

# Úlohy pro praktická cvičení v Packet Tracer

Juraj Michalec

---

Bakalářská práce  
2016



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2015/2016

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Juraj Michalec**  
Osobní číslo: **A12112**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **prezenční**

Téma práce: **Úlohy pro praktická cvičení v Packet Tracer**  
Téma anglicky: **Tasks for Practical Exercises in Packet Tracer**

Zásady pro vypracování:

1. Nastudujte a popište simulační prostředí Packet Tracer.
2. Navrhněte sadu úloh pro předmět Provoz počítačových sítí.
3. Vypracujte k navrženým úlohám zadání a zapojení v simulátoru.
4. Popište způsob tvorby automaticky hodnocených úloh.
5. Vytvořte dvě automaticky hodnocené úlohy.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **SOSINSKY, Barrie A.** Mistrovství počítačové sítě. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.
2. **THOMAS, Thomas M.** Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.
3. **KÁLLAY, Fedor.** Počítačové sítě LAN/MAN/WAN a jejich aplikace. 2. aktualiz. vyd. Praha: Grada, 2003, 356 s. ISBN 80-247-0545-1.
4. **VELTE, Toby J a Anthony T VELTE.** Síťové technologie Cisco: velký průvodce. vyd. 1. Brno: Computer Press, 2003, 759 s. ISBN 80-722-6857-0.
5. **SHINDER, Debra Littlejohn.** Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.
6. **ODOM, Wendell a Rick MCDONALD.** Routers and routing basics: CCNA 2 companion guide. Indianapolis: Cisco Press, 2007, xxviii, 473 s. ISBN 15-871-3166-8.

Vedoucí bakalářské práce:

**Ing. Jiří Korbel, Ph.D.**

Ústav počítačových a komunikačních systémů

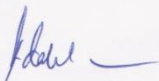
Datum zadání bakalářské práce:

**27. července 2016**

Termín odevzdání bakalářské práce:

**23. srpna 2016**

Ve Zlíně dne 8. srpna 2016



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



Ing. Jan Valjouch, Ph.D.  
*ředitel ústavu*

**Jméno, příjmení:**

**Název bakalářské/diplomové práce:**


**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s 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 použítou 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, dne

  
.....  
podpis diplomanta

## **ABSTRAKT**

Bakalárska práca „Úlohy pro praktická cvičení v Packet Tracer“ sa zaoberá konfiguráciou dynamických a smerovacích protokolov. Teoretická časť uvádza problematiku sietí, ich delenie a filtrovanie sieťovej prevádzky. Ďalšia kapitola pojednáva o rozdieloch a charakteristikách smerovacích a dynamických protokolov, pre lepšie pochopenie ich odlišností. Praktickú časť tvorí popis programu Cisco Packet Tracer a konfigurácia jednotlivých smerovacích protokolov a access listov. Na záver boli v simulačnom prostredí vytvorené dve automaticky hodnotiace úlohy.

Kľúčová slova: smerovač, smerovací protokol, RIP, OSPF, EIGRP, ACL, Cisco Packet Tracer,

## **ABSTRACT**

Bachelor thesis "Tasks for practical exercises in Packet Tracer" is engaged in configuration of dynamic and routing protocols. The theoretical part explains networking issues, types of networks and filtering of network operation. The next chapter discusses the differences and characteristics of dynamic and routing protocols to better understand their differences. The practical part is description of Cisco Packet Tracer configuration and various routing protocols and access lists. In the conclusion, there were created two evaluation tasks automatically in the simulation environment.

Keywords: router, routing protokol, RIP, OSPF, EIGRP, ACL, Cisco Packet Tracer

## **POĎAKOVANIE**

Ďakujem svojmu školiteľovi Ing. Jiřímu Korbelovi Ph.D. Za odbornú pomoc, cenné rady, skúsenosti a vynaložený čas pri tvorbe tejto bakalárskej práce.

## **PREHLÁSENIE**

Prehlasujem, že odovzdaná verzia bakalárskej/diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

# OBSAH

<b>ÚVOD</b> .....	<b>10</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>11</b>
<b>1 ZÁKLADNÉ ČASTI SIETE</b> .....	<b>12</b>
1.1 PASÍVNE PRVKY.....	12
1.2 AKTÍVNE PRVKY.....	15
<b>2 DELENIE POČÍTAČOVÝCH SIETÍ</b> .....	<b>19</b>
2.1 ROZDELENIE PODĽA ROZĽAHLOSTI.....	19
2.1.1 LAN.....	19
2.1.2 MAN .....	20
2.1.3 WAN .....	20
2.1.4 PAN.....	20
2.2 ROZDELENIE PODĽA TOPOLOGIE.....	21
<b>3 ADRESÁCIA POČÍTAČOVÝCH SIETÍ</b> .....	<b>23</b>
3.1 IP ADRESA.....	23
3.1.1 Sieťová maska.....	24
3.2 SKRÁTENÝ ZÁPIS MASKY MEDZI DOMÉNAMI (CIDR) .....	25
<b>4 SMEROVANIE</b> .....	<b>27</b>
DÔLEŽITÉ POJMY PRE SMEROVANIE .....	28
4.1 STATICKÉ SMEROVANIE.....	28
4.2 DYNAMICKÉ SMEROVANIE .....	28
4.2.1 RIP.....	29
4.2.1.1 Časovače v RIP protokole.....	30
4.2.1.2 Konfigurácia RIP protokolu.....	30
4.2.2 OSPF.....	31
4.2.2.1 Činnosť OSPF .....	31
4.2.2.2 Základná konfigurácia OSPF.....	32
4.2.3 EIGRP .....	33
4.2.3.1 Metrika protokolu EIGRP.....	34
4.2.3.2 Protokol RPT (Reliable Transport Protocol) .....	34
4.2.3.3 Konfigurácia EIGRP.....	35
<b>5 ÚVOD DO PRÍSTUPOVÝCH ZOZNAMOV</b> .....	<b>36</b>
5.1 FILTROVANIE SIEŤOVEJ PREVÁDZKY .....	37
5.1.1 Štandardný ACL.....	38
5.1.2 Rozšírený ACL.....	38
5.2 POTLAČENIE BEZPEČNOSTNÝCH HROZIEB S ACL .....	38
5.2.1 Zástupné masky.....	39
5.2.2 Umiestnenie ACL.....	39
5.2.3 ACL protokolov transportnej vrstvy .....	40
5.2.4 ACL riadiacich protokolov .....	41
<b>II PRAKTICKÁ ČÁST</b> .....	<b>42</b>
<b>6 PACKET TRACER</b> .....	<b>43</b>

6.1	ZÁKLADNÝ POPIS SIMULAČNÉHO PROSTREDIA .....	43
6.2	VKLADANIE ZARIADENÍ A ICH PREPOJENIE .....	45
<b>7</b>	<b>ÚLOHA ČÍSLO 1 – ZÁKLADNÁ KONFIGURÁCIA.....</b>	<b>48</b>
7.1	CIELE ÚLOHY .....	48
7.2	ZÁKLADNÁ KONFIGURÁCIA NA SMEROVAČI. ....	49
7.2.1	Overenie stavu portov .....	50
<b>8</b>	<b>ÚLOHA ČÍSLO 2 – KONFIGURÁCIA RIP VERZIA 1 .....</b>	<b>51</b>
8.1	CIELE ÚLOHY .....	51
8.2	KONFIGURÁCIA PROTOKOLU RIP. ....	52
<b>9</b>	<b>ÚLOHA ČÍSLO 3 – KONFIGURÁCIA RIP VERZIA 2 .....</b>	<b>55</b>
9.1	CIELE ÚLOHY .....	55
9.2	ZÁKLADNÁ KONFIGURÁCIA PROTOKOLU RIPv2 :.....	56
9.2.1	Overenie činnosti RIPv2 .....	57
<b>10</b>	<b>ÚLOHA ČÍSLO 4 – KONFIGURÁCIA EIGRP .....</b>	<b>60</b>
10.1	CIELE ÚLOHY .....	61
10.1.1	Susedia EIGRP .....	62
10.1.2	Overenie EIGRP.....	63
<b>11</b>	<b>ÚLOHA ČÍSLO 5 – KONFIGURÁCIA OSPF .....</b>	<b>66</b>
11.1	CIELE ÚLOHY .....	66
11.2	KONFIGURÁCIA PROTOKOLU OSPF.....	67
<b>12</b>	<b>ÚLOHA ČÍSLO 6 – KONFIGURÁCIA OSPF A ACCESS LISTOV.....</b>	<b>70</b>
12.1.1	Overenie ospf: show ip route ospf .....	73
12.2	KONFIGURÁCIA ŠTANDARDNÉHO ACL.....	74
12.3	ROZŠÍRENÝ ACL.....	77
12.3.1	Overenie ACL .....	78
<b>13</b>	<b>AUTOMATICKÉ HODNOTENÉ ÚLOHY .....</b>	<b>80</b>
	<b>ZÁVĚR .....</b>	<b>86</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>87</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>90</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>91</b>
	<b>SEZNAM TABULEK.....</b>	<b>94</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>95</b>

## ÚVOD

V dnešnej dobe sú počítačové siete neoddeliteľnou súčasťou života. Pod pojmom počítačová sieť rozumieme napríklad zapojenie dvoch a viac počítačov, aby mohli navzájom zdieľať svoje dáta. História počítačových sietí siaha do 60. rokov 20. storočia, kde začali prvé pokusy o komunikáciu počítačov. Počítačové siete nám uľahčujú život a môžeme ich využívať pri internetovom obchodovaní, zjednodušenie komunikácie, alebo udržiavanie siete vo firmách a školách. V súčasnosti už pomocou siete komunikujú aj zariadenia, pre ktoré to nebol prvotný záujem. Zjednodušujú a skvalitňujú komunikáciu, získavanie správnych informácií je o niečo jednoduchšie a tým nám uľahčujú život.

Dôležitou súčasťou každej počítačovej siete sú sieťové káble, či už medené, alebo optické. Srdcom a mozgom každej siete je router (smerovač). Jeho úlohou je podľa špecifických pravidiel rozposielať pakety ďalej po sieti. Tento proces nazývame smerovanie a delíme ho na statické a dynamické. V tejto práci si vysvetlíme tieto pojmy a popíšeme ich základné vlastnosti. Prvý smerovač, IMP (Interface Message Processor) bol vyrobený v roku 1969. Kde prepojoval jednotlivé časti Arpanetu (predchodca internetu). Jeho úlohou je podľa špecifických pravidiel rozposielať pakety ďalej po sieti.

Cieľom tejto bakalárskej práce je vytvorenie sady úloh, kde si predvedieme smerovanie pomocou dynamických smerovacích protokolov a ukážkových topológií v programe Cisco Packet Tracer od spoločnosti Cisco.

## **I. TEORETICKÁ ČÁST**

# 1 ZÁKLADNÉ ČASTI SIETE

Počítačová sieť pozostáva zo základných častí:

- Hardware siete – zahrňuje všetky technické prostriedky.
- Software siete – je to programové vybavenie.
- Organizačné zaistenie – reprezentuje opatrenia zaisťujúce správu siete [18].

## 1.1 Pasívne prvky

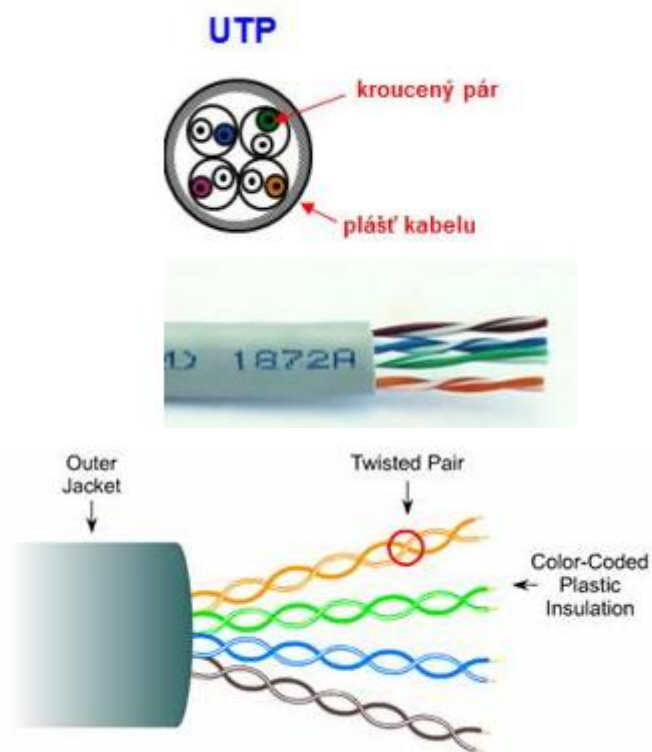
Sú to prvky, ktoré dáta len prenášajú. Dnes sa najčastejšie používa krútená dvojlinka (STP, UTP kábel), optické káble, koaxiálne káble sa pre moderné počítačové siete nepoužívajú.

1. **Krútená dvojlinka (twister pair cable)** – tento kábel sa okrem počítačových sieťach využíva v telekomunikáciách. Je tvorený vodičmi, ktoré sú vo svojej dĺžke skrútené. Funguje na princípe elektromagnetickej indukcie. Dva súbežné vodiče, sa chovajú ako anténa a vyžarujú do svojho elektromagnetického poľa. Ale ak sú vodiče vzájomne skrútené, vyžarovanie elektromagnetického pola sa navzájom ruší. V súčasnosti najrozšírenejším vodičom v sieťach LAN. Krútená dvojlinka môže byť spojitá, alebo nespojitá [20].



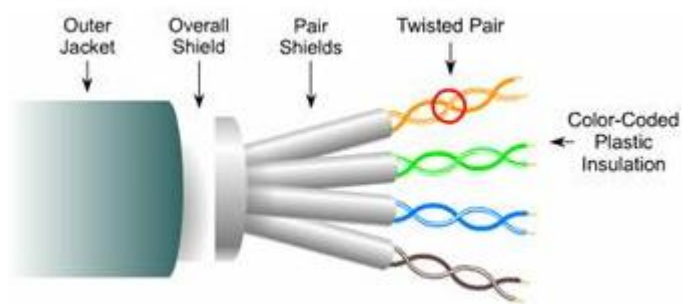
Obr. 1. Symetria krútenej dvojlinky [28]

2. **UTP kábel (Unshielded Twisted Pair)** - pozostáva zo 4 párov vodičov, každý pár sú 2 prepletené vodiče. Vodiče sú twistované pre kompenzáciu rušenia medzi dvoma vodičmi. Výhody sú jednoduchá inštalácia, cena a rýchlosť prenosu. Nevýhodou je náchylnosť pre vonkajšie rušenie [20].



Obr. 2. Zloženie UTP kábla [28]

3. **STP kábel ( Shielded Twisted Pair)** - každý pár je tienený a takisto aj všetky 4 páry sú tienené. Výhodou je dobré odrušenie káblu. Nevýhodou je cena, náročná inštalácia a maximálna vzdialenosť prenosu na 100m [21].



Obr. 3. Zloženie STP káblu [6]



Obr. 4. Ukážka STP a FTP kábla [28]

Preto vznikol kompromis medzi týmito dvoma káblami a to je FTP kábel, ktorý pozostáva zo štyroch párov a má len vonkajšie tienenie. Preto je chránený a uzemnením na koncovom bode.

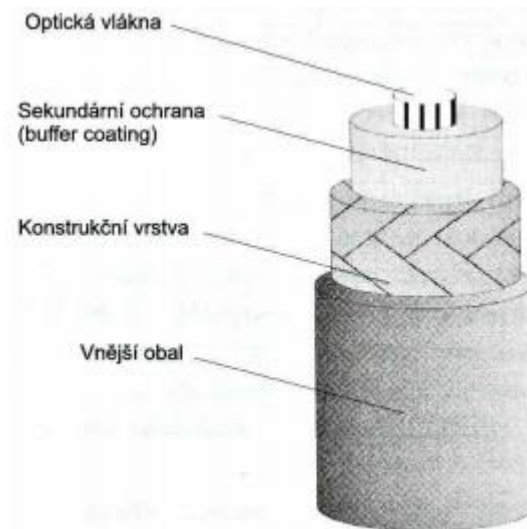
4. **Optické káble** - je založený na inom princípe ako predchádzajúce kable. Dáta nie sú prenášané ako elektrické impulzy v kovových vodičoch, ale svetelnými impulzmi v optických vláknach. Optické vlákna sú veľmi tenké a sú uložené v ochrannom obale. Sú citlivé na mechanické namáhanie a ohyby [20].

**Výhody:**

- prenos dát na veľké vzdialenosti,
- bezpečnosť (vysoká spoľahlivosť prenosu dát),
- vysoká rýchlosť prenosu,
- odolnosť voči elektromagnetickému rušeniu,
- minimálne riziko skratu.

**Nevýhody:**

- cena,
- zložité a drahé spojovanie optických káblov [21].

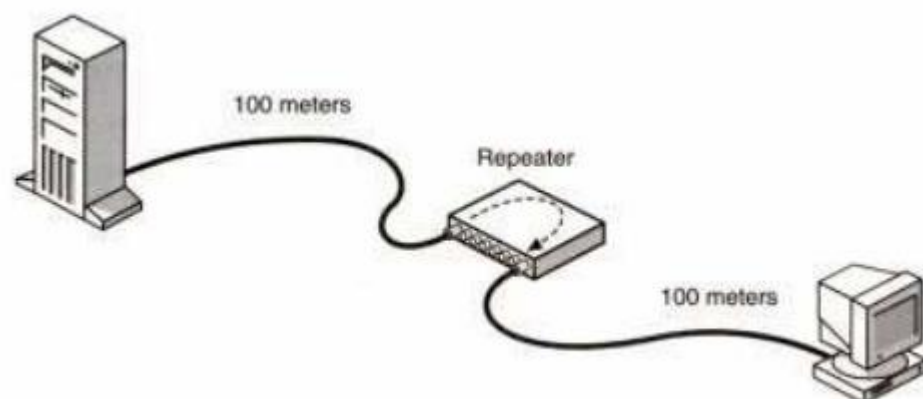


Obr. 5. Zloženie optického kábla [20]

## 1.2 Aktívne prvky

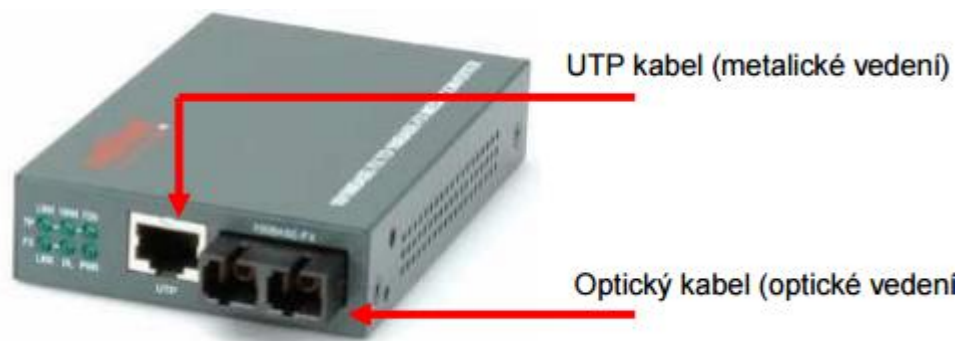
Jedná sa o elektronické zariadenia, ktoré sa aktívne podieľajú na prenose dát po sieti.

1. **Opakovač (repeater)** – pracuje na L1, kde definuje parametre. Opakovač je sieťové zariadenie, slúžiace na zosilnenie, upravenie signálu, predĺženie vetvy, zosilňuje a upravuje signál. Toto zariadenie sa nedá menežovať a taktiež nedokáže filtrovať pakety, takže ich rozosiela všetkým PC staniciam v sieti [19].



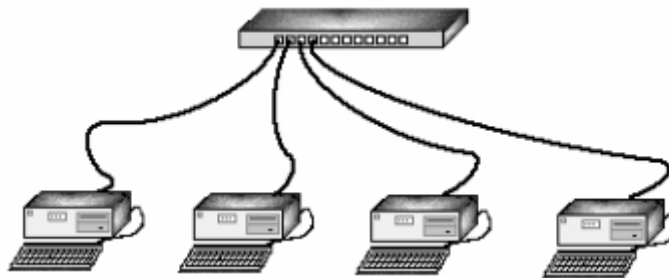
Obr. 6. Zapojenie opakovača v praxi [20]

2. **Prevodník (tranceiver)** - pracuje na L1. Slúži podobne, ako zosilňovač na zosilnenie signálu. Avšak má jednu veľkú odlišnosť. Okrem toho, že signál zosíli, umožňuje prechod napr. z krútenej dvojlinky na optický kábel. Takže dovoľuje meniť typ káblu a aj prenášaný zosilnený signál.



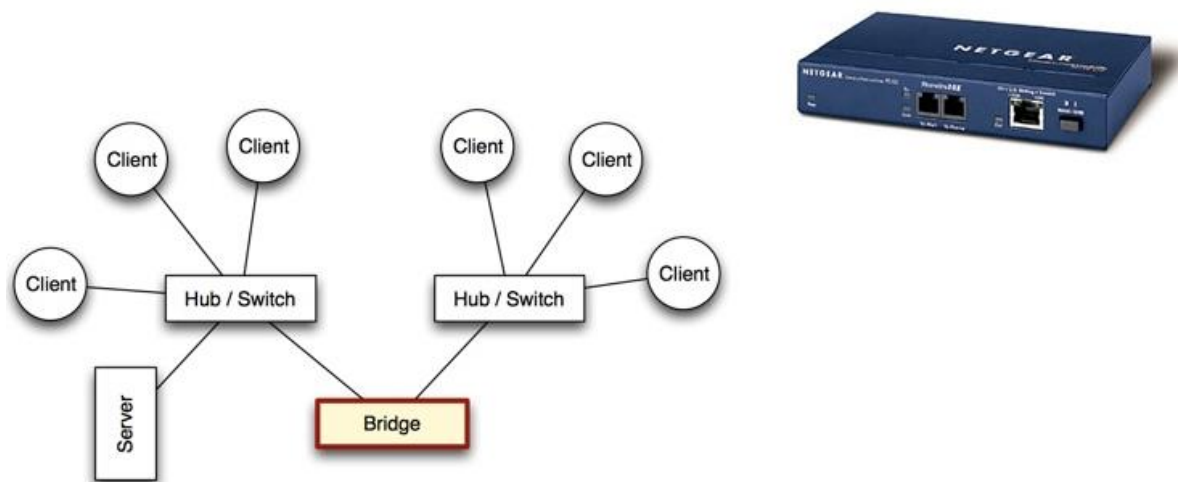
Obr. 7. Porty prevodníka [20]

3. **Hub (rozbočovač)** – multiportový (viacportový repeater), ktorý slúži na sprístupnenie PC siete ďalším užívateľom. Všetky prichádzajúce dáta rozposiela ostatným zariadeniam. Pracuje na L1. Každý dátový paket odošle na každý svoj port. Hub negarantuje rýchlosť na porte. V súčasnosti sa už takmer nepoužíva. Bol nahradený prepínačom (switchom) [19].



