494. VLAN 1002 až 1005 jsou rezervovány pro Token Ring a FDDI (Fiber Distributed Data Interface) [2]. Rozšířený rozsah nepodporuje protokol VTP pro šíření informací o VLAN sítích mezi přepínači. Informace o VLAN sítích jsou uloženy v souboru vlan.dat v paměti FLASH.

#### 3.3.1 Vytvoření VLAN

Pro vytvoření VLAN sítě jsou třeba následující příkazy:

```
prepinac(config)# VLAN číslo_vlan
```

```
prepinac(config-vlan)# NAME jméno
```

Pro smazání VLAN sítě musí být zadání **NO VLAN**. Nebo také smazáním souboru vlan.dat pomocí: **DELETE FLASH: vlan.dat**.

#### 3.3.2 Přiřazení portu do správného módu

Při konfiguraci je důležité zařadit port do správného módu, podle toho zdali se jedná o port, ke kterému jsou připojeni hosti, či port, který přenáší data z více VLAN sítí. Mód, který je použit pro hosty se nazývá access mód. Mód, který je používán pro přenos dat z více VLAN sítí se nazývá trunk.

Je také nutné zařadit port do správné VLAN sítě.

Přiřazení do access módu:

```
prepinac(config-if)# SWITCHPORT MODE ACCESS
```

```
prepinac(config-if)# SWITCHPORT ACCESS VLAN číslo_vlan
```

Pokud je třeba odstranit přiřazení k určité VLAN síti, před přiřazovací příkaz se přidá slovo **NO**.

Přiřazení do trunk módu:

**prepinac(config-if)# SWITCHPORT MODE TRUNK**

**prepinac(config-if)# SWITCHPORT MODE TRUNK NATIVE VLAN číslo\_vlan**

Přiřazení do nativní VLAN sítě.

**prepinac(config-if)# SWITCHPORT TRUNK ALLOWED VLAN čísla\_vlan\_síť**

Povolení, které VLAN sítě mohou být přenášeny přes trunk spojení.

**prepinac(config-if)# NO SWITCHPORT TRUNK ALLOWED VLAN**

Pro povolení přenosu všech VLAN sítí.

**prepinac(config-if)# NO SWITCHPORT TRUNK NATIVE VLAN**

Jako nativní VLAN síť nastaví výchozí VLAN 1.

### 3.3.3 Ověření nastavení VLAN sítí

Příkazy sloužící pro ověření správnosti nastavení.

**prepinac# SHOW INTERFACES port SWITCHPORT**

Zobrazí nastavení týkající se VLAN sítí pro daný port.

**prepinac# SHOW VLAN {BRIEF/ID číslo\_vlan/NAME jméno\_vlan/SUMMARY}**

*BRIEF* zobrazí všeobecné informace o VLAN sítích. Při použití *ID* či *NAME* se zobrazí informace o dané VLAN síti. *SUMMARY* zobrazí informaci o počtu existujících VLAN sítí.

**prepinac# SHOW INTERFACES TRUNK**

Zobrazí, které porty jsou v trunk módu [3].

### 3.4 DTP

DTP (Dynamic Trunking Protocol) protokol slouží k automatickému vyjednávání o tom, zdali daný port bude v módu trunk či ne. Je doporučeno ho nepoužívat a je lepší porty přímo přiřazovat do access či trunk módu. Tento protokol podporují jenom zařízení Cisco.

Tab. 2. Možné DTP módy a jejich výsledky [8].

Mód portu	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Omezené spojení
Access	Access	Access	Omezené spojení	Access

**prepinac(config-if)# SWITCHPORT MODE DYNAMIC AUTO**

**prepinac(config-if)# SWITCHPORT MODE DYNAMIC DESIRABLE**

Příkazy sloužící pro přiřazení do módů dynamic auto a dynamic desirable.

**prepinac(config-if)# SWITCHPORT NONEGOTIATE**

Vypne automatické vyjednávání o módech portů.

V tabulce jsou uvedeny, v modré části, do kterých módu je možné nastavit port. V bezbarvé části jsou módy, které se aktivují, pokud budou jednotlivé konce spojení nastaveny do daných módů. Například když jedna strana spojení je nastavena na dynamic desirable a druhá na dynamic auto, výsledný mód bude trunk.

## **3.5 Bezpečnost VLAN sítí**

### **3.5.1 Falešný přepínač**

V případě tohoto útoku záškodník předstírá, že je trunk port na přepínači. Když je druhá strana nastavena na dynamic auto, záškodník získá přístup ke všem VLAN sítím. Nej-jednodušší obranou je nastanovat do trunk režimu jenom ty porty u který je to nutné. V žádné případě nenastavovat na trunk či do módů, které trunk umožňují na uživatelských portech.

### **3.5.2 Falešný tag**

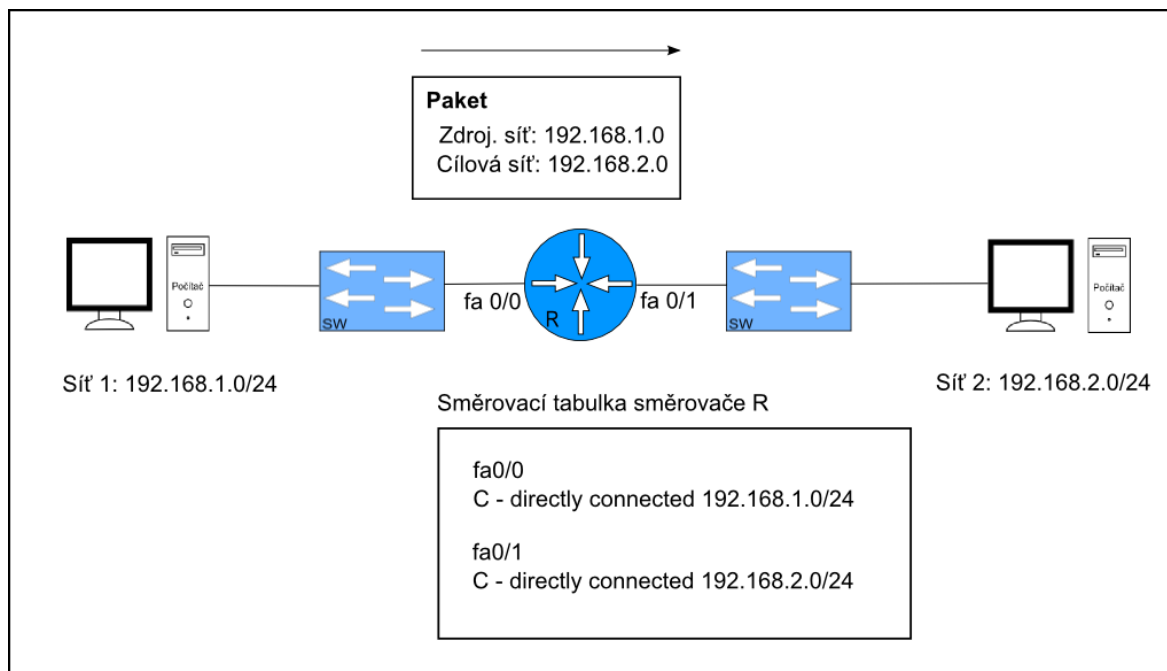
Je případ útoku, kdy záškodník, který je součástí nativní VLAN sítě přidá pod svoje oprávněné 802.1Q označení falešné 802.1Q označení pro jinou VLAN. Když rámec přijde na přepínač, označení pro nativní VLAN síť je odhozeno a rámec pokračuje co cílového přepínače. Zde přepínač zjistí, podle falešného označení, že rámec je určen pro jiného hosta. Obrana proti tomuto útoku je, aby žádný host nebyl součástí nativní VLAN sítě [5].

## 4 ÚVOD DO SMĚROVANÝCH SÍTÍ

Směrovač je zařízení v síti, které se stará o přeposílání paketů do jiné sítě. Této činnosti se říká směrování a provádí ji směrovač. Když paket přijde na směrovač a směrovač vidí, že tento paket patří do jiné sítě, nasměruje ho tam. Směrovač směřuje na základě cílové IP adresy. Přepínač naopak přepíná pakety v lokální síti a rozhoduje se na základě MAC adresy [2]. Hlavní účel směrovačů je propojovat sítě. Každá síť musí mít vlastní port na směrovači a patřit do vlastní IP sítě.

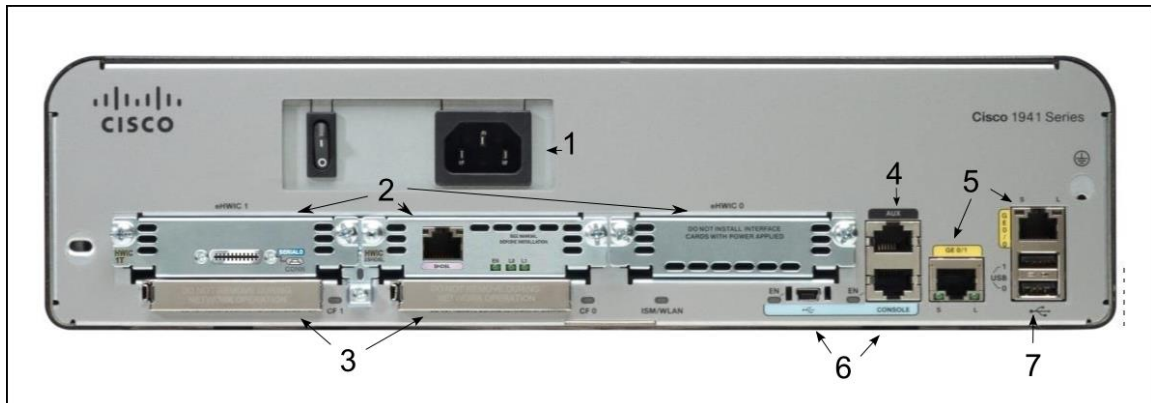
### 4.1 Směrování

Pokud paket nepatří do lokální sítě, přijde na směrovač. Port s IP adresou dané lokální sítě se nazývá brána. Směrovač se podívá na cílovou IP adresu a podívá do své směrovací tabulky, pokud najde shodu, nasměruje tento paket do správného portu. Směrovač se snaží najít v tabulce tu nejlepší cestu do cíle.



Obr. 11. Směrování paketu.

## 4.2 Směrovač a připojení



Obr. 12. Směrovač Cisco 1941 [10].

1. Napájení.
2. Sloty pro přídavné moduly.
3. Sloty pro FLASH paměť.
4. AUX (Auxiliary Port) port pro vzdálený přístup přes telefonní síť.
5. Gb Ethernet porty.
6. Console porty pro konfiguraci.
7. USB (Universal Serial Bus) porty.

Při vybalení směrovače či přepínače je třeba toto zařízení zapojit do zásuvky a zapnout ho. Následně je třeba připojit konzolový kabel do konzolového portu a pomocí Putty toto zařízení nakonfigurovat. Sloty pro přídavné karty jsou použity, pokud je nutno připojit ADSL připojení, sériové připojení a jiné. Jejich hlavní účel je rozšířit počet dostupných portů na směrovači.

## 4.3 Dokumentace sítě

Při tvorbě sítě skládající se z mnoha sítí je důležité tuto síť dokumentovat. Ve fyzické dokumentaci by mělo být uvedeno, kde jsou zařízení umístěna, typy kabelů, výrobci zařízení, typy konektorů a jiné. V logické dokumentaci by mělo být uvedeno, jaké porty jsou na jaké porty připojeny, IP adresy těchto portů, typ protokolu na druhé síťové vrstvě a jiné informace potřebné pro správnou orientaci v síti.

## 4.4 Základní konfigurace směrovače

Konfigurace základních věcí je stejná jako u přepínače. Rozdíl je v tom, že portům lze přiřadit IP adresa, jelikož směrovač je zařízení pracující na třetí síťové vrstvě.

Konfigurace IPv4 adresy pro port:

**smerovac(config)# INTERFACE** *port*

Portem může být fastEthernet, gigabyteEthernet, serial a jiné.

**smerovac(config-if)# IP ADDRESS** *ipv4\_adresa maska*

Přiřazení IPv4 adresy portu.

**smerovac(config-if)# NO SHUTDOWN**

Porty směrovače jsou ve výchozím nastavení vypnuté, proto je třeba aktivovat.

Port je možno pojmenovat pomocí příkazu **DESCRIPTION**.

Konfigurace IPv6 adresy pro port:

**smerovac(config)# INTERFACE** *port*

Portem může být fastEthernet, gigabyteEthernet, serial a jiné.

**smerovac(config-if)# IPv6 ADDRESS** *ipv6\_adresa/prefix*

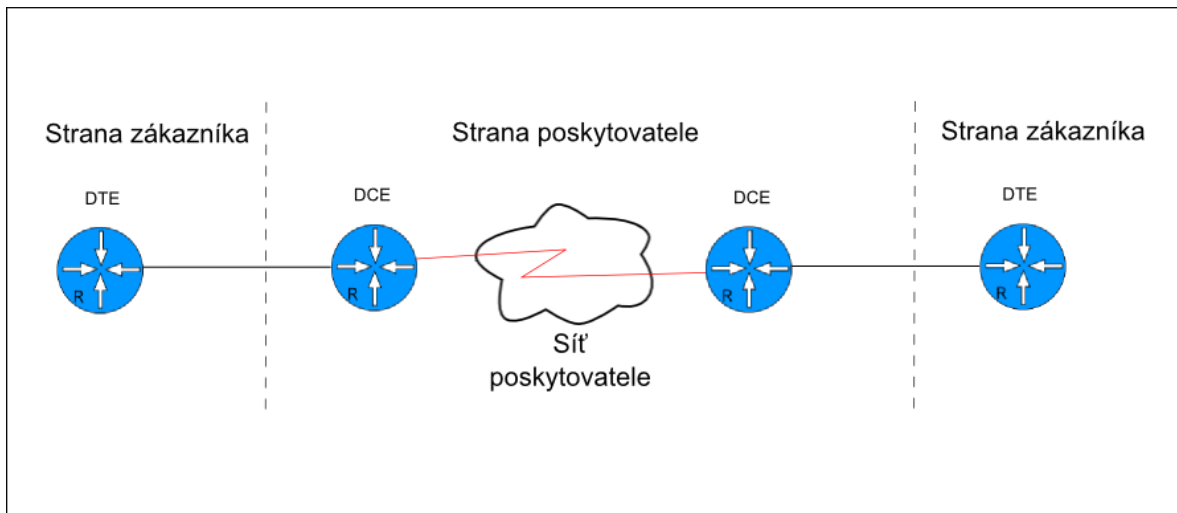
Přiřazení IPv6 adresy portu.

**smerovac(config-if)# NO SHUTDOWN**

Porty směrovače jsou ve výchozím nastavení vypnuté, proto je třeba aktivovat.

Port je možno pojmenovat pomocí příkazu **DESCRIPTION**.

## 4.5 DTE, DCE a clock rate



Obr. 13. DTE a DCE.

DTE (Data Termination Equipment) je směrovač, který vlastní zákazník poskytovatele, je to ukončení jeho sítě. Tento směrovač se napojuje na směrovač nazývaný DCE. Tento směrovač je majetek poskytovatele a připojuje DTE k síti poskytovatele.

DCE (Data Communications Equipment) poskytuje clock rate, což je omezení rychlosti pronajaté linky poskytovatelem. Je také důležitý pro synchronizaci, jelikož DTE konec spojení musí vědět, jak často má vyslat bit.

**smerovac(config)# INTERFACE SERIAL číslo**

**smerovac(config-if)# CLOCK RATE počet\_bitů\_za\_sekundu**

Pokud je CLOCK RATE nastaven na 64000 bitů. Je rychlost připojení 64 Kb/s. Směrovače také ví, že mají vyslat bit 1x za 1/64000 sekundy.

Tento příkaz je odlišný od příkazu BANDWIDTH, který udává rychlost linek pro výpočet nejlepších cest ve směrovacích protokolech, kdežto CLOCK RATE udává fyzickou rychlost spojení.

## 4.6 Loopback port

Je virtuální port, který je používán pro testování sítě, není svázan s žádným fyzickým portem.

**smerovac(config)# INTERFACE loopback číslo**

**smerovac(config-if)# IP ADDRESS ip\_adresa maska**

Příkazy pro konfiguraci loopback port.

## 4.7 Ověření konfigurace portů

Pro IPv4 adresu:

```
smerovac# SHOW IP INTERFACE BRIEF
```

Zobrazuje, zdali je port aktivní na 1 a 2 vrstvě a také nastavenou IPv4 adresu.

```
smerovac# SHOW IP ROUTE
```

Zobrazuje směrovací tabulku.

Pro IPv6 adresu:

```
smerovac# SHOW IPv6 INTERFACE BRIEF
```

Zobrazuje, zdali je port aktivní na 1 a 2 vrstvě a také nastavenou IPv6 adresu.

```
smerovac# SHOW IPv6 ROUTE
```

Zobrazuje směrovací tabulku [8].

## 4.8 Určení nejlepší cesty v síti

Když paket dorazí na port, je prohlédnuta jeho IP adresa. Pokud je nalezena shoda s přímo připojenými sítěmi je tento paket zaslán na daný odchozí port. Pokud se neshoduje přímo připojenými sítěmi, směrovač se podívá, zdali má ve směrovací tabulce záznam o vzdálené síti, pokud ano zašle paket tímto směrem. Pokud není nalezena shoda ani s přímo připojenou ani vzdálenou sítí, je paket odeslán do defaultní routy (výchozí cesta).

Nejlepší cesta k cíli se určuje pomocí metriky, což je speciální údaj, který sděluje jak je cesta výhodná. Směrovací protokol RIP (Routing Information Protocol) má jako metriku počet směrovačů v cestě. Jiné protokoly do metriky započítávají údaje jako rychlost spojení, zpoždění spojení, zatížení spojení a spolehlivost spojení.

## 4.9 Vyvažování zátěže

Pokud jsou v síti dvě cesty se stejnou metrikou. Směrovač příchozí pakety rovnoměrně rozdělí mezi tyto spojení. V angličtině se tato funkce nazývá load balancing a v češtině vyvažování zátěže.

## 4.10 Administrativní vzdálenost

Je číslo, které udává prioritu směrovacího protokolu. Pokud směrovač má nakonfigurováno více směrovacích protokolů a v každém se vyskytuje cesta do stejné sítě, je využit ten směrovací protokol, který má nižší administrativní vzdálenost.

Tab. 3. Administrativní vzdálenost [8].

Směrovací protokol	Administrativní vzdálenost
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

## 4.11 Typy naučení cest k sítím

### 4.11.1 Přímo připojené cesty

Jsou cesty k sítím, které se směrovač naučil přímo od svých připojených sítí.

### 4.11.2 Statické směrování

Je směrování, při kterém administrátor přímo vkládá cesty k sítím do směrovací tabulky manuálně.

### 4.11.3 Dynamické směrovací protokoly

Jsou protokoly, které učí směrovač o cestách k sítím dynamicky. Mezi tyto protokoly patří RIP, EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol) a jiné.

## 4.12 Výchozí cesta

Je cesta, do které budou směrovány všechny pakety, které mají cílovou IP adresu, která se neshoduje s ostatními cestami ve směrovací tabulce.

Výchozí cesta se také používá pro tzv. stub networks. Stub networks jsou sítě, které mají pouze jeden odchozí port a tím pádem jsou všechny pakety směrovány tímto směrem.

```
smerovac(config)# IP ROUTE 0.0.0.0 0.0.0.0 {odchozí port/ next-hop IP adresa}
```

Výchozí cesta pro IPv4.

```
smerovac(config)# IPv6 ROUTE ::/0 {odchozí port/ next-hop IP adresa}
```

Výchozí cesta pro IPv6.

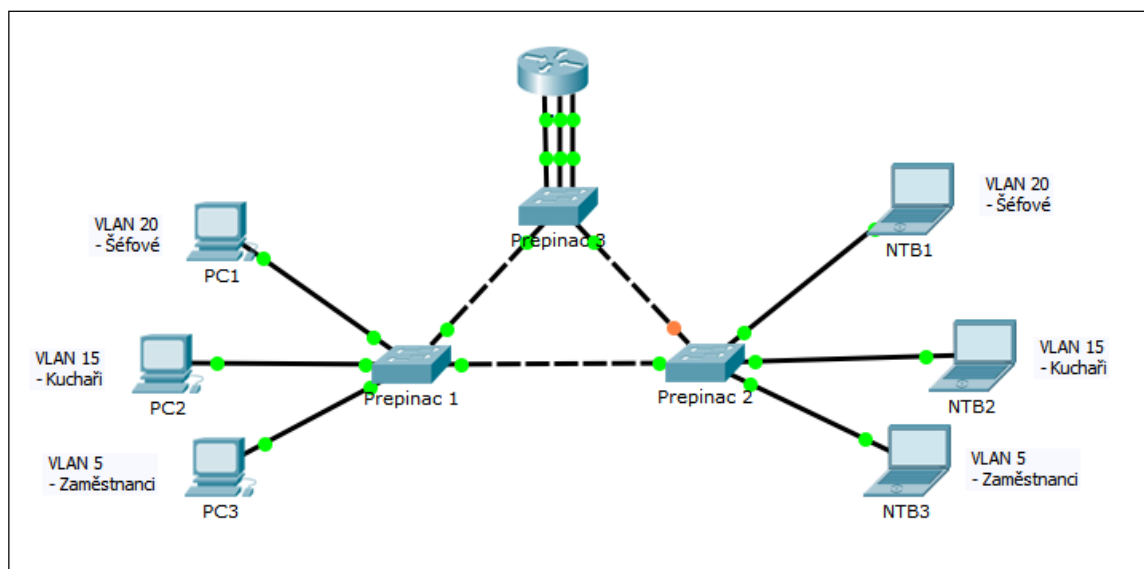
## 5 INTER-VLAN SMĚROVÁNÍ

Když je síť rozdělena pomocí VLAN, tyto sítě jsou stejné jako LAN sítě. Je mezi nimi třeba směrovat, aby bylo možno komunikovat. Toho lze docílit použitím směrovače a nebo L3 přepínače. Toto směrování mezi VLAN sítěmi se nazývá Inter-VLAN směrování.

### 5.1 Typy Inter-VLAN směrování

#### 5.1.1 Zastaralé Inter-VLAN směrování

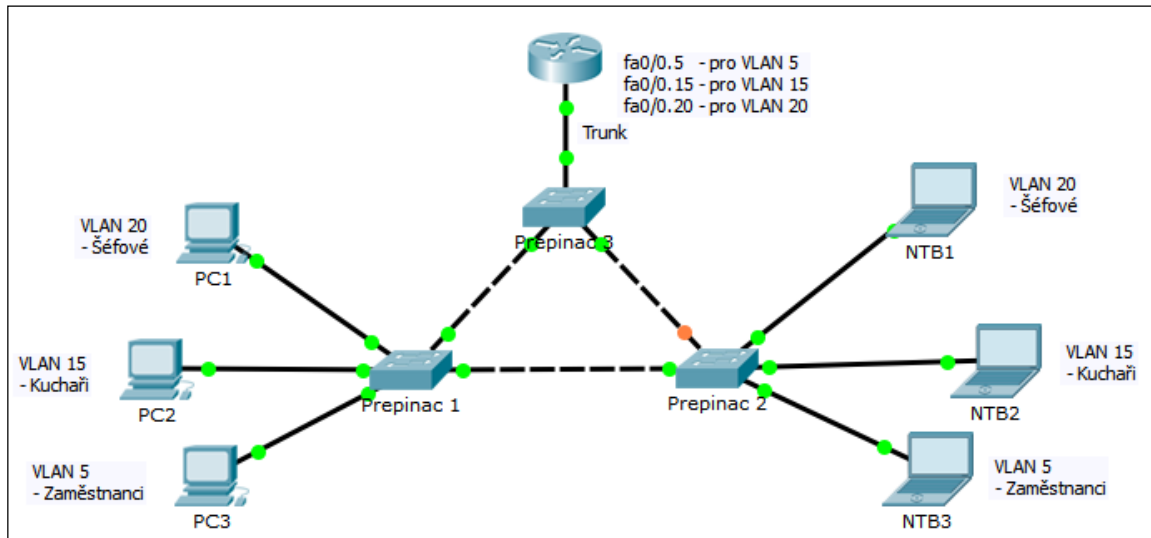
Je způsob směrování mezi VLAN sítěmi. Je založené na tom, že v síti je přítomen směrovač, který směruje mezi VLAN sítěmi. Kolik je VLAN sítí mezi, kterými je třeba směrovat tolik musí být použito portů na směrovači. Porty jsou následně v přepínači, který je připojen ke směrovači v access módu, každý pro danou VLAN síť. Směrovač přijme paket na jednom portu a nasměruje ho na cílový port podle směrovací tabulky. Tento systém je neefektivní jelikož je zde nutnost co VLAN síť to jeden port na směrovači.



Obr. 14. Zastaralé Inter-VLAN směrování.

#### 5.1.2 Router-on-a-stick

Je typ směrování mezi VLAN sítěmi, kdy stačí jeden fyzický port na směrovači. Přepínač je propojen se směrovačem na jednom portu. Port na přepínači je v trunk módu. Na směrovači jsou vytvořeny subinterfacy, každému z nich je přiřazena IP adresa z dané VLAN sítě a zapouzdření pro danou VLAN síť. Směrovač pak směruje z jednoho subinterfacy na jiný. Výhoda tohoto řešení je, že není třeba tolik fyzických portů na směrovači.



Obr. 15. Route-on-a-stick směrování.

### 5.1.3 Směrování pomocí L3 přepínače

Místo směrovače je možno použít L3 přepínač, který má částečnou funkcionalitu směrovače a může směrovat mezi VLAN sítěmi. V tomto případě když dojde paket na L3 přepínač například z VLAN 5 a chce být poslán na VLAN 15. L3 přepínač odstraní označení 802.1Q pro VLAN 5 při přijmutí a při odeslání mu přidá označení 802.1Q pro VLAN 15 [5]. Toto směrování je dostupné na L3 přepínačích jako Cisco 3550 a 3560 a vyšší a také Cisco 2960.

## 5.2 Konfigurace router-on-a-stick

Na portu přepínače, který je připojen k směrovači je třeba nastavit port do trunk módu, jelikož i tento port přenáší data z více VLAN sítí.

Lze provést pomocí:

```
prepinac(config-if)# SWITCHPORT MODE TRUNK
```

Port směrovače je třeba nakonfigurovat v subinterfezech. Každý subinterface reprezentuje skutečný port směrovače na který by byla připojena síť LAN. Každý subinterface má IP adresu z dané VLAN sítě.

```
smerovac(config) # INTERFACE port . číslo_vlan
```

Tímto příkazem se dostává do konfigurace subinterfacu. Skladba tohoto příkazu je INTERFACE port . číslo\_vlan.. Číslo za tečkou udává číslo VLAN sítě.

**smerovac(config-subif) # ENCAPSULATION DOT1Q** *číslo\_vlan*

Tímto příkazem je dosaženo toho, že tento port bude používat protokol 802.1Q pro označování rámců z různých VLAN sítí. *Číslo\_vlan* udává jaké označení bude přidáno do rámce na daném subinterfacu.

**smerovac(config-subif) # ENCAPSULATION DOT1Q** *číslo\_vlan* **NATIVE**

Klíčové slovo NATIVE se používá u subinterfacu pro nativní VLAN síť pokud ji chceme směrovat.

**smerovac(config-subif) # IP ADDRESS** *ip\_adresa maska*

Nastavení IP adresy pro subinterface.

**smerovac(config) # INTERFACE** *port*

**smerovac(config-if) # NO SHUTDOWN**

Na konci konfigurace je třeba port aktivovat pomocí NO SHUTDOWN.

**smerovac(config) # DEFAULT INTERFACE** *port . číslo\_vlan*

**smerovac(config) # NO INTERFACE** *port . číslo\_vlan*

Tyto příkazy slouží ke smazání subinterfacu.

Nastavení router-on-a-stick směrování lze ověřit pomocí příkazů SHOW VLAN, SHOW RUN, SHOW IP ROUTE, PING a TRACERT [3].

## 6 STATICKÉ SMĚROVÁNÍ

Je metoda směrování, kdy jsou cesty do směrovací tabulky zadávány manuálně administrátorem. Naproti tomu dynamické směrování si vytváří cesty na základně zadaných vstupních údajů do směrovacího protokolu.

Statické směrování je použito v malých sítích, kde není očekávaná změna. V sítích, kde je jenom jedna výstupní cesta a pro statické výchozí cesty, které se používají, když není nalezena shoda IP adresy paketu s žádnou cestou.

### 6.1 Typy statických cest

#### 6.1.1 Standartní statická cesta

Je standartní statická cesta, která se používá pro směrování do určité sítě.

#### 6.1.2 Výchozí statická cesta

Je cesta, která se používá, když není nalezena shoda s ostatními cestami ve směrovací tabulce. Typické použití je pro stub network a cesta do sítě Internet.

#### 6.1.3 Souhrnná statická cesta

Je cesta, která se používá na hranici sítí, ve kterých jsou blízké IP adresy. Například máme sítě: 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24. Tyto sítě lze shrnout do souhrnné statické cesty: 192.168.0.0/22. Všechny pakety, které jsou určeny do čtyřech uvedených sítí a ve směrovací tabulce je uvedena souhrnná statická cesta si vyberou tuhle cestu.

#### 6.1.4 Záložní statická cesta

Je cesta, která funguje jako záloha proto, když primární cesta k cílové síti selže. Pokud má OSPF AD (Administrative Distance) 110 a je třeba vytvořit záložní cestu, tato cesta bude mít AD 115.

## 6.2 Konfigurace IPv4 statických cest

Statickou cestu lze nakonfigurovat:

```
smerovac(config) # IP ROUTE ip_adresa_sítě maska_sítě {next-hop IP/ odchozí port}
```

, kde *ip\_adresa* a *maska* je IP adresa a maska vzdálené sítě do které je třeba směřovat a *next-hop IP* je IP adresa portu směrovače následujícího v řadě a *odchozí port* je port na směrovači na kterém je cesta konfigurována. Cesta může být identifikována i oběma údaji.

Správnost zadaných cest lze ověřit pomocí:

```
smerovac# SHOW IP ROUTE
```

Zobrazí všechny cesty.

```
smerovac# SHOW IP ROUTE STATIC
```

Zobrazí statické cesty.

```
smerovac# SHOW IP ROUTE IP_adresa_sítě
```

Zobrazí informace o určité cestě.

## 6.3 Konfigurace IPv6 statických cest

Pro aktivaci IPv6 směrování:

```
smerovac(config) # IPV6 UNICAST-ROUTING
```

Tento příkaz povolí směrování IPv6 paketů.

Pro konfiguraci statické cesty:

```
smerovac(config) # IP ROUTE ipv6_adresa_sítě/prefix {next-hop IPv6/ odchozí port}
```

Přefix zde slouží jako maska sítě.

Správnost zadaných cest lze ověřit pomocí:

**smerovac # SHOW IPV6 ROUTE**

Zobrazí všechny cesty.

**smerovac # SHOW IPV6 ROUTE STATIC**

Zobrazí statické cesty.

**smerovac # SHOW IPV6 ROUTE *IP\_adresa\_sítě***

Zobrazí informace o určité cestě.

## 6.4 Typy směrování

### 6.4.1 Classful směrování

Je typ směrování, kdy nejsou posílány masky sítí pomocí směrovacího protokolu, jelikož jsou známy z tříd IP adres. Třída A má masku 255.0.0.0, třída B má masku 255.255.0.0 a třída C má masku 255.255.255.0. To znamená, pokud jsou zvoleny IP adresy z třídy C, směrovací protokol automaticky ví, že maska je /24. Classful směrování používá protokol RIPv1. Nevýhoda tohoto typu směrování je, že dochází k obrovskému plýtvání IP adres [2].

### 6.4.2 Classless směrování

Je typ směrování, kde může být zvolena jakákoliv maska. Masky jsou posílány v aktualizacích směrovacích protokolů.

## 6.5 VLSM

VLSM je typ rozdělování IP adres do podsítí, kdy každá podsíť může mít jinou velikost. Například má být rozdělena síť 192.168.1.0/24, která je segmentována na 192.168.1.0/25, 192.168.1.128/26, 192.168.1.192/27, 192.168.1.224/27. Do směrovací tabulky ale může být pouze uloženo 192.168.1.0/24 na hraničním směrovači, jelikož do téhle sítě spadají všechny, které jsou zde vypsány.

## 7 DYNAMICKÉ SMĚROVÁNÍ

Tento typ směrování je určen do větších sítí. Směrovače, na kterých běží dynamický směrovací protokol se sami informují o sítích v dosahu. Používají k tomu speciální pakety, které obsahují informace o cestách v síti. Jeho hlavní výhodou je v tom, že pokud se změní topologie sítě či dojde k výpadku nějakého spojení, směrovací protokol přepočítá trasy a síť dále funguje. Nevýhodou dynamického směrování je v jeho vyšší náročnost na zdroje směrovače a také je třeba větší znalost příkazů.

### 7.1 Zjišťování cest

Je proces vyměňování informací o cestách mezi směrovači.

#### 7.1.1 Počáteční zjišťování

V prvním kroku každý směrovač naplní svoji směrovací tabulku svými přímo připojenými sítěmi.

#### 7.1.2 Výměna směrovacích informací mezi směrovači

V dalších krocích si již směrovače vyměňují informace mezi sebou v několika krocích. V prvním soused informuje souseda o svých přímo připojených sítích. V následujícím kroku soused, který přijmul informace od souseda, vyšle tyto informace dalšímu sousedovi v řadě. Tohle provádí, dokud každý směrovač nemá úplné informace o síti.

#### 7.1.3 Konvergence

Je stav směrovacího protokolu, kdy každý směrovač má úplné informace o síti. Každý směrovací protokol má jinak dlouhou konvergenci tzn. čas, který je třeba k přeposlání úplných informací o cestách každému směrovači v síti.

## 7.2 Typy směrovacích protokolů

### 7.2.1 Interní a Externí směrovací protokoly

Internetová síť je rozdělena na AS. AS je autonomní systém. AS značí oblast, která spadá pod jedno administrační středisko. Internet je síť, kde je mnoho AS, a tyto AS jsou

spojeny. Pro směrování v AS se používají interní směrovací protokoly jako RIPv2, OSPF, EIGRP a IS-IS (Intermediate System to Intermediate System). Pro směrování mezi AS se používají externí směrovací protokoly jako BGP.

### 7.2.2 Vektorové a link-state směrovací protokoly

Vektorové směrovací protokoly jsou ty, které k určení směru používají vzdálenost k cíli (počet směrovačů v cestě) a směr (port na směrovači). Jednotlivé směrovače nemají informace o celé topologii sítě, pouze ví, kterým směrem se nachází cílová síť. Mezi tyto protokoly patří RIP a EIGRP. V těchto protokolech jsou posílány pravidelné aktualizace.

Link-state směrovací protokoly jsou ty protokoly, kde každý směrovač má mapu celé topologie sítě. Z této mapy pak vybírá nejlepší cestu k cíli. V těchto směrovacích protokolech se neposílají pravidelné aktualizace, ale jenom když dojde ke změně topologie. Mezi tyto protokoly patří OSPF, BGP a IS-IS.

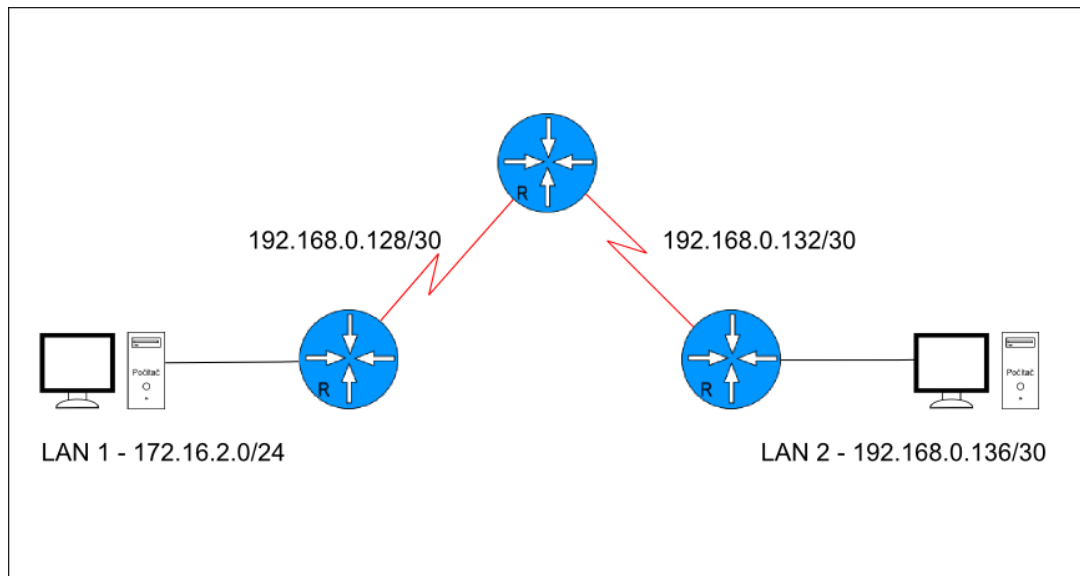
### 7.2.3 Classful a classless směrovací protokoly

Classful směrovací protokoly jsou ty, které neposílají v aktualizacích masku sítě. Představitelem této kategorie je RIPv1. Maska sítě je určena podle toho, do které třídy IP adres síť spadá anebo pokud aktualizace RIP tabulky má IP adresu spadající do stejné třídy jako IP adresa portu na který tato RIP aktualizace přichází, pak tato síť přebírá masku tohoto portu. Pro správné směrování RIPv1 je třeba použít kontinuální IP adresový prostor.

Kontinuální IP adresový prostor znamená, že musí být zvoleny IP adresy ze stejné třídy. Není nutnost používat masku třídy A, B, C. Musí být ale u všech podsítí použito stejné masky.

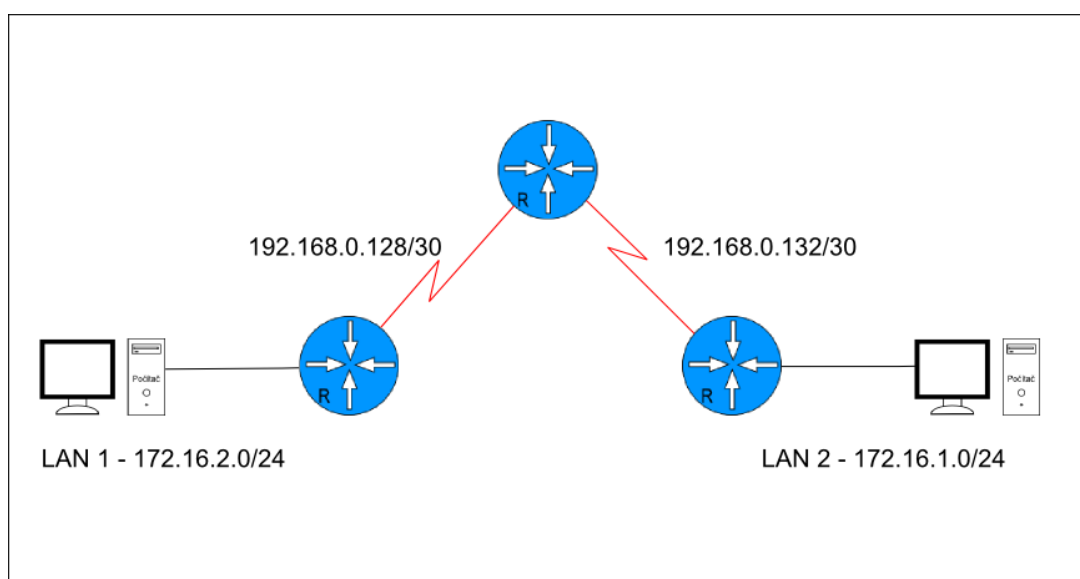
Classless směrovací protokoly jsou ty, které posílají v aktualizacích směrovacích tabulek masku podsítě. Není tedy třeba řešit kontinuitu použitého IP prostoru.

Toto směrování bude vysvětleno na následujících dvou obrázcích (Obr. 16 a 17.).



Obr. 16. Classful směrovací protokol příklad č. 1.

Na tomto příkladu bude pro sítě 192.168.0.128/30, 192.168.0.128/30 a pro 192.168.0.126/30 ve směrovacích tabulkách použita maska /30 jelikož se jedná o IP adresy ze stejné třídy a se stejnou maskou a tedy bude použita maska portů. IP síť 172.16.2.0/24 se ve směrovači napravo objeví jako 172.16.0.0 s maskou 255.255.0.0 jelikož se neposílají masky, a tato síť převezme masku třídy B a také proto, že na příchozím portu není IP adresa ze stejné třídy a tak není převzata maska portu. V tomto příkladu je použit kontinuální prostor IP adres.



Obr. 17. Classful směrování protokol příklad č. 2.

V tomto příkladu jsou sítě 172.16.1.0/24, 172.16.2.0/24 a 192.168.0.128/30, 192.168.0.132/30. První dvě jsou z třídy B a druhé dvě jsou z třídy C. Prostřední směrovač obdrží aktualizaci směrovací tabulky z obou dvou směrovačů. Jelikož porty na prostředním směrovači nemají IP adresu ze stejné třídy, nebude převzata maska portu, ale maska třídy B, která je 255.255.0.0. Ve směrovací tabulce prostředního směrovače budou dvě stejné cesty se stejnou metrikou a stejnou IP adresou sítě. To vyústí ve špatné směrování. V tomto příkladu není použito kontinuální IP prostoru, jelikož sítě 172.16.1.0/24 a 172.16.2.0/24 jsou přerušeny sítěmi 192.168.0.128/30 a 192.168.0.132/30.

### 7.3 Metrika

K cíli může existovat mnoho cest, kvůli tomu je každá cesta ohodnocena její výhodností. Tato výhodnost se nazývá metrika. U RIP protokolů je to počet směrovačů po cestě k cíli. U EIGRP je metrika ve výchozím nastavení vypočtena ze zpoždění a propustnosti spojení. U OSPF je metrika vypočtena z propustnosti spojení.

### 7.4 RIP a RIPng

RIP a RIPng (Routing Information Protocol next generation) jsou vektorové směrovací protokoly. Jako metriku používají počet směrovačů v cestě k cíli. Maximální počet směrovačů v cestě je 15. Při 16 je již cesta označena jako nedostupná. Tyto protokoly posílají periodické aktualizace směrovacích tabulek svým sousedům. Jejich AD je 120.

RIPv1 je původní verze RIP protokolu, nepodporuje CIDR a VLSM (Classless Inter-Domain Routing). Neposílá masky v aktualizacích směrovacích tabulek. Je buď použito masky třídy IP adres anebo masky portu, pokud IP sítě v aktualizaci směrovací tabulky patří do stejné třídy IP adres. Je potřeba použít kontinuální IP adresový prostor pro správné směrování. Tento protokol se již nepoužívá a byl nahrazen RIPv2.

RIPv2 je aktualizovaná verze protokolu, podporuje CIDR a VLSM. V aktualizacích posílá masku sítě. Je možno použít jakékoliv masky při tvorbě podsítí. Na hranicích sítě sumarizuje podsítě, což lze vypnout. Podporuje šifrování aktualizací směrovacích tabulek.

RIPng je verze pro IPv6 [5].

## 7.5 Konfigurace RIP

Konfigurace RIPv1:

**smerovac(config) # ROUTER RIP**

Aktivuje RIP pro směrování.

**smerovac(config-router) # NETWORK *ip\_adresa\_sítě***

Přidává do RIP protokolu informace o síti, která má být směrována. Zadáváno v classful formátu.

**smerovac(config-router) # PASSIVE-INTERFACE *port***

Po zadání tohoto příkazu se směrovací informace nebudou posílat na daný *port*.

**smerovac(config-router) # DEFAULT-INFORMATION ORIGINATE**

Pře pošle výchozí bránu sousedům.

Konfigurace RIPv2:

**smerovac(config-router) # VERSION 2**

Aktivuje RIPv2.

**smerovac(config-router) # NETWORK *ip\_adresa\_sítě***

Zadává se IP adresa sítě v classful formátu.

**smerovac(config-router) # NO AUTO-SUMMARY**

Vypne sumarizaci cest na hraničních směrovači.

Konfigurace RIPng:

**smerovac(config) # IPV6 UNICAST-ROUTING**

Aktivace směrování IPv6 adres.

**smerovac(config-if) # IPV6 RIP *název* ENABLE**

Aktivace RIPng jako směrovacího protokolu na portu, *název* je identifikace instance RIPng.

**smerovac(config-if) # IPV6 ROUTE 0::/0 {*odchozí\_port/next-hop IP*}**

Konfigurace statické výchozí cesty.

**smerovac(config-if) # IPV6 RIP *název* DEFAULT-  
INFORMATION  
ORIGINATE**

Přeposlání statické výchozí cesty na daném portu [8].

Ověření konfigurace dynamických protokolů:

**smerovac # SHOW IP PROTOCOLS**

Zobrazí nastavení směrovacího protokolu.

**smerovac# SHOW IPV6 PROTOCOLS**

Zobrazí nastavení směrovacího protokolu pro IPv6.

## 8 OSPF

Je link-state směrovací protokol pro využití ve velkých sítích. Pro metriku je využito propustnosti linek. Má hierarchický návrh, jelikož je rozdělen do oblastí. Tyto oblasti se chovají jako jeden autonomní systém, ale informace o sousedech se šíří pouze v dané oblasti. Jeho AD je 110. Je to classless směrovací protokol.

Před vysíláním informací o svých přímo připojených spojích se vysílají hello pakety za pomoci, kterých se směrovače informují o tom, že mají sousedy a navážou sousedské vztahy. Tito sousedé jsou uloženi v tabulce sousedů. Hello pakety také slouží jako keepalive pakety. Ve výchozím nastavení jsou vysílány každých 10 s na mutliaccess a point-to-point sítích. Následně jsou vysílány LSA (Link-State Advertisements) zprávy, které sousedům pošlou informace o přímo připojených spojeních sousedů. Z těchto se pak vytvoří topologická tabulka v Link-state databázi. Jsou vysílány při počáteční konfiguraci a pak při změnách v síti. Potom jsou z link-state databáze pomocí SPF (Shortest Path First) algoritmu vybrány ty nejkratší cesty a uloženy do směrovací tabulky.

Pro IPv4 je zde OSPFv2 a pro IPv6 je zde OSPFv3 [5].

Příkazy pro zobrazení:

**smerovac# SHOW IP OSPF NEIGHBOR**

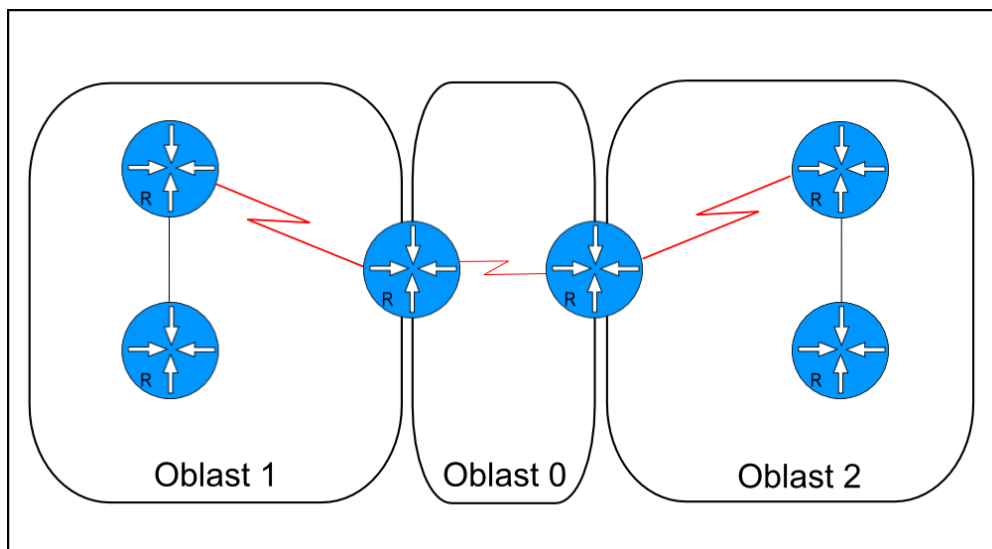
Zobrazí sousedy směrovače.

**smerovac# SHOW IP OSPF DATABASE**

Zobrazí link-state databázi.

### 8.1 OSPF oblasti

Oblasti slouží k rozdělení autonomního systému na menší oblasti. Každá oblast má vlastní link-state databázi. Když dojde ke změně v jedné oblasti, LSA paket je rozeslán v jedné oblasti. Výhoda tohoto řešení jsou menší LS databáze. Páteřní oblastí je oblast 0 (area 0). K této oblasti musí být přímo připojeny všechny ostatní oblasti, pokud není řešeno virtual-linkem. Pokud spadá směrovač do více oblastí, nazývá se ABR (Area Border Router). Pokud je směrovač na hranici oblasti 0 a jiného autonomního systému, nazývá se ASBR (Autonomous System Border Router). Ostatní směrovače se nazývají interní směrovače.



Obr. 18. OSPF oblasti.

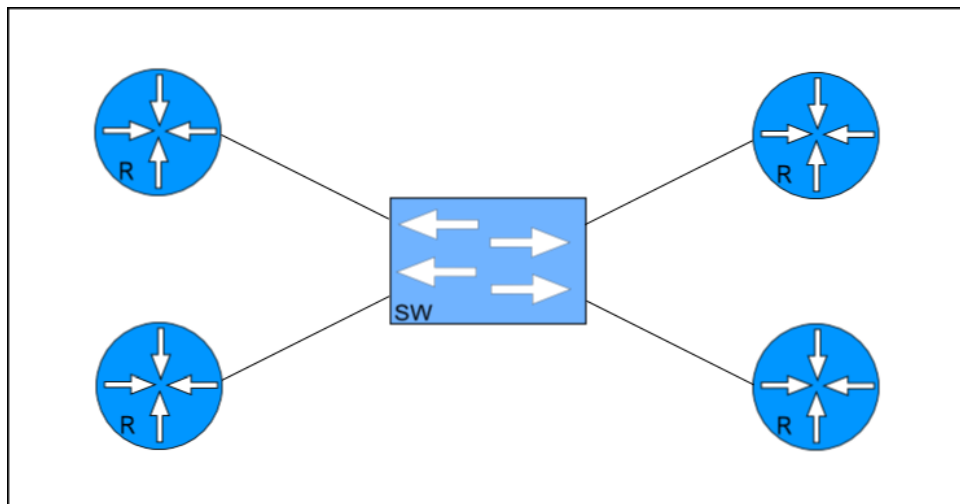
## 8.2 Stavby OSPF

Porty při synchronizaci OSPF prochází několika stavy:

- Down state – Porty si neposílají hello pakety.
- Init state – Hello pakety jsou přijmuty s ID sousedního směrovače.
- Two-way state – Volí se DR (Designated Router) a BDR (Backup Designated Router).
- ExStart state – Vyjednává se o master/slave vztahu a DBD (Database Descriptors) pořadovém čísle.
- ExChange state – Směrovače si vyměňují DBD pakety.
- Loading state – Výměna LSA paketů a výpočet nejkratších cest pomocí SPF algoritmu.
- Full state – Mezi směrovači došlo ke konvergenci [8].

## 8.3 DR a BDR

Ve více přístupové síti jako na obrázku je třeba zvolit DR a BDR. Každý směrovač v síti s OSPF posílá LSA pakety každému sousednímu směrovači. To by v tomhle případě znamenalo, že by bylo posláno příliš mnoho LSA paketů. Z toho důvodu je třeba zvolit DR a BDR (záložní DR). V tomhle případě pak každý směrovač vyšle LSA pakety DR směrovači a ten tyto LSA pakety dále distribuuje ostatním směrovačům ve více přístupové síti.



Obr. 19. Více přístupová síť.

## 8.4 ID směrovače

Každý směrovač podílející v OPSF směrování má ID, které ho identifikuje. Toto ID je důležité pro volbu DR a BDR a identifikaci směrovačů v OSPF AS. ID je reprezentováno IP adresou. Je buď nakonfigurováno ručně. Pokud není, je vybrána IP adresa loopback portu. Pokud není, je vybrána nejvyšší IP adresa přidělená některému portu směrovače. 192.168.0.1 je vyšší IP adresa než 10.0.0.1.

## 8.5 Metrika OSPF

Metrika OSPF je založena na propustnosti spojení na cestě k cíli. Čím vyšší číslo, tím nižší rychlost spojení. Jednotlivé propustnosti spojení se po cestě k cíli sčítají.

Metrika se dá spočítat pomocí:

$$\text{cena spojení} = \frac{\text{ref. propustnost}}{\text{propustnost spojení}}$$

, kde referenční propustnost je měnitelný údaj, ve výchozím stavu je to 100 Mb/s a propustnost spojení je spojení mezi směrovači [5].

## 8.6 Konfigurace OSPF

Konfigurace směrování OSPF:

**smerovac(config) # ROUTER OSPF *process\_id***

Aktivuje OSPF jako směrovací protokol, *process\_id* je číslo od 1 do 65536, má pouze lokální význam a může být na každém směrovači jiné.

**smerovac(config-router) # ROUTER-ID *ip\_adresa***

Nastavení ID směrovače.

**smerovac(config-router) # NETWORK *ip\_adresa\_sítě wildcard\_maska AREA číslo\_oblasti***

Přidání sítě do směrovacího protokolu, *wildcard\_maska* je opačná klasická maska.

255.255.255.252 -> 0.0.0.3 -> 255.255.255.0 -> 0.0.0.255. Místo *ip\_adresa\_sítě* může být zadána i IP adresa portu na směrovači.

**smerovac(config-router) # DEFAULT-INFO RMATION ORIGINATE**

Distribuuje výchozí statickou cestu do OPSF protokolu.

**smerovac(config-router) # PASSIVE-INTEFACE *port***

Po zadání se LSA a hello pakety nebudou posílat na daný port.

**smerovac(config-router) # AUTO-COST REFERENCE-BANDWIDTH *propustnost\_v\_Mb/s***

Úprava referenční propustnosti pro výpočet metriky. Musí být konzistentní na všech směrovačích.

**smerovac(config-if) # BANDWIDTH *propustnost\_v\_Kb/s***

Úprava propustnosti spojení. Musí být stejné na obou koncích spojení.

**smerovac(config-if) # IP OSPF COST *cena***

Úprava ceny spojení. Musí být stejné na obou koncích spojení.

Ověření nastavení OSPF směrovacího protokolu:

**smerovac# SHOW IP OSPF**

Zobrazí informace o OSPF.

**smerovac# SHOW IP OSPF INTERFACE BRIEF**

Zobrazí informace o jednotlivých portech a jejich OSPF nastavení.

## 9 ACCESS CONTROL LISTY

ACL (Access Control List) značí sadu pravidel podle kterých je filtrován provoz v síti. Provoz lze buď povolit či zakázat. Tento provoz lze filtrovat na základě IP adresy zdroje a cíle, typu přenosu (TCP nebo UDP) a typu protokolu (HTTP – 80). Existují standardní ACL a rozšířené ACL. Standardní ACL filtruje na základě zdrojové IP adresy. Rozšířené ACL filtruje na základě IP adresy zdroje, cíle a podle typu přenosu a protokolu.

### 9.1 Fungování ACL

ACL list je sada řádků příkazů pro filtraci provozu. Na konci každého ACL je implicit deny, což značí, že je vše zakázáno, kromě toho co je povoleno. Shoda v řádcích je nacházena z vrchu dolů, proto je dobré pravidlo ty důležitější umístit na vrch seznamu. ACL list lze aplikovat buď v příchozím nebo v odchozím směru na port.

### 9.2 Pravidla pro použití ACL

Lze použít 1 ACL list pro port, pro protokol a pro směr. Standardní ACL list je dobré použít co nejbližší k cíli a rozšířený ACL list je dobré použít co nejbližší ke zdroji provozu [2].

### 9.3 Standardní číslované ACL

Standardní ACL filtruje na základě zdrojové IP adresy. Mohou být buď číslované nebo pojmenované. Pro standardní ACL jsou vyhrazena čísla od 1 do 99 a od 1300 do 1999.

Vytvoření číslovaného standardního ACL:

```
smerovac(config) # ACCESS-LIST [1-99] [PERMIT | DENY] [zdrojová IP adresa]  
[wildcard maska] [log]
```

, kde 1-99 je číslo ACL, PERMIT a DENY je povolit či zakázat provoz a log je pro logování ACL.

Pokud je potřeba povolit či zakázat 1 hosta je použito klíčové slovo HOST. Pokud je třeba povolit všechny hosty je nutno použít klíčového slova ANY.

```
smerovac(config-if) # IP ACCESS-GROUP číslo_ACL [IN/OUT]
```

Aplikace ACL na port. *IN* pro vstupní provoz a *OUT* pro výstupní provoz.

**smerovac(config-line) # ACCESS-CLASS číslo\_ACL [IN/OUT]**

Aplikace ACL na telnet. *IN* pro vstupní provoz a *OUT* pro výstupní provoz.

**smerovac # SHOW IP ACCESS-LISTS**

Ověření konfigurace ACL listů.

## 9.4 Rozšířené číslované ACL

Rozšířené ACL filtruje na základě zdrojové a cílové IP adresy, podle přenosu a podle protokolu. Mohou být buď číslované nebo pojmenované. Pro rozšířené ACL jsou vyhrazena čísla od 100 do 199 a od 2000 do 2699.

Vytvoření rozšířeného číslovaného ACL

**smerovac(config) # ACCESS-LIST [100-199] [PERMIT | DENY] [přenos] [zdrojová IP adresa] [wildcard maska] [cílová IP adresa] [wildcard maska] [operátor] [protokol] [log]**

, kde *přenos* je TCP, UDP či ICMP, *operátor* je EQ (rovno), LT (méně než), GT (více než), NEG (všechny kromě) či RANGE (od do).

**smerovac(config-if) # IP ACCESS-GROUP číslo\_ACL [IN/OUT]**

Aplikace ACL na port. *IN* pro vstupní provoz a *OUT* pro výstupní provoz.

**smerovac(config) # SHOW IP ACCESS-LISTS**

Ověření konfigurace ACL listů.

## 9.5 Pojmenované ACL

ACL listy je také možno pojmenovat. Syntaxe těchto příkazů je:

**smerovac(config) # IP ACCESS-LIST [STANDARD/EXTENDED] jméno\_ACL**

Vytvoření pojmenovaného ACL.

Po něm se zobrazí buď **smerovac(config-std-nacl) #** nebo **smerovac(config-ext-nacl) #** režim, ve kterém je možno definovat jednotlivé řádky ACL ve formátu:

**smerovac(config-std-nacl) #** *[PERMIT | DENY] [zdrojová IP adresa] [wildcard maska]*

**smerovac(config-ext-nacl) #** *[PERMIT | DENY] [přenos] [zdrojová IP adresa]  
[wildcard maska] [cílová IP adresa] [wildcard maska]  
[operátor] [protokol]*

## 10 DHCP

DHCP je služba sloužící k přidělování údajů klientům, které jsou potřebné pro jejich správnou komunikaci. Mezi tyto údaje patří IP adresa, maska sítě, brána, DNS servery a jiné.

### 10.1 Průběh přidělování s DHCP

Přidělování probíhá ve 4 krocích.

#### 10.1.1 DHCP Discover

Zpráva, která je vyslána hostem pro vyhledání DHCP serveru.

#### 10.1.2 DHCP Offer

Zpráva, kterou host obdrží jako odpověď na DHCP Discover. Obsahuje potřebné údaje.

#### 10.1.3 DHCP Request

Zpráva, která je vyslána hostem jako odpověď na DHCP Offer. Zpráva obsahuje, že host souhlasí s přijmutím nabízených údajů.

#### 10.1.4 DHCP Pack

Zpráva, která potvrzuje hostovo přijmutí nabízených údajů [5].

### 10.2 Konfigurace DHCP

```
smerovac(config) # IP DHCP POOL jméno
```

Vytvoření instance DHCP.

```
smerovac(dhcp-config) # NETWORK počáteční_IP konečná_IP
```

Přidělení IP prostoru pro přidělování.

```
smerovac(dhcp-config) # DEFAULT-ROUTER brána
```

Přidělení výchozí brány.

**smerovac(dhcp-config) # DNS-SERVER** *ip\_adresa\_DNS\_serveru*

**smerovac(dhcp-config) # DOMAIN-NAME** *doménové\_jméno*

Nastavení ostatních údajů pro DHCP instanci.

**smerovac(config-if) # IP DHCP EXCLUDED-ADDRESS** *počáteční\_IP konečná\_IP*

Vyjmutí specifikovaných IP adres z přidělování.

**smerovac(config-if) # IP HELPER-ADDRESS** *ip\_adresa*

Nastavení IP adresy vzdáleného DHCP serveru na portu.

## 11 NETWORK ADDRESS TRANSLATION

IP adresový prostor se dělí na privátní a veřejný. Privátní IP adresy nejsou směrovatelné v Internetu. Veřejné IP jsou směrovatelné v Internetu. Veřejné IP adresy jsou přidělovány lokálními RIR (Regional Internet registry) organizacemi. Privátní IP adresy mohou organizace využívat bez registrace. Na hranicích mezi privátním a veřejným IP prostorem musí docházet k překladu IP adres. Tento překlad se nazývá NAT.

Do privátního IP adresového prostoru patří tyto IP adresy:

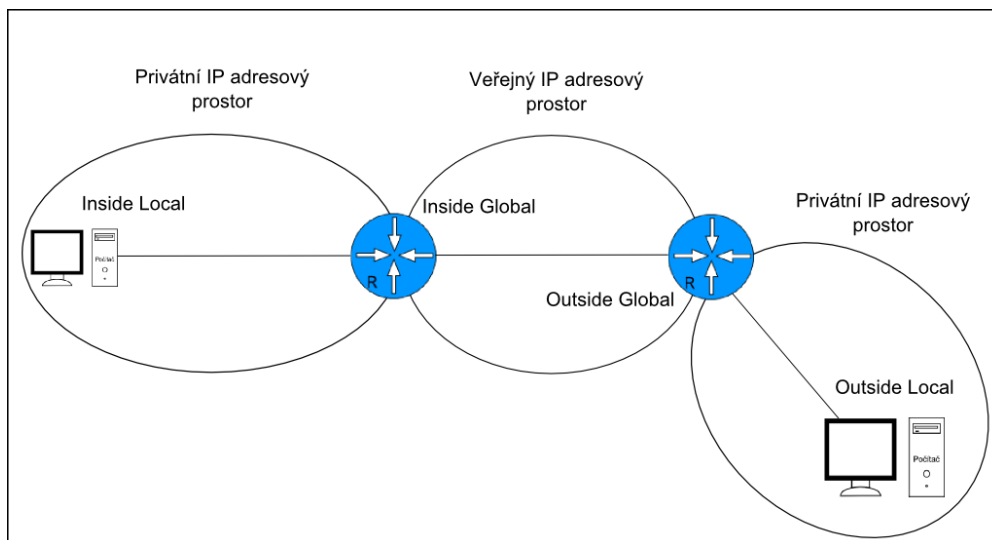
*Tab. 4. Privátní IP adresy [1].*

Třída IP adres	Rozsah IP adres
Třída A	10.0.0.0 – 10.255.255.255
Třída B	172.16.0.0 – 172.31.255.255
Třída C	192.168.0.0 – 192.168.255.255

### 11.1 Překlad NAT

Host v LAN síti má IP adresu nazývanou inside local, tato LAN síť má hranici. Na hranici, kde se připojuje k veřejnému Internetu se provádí překlad IP adres. Inside local IP adresa je přeložena do inside global IP adresy. Vzdálený host pak tohoto vnitřního hosta vidí pod inside global IP adresou. Hraniční směrovač uchovává NAT tabulku překladu, kde je inside global IP adresa přidělena inside local IP adrese. V této tabulce jsou všechny 4 IP adresy zmíněné pod tímto odstavcem.

- Inside local – IP adresa hosta, která má být přeložena NAT překladem.
- Inside global – Veřejná IP adresa do které je přeložena Inside local IP adresa.
- Outside local – IP adresa vzdáleného hosta, která je překládána NAT překladem.
- Outside global – IP adresa do které je přeložena outside local IP adresa vzdáleného hosta [8].



Obr. 20. IP adresy v NAT překladu.

## 11.2 Typy NAT překladu

### 11.2.1 Statický překlad

Jedné inside local IP adrese je přiřazena jedna inside global IP adresa.

### 11.2.2 Dynamický překlad

Inside local IP adresám jsou přiřazeny dočasně právě dostupné inside global IP adresy.

### 11.2.3 Port address translation

Pokud je potřeba přeložit současně více inside local IP adres a počet inside local IP adres převyšuje počet dostupný inside global IP adres je třeba použít PAT (Port Address Translation). Při PAT je každému požadavku na překlad přiřazen port protokolu a je tak možno odlišit od jakého hosta byl požadavek vyslán.

### 11.3 Konfigurace NAT a PAT

Konfigurace statického překladu:

```
smerovac(config) # IP NAT INSIDE SOURCE STATIC inside_local_IP inside_global_IP
```

Definování IP adres pro překlad.

```
smerovac(config-if) # IP NAT [INSIDE/OUTSIDE]
```

Definování směru překladu na portech.

Konfigurace dynamického překladu:

```
smerovac(config) # IP NAT POOL název počáteční_IP konečná_IP [ NETMASK maska / PREFIX prefix]
```

Vytvoření rozsahu inside global IP adres.

```
smerovac(config) # ACCESS-LIST číslo PERMIT ip_adresa wildcard_maska
```

Povolení IP adres, které mohou být přeloženy.

```
smerovac(config) # IP NAT INSIDE SOURCE LIST číslo POOL název OVERLOAD
```

Svázání access listu s rozsahem IP adres pro překlad NAT. Přidáním klíčového slova OVERLOAD je použit PAT překlad [3].

Ověření překladu NAT:

```
smerovac # SHOW IP NAT [ TRANSLATIONS / STATISTICS ]
```

## **II. PRAKTICKÁ ČÁST**

## 12 PROVEDENÍ PRAKTICKÉ ČÁSTI

V praktické části jsou obsaženy úlohy pro program Packet tracer. Tento program simuluje reálné počítačové sítě na zařízeních firmy Cisco. Tato firma vyrábí profesionální směrovače, prepínače a jiná síťová zařízení. Je vytvořeno 11 těchto úloh. Pro každou kapitolu jedna. Každá úloha byla vypracována ve dvou verzích. První je zadání a druhá je řešení. Ke každé úloze jsou přiloženy dva soubory .pkt (soubor programu Packet tracer). V jedné je zadání a v druhé je řešení. Úlohy jsou také přiloženy jako přílohy v .pdf, které jsou vhodné použití ve výuce.

### 12.1 Zadání úlohy

V každém písemném zadání je na obrázku model síťové úlohy. Následně jsou zde body zadání pro konfiguraci. K úloze je přiložen soubor .pkt se zadáním v Packet traceru.

### 12.2 Řešení úlohy

Řešení se skládá z písemného vysvětlení příkazů a v přiloženém souboru .pkt je také úloha vyřešena.

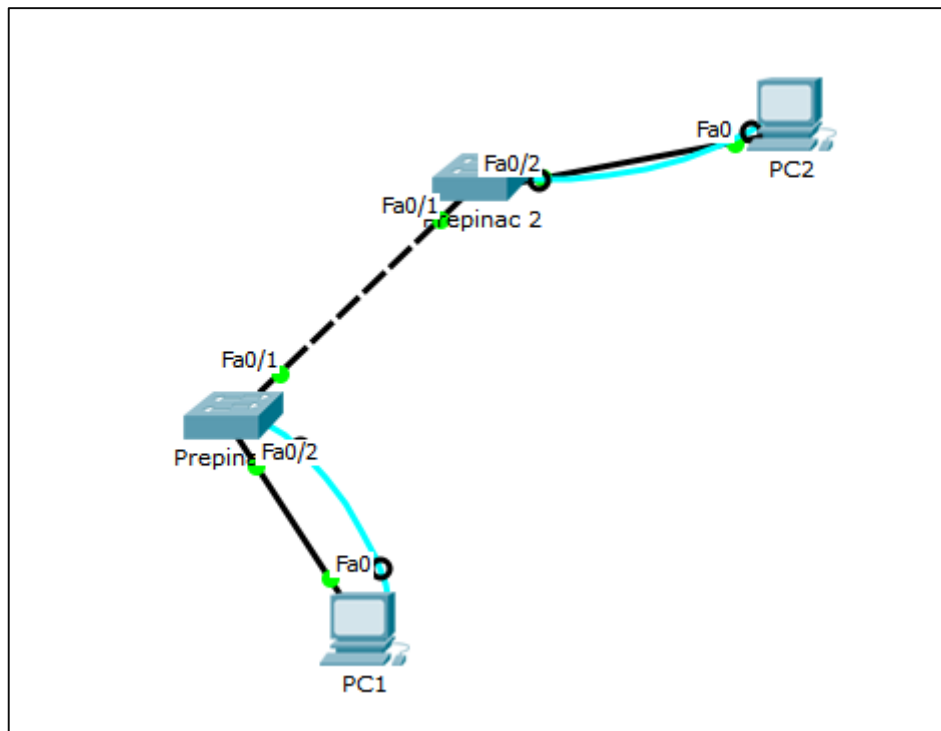
### 12.3 Provedení konfigurace

K dispozici pro testování úloh bylo 2x Cisco 2950 prepínač, 1x Cisco 3550 prepínač, 2x Cisco 1721 směrovač a 1x Cisco 1751 směrovač, krimpovací kleště a jiné potřebné kabely pro propojení a správnou konfiguraci. Zařízení byla konfigurována pomocí programu Putty pro přístup přes příkazovou řádku. Nejdříve bylo navrženo zadání, které bylo při konfiguraci v Packet traceru vyladováno. Následně byla každá konfigurace odzkoušena na výše zmíněném Cisco zařízení.

### 12.4 Doporučení pro konfigurování úloh

Každá úloha by měla být prováděna na skutečném Cisco zařízení, některé příkazy nemusí fungovat v Packet traceru. Při propojování zařízení by si student měl kreslit fyzické schéma zapojení a také si popsat jednotlivá zařízení, aby mohl efektivně řešit problémy s fyzickou vrstvou.

## 13 ÚLOHA 1 – ZÁKLADNÍ NASTAVENÍ



Obr. 21. Úloha 1 – Zadání v PT.

### 13.1 Zadání

V této úloze budete konfigurovat základní nastavení přepínačů.

1. Pro tuto síť/konfiguraci si vyberte IP adresy z třídy B, soukromé IP adresy. Rozsah IP adres musí dostačovat pro 126 klientů.
2. Přepínače konfigurujte pomocí konzolového připojení.
3. První dostupnou IP adresu z podsítě přiřaďte rozhraní vlan 1 pro přepínač 1, druhou dostupnou IP adresu přiřaďte pro rozhraní vlan 1 přepínače č. 2.
4. Pro klienty přiřaďte libovolné IP adresy kromě poslední dostupné.
5. Pojmenujte přepínač 1, hostname prepinač1, pojmenujte přepínač 2 hostnameem prepinač2.
6. Heslo k privilegovanému módu nastavte na class u obou přepínačů.
7. Nastavte hesla pro console line a vty lines na cisco.
8. Zajistěte, aby všechny hesla byla šifrovaná.
9. Nastavte zprávu „Zadejte heslo“, tak aby se zobrazoval tehdy, když je po vás chtěno heslo z konzolového či vzdáleného přístupu (telnet).
10. Nastavte uvítací zprávy „Vítejte na prepinači 1“ a „Vítejte na prepinači 2“.
11. Nastavte IP adresy pro daná rozhraní a počítače.
12. Pingněte na rozhraní vlan 1 na obou přepínačích a z pc 1 na pc 2 a naopak.
13. Předvedte, že uvítací zprávy (bannery) se zobrazují opravdu tehdy kdy mají.
14. Uložte právě běžící konfiguraci do konfigurace, která se načítá po startu přepínače, vypněte a zapněte přepínače, zkuste pingnout na vlan 1 obou přepínačů znovu a zkontrolujte, zdali jsou stále nakonfigurované.

## 13.2 Řešení

1. Pro tuto síť/konfiguraci si vyberte IP adresy z třídy B, soukromé IP adresy. Rozsah IP adres musí dostačovat pro 126 klientů.

Privátní IP adresy třídy B jsou v rozsahu 172.16.0.0 až 172.31.255.255

Maska potřebná pro 126 klientů je /25, 255.255.255.128

Zvolený rozsah:

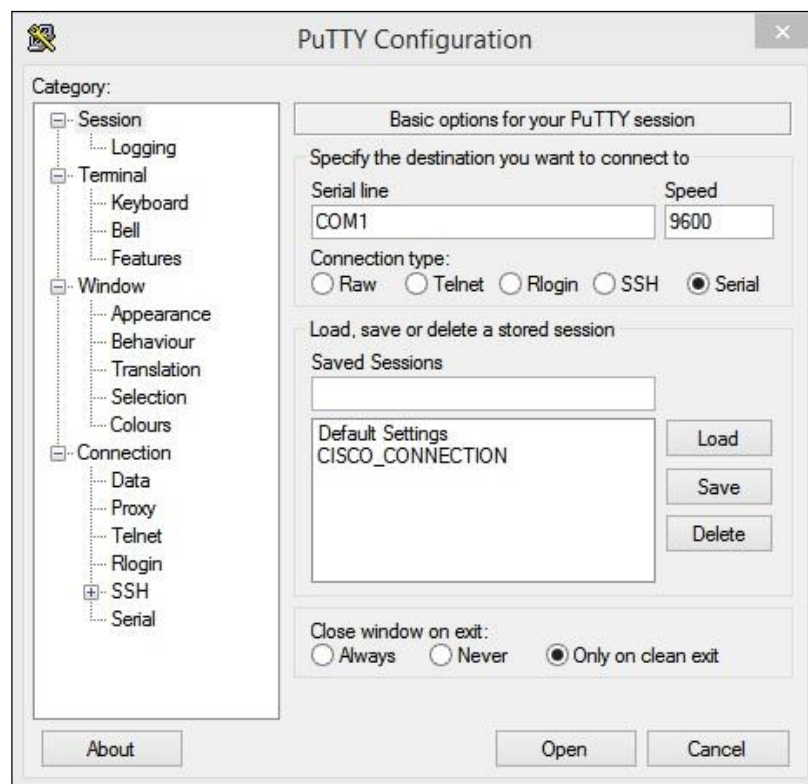
172.16.0.0/25 – IP podsítě

.1 až .126 - dostupné pro hosty v síti

.127 – broadcastová IP adresa

2. Přepínače konfiguruje pomocí konzolového připojení.

Přepínač musí být k počítači připojen pomocí konzolového kabelu, z jedné strany je RJ-45 a z druhé RS-232, pokud nemáte tento konektor na svém počítači, pořídíte si RS-232-USB převodník. Z počítače se na přepínač dostanete pomocí programu Putty, který se používá pro vzdálený přístup pomocí telnet či přes RS-232 (sériové spojení). Zde zvolíte Category->Serial, COM port je váš port pro konektor RS-232, liší se v každém počítači. Kliknete na open.



Obr. 22. Putty připojení k přepínači.

3. První dostupnou IP adresu z podsítě přiřadíte rozhraní vlan 1 pro přepínač 1, druhou dostupnou IP adresu přiřadíte pro rozhraní vlan 1 přepínače č. 2.

Pro rozhraní vlan 1, přepínač 1 je to IP adresa: 172.16.0.1/25

Pro rozhraní vlan 1, přepínač 2 je to IP adresa: 172.16.0.2/25

**4. Pro klienty přiřaďte libovolné IP adresy kromě poslední dostupné.**

Mohou být libovolné dostupné.

Pro řešení je zvoleno:

PC1 – 172.16.0.10/25

PC2 – 172.16.0.44/25

**5. Pojmenujte přepínač 1, hostnámem prepinač1, pojmenujte přepínač 2 hostnámem prepinač2.**

Konfigurovat je nutno v konfiguračním módu.

Posloupnost módů v Cisco IOS. Zleva doprava.

*Tab. 5. Konfigurační módy.*

user EXEC	privileged EXEC	global conf. mode	interface mode,lines mode
switch>	switch#	switch(config)#	switch(config-if)# switch(config-line)# router(config-router)#

**switch>** ENABLE

**switch#** CONFIGURE TERMINAL

**switch(config)#** HOSTNAME *prepinac1*

**switch>** ENABLE

**switch#** CONFIGURE TERMINAL

**switch(config)#** HOSTNAME *prepinac2*

**6. Heslo k privilegovanému módu nastavte na class u obou přepínačů.**

**prepinac1(config)#** ENABLE SECRET *class*

**prepinac2(config)#** ENABLE SECRET *class*

**7. Nastavte hesla pro console line a vty lines na cisco.**

**prepinac1(config)#** LINE CONSOLE 0

**prepinac1(config-line)#** PASSWORD *cisco*

**prepinac1(config-line)#** LOGIN (po zadání tohoto příkazu, budete heslo vyžádání zadat)

**prepinac2(config)#** LINE CONSOLE 0

**prepinac2(config-line)#** PASSWORD *cisco*

**prepinac2(config-line)#** LOGIN

**prepinac1(config)#** LINE VTY 0 15

**prepinac1(config-line)#** PASSWORD *cisco*

**prepinac1(config-line)#** LOGIN

**prepinac2(config)#** LINE CONSOLE 0 15

**prepinac2(config-line)#** PASSWORD *cisco*

**prepinac2(config-line)#** LOGIN

8. Zajistěte, aby všechny hesla byla šifrovaná.

```
prepinac1(config)# SERVICE PASSWORD-ENCRYPTION  
prepinac2(config)# SERVICE PASSWORD-ENCRYPTION
```

9. Nastavte zprávu „Zadejte heslo“, tak aby se zobrazovala tehdy, když je po vás chtěno heslo z konzolového či vzdáleného přístupu (telnet).

```
prepinac1(config)# BANNER LOGIN c Zadejte heslo c  
prepinac2(config)# BANNER LOGIN c Zadejte heslo c  
c – ukončovací znak řetězce
```

10. Nastavte uvítací zprávy „Vítejte na prepínaci 1“ a „Vítejte na prepínaci 2“.

```
prepinac1(config)# BANNER MOTD x Vítejte na prepínaci 1 x  
prepinac2(config)# BANNER MOTD x Vítejte na prepínaci 2 x  
x- ukončovací znak
```

11. Nastavte IP adresy pro daná rozhraní a počítače.

```
prepinac1(config)# INTERFACE VLAN 1  
prepinac1(config-if)# IP ADDRESS 172.16.0.1 255.255.255.128
```

```
prepinac2(config)# INTERFACE VLAN 1  
prepinac2(config-if)# IP ADDRESS 172.16.0.2 255.255.255.128
```

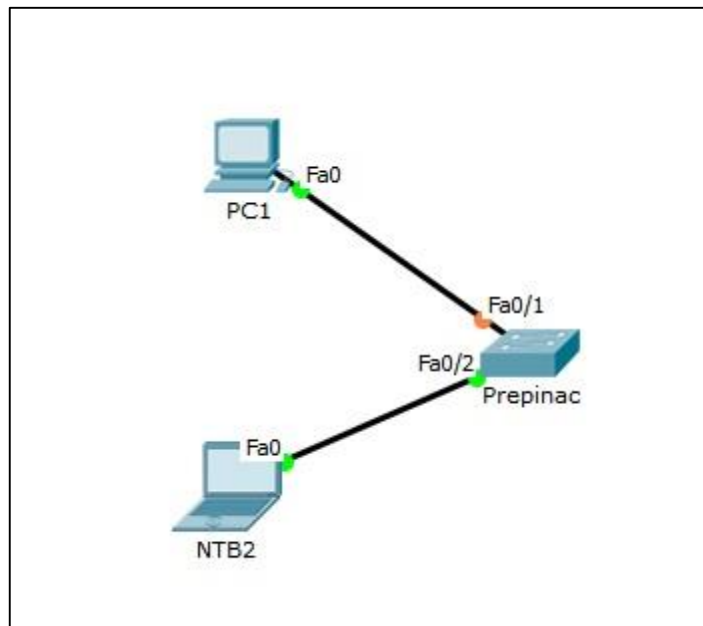
12. Pingněte na rozhraní vlan 1 na obou přepínačích a z pc 1 na pc 2 a naopak.

13. Předved'te, že uvítací zprávy (bannery) se zobrazují opravdu tehdy kdy mají.

14. Uložte právě běžící konfiguraci do konfigurace, která se načítá po startu přepínače, vypněte a zapněte přepínače, zkuste pingnout na vlan 1 obou přepínačů znovu a zkontrolujte, zdali jsou stále nakonfigurované.

```
prepinac1# COPY RUNNING-CONFIG STARTUP-CONFIG  
prepinac2# COPY RUNNING-CONFIG STARTUP-CONFIG  
COPY odkud kam
```

## 14 ÚLOHA 2 – VZDÁLENÝ PŘÍSTUP, NASTAVENÍ PORTŮ A BEZPEČNOST



Obr. 23. Úloha 2 – Zadání v PT.

### 14.1 Zadání

V této úloze budete konfigurovat vzdálený přístup, nastavení portů a bezpečnost.

1. Pro tuto síť/konfiguraci si vyberte IP adresy z třídy C, soukromé IP adresy. Rozsah IP adres musí dostačovat pro 62 klientů.
2. Přepínače konfigurujte pomocí konzolového připojení z PC1 dokud nebude nastaven vzdálený přístup pomocí SSH.
3. Pojmenujte přepínač hostnámem prepinac.
4. Poslední dostupnou IP adresu z podsítě přiřaďte rozhraní vlan 1 pro přepínač.
5. Pro klienty přiřaďte libovolné IP adresy kromě poslední dostupné.
6. Heslo k privilegovanému módu nastavte na class u přepínače.
7. Nastavte rychlost u portů využitých klienty a u stanic (pokud je třeba) na 100 Mbps a full-duplex.
8. Pingněte mezi stanicemi a na vlan 1 u přepínače.

#### Nastavení SSH pro vzdálený přístup

9. Nakonfigurujte doménové jméno a vygenerujte šifrovací klíč.
10. Nastavte SSH na verzi 2.
11. Do lokální databáze na přepínači vytvořte účet s uživatelským jménem admin a heslem 1234.
12. Nastavte správně vty lines tak, abyste se mohli následně z PC1 či NTB2 přihlásit na přepínač přes SSH.
13. Ověřte, zdali funguje přístup na přepínač přes SSH.

Zabezpečení přepínače a portů

14. Zařídte, aby všechna hesla byla šifrovaná.
15. Aktivujte Port security na portech na kterých je třeba.
16. Nastavte port fastEthernet 0/24 jako trusted port ke kterému bude připojený DHCP server.
17. Vypněte všechny nepoužité porty.
18. Klientské porty nastavte tak, aby mohli vysílat pouze 10 DHCP zpráv za 1 s.
19. Pro oba porty, na kterých jsou připojeni klienti nastavte maximum MAC adres na 5.
20. Nastavte mód porušení pravidel na takový, aby při porušení bylo vyvolána zpráva SNMP protokolu o porušení pravidel.
21. Uložte konfiguraci.
22. Vypněte a zapněte či reloadujte přepínač a pingněte znovu.

## 14.2 Řešení

1. **Pro tuto síť/konfiguraci si vyberte IP adresy z třídy C, soukromé IP adresy. Rozsah IP adres musí dostačovat pro 62 klientů.**

Privátní IP adresy třídy C jsou v rozsahu 192.168.0.0 až 192.168.255.255  
Maska potřebná pro 62 klientů je /26, 255.255.255.192

Zvolený rozsah:

192.168.144.0/26 – IP podsítě  
.1 až .62 - dostupné pro hosty v síti  
.63 – broadcastová IP adresa

2. **Přepínače konfigurujte pomocí konzolového připojení z PC1 dokud nebude nastaven vzdálený přístup pomocí SSH.**
3. **Pojmenujte přepínač hostnamem prepinač.**  

```
switch> ENABLE  
switch# CONFIGURE TERMINAL  
switch(config)# HOSTNAME prepinac
```
4. **Poslední dostupnou IP adresu z podsítě přiřaďte rozhraní vlan 1 pro přepínač.**  

```
prepinac(config)# INTERFACE VLAN 1  
prepinac(config-if)# IP ADDRESS 192.168.144.62 255.255.255.192
```
5. **Pro klienty přiřaďte libovolné IP adresy kromě poslední dostupné.**  
PC1 – 192.168.144.10  
NTB2 – 192.168.144.20
6. **Heslo k privilegovanému módu nastavte na class u přepínače.**  

```
prepinac(config)# ENABLE SECRET class
```

7. Nastavte rychlost u portů využitých klienty a u stanic (pokud je třeba) na 100 Mbps a full-duplex.

```
prepinac(config)# INTERFACE fa0/1
prepinac(config-if)# SPEED 100
prepinac(config-if)# DUPLEX FULL
```

```
prepinac(config)# INTERFACE fa0/2
prepinac(config-if)# SPEED 100
prepinac(config-if)# DUPLEX FULL
```

8. Pingněte mezi stanicemi a na vlan 1 u přepínače.

Nastavení SSH pro vzdálený přístup

9. Nakonfigurujte doménové jméno a vygenerujte šifrovací klíč.

```
prepinac(config)# IP DOMAIN-NAME domena.cz
prepinac(config)# CRYPTO KEY GENERATE RSA
```

10. Nastavte SSH na verzi 2.

```
prepinac(config)# IP SSH VERSION 2
```

11. Do lokální databáze na přepínači vytvořte účet s uživatelským jménem admin a heslem 1234.

```
prepinac(config)# USERNAME admin PASSWORD 1234
```

12. Nastavte správně vty lines tak, abyste se mohli následně z PC1 či NTB2 přihlásit na přepínač přes SSH.

```
prepinac(config)# LINE VTY 0 15
prepinac(config-line)# TRANSPORT INPUT SSH
prepinac(config-line)# LOGIN LOCAL
```

TRANSPORT INPUT SSH říká, že pro autentifikaci bude použito SSH.

LOGIN LOCAL říká, že bude použito uživ. účtu z lokální databáze na přepínači.

13. Ověřte, zdali funguje přístup na přepínač přes SSH.

Pro ověření je třeba použít program Putty ze stanice připojené k přepínači, v Putty stačí místo Serial zvolit SSH a napsat IP adresu daného přepínače. V tomto případě 192.168.144.62.

Zabezpečení přepínače a portů

14. Zaříd'te, aby všechna hesla byla šifrovaná.

```
prepinac(config)# SERVICE PASSWORD-ENCRYPTION
```

15. Aktivujte Port security na portech na kterých je třeba.

Je třeba aktivovat na uživatelský portech, v našem případě fa0/1 a fa0/2. Nejdříve je třeba přepnout do access módu.

```
prepinac(config)# INTERFACE fa0/1
prepinac(config-if)# SWITCHPORT MODE ACCESS
prepinac(config-if)# SWITCHPORT PORT-SECURITY
```

```
prepinac(config)# INTERFACE fa0/1
prepinac(config-if)# SWITCHPORT MODE ACCESS
prepinac(config-if)# SWITCHPORT PORT-SECURITY
```

16. Nastavte port fastEthernet 0/24 jako trusted port ke kterému bude připojený DHCP server.

```
prepinac(config)# INTERFACE fa0/24
prepinac(config-if)# IP DHCP SNOOPING TRUST
```

17. Vypněte všechny nepoužité porty.

```
prepinac(config)# INTERFACE RANGE fastEthernet 0/3-23
prepinac(config-if-range)# SHUTDOWN
```

18. Klientské porty nastavte tak, aby mohli vysílat pouze 10 DHCP zpráv za 1 s.

```
prepinac(config)# INTERFACE RANGE fastEthernet 0/1-2
prepinac(config-if-range)# IP DHCP SNOOPING LIMIT RATE 10
```

19. Pro oba porty, na kterých jsou připojeni klienti nastavte maximum MAC adres na 5.

```
prepinac(config)# INTERFACE RANGE fastEthernet 0/1-2
prepinac(config-if-range)# SWITCHPORT PORT-SECURITY MAXIMUM 5
```

20. Nastavte mód porušení pravidel na takový, aby při porušení bylo vyvolána zpráva SNMP protokolu o porušení pravidel.

```
prepinac(config)# INTERFACE RANGE fastEthernet 0/1-2
prepinac(config-if-range)# SWITCHPORT PORT-SECURITY VIOLATION
RESTRICT
```

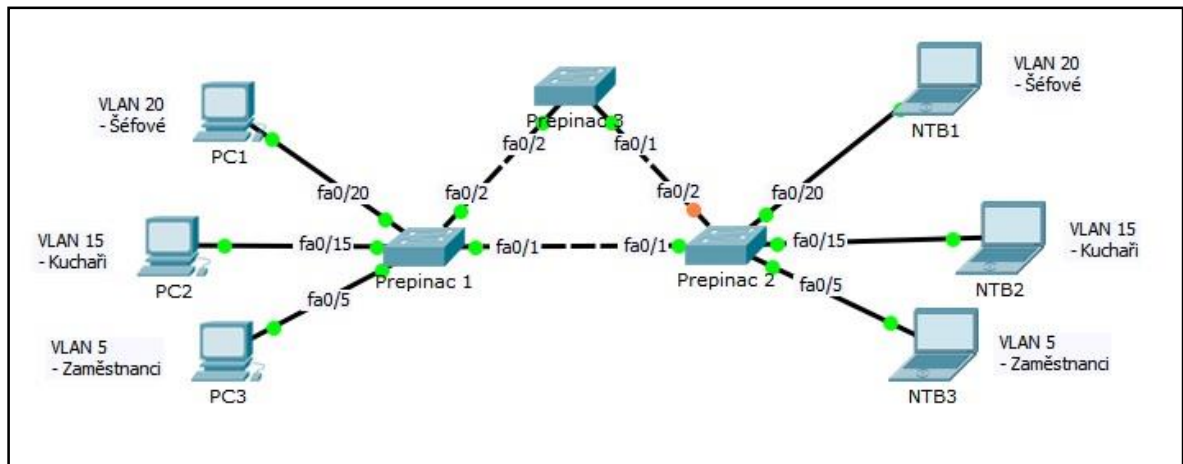
21. Uložte konfiguraci.

```
prepinac# COPY RUNNING-CONFIG STARTUP-CONFIG
```

22. Vypněte a zapněte či reloadujte přepínač a pingněte znovu.

```
prepinac# RELOAD
```

## 15 ÚLOHA 3 – NASTAVENÍ VLAN



Obr. 24. Úloha 3 – Zadání v PT.

### 15.1 Zadání

V této úloze budete konfigurovat VLAN síť.

1. V této úloze konfigurujte VLAN 5 – Zaměstnanci, VLAN 15 – Kuchaři a VLAN 20 – Šéfové pro potřebu hostů. Dále konfigurujte VLAN 80 – Správa pro správu přepínačů a VLAN 99 jako nativní VLAN.
2. Pro VLAN 5 vyberte IP adresy z třídy A pro aspoň 1022 hostů.  
Pro VLAN 15 vyberte IP adresy z třídy B pro aspoň 254 hostů.  
Pro VLAN 20 vyberte IP adresy z třídy C pro aspoň 62 hostů.  
Pro VLAN 80 vyberte IP adresy z třídy C pro aspoň 6 hostů.
3. Konfigurujte z počítačů přes konzolový kabel.
4. Nakonfigurujte hostnamy přepínačů podle obr. č. 1., heslo do privilegovaného režimu nastavte na class, hesla pro vzdálený a konzolový přístup nakonfigurujte na cisco.
5. Vytvořte VLANy a správně je pojmenujte.
6. Správně přiřaďte porty do access a trunk módu.
7. Vypněte DTP na trunk portech.
8. Na trunk spojeních povolte pouze ty VLANy které potřebují komunikovat.
9. Pro vzdálený přístup pro SVI virtuální porty VLAN 80 na všech přepínačích použijte první IP pro přepínač 1, druhou IP pro přepínač 2 a třetí IP pro přepínač 3.
10. Vytvořte tyto virtuální porty (SVI) na všech přepínačích.
11. Nakonfigurujte jakékoliv IP adresy pro počítače ze správné podsítě.
12. Uložte konfigurace.
13. Ověřte, že počítače v každé VLAN síti mohou mezi sebou komunikovat.
14. Restartujte či reloadujte přepínače.
15. Ověřte komunikaci znovu.

## 15.2 Řešení

1. V této úloze konfigurujte VLAN 5 – Zaměstnanci, VLAN 15 – Kuchaři a VLAN 20 – Šéfové pro potřebu hostů. Dále konfigurujte VLAN 80 – Správa pro správu přepínačů a VLAN 99 jako nativní VLAN.
2. Pro VLAN 5 vyberte IP adresy z třídy A pro aspoň 1022 hostů.  
Pro VLAN 15 vyberte IP adresy z třídy B pro aspoň 254 hostů.  
Pro VLAN 20 vyberte IP adresy z třídy C pro aspoň 62 hostů.  
Pro VLAN 80 vyberte IP adresy z třídy C pro aspoň 6 hostů.

### Pro VLAN 5 – Zaměstnanci

Privátní IP adresy třídy A jsou v rozsahu 10.0.0.0 až 10.255.255.255

Maska potřebná pro 1022 klientů je /22, 255.255.252.0

Zvolený rozsah:

10.48.4.0/22 – IP podsítě

.4.1 až .7.254 - dostupné pro hosty v síti

.7.255 – broadcastová IP adresa

### Pro VLAN 15 – Kuchaři

Privátní IP adresy třídy B jsou v rozsahu 172.16.0.0 až 172.16.31.255

Maska potřebná pro 254 klientů je /24, 255.255.255.0

Zvolený rozsah:

172.20.45.0/24 – IP podsítě

.1 až .254 - dostupné pro hosty v síti

.255 – broadcastová IP adresa

### Pro VLAN 20 – Šéfové

Privátní IP adresy třídy C jsou v rozsahu 192.168.0.0 až 192.168.255.255

Maska potřebná pro 62 klientů je /26, 255.255.255.192

Zvolený rozsah:

192.168.27.0/26 – IP podsítě

.1 až .62 - dostupné pro hosty v síti

.63 – broadcastová IP adresa

### Pro VLAN 80 – Správa

Privátní IP adresy třídy C jsou v rozsahu 192.168.0.0 až 192.168.255.255

Maska potřebná pro 6 klientů je /29, 255.255.255.248

Zvolený rozsah:

192.168.80.0/29 – IP podsítě

.1 až .6 - dostupné pro hosty v síti

.7 – broadcastová IP adresa

3. Konfigurujte z počítačů přes konzolový kabel.
4. Nakonfigurujte hostnamy přepínačů podle obr. č. 1., heslo do privilegovaného režimu nastavte na class, hesla pro vzdálený a konzolový přístup nakonfigurujte na cisco.

Popsáno v řešení úloh 1. a 2.

5. Vytvořte VLANy a správně je pojmenujte.

```
prepinac1(config)# VLAN 5
prepinac1(config-vlan)# NAME Zamestnanci
```

```
prepinac1(config)# VLAN 15
prepinac1(config-vlan)# NAME Kuchari
```

```
prepinac1(config)# VLAN 20
prepinac1(config-vlan)# NAME Sefove
```

```
prepinac1(config)# VLAN 80
prepinac1(config-vlan)# NAME Sprava
```

```
prepinac1(config)# VLAN 99
prepinac1(config-vlan)# NAME NativeVLAN
```

Toto nastavení je třeba provést na všech 3 přepínačích.

6. Správně přiřadíte porty do access a trunk módu.

Porty na které jsou připojení hosti musí být přiřazeny do access módu a do správné VLAN sítě.

Porty, které přenášejí data z více VLAN sítí musí být nastaveny do trunk módu a musí být přiřazeny do nativní VLAN sítě.

Nastavení přepínače 1:

```
prepinac1(config)# INTERFACE fa0/5
prepinac1(config-if)# SWITCHPORT MODE ACCESS
prepinac1(config-if)# SWITCHPORT ACCESS VLAN 5
```

```
prepinac1(config)# INTERFACE fa0/15
prepinac1(config-if)# SWITCHPORT MODE ACCESS
prepinac1(config-if)# SWITCHPORT ACCESS VLAN 15
```

```
prepinac1(config)# INTERFACE fa0/20
prepinac1(config-if)# SWITCHPORT MODE ACCESS
prepinac1(config-if)# SWITCHPORT ACCESS VLAN 20
```

```
prepinac1(config)# INTERFACE fa0/1
prepinac1(config-if)# SWITCHPORT MODE TRUNK
prepinac1(config-if)# SWITCHPORT TRUNK NATIVE VLAN 99
```

```
prepinac1(config)# INTERFACE fa0/2
prepinac1(config-if)# SWITCHPORT MODE TRUNK
prepinac1(config-if)# SWITCHPORT TRUNK NATIVE VLAN 99
```

Nastavení přepínače 2:

```
prepinac2(config)# INTERFACE fa0/5
prepinac2 (config-if)# SWITCHPORT MODE ACCESS
prepinac2 (config-if)# SWITCHPORT ACCESS VLAN 5
```

```
prepinac2 (config)# INTERFACE fa0/15
prepinac2 (config-if)# SWITCHPORT MODE ACCESS
prepinac2 (config-if)# SWITCHPORT ACCESS VLAN 15
```

```
prepinac2 (config)# INTERFACE fa0/20
prepinac2 (config-if)# SWITCHPORT MODE ACCESS
prepinac2 (config-if)# SWITCHPORT ACCESS VLAN 20
```

```
prepinac2 (config)# INTERFACE fa0/1
prepinac2 (config-if)# SWITCHPORT MODE TRUNK
prepinac2 (config-if)# SWITCHPORT TRUNK NATIVE VLAN 99
```

```
prepinac2 (config)# INTERFACE fa0/2
prepinac2 (config-if)# SWITCHPORT MODE TRUNK
prepinac2 (config-if)# SWITCHPORT TRUNK NATIVE VLAN 99
```

Nastavení přepínače 3:

```
prepinac3 (config)# INTERFACE fa0/1
prepinac3 (config-if)# SWITCHPORT MODE TRUNK
prepinac3 (config-if)# SWITCHPORT TRUNK NATIVE VLAN 99
```

```
prepinac3 (config)# INTERFACE fa0/2
prepinac3 (config-if)# SWITCHPORT MODE TRUNK
prepinac3 (config-if)# SWITCHPORT TRUNK NATIVE VLAN 99
```

## 7. Vypněte DTP na trunk portech.

Je třeba vypnout automatizované vyjednávání o módu portu na všech trunk portech.

```
prepinac1 (config)# INTERFACE RANGE fa 0/1 – 2
prepinac1 (config-if-range)# SWITCHPORT NONEGOTIATE
```

Toto nastavení je třeba provést na všech trunk portech.

**8. Na trunk spojeních povolte pouze ty VLANy které potřebují komunikovat.**

V tomto případě je třeba na všech trunk portech povolit VLAN 1,5,15,20,80,99. VLAN 1 proto, že přenáší řídicí informace protokolů jako CDP či VTP a jiné.

```
prepinac1 (config)# INTERFACE RANGE fa 0/1 – 2
prepinac1(config-if-range)# SWITCHPORT TRUNK ALLOWED VLAN
1,5,15,20,80,99
```

Toto nastavení je třeba provést na všech trunk portech.

**9. Pro vzdálený přístup pro SVI virtuální porty VLAN 80 na všech přepínačích použijte první IP pro přepínač 1, druhou IP pro přepínač 2 a třetí IP pro přepínač 3.**

Pro přepínač 1: 192.168.80.1/29

Pro přepínač 2: 192.168.80.2/29

Pro přepínač 3: 192.168.80.3/29

**10. Vytvořte tyto virtuální porty (SVI) na všech přepínačích.**

```
prepinac1 (config)# INTERFACE VLAN 80
prepinac1 (config-if)# IP ADDRESS 192.168.80.1 255.255.255.248
```

```
prepinac2 (config)# INTERFACE VLAN 80
prepinac2 (config-if)# IP ADDRESS 192.168.80.2 255.255.255.248
```

```
prepinac3 (config)# INTERFACE VLAN 80
prepinac3 (config-if)# IP ADDRESS 192.168.80.3 255.255.255.248
```

**11. Vyzkoušejte se na přepínač 1 připojit pomocí telnetu.**

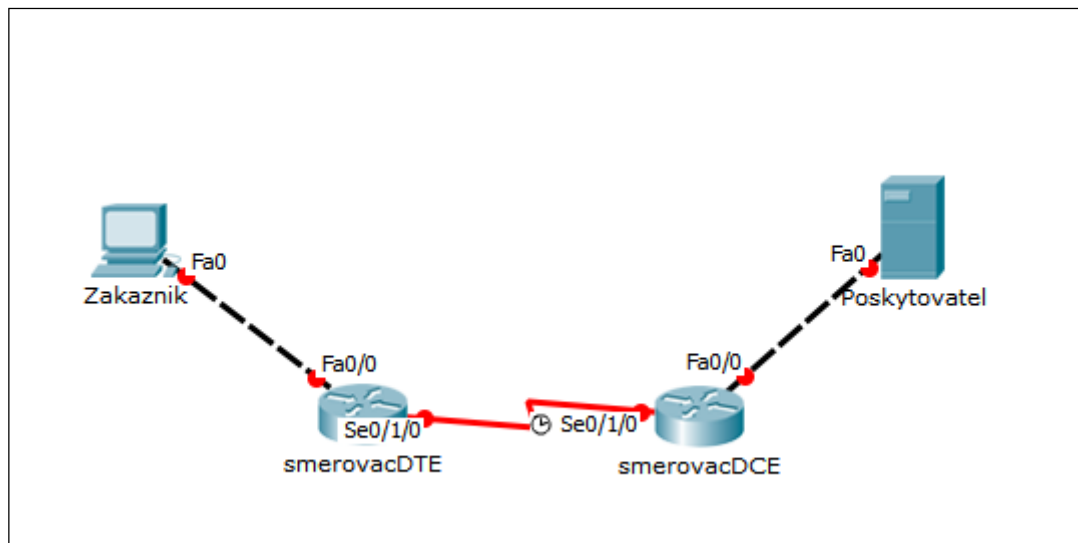
Pro vzdálený přístup je potřeba, aby aspoň 1 port byl přiřazen do VLAN sítě pro správu. Proto port fa0/8 přiřadíte do VLAN 80, připojíte počítač a do něj nakonfigurujete IP adresu z podsítě, kterou jsme si vyhradili pro Správu.

**12. Nakonfigurujte jakékoliv IP adresy pro počítače ze správné podsítě.****13. Uložte konfigurace.**

Viz úloha 1 a 2.

**14. Ověřte, že počítače v každé VLAN síti mohou mezi sebou komunikovat.****15. Restartujte či reloadujte přepínače.****16. Ověřte komunikaci znovu.**

## 16 ÚLOHA 4 – NASTAVOVÁNÍ PORTŮ SMĚROVAČE



Obr. 25. Úloha 4 – Zadání v PT.

### 16.1 Zadání

V této úloze budete simulovat poskytovatele na straně DCE a zákazníka na straně DTE.

1. Pro zákazníka si vyberte síť pro 254 klientů, pro poskytovatele si vyberte síť pro 32 klientů a pro spoj mezi směrovači síť pro 2 klienty.
2. Na směrovačích nakonfigurujte hostnamy podle popisků, heslo pro privilegovaný mód na class a hesla pro konzolový a vzdálený přístup na cisco.
3. Směrovači DCE přiřadíte první dostupnou IP a pro směrovač DTE poslední dostupnou IP adresu a pro porty směřující k zákazníkovi a poskytovateli první dostupnou IP adresu.
4. Stranu DCE nakonfigurujte tak, aby pro zákazníka byla dostupná linka o rychlosti 250 kb/s
5. Pro hosty konfigurujte příslušné dostupné adresy z daných sítí, masku a bránu.
6. Pingněte brány a mezi směrovači.

### 16.2 Řešení

1. Pro zákazníka si vyberte síť pro 254 klientů, pro poskytovatele si vyberte síť pro 32 klientů a pro spoj mezi směrovači síť pro 2 klienty.

#### Pro zákazníka

Zvolený rozsah:

192.168.1.0/24 – IP podsítě, 255.255.255.0  
 .1 až .254 - dostupné pro hosty v síti  
 .255 – broadcastová IP adresa

Pro poskytovatele

Zvolený rozsah:

192.168.100.0/27 – IP podsítě, 255.255.255.224  
.1 až .30 - dostupné pro hosty v síti  
.31 – broadcastová IP adresa

Spoj mezi DTE a DCE směrovačem

Zvolený rozsah:

10.0.0.0/30 – IP podsítě, 255.255.255.252  
.1 až .2 - dostupné pro hosty v síti  
.3 – broadcastová IP adresa

2. Na směrovačích nakonfigurujte hostnamy podle popisků, heslo pro privilegovaný mód na class a hesla pro konzolový a vzdálený přístup na cisco.

Viz předchozí úlohy.

3. Směrovači DCE přiřadíte první dostupnou IP a pro směrovač DTE poslední dostupnou IP adresu a pro porty směřující k zákazníkovi a poskytovateli první dostupnou IP adresu.

Pro DCE směrovač: 10.0.0.1/30

Pro DTE směrovač: 10.0.0.2/30

```
smerovacDCE(config)# INTERFACE s0/1/0  
smerovacDCE(config-if)# IP ADDRESS 10.0.0.1 255.255.255.252
```

```
smerovacDTE(config)# INTERFACE s0/1/0  
smerovacDTE(config-if)# IP ADDRESS 10.0.0.2 255.255.255.252
```

Pro fa0/0 u DCE: 192.168.100.1/27

Pro fa0/0 u DTE: 192.168.1.1/24

```
smerovacDCE(config)# INTERFACE fa0/0  
smerovacDCE(config-if)# IP ADDRESS 192.168.100.1 255.255.255.224
```

```
smerovacDTE(config)# INTERFACE fa0/0  
smerovacDTE(config-if)# IP ADDRESS 192.168.1.1 255.255.255.0
```

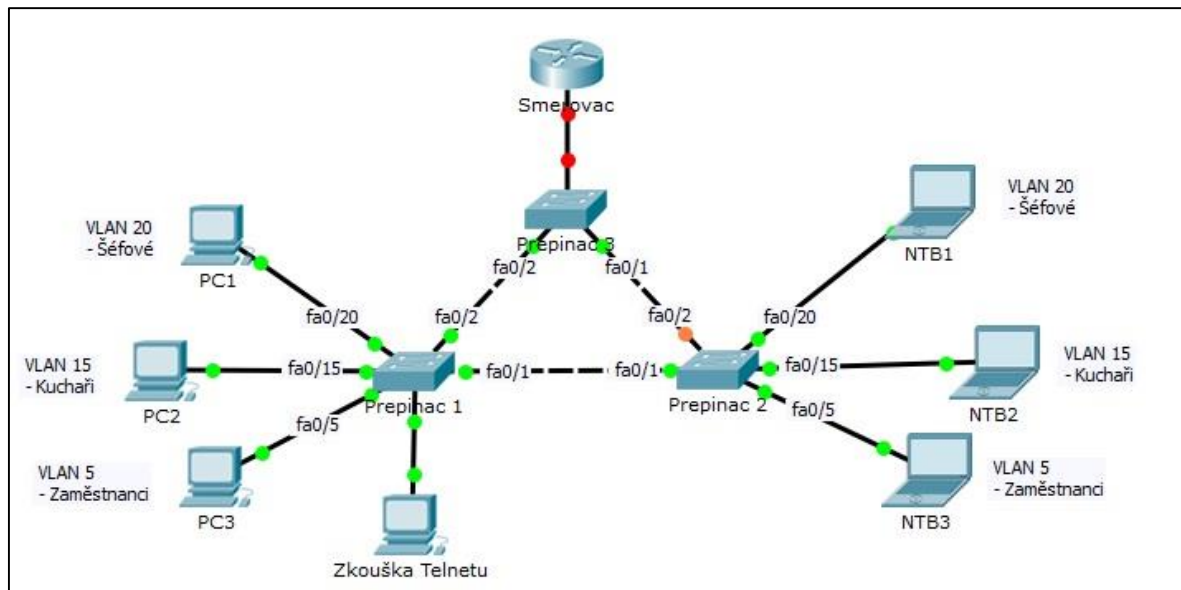
4. Stranu DCE nakonfigurujte tak, aby pro zákazníka byla dostupná linka o rychlosti 250 kb/s.

Pro DCE konec, který patří poskytovateli je třeba nastavit rychlost, aby zákazník dostal tolik za kolik si zaplatil a také poskytnout synchronizaci obou stran. Pro tento účel slouží příkaz CLOCK RATE {počet\_bitů\_za\_sekundu}. Zákazník si zaplatil za 250 kb/s což je 250000 bitů/s.

```
smerovacDCE(config)# INTERFACE s0/1/0  
smerovacDCE(config-if)# CLOCK RATE 250000
```

5. Pro hosty konfiguruje příslušné dostupné adresy z daných sítí, masku a bránu.
6. Pingněte brány a mezi směrovači.

## 17 ÚLOHA 5 – INTER-VLAN SMĚROVÁNÍ



Obr. 26. Úloha 5 – Zadání v PT.

### 17.1 Zadání

V této úloze je použito úlohy 3 – nastavování VLAN. V téhle úloze budeme nastavovat Inter-VLAN směrování na směrovači.

1. Nakonfigurujte hostname smerovac, heslo pro privilegovaný mód, konzolový a vzdálený přístup.
2. Nakonfigurujte Inter-VLAN směrování na portu směrovače pro VLAN sítě 5,15,20,80. Pro subinterfacy zvolte poslední dostupnou IP adresu.  
Port fa 0/24 je použit na přepínači 3 směrem k směrovači. Na směrovači je použit port fa 0/0.
3. Nakonfigurujte brány na počítačích.
4. Ověřte, že lze pingovat mezi počítači v různých VLAN sítích.
5. Zařídte ať je možno se vzdáleně připojit k přepínačům z jakékoliv VLAN sítě.

### 17.2 Řešení

1. **Nakonfigurujte hostname smerovac, heslo pro privilegovaný mód, konzolový a vzdálený přístup.**  
Vysvětleno v předcházejících úlohách.
2. **Nakonfigurujte Inter-VLAN směrování na portu směrovače pro VLAN sítě 5,15,20,80. Pro subinterfacy zvolte poslední dostupnou IP adresu.**  
Port fa 0/24 je použit na přepínači 3 směrem k směrovači. Na směrovači je použit port fa 0/0.

Port fa0/24 je třeba dát do módu trunk:

```
prepinac3(config-if)# SWITCHPORT MODE TRUNK
```

Konfigurace subinterfacu pro VLAN 5:

```
smerovac(config)# INTERFACE fa0/0.5
```

Tímto příkazem se dostanete do konfigurace subinterfacu.

```
smerovac(config-subif)# ENCAPSULATION DOT1Q 5
```

Tímto příkazem nastavíte, že do rámce je přidáno 802.1Q označení pro VLAN 5.

```
smerovac(config-subif)# IP ADDRESS 10.48.7.254 255.255.252.0
```

Konfigurace subinterfacu pro VLAN 15:

```
smerovac(config)# INTERFACE fa0/0.15
```

```
smerovac(config-subif)# ENCAPSULATION DOT1Q 15
```

```
smerovac(config-subif)# IP ADDRESS 172.20.45.254 255.255.255.0
```

Konfigurace subinterfacu pro VLAN 20:

```
smerovac(config)# INTERFACE fa0/0.20
```

```
smerovac(config-subif)# ENCAPSULATION DOT1Q 20
```

```
smerovac(config-subif)# IP ADDRESS 192.168.27.62 255.255.255.192
```

Konfigurace subinterfacu pro VLAN 80:

```
smerovac(config)# INTERFACE fa0/0.80
```

```
smerovac(config-subif)# ENCAPSULATION DOT1Q 80
```

```
smerovac(config-subif)# IP ADDRESS 192.168.80.6 255.255.255.248
```

Na konci je třeba ještě port aktivovat:

```
smerovac(config)# INTERFACE fa0/0
```

```
smerovac(config-if)# NO SHUTDOWN
```

### 3. Nakonfigurujte brány na počítačích.

Brány jsou v tomto případě IP adresy subinterfaců. Jelikož je to odchozí IP adresa z dané VLAN sítě.

### 4. Ověřte, že lze pingovat mezi počítači v různých VLAN sítích.

### 5. Zaříd'te at' je možno se vzdáleně připojit k přepínačům z jakékoliv VLAN sítě.

Důvod proč nelze pingnout ze stanic ve VLAN sítích 5,15,20 je ten, že přepínače nemají nastavenou bránu.

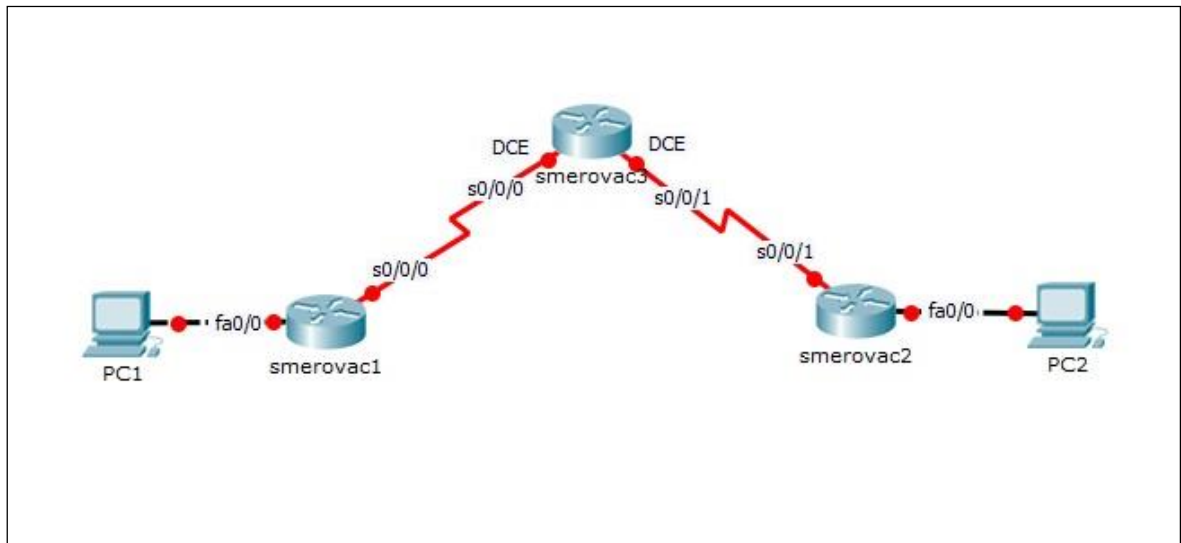
Pro nastavení brány na přepínači slouží:

```
prepinac1(config)# IP DEFAULT-GATEWAY 192.168.80.6
```

```
prepinac2(config)# IP DEFAULT-GATEWAY 192.168.80.6
```

```
prepinac3(config)# IP DEFAULT-GATEWAY 192.168.80.6
```

## 18 ÚLOHA 6 – STATICKÉ SMĚROVÁNÍ



Obr. 27. Úloha 6 – Zadání v PT.

### 18.1 Zadání

V této úloze budete konfigurovat statické směrování.

1. Vyberte IP adresy pro sítě.  
Sít' s PC1 – 14 hostů  
Sít' z PC2 – 30 hostů  
Pro sítě mezi směrovači, vyberte tolik kolik je potřeba, ani o jeden více.
2. Nakonfigurujte hostnamy podle obrázku, pro heslo do privilegovaného režimu zvolte class a pro konzolový a vzdálený přístup cisco.
3. Pro porty směrovačů vedoucí směrem k sítím s pc 1 a pc 2 zvolte první dostupnou IP adresu, pro počítače si vyberte, jaké chcete.
4. První dostupné IP adresy přiřaďte směrovači 3 a nakonfigurujte rychlost linky na 64 kb/s.
5. Vytvořte loopback rozhraní na směrovači 3 ke kterému bude vést výchozí cesta (Simulace internetového připojení).
6. Nakonfigurujte statické směrování.
7. Pingněte z PC1 na PC2 a naopak.
8. Zjednodušte směrovací tabulky v přepínačích 1 a 2.

### 18.2 Řešení

1. Vyberte IP adresy pro sítě.  
Sít' s PC1 – 14 hostů  
Sít' s PC2 – 30 hostů  
Pro sítě mezi směrovači, vyberte tolik kolik je potřeba, ani o jeden více.

Pro síť s PC2 – 10.1.1.0/27  
Pro síť s PC1 – 10.1.1.32/28  
Spoj mezi směrovačem 1 a směrovačem 3 – 10.1.1.48/30  
Spoj mezi směrovačem 3 a směrovačem 2 – 10.1.1.52/30

2. **Nakonfigurujte hostnamy podle obrázku, pro heslo do privilegovaného režimu zvolte class a pro konzolový a vzdálený přístup cisco.**

Vysvětleno v předcházejících úlohách.

3. **Pro porty směrovačů vedoucí směrem k sítím s pc 1 a pc 2 zvolte první dostupnou IP adresu, pro počítače si vyberte, jaké chcete.**

Pro port fa0/0 směrovače 1 – 10.1.1.33/28

Pro port fa0/0 směrovače 2 – 10.1.1.1/27

4. **První dostupné IP adresy přiřadte směrovači 3 a nakonfigurujte rychlost linky na 64 kb/s.**

Směrovač 3 s0/0/0 – 10.1.1.49/30

Směrovač 3 s0/0/1 – 10.1.1.53/30

Konfigurace rychlosti linek:

```
smerovac3(config)# INTERFACE s0/0/0  
smerovac3(config-if)# CLOCK RATE 64000
```

```
smerovac3(config)# INTERFACE s0/0/1  
smerovac3(config-if)# CLOCK RATE 64000
```

5. **Vytvořte loopback rozhraní na směrovači 3 ke kterému bude vést výchozí cesta. (Simulace internetového připojení)**

Pro loopback 0 si můžete zvolit síť 172.16.0.0/24.

```
smerovac3(config)# INTERFACE loopback 0  
smerovac3(config-if)# IP ADDRESS 172.16.0.1 255.255.255.0
```

6. **Nakonfigurujte statické směrování.**

Pro směrovač 1:

```
smerovac1(config)# IP ROUTE 10.1.1.52 255.255.255.252 Serial0/0/0  
smerovac1(config)# IP ROUTE 10.1.1.0 255.255.255.224 Serial0/0/0
```

Pro směrovač 2:

```
smerovac2(config)# IP ROUTE 10.1.1.32 255.255.255.240 Serial0/0/1  
smerovac2(config)# IP ROUTE 10.1.1.48 255.255.255.252 Serial0/0/1
```

Pro směrovač 3:

```
smerovac3(config)# IP ROUTE 0.0.0.0 0.0.0.0 Loopback0  
smerovac3(config)# IP ROUTE 10.1.1.32 255.255.255.240 Serial0/0/0  
smerovac3(config)# IP ROUTE 10.1.1.0 255.255.255.224 Serial0/0/1
```

7. **Pingněte z PC1 na PC2 a naopak.**

**8. Zjednodušte směrovací tabulky v přepínačích 1 a 2.**

Jelikož z LAN sítí u směrovačů vede jenom jedna cesta ven přes směrovače, nazývají se tyto sítě stub networks (koncové sítě). Místo výše zmíněných cest lze použít výchozí cesty.

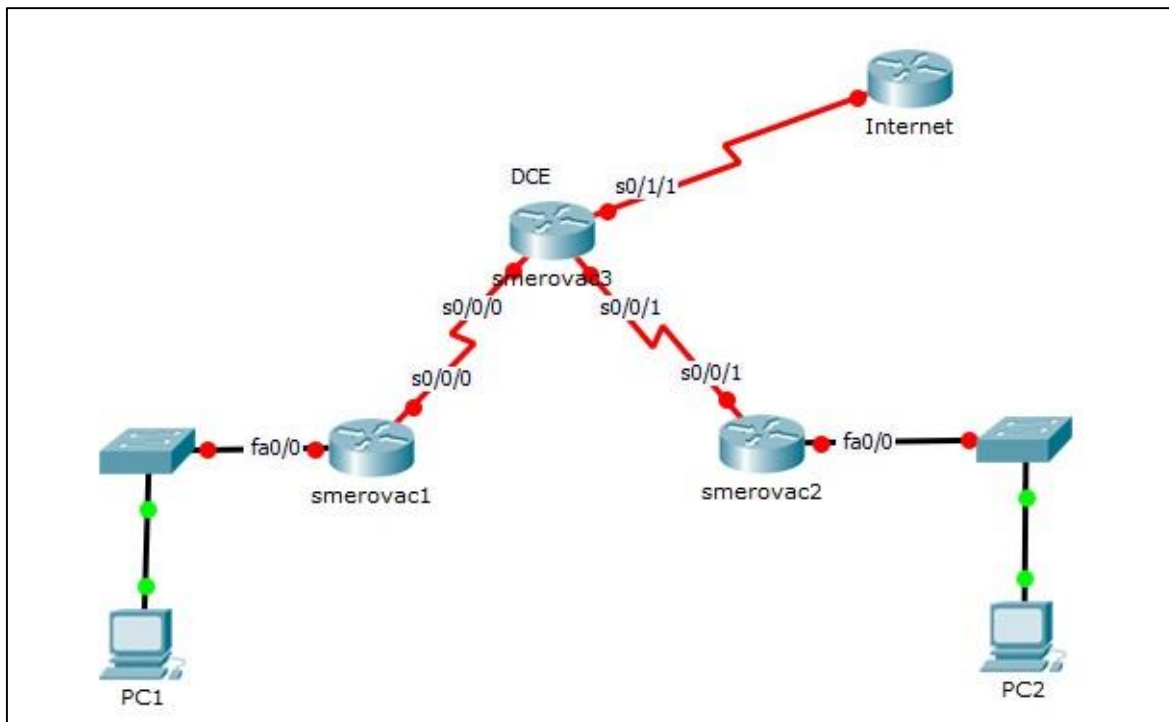
Pro směrovač 1:

```
smerovac1(config)# IP ROUTE 0.0.0.0 0.0.0.0 Serial0/0/0
```

Pro směrovač 2:

```
smerovac2(config)# IP ROUTE 0.0.0.0 0.0.0.0 Serial0/0/1
```

## 19 ÚLOHA 7 – KONFIGURACE RIPV2



Obr. 28. Úloha 7 – Zadání v PT.

### 19.1 Zadání

V této úloze budete konfigurovat RIPv2 směrování.

1. Vyberte IP adresy pro sítě.  
 Síť s PC1 – 58 hostů  
 Síť z PC2 – 94 hostů  
 Pro síť mezi směrovači, vyberte tolik kolik je potřeba, ani o jeden více. Spojení mezi směrovačem 3 a Internetem je již nakonfigurováno (IP adresa Internetu je 172.16.0.1).
2. Nakonfigurujte hostnamy podle obrázku, pro heslo do privilegovaného režimu zvolte class a pro konzolový a vzdálený přístup cisco.
3. Pro porty směrovačů vedoucí směrem k sítím s pc 1 a pc 2 zvolte první dostupnou IP adresu, pro počítače si vyberte, jaké chcete.
4. První dostupné IP adresy přiřaďte směrovači 3 a nakonfigurujte rychlost linky na 128 kb/s.
5. Nakonfigurujte výchozí cestu směrem k Internetu.
6. Nakonfigurujte RIPv2 směrování a vypněte autosumarizaci.
7. Distribuuje statickou cestu do směrovačů 1 a 2.
8. Vypněte aktualizace směrovacích protokolů na portech, kde nejsou třeba.
9. Pingněte z PC1 na PC2 a naopak, pingněte z PC1 a PC2 Internet.

## 19.2 Řešení

### 1. Vyberte IP adresy pro síť.

Pro síť mezi směrovači, vyberte tolik kolik je potřeba, ani o jeden více. Spojení mezi směrovačem 3 a Internetem je již nakonfigurováno (IP adresa Internetu je 172.16.0.1).

Síť s PC1 – 58 hostů - 192.168.1.0/26

Síť z PC2 – 94 hostů - 192.168.2.0/25

Směrovač 1 – Směrovač 3 - 10.2.1.0/30

Směrovač 2 – Směrovač 3 - 10.2.1.4/30

### 2. Nakonfigurujte hostnamy podle obrázku, pro heslo do privilegovaného režimu zvolte class a pro konzolový a vzdálený přístup cisco.

Vysvětleno v předcházejících úlohách.

Malý tip pro zjednodušení: Pokud se vám nechce pořád psát stejné příkazy, zkopírujte si je do .txt a pak je jenom kopírujte do příkazové řádky.

### 3. Pro porty směrovačů vedoucí směrem k sítím s pc 1 a pc 2 zvolte první dostupnou IP adresu, pro počítače si vyberte, jaké chcete.

Pro fa0/0 u směrovače 1 - 192.168.1.1/26

Pro fa0/0 u směrovače 2 - 192.168.2.1/26

Konfigurace v předcházejících úlohách.

### 4. První dostupné IP adresy přiřaďte směrovači 3 a nakonfigurujte rychlost linky na 128 kb/s. Rychlost linky se nastavuje pomocí CLOCK RATE, vysvětlení v přechozích úlohách.

### 5. Nakonfigurujte výchozí cestu směrem k Internetu.

```
smerovac3(config)# IP ROUTE 0.0.0.0 0.0.0.0 s0/1/1
```

### 6. Nakonfigurujte RIPv2 směrování a vypněte autosumarizaci.

Konfigurace pro směrovač 1:

```
smerovac1(config)# ROUTER RIP
```

Aktivace RIP směrování na směrovači.

```
smerovac1(config-router)# VERSION 2
```

Volba RIPv2.

```
smerovac1(config-router)# NO AUTO-SUMMARY
```

Vypnutí autosumarizace.

```
smerovac1(config-router)# NETWORK 192.168.1.0
```

Přidání sítě 192.168.1.0 do směrovacího protokolu.

```
smerovac1(config-router)# NETWORK 10.0.0.0
Přidání sítě 10.0.0.0 do směrovacího protokolu.
```

Konfigurace pro směrovač 2:

```
smerovac2(config)# ROUTER RIP
smerovac2(config-router)# VERSION 2
smerovac2(config-router)# NO AUTO-SUMMARY
smerovac2(config-router)# NETWORK 192.168.2.0
smerovac2(config-router)# NETWORK 10.0.0.0
```

Konfigurace pro směrovač 3:

```
smerovac3(config)# ROUTER RIP
smerovac3(config-router)# VERSION 2
smerovac3(config-router)# NO AUTO-SUMMARY
smerovac3(config-router)# NETWORK 10.0.0.0
```

### 7. Distribuuje statickou cestu do směrovačů 1 a 2.

Na směrovači 3:

```
smerovac3(config-router)# DEFAULT-INFO ORIGINATE
```

### 8. Vypněte aktualizace směrovacích protokolů na portech, kde nejsou třeba.

Konfigurace pro směrovač 1:

```
smerovac1(config-router)# PASSIVE-INTERFACE fa0/0
```

Vypnuto na tomto portu, jelikož zde není třeba posílat aktualizace RIP protokolu, jelikož na této straně jsou uživatelé.

Konfigurace pro směrovač 2:

```
smerovac2(config-router)# PASSIVE-INTERFACE fa0/0
```

Vypnuto na tomto portu, jelikož zde není třeba posílat aktualizace RIP protokolu, jelikož na této straně jsou uživatelé.

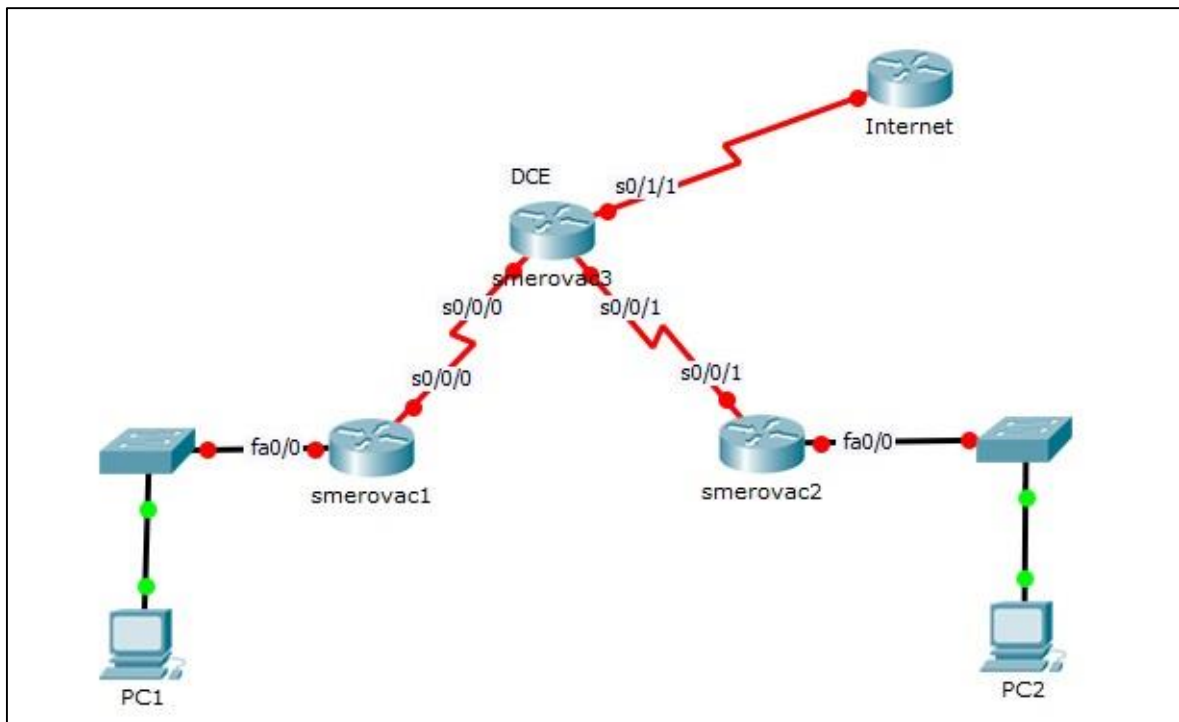
Konfigurace pro směrovač 3:

```
smerovac3(config-router)# PASSIVE-INTERFACE s0/1/1
```

Vypnuto na tomto portu, jelikož, zde je cesta nastavena statickým směrováním.

### 9. Pingněte z PC1 na PC2 a naopak, pingněte z PC1 a PC2 Internet.

## 20 ÚLOHA 8 – KONFIGURACE OSPFV2



Obr. 29. Úloha 8 – Zadání v PT.

### 20.1 Zadání

V této úloze budete konfigurovat OSPFv2 směrování.

1. Vyberte IP adresy pro síť.  
Síť s PC1 – 72 hostů  
Síť z PC2 – 8 hostů  
Pro síť mezi směrovači, vyberte tolik kolik je potřeba, ani o jeden více. Spojení mezi směrovačem 3 a Internetem je již nakonfigurováno (IP adresa Internetu je 172.16.0.1).
2. Nakonfigurujte hostnamy podle obrázku, pro heslo do privilegovaného režimu zvolte class a pro konzolový a vzdálený přístup cisco.
3. Pro porty směrovačů vedoucí směrem k sítím s pc 1 a pc 2 zvolte první dostupnou IP adresu, pro počítače si vyberte, jaké chcete.
4. První dostupné IP adresy přiřaďte směrovači 3 a nakonfigurujte rychlost linky na 250 kb/s.
5. Nakonfigurujte výchozí cestu směrem k Internetu.
6. Nakonfigurujte OSPFv2 směrování.
7. Distribuuje statickou výchozí cestu do směrovačů 1 a 2.
8. Vypněte aktualizace směrovacích protokolů na portech, kde nejsou třeba.
9. Nastavte manuálně referenční propustnost na správnou hodnotu.
10. Pingněte z PC1 na PC2 a naopak, pingněte z PC1 a PC2 Internet.

## 20.2 Řešení

### 1. Vyberte IP adresy pro sítě.

Síť s PC1 – 72 hostů

Síť z PC2 – 8 hostů

Pro sítě mezi směrovači, vyberte tolik kolik je potřeba, ani o jeden více. Spojení mezi směrovačem 3 a Internetem je již nakonfigurováno (IP adresa Internetu je 172.16.0.1).

Síť s PC1 – 72 hostů - 192.168.1.0/25

Síť z PC2 – 8 hostů - 192.168.2.0/28

Směrovač 1 – Směrovač 3 - 10.2.1.0/30

Směrovač 2 – Směrovač 3 - 10.2.1.4/30

### 2. Nakonfigurujte hostnamy podle obrázku, pro heslo do privilegovaného režimu zvolte class a pro konzolový a vzdálený přístup cisco.

V přecházejících úlohách.

### 3. Pro porty směrovačů vedoucí směrem k sítím s pc 1 a pc 2 zvolte první dostupnou IP adresu, pro počítače si vyberte, jaké chcete.

Pro fa0/0 u směrovače 1 - 192.168.1.1/25

Pro fa0/0 u směrovače 2 - 192.168.2.1/28

Konfigurace v předcházejících úlohách.

### 4. První dostupné IP adresy přiřad'te směrovači 3 a nakonfigurujte rychlost linky na 250 kb/s.

Rychlost linky se nastavuje pomocí CLOCK RATE, vysvětlení v přechozích úlohách.

### 5. Nakonfigurujte výchozí cestu směrem k Internetu.

```
smerovac3(config)# IP ROUTE 0.0.0.0 0.0.0.0 s0/1/1
```

### 6. Nakonfigurujte OSPFv2 směrování.

Konfigurace pro směrovač 1:

```
smerovac1(config)# ROUTER OSPF 1
```

Aktivace RIP směrování na směrovači.

```
smerovac1(config-router)# NETWORK 10.2.1.0 0.0.0.3 AREA 0
```

Přidání sítě 10.2.1.0 do směrovacího protokolu.

```
smerovac1(config-router)# NETWORK 192.168.1.0 0.0.0.127 AREA 0
```

Přidání sítě 192.168.1.0 do směrovacího protokolu.

Konfigurace pro směrovač 2:

```
smerovac2(config)# ROUTER OSPF 1
```

```
smerovac2(config-router)# NETWORK 10.2.1.0 0.0.0.3 AREA 0
```

```
smerovac2(config-router)# NETWORK 192.168.2.0 0.0.0.15 AREA 0
```

Konfigurace pro směrovač 3:

```
smerovac3(config)# ROUTER OSPF 1
smerovac3(config-router)# NETWORK 10.2.1.0 0.0.0.3 AREA 0
smerovac3(config-router)# NETWORK 10.2.1.4 0.0.0.15 AREA 0
```

**7. Distribuuje statickou výchozí cestu do směrovačů 1 a 2.**

Redistribuce výchozí statické cesty:

```
smerovac3(config-router)# DEFAULT-INFO ORIGINATE
```

**8. Vypněte aktualizace směrovacích protokolů na portech, kde nejsou třeba.**

Vypnutí aktualizací směrovacího protokolu:

```
smerovac1(config-router)# PASSIVE-INTERFACE fa0/0
smerovac2(config-router)# PASSIVE-INTERFACE fa0/0
smerovac3(config-router)# PASSIVE-INTERFACE s0/0/1
```

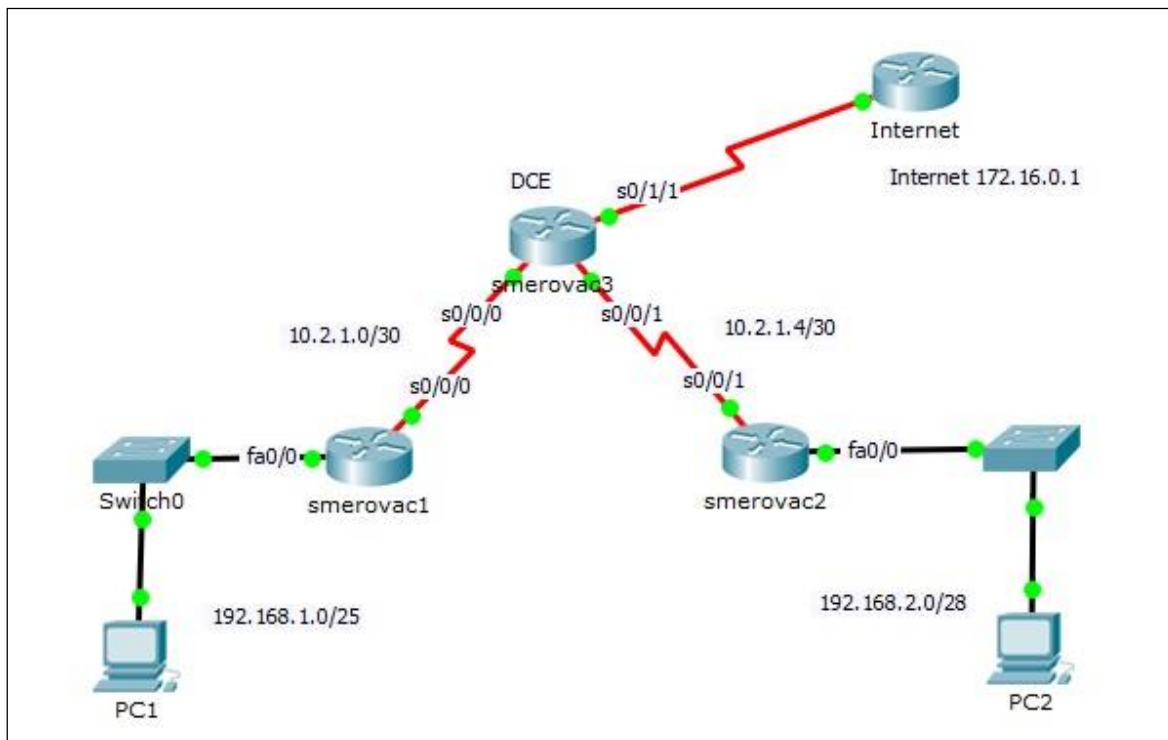
**9. Nastavte manuálně referenční propustnost na správnou hodnotu.**

Nastavení referenční hodnoty:

```
smerovac1(config-router)# AUTO-COST REFERENCE-BANDWIDTH 100
smerovac2(config-router)# AUTO-COST REFERENCE-BANDWIDTH 100
smerovac3(config-router)# AUTO-COST REFERENCE-BANDWIDTH 100
```

**10. Pingněte z PC1 na PC2 a naopak, pingněte z PC1 a PC2 Internet.**

## 21 ÚLOHA 9 – ACL LISTY



Obr. 30. Úloha 9 – Zadání v PT.

### 21.1 Zadání

V této úloze budete konfigurovat ACL listy, je použito sítě z úlohy 8. – konfigurace OSPFv2.

1. Přístup k telnetu na všech směrovačích povolte pouze hostu PC1.
2. Z venkovního Internetu zakažte pingování a telnet a povolte pouze http.
3. Ze sítě z PC2 zakažte FTP přístup na PC1. Vytvořte pojmenovaný ACL list.
4. Ověřte správnou konfiguraci.

### 21.2 Řešení

1. Přístup k telnetu na všech směrovačích povolte pouze hostu PC1.

```
smerovac1(config)# ACCESS-LIST 1 PERMIT HOST 192.168.1.2
```

Konfigurace ACL list, pouze host 192.168.1.2 má povoleno.

```
smerovac1(config)# LINE VTY 0 15
```

```
smerovac1(config-line)# ACCESS-CLASS 1 IN
```

Aplikace na vty lines na směrovači. Je třeba provést na směrovači 1, 2 a 3.

**2. Z venkovního Internetu zakažte pingování a telnet a povolte pouze http.**

```
smerovac3(config)# ACCESS-LIST 100 PERMIT TCP 172.16.0.0 0.0.0.255 any
EQ 80
```

Povolení http protokolu.

```
smerovac3(config)# ACCESS-LIST 100 PERMIT ICMP 172.16.0.0 0.0.0.255 any
echo-reply
```

Povolení odpovědí ping, aby bylo možno pingnout Internet.

```
smerovac3(config)# ACCESS-LIST 100 DENY ICMP 172.16.0.0 0.0.0.255 any
echo
```

Zákaz ping požadavků, aby nebylo možno pingnout z Internetu do vnitřní sítě.

```
smerovac3(config)# ACCESS-LIST 100 DENY TCP 172.16.0.0 0.0.0.255 any EQ
23
```

Zákaz telnetu, aby nebyl možný vzdálený přístup do sítě LAN.

```
smerovac3(config)# INTEFACE s0/1/1
```

```
smerovac3(config-if)# IP ACCESS-GROUP 100 IN
```

Aplikace pravidel na port.

**3. Ze sítě z PC2 zakažte FTP přístup na PC1. Vytvořte pojmenovaný ACL list.**

```
smerovac2(config)# IP ACCESS-LIST EXTENDED ftpZakaz
Vytvoření pojmenovaného ACL listu.
```

```
smerovac2(config-ext-nacl)# DENY TCP 192.168.2.0 0.0.0.255 HOST
192.168.1.2 EQ 21
```

```
smerovac2(config-ext-nacl)# DENY TCP 192.168.2.0 0.0.0.255 HOST
192.168.1.2 EQ 20
```

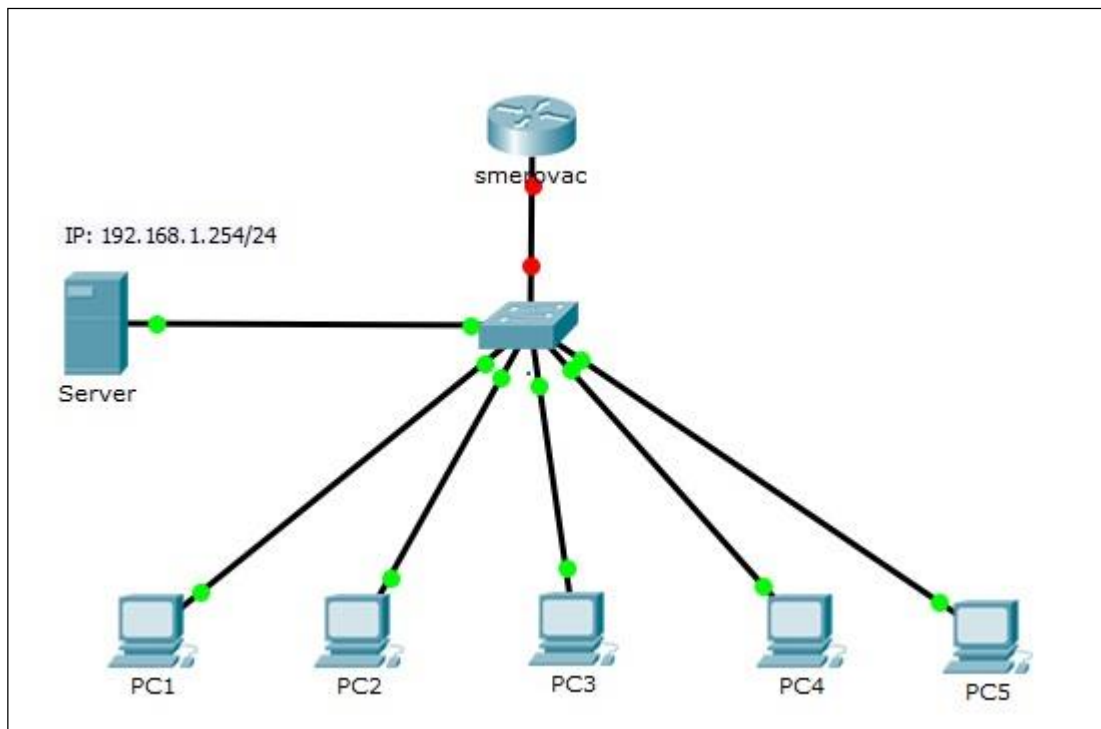
Zákaz FTP, 21 je řídicí port a 20 je datový port.

```
smerovac2(config-ext-nacl)# PERMIT IP ANY ANY
```

Povolení všeho ostatního provozu.

**4. Ověřte správnou konfiguraci.**

## 22 ÚLOHA 10 – DHCP



Obr. 31. Úloha 10 – Zadání v PT.

### 22.1 Zadání

V této úloze budete konfigurovat DHCP.

1. V této úloze používejte podsíť 192.168.1.0/24. Pro port na směrovači vyberte první dostupnou IP adresu.
2. Nastavte název směrovače na smerovac, nastavte heslo do privilegovaného režimu na class a do konzolového přístupu a vzdáleného přístupu na cisco.
3. Vyjměte ty IP adresy, které nemají být přidělovány.
4. Vytvořte rozsah IP adres pro DHCP.
5. Pingněte z počítačů na server a směrovač.

### 22.2 Řešení

1. **V této úloze používejte podsíť 192.168.1.0/24. Pro port na směrovači vyberte první dostupnou IP adresu.**  
IP adresa pro směrovač: 192.168.1.1/24
2. **Nastavte název směrovače na smerovac, nastavte heslo do privilegovaného režimu na class a do konzolového přístupu a vzdáleného přístupu na cisco, nastavte IP adresu portu na směrovači.**  
V přecházejících úlohách.

**3. Vyjměte ty IP adresy, které nemají být přidělovány.**

```
smerovac(config)# IP DHCP EXCLUDED ADDRESS 192.168.1.1  
smerovac(config)# IP DHCP EXCLUDED ADDRESS 192.168.1.254
```

Tyto adresy jsou vyjmuty, protože jsou použity pro server a port na směrovači.

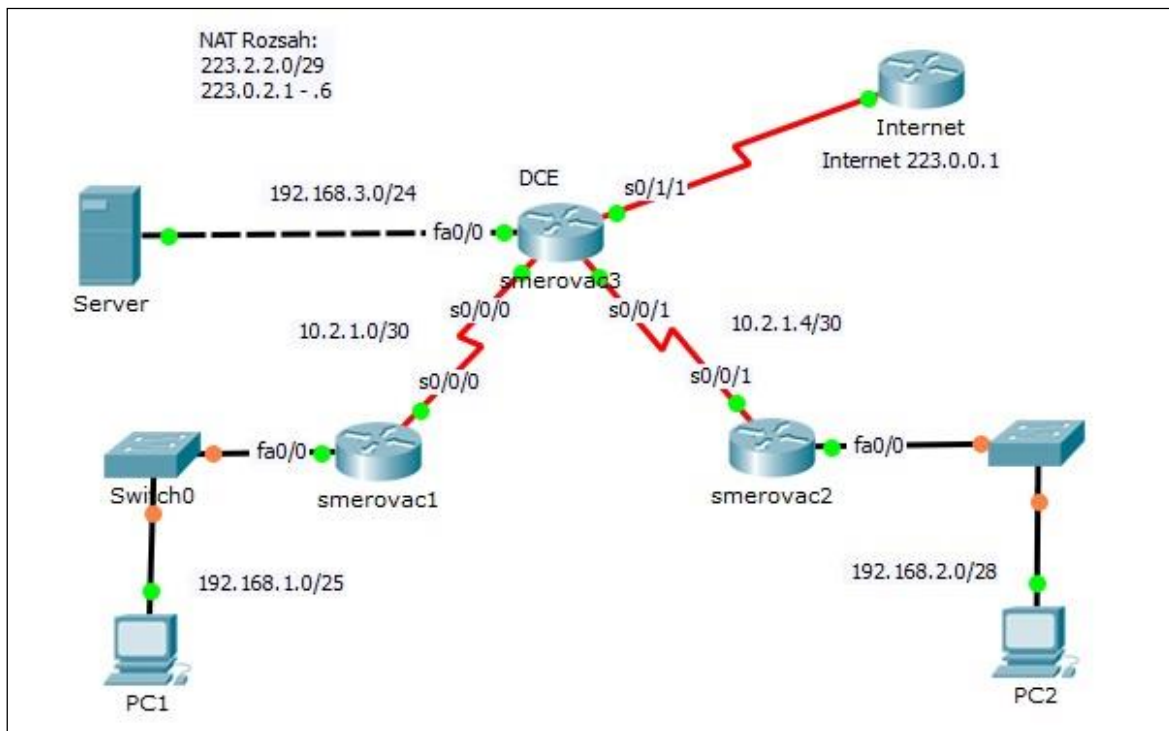
**4. Vytvořte rozsah IP adres pro DHCP.**

```
smerovac(config)# IP DHCP POOL Ip192Rozsah  
smerovac(dhcp-config)# NETWORK 192.168.1.0 255.255.255.0  
smerovac(dhcp-config)# DEFAULT-ROUTER 192.168.1.1
```

Definování názvu rozsahu, přidělení rozsahu a přidělení výchozí brány.

**5. Pingněte z počítačů na server a směrovač.**

## 23 ÚLOHA 11 – NAT



Obr. 32. Úloha 11 – NAT – Zadání v PT.

### 23.1 Zadání

V této úloze budete konfigurovat NAT.

1. Konfigurujte statický NAT překlad mezi serverem (192.168.1.254) a 223.0.2.1.
2. Konfigurujte dynamický NAT překlad pro síť s PC1 a PC2 s přetížením.
3. Pingněte IP adresu 223.0.0.1 a prohlédněte si statistiku překladu na směrovači 3.

### 23.2 Řešení

1. Konfigurujte statický NAT překlad mezi serverem (192.168.1.254) a 223.0.2.1.

```
smerovac3(config)# IP NAT INSIDE SOURCE STATIC 192.168.1.254 223.0.2.1
Vytvoření překladu mezi 192.168.1.254 a 223.0.2.1.
```

```
smerovac3(config)# INTERFACE s0/1/1
smerovac3(config-if)# IP NAT OUTSIDE
```

```
smerovac3(config)# INTERFACE fa0/0
smerovac3(config-if)# IP NAT INSIDE
Definování směru překladu na portech směrovače.
```

2. Konfigurujte dynamický NAT překlad pro síť s PC1 a PC2 s přetížením z dostupného NAT rozsahu.

```
smerovac3(config)# IP NAT POOL POOL1 223.0.2.2 223.0.2.6 NETMASK  
255.255.255.248
```

Vytvoření rozsahu pro NAT překlad.

```
smerovac3(config)# ACCESS-LIST 1 PERMIT 192.168.1.0 0.0.0.127  
smerovac3(config)# ACCESS-LIST 1 PERMIT 192.168.2.0 0.0.0.15
```

Adresy, kterým je povoleno být přeloženy.

```
smerovac3(config)# IP NAT INSIDE SOURCE LIST 1 POOL POOL1  
OVERLOAD
```

Svázání IP NAT rozsahu s access-listem a nastavení přetížení.

```
smerovac3(config)# INTERFACE s0/0/0  
smerovac3(config-if)# IP NAT INSIDE
```

```
smerovac3(config)# INTERFACE s0/0/1  
smerovac3(config-if)# IP NAT INSIDE
```

Definování směru NAT překladu.

3. Pingněte IP adresu 223.0.0.1 a prohlédněte si statistiku překladu na směrovači 3.

## ZÁVĚR

Cílem této práce bylo vytvoření laboratorních úloh pro kurz Cisco CCNA R@S Routing and Switching Essentials. V této práci byla popsána jednotlivá témata podle kapitol v tomto kurzu. Vzhledem k tomu, že byly k dispozici směrovače podporující pouze IPv4, práce se primárně zaměřuje na tento protokol.

Bylo vypracováno 11 praktický úloh do cvičení kurzu Cisco CCNA R@S Routing and Switching Essentials. Jednotlivé úlohy jsou uvedeny ve dvou provedeních. První je zadání a druhé je řešení. Každá úloha má zadání i řešení v Packet traceru. Jednotlivé úlohy jsou přiloženy i jako přílohy pro lepší využití pro výuku.

Zpracováním tohoto tématu bylo docíleno objevení informací, které mě nebyly známy a které jsou obohacující pro ty, kteří budou tuto práci využívat. To bylo způsobeno převážně tím, že mi bylo k dispozici zařízení Cisco, na kterém mohlo být pracováno. Při práci s těmito zařízeními byl spuštěn program WireShark. Díky této aplikaci bylo možno sledovat síťový provoz. Po rozboru tohoto provozu byly některé věci jasnější. Mezi tyto věci patří DCE a clock rate, nativní VLAN, classful a classless síť, nastavení firewallu v hostech připojených k cisco zařízením, použití programu Putty, použití správných kabelů mezi síťovými zařízeními a s tím související identifikace problému v síti a také velkou důležitost dokumentace sítě, ať již na papíře, či správná pojmenování zařízení a pojmenování portů v IOS. Dokumentace patří mezi velmi významné části návrhu sítě spolu se správným navrhnutím IP adresového prostoru pro zjednodušení směrovacích tabulek. Nevýhodou práce v programu Packet tracer je nepřijetí do styku s fyzickou strukturou a zapojením, které je třeba vložit do dokumentace. Další nevýhodou je, že ve skutečném prostředí s fyzickými zařízeními je vyšší pravděpodobnost se setkáni s problémy síťové komunikace, které se v Packet traceru tak často nevyskytují. Tyto problémy vycházejí z fyzického zapojení, použití správných kabelů a nastavení komunikujících hostů. S každým problémem se sítí, který je třeba vyřešit, přichází i poučení z řešení těchto problémů.

Práce by mohla být rozšířena o problematiku IPv6, která zde je pokryta okrajově. V budoucnu by mohly být vytvořeny úlohy pokrývající směrovací protokoly RIPng a OSPFv3, které jsou používány protokolem IPv6. Dále také úloha pro Access control listy pro IPv6 a DHCPv6.

**SEZNAM POUŽITÉ LITERATURY**

- [1] KUROSE, James F a Keith W ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.
- [2] LAMMLE, Todd a Keith W ROSS. CCNA: výukový průvodce přípravou na zkoušku 640-802. 1. vyd. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.
- [3] EMPSON, Scott. CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. 1. vyd. Brno: Computer Press, 2009, 336 s. ISBN 978-80-251-2286-0.
- [4] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce: autorizovaný výukový průvodce. 5. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-80-251-3176-3
- [5] LAMMLE, Todd. CCNA: routing and switching: study guide. 1. vyd. Wiley-Blackwell, 2013, 1176 s. ISBN 11-187-4961-8.
- [6] Fiber Optical Media Converters GEPON, EPON, Serial converter, E1 Ethernet manufacturer from Taiwan: Format of a standard Ethernet frame. [online]. [cit. 2015-04-19]. Dostupné z: [http://www.ad-net.com.tw/pics/Format\\_of\\_a\\_standard\\_Ethernet\\_frame.png](http://www.ad-net.com.tw/pics/Format_of_a_standard_Ethernet_frame.png)
- [7] Cisco: Cisco installation guide for Cisco 2950 [online]. San Jose: Cisco, 2004 [cit. 2015-04-25]. Dostupné z: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/hardware/installation/guide/2950hig.pdf>
- [8] CCNA Routing and Switching: Routing and Switching Essentials. Cisco akademie [online]. [cit. 2015-04-25]
- [9] Ciscohite: Difference between ISL & 802.1q. [online]. [cit. 2015-04-25]. Dostupné z: <http://ciscohite.files.wordpress.com/2013/05/802.png?w=460>
- [10] Cisco: Cisco 1941 [online]. [cit. 2015-05-19]. Dostupné z: [http://www.cisco.com/c/dam/en/us/td/i/300001-400000/300001-310000/302001-303000/302960.tif/\\_jcr\\_content/renditions/302960.jpg](http://www.cisco.com/c/dam/en/us/td/i/300001-400000/300001-310000/302001-303000/302960.tif/_jcr_content/renditions/302960.jpg)

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

ABR	Area Border Router
ACL	Access Control List
AD	Administrative Distance
AS	Autonomous System
ASBR	Autonomous System Border Router
AUX	Auxiliary Port
BDR	Backup Designated Router
BGP	Border Gateway Protocol
CAM	Content Addressable Memory
CDP	Cisco Discovery Protocol
CIDR	Classless Inter-Domain Routing
CRC	Cyclic Redundancy Check
DBD	Database Descriptors
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DR	Designated Router
DTE	Data Termination Equipment
DTP	Dynamic Trunking Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
Gb/s	Gigabite per second
HTTP	HyperText Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers

---

IGRP	Interior Gateway Routing Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ISO/OSI	ISO's Open Systems Interconnect
ISP	Internet Service Provider
Kb/s	Kilobits per second
LSA	Link-State Advertisements
MAC	Media Access Control
Mb/s	Megabyte per second
NAT	Network Address Translation
OSPF	Open Shortest Path First
PAT	Port Address Translation
PDU	Protocol Data Unit
PoE	Power over Ethernet
POST	Power On Self Test
RAM	Random Access Memory
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RIR	Regional Internet Registry
ROM	Read Only Memory
SPF	Shortest Path First
SSH	Secure SHell
STP	Spanning-Tree Protocol
SVI	Switch Virtual Interface

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VoIP	Voice over IP
VTP	VLAN Trunk Protocol
WAN	Wide Area Network

**SEZNAM OBRÁZKŮ**

<i>Obr. 1. Konvergované sítě.</i>	14
<i>Obr. 2. Hierarchický model sítě.</i>	15
<i>Obr. 3. Ethernet rámeček.</i>	16
<i>Obr. 4. Kolizní doména.</i>	17
<i>Obr. 5. Broadcastová doména.</i>	18
<i>Obr. 6. Přední panel přepínače Cisco 2950 [7].</i>	20
<i>Obr. 7. Výstup z přepínače.</i>	24
<i>Obr. 8. VLAN sítě.</i>	28
<i>Obr. 9. Trunk spojení mezi zařízeními, které potřebují přenášet data z více než 1 VLAN sítě.</i>	30
<i>Obr. 10. 802.1Q rámeček [9].</i>	30
<i>Obr. 11. Směrování paketu.</i>	35
<i>Obr. 12. Směrovač Cisco 1941 [10].</i>	36
<i>Obr. 13. DTE a DCE.</i>	38
<i>Obr. 14. Zastaralé Inter-VLAN směrování.</i>	42
<i>Obr. 15. Route-on-a-stick směrování.</i>	43
<i>Obr. 16. Classful směrovací protokol příklad č. 1.</i>	50
<i>Obr. 17. Classful směrování protokol příklad č. 2.</i>	50
<i>Obr. 18. OSPF oblasti.</i>	55
<i>Obr. 19. Více přístupová síť.</i>	56
<i>Obr. 20. IP adresy v NAT překladu.</i>	65
<i>Obr. 21. Úloha 1 – Zadání v PT.</i>	69
<i>Obr. 22. Putty připojení k přepínači.</i>	70
<i>Obr. 23. Úloha 2 – Zadání v PT.</i>	73
<i>Obr. 24. Úloha 3 – Zadání v PT.</i>	77
<i>Obr. 25. Úloha 4 – Zadání v PT.</i>	82
<i>Obr. 26. Úloha 5 – Zadání v PT.</i>	84
<i>Obr. 27. Úloha 6 – Zadání v PT.</i>	86
<i>Obr. 28. Úloha 7 – Zadání v PT.</i>	89
<i>Obr. 29. Úloha 8 – Zadání v PT.</i>	92
<i>Obr. 30. Úloha 9 – Zadání v PT.</i>	95
<i>Obr. 31. Úloha 10 – Zadání v PT.</i>	97

---

*Obr. 32. Úloha 11 – NAT – Zadání v PT.....99*

**SEZNAM TABULEK**

<i>Tab. 1. Konfigurační módy zařízení Cisco. ....</i>	19
<i>Tab. 2. Možné DTP módy a jejich výsledky [8]. ....</i>	33
<i>Tab. 3. Administrativní vzdálenost [8]. ....</i>	40
<i>Tab. 4. Privátní IP adresy [1]. ....</i>	64
<i>Tab. 5. Konfigurační módy. ....</i>	71

**SEZNAM PŘÍLOH NA CD**

- P I: Úloha č. 1. – Základní nastavení.
- P II: Úloha č. 2. – Nastavení portů, SSH a bezpečnost.
- P III: Úloha č. 3. – Nastavení VLAN.
- P IV: Úloha č. 4. – Nastavování portů směrovače.
- P V: Úloha č. 5. – Inter-VLAN směrování.
- P VI: Úloha č. 6. – Statické směrování.
- P VII: Úloha č. 7. – Konfigurace RIPv2.
- P VIII: Úloha č. 8. – Konfigurace OSPFv2.
- P IX: Úloha č. 9. – Access control listy
- P X: Úloha č. 10. – DHCP
- P XI: Úloha č. 11. – NAT