

# **Tvorba a úprava studijních materiálů pro kurz CCNA2**

Creation and editing of educational materials for course CCNA2

Ivan Sedlák

---

Bakalářská práce  
2010



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2009/2010

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Ivan SEDLÁK**

Osobní číslo: **A07090**

Studijní program: **B 3902 Inženýrská informatika**

Studijní obor: **Informační a řídicí technologie**

Téma práce: **Tvorba a úprava studijních materiálů pro kurz CCNA 2**

Zásady pro vypracování:

1. Zpracování charakteristiky kurzu po obsahové stránce.
2. Vypracování českých studijních materiálů v MS Word.
3. Příprava prezentací pro přednášky kurzu v MS PowerPoint.
4. Vytvoření ukázkových příkladů v programu Packet Tracer.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ODOM, Wendell, MCDONALD, Rick. Routers and Routing Basics: CCNA2 Companion Guide. Indianapolis : Cisco Press, 2007. 473 s. ISBN 1-58713-166-8.**
2. **Cisco Systems. Cisco Networking Academy : CCNA 2 Curriculum [online]. c2007 [cit. 2010-01-22]. Dostupný z WWW: <http://cisco.netacad.net/>.**
3. **PECINOVSKÝ, Josef. Microsoft PowerPoint 2007: hotová řešení. Brno : Computer Press, 2008. 240 s. ISBN 978-80-251-2123-8.**
4. **PIERCE, John. Mistrovství v Microsoft Office 2007. Brno : Computer Press, 2008. 1120 s. ISBN 978-80-251-2066-8.**
5. **BIGELOW, Stephen J. Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů. 1. vyd. Brno : Computer Press, 2004. 990 s. ISBN 8025101789.**

Vedoucí bakalářské práce:

**Ing. Jiří Korbel**

Ústav počítačových a komunikačních systémů


Datum zadání bakalářské práce:

**5. března 2010**

Termín odevzdání bakalářské práce:

**1. června 2010**

Ve Zlíně dne 5. března 2010

  
prof. Ing. Vladimír Vašek, CSc.  
*děkan*



  
doc. Ing. Ivan Zelinka, Ph.D.  
*ředitel ústavu*

## **ABSTRAKT**

Bakalárska práca opisuje tému smerovania v počítačových sieťach, ktoré je základom pre počítačové siete. Základom bakalárskej práce je statické a dynamické smerovanie, ktoré sa delí na ďalšie podkapitoly. Taktiež predmetom tejto práce je router, ktorý je hlavnou súčasťou smerovania. Praktická časť bakalárskej práce obsahuje výukové materiály pre kurz Cisco CCNA2 Exploration: Smerovacie protokoly a pojmy.

Kľúčové slová: statické smerovanie, dynamické smerovanie, smerovacie protokoly, RIP, RIPv2, VLSM, CIDR, EIGRP, OSPF, IS-IS

## **ABSTRACT**

Bachelor thesis topic describes routing in computer networks, which is the basic for computer networks. Basic of this work are static and dynamic routing, which is divided into subchapters. Also the subject of this work is a router, which is a major part of routing. The practical part of the bachelor thesis contains teaching materials for Cisco CCNA2 Exploration: Routing Protocols and Concepts.

Keywords: static routing, dynamic routing, routing protocols, RIP, RIPv2, VLSM, CIDR, EIGRP, OSPF, IS-IS

Chcel by som sa poďakovať Ing. Jířimu Korbelovi za konzultácie pre tvorbu tejto bakalárskej práce.

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 STATICKÉ SMEROVANIE</b> .....	<b>11</b>
1.1 ÚVOD .....	11
1.2 VÝHODY STATICKÉHO SMEROVANIA .....	11
1.3 NEVÝHODY STATICKÉHO SMEROVANIA .....	11
1.4 PRINCÍP STATICKÉHO SMEROVANIA .....	11
1.5 SMEROVANIE IP PAKETU .....	12
1.5.1 Zoznam polí .....	12
1.6 PREDÁVANIE PAKETU .....	13
1.7 KONFIGURÁCIA .....	15
1.7.1 Konfigurácia sériového rozhrania .....	15
1.7.1.1 Vykonávanie adds, presun a zmeny .....	15
1.7.2 Konfigurácia Ethernetového rozhrania .....	16
<b>2 DYNAMICKÉ SMEROVANIE</b> .....	<b>17</b>
2.1 VÝHODY DYNAMICKÉHO SMEROVANIA .....	18
2.2 NEVÝHODY DYNAMICKÉHO SMEROVANIA .....	18
2.3 RIPv1 .....	19
2.3.1 Úvod .....	19
2.3.2 Vlastnosti a formát zprávy .....	19
2.3.3 Konfigurácia RIPv1 .....	21
2.4 RIPv2 .....	22
2.4.1 Úvod .....	22
2.4.2 Vlastnosti .....	23
2.4.3 Konfigurácia RIPv2 .....	23
2.5 OSPF .....	24
2.5.1 Úvod .....	24
2.5.2 Konfigurácia OSPF .....	25
2.5.3 Funkcie OSPF .....	26
2.5.4 Výhoda OSPF .....	27
2.6 IS-IS .....	27
2.6.1 Vlastnosti IS-IS .....	27
2.7 EIGRP .....	29
2.7.1 Koncept a terminológia .....	29
2.7.2 Technológia .....	29
2.7.3 Konfigurácia .....	30
<b>ZÁVER</b> .....	<b>32</b>
<b>CONCLUSION</b> .....	<b>33</b>

<b>ZOZNAM POUŽITEJ LITERATÚRY .....</b>	<b>34</b>
<b>ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....</b>	<b>35</b>
<b>ZOZNAM OBRÁZKOV .....</b>	<b>36</b>
<b>ZOZNAM PRÍLOH .....</b>	<b>37</b>



## ÚVOD

Všade okolo nás sú počítačové siete, či už je to v škole, podnikoch, domácnostiach alebo na úradoch. Stretávame sa s nimi skoro každý deň a každý o nich vie. Ale málokto vie o tom ako to všetko funguje, čo sa vlastne odohráva v jednotlivých zariadeniach. Napr. taký router (smerovač) je využitý skoro v každej počítačovej sieti. Väčšina ľudí, prevažne mladých pozná toto zariadenie. Internetový poskytovatelia dávajú možnosť zakúpiť si u nich tento router. To využívajú najmä zákazníci, ktorí majú v domácnosti dva alebo viac počítačov. Router pre bežného zákazníka rozdeľuje internetové pripojenie na viac počítačov. Existujú aj takzvané wi-fi routery, ktoré sa dajú štandardne pripojiť sieťovým káblom, ale ich hlavná výhoda je, že prenášajú signál bezdrôtovo. Čo v dnešnej dobe využívajú hlavne prenosné počítače – notebooky. Môžeme sa tak pripojiť hocikde, kde je wi-fi signál, či už vo firme, škole alebo niekde v kaviarni, ale to už nie je téma tejto práce.

Cieľom tejto práce je oboznámenie toho ako to vlastne funguje v routery. Ako, kde a akým spôsobom sa posielajú údaje do jednotlivých počítačov. To všetko je cieľom tejto bakalárskej práce, čo je popísané v teoretickej časti. Podrobnejší popis, následné úlohy a konfigurácie sú v praktickej časti v jednotlivých kapitolách, ktoré sú v prílohe na CD.

## I. TEORETICKÁ ČÁST

# 1 STATICKÉ SMEROVANIE

## 1.1 Úvod

Smerovanie je jadrom každej dátovej siete, pohybovanie informácie cez Internetwork od zdroja k cieľu. Routery sú zariadenia, zodpovedné za prenos paketov z jednej siete do druhej.

Routery študujú vzdialené siete buď dynamicky pomocou smerovacích protokolov, alebo ručne pomocou statických ciest. V mnohých prípadoch routery používajú kombináciu oboch, dynamických smerovacích protokolov a statických ciest.

## 1.2 Výhody statického smerovania

- Minimálna záťaž na CPU a pamäť smerovača
- Vyššia úroveň bezpečnosti – smerovače neposielajú ani neprijímajú žiadne smerovacie informácie
- Vysoká úroveň kontroly – vždy sa vie akou cestou sú pakety v sieti prenášané
- Sú veľmi časté a nevyžadujú rovnaké množstvo spracovania ako dynamické protokoly

## 1.3 Nevýhody statického smerovania

- Pri väčších sieťach je problém s administrovaním statických ciest
- Statické cesty sa nedokážu prispôbiť zmenám v typológii siete
- Je vhodné len pre veľmi jednoduché siete

## 1.4 Princíp statického smerovania

Každý router musí urobiť rozhodnutie o smerovaní paketu sám, na základe svojej vlastnej smerovacej tabuľky. Skutočnosť, že jeden router má určité informácie vo svojej smerovacej

tabuľke neznamena, že ostatné routery majú tie isté informácie. Smerovacie informácie o ceste z jednej siete do druhej neposkytujú informácie o spätnej, návratovej ceste.

## 1.5 Smerovanie IP paketu

Routery vykonávajú rozhodovanie na základe skúmania cieľovej IP adresy paketu. Pred tým, než je paket vyslaný na správne rozhranie routeru, je potrebné paket zabaliť do správneho rámca druhej a to dátovej vrstvy OSI modelu. Internet protokol špecifikuje v RFC 791 ako má vyzerat' formát IP paketu. IP hlavička má špecifické polia, ktoré obsahujú informácie týkajúce sa paketu a ohľadom hostí, ktorí spolu chcú komunikovať. Nasleduje zoznam všetkých polí s krátkym popisom. Medzi najdôležitejšie polia patrí cieľová a zdrojová IP adresa, verzia, TTL (Time To Live).

Byte 1	Byte 2	Byte 3	Byte 4
Vers.	IHL	Service Type	Packet Length
Identification		Flag	Frag. Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

Obr. 1. Formát IP paketu

### 1.5.1 Zoznam polí

**Verzia** – číslo verzie (4 bity), dominantnou verziou je stále IPv4

**Dĺžka IP hlavičky** – 32 bitov

**Priorita a typ služby** - určuje, ako bude sa paketom zaobchádzať, prvé 3 bity určujú prioritu, boli postupne nahradené Differentiated Services Code Point [DSCP], ktorá používa 6 bitov (2 sú rezervné)

**Dĺžka paketu** - celková dĺžka (hlavička + dáta) (16 bitov)

**Identifikácia** - Unikátna hodnota IP datagramu (16 bitov)

**Flags** - kontrolujú fragmentáciu

**Fragmentová kompenzácia (Fragment offset)** - podporuje fragmentáciu datagramov, vďaka tomu umožňuje rozdielne veľkosti maximum transmission

**Time - To - Live** - Identifikuje koľko ciest môže paket prejsť kým nie je zahodený (8 bitov)

**Protokol** - protokol vyšších vrstiev, ktorý vyslal diagram (8 bitov)

**Kontrolný súčet hlavičky (Header checksum)**

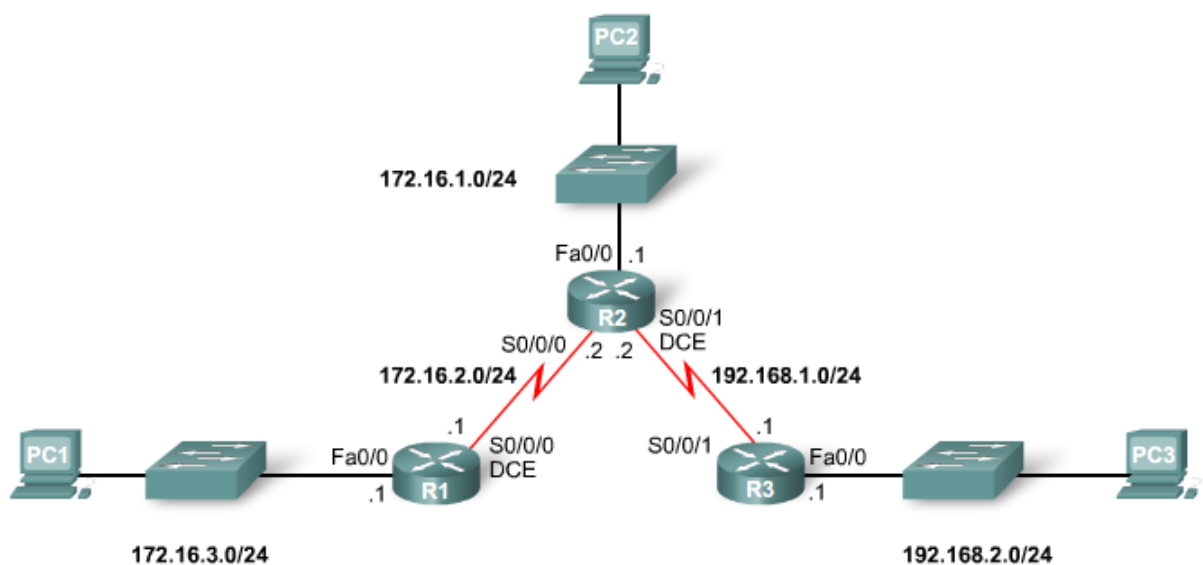
**Zdrojová IP adresa** - 32-bitová IP adresa

**Cieľová IP adresa** - 32-bitová IP adresa

**IP voľby (IP options)** - testovanie siete, debugging (ladenie), bezpečnosť a ďalšie - 0 - 32 bitov

**Padding** – Patička

## 1.6 Predávanie paketu



Obr. 2. Topológia

1. Paket príde na rozhranie FastEthernet 0 / 0 routeru R1.

2. R1 nemá konkrétnu cestu do cieľovej siete 192.168.2.0/24, a preto R1 používa predvolenú statickú cestu.

3. R1 zapúzdří paket do nového framu. Pretože spojenie na R2 je point-to-point spojenie,

R1 pridáva "all 1s" adresu pre cieľovú adresu vrstvy 2.

4. Frame je prenášaný preč zo sériového rozhrania 0/0/0. Paket prichádza na sériové rozhranie 0/0/0 na R2.

5. R2 vypúzdri frame a hľadá cestu k cieľu. R2 má statickú cestu do 192.168.2.0/24 preč zo Serial0/0/1.

6. R2 zapúzdri paket do nového framu. Pretože spojenie na R3 je point-to-point spojenie, R2 pridáva "all 1s" adresu pre cieľovú adresu vrstvy 2.

7. Frame je prenášaný z rozhrania Serial0/0/1. Paket prichádza na rozhranie Serial0/0/1 na R3.

8. R3 vypúzdri frame a hľadá cestu k cieľu. R3 má pripojenú cestu do 192.168.2.0/24 preč z FastEthernet 0 / 1.

9. R3 vyhľadá záznam ARP tabuľky pre 192.168.2.10 na nájdenie MAC adresy vrstvy 2 pre PC3.

a. Ak žiadny záznam neexistuje, R3 pošle požiadavku ARP z FastEthernet 0 / 0.

b. PC3 odpovie s ARP odpoveďou, ktorá obsahuje MAC adresu PC3.

10. R3 zapúzdri paket do nového framu s MAC adresou rozhrania FastEthernet 0 / 0 ako zdrojovú adresu vrstvy 2 a MAC adresou PC3 ako cieľovú MAC adresu.

11. Frame je odovzdaný z rozhrania FastEthernet 0 / 0. Paket dorazí na rozhranie NIC na PC3.

## 1.7 Konfigurácia

### 1.7.1 Konfigurácia sériového rozhrania

Môže byť konfigurované cez konzolu alebo cez virtual terminal line. Postup:

1. vstup do globálneho konfiguračného módu
2. vstup do módu rozhrania
3. uviesť adresu pre rozhranie a masku
4. nastaviť clock rate ak ide o DCE
5. zapnúť rozhranie

Každé pripojené sériové rozhranie musí mať IP adresu a masku siete. Príklad:  
Router(config)#interface serial 0/0 Router(config-if)#ip address <ip address> <netmask>  
Sériové rozhranie vyžaduje hodinový signál na kontrolu časovania komunikácie. DCE zariadenie treba nastaviť na nastavenie poskytovania hodinového signálu. **clock rate** – spúšťa časovač a definuje rýchlosť: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, alebo 4000000. **no shutdown** – zapína rozhranie **shutdown** – vypína rozhranie príklad využitia príkazov pri rýchlosti 56000:

```
Router(config)#interface serial 0/0 Router(config-if)#clock rate 56000 Router(config-if)#no shutdown
```

#### 1.7.1.1 *Vykonávanie adds, presun a zmeny*

Ak konfigurácia vyžaduje konfiguráciu, treba prejsť do potrebného módu, napríklad ak potrebujem zapnúť nejaké rozhranie, spustím globálny konfiguračný módu, vstúpim do módu daného rozhrania a spustím ho cez príkaz **no shutdown**. **show running-config** – overenie aktuálnej konfigurácie, je čítaná z RAM  
Postup, ak zmeny nerobia požadované:

1. Zrušenie/zmena konfiguračného príkazu v príslušnom konfiguračnom móde!!!–no príkaz(no ip address, no shutdown)
2. obnovenie konfigurácie z NVRAM
3. skopírovať konfiguráciu cez TFTP

- **erase startup-config** – odstráni spúšťiaciu konfiguráciu z NVRAM, po reštarte prejsť do setup módu **copy running-config startup-config** – uloží bežiacu konfiguráciu do VNRAM

### 1.7.2 Konfigurácia Ethernetového rozhrania

Je možné konfigurovať cez konzolu alebo cez virtual terminal line. Každé Ethernetové rozhranie musí mať IP a masku. Postup konfigurácie:

1. spustiť globálny konfiguračný mód
2. spustiť konfiguračný mód rozhrania
3. špecifikovať IP a masku
4. povoliť rozhranie Rozhranie je prednastavené ako vypnuté, spustíme ho cez **no shutdown**, vypneme cez **shutdown**.



## 2 DYNAMICKÉ SMEROVANIE

Vzdialené siete môžu byť pridané do smerovacej tabuľky použitým dynamického smerovacieho protokolu. Tie slúžia na zdieľanie informácií o dosiahnuteľnosti a stave vzdialených sietí. Vykonávajú niekoľko aktivít ako prieskum siete, či aktualizácie a údržbu smerovacích tabuliek.

### Automatický prieskum siete

Prieskum siete je schopnosť smerovacích protokolov zdieľať informácie týkajúce sa sietí, ktoré už pozná s inými routery, ktoré používajú rovnaký smerovací protokol a sieť nepoznajú. Na rozdiel od toho, aby sme konfigurovali statické cesty na každom routeru, dynamický smerovací protokol umožní, aby si routery navzájom odovzdávali informácie o vzdialených sieťach. Tieto siete sú spolu s najlepšou cestou pridané do smerovacej tabuľky a označené ako siete určené pomocou konkrétneho smerovacieho protokolu.

### Údržba routovacích tabuliek

Po spustení prieskumu siete dynamické smerovacie protokoly aktualizujú a udržiavajú siete v ich smerovacích tabuľkách. Nielen, že stanovujú najlepšiu cestu do rôznych sietí, ale tiež zvolia inú najlepšiu cestu v prípade, že použitá cesta sa stane neaktívna alebo dôjde k zmene topológie. Toto je jedna z drvivých výhod dynamických protokolov oproti použitiu statiky. Všetky tieto zmeny sa dejú automaticky bez potreby zásahu administrátora.

### IP směrovací protokoly

Existuje niekoľko dynamických smerovacích protokolov pre IP pakety.

**RIP** (Routing Information Protocol)

**IGRP** (Interior Gateway Routing Protocol)

**EIGRP** (Enhanced Interior Gateway Routing Protocol)

**OSPF** (Open Shortest Path First)

**IS-IS** (Intermediate System-to-Intermediate System)

**BGP** (Border Gateway Protocol)

	Interior Gateway Protocols		Exterior Gateway Protocols	
	Distance Vector Routing Protocols	Link State Routing Protocols	Path Vector	
Classful	RIP	IGRP	EGP	
Classless	RIPv2	EIGRP	OSPFv2	IS-IS
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6
				BGPv4 for IPv6

Obr. 3. Rozdelenie dynamických protokolov

## 2.1 Výhody dynamického smerovania

- smerovač si vytvorí smerovaciu tabuľku na základe informácií, ktoré si vymieňa s okolitými smerovačmi
- výmena aktuálnych informácií prostredníctvom smerovacích protokolov
- výber najvhodnejšej cesty pre smerovanie na základe rôznych kritérií
- kritériá výberu ( počet smerovačov k cieľu, priepustnosť prenosovej cesty, spoľahlivosť doručenia paketu, zaťaženie prenos.cesty, max.vel'kosť prenášaného paketu – **metrika smerovania**)
- veľká časová i personálna úspora
- okamžitá aktualizácia zmien v sieti
- finančne nákladnejšie, zložitejšie zariadenia, zvýšené odborné znalosti personálu

## 2.2 Nevýhody dynamického smerovania

- Vyššia záťaž na CPU a pamäť smerovača
- Výmeny smerovacích informácií spotrebúvajú kapacitu prenosových liniek
- Nižšia úroveň kontroly nad smerovaním z pohľadu administrátora

- Odporúča sa všade tam, kde statické smerovanie je nedostačujúce – komplexné siete s redundantnými spojmi, ktoré nemôžu tolerovať žiaden, popr. len veľmi krátkodobý výpadok nefunkčnosti

## 2.3 RIPv1

### 2.3.1 Úvod

V priebehu rokov sa smerovacie protokoly vyvinuli, aby uspokojili rastúce požiadavky zložitých sietí. Prvý používaný protokol bol Routing Information Protocol (RIP). RIP má stále popularitu vďaka svojej jednoduchosti a širokej podpore.

Pochopenie RIP je dôležité pre sieťové štúdie z dvoch dôvodov. Po prvé sa RIP používa aj dnes. Môžeme sa stretnúť s implementáciou siete, ktorá je dostatočne veľká a potrebuje smerovací protokol, pre jednoduchosť použijeme efektívne RIP. Po druhé znalosť mnohých základných pojmov RIP vám pomôže porovnať RIP s inými protokolmi. Pochopenie ako funguje RIP a jeho realizácia vám umožní jednoduchšie vzdelávanie ďalších smerovacích protokolov.

### 2.3.2 Vlastnosti a formát zprávy

#### **RIP (RFC 1058):**

- Využíva DVA (distance vector algoritmus), pravidelne posiela smerovaciu tabuľku svojim susedom
- Ako metrika pri výbere cesty sa používa počet skokov (počet smerovačov)
- Aby sa predišlo nekonečným smerovacím slučkám, RIP implementuje maximálny počet dovolených skokov na ceste od zdroja k cieľu. Maximálny počet skokov je 15. Ak smerovač príme aktualizáciu od suseda, ktorá obsahuje novú alebo zmenenú položku, metrika je zvýšená o 1. Ak je táto metrika väčšia ako 15, cieľová sieť je označená ako nedosiahnuteľná.
- RIP podporuje „load balancing“ až cez 6 ciest s rovnakou metriku. Prednastavené je použitie 4 ciest a ich výber sa vykonáva na základe algoritmu „round robin“.
- RIP v1 má nasledujúce obmedzenia:

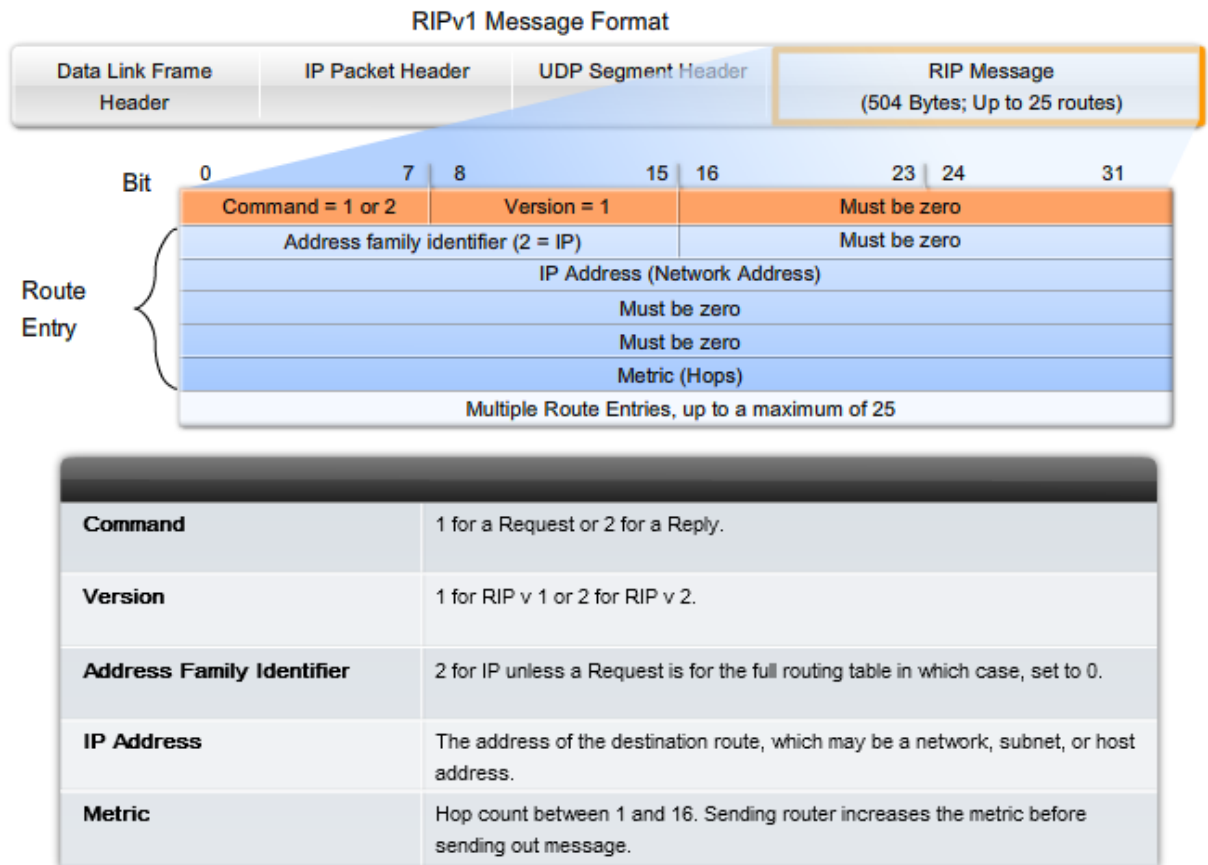
- Classful Routing Protocol
- Vo svojich aktualizáciách neposiela údaj o maske.
- Aktualizácie posiela ako broadcast (255.255.255.255).
- Nepodporuje autentifikáciu
- Nepodporuje VLSM a CIDR

### **Formát správy RIP: Hlavička RIP**

Tri polia sú špecifikované v štyroch bajtoch časti hlavičky. Príkazové pole určuje typ správy. Verzia poľa je nastavená na 1 pre verziu RIP 1. Tretia oblasť je označená must be zero (musí byť nula). Oblasti "Must be zero" poskytujú priestor pre budúce rozšírenie protokolu.

### **Formát správy RIP: Cesta záznamu**

Časť správy cesty záznamu obsahuje tri oblasti s obsahom: Identifikátor adresy rodiny (nastavený na 2 pre IP, ak router požaduje plnú smerovaciu tabuľku, v tomto prípade je pole nastavené na nulu), IP adresa a Metrika. Cesta časti záznamu predstavuje jednu cieľovú cestu s jej spojenou metrikou. Jeden update RIP môže obsahovať viac ako 25 položiek cesty. Maximálna veľkosť diagramu je 504 bajtov, nie vrátane IP alebo UDP hlavičky.



Obr. 4. RIPv1 formát správy

### 2.3.3 Konfigurácia RIPv1

**router rip**, spustenie smerovacieho protokolu RIP.

**network**, povie routru, na ktorom rozhraní beží RIP, definujú sa len pre priamo pripojené siete.

Smerovací proces potom spojí špecifické rozhranie so sieťovou adresou a začne prijímať a vysielat' RIP aktualizácie na toto rozhranie. Keď router prijme smerovacie pakety, ktoré obsahujú nové záznamy, pridá ich do svojej smerovacej tabuľky. Hodnota prijatej metriky pre cestu je zväčšená o 1, na základe tejto hodnoty sa dá určiť počet hopov. RIP route udržiavajú vo svojich smerovacích tabuľkách len najlepšie cesty, ale môžu ich obsahovať aj viac.

**ip rip triggered** príkaz, RIP posielá aktualizácie pri zmene na sieti. Je ho možné nastaviť len pre sériové rozhraní na routri. Po zmene smerovacej tabuľky, hneď začne prenášať zmeny, smerovacie zmeny na iné route.

### Použitie príkazu IP classless

Supernetroute = smer, ktorý pokrýva jednou položkou viacero smerov do podsietí; napr., ak máme podsiete 10.1.33.0/24, 10.1.34.0/24, 10.1.36.0/24, supernet môže byť napr. 10.1.0.0/16, ale aj 10.1.32.0/21 (prvých 21 bitov je u všetkých adries rovnakých) **ip classless**, umožní smerovanie paketov do viacerých sietí, je dostupný od Cisco IOS Software Release 11.3 a neskorších, zadáva sa v GKM, zakázanie je robené cez **no** pred príkazom **IP classless** nemá žiadny vplyv na vybudovanú smerovaciu tabuľku.

### Všeobecné konfiguračné otázky pri RIP

Routre založené na RIP sa musia spoliehať na informácie o sieti z iných routrov. Keďže je založený na vektorovom smerovacom protokole, jeho konvergencia je pomalá.

### Overovanie konfigurácie RIP

Na overovanie RIP je možné použiť niekoľko príkazov. **show ip protocols**, zobrazí smerovacie protokoly Body na overenie funkčnosti:

1. či je RIP nakonfigurovaný
2. či sú na správnych rozhrania prijímané a vysielané RIP aktualizácie
3. aké siete oznamuje

**show ip route**, overenie, či sú v smerovacej tabuľke záznamy získané cez RIP, v smerovacej tabuľke je RIP označené písmenom **R**.

## 2.4 RIPv2

### 2.4.1 Úvod

RIP verzia 2 (RIPv2) je definovaná v RFC 1723. Jedná sa o prvý beztriedny smerovací protokol. Hoci RIPv2 je vhodný smerovací protokol pre určité prostredie, stratil popularitu v porovnaní s inými smerovacími protokolmi, ako sú EIGRP, OSPF a IS-IS, ktoré ponúkajú viac funkcií a sú viac škálovateľné. I keď môže byť menej populárny ako iné smerovacie

protokoly, obe verzie RIP sú ešte vhodné v niektorých situáciách. Hoci RIP chýba schopnosť mnohých novších protokolov, jeho naprostá jednoduchosť a široké využitie v rôznych operačných systémoch ho robí ideálnym kandidátom na menšie, homogénne siete, kde je multi-vendor podpora nevyhnutná - najmä v prostredí UNIX.

#### 2.4.2 Vlastnosti

**RIP v2 vychádza z RIP v1 a obsahuje tieto vylepšenia:**

- Posielanie prídavných smerovacích informácií
- Autentifikačný mechanizmus
- Podpora VLSM

**Obidve verzie RIP majú nasledujúce vlastnosti:**

- DV protokol, ktorý ako metriku používa počet skokov
- Používa „holddown timers“ (180 sekúnd) a „split horizon“ na predchádzanie smerovacích slučiek
- A využívajú 16 skokov ako metriku pre nedosiahnutelnú sieť
- Podporuje posielanie masky siete spolu s aktualizáciou a tým aj VLSM – je to „classless routing protocol“
- Poskytuje autentifikáciu
- RIP v2 informácie posiela cez multicast na adrese 224.0.0.9

#### 2.4.3 Konfigurácia RIPv2

Príkaz router spustí proces smerovania, príkaz network implementuje tri funkcie: Smerovacie updaty sú ako multicast zasielané na zadanom rozhraní. Smerovacie updaty sú spracované, pokiaľ sú prijaté na rovnakom rozhraní. Podsiete priamo pripojené k rozhraniu sú obsiahnuté v ohlásení (advertisements). Príkaz network je nutný, aby bolo možné určiť rozhranie, ktoré sa zúčastňuje odosielania a

prijímania smerovacích aktualizácií. Príkaz spustí smerovací protokol na všetkých rozhraniach, ktoré router v danej sieti má a tiež umožní nahlasovanie tejto siete.

### **Príklad konfigurácie:**

*router rip // aktivuje RIP*

*version 2 // identifikuje, že používame verziu 2*

*network 172.16.0.0 // zadáme priamo pripojenú sieť*

*network 10.0.0.0 // a ďalšiu priamo pripojenú sieť*

Rozhranie routera pripojené k sieťam 172.16.0.0. a 10.0.0.0, prípadne ich podsieťam, budú odosielať a prijímať RIP v2 updaty, ktoré routeru umožnia zistiť topológiu siete. Na ďalších routeroch je nastavenie rovnaké, ale samozrejme vždy uvádzame priamo pripojené siete konkrétneho routera.

## **2.5 OSPF**

### **2.5.1 Úvod**

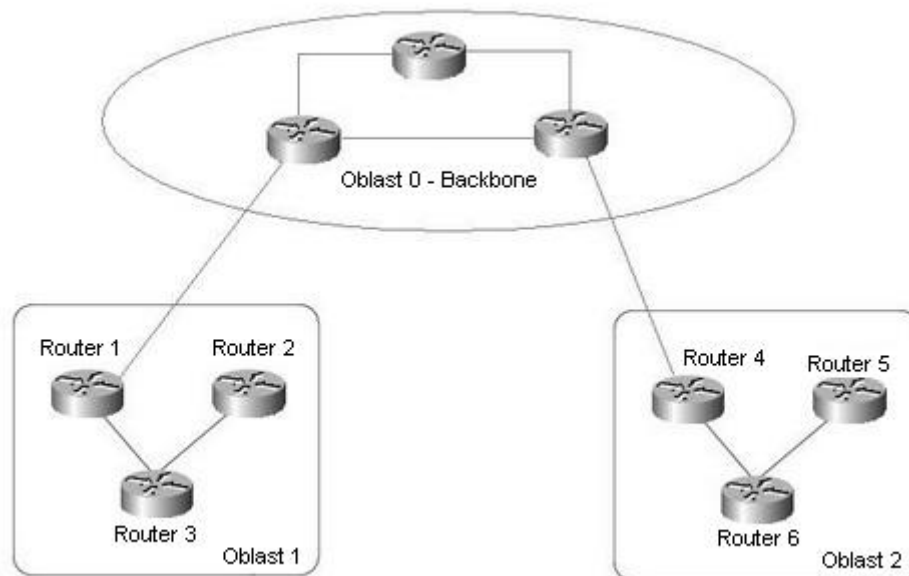
Smerovací protokol OSPF (Open Shortest Path Find) je lepším variantom k protokolu RIP. Bol navrhnutý pre rozsiahlejšie IP siete. Vychádza z algoritmu SPF (Shortest Path Find), prostredníctvom, ktorého každý smerovač v sieti hodnotí najlepšiu cestu paketu k ľubovoľnému uzlu siete. Prostredníctvom správ LSA (Link State Advertisement) vykonáva protokol OSPF kontrolu dostupných smerovačov a kontrolu stavu pripojených liniek. V správach LSA je opísaný stav lokálneho smerovača a liniek vedúcich do susedných smerovačov. Na základe týchto LSA správ sú v každom smerovači siete vytvárané a aktualizované tzv databázy topológie siete OSPF.

Z databázy siete je v každom smerovači vytvorený stromový graf najkratšej cesty paketu v sieti. Strom grafu reprezentuje aktuálny smerovač, ktorý poskytuje informácie nielen o najkratšej ceste paketu, ale aj o najlepšej alternatívnej ceste. Z týchto grafov sú potom následne konštruované vlastné smerovacie tabuľky OSPF. K aktualizáciám prostredníctvom



správ dochádza v periodických časových intervaloch. Neprenáša sa komplexné smerovacie tabuľky, ale len zmeny v stave liniek a čiastkové zmeny, čím sa šetrí prenosová kapacita liniek.

Protokol OSPF rozčleňuje sieť do dvoch hierarchických úrovní: na chrbticovú sieť BA (Back Bone Area) a čiastkové oblasti A (Area). Čiastková oblasť reprezentuje skupinu smerovačov, uzlov s vlastným algoritmom OSP a databáz topológií oblasti. Oblasti sú vzájomne prepojené chrbticou BA, ktorá tvorí samostatnú oblasť pozostávajúca zo skupiny sietí a smerovačov slúžiacie na smerovanie informácií medzi jednotlivými skupinami. Na nasledujúcom obrázku je vidieť topológiu siete OSPF.



Obr. 5. Topológia OSPF

### 2.5.2 Konfigurácia OSPF

OSPF smerovanie používa koncept oblastí. Každý router obsahuje kompletnú databázu stavu liniek špecifickej oblasti, tá môže byť v rozsahu 0 – 65535. Samostatnej oblasti je pridelené číslo 0, tiež sa jej hovorí oblasť 0 alebo **chrbtica**. V multi-area sieťach vyžadujú routre pripojenie na oblasť 0. Povolenie OSPF konfigurácie vyžaduje router s pridelenou IP adresou, wildcard maskou a informáciou o oblasti. **router**

**ospf** process-id, povolenie OSPF smerovania v GKM Process-id je číslo, ktoré je použité na identifikovanie OSPF smerovacieho procesu na routri, je možné spustiť viac procesov na jednom routri. Router(config-router)#**network** address wildcard-mask **area** area-id, pridanie siete do smerovacieho procesu **adresa** – adresa siete, podsiete, hosta, spolu s <wildcard mask> popisuje, ktoré linky sa propagujú a zúčastňujú OSPF procesu a ktoré siete sa propagujú. U <wildcard mask> bit 0 znamená „zhoda“ a 1 „ľubovoľná hodnota“ v porovnaní so zodpovedajúcim bitom v <adresa> (ako u ACL !!!) **area-id** - oblasť, do ktorej patrí adresa. (U single area OSPF 0) **process-id** - číslo procesu OSPF na smerovači (1-65535)

### 2.5.3 Funkcie OSPF

- Smerovač vysiela cez svoje rozhranie tzv Hello pakety. Ak sa dva navzájom prepojené routery pomocou týchto paketov dohodnú na určitých spoločných parametroch, stávajú sa susedmi (Neighbors).
- Medzi niektorými zo susedov sa vytvárajú užšie väzby. Tieto routre sa potom označujú ako príľahlé (adjacent).
- Príľahlé routery si navzájom vymieňajú pakety obsahujúce LSA (Link State Advertisement) informácie. Tie opisujú stav rozhrania smerovača alebo zoznam smerovačov pripojených k danej sieti.
- Všetky smerovače si ukladajú prijaté LSA do svojej lokálnej topologickej databázy a zároveň ich preposielajú na ostatné príľahlé smerovače. Tým sa informácie postupne rozšíria medzi všetky smerovače v sieti. Výsledkom bude zhodná topologická databáza na všetkých smerovačoch.
- Po naplnení databázy každý smerovač vykoná výpočet pomocou SPF (Dijkstrova) algoritmu. Jeho výsledkom bude nájdenie najkratšej cesty do každej známej siete a odstránenie slučiek v topológii siete.
- Na základe vypočítaných dát je možné naplniť smerovaciu tabuľku routeru.
- Ak dôjde k zmene topológie siete, smerovač na ktorom k zmene došlo, odošle príľahlým smerovačom informáciu v podobe LSA dátových položiek v OSPF

paketu. Tá sa postupne rozšíri po celej sieti a každý smerovač upraví svoju topologickú databázu a urobí nový výpočet SPF algoritmu.

#### 2.5.4 Výhoda OSPF

Veľkou výhodou protokolu OSPF proti starším smerovacím protokolom (napr. RIP) je jeho schopnosť pracovať v relatívne veľkých sieťach. Dosiahlo sa toho zavedením dvoch úrovní hierarchie. Sieť je rozdelená na takzvané oblasti (area). LSA sa bežne šíria len vnútri danej oblasti a tiež výpočet SPF algoritmu sa spúšťa pre každú oblasť samostatne. Z jednej oblasti do druhej sa odovzdávajú len sumárne informácie. Zmena topológie siete v jednej oblasti preto nevyvolá prepočet SPF algoritmu v ostatných oblastiach.

## 2.6 IS-IS

### 2.6.1 Vlastnosti IS-IS

- štandardizovaný ISO (otvorený štandard)
- používa Dijkstrov SPF algoritmus, oblasti a hierarchickú topológiu
- pomocou Hello paketov zostavuje susedstvo
- pre broadcast multi-access používa voľbu DR routeru
- jedná sa o classless protokol / VLSM / CIDR
- používa sumarizáciu
- podporuje autentifikáciu
- beží na sieťovej vrstve OSI (layer 3), je to ISO CLNP protokol, ai keď routuju iba TCP / IP (teda podporuje aj IPv6), tak pakety, pomocou ktorých IS-IS komunikuje, sú CLNS PDU (protocol data unit), takže všetky routery musia podporovať ISO CLNS protokol. Preto nezáleží na IP adresách interface (môžu byť z iných subnet) a susedstvo sa rovnako nadviaže (u susedných routerov)

- CLNS (Connectionless Network Service) je služba sieťovej vrstvy, ktorá komunikuje cez CLNP (Connectionless Network Protocol)
- využíva Network Service Access Point (nsapi) adresy - styčný bod, ktorý leží medzi 3 a 4 vrstvou OSI - sieťové služby OSI sú dostupné pre transportnú vrstvu, existuje viacero formátov NSAP adries, skladá sa z 3 častí - adresa oblasti, system ID, NSAP selektor, má dĺžku 8 až 20 bytov, začiatok 49 znamená privátna adresa pre Cisco, začneme sprava (pr. 49.0001.0002.0003.0004.00) - 1byte (00) NSEL, 6byte (0002.0003.0004) system ID, zvyšok area ID (49.0001)
- NET address (Network Entity Titles) - area ID (prvý 1 alebo 2 OCTET), system ID (identifikácia routeru, až 8 OCTET - Cisco 6, býva MAC, ale nemusí), SEL (NSAP selector byte, 1 octet, reprezentuje službu na routeru, Cisco 00)
- NET je NSAP, kde je N-selector = 00
- nevyužíva IP protokol, ale OSI networking
- LSP, Hello PDU, routing PDU sa posielajú ako OSI pakety (nie IP pakety, do ktorých sa ale môžu zabaliť) = PDU sú Encapsulated priamo do data-link frame
- viac časovačov (Timers) pre ladenie, menej typov oblastí ako OSPF, používa menej link-state PDU (LSP)
- menšie zaťaženie CPU, ešte rýchlejší konvergencie ako OSPF
- na routeru môže bežať iba jeden IS-IS routing proces

### **Rozdiely oproti OSPF:**

- IS-IS posielajú všetky údaje v jednom sete paketov ako TLV, OSPF má rôzne typy LSA.
- IS-IS balí svoje dáta priamo do DATA-LINK rámca, OSPF využíva IP
- IS-IS rozlišuje iba 2 médiá, broadcast multiaccess a point-to-point
- IS-IS vyberá DIS ktorý je preemtívny (vždy sa vyberá) a neexistuje záložné

## 2.7 EIGRP

- Dokáže rýchlo zareagovať na zmenu v sieti
- Čas konverencie je veľmi malý
- Protokol si udržiava nielen najlepšiu cestu, ale má aj zálohu, ak by najlepší smer zlyhal.
- Efektívne využitie šírky pásma
- Podpora VLMS a CIDR

### 2.7.1 Koncept a terminológia

EIGRP routre ukladajú naučené smerovania do tabuliek. Udržujú 3 tabuľky:

- **tabuľku susedov**, sú v nej všetci EIGRP susedné routre. Po nájdení nového suseda je zaznamenaná informácia o adrese a o rozhraní suseda. Táto informácia je uložená v dátovej štruktúre susedov. Keď sused pošle hello paket, oznámi v ňom **hold time**, po uplynutí tohto času je sused označený ako nedosiahnuteľný a zmeny musia byť prepočítané do novej topológie. **show ip eigrp neighbors** – zobrazí všetkých EIGRP susedov
- **topologickú tabuľku**, tvoria ju všetky smerovacie tabuľky v AS. Diffusing Update Algorithm (DUAL), použije informácie z tabuľky susedov a topologickej tabuľky na výpočet nižšej ceny smerovania do každého cieľového miesta. **show ip route eigrp** – zobrazenie topologickej tabuľky
- **smerovaciú tabuľku**, udržiavajú najlepšiu cestu do cieľa. **successor** (následník), je susedný router na ceste do daného cieľa

### 2.7.2 Technológia

Nové technológie:

1. zistenie susedov a obnova
2. spoľahlivý transportný protokol

3. algoritmus DUAL
4. protokolovo závislé moduly

Jednoduché vzdialenostné smerovacie protokoly, ako IGRP alebo RIP, nevytvárajú vzťahy so susedmi. Naopak EIGRP aktívne vytvárajú vzťahy so svojimi susedmi, podobne ako je tomu u OSPF. EIGRP routre vysielajú **hello pakety** susedným routrom každých 5 sekúnd, slúžia na overenie stavu linky. Vytváranie susedov:

1. dynamicky sa učia o nových routroch pripojených na sieť
2. identifikujú routre, ktoré sú nedosiahnuteľné alebo nefunkčné
3. identifikujú routre, ktoré boli nedosiahnuteľné

**Reliable Transport Protocol (RTP)** – spoľahlivý protokol pre doručovanie EIGRP paketov, nie je závislý