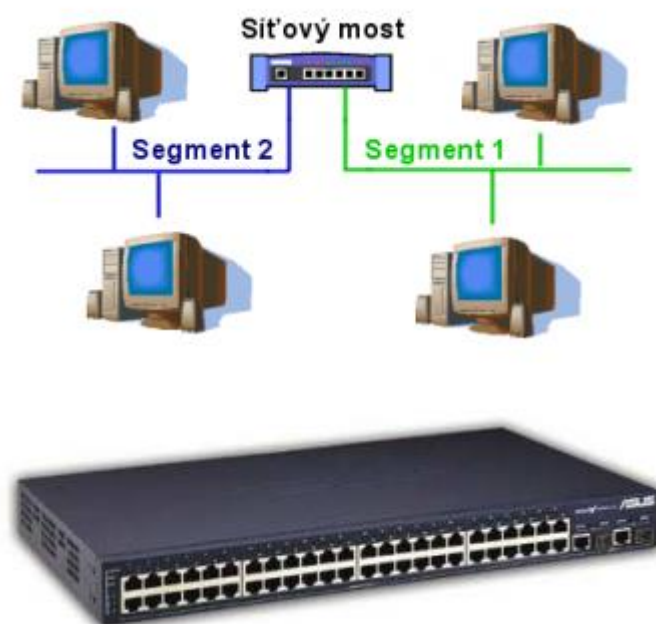
Obr. 8. Zapojenie rozbočovača [20]

4. **Most (bridge)** - pracuje na L2. Je to zariadenie, ktoré nám premostí 2 PC siete. Dokáže premostiť siete s rôznymi médiami (vodiče). Dá sa menežovať a má schopnosť filtrovať dátové rámce a vytvárať štatistiky na portoch [19].



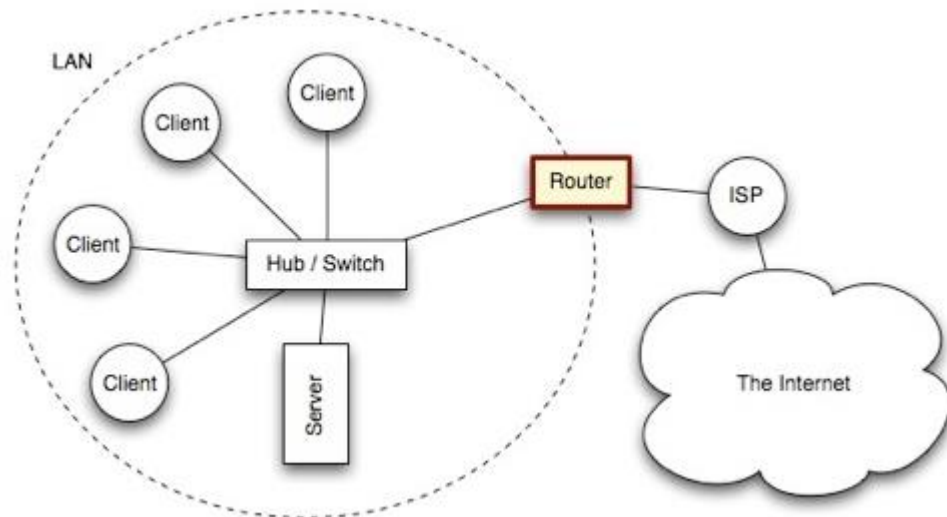
Obr. 9. Premosťovanie siete pomocou mosta [1]

5. **Prepínač (switch)** – pracuje na L2. V podstate môžeme povedať, že je to multiportový bridge. Predlžuje počítačovú sieť. Je zariadenie, ktoré sprístupňuje LAN ďalším zariadeniam. Rozdeľuje kolíznu doménu na menšie kolízne domény. Switch garantuje rovnakú prenosovú rýchlosť na každom porte [19].



Obr. 10. Zariadenie switch [20]

6. **Smerovač (router)** - je sieťové zariadenie, ktoré spája dve, alebo viac sietí. Plne použiteľné k pripojeniu LAN, alebo WAN. Jeho hlavnou činnosťou je správne doručenie dátového paketu správnou cestou. Prepája PC v lokálnej sieti s inými PC, ktoré sa nachádzajú v iných sieťach [19].



Obr. 11. Spojenie dvoch sietí pomocou smerovača [19]

7. **Brána (gateway)** – je zariadenie, ktoré dokáže spojiť dve siete s odlišnými protokolmi. Hlavná funkcia brány je zaistenie dátovej komunikácie paketov [19].

## 2 DELENIE POČÍTAČOVÝCH SIETÍ

Počítačová sieť vznikne vo chvíli, keď dva, alebo viac PC prepojíme pomocou telekomunikačného systému za účelom zdieľania zdrojov. Počítačové siete sa delia podľa rôznych kritérií. Napríklad podľa veľkosti, technológie a topologie. Sieť je spojením hardwaru, softwaru a vodičov, ktoré spoločne umožňujú vzájomnú komunikáciu rôznych PC zariadení. Ak PC prepojené ďalšími PC zdieľajú spoločné prostriedky, označujeme skupinu PC ako PC sieť. Jedná sa o softwarové a hardwarové prostriedky.

Počítače môžu zdieľať:

- dáta,
- správy,
- grafiku
- faxové prístroje
- modemy

### 2.1 Rozdelenie podľa rozľahlosti

A s rastúcim vývojom sa technológie stále rozširujú. Počítačové siete podľa rozľahlosti delíme na LAN, MAN, WAN a PAN.

#### 2.1.1 LAN

Sieť typu LAN ( Local Area Network)) je lokálna sieť, alebo miestna sieť, ktorá prepojuje počítače s ďalšími zariadeniami. Jedná sa o malú sieť na malej geografickej oblasti, napríklad v rámci firmy, domácnosti, alebo úradu. LAN prepojuje množstvo zariadení, ale v dnešnej dobe je väčšinou prepojená do internetu, teda WAN siete [22], [23].

Siete LAN sa delia podľa nasledujúcich atribútov:

- topológia,
- prenosové médium,
- technologické štandardy,
- veľkosť,
- charakteristiky správy [25].

### 2.1.2 MAN

MAN (Metropolitan Area Network) prepojuje lokálne siete v mestskej zástavbe, medzi budovami, slúži na prenos dát. Spája počítače na vzdialenosti jednotiek až desiatok km. Výhodou je použitie optických liniek. Prenosová rýchlosť býva vysoká a vychádza z rýchlosti LAN siete [22], [23].

### 2.1.3 WAN

Sieť WAN (Wide Area Network) spája a existuje na väčších územiach, regiónov štátov. Poskytuje prepojenie dátových služieb v globálnom rozsahu. Najznámejším príkladom siete WAN je internet. Prenosová rýchlosť WAN siete sa pohybuje od desiatok Kbit/s až rádo do stoviek Gbit/s. Lokálne siete sú prepojené cez prenosové kanály [22], [23].

Siete WAN môžeme rozdeliť do štyroch hrubých kategórií:

- 1) Prepínanie okruhov – tento druh sa využíva, pre pevné telefónne linky. Medzi koncovými bodmi je vždy stanovený pevný okruh.
- 2) Prepínanie paketov – v sieti WAN, založenej na prepínaní paketov sa pre zasielanie paketov z jednej stanice na druhú používajú virtuálne okruhy.
- 3) Predávanie buniek – jedná sa o techniku podobnú prepínaniu paketov s tým, že sa pripravujú menšie takzvané bunky o pevnej veľkosti.
- 4) Prenajatá linka – jedná sa o vyhradené spojenie medzi dvoma koncovými bodmi. Komunikácia odchádza z definovaného zdroja a mieri na pevný daný cieľ, tieto spoje sú bezpečné, veľmi rýchle, ale zároveň drahé [25].

### 2.1.4 PAN

PAN (Personal Area Network) je sieť, ktorá je tvorená prepojením osobných elektronických zariadení, ako sú napríklad mobilné telefóny, PDA, laptopy a podobne. Rýchlosť PAN neprekračuje jednotky Mbit/s. Pre tieto siete je dôležitá odolnosť proti rušeniu, nízka spotreba a ľahká konfigurovateľnosť. Medzi PAN siete patria napríklad Bluetooth, Zigbee, alebo Irda [22].

## 2.2 Rozdelenie podľa topológie

**Topológia** je určitý spôsob pripojenia PC ku sieti.

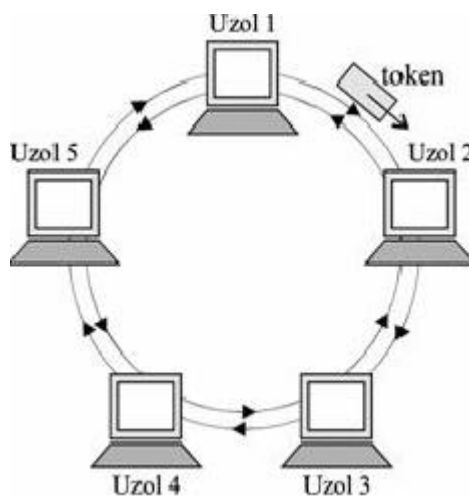
**KRUH (Kruhová topológia)** – Počítače sú navzájom poprepájané do kruhu. Táto topológia sa využívala najmä v minulosti. Vždy komunikuje len jeden PC, ktorý vlastní TOKEN. **TOKEN** je špeciálny paket (určitý balík dát) a ten určuje, ktorý PC bude posielať dáta [22].

### Výhody:

- ľahko sa dá vypočítať rýchlosť prenosu dát po sieti,
- nevznikajú kolízie, rovnomerný prístup pre všetky PC.

### Nevýhody:

- pomalá, zlá inštalácia, obmedzený počet PC,
- pri prerušení kabeláže sa sieť stáva nefunkčnou, preto sa používajú dva okruhy (redundantný záložný zdroj).



Obr. 12. Zapojenie kruhovej topológie [30]

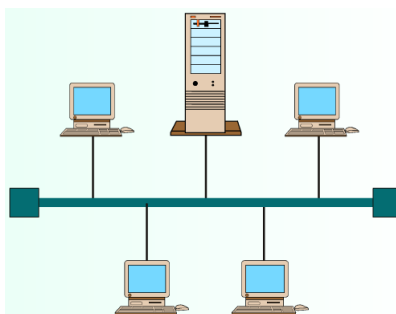
**Zbernica (zbernicová topológia)** – Pozostáva z jedného vodiča, alebo zo súboru vodičov nazývaný chrbtica, na ktorý sú napájané ostatné počítače prostredníctvom odbočiek. Pozostáva zo jednej zbernice, na ktorú sa pripájajú sieťové komponenty. Používaná prevažne v minulosti, ale aj teraz. Rýchlosť je 10 Mb/s [22].

**Výhody:**

- lacná,
- jednoduché pripojenie.

**Nevýhody:**

- pomalá,
- pri prerušení chrbtice (zbernice) počítače prestanú komunikovať [22].



Obr. 13. Zapojenie zbernicovej topológie [30]

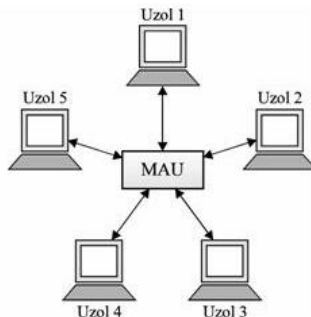
**Hviezdicová topológia (hviezda)** – Najpoužívanejšia topológia v súčasnosti. Každý PC je pripojený do centrálného uzla (hub, switch). V priemysle sa často používa. Ak zlyhá centrálny uzol, celá sieť sa stáva nefunkčnou [22].

**Výhody:**

- lacné pripojenie do siete,
- jednoduché rozšírenie siete,
- vysoká rýchlosť 100 Mb/s, 1000Mb/s.

**Nevýhody:**

- vyššie zriaďovacie náklady [22].



Obr. 14. Zapojenie hviezdicovej topológie [30]

### 3 ADRESÁCIA POČÍTAČOVÝCH SIETÍ

#### 3.1 IP adresa

Je logická adresa zariadenia v sieti. Skladá sa z 32 bitového čísla, takže sa musí skladať zo štyroch častí, ktoré nazývame oktety. Každá časť je veľká 8 bitov a zapisujeme ich oddelenou bodkou. Najčastejšie sa adresa zapisuje v dekadickej forme, ale pre výpočet sa používa binárny zápis. V podstate je adresný rozsah od 0.0.0.0 – 255.255.255.255. Príklad vymyslenej adresy môže byť 108.45.6.10. V dnešnej dobe sa prechádza na adresy dlhé 128 bitov, pretože 32 bitové adresy sa pomaly mňajú.

Pre pochopenie adres je dobré chápať binárnu matematiku. Binárne sústava má základ 2 a zapisujeme ich pomocou 0 a 1. Hodnota jednotky je len pozícia, kde sa nachádza. Pre prevod čísla, prevedieme jednotky do desiatkovej hodnoty a spočítame ich. Osem bitové číslice majú hodnoty od 0 – 255. Takže celkový súčet je 256 hodnôt [24], [3].

pozice	7	6	5	4	3	2	1	0	
výpočet	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	
hodnota	128	64	32	16	8	4	2	1	součet je 255

Obr. 15. Binárna sústava IP adresy [27]

1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1
192								168								1								135									
192.168.1.135																																	

	Zdroj	Cíl
<b>IP adresa</b>	10.0.2.56	10.0.1.30
<b>Maska</b>	22 (255.255.252.0)	neznámá

Obr. 16. Rozdelenie IP adresy [10]

Znázornená adresa v binárnom tvare a jej prepis do bežného formátu v dekadickom zápise.

### 3.1.1 Sieťová maska

Maska siete je číslo, ktoré nám udáva, ako veľká je sieť. Dá sa napísať ako obyčajné číslo z rozsahu 0 až 32. Číselná reprezentácia nám uvádza, koľko bitov z ľava má hodnotu 1. Napríklad pre masku 8 to bude 11111111 a zvyšok samé nuly. V zápise formou IP adresy má maska 8 podobu 255.0.0.0. Maska je dôležitá pre smerovanie, umožňuje nám zlučovať siete do jedného záznamu [10].

Podsieť je maska podsiete. Sieť sa delí na podsiete (subnets). Slúžia k logickému deleniu siete do menších hierarchických častí. Správca siete vytvára 32 bitovú masku podsiete (nuly a jednotky). Hodnoty 1 v maske podsiete reprezentujú pozície, ktoré sa týkajú spoločných adries, alebo podsietí [24].

*Tab. 1. Hodnoty jednotlivých oktétov pre masku*

Binárne	Dekadicky
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Niektoré siete sa navzájom obídu bez podsietí a používajú teda východiskovú masku podsiete. Takže sú určité masky typu A, B a C, ktoré nemôžeme meniť. Teda nemôžeme masku B nastaviť na 255.0.0.0. Hostiteľ totižto bude adresu považovať za neplatnú [24], [3].

Tab. 2. Adresný priestor A,B,C

Trieda	Formát	Vychádzajúca maska podsiete
A	sieť.uzol.uzol.uzol	255.0.0.0
B	sieť.sieť.uzol.uzol.	255.255.0.0
C	sieť.sieť.sieť.uzol	255.255.255.0

### 3.2 Skrátený zápis masky medzi doménami (CIDR)

CIDR- Classless Inter-Domain Routing, v praxi pomocou tejto metódy pridelujeme adresy zákazníkom, firmám a domácnostiam. Adresy sa poskytujú po blokoch určitej veľkosti.

Subnet mask sa môže zapisovať v skrátenej forme, ktorá si hovorí CIDR notácia. Tá sa zapisuje ako IP adresa nasledovaná lomítkom a číslom, ktoré definuje počet bitov v maske podsiete. Vzhľadom na celkový počet bitov v maske a to 32, tak počet núl je 32 [3].

Tab. 3. Skrátený zápis masky

Dekadicky	255.	255.	240.	0	
Binárne	11111111	11111111	11110000	00000000	
Súčet jednotiek	8	8	4	0	=20

Tab. 4. Premena masky na jej skrátenu hodnotu

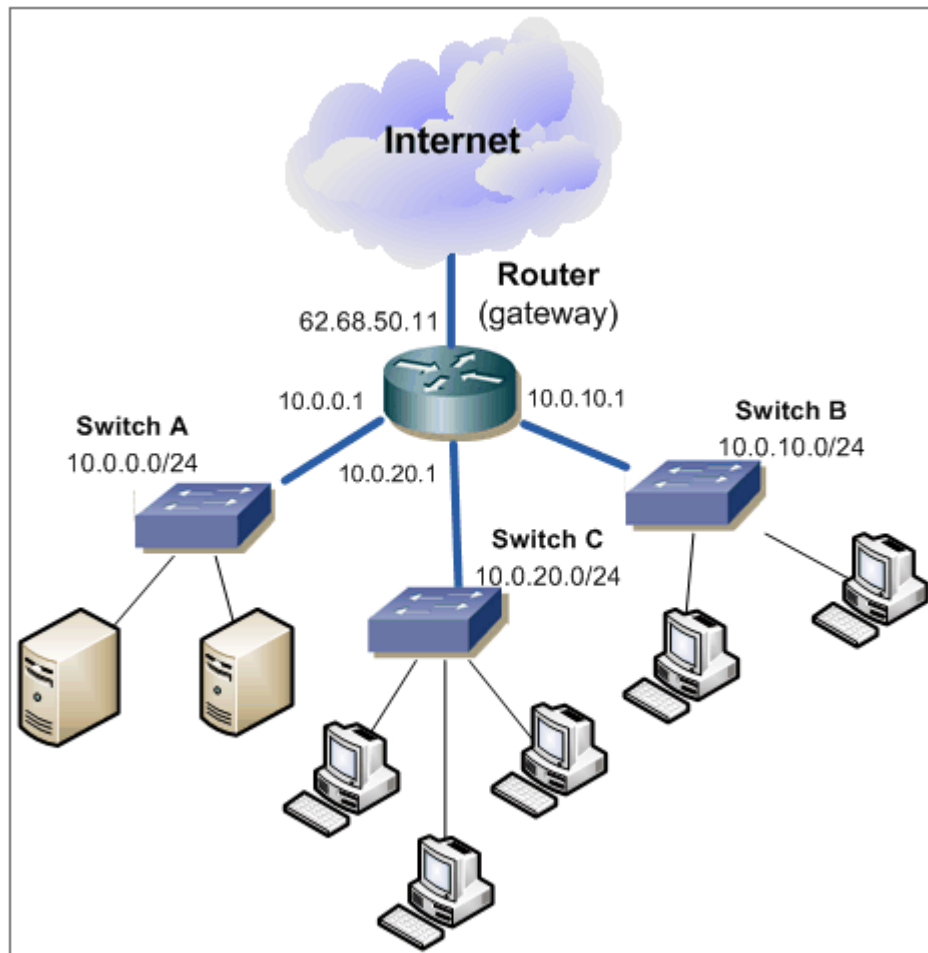
Maska podsiete	Hodnota CIDR
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Masky /8 až /15 sa používajú len so sieťovými adresami triedy A. Masky /16 až /23 sú kompatibilné so sieťovými adresami triedy A a B. Masky /24 až /30 sa uplatňujú u sieťových adres tried A,B a C. Väčšina firiem volí sieťové adresy triedy A. Vzhľadom na to, že môžu používať všetky masky podsiete, získavajú pri návrhu siete maximálnu pružnosť a efektivitu [3].

## 4 SMEROVANIE

Smerovanie, znamená routing, alebo častejšie routovanie. Jedná sa o techniku, ktorá slúži na prepojenie jednotlivých sietí. Hlavnou úlohou je smerovanie paketov z jedného miesta do druhého. Pôvodným zariadením určeným pre routovanie bol router, ale v dnešnej dobe sa využívajú switche, servery, alebo počítače. Router preposiela komunikáciu z jednej siete do druhej.

Na obrázku môžeme vidieť príklad siete, kde máme subnety A, B a C. Sú prepojené cez router medzi sebou a tiež sú prepojené s internetom. Takže, ak chce komunikovať PC zo subnetu C so serverom subnetu A, tak pošle dáta na router a ten zaradí doručenie do správneho subnetu [16].



Obr. 17. Smerovanie pomocou routra [20]

## Dôležité pojmy pre smerovanie

Router – zariadenie, ktoré prevádza routovanie.

Routing – pre posielanie (forwarding) dát medzi sieťami.

Route – cesta, zapísaná v routovacej tabuľke.

Routing table – routovacia tabuľka obsahujúca záznamy o jednotlivých cestách.

Routing protocol – určuje najlepšiu cestu k cieľu a posiela informácie ďalším routrom.

Router on stick – je router, ktorý je pripojený do switchu pomocou trunk portu [14].

### 4.1 Statické smerovanie

Ručne zadané smery so smerovacej tabuľky, ktoré administrátori zadávajú manuálne. Je založené na ručne písaných smerovacích tabuľkách aktívnych zariadení. Jedná sa o jednoduché nastavovanie hodnôt. Smerovanie je vhodné pre menšie siete [17].

#### Výhody:

- jednoduché rootovanie,
- má najvyššiu prioritu,
- nezaťažuje hardware,
- vysoká bezpečnosť [14].

#### Nevýhody:

- vhodné pre autonómne systémy,
- pri zmene adresácie destinačnej siete, nutnosť rekonfigurácie,
- administrátor musí poznať topológiu [14].

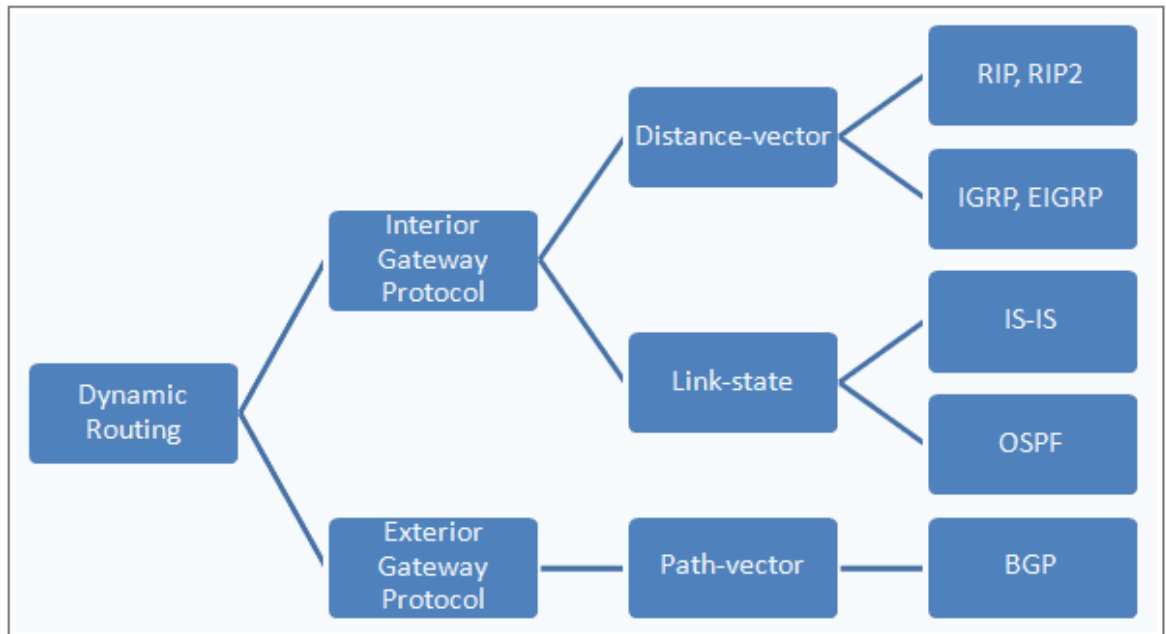
### 4.2 Dynamické smerovanie

U dynamického smerovania (dynamic routing) komunikuje protokol smerovača s rovnakým protokolom, ktorý funguje u susedných smerovačov. Smerovače potom aktualizujú informácie o všetkých sieťach a umiestňujú dáta do svojich smerovacích tabuliek. Automaticky sa vypočítavajú cesty pomocou routovacieho protokolu. Dynamické routovacie protokoly sú dvoch základných typov:

- Distance – Vector Routing Protocol
- Link – State Routing Protocol [17].

Ďalej ich delíme podľa toho, či sú určene pre nasadenie vo vnútri lokálnej siete. Lepšie povedané vo vnútri AS, ktorý môže obsahovať niekoľko LAN [14].

- Interior Gateway Protocol – IGP – routuje vo vnútri AS
- Exterior Gateway Protocol – EGP – routuje medzi AS



Obr. 18. Delenie protokolov [29]

#### 4.2.1 RIP

Protokol RIP (Routing Information Protocol) je typickým príkladom smerovacieho protokolu s vektorom vzdialenosti. Je to vnútorný smerovací protokol, založený na distančnom vektore. Prvá verzia bola vydaná v roku 1982. Jedná sa o jeden z najstarších smerovacích protokolov. Smeruje do vzdialenosti maximálne 15 next hopov. Takže cieľ vzdialený 16 skokov je už nedosiadnuteľný. Rootovacie tabuľky sa posielajú každých 30 sekúnd a obsahujú priamo pripojené siete. Tiež sa automaticky pre posielajú susedným rotorom a odovzdávajú informácie o susedných rotoroch. Jeho administratívna vzdialenosť je 120. Protokol RIP dobre funguje v malých sieťach a vo veľkých sieťach, kde je aplikovaných mnoho smerovačov nie je efektívny. Protokol používa len triedne smerovanie, takže všetka zariadenia v sieti musia mať rovnakú masku podsiete. Protokol RIP verzia 1 používa len triedne smerovanie, takže všetky zariadenia používajú rovnakú masku podsiete. Táto verzia nedosiela informácie o maske podsiete. Protokol RIP verzie 2 poskytuje funkciu, ktorá sa označuje ako smerovanie podľa prefixu (prefix routing)

a odosiela aj údaje o maske podsiete. Túto funkciu nazývame beztriedne smerovanie [3], [16].

#### 4.2.1.1 Časovače v RIP protokole

**Update Timer** - časovač, slúžiaci na pravidelné zasielanie aktualizácií (30s).

**Invalid Timer** - slúži na označenie neplatnej cesty. Ak do 180s nepríde update.

**Flash Timer** – o 60s predĺžený invalid timer (240s). Ak do tohto času nepríde aktualizácia zo susedného rotora, cesta bude z rootovacej tabuľky vymazaná.

**Hold Down Timer** – stabilizuje smerovacie informácie a zabraňuje vzniku rootovacích služieb. V priebehu konvergencie siete, tento timer zabraňuje šíriť nové informácie o topológiách [3].

#### 4.2.1.2 Konfigurácia RIP protokolu

- Konfigurácia RIP:

```
Router(config)# router rip
```

```
Router(config-router)# network [siet']
```

- Verzia RIP:

```
Router(config-router)# version [1/2]
```

- Zrušenie siete:

```
Router(config-router)# no network [siet']
```

- Rozhranie bude posielat' pakety RIP [verzia]:

```
Router(config-if)# ip rip send version [verzia]
```

- Zapnutie RIP autentifikácie:

```
Router(config-if)# ip rip authentication key-chain [heslo]
```

- Či sa bude používať md5 alebo plain text:

```
Router(config-if)# ip rip authentication mode [text | md5]
```

- Rozhranie bude prijímat' pakety RIP [verzia]:

```
Router(config-if)# ip rip receive version [verzia]
```

- Na danom rozhraní (nebude posielat' aktualizácie):

```
Router(config-if)# passive-interface [rozhranie]
```

- Zrušenie RIP:

```
Router(config-router)# no router rip
```

#### 4.2.2 OSPF

Protokol OSPF (Open Shorted Path First) je smerovací protokol otvoreného štandardu. V súčasnosti jeden z najrozšírenejších smerovacích protokolov. Jeho metrika je cost (cena). Jedná sa o classless protokol, takže podporuje VLSM. Používa Dijkstrov algoritmus najkratšej cesty. Najskôr je vytvorený strom kratších ciest a potom sú do smerovacej tabuľky umiestnené optimálne trasy. OSPF konverguje veľmi rýchlo. Podobne ako EIGRP je kompatibilný so smerovanými protokolmi IP a IPv6 [12],[13].

##### **Výhody:**

- open show pad first,
- otvorený protokol, ktorý vyhľadáva krátku cestu,
- výkonný, najpoužívanejší routovací protokol,
- bez triedny protokol,
- rýchla konvergencia,
- bez slučkový protokol,
- podporuje veľké siete,
- efektívne smerovanie [13].

##### **Nevýhody:**

- ťažšie konfigurovateľný,
- vysoké nároky na výpočtový výkon rotora.

##### 4.2.2.1 Činnosť OSPF

- 1) Smerovače si navzájom vymieňajú hello pakety, pomocou ktorých sa dohodnú na určitých parametroch.
- 2) Ak sa dohodnú na parametroch, stávajú sa susedia. Medzi niektorými susedmi nastávajú užšie väzby susedstva. Smerovače sa označujú ako príahlé.

- 3) Priľahlé smerovače si navzájom vymieňajú medzi sebou pakety, ktoré voláme LSU (Link State Updates). LSU obsahujú oznamovače LSA (Link State Advertisement).
- 4) Všetky smerovače si z LSA ukladajú do svojej lokálnej topologickej databázy LSDB a zároveň ich preposielajú na susedné smerovače. Tým sa informácia záplavovo šíri po celej sieti a výsledok toho je zhodná topologická databáza všetkých smerovačov.
- 5) Po naplnení LSDB, každý smerovač urobí výpočet pomocou SPF (Dikstrov algoritmus) a jeho výsledok je najkratšia cesta do každej časti siete bez slučiek.

Na základe týchto výpočtov sa naplní smerovacia tabuľka najlepšimi cestami. V prípade zmeny topológie smerovača odošle príľahlým smerovaním LSA v LSU pakete, to sa rozšíri do celej siete a každý smerovač si upraví topologickú databázu [12].

#### 4.2.2.2 Základná konfigurácia OSPF

- Konfigurácia OSPF:

```
Router(config)# router ospf [číslo procesu]
```

```
Router(config-router)# network [sieť] [wildcard maska] area [číslo arey]
```

- Zapnutie autentifikácie medzi routrami na danom rozhraní:

```
Router(config-if)# ip ospf authentication [message-digest | null]
```

- Nastaví heslo pre autentifikáciu medzi routrami na danom rozhraní:

```
Router(config-if)# ip ospf message-digest-key [key_id] md5 [kľúč]
```

- Nastavenie priority – vyššia priorita = väčšia pravdepodobnosť zvolenia ako DR:

```
Router(config-if)# ip ospf priority [priorita]
```

- Nastavenie ceny cesty – vyššie číslo = horšia cesta:

```
Router(config-if)# ip ospf cost [cena]
```

- Nastavenie intervalu medzi hello pakety:

```
Router(config-if)# ip ospf hello-interval [čas v sekundách]
```

- Interval, kedy je router považovaný za stratený:

Router(config-if)# ip ospf dead-interval [čas v sekundách] [12].

### 4.2.3 EIGRP

EIGRP (Enhanced Interior Gateway Protocol) je beztriedny zdokonalený protokol s vektorom vzdialenosti, ktorý poskytuje výhody oproti inému protokolu spoločnosti CISCO. Je to pokročilý CISCO distance vector protokol. Na rozdiel od RIPu sa snaží zrýchliť konvergenciu a vybrať najlepšiu cestu na základe metriky a obmedziť šírku pásma. Susedné smerovače ležia na rovnakom adresovanom segmente.

Protokol EIGRP sa niekedy označuje ako hybridný smerovací protokol. EIGRP neodosiela pakety so stavom linky, ako to robí protokol OSPF. Namiesto toho odosiela aktualizácie s vektorom vzdialenosti, ktoré obsahujú informácie o sieťach. Pri spustení synchronizuje smerovacie tabuľky medzi susednými smerovačmi a potom ich odosiela. Je vhodný pre veľmi veľké siete. Nie je náchylný na rootovacie slučky, vzhľadom na jeho metriku. JE spätne kompatibilný s IGRP.

#### Výhody:

- class less protokol,
- efektívne zaist'ovanie susedov,
- podpora nespojitých sietí,
- podpora VLSM/CIDR,
- komunikácia s protokolom RTP ,
- výber najlepšej trasy pomocou DUAL.

Smerovač používa 3 tabuľky:

1. Tabuľka susedov – nachádzajú sa tu všetky susedné rotore, ktoré sa refrešujú pomocou hello paketu. Po uplynutí hold time (30s) odoslaného v hello pakete je sused označený za nedosiahnuteľný.
2. Topologická tabuľka – tvoria všetky smerovacie tabuľky v AS, kde EIGRP využíva DUAL algoritmus na výpočet najnižšej ceny smerovania.
3. Smerovacia tabuľka – udržuje najlepšiu cestu do cieľa.

#### 4.2.3.1 *Metrika protokolu EIGRP*

Protokol EIGRP sa vyznačuje jednou špeciálnou vlastnosťou: na rozdiel od iných protokolov, ktoré porovnávajú trasy a vyberajú z nich optimálnu trasu na základe jediného faktoru, používa protokol EIGRP kombináciu štyroch parametrov.

- šírka pásma,
- oneskorenie,
- záťaž,
- spoľahlivosť.

Rovnako ako IGRP, tak aj EIGRP štandardne určuje optimálnu trasu do vzdialenej siete pomocou šírky pásma a oneskorenia linky. Niekedy tieto parametre označujeme ako hodnota šírky pásma trasy (bandwidth a value) a komunikatívne oneskorenie linky (cumulative line delay).

Typy EIGRP paketov môžu byť:

1. Hello – na prieskum overenia,
2. potvrdzovanie ( Acknowledgment),
3. aktualizácie (Update),
4. požiadavky Query,
5. odpovede (reply).

Hello interval – router ktorý je nakonfigurovaný, pravidelne posielajú aktualizácie. Je závislý od šírky pásma rozhrania. EIGRP používajú pakety na potvrdenie EIGRP paketov počas prenosu. Pakety Hello sú posielané ako multicast a odpovede sú unicast. Query paket vysiela router, v prípade ak potrebuje informáciu z jedného, alebo všetkých susedov. Paket Reply sa používa ako odpoveď na Query. [6].

#### 4.2.3.2 *Protokol RPT (Reliable Transport Protocol)*

Protokol EIGRP nám slúži na prenos správ pomocou firemného protokolu, ktorý sa nazýva RTP protokol. Jeden z kľúčových požiadavkov je jeho spoľahlivosť. Tento mechanizmus je založený na viacsmerových a jednosmerových vysielaniach, ktorý poskytuje rýchle aktualizácie a sleduje určenie dát.

V momente, keď protokol EIGRP vysiela, používa adresu triedy D 224.0.0.10. Pre každé viacsmerové vysielanie udržiava zoznam susedov, ktorý naň odpovedali. AK protokol

EIGRP nedostane od suseda odpoveď, považuje svojho suseda za nefunkčného. Tento proces nazývame ako spoľahlivé viacsmerové vysielanie.

Smerovače udržujú prehľad o odosielaných informáciách tak, že každému paketu priradia číslo. Tento postup nám umožňuje, aby zachytili prijatie starého či nadbytočného paketu, alebo informácie doručené mimo poradia [3].

#### 4.2.3.3 Konfigurácia EIGRP

- Konfigurácia EIGRP (číslo autonómneho systému môže byť rovnaký s IGRP):

```
Router(config)# router eigrp [číslo autonómneho systému]
```

```
Router(config-router)# network [sieť]
```

- Povolenie logovania zmien:

```
Router(config-router)# eigrp log-neighbor-changes
```

- Autosumarizácia:

```
Router(config-router)# auto-summary
```

```
Router(config-router)# no auto-summary
```

- Autosumarizácia na rozhraní:

```
Router(config-if)# ip summary-address eigrp [aut.sys] [IP] [maska]
```

- Zapnutie autentifikácie MD5 kľúčom:

```
Router(config-if)# ip authentication mode eigrp [aut.syst] md5
```

```
Router(config-if)# ip authentication key-chain eigrp [aut.syst] [kľúč]
```

- Konfigurácia kľúča:

```
Router(config)# key chain [kľúč] md5 Router(config-keychain)# key [číslo]
```

```
Router(config-keychain-key)# key-string [text]
```

- Nastavenie intervalu medzi hello pakety:

```
Router(config-if)# ip hello-interval eigrp [aut.sys] [čas v sekundách]
```

- Vypnutie split-horizon:

```
Router(config-if)# no ip split-horizon eigrp [aut.sys]
```

## 5 ÚVOD DO PRÍSTUPOVÝCH ZOZNAMOV

Prístupový zoznam (access list) je v praxi zoznam podmienok, ktoré charakterizujú pakety. ACL (Access Control List) čo znamená zoznam kontroly prístupu. Jedná sa o zoznam pravidiel, pomocou ktorého kontrolujeme sieťovú komunikáciu. Prístupové zoznamy sú užitočné a uľahčujú nám prácu nad kontrolou sieťového systému. Je dôležité definovať ACL pre každé sieťové zariadenie a pre každý smer komunikácie [11].

Zabezpečenie siete sa nedá zaistiť jedným ACL, ale kombinuje sa funkčnosť niekoľkých rôznych ACL umiestnených na zariadeniach. Na každé rozhranie je možné umiestniť vždy jeden ACL filtrujúci prevádzku vstupujúcu do rozhrania a jeden ACL filtrujúci vystupujúcu prevádzku [14].

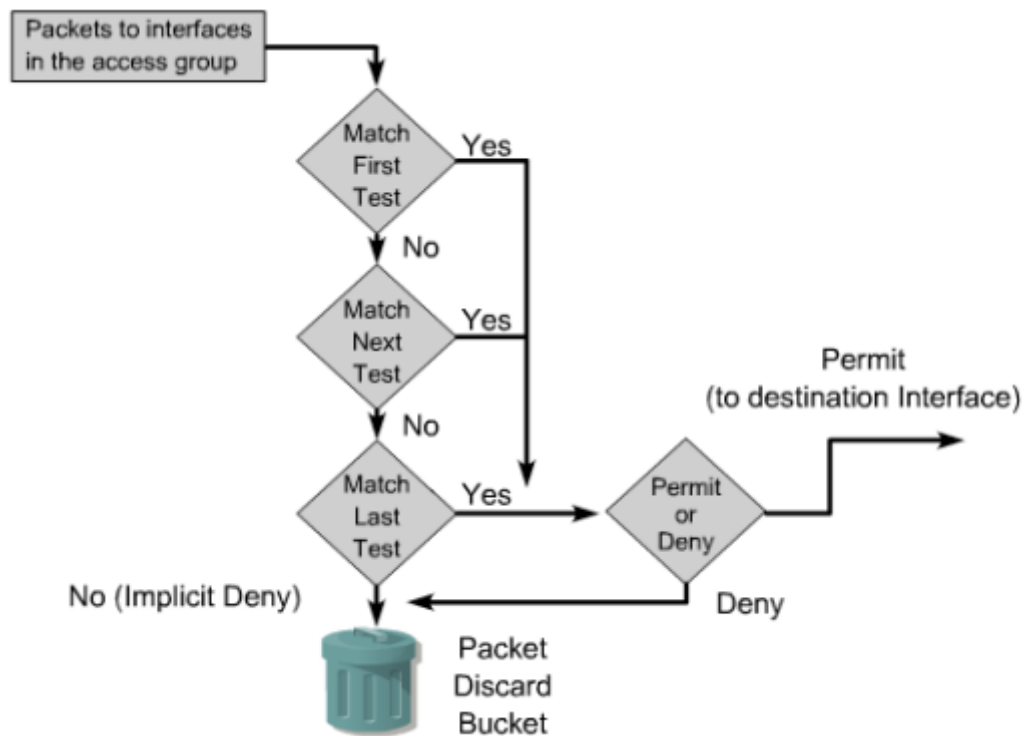
Môžeme ich nastaviť tak, aby prijímali len konkrétne rozhodnutie o regulácii schém, takže k webovým prostriedkom Internetu budú mať prístup len určití hostitelia. Tí ostatní budú mať obmedzený prístup. Prístupové zoznamy dávajú správcovi siete schopnosť vynútiť dobrú zásadu v bezpečnosti siete.

Fungovanie ACL:

ACL pozostávajú zo zoznamu pravidiel. Sú to pravidlá, založené na kombinácii týchto atribútov:

- Zdrojová/cieľová adresa.
- Číslo portu/ názov protokolu.
- Sieťový protokol.

Postupne sa kontrolujú všetky pravidla v ACL. Ak je všetko v poriadku, smerovač zablokuje, alebo povolí komunikáciu. Ak nedôjde v zhode, tak sa len postúpi na ďalšie pravidlo v zozname. Ak nastane, že komunikácia nezodpovedá ani jednému z daných pravidiel, tak sa pretlačí implicitný zákaz všetkej komunikácie, ktorý je daný, ako posledná možnosť v každom ACL. Postup si môžeme pozrieť na obrázku [3], [9].



Obr. 19. Princíp aplikovania ACL [7]

## 5.1 Filtrovanie sieťovej prevádzky

Vytváranie prístupových zoznamov sa v praxi podobá programovaniu podmienkových príkazov, ak je podmienka splnená, nasleduje príslušná akcia. Ak podmienka splnená nie je, nič sa nestane a vyhodnotí sa ďalší príkaz. Príkazy prístupových zoznamov sú filtre, podľa ktorých sa porovnávajú, trieda a spracovávajú pakety. Štandardné prístupové zoznamy IP filtrujú prevádzku na základe IP adresy v pakete. Štandardné prístupové zoznamy IP sa vytvárajú s číslami access-list 1-99, alebo v rozšírenom rozsahu 1300-1999. Prístupové zoznamy sú vytvorené tak, aby filtrovali prevádzku prechádzajúcu cez smerovač. Nefiltrujú prevádzku, ktorá je generovaná smerovačom [3], [8].

Pri návrhu filtrácie prevádzky pomocou ACL je podstatné vždy stanoviť:

- na ktorom rozhraní, ktorého smerovača bude ACL aplikovaný,
- či bude filtrovať prevádzku vstupujúcu do tohto, alebo z tohto rozhrania vystupujúceho,
- kritéria, ktoré spôsobujú prepustenie, alebo zahodenie prichádzajúcich paketov.

### 5.1.1 Štandardný ACL

Je to jednoduchý ACL. Slúži na základne filtrovanie IP komunikácie. Tieto zoznamy používajú ako testovaciu podmienku len zdrojovú IP adresu v pakete IP. Všetky prijaté rozhodnutia sú založené na zdrojovej IP adrese. Takže štandardné zoznamy povoľujú, alebo zakazujú celé sady protokolov. Má jednoduchú syntax. Používa sa pre blokovanie prevádzky blízkeho cieľa. Pomocou čísiel z rozsahu 1-99 alebo 1300-1999 informujeme smerovač, že chceme vytvoriť štandardný prístupový zoznam IP. Smerovač bude na testovacích riadkoch očakávať syntax, ktorá definuje IP adresu [9], [11], [4].

Vytvára sa pomocou príkazu:

- `access-list access-list-number {deny | permit} source [source-wildcard]`

```
access-list 2 deny 172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny 172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
```

Obr. 20. Definícia základného ACL [7]

### 5.1.2 Rozšírený ACL

Rozšírené prístupové zoznamy umožňujú vyhodnocovať polia v hlavičkách vrstvy 3 a 4 paketu IP. Môžu analyzovať zdrojovú a cieľovú IP adresu, pole protokolu v hlavičke sieťovej vrstvy a číslo portu v hlavičke transportnej vrstvy. Rozšírené prístupové zoznamy môžu pri riadení prevádzky uplatňovať jemnejšie pravidla. Môže blokovať prevádzku kdekoľvek (najlepšie blízko zdroja). Príklad vytvorenia rozšíreného ACL [9], [14], [4].

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

Obr. 21. Príklad rozšíreného ACL [7]

## 5.2 Potlačenie bezpečnostných hrozieb s ACL

Najčastejšie typy útokov sú DoS (Denial of service – útoky typu odoprenia služieb). Spoločnosť CISCO predáva zariadenia ASA (adaptive Security Appliance), ktoré obsahujú

moduly IDS/IPS ( intrusion detection system/intrusion prevention system), ale podobné produkty produkujú aj iné firmy.

Zoznam bezpečnostných hrozieb, pred ktorými nás môžu ACL zoznamy chrániť:

- falšovanie IP adries, prichádzajúcich,
- falšovanie IP adries, odchádzajúcich,
- útoky Dos TCP SYN, blokovanie externých útokov,
- útoky DoS typu SYN, použitie TCP,
- útoky DoS smurf,
- blokovanie/filtrovanie správ ICMP, prichádzajúce,
- blokovanie/filtrovanie správ ICMP, odchádzajúce,
- blokovanie/filtrovanie príkazu traceroute [4].

### 5.2.1 Zástupné masky

Zástupné znaky v prístupových zoznamoch určujú jednotlivého hostiteľa, sieť, alebo konkrétny rozsah siete. Pokiaľ chceme definovať 34 sietí, potrebujeme veľkosť bloku 64. V prípade 15 hostiteľov vyhovuje veľkosť bloku 32. Ak špecifikujeme len 2 siete, postačí veľkosť bloku 4.

Zástupné masky sieťovej adresy informujú smerovač o rozsahu dostupných adries pre filtrovanie.

172.16.30.5 0.0.0.0

Štyri nuly predstavujú jednotlivé oktety adresy. Ak je uvedená nula, znamená to, že oktet v adrese sa musí presne zhodovať s odpovedajúcim referenčným oktetom. Pokiaľ chceme nadstaviť, aby oktet mohol mať ľubovoľnú aktivitu, zadáme číslo 255. Podsieť /24 definujeme pomocou masky:

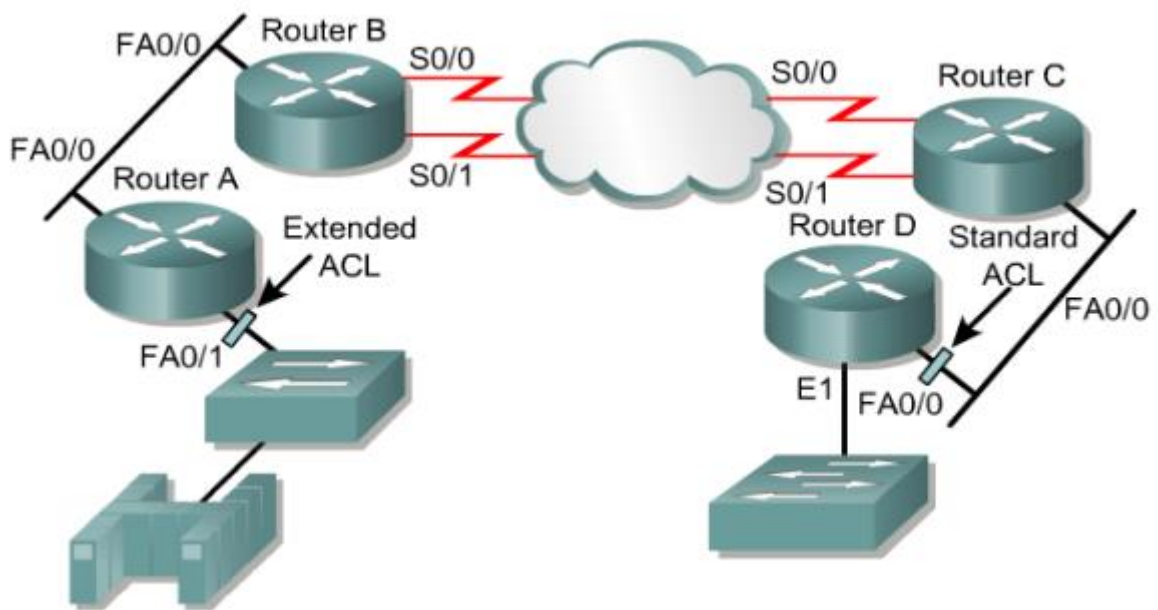
172.16.30.0 0.0.0.255

Tento zápis smerovači uvádza, aby vyhľadal presnú zhodu v prvých troch oktetoch, ale posledný oktet môže mať ľubovoľnú hodnotu [4].

### 5.2.2 Umiestnenie ACL

Ak je sieť rozľahlá a ťažko sa v nej orientujeme, existuje niekoľko možností ako aplikovať ACL. Na začiatok si musíme uvedomiť, či používame rozšírenie, alebo

štandardné ACL. Ďalej je dôležité na ktoré rozhranie a v ktorom smere ACL nakonfigurujeme. Štandardný ACL nám filtruje prevádzku na základe zdrojovej adresy, takže ho zaradíme na vonkajšie rozhranie smerovača. Je dobré, aby bol ACL čo najbližšie k cieľu komunikácie. Rozšírený ACL nám umožňuje definovať aj cieľovú adresu, takže je dobré odfiltrovať nežiaducu komunikáciu podľa cieľovej adresy. Takže môžeme priradiť ACL na vonkajšie rozhranie smerovača. Toto riešenie aj ušetrí prenosové pásmo z dôvodu zachycovania dát [7].



Obr. 22. Umiestnenie ACL [7]

### 5.2.3 ACL protokolov transportnej vrstvy

U protokolov transportnej vrstvy (UDP, CDP) môžeme filtrované kritéria rozšíriť o čísla zdrojových a cieľových portov a tiež aj o niektoré príznaky z hlavičky TCP segmentu. Kontrolu na zhodu portu zaistíme výrazom `eq číslo portu` za špecifikácie zdrojovej, cieľovej adresy. Slovo `lt`, `gt` je možnosť vybrať všetky čísla portov menšie, alebo väčšie než je zadaná hodnota a za kľúčovým slovom `range` uviesť minimálnu a maximálnu hodnotu portu [7].

`permit udp host 10.0.0.1 eq 520 any`

- Prepustí UDP pakety zo stanice 10.0.0.1 so zdrojovým portom 520:

`deny tcp 172.16.0.0 0.0.255.255 gt 5000 host 120.1.1.100 eq 23`

- Zakáže zo siete 172.16.0.0 /16 a z portov vyšších než 5000TCP spojenie na port 23 ( Telnet server ) stanica 120.1.1.100:

```
permit udp any range 16000 17000 host 172.16.1.100 gt 4096
```

- Prepustí UDP datagramy z ktorejkoľvek adresy z rozsahu zdrojových portov 16000 až 17000 na adresu 172.16.1.100 na cieľové porty väčšie ako 4096.

#### 5.2.4 ACL riadiacich protokolov

U protokolov ICMP a IGMP je základná syntax zápisu ACL rozšírená, aby bolo možné filtrovať selektívne jednotlivé typy správ. Typy správ sa pomenovávajú symbolicky, ich prehľad zaistiť z kontextovej nápovede IOS stiskom otázniku pri vkladaní ACL.

Aby vyselektovaný ACL začal filtrovať, je potrebné ho najskôr priradiť na príslušné rozhranie a zvoliť smer prevádzky. Ktorý má filtrovať. To vyskúšame v sekcii požiadaneho rozhrania príkazom `ip access-group` s daným číslom ACL a smerom prevádzky. Smer do rozhrania sa označuje kľúčovým slovom `in`, smer z rozhrania von sa označuje `out`.

```
interface FastEthernet 0/0
```

```
ip access-group 101 in
```

```
ip access-group 102 out
```

NA každé rozhranie môžeme priradiť najviac jeden ACL vo smere `in` a jeden v smere `out`. Pokiaľ je to užitočné, môže byť jeden ACL priradený aj na viac rozhraní a to v smere `in` aj `out` [14], [7].

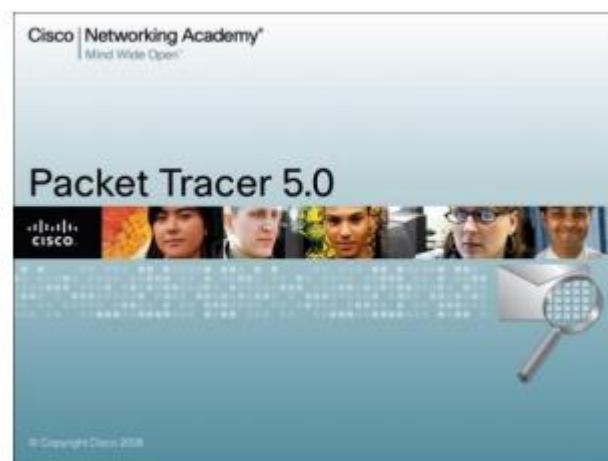
## **II. PRAKTICKÁ ČÁST**

## 6 PACKET TRACER

Svoju bakalársku prácu som formuloval v program Packet tracer. Jedná sa o výukový softvér od spoločnosti Cisco Systems. Program slúži na simuláciu reálnej ukážky práce v počítačových sieťach. Môžeme simulovať akúkoľvek veľkú sieť. Jedná sa o špičkový softvér, ktorý môžeme využívať úplne zdarma. Je voľne stiahnuteľný na oficiálnych Cisco stránkach.

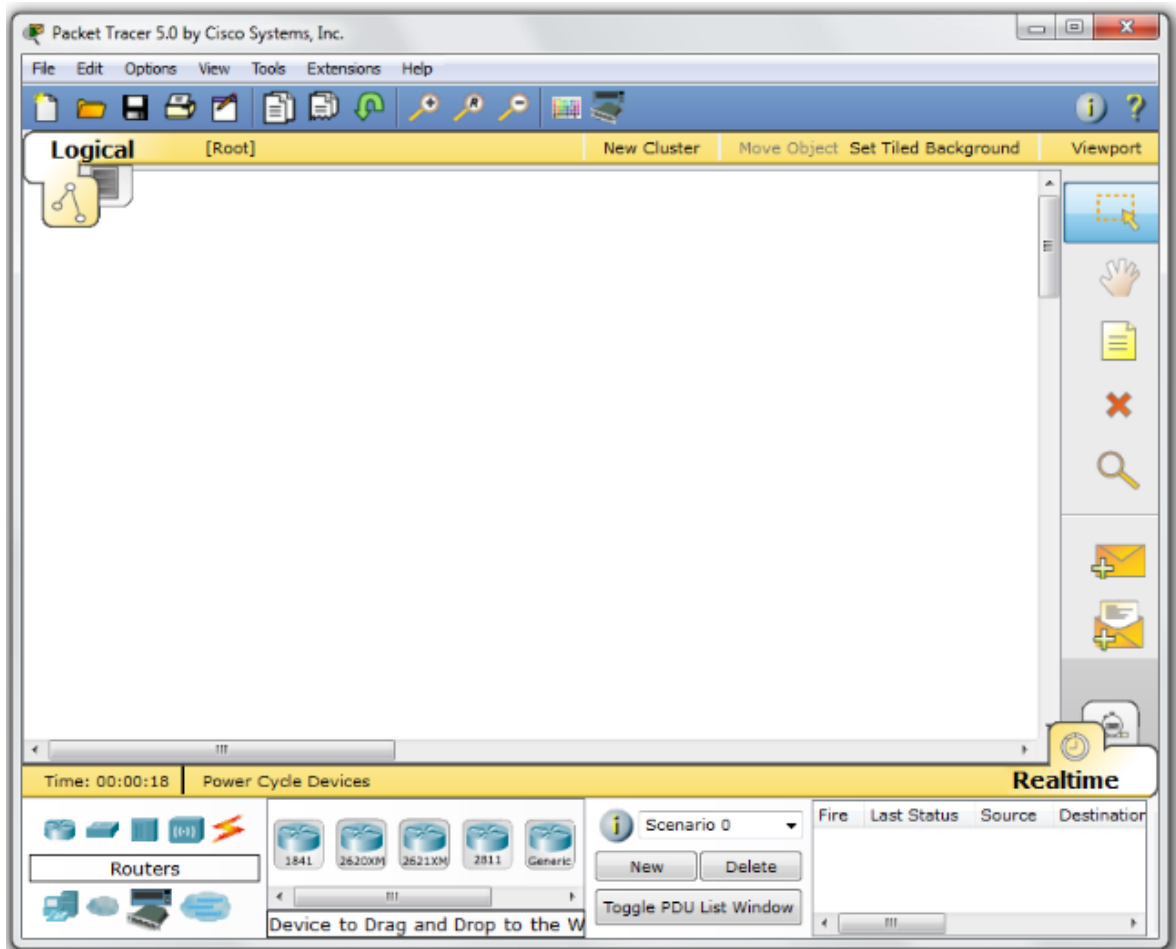
### 6.1 Základný popis simulačného prostredia

Program Packet tracer nie je náročný na inštaláciu a nevyžaduje vysoký nárok na HW. Po spustení programu uvidíme splashscreen a potom sa už spustí aplikácia



Obr. 23. Cisco packet tracer 5.0

Pri spustení aplikácie vidíme vo vrchnej časti obrazovky výber z hlavného menu a panel pre rýchle spustenie. Priamo v strede je voľná plocha, na ktorú sa ukladajú všetky prvky a topológie siete. V ľavej spodnej časti si môžeme vybrať všetky dostupné sieťové koncové zariadenia. Pravá strana obrazovky tvorí lišta s panelom nástrojov. V spodnej pravej časti vidíme prepínač reálneho a simulačného módu.



Obr. 24. Uživatelské prostredie programu

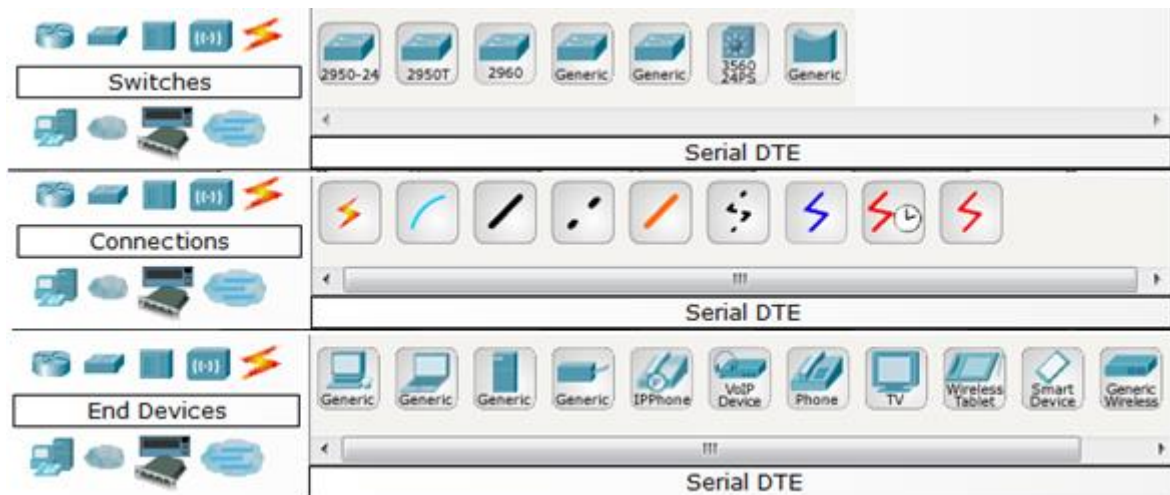
V pravej strane vidíme ikony, ktoré vyzerajú ako obálky. Tvoria dôležitú súčasť systému a overujú funkčnosť dátového paketu v nakonfigurovanej sieti. Tieto obálky nám overujú, či bol prenos paketu úspešný, alebo neúspešný.



Obr. 25: Overovacia obálka

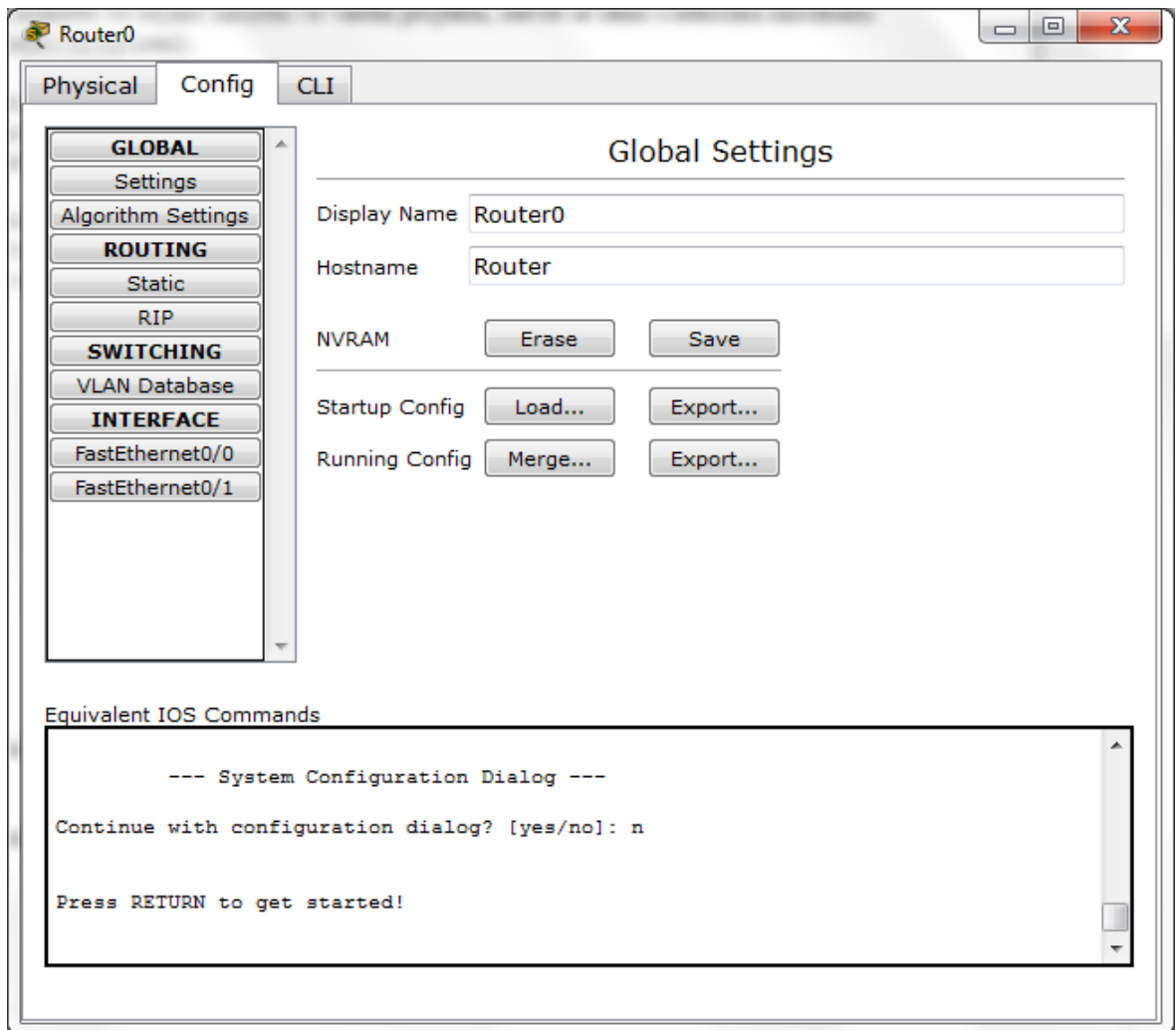
## 6.2 Vkládání zariadení a ich prepojenie

V spodnej časti programu vidíme sieťové koncové prvky, s ktorými môžeme pracovať a vkladať na pracovnú plochu. Patria tu prevažne routre, switchce, a koncové zariadenia ako server, televízia a podobne. Dôležitá je správnosť zapojenia, ktorými sa tieto prvky prepájajú v sieťovej topológii.



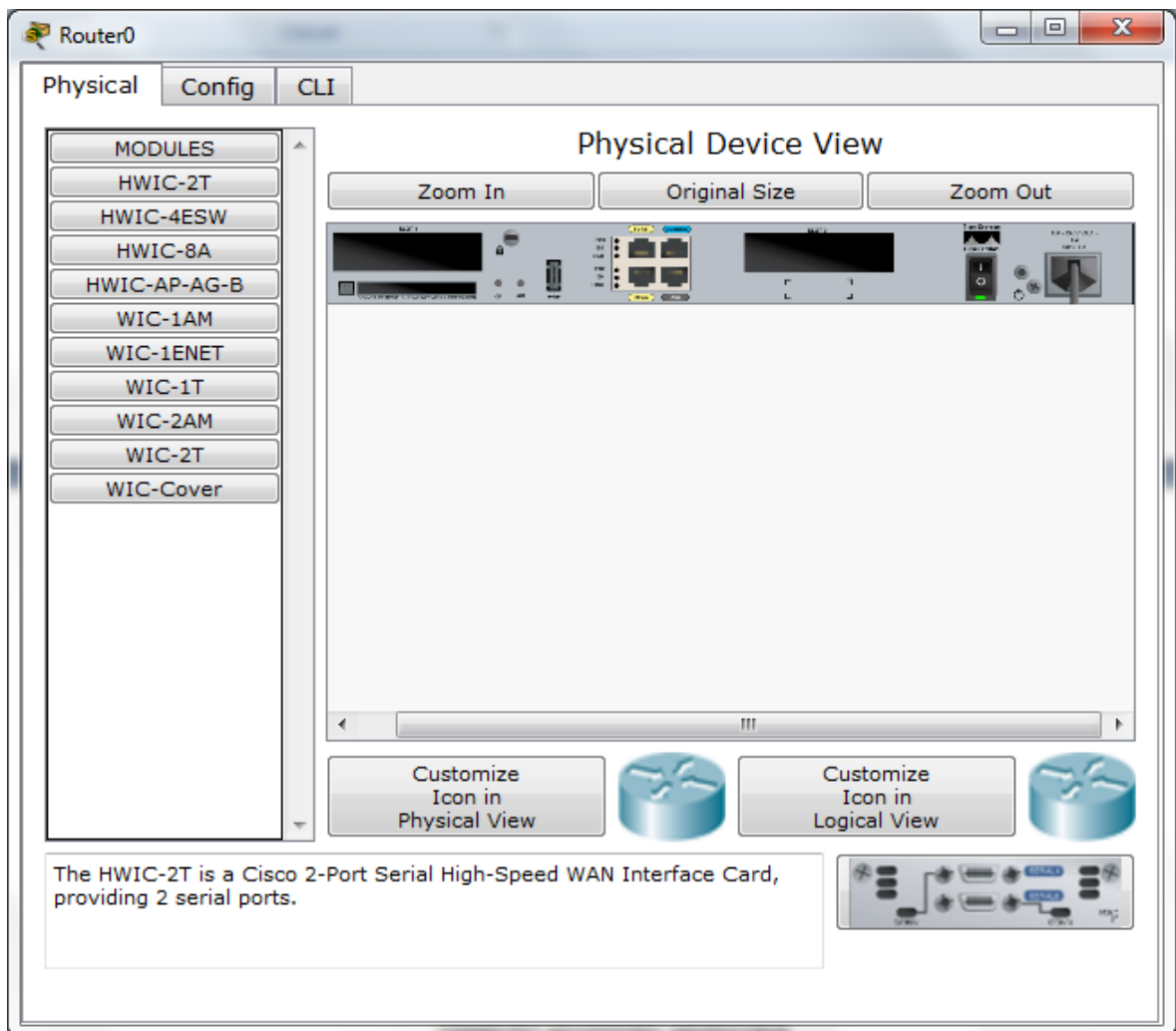
Obr. 26. Aktívne zariadenia a druhy pripojenia

V záložce Config můžeme vykonať globálne nastavenia, nastaviť akékoľvek inštalované rozhranie. Môžeme vidieť grafické rozhranie, kde sa konfigurujú primárne funkcie smerovača. Môžeme si nastaviť napríklad meno smerovača, alebo uložiť svoju konfiguráciu. Prostredie je vhodné, pre začínajúcich užívateľov.



Obr. 27. Grafické prostredie smerovača v záložke Config

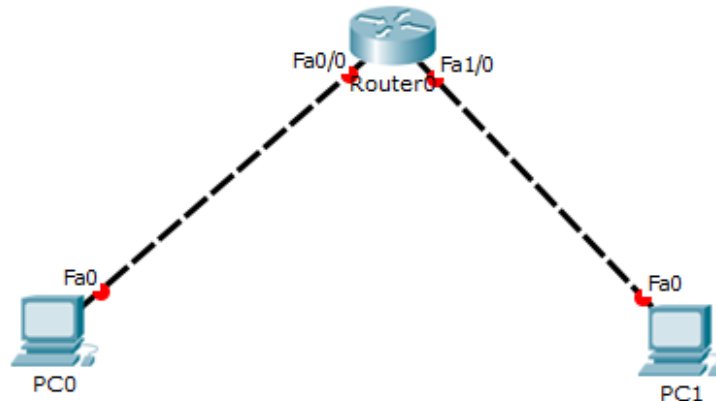
V záložce Physical můžeme nastavovat naše zariadenie správnym sieťovým modulom. Na obrázku vidíme, ako v skutočnosti vypadá tento typ smerovača. Na smerovači sa nachádzajú jednotlivé porty a vypínač, ktorý slúži na pridanie ďalšej jednotky. To znamená, že vypínač musíme vypnúť a až potom pridať zariadenie. Na ľavej strane su rozmiestnené moduly s prídavnými portami.



Obr. 28. Grafické prostredie smerovača v záložke Physical

## 7 ÚLOHA ČÍSLO 1 – ZÁKLADNÁ KONFIGURÁCIA

**Topológia:**



Obr. 29. Zapojenie smerovača

**Adresovacia tabuľka:**

Tab. 5: IP adresy pre rozhranie smerovačov a PC zariadení

Zariadenie	Interface	IP Adress	Subnet Mask	Default Gateway
PC0		192.168.1.100	255.255.255.0	192.168.1.1
PC1		192.168.4.100	255.255.255.0	192.168.4.1
Router0	Fa0/0	192.168.1.1	255.255.255.0	
	Fa1/0	192.168.4.1	255.255.255.0	

### 7.1 Ciele úlohy

#### Prvá časť: Zostaviť topológiu

- Vytvorenie a nastavenie topológie pomocou správnych zariadení.
- Zapojenie káblov a portov, aby zodpovedala topológii siete.
- Zapnutie všetkých zariadení v topológii.

#### Druhá časť: Základná konfigurácia

- Konfigurácia zariadenia a overiť dostupnosť zariadenia.
- Konfigurácia PC rozhraní.
- Nastavenie mena na UTB.
- Nastavenie hesla pre privilegovaný mod, md5 hash.
- Nastavenie hesla pre telnet.
- Nastavenie hesla pre konzolu.
- Nastavenia hesla pre AUX port.
- Zahashovanie hesiel pomocou md5.

## 7.2 Základná konfigurácia na smerovači.

V praxi musí byť smerovač napojený na napájanie. Tiež musí byť pripojený káblom do konzolového portu. Na čistom smerovači nie sú nastavené žiadne hesla, takže sa hneď pustíme do konfigurácie.

Smerovač sa najskôr nachádza v užívateľskom móde. Prvý krok je prepnutie do privilegovaného módu.

```
Router> enable
```

- *Prepnutie do privilegovaného módu.*

```
Router# configure terminal
```

- *Prepnutie do globálnej konfigurácie, vstup do konfiguračného módu*

```
Router (config)# hostname UTB
```

- *Nastavenie mena na smerovači.*

```
UTB (config)# enable password Cisco
```

- *Nastavenie hesla Cisco pre privilegovaný mód.*

```
UTB (config)# enable secret heslo
```

- *Nastavenie kľúča heslo pre privilegovaný mód. Kľúč je zakrytovaný a prevyšuje heslo.*

```
UTB (config)# line con 0
```

```
UTB (config-line)# login
```

```
UTB (config-line)# password Cisco
```

- *Nastavenie hesla pre konzolu.*

```
UTB (config)# line aux 0
```

```
UTB (config-line)# password cisco
```

```
UTB (config-line)# login
```

- *Nastavenie hesla pre AUX port*

```
UTB (config)# line vty 0 4
```

```
UTB (config-line)# login
```

```
UTB (config-line)# password Cisco
```

- *Nastavenie hesla cisco pre telnet.*

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

- *Zaheslovanie Hesiel vo vypise show run*

```
UTB (config)# interface fastethernet 0/0
```

```
UTB (config-if)# ip address 192.168.1.1 255.255.255.0
```

```
UTB (config-if)# no shutdown
```

- *Konfigurácia rozhrania a následné zapnutie do stavu ON.*

### 7.2.1 Overenie stavu portov

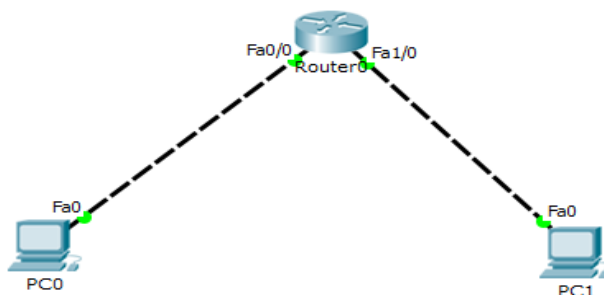
```
UTB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP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

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0
```

*Obr. 30. Výpis príkazu show ip route*

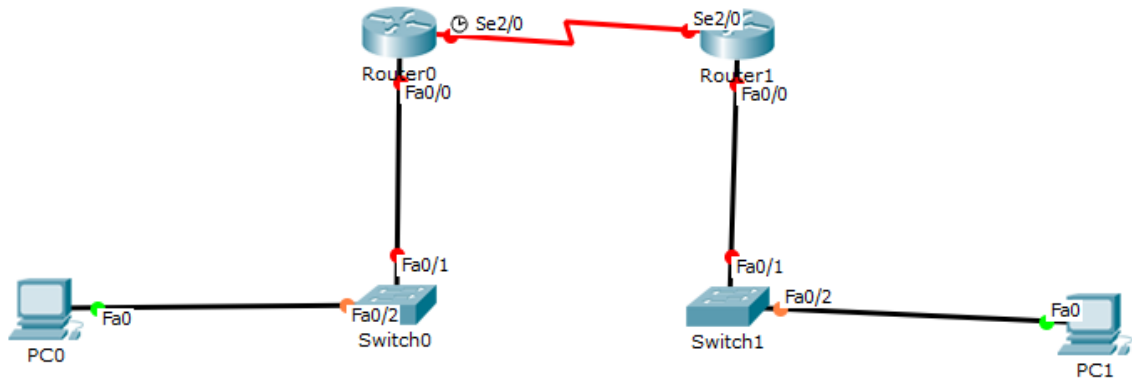
Ako si môžeme všimnúť na obrázku 31 sú porty v stave UP a taktiež aj nakonfigurované, čo signalizuje zelená farba.



*Obr. 31. Funkčné zapojenie siete*

## 8 ÚLOHA ČÍSLO 2 – KONFIGURÁCIA RIP VERZIA 1

Topológia:



Obr. 32. Ukážkové zapojenie RIPv1

Adresovacia tabuľka:

Tab. 6: IP adresy pre rozhranie smerovačov a PC zariadení

Zariadenie	Interface	IP Address	Subnet Mask	Default Gateway
PC 0		192.168.10.2	255.255.255.0	192.168.10.1
PC 1		192.168.11.2	255.255.255.0	192.168.11.1
Router0	Fa0/0	192.168.10.1	255.255.255.0	
	Se2/0	10.10.0.2	255.255.255.224	
Router1	Fa0/0	192.168.11.1	255.255.255.0	
	Se2/0	10.10.0.3	255.255.255.224	
Switch0		VLAN 1		
Switch1		VLAN 1		

### 8.1 Ciele úlohy

**Prvá časť: Zostaviť a nakonfigurovať základné nastavenia zariadení**

- Vytvorenie a nastavenie topológie pomocou správnych zariadení.
- Základná konfigurácia aktívnych zariadení.
- Konfigurácia šifrovania hesiel.
- Priradenie triedy do privilegovaného EXEC hesla.
- Nastavenie konzoly a vty hesiel.
- Konfigurácia pre synchronne prihlasovanie pre konzolu linky.
- Konfigurovať IP adresu uvedenú v tabuľke pre všetky rozhrania.

- Overovanie pomocou príkazu ping.
- Test pripojenia.

### **Druhá časť: Konfigurácia a overenie protokolu RIP**

- Konfigurácia a overenie protokolu RIP na smerovačoch.
- Konfigurácia pasívneho rozhrania.
- Skontrolovanie, pomocou smerovacích tabuliek.
- Zakázať automatickú sumarizáciu.
- Skontrolovanie end-to-end konektivitu.

## **8.2 Konfigurácia protokolu RIP.**

Pri konfigurácii smerovacieho protokolu RIP najskôr router inštruujeme k spusteniu príslušného smerovacieho procesu príkazom **router rip**. Tak vznikne nová sekcia konfiguračného súboru, ktorý sa týka tohto smerovacieho procesu. Musíme určiť priamo pripojené siete. Každá sieť, ktorá ma generovať a poslúchať správy protokolu RIP sa musí explicitne uviesť pomocou príkazu **network [sieť]**.

1. Na príslušných smerovačoch nakonfigurovať protokol RIP a inzerovať do príslušnej siete.

```
Router# config t
```

```
Router(config)# router rip
```

- Príkaz router RIP spustí smerovací prenos.
- Otvára režim konfigurovania protokolu RIP.

```
Router(config-router)# network 192.168.10.0
```

```
Router(config-router)# network 10.0.0.0
```

```
Router(config-router)# network 192.168.11.0
```

Príkaz network na slúži:

- Na rozhraniach do každej adresy siete spustí zasielanie a prijímanie aktualizácií.
- Na smerovači musí byť daná IP adresa.
- Rozhranie však musí byť v stave UP.

Overenie sériových zapojení skontrolujeme na obidvoch smerovačoch príkazom **show ip interface brief**. Tento príkaz nám zobrazí základné informácie o fyzických

stavoch portoch (rozhraniach) napr. serial2/0, ku ktorému je priradená IP adresa a je v stave UP.

```
Router#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.11.1    YES manual up          up
FastEthernet1/0    unassigned      YES unset   administratively down down
Serial2/0          10.10.0.3       YES manual up          up
```

Obr. 33. Tabuľka rozhraní smerovača Router1

```
Router#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.10.1    YES manual up          up
FastEthernet1/0    unassigned      YES unset   administratively down down
Serial2/0          10.10.0.2       YES manual up          up
```

Obr. 34. Tabuľka rozhraní smerovača Router0

Na skontrolovanie protokolu RIP na smerovačoch používame príkazy: **debug ip rip**, **show ip protocols** a **show run**. Príkaz **show ip protocols** je uvedený nižšie.

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 11 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  FastEthernet0/0    1     2 1
  Serial2/0          1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  192.168.11.0
Passive Interface(s):
Routing Information Sources:
  Gateway            Distance    Last Update
  10.10.0.2           120        00:00:15
Distance: (default is 120)
```

Obr. 35. Tabuľka protokolu RIP

Príkaz **show ip route** nám overuje smerovanie a ukáže spojenia ciest. Prvoradou funkciou smerovača je určiť najlepšiu cestu do cieľa a tie vidíme na obrázkoch 36 a 37.

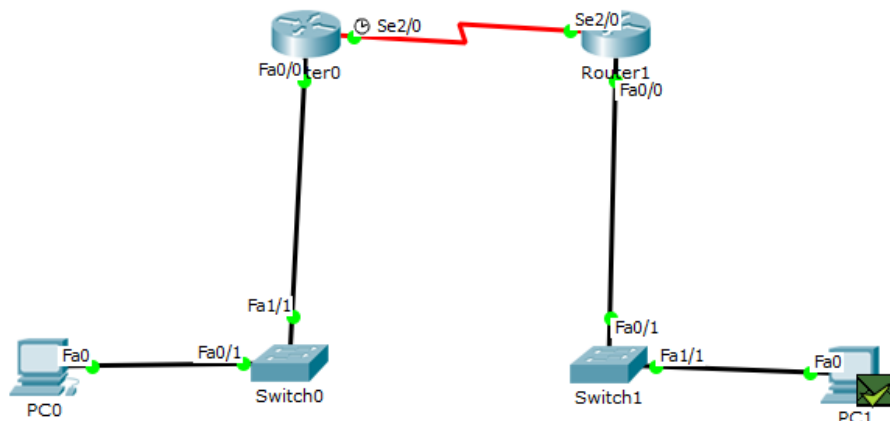
```
C 10.0.0.0/8 is directly connected, Serial2/0
C 192.168.10.0/24 is directly connected, FastEthernet0/0
R 192.168.11.0/24 [120/1] via 10.10.0.3, 00:00:19, Serial2/0
```

Obr. 36. Smerovacia tabuľka smerovača Router0

```
C 10.0.0.0/8 is directly connected, Serial2/0
R 192.168.10.0/24 [120/1] via 10.10.0.2, 00:00:24, Serial2/0
C 192.168.11.0/24 is directly connected, FastEthernet0/0
```

Obr. 37. Smerovacia tabuľka smerovača Router1

Na obrázku 38 je vidieť, že všetky porty sú nakonfigurované. Signalizuje to zelená farba na všetkých fastethernetových a sériových portoch.



Obr. 38. Nakonfigurované a spustené zapojenie

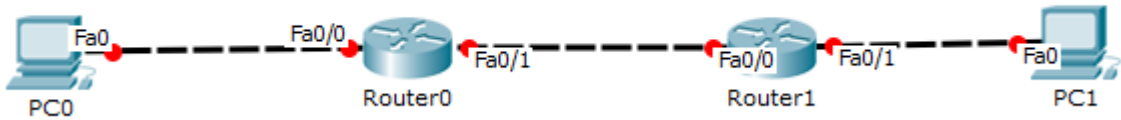
Nakoniec, po nakonfigurovaní siete vyskúšame funkčnosť siete pomocou dátového paketu ako môžeme vidieť nižšie na obrázku.

Fire	Last Status	Source	Destination	Type
●	Successful	PC1	PC0	ICMP
●	Successful	PC1	Router1	ICMP
●	Successful	PC1	Router0	ICMP

Obr. 39. Funkčnosť zapojenia

## 9 ÚLOHA ČÍSLO 3 – KONFIGURÁCIA RIP VERZIA 2

Topológia:



Obr. 40. Ukážkové zapojenie RIPv2

Adresovacia tabuľka:

Tab. 7: IP adresy pre rozhranie smerovačov a PC zariadení

Zariadenie	Interface	IP Address	Subnet Mask	Default Gateway
PC0	Fa0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	Fa0	192.168.20.2	255.255.255.0	192.168.20.1
Router0	Fa0/0	192.168.10.1	255.255.255.0	
	Fa0/1	10.10.10.1	255.255.255.252	
Router1	Fa0/0	10.10.10.2	255.255.255.252	
	Fa0/1	192.168.10.1	255.255.255.0	

### 9.1 Ciele úlohy

**Prvá časť: Zostaviť a nakonfigurovať základné nastavenia zariadení**

- Vytvorenie a nastavenie topológie pomocou správnych zariadení.
- Základná konfigurácia aktívnych zariadení.
- Konfigurácia šifrovania hesiel.
- Priradenie triedy do privilegovaného EXEC hesla.
- Nastavenie konzoly a vty hesiel.
- Konfigurácia pre synchronne prihlasovanie pre konzolu linky.
- Konfigurovať IP adresu uvedenú v tabuľke pre všetky rozhrania.
- Overovanie pomocou príkazu ping.
- Test pripojenia.

**Druhá časť: Konfigurácia a overenie protokolu RIPv2**

- Konfigurácia a overenie protokolu RIPv2 na smerovačoch.
- Konfigurácia pasívneho rozhrania.
- Skontrolovanie, pomocou smerovacích tabuliek.
- Zakázať automatickú sumarizáciu.
- Skontrolovanie end-to-end konektivity.
- Skontrolovanie konektivity pomocou príkazu PING.

**Ripv2 ma väčšinu podobných vlastností:**

- Rovnaká metrika.
- Rovnaké ohraničenie maxima.
- Používajú rovnaké časovače.
- Update každých 30s.

**Zmeny:**

- Autentifikácia.
- Manuálna, alebo automatická sumarizácia.
- Classless.

**9.2 Základná konfigurácia protokolu RIPv2 :****Router 0**

```
Router>enable
```

```
Router#config t
```

```
Router(config)# interface fastEthernet 0/1
```

```
Router(config-if)# ip address 10.10.10.1 255.255.255.0
```

```
Router(config-if)# no shutdown
```

```
Router(config-if)# exit
```

```
Router(config)# interface fastEthernet 0/0
```

```
Router(config-if)# ip address 192.168.10.1 255.255.255.0
```

```
Router(config-if)# no shutdown
```

```
Router(config-if)# exit
```

```
Router(config)# router rip
```

```
Router(config-router)# version 2
```

```
Router(config-router)# network 10.10.10.0
```

```
Router(config-router)# network 192.168.10.0
```

## Router 1

```
Router>enable
```

```
Router#config t
```

```
Router(config)# interface fastEthernet 0/0
```

```
Router(config-if)# ip address 10.10.10.2 255.255.255.0
```

```
Router(config-if)# no shutdown
```

```
Router(config-if)# exit
```

```
Router(config)# interface fastEthernet 0/1
```

```
Router(config-if)# ip address 192.168.20.1 255.255.255.0
```

```
Router(config-if)# no shutdown
```

```
Router(config-if)# exit
```

```
Router(config)# router rip
```

```
Router(config-router)# version 2
```

```
Router(config-router)# network 10.10.10.0
```

```
Router(config-router)# network 192.168.20.0
```

Príkaz network slúži na:

- Rozhodne do ktorej priamo pripojenej siete pošleme RIP pakety.
- Rozhodne z ktorej priamo pripojenej siete prijmemme RIP pakety.

### 9.2.1 Overenie činnosti RIPv2

Na overenie činnosti použijeme príkaz **show ip interfaces brief**.

```
Router#show ip interface brief
Interface                IP-Address      OK? Method Status  Protocol
FastEthernet0/0          192.168.10.1    YES manual up      up
FastEthernet0/1          10.10.10.1      YES manual up      up
```

*Obr. 41. Tabuľka na overenie portov*

Príkazom **show ip protocols**, nadobudneme informácie o protokole a taktiež aj určenie poslednej smerovacej aktualizácie. Zobrazí informácie o protokole RIP a taktiež aj o intervaloch updatov ako môžeme vidieť na obrázku 42.

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
FastEthernet0/0      2     2
FastEthernet0/1      2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  192.168.10.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  10.10.10.2      120           00:00:29
```

*Obr. 42. Tabuľka protokolu RIPv2*

Príkazom **show ip route** zistíme akým spôsobom si porty pripojené. Po zadaní príkazu sa zobrazí smerovanie. Obsah tabuľky obsahuje známe siete a podsiete.

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

Gateway of last resort is not set

  10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/1
C       192.168.10.0/24 is directly connected, FastEthernet0/0
R       192.168.20.0/24 [120/1] via 10.10.10.2, 00:00:29, FastEthernet0/1
```

*Obr. 43. Smerovacia tabuľka*

Funkčnost siete sme si overili príkazom ping. Komunikácia musí prebiehať medzi koncovými zariadeniami. Po zadaní IP adresy, zobrazí správnosť doručenia paketov.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

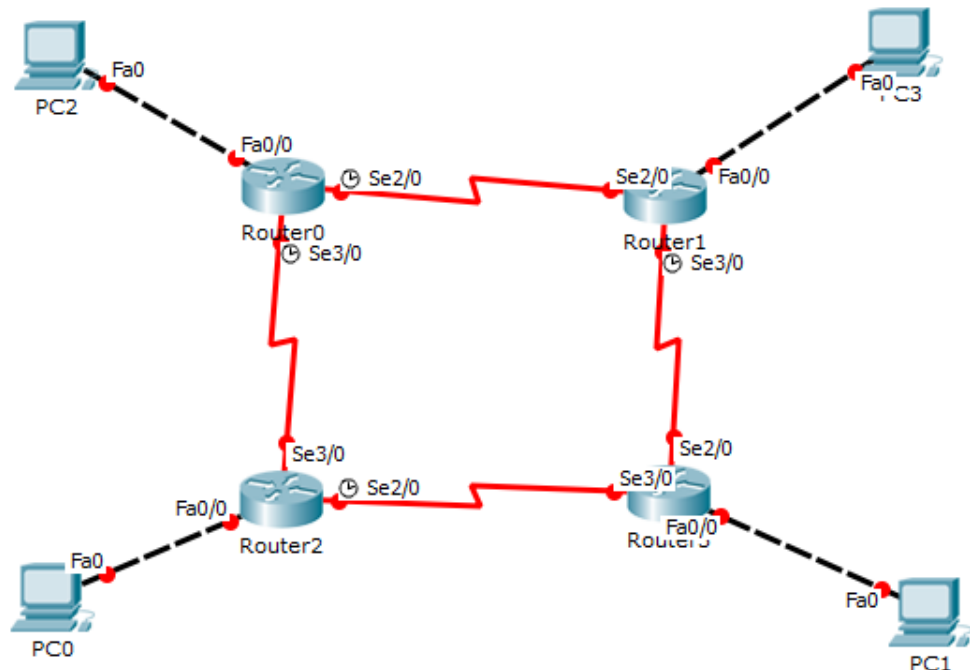
Request timed out.
Reply from 192.168.10.2: bytes=32 time=0ms TTL=126
Reply from 192.168.10.2: bytes=32 time=0ms TTL=126
Reply from 192.168.10.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

*Obr. 44. Príkaz PING na vyskúšanie zapojenia*

## 10 ÚLOHA ČÍSLO 4 – KONFIGURÁCIA EIGRP

Topológia:



Obr. 45. Ukážkové zapojenie EIGRP

Adresovacia tabuľka:

Tab. 8: IP adresy pre rozhranie smerovačov a PC zariadení

Zariadenie	Interface	IP address	Subnet Mask	Default Gateway
PC 0		192.168.15.66	255.255.255.240	192.168.15.65
PC 1		192.168.15.50	255.255.255.240	192.168.15.49
PC 2		192.168.15.2	255.255.255.224	192.168.15.1
PC 3		192.168.15.34	255.255.255.240	192.168.15.33
Router0	Se2/0	192.168.10.1	255.255.255.252	
	Se3/0	192.168.40.2	255.255.255.252	
	Fa0/0	192.168.15.1	255.255.255.224	
Router1	Se2/0	192.168.10.2	255.255.255.252	
	Se3/0	192.168.20.1	255.255.255.252	
	Fa0/0	192.168.15.33	255.255.255.240	
Router2	Se3/0	192.168.40.1	255.255.255.252	
	Se2/0	192.168.30.2	255.255.255.252	
	Fa0/0	192.168.15.65	255.255.255.240	
Router3	Se2/0	192.168.20.2	255.255.255.252	
	Se3/0	192.168.30.1	255.255.255.252	
	Fa0/0	192.168.15.49	255.255.255.240	

## 10.1 Ciele úlohy

### Prvá časť: Zostaviť a nakonfigurovať základné nastavenia zariadení

- Vytvorenie a nastavenie uvedenej topológie.
- Konfigurácia šifrovania hesiel.
- Nastavenie hesiel pre privilegovaný mód.
- Zabezpečenie a nastavenie hesla pre konzolu.
- Nastavenie hesiel pre telnet, ssh (virtuálne terminály).
- Konfigurovať názov zariadenia, ako je uvedené v topológii.
- Nastavenie clock-rate na portoch.
- Konfigurácia pre synchrónne prihlasovanie pre konzolu linky.
- Konfigurácia PC zariadení.
- Test pripojenia.

### Druhá časť: Konfigurácia a overenie protokolu EIGRP

- Konfigurácia EIGRP na smerovačoch.
- Overenie informácií o smerovaní.
- Overenie nastavení protokolu EIGRP.
- Overenie informácií o procese.
- Skontrolovanie nastavenia rozhrania EIGRP.
- Skontrolovanie end-to-end konektivity.

#### Router 0

```
Router(config)# router eigrp 1
```

```
Router(config-router)# network 192.168.10.0 0.0.0.3
```

```
Router(config-router)# network 192.168.40.0 0.0.0.3
```

```
Router(config-router)# no auto-summary
```

#### Router 1

```
Router(config)# router eigrp 1
```

```
Router(config-router)# network 192.168.20.0 0.0.0.3
```

```
Router(config-router)# network 192.168.10.0 0.0.0.3
```

```
Router(config-router)# no auto-summary
```

## Router 2

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.30.0 0.0.0.3
Router(config-router)# network 192.168.40.0 0.0.0.3
Router(config-router)# no auto-summary
```

## Router 3

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.30.0 0.0.0.3
Router(config-router)# network 192.168.30.0 0.0.0.3
Router(config-router)# no auto-summary
```

### 10.1.1 Susedia EIGRP

Po výpise pomocou príkazu **show ip eigrp neighbors** sa nám vytvorí tabuľka. Na prvom mieste máme číslice 0 a 1. Jedná sa o poradie v ktorom bola založená relácia s daným susedom. Nasleduje susedova IP adresa. Ďalej vidíme rozhranie prijímajúce heloo pakety. **Hold (sec)** nám ukazuje o koľko sekúnd sa stane sused neaktívny, ak sa neozve platný EIGRP paket. **Uptime** nám ukazuje životnosť paketu. **SRTT** indikuje trvanie dokiaľ sused odpovie na naše pakety. **RTO** indikuje, ako dlho čakáme na retransmisiu. **Q Count** býva vždy 0. V opačnom prípade je zahľtená linka. **Seq num** je číslo posledného update.

```
Zlin#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address          Interface          Hold Uptime      SRTT   RTO   Q   Seq
   (sec)              (ms)              Cnt   Num
0   192.168.40.1       Se3/0              14    02:19:49  40    1000  0   9
1   192.168.10.2       Se2/0              11    02:19:47  40    1000  0   7
```

Obr. 46. Tabuľka susedov na smerovači Zlín

### 10.1.2 Overenie EIGRP

Prvé písmeno nám indikuje, či je sieť aktívna, alebo pasívna. Ďalej nasleduje **cieľová IP adresa** a počet successorov. **FD** je feasible distance. Pokračujeme ip adresou next hopu. Posledný údaj je rozhranie použité na dosiahnutie danej siete.

```
Zlin#show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.10.0/30, 1 successors, FD is 20512000
   via Connected, Serial2/0
P 192.168.15.0/27, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 192.168.20.0/30, 1 successors, FD is 21024000
   via 192.168.10.2 (21024000/20512000), Serial2/0
P 192.168.30.0/30, 1 successors, FD is 21536000
   via 192.168.10.2 (21536000/21024000), Serial2/0
P 192.168.40.0/30, 1 successors, FD is 20512000
   via Connected, Serial3/0
IP-EIGRP Topology Table for AS 86
```

Obr. 47. Tabuľka susedov na smerovači Zlín

Smerovanie EIGRP záznamu zistíme použitím príkazom **show ip route** kde nám zobrazí obsah smerovacej tabuľky, ktorá obsahuje záznamy o všetkých známych sieťach a taktiež aj spôsob vytvorenia, akým bol záznam vytvorený.

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

Gateway of last resort is not set

192.168.10.0/30 is subnetted, 1 subnets
C    192.168.10.0 is directly connected, Serial2/0
192.168.15.0/27 is subnetted, 1 subnets
C    192.168.15.0 is directly connected, FastEthernet0/0
192.168.20.0/30 is subnetted, 1 subnets
D    192.168.20.0 [90/21024000] via 192.168.10.2, 00:08:41, Serial2/0
192.168.30.0/30 is subnetted, 1 subnets
D    192.168.30.0 [90/21536000] via 192.168.10.2, 00:08:41, Serial2/0
192.168.40.0/30 is subnetted, 1 subnets
C    192.168.40.0 is directly connected, Serial3/0
```

Obr. 48. Smerovacia tabuľka smerovača Zlín

Overenie EIGRP príkazom **show ip protocols**, kde zistíme informácie o protokole, ktorý bol nakonfigurovaný na smerovači Zlín.

```
Zlin#show ip protocols

Routing Protocol is "eigrp 1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 1
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.15.0/27
    192.168.10.0/30
    192.168.40.0/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.2     90            95199705
    192.168.40.1     90            95199698
  Distance: internal 90 external 170
```

*Obr. 49. Tabuľka o protokole EIGRP na smerovači Zlín*

Overenie EIGRP pomocou príkazu **show ip route EIGRP**. Na obrázku 50 vidíme informácie o cestách a smerovaní do každého cieľového miesta.

```
Zlin#show ip route
Gateway of last resort is not set

  192.168.10.0/30 is subnetted, 1 subnets
C       192.168.10.0 is directly connected, Serial2/0
  192.168.15.0/27 is subnetted, 1 subnets
C       192.168.15.0 is directly connected, FastEthernet0/0
  192.168.20.0/30 is subnetted, 1 subnets
D       192.168.20.0 [90/21024000] via 192.168.10.2, 00:08:41, Serial2/0
  192.168.30.0/30 is subnetted, 1 subnets
D       192.168.30.0 [90/21536000] via 192.168.10.2, 00:08:41, Serial2/0
  192.168.40.0/30 is subnetted, 1 subnets
C       192.168.40.0 is directly connected, Serial3/0
Zlin#show ip route ei
Zlin#show ip route eigrp
  192.168.20.0/30 is subnetted, 1 subnets
D       192.168.20.0 [90/21024000] via 192.168.10.2, 00:08:41, Serial2/0
  192.168.30.0/30 is subnetted, 1 subnets
D       192.168.30.0 [90/21536000] via 192.168.10.2, 00:08:41, Serial2/0
```

*Obr. 50. Topologická tabuľka smerovača Zlín*

Overenie EIGRP príkazom **show ip eigrp interfaces**, kde sa nám ukážu všetci EIGRP susedia. Na obrázku 51 máme zobrazenú tabuľku susedov.

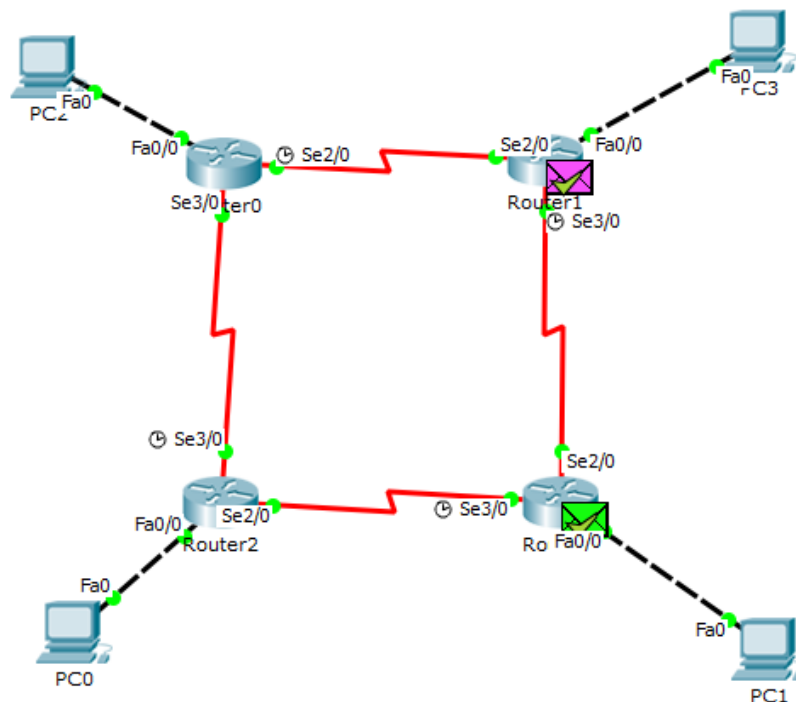
```

Zlin#show ip eigrp inter
Zlin#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

Interface          Xmit Queue    Mean Spacing   Pacing Time   Multicast     Pending
                   Un/Reliable   SRTT        Un/Reliable   Flow Timer    Routes
-----
Fa0/0              0             0/0         1236         0/10         0            0
Se3/0              1             0/0         1236         0/10         0            0
Se2/0              1             0/0         1236         0/10         0            0
IP-EIGRP interfaces for process 86

```

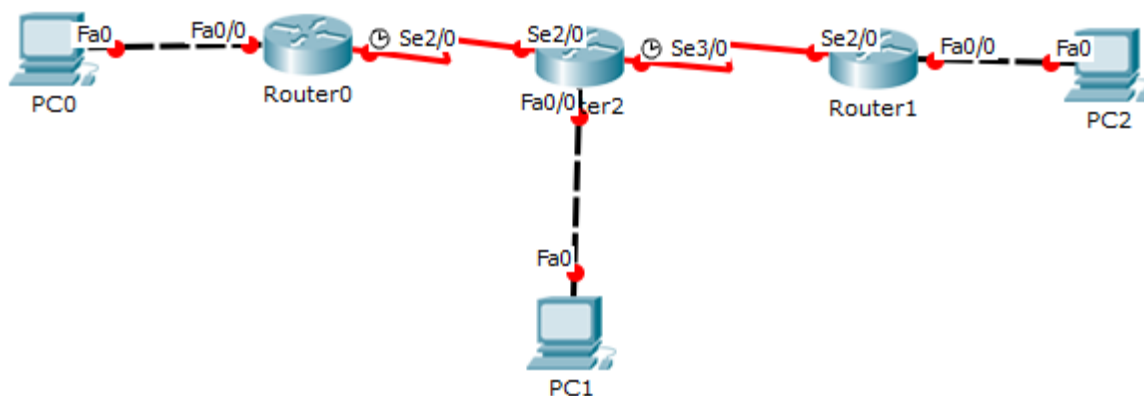
Obr. 51. Tabuľka rozhraní na smerovači Zlín.



Obr. 52. Nakonfigurované a spustené zapojenie

## 11 ÚLOHA ČÍSLO 5 – KONFIGURÁCIA OSPF

Topológia:



Obr. 53. Ukážkové zapojenie OSPF

Adresovacia tabuľka:

Tab. 9: IP adresy pre rozhranie smerovačov a PC zariadení

Zariadenie	Interface	IP address	Subnet Mask	Default Gateway
PC0		172.16.10.2	255.255.255.0	172.16.10.1
PC1		172.16.30.2	255.255.255.0	172.16.30.1
PC2		172.16.50.2	255.255.255.0	172.16.50.1
Router0	Fa0/0	172.16.10.1	255.255.255.0	
	Se2/0	172.16.20.1	255.255.255.252	
Router1	Se2/0	172.16.20.2	255.255.255.252	
	Se3/0	172.16.40.1	255.255.255.252	
	Fa0/0	172.16.30.1	255.255.255.0	
Router2	Se2/0	172.16.40.2	255.255.255.252	
	Fa0/0	172.16.50.1	255.255.255.0	

### 11.1 Ciele úlohy

**Prvá časť: Zostaviť a nakonfigurovať základné nastavenia zariadení**

- Vytvorenie a nastavenie uvedenej topológie.
- Konfigurácia šifrovania hesiel.
- Nastavenie hesiel pre privilegovaný mód.
- Zabezpečenie a nastavenie hesla pre konzolu.
- Nastavenie hesiel pre telnet, ssh (virtuálne terminály).
- Konfigurovať názov zariadenia, ako je uvedené v topológii.
- Nastavenie clock-rate na portoch.

- Konfigurácia pre synchronne prihlasovanie pre konzolu linky.
- Konfigurácia PC zariadení.
- Test pripojenia.

#### **Druhá časť: Konfigurácia a overenie protokolu OSPF**

- Konfigurácia OSPF na smerovačoch.
- Overenie informácií o smerovaní.
- Overenie nastavení protokolu OSPF.
- Overenie informácií o procese.
- Skontrolovanie nastavenia rozhrania OSPF.
- Skontrolovanie end-to-end konektivity

### **11.2 Konfigurácia protokolu OSPF.**

Na spustenie procesu OSPF použijeme príkaz **router ospf 38**. Číslo procesu je 38, ale môže to byť ľubovoľné číslo od 1 do 65 535 a je vždy lokálne pre daný router. V ďalšom kroku definujeme zoznam rozhraní, ktoré budú spoločne so svojimi sieťami zaradené do OSPF procesu. Na príslušných smerovačoch je nutné nakonfigurovať protokol OSPF a inzerovať do príslušnej siete.

```
Router# config t
```

```
Router(config)# router ospf 38
```

```
Router(config-router)# network 172.16.0.0 0.0.255.255 area 0
```

```
Router(config-router)# exit
```

Základné informácie o smerovacích procesoch, ktoré sú spustené na smerovači si zistíme príkazom **show ip protocols**.

```
Router#show ip protocols

Routing Protocol is "ospf 38"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.20.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.0.0 0.0.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  172.16.20.1             110          00:17:49
  172.16.40.1             110          00:17:51
  172.16.50.1             110          00:18:01
```

*Obr. 54. Tabuľka o protokole OSPF na smerovači Router1*

Pomocou príkazu **show ip ospf neighbor** zistíme výpisy OSPF susedov a susedského stavu. Na prvom mieste je zoznam RID susedov v poradí, v akom boli naučený. Na druhom mieste je priorita na danom OSPF rozhraní. Na ďalšom mieste je stav. **FULL** znamená, že máme identické DB. **Dead Time** je čas, dokiaľ sused nebude down. Po prijatí Hello paketu sa obnoví časovač. Nasleduje **IP adresa** rozhrania, ku ktorému sme priamo pripojený. Posledný **interface** je rozhranie, cez ktoré sme pripojený s daným susedom.

```
Router#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.20.1	0	FULL/ -	00:00:36	172.16.20.1	Serial2/0
172.16.50.1	0	FULL/ -	00:00:36	172.16.40.2	Serial3/0

*Obr. 55. Susedia na smerovači Router1*

Príkazom **show ip interface brief** sa pozrieme, na prehľad stavu všetkých rozhraní. Zaujímavé sú pre nás rozhrania, kde sú nakonfigurované IP adresy.

```
Router#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	172.16.30.1	YES	manual	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	172.16.20.2	YES	manual	up	up
Serial3/0	172.16.40.1	YES	manual	up	up
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down

*Obr. 56. Stav rozhraní na Router1*

Spojenie a Overenie ospf si overíme **show ip route ospf**, kde môžeme vidieť pripojené zariadenia v smerovacej tabuľke.

```
Router#show ip route ospf
```

```
172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O    172.16.10.0 [110/65] via 172.16.20.1, 01:11:10, Serial2/0
O    172.16.50.0 [110/65] via 172.16.40.2, 01:11:21, Serial3/0
```

*Obr. 57. Smerovacia tabuľka na smerovači Router1*

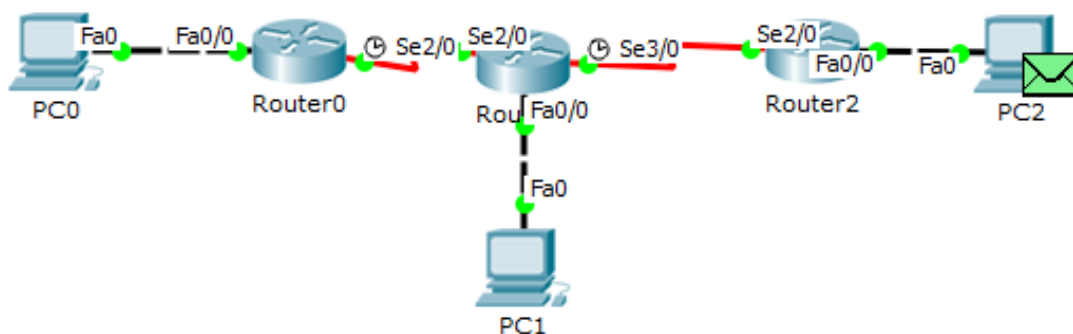
Príkazom **show ip ospf interface** si pozrieme na obrázku 58 v akom je stave je rozhranie (buď UP, alebo DOWN))

```
Router#show ip ospf interface serial 2/0

Serial2/0 is up, line protocol is up
 Internet address is 172.16.20.2/30, Area 0
 Process ID 38, Router ID 172.16.40.1, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:05
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1 , Adjacent neighbor count is 1
   Adjacent with neighbor 172.16.20.1
 Suppress hello for 0 neighbor(s)
```

Obr. 58. Výpis seriálového portu 2/0 na smerovači Router1

Vyskúšanie nakonfigurovaného zapojenia prebehlo úspešne. Dátový paket prišiel do PC1,PC2 a taktiež aj opačne.

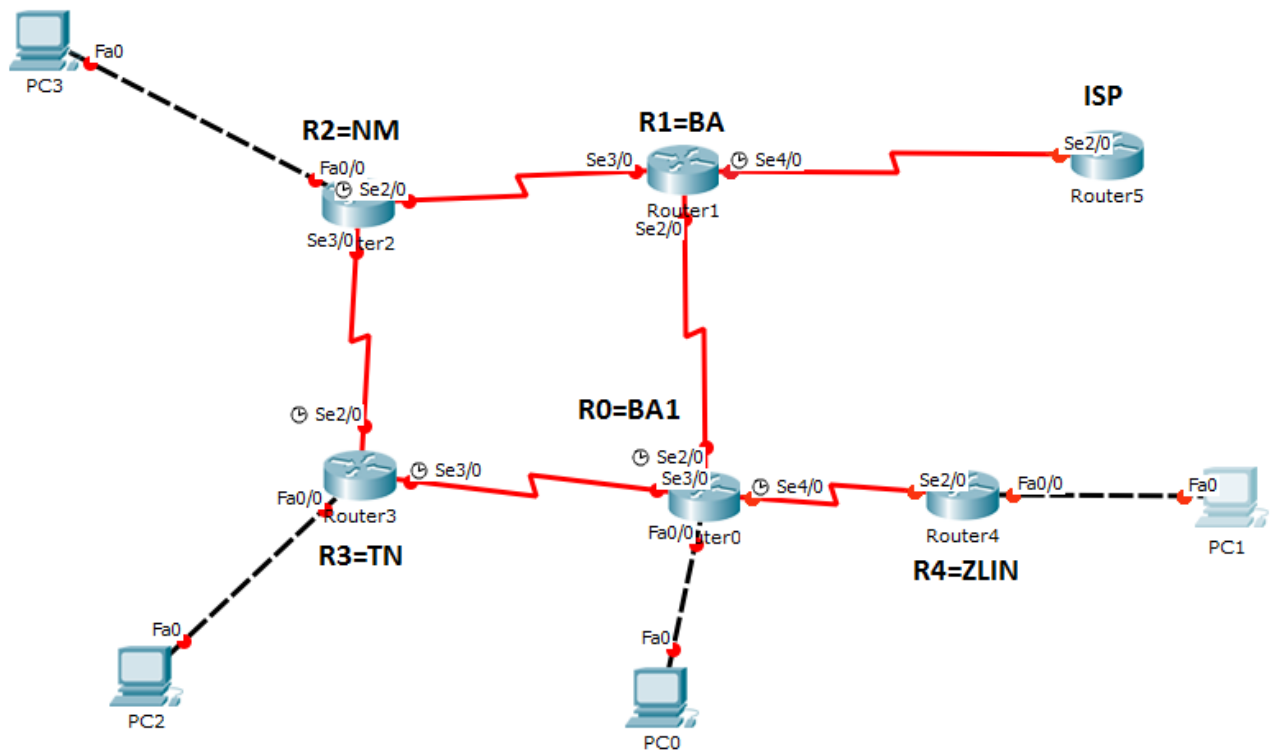


Obr. 59. Nakonfigurovaná a spustená sieť

## 12 ÚLOHA ČÍSLO 6 – KONFIGURÁCIA OSPF A ACCESS LISTOV

Táto sieť je nakonfigurovaná pomocou protokolu OSPF. Tento protokol zaisťuje kvalitný prenos dát. Protokol nie je zložitý na konfiguráciu, podstatné je pochopiť princíp. Sieť simuluje reálne zapojenie v praxi. Sieť je nakonfigurovaná pre zvýšenú kapacitu, kvôli rozširovaniu a pridávaniu aktívnych zariadení (myslené do budúcnosti). Do tejto siete sme vkladali ACL listy, pomocou ktorých sme zakazovali a povoľovali rôzne nastavenia. Pomocou access listov zvolíme pravidlá, ktoré užívatelia budú potrebovať k výkonu svojej práce.

### Topológia:



Obr. 60. Ukázkové zapojenie siete

**Adresovacia tabuľka:***Tab. 10: IP adresy pre rozhranie smerovačov a PC zariadení*

Zariadenie	Interface	IP address	Subnet Mask	Default Gateway
PC 0		200.15.4.66	255.255.255.192	200.15.4.65
PC 1		192.168.89.2	255.255.255.0	192.168.89.1
PC 2		192.168.14.2	255.255.255.192	192.168.14.1
PC 3		50.14.0.2	255.25.255.224	50.14.0.1
ISP		210.8.0.64	255.255.255.252	
	Se 2/0	210.8.0.66	255.255.255.252	
Router 0-BA1	Se 4/0	192.168.88.2	255.255.255.252	
	Se 2/0	200.15.4.134	255.255.255.252	
	Fa 0/0	200.15.4.65	255.255.255.192	
	Se 3/0	50.14.0.38	255.255.255.252	
Router 1- BA	Se 2/0	200.15.4.133	255.255.255.252	
	Se 3/0	200.15.4.130	255.255.255.252	
	Se 4/0	210.8.0.65	255.255.255.252	
Router 2-NM	Fa 0/0	50.14.0.1	255.255.255.224	
	Se 2/0	200.15.4.129	255.255.255.252	
	Se 3/0	50.14.0.33	255.255.255.252	
Router 3-TN	Fa 0/0	192.168.14.1	255.255.255.192	
	Se 2/0	50.14.0.34	255.255.255.252	
	Se 3/0	50.14.0.37	255.255.255.252	
Router 4-Zlin	Fa 0/0	192.168.89.1	255.255.255.0	
	Se 2/0	192.1688.88.1	255.255.255.252	

**Ciele úlohy****Prvá časť: Zostaviť a nakonfigurovať základné nastavenia zariadení**

- Vytvorenie a nastavenie uvedenej topológie.
- Konfigurácia šifrovania hesiel.
- Nastavenie hesiel pre privilegovaný mód.
- Zabezpečenie a nastavenie hesla pre konzolu.
- Nastavenie hesiel pre telnet, ssh (virtuálne terminály).
- Konfigurovať názov zariadenia, ako je uvedené v typológii.
- Nastavenie clock-rate na portoch.
- Konfigurácia pre synchrónne prihlasovanie pre konzolu linky.
- Konfigurácia PC zariadení.
- Test pripojenia.

**Druhá časť: Konfigurácia a overenie protokolu OSPF**

- Konfigurácia OSPF na smerovačoch.
- Overenie informácií o smerovaní.
- Overenie nastavení protokolu OSPF.
- Overenie informácií o procese.
- Skontrolovanie nastavenia rozhrania OSPF.
- Skontrolovanie end-to-end konektivity.

**Tretia časť: Konfigurácia štandardných ACL**

- Konfigurácia štandardných ACL.
- Overiť a pomenovať ACL.
- Vytvoriť ACL, ktorý zakáže prístup všetkým zariadeniam z NM do TN.
- Test ACL.

**Štvrtá časť: Konfigurácia rozšírených ACL.**

- Konfigurácia štandardných ACL.
- Overiť a pomenovať ACL.
- Vytvoriť ACL, ktorý zakáže všetkým zariadeniam v sieti BA prístup na internet.
- Test ACL.

Základné informácie o smerovacích procesoch, ktoré sú spustené na smerovači si zistíme príkazom **show ip protocols**.

```
BA1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 200.15.4.134
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    50.14.0.36 0.0.0.3 area 1
    200.15.4.132 0.0.0.3 area 1
    192.168.88.0 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
  192.168.14.1          110          00:11:39
  192.168.89.1          110          00:11:41
  200.15.4.129          110          00:11:41
  200.15.4.134          110          00:11:41
  210.8.0.65            110          00:11:39
```

*Obr. 61. Overenie protokolu OSPF na smerovači Router0 (BA1)*

Na zistenie v akom stave je susedný port, použijeme príkaz **show ip ospf neighbor**. Na obrázku 62 vidíme všetkých aktívnych susedov.

```
BA1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
210.8.0.65       0    FULL/ -         00:00:34   200.15.4.133 Serial2/0
192.168.14.1     0    FULL/ -         00:00:36   50.14.0.37  Serial3/0
192.168.89.1     0    FULL/ -         00:00:35   192.168.88.1 Serial4/0
```

*Obr. 62. Susedné porty na smerovači Router0 (BA1)*

Príkazom show **ip interface brief** sa pozrieme, na prehľad stavu všetkých rozhraní na smerovači Router0.

```
BA1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    200.15.4.65     YES manual up          up
FastEthernet1/0    unassigned      YES unset  administratively down down
Serial2/0          200.15.4.134    YES manual up          up
Serial3/0          50.14.0.38      YES manual up          up
Serial4/0          192.168.88.2    YES manual up          up
FastEthernet5/0    unassigned      YES unset  administratively down down
```

Obr. 63. Stav rozhraní na smerovači Router0 (BA1)

### 12.1.1 Overenie ospf: show ip route ospf

Na obrázkoch 64 a 65 si môžeme pozrieť overenie smerovacej tabuľky a overenie stavu sériového rozhrania 3/0.

```
BA1#show ip route ospf
 50.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O   50.14.0.0 [110/129] via 200.15.4.133, 05:18:00, Serial2/0
    [110/129] via 50.14.0.37, 05:18:00, Serial3/0
O   50.14.0.32 [110/128] via 50.14.0.37, 05:18:00, Serial3/0
192.168.14.0/26 is subnetted, 1 subnets
O   192.168.14.0 [110/65] via 50.14.0.37, 05:18:00, Serial3/0
O   192.168.89.0 [110/65] via 192.168.88.1, 05:18:00, Serial4/0
200.15.4.0/24 is variably subnetted, 3 subnets, 2 masks
O   200.15.4.128 [110/128] via 200.15.4.133, 05:18:00, Serial2/0
210.8.0.0/30 is subnetted, 1 subnets
O   210.8.0.64 [110/128] via 200.15.4.133, 05:18:00, Serial2/0
```

Obr. 64. Smerovacia tabuľka na smerovači Router0 (BA1)

```
BA1#show ip ospf interface serial 3/0

Serial3/0 is up, line protocol is up
 Internet address is 50.14.0.38/30, Area 1
 Process ID 1, Router ID 200.15.4.134, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:04
 Index 3/3, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1 , Adjacent neighbor count is 1
   Adjacent with neighbor 192.168.14.1
 Suppress hello for 0 neighbor(s)
```

Obr. 65. Overenie protokolu OSPF na sériovom porte3/0

## 12.2 Konfigurácia štandardného ACL

```
Router(config)#access-list ACCESS-LIST-# [deny | permit | remark]
TEST_PODMIENKA [WILDCARD] [log]

Router(config)#access-list 1 deny 50.14.0.0 0.0.0.31

Router(config)# interface fastethernet 0/0

Router(config-if)#ip access- group 1 out

Router(config)# exit
```

- Access-list

*Jedná sa o číslo ACL. Príslušnosť k danému ACL je uvedené týmto číslom.*

- Deny

*Znamená zakázať paketu splňujúcu podmienku*

- Permit

*Znamená povoliť paketu splňujúcu podmienku*

- Remark

*Znamená vložiť poznámku o nasledujúcej položke*

- TEST\_PODMIENKA

*Identifikuje podmienky vo forme IP adresy. Podľa tejto podmienky sa budú porovnávať zdrojové IP adresy vstupujúcich paketov.*

- Log

*Loguje pakety, ktoré odpovedajú kritéri*

Funkciou tohto access listu je povoliť užívateľom zo siete prístup na internet, komunikácia je možná len s IP adresou 210.8.0.66. Zvyšok komunikácie je zamietnutý príkazom *deny any*.

Ukážka konfigurácie štandardného ACL na smerovači BA 1.

```
BA1(config)#access-list 2 permit host 210.8.0.66
```

```
BA1(config)#interface fastEthernet 0/0
```

```
BA1(config-if)#ip access-group 2 in
```

```
BA1(config-if)# exit
```

```
BA1(config)#access-list 2 permit host 210.8.0.66
```

```
BA1(config)#access-list 2 deny any
```

```
BA1(config)#interface fastEthernet 0/0
```

```
BA1(config-if)#ip access-group 2 in
```

```
BA1(config)# exit
```

```

BA1(config)#access-list 2 permit host 210.8.0.66
BA1(config)#ac
BA1(config)#access-list deny?
% Unrecognized command
BA1(config)#inter
BA1(config)#interface fas
BA1(config)#interface fastEthernet 0/0
BA1(config-if)#ip
BA1(config-if)#ip acc
BA1(config-if)#ip access-group 2 in
BA1(config-if)#acc
BA1(config-if)#exit
BA1(config)#ac
BA1(config)#access-list 2 permin host 210.8.0.66
^
% Invalid input detected at '^' marker.

BA1(config)#access-list 2 permit host 210.8.0.66
BA1(config)#ac
BA1(config)#access-list 2 den
BA1(config)#access-list 2 deny an
BA1(config)#access-list 2 deny any
BA1(config)#inter
BA1(config)#interface fas
BA1(config)#interface fastEthernet 0/0
BA1(config-if)#ip
BA1(config-if)#ip acc
BA1(config-if)#ip access-group 2 in

```

Obr. 66. Štandardný ACL

```

BA1>enable
Password:
BA1#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
BA1(config)#
BA1(config)#ac
BA1(config)#access-list 2 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
BA1(config)#access-list 2 permi
BA1(config)#access-list 2 permit ?
  A.B.C.D Address to match
  any     Any source host
  host    A single host address
BA1(config)#access-list 2 permit hos
BA1(config)#access-list 2 permit host ?
  A.B.C.D Host address
BA1(config)#access-list 2 permit host 210.8.0.66 ?
  <cr>
BA1(config)#access-list 2 permit host 210.8.0.66

```

Obr. 67. Štandardný ACL

## 12.3 Rozšířený ACL

Rozšířené ACL slúžia na kontrolovanie a testovanie protokolovej sady, zdrojovej IP, zdrojového portu a cieľovej IP. ACL kontroluje zdrojovú adresu a aj cieľovú adresu.

```
BA1(config)#access-list 101 deny tcp 200.15.4.64 0.0.0.61 any eq 80
BA1(config)#access-list 101 deny tcp 200.15.4.64 0.0.0.61 any eq 443
```

*Obr. 68. Rozšířený ACL*

Vytvorený ACL, ktorý zakáže všetkým hostom zo siete 200.15.4.64/27 http a HTTPS kamkoľvek. Prvý ACL je definovaný portom 80. Zakazuje všetkým zariadeniam v sieti BA prístup na http. Druhý ACL zakazuje protokol HTTPS, ktorý je definovaný portom 443.

```
BA1(config)#access-list 101 deny tcp 200.15.4.64 0.0.0.61 any eq 80
BA1(config)#access-list 101 deny tcp 200.15.4.64 0.0.0.61 any eq 443
BA1(config)#inte
BA1(config)#interface fas
BA1(config)#interface fastEthernet 0/0
BA1(config-if)#ip acc
BA1(config-if)#ip access-group 101 in
```

*Obr. 69. Rozšířený ACL*

```
ZLIN(config)#access-list 102 deny tcp 192.168.89.0 0.0.0.255 any eq 23
ZLIN(config)#ac
ZLIN(config)#access-list 102 permit ip ann any
^
% Invalid input detected at '^' marker.

ZLIN(config)#access-list 102 permit ip any any
ZLIN(config)#int fa 0/0
ZLIN(config-if)#ip acc
ZLIN(config-if)#ip access-group 104 in
```

*Obr. 70. Ukážka zakázania a povolenia ACL*

### 12.3.1 Overenie ACL

Príkazom **show access-list**, alebo **show ip access-list** si overíme, aké ACL listy sme vytvorili.

```
BA1#show access-lists
Extended IP access list 101
 10 deny tcp 200.15.4.64 0.0.0.61 any eq www
 20 deny tcp 200.15.4.64 0.0.0.61 any eq 443
Standard IP access list 2
 10 permit host 210.8.0.66
 20 deny any
```

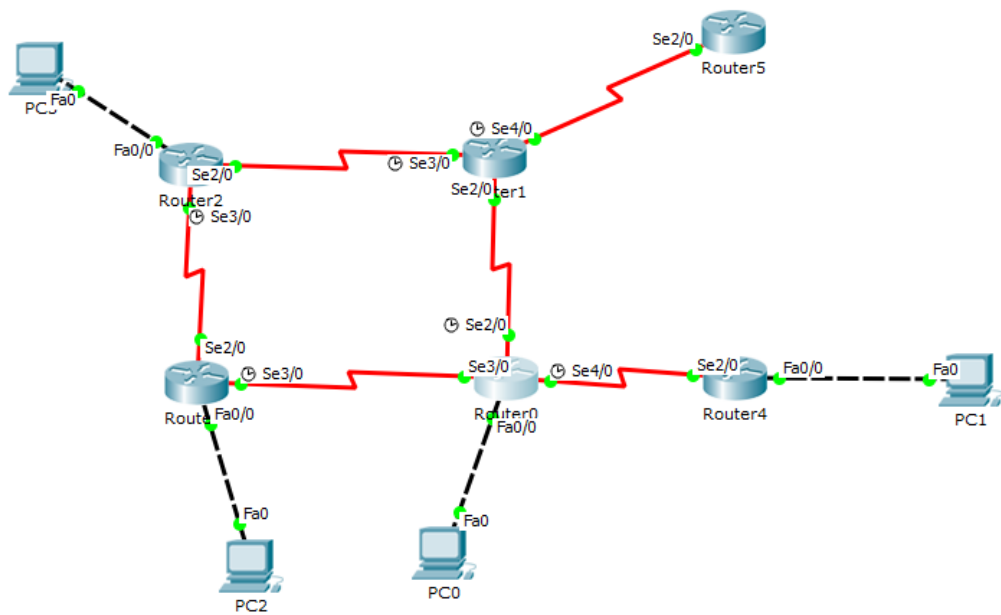
Obr. 71. ACL listy na smerovači Router0(BA1)

Príkazom **show running config**, uvidíme v sieti a vo fungujúcej konfigurácii aplikácie ACL a ich informácie o ACL:

```
interface FastEthernet0/0
ip address 200.15.4.65 255.255.255.192
ip access-group 2 in
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
ip address 200.15.4.134 255.255.255.252
clock rate 9600
!
interface Serial3/0
ip address 50.14.0.38 255.255.255.252
clock rate 2000000
!
interface Serial4/0
ip address 192.168.88.2 255.255.255.252
clock rate 9600
!
interface FastEthernet5/0
no ip address
shutdown

router ospf 1
log-adjacency-changes
network 50.14.0.36 0.0.0.3 area 1
network 200.15.4.132 0.0.0.3 area 1
network 192.168.88.0 0.0.0.3 area 1
!
ip classless
!
ip flow-export version 9
!
!
access-list 101 remark vypnutie internetovej prevadzky
access-list 101 deny tcp 200.15.4.64 0.0.0.61 any eq www
access-list 101 deny tcp 200.15.4.64 0.0.0.61 any eq 443
access-list 2 permit host 210.8.0.66
access-list 2 deny any
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login
```

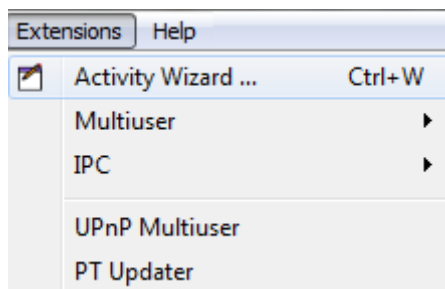
Obr. 72. Informácie o ACL



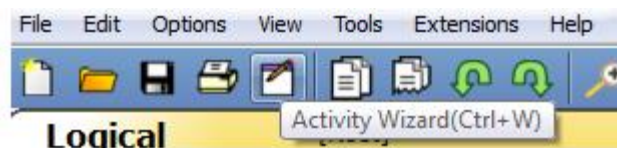
Obr. 73. Nakonfigurovaná a spustená sieť

### 13 AUTOMATICKÉ HODNOTENÉ ÚLOHY

V tejto kapitole si vyhodnotíme automaticky hodnotené úlohy. Úlohy spracujeme v simulačnom prostredí Packet Traceru. Klikneme na záložku Extension, alebo rovno v záložke symbolov na poznámkový blok. V skutočnosti klikneme na Activity Wizard. Máme dve možnosti spustenia podprogramu. Prvá úloha bude zapojenie predchádzajúcej siete, kde sme použili protokol OSPF. Postup vytvárania automatickej úlohy:



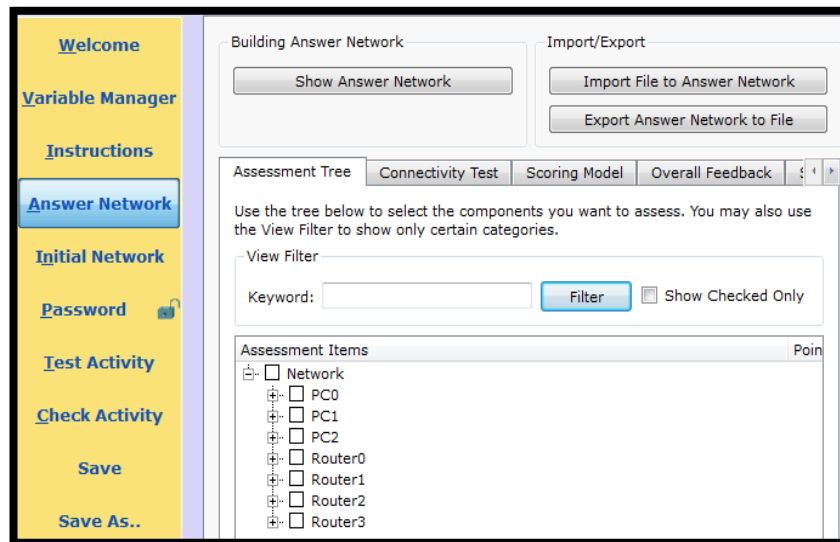
Obr. 74. Spustenie Activity Wizard



Obr. 75. Spustenie Activity Wizard

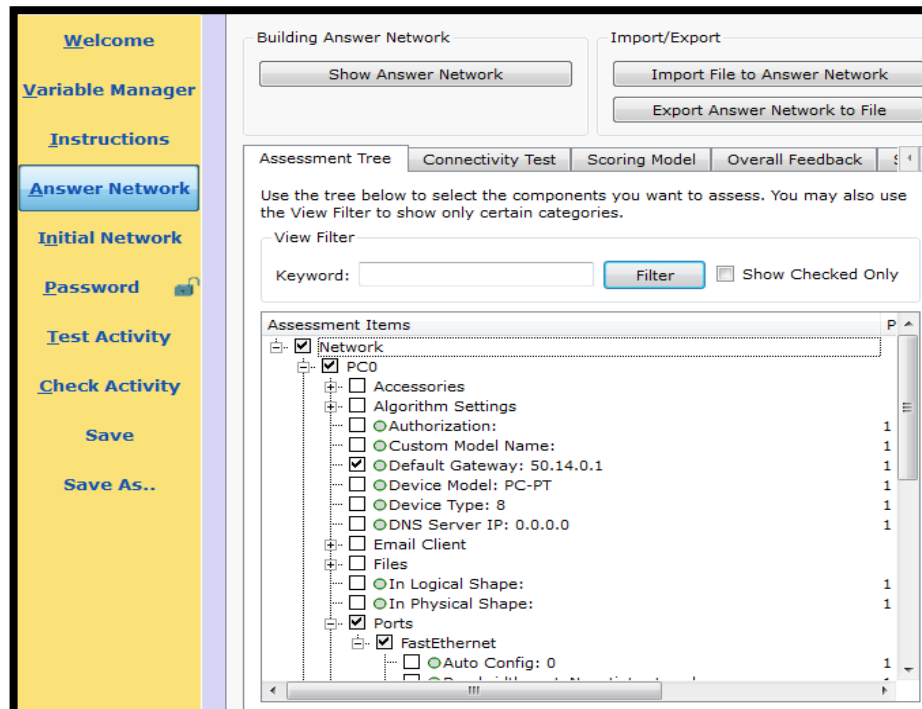
Prvým krokom je spustenie a nastavenie úrovne. My budeme používať úroveň intermediate (strednú). V ďalšom kroku si zvolíme postup jednotlivých úloh. Nastavenie všetkým WAN sietí, nastavenie IP adries na smerovačoch, zhodenie portov, nastavenie IP adries na PC zariadeniach a následná OSPF konfigurácia.

V položke Answer Network importujeme už nakonfigurovanú sieť. Po vložení siete sa nám otvoria všetky zariadenia v sieti.



Obr. 76. Záložka Answer Network a aktívne zariadenia v sieti

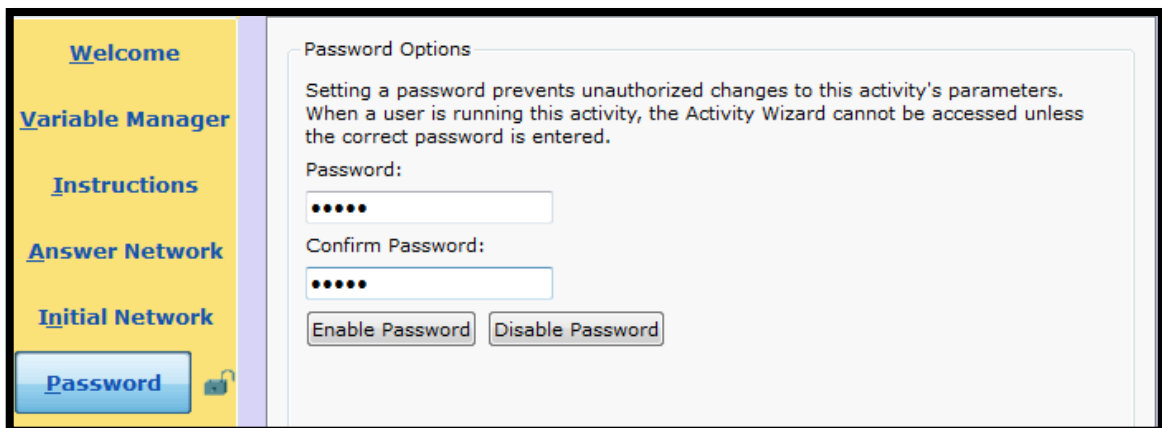
V ďalšom kroku vyberieme z každého počítača a routra informácie, ktoré budú potrebné ku konfigurácii. Za každú správnu nakonfigurovanú ip adresu, alebo portu nám budú pribúdať percentá až kým nedosiahneme 100%. Pri zložitejšej konfigurácii môžeme zmeniť hodnotenie z nižšieho na vyššie.



Obr. 77. Záložka Answer Network

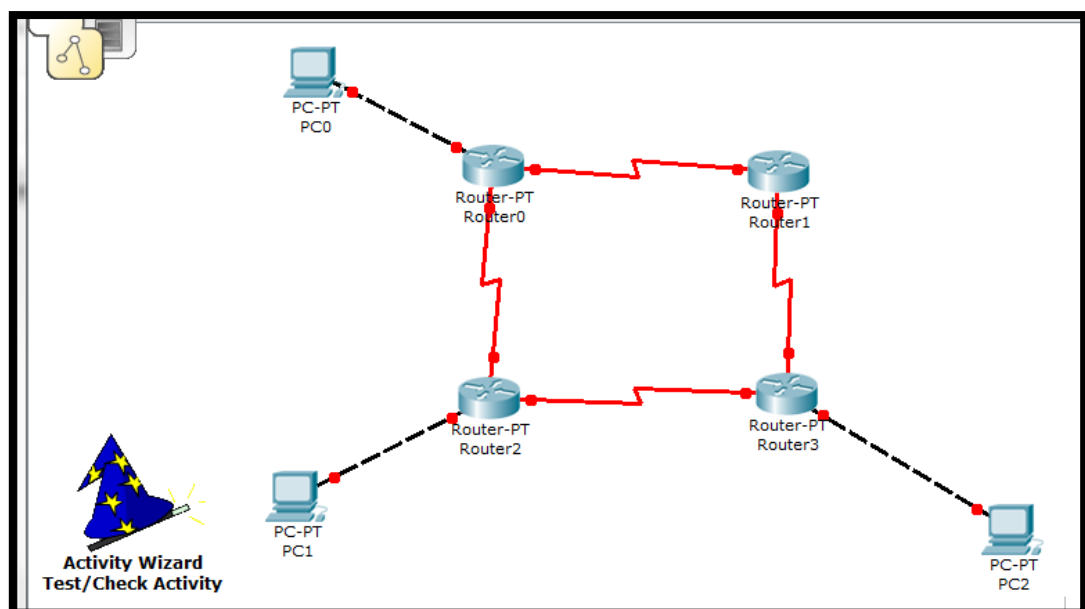
Po vybratí všetkých možností sa presúvame do záložky initial network. Už podľa názvu môžeme vedieť, že v tomto kroku budeme importovať nenakonfigurovanú sieť do simulačného prostredia.

V ďalšom kroku si zvolíme heslo. Aby sme predišli neoprávneným prístupom a zmenám na sieti.

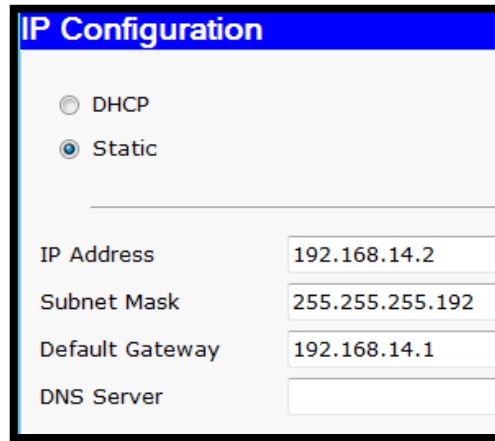


Obr. 78. Záložka na nastavenie hesiel

Po dôkladnom zaheslovaní súbor uložíme a môžeme sa pustiť do konfigurácie. Z nasledujúcej schémy si vyberieme napríklad PC1. Doňho vpíšeme konfiguráciu IP adres.

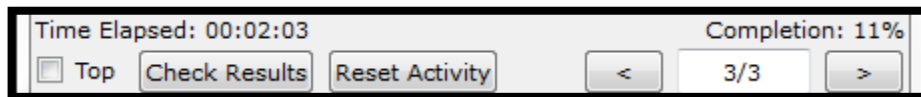


Obr. 79. Nefunkčné zapojenie OSPF



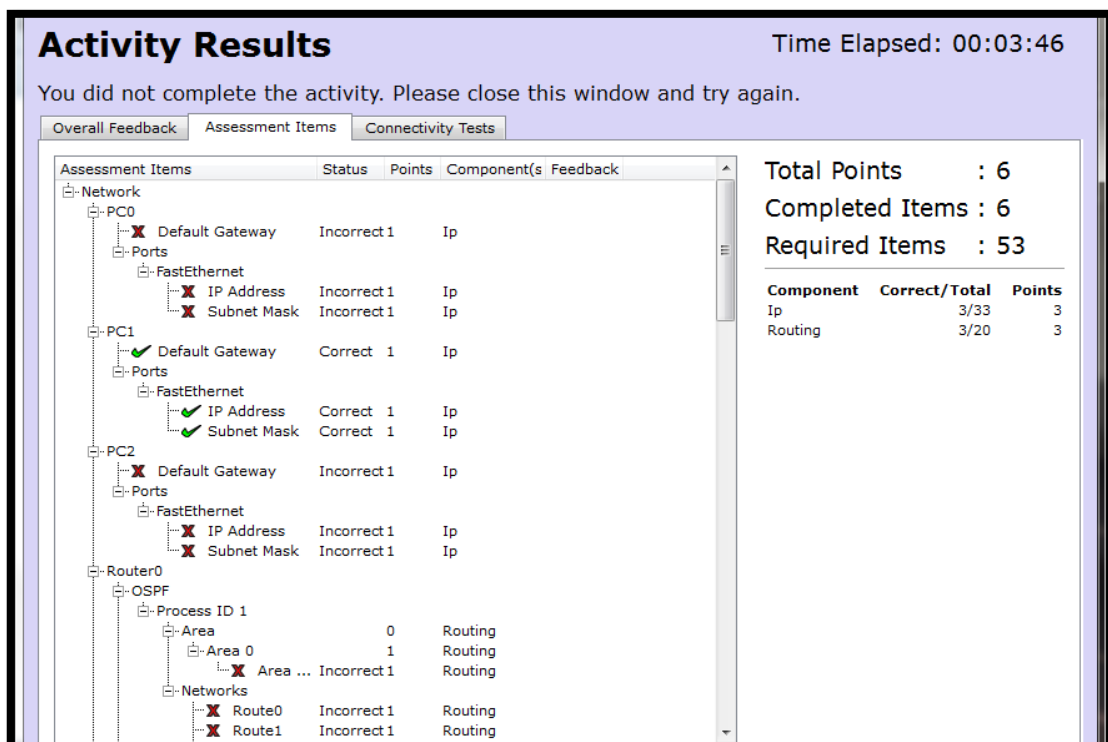
Obr. 80. IP adresácia PC1

Po vypísaní IP adresy sa nám vypíše na koľko percent je sieť nakonfigurovaná.



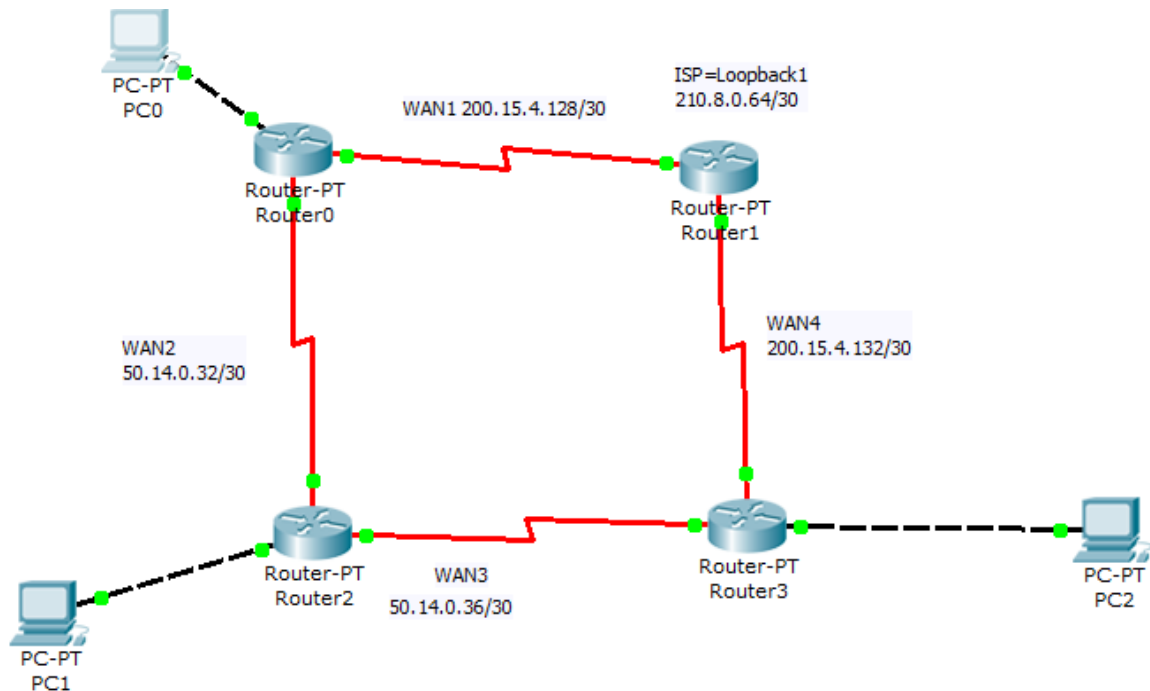
Obr. 81. Percentuálny stav

V záložke Activity Results nám posúdi položky. Zelenou fajkou nám označuje nakonfigurované Ip adresy a červeným krížikom označujeme nedoplnené informácie.



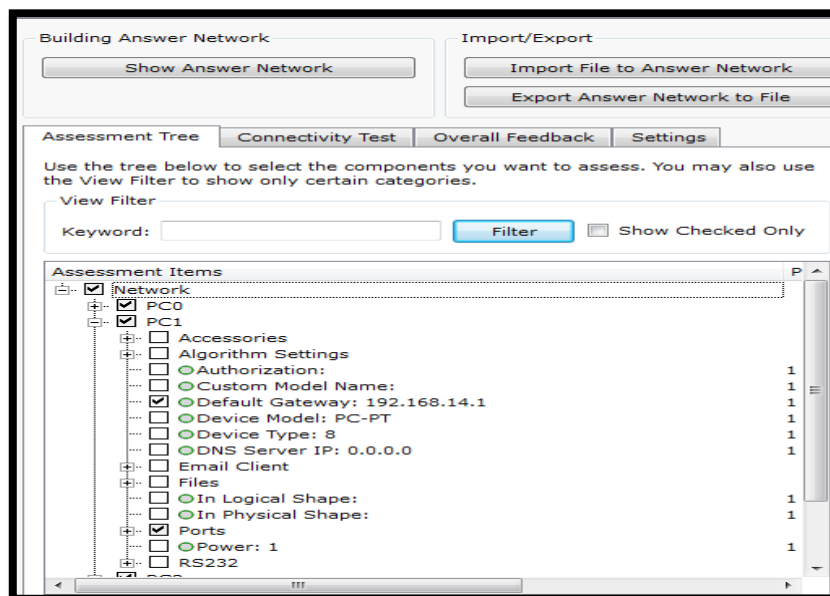
Obr. 82 Vyhodnocovacia tabuľka

V momente keď, bude všetko nakonfigurované (100%), porty budú svietiť na zeleno.

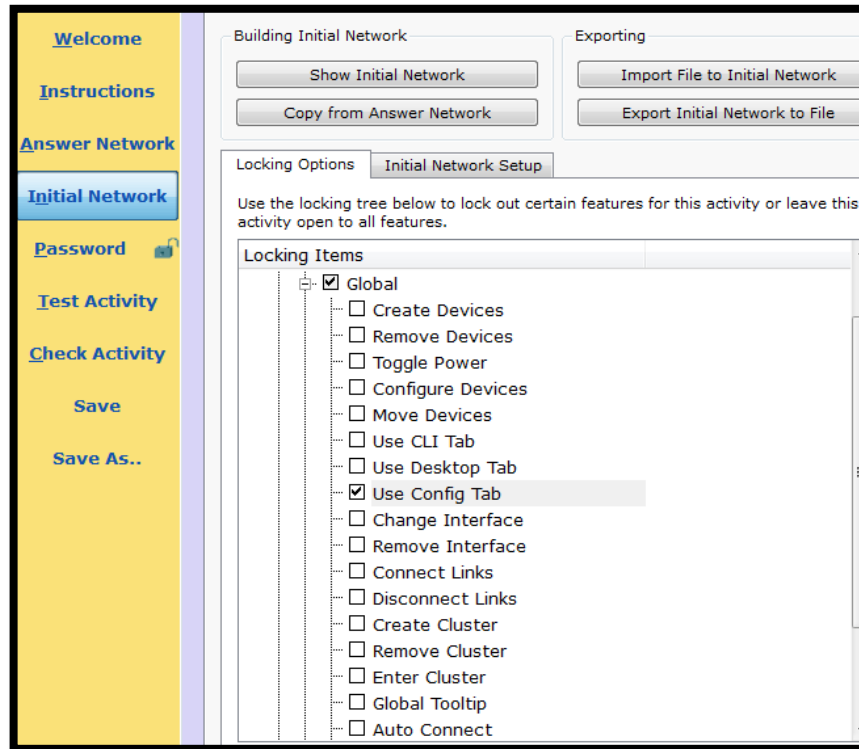


Obr. 83. Funkčné zapojenie siete OSPF

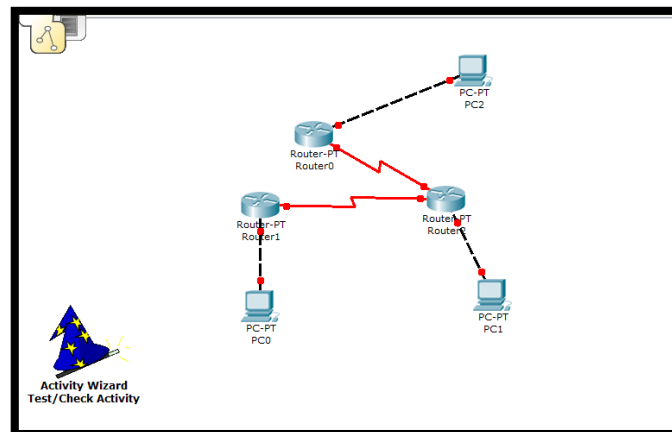
Druhá úloha bola zameraná na protokol RIP. Všetky kroky sú takmer rovnaké. Je len na nás aké hodnoty nastavíme. Postup je predchádzajúci ako v predošlej úlohe. Môžeme napríklad zameniť pridanú hodnotu bodov k IP adresám.



Obr. 84. Vyhodnocovacia tabuľka



Obr. 85. Záložka Initial Network



Obr. 86. Výsledná sieť

## ZÁVĚR

Cieľom bakalárskej práce bolo vytvorenie sadu úloh, pomocou dynamických a smerovacích protokolov. Tieto zapojenia sme vytvárali v programe Cisco Packet Tracer od spoločnosti Cisco.

Aby sme pochopili, ako sieť funguje, ako je rozdelená a aké zariadenia v nej pracujú, bolo dôležité oboznámiť sa s teoretickými informáciami, ktoré sú popísané v teoretickej časti práce. Postupne sme sa zoznámili so súčasťami počítačových sietí (aktívnymi a pasívnymi) s ktorými sa môžeme v sieti stretnúť. V ďalšej časti sme prebrali delenie počítačových sietí podľa ich rozľahlosti a topológie. Dôležitou časťou bola adresácia počítačových sietí, kde sme si vysvetlili ako sa s IP adresami pracujeme. Najdôležitejšou časťou bolo smerovanie a popis jednotlivých protokolov. K pochopeniu dynamického smerovania bol vysvetlený Dijkstrov algoritmus. V práci sme opisovali RIP protokol ktorý patrí do skupiny s vektorom vzdialenosti. Protokol OSPF patrí do skupiny so stavom linky a EIGRP má vlastnosti z obidvoch skupín. V poslednej časti sme popísali činnosť ACL listov, ktoré sú štandardné, alebo rozšírené a slúžia na filtrovanie siete.

Celá praktická časť sa spracovala v simulačnom prostredí Cisco Packet Tracer. V tomto prostredí sa vyskúšali rôzne protokoly a príkazy, ktoré sa používajú v reálnej praxi. Hneď zo začiatku praktickej časti je vysvetlené prostredie programu, ako funguje. Ďalšie v poradí sú vytvorené úlohy. Prvé zapojenie je najjednoduchšie. Jedná sa o základnú konfiguráciu smerovača. Druhé v poradí bolo zapojenie RIPv1 a po tejto úlohe nasledovala úloha s protokolom RIPv2 a výhodou tohto zapojenia je možnosť variabilného podsieťovania. Ako ďalší, sme použili protokol OSPF. Do tejto konfigurácie sa uvádzali aj ACL listy, pomocou ktorých môže správca siete zakázať a povoliť prístup. Posledná časť je tvorená dvoma automatickými vyhodnocovacími úlohami, kde je popísaný postup vytvárania daných úloh.

**SEZNAM POUŽITÉ LITERATURY**

- [1] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
- [2] KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě a jejich aplikace: LAN / MAN / WAN*. 2. aktualiz. vyd. Praha: Grada, 2003. ISBN 80-247-0545-1.
- [3] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.
- [4] LAMMLE, Todd. *CCNA: výukový průvodce*. Překlad Jakub Goner. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [5] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Brno: Computer Press, 2009. Samostudium. ISBN 978-80-251-2520-5.
- [6] EIGRP. *Cisco Networking academy* [online]. [cit. 2016-05-27]. Dostupné z: <http://cisco-academy.aspone.cz/eigrp.html>.
- [7] BUTELA, Michal a Lukáš HÝBNER. *Technologie sítí WAN* [online]. [cit. 2016-05-15].
- [8] ACL- access control list. *Http://www.samuraj-cz.com/* [online]. [cit. 2016-05-15]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/>
- [9] Zabezpečenie pomocou Access list. *THREATED CASE of STUDY (TCS)* [online]. 2003 [cit. 2016-05-17]. Dostupné z: <http://www.nacestach.sk/pg/ja/cisco/acl.htm>.
- [10] VOTAVA, Ondrej. *Výukový a testovací modul na číslování počítačových sítí* [online]. [cit. 2016-05-19]. Dostupné z: [http://data.cedupoint.cz/oppa\\_e-learning/1\\_STM/25.pdf](http://data.cedupoint.cz/oppa_e-learning/1_STM/25.pdf). Počítačové siete. ČVUT v Praze, FEL.
- [11] Zabezpečenie pomocou IGRP. *THREATED CASE of STUDY (TCS) Desert View* [online]. 2003 [cit. 2016-05-14]. Dostupné z: <http://www.nacestach.sk/pg/ja/cisco/igrp.htm>.
- [12] Palo. *Úvod do škálovania sietí a smerovania* [online]. , 155 [cit. 2016-05-30]. Dostupné z: <http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccnp-route-v6/BSCI%20M3-v2.pdf>.
- [13] Cisco Routing 3 - OSPF - Open Shortest Path First. *Samuraj* [online]. [cit. 2016-05-24]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-routing-3-ospf-open-shortest-path-first/>.

- [14] Cisco IOS 8 - ACL - Access Control List. *Samuraj* [online]. 2009 [cit. 2016-05-25]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/>.
- [15] TCP/IP - Routing - směrování. *Samuraj* [online]. 2007 [cit. 2016-05-26]. Dostupné z: <http://www.samuraj-cz.com/clanek/tcpip-routing-smerovani/>.
- [16] ŠVAMBERG, Marek. *Současné routovací protokoly* [online]. 2014 [cit. 2016-05-30] Dostupné z: [https://otik.uk.zcu.cz/bitstream/handle/11025/15288/BP\\_Marek\\_Svamberg.pdf?sequence=1](https://otik.uk.zcu.cz/bitstream/handle/11025/15288/BP_Marek_Svamberg.pdf?sequence=1). Západočeská Univerzita v Plzni. Vedoucí práce Ing. Jan Broulím.
- [17] KRČMÁRIK, Petr. *Animace směrování v IP sítích* [online]. Brno, 2012 [cit. 2016-05-18]. Dostupné z: [https://is.muni.cz/th/359259/fi\\_b\\_a2/Animace\\_smerovani\\_v\\_IP\\_sitich.pdf](https://is.muni.cz/th/359259/fi_b_a2/Animace_smerovani_v_IP_sitich.pdf). BAKALÁŘSKÁ PRÁCE. Masarykova Univerzita. Vedoucí práce Doc. RNDr. Eva Hladká, Ph.D.
- [18] Počítačové siete. *Wick* [online]. 2005 [cit. 2016-05-22]. Dostupné z: <http://wick.wz.cz/pc/zaklady%20siti.htm>.
- [19] Networking Hardware | IGCSE ICT. *Igcseict* [online]. [cit. 2016-05-29]. Dostupné z: <http://www.igcseict.info/theory/4/hware/>.
- [20] Počítačové siete: Paket vs. rámeček. *Boucpe* [online]. [cit. 2016-05-20]. Dostupné z: <http://boucpe.wz.cz/et3/psi3.pdf>.
- [21] Cisco Networking academy. *Cisco-academy* [online]. 2008 [cit. 2016-05-19]. Dostupné z: <http://cisco-academy.aspone.cz/sietove-media.html>
- [22] VAŠEK, Martin. *Návrh a realizace bezdrátových sítí* [online]. 2009 [cit. 2016-05-30]. Dostupné z: [http://digilib.k.utb.cz/bitstream/handle/10563/10793/va%C5%A1ek\\_2009\\_bp.pdf?sequence=1](http://digilib.k.utb.cz/bitstream/handle/10563/10793/va%C5%A1ek_2009_bp.pdf?sequence=1). Bakalářská práce. UTB. Vedoucí práce Doc.Mgr.Milan Adámek, Ph.D.
- [23] Počítačové sítě a jejich typy: Local Area Network - LAN. *Samuraj* [online]. 2007 [cit. 2016-05-23]. Dostupné z: <http://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/>.
- [24] TCP/IP - adresy, masky, subnety a výpočty: IP adresa - IP address. *Samuraj* [online]. 2008 [cit. 2016-05-18]. Dostupné z: <http://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/>.

- [25] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.
- [26] *Access Control Lists (ACL): Použití ACL na Cisco IOS* [online]. [cit. 2016-05-18]. Dostupné z: <http://www.cs.vsb.cz/grygarek/PS/lect/bezpec-nost.pdf>.
- [27] Co je network a subnet (sít' a podsít'): Maska podsítě - Subnet mask. *Samuraj* [online]. 2008 [cit. 2016-05-26]. Dostupné z: <http://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/>.
- [28] PAULOVÁ, Martina. *NÁVRH POČÍTAČOVÉ SÍŤE PRO RODINNÝ DŮM* [online]. Brno, 2014 [cit. 2016-05-21]. Dostupné z: [https://www.vutbr.cz/www\\_base/zav\\_prace\\_soubor\\_verejne.php?file\\_id=85081](https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=85081). Vysoké učení technické. Vedoucí práce Ing. VIKTOR ONDRÁK, Ph.D.
- [29] Cisco Routing 1 - obecné vlastnosti směrovacích protokolů: Dělení routovacích protokolů. *Samuraj* [online]. 2009 [cit. 2016-05-28]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-routing-1-obecne-vlastnosti-smerovacich-protokolu/>.
- [30] *LOKÁLNE SIETE: Topológia lokálnych sietí* [online]. [cit. 2016-05-27]. Dostupné z: <http://ap.urpi.fei.stuba.sk/pkom/html/kapitola3.htm>.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

AS	Autonomous system
RIP	Routing Information Protocol
IGRP	Interior Gateway Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
BGP	Border Gateway protokol
LSA	Link-state advertisement
IP	Internet Protocol
HW	Hardware
L1	Physical Layer
L2	Data Link Layer
PC	Computer
LAN	Local Area Network
VLSM	Variable Length Subnet Masking
RTP	Real-time Transport Protocol
CIDR	Classless Inter-Domain Routing
UDP	User Datagram Protocol
CDP	Cisco Discovery Protocol
CMP	Connectivity Management Processor
IMP	Interface Message Processor
Arpanet	Advanced Research Projects
NVRAM	Non-Volatile Random access Memory

## SEZNAM OBRÁZKŮ

<i>Obr. 1. Symetria krútenej dvojlinky [28]</i> .....	12
<i>Obr. 2. Zloženie UTB kábla [28]</i> .....	13
<i>Obr. 3. Zloženie STP káblu [6]</i> .....	13
<i>Obr. 4. Ukážka STP a FTP kábla [28]</i> .....	14
<i>Obr. 5. Zloženie optického kábla [20]</i> .....	15
<i>Obr. 6. Zapojenie opakovača v praxi [20]</i> .....	15
<i>Obr. 7. Porty prevodníka [20]</i> .....	16
<i>Obr. 8. Zapojenie rozbočovača [20]</i> .....	16
<i>Obr. 9. Premosťovanie siete pomocou mosta [1]</i> .....	17
<i>Obr. 10. Zariadenie switch [20]</i> .....	17
<i>Obr. 11. Spojenie dvoch sietí pomocou smerovača [19]</i> .....	18
<i>Obr. 12. Zapojenie kruhovej topológie [30]</i> .....	21
<i>Obr. 13. Zapojenie zbernicovej topológie [30]</i> .....	22
<i>Obr. 14. Zapojenie hviezdicovej topológie [30]</i> .....	22
<i>Obr. 15. Binárna sústava IP adresy [27]</i> .....	23
<i>Obr. 16. Rozdelenie IP adresy [10]</i> .....	23
<i>Obr. 17. Smerovanie pomocou routra [20]</i> .....	27
<i>Obr. 18. Delenie protokolov [29]</i> .....	29
<i>Obr. 19. Princíp aplikovania ACL [7]</i> .....	37
<i>Obr. 20. Definícia základného ACL [7]</i> .....	38
<i>Obr. 21. Príklad rozšíreného ACL [7]</i> .....	38
<i>Obr. 22. Umiestnenie ACL [7]</i> .....	40
<i>Obr. 23. Cisco packet tracer 5.0</i> .....	43
<i>Obr. 24. Uživatelské prostredie programu</i> .....	44
<i>Obr. 25: Overovacia obálka</i> .....	44
<i>Obr. 26. Aktívne zariadenia a druhy pripojenia</i> .....	45
<i>Obr. 27. Grafické prostredie smerovača v záložke Config</i> .....	46
<i>Obr. 28. Grafické prostredie smerovača v záložke Physical</i> .....	47
<i>Obr. 29. Zapojenie smerovača</i> .....	48
<i>Obr. 30. Výpis príkazu show ip route</i> .....	50
<i>Obr. 31. Funkčné zapojenie siete</i> .....	50
<i>Obr. 32. Ukážkové zapojenie RIPv1</i> .....	51

<i>Obr. 33. Tabuľka rozhraní smerovača Router1</i> .....	53
<i>Obr. 34. Tabuľka rozhraní smerovača Router0</i> .....	53
<i>Obr. 35. Tabuľka protokolu RIP</i> .....	53
<i>Obr. 36. Smerovacia tabuľka smerovača Router0</i> .....	54
<i>Obr. 37. Smerovacia tabuľka smerovača Router1</i> .....	54
<i>Obr. 38. Nakonfigurované a spustené zapojenie</i> .....	54
<i>Obr. 39. Funkčnosť zapojenia</i> .....	54
<i>Obr. 40. Ukázkové zapojenie RIPv2</i> .....	55
<i>Obr. 41. Tabuľka na overenie portov</i> .....	57
<i>Obr. 42. Tabuľka protokolu RIPv2</i> .....	58
<i>Obr. 43. Smerovacia tabuľka</i> .....	58
<i>Obr. 44. Príkaz PING na vyskúšanie zapojenia</i> .....	59
<i>Obr. 45. Ukázkové zapojenie EIGRP</i> .....	60
<i>Obr. 46. Tabuľka susedov na smerovači Zlín</i> .....	62
<i>Obr. 47. Tabuľka susedov na smerovači Zlín</i> .....	63
<i>Obr. 48. Smerovacia tabuľka smerovača Zlín</i> .....	63
<i>Obr. 49. Tabuľka o protokole EIGRP na smerovači Zlín</i> .....	64
<i>Obr. 50. Topologická tabuľka smerovača Zlín</i> .....	64
<i>Obr. 51. Tabuľka rozhraní na smerovači Zlín</i> .....	65
<i>Obr. 52. Nakonfigurované a spustené zapojenie</i> .....	65
<i>Obr. 53. Ukázkové zapojenie OSPF</i> .....	66
<i>Obr. 54. Tabuľka o protokole OSPF na smerovači Router1</i> .....	67
<i>Obr. 55. Susedia na smerovači Router1</i> .....	68
<i>Obr. 56. Stavy rozhraní na Router1</i> .....	68
<i>Obr. 57. Smerovacia tabuľka na smerovači Router1</i> .....	68
<i>Obr. 58. Výpis seriálového portu 2/0 na smerovači Router1</i> .....	69
<i>Obr. 59. Nakonfigurovaná a spustená sieť</i> .....	69
<i>Obr. 60. Ukázkové zapojenie siete</i> .....	70
<i>Obr. 61. Overenie protokolu OSPF na smerovači Router0 (BA1)</i> .....	72
<i>Obr. 62. Susedné porty na smerovači Router0 (BA1)</i> .....	72
<i>Obr. 63. Stav rozhraní na smerovači Router0 (BA1)</i> .....	73
<i>Obr. 64. Smerovacia tabuľka na smerovači Router0 (BA1)</i> .....	73
<i>Obr. 65. Overenie protokolu OSPF na sériovom porte3/0</i> .....	74

---

<i>Obr. 66. Štandardný ACL</i> .....	76
<i>Obr. 67. Štandardný ACL</i> .....	76
<i>Obr. 68. Rozšírený ACL</i> .....	77
<i>Obr. 69. Rozšírený ACL</i> .....	77
<i>Obr. 70. Ukážka zakázania a povolenia ACL</i> .....	77
<i>Obr. 71. ACL listy na smerovači Router0(BA1)</i> .....	78
<i>Obr. 72. Informácie o ACL</i> .....	78
<i>Obr. 73. Nakonfigurovaná a spustená sieť</i> .....	79
<i>Obr. 74. Spustenie Activity Wizard</i> .....	80
<i>Obr. 75. Spustenie Activity Wizard</i> .....	80
<i>Obr. 76. Záložka Answer Network a aktívne zariadenia v sieti</i> .....	81
<i>Obr. 77. Záložka Answer Network</i> .....	81
<i>Obr. 78. Záložka na nastavenie hesiel</i> .....	82
<i>Obr. 79. Nefunkčné zapojenie OSPF</i> .....	82
<i>Obr. 80. IP adresácia PCI</i> .....	83
<i>Obr. 81. Percentuálny stav</i> .....	83
<i>Obr. 82. Vyhodnocovacia tabuľka</i> .....	83
<i>Obr. 83. Funkčné zapojenie siete OSPF</i> .....	84
<i>Obr. 84. Vyhodnocovacia tabuľka</i> .....	84
<i>Obr. 85. Záložka Initial Network</i> .....	85
<i>Obr. 86. Výsledná sieť</i> .....	85

**SEZNAM TABULEK**

<i>Tab. 1. Hodnoty jednotlivých oktétov pre masku</i> .....	24
<i>Tab. 2. Adresný priestor A,B,C</i> .....	25
<i>Tab. 3. Skrátený zápis masky</i> .....	25
<i>Tab. 4. Premena masky na jej skrátenú hodnotu</i> .....	26
<i>Tab. 5: IP adresy pre rozhranie smerovačov a PC zariadení</i> .....	48
<i>Tab. 6: IP adresy pre rozhranie smerovačov a PC zariadení</i> .....	51
<i>Tab. 7: IP adresy pre rozhranie smerovačov a PC zariadení</i> .....	55
<i>Tab. 8: IP adresy pre rozhranie smerovačov a PC zariadení</i> .....	60
<i>Tab. 9: IP adresy pre rozhranie smerovačov a PC zariadení</i> .....	66
<i>Tab. 10: IP adresy pre rozhranie smerovačov a PC zariadení</i> .....	71

## SEZNAM PŘÍLOH

Príloha P I: CD s nakonfigurovanými úlohami

## **PŘÍLOHA P I: NÁZEV PŘÍLOHY**

Na CD sa nachádzajú nakonfigurované jednotlivé siete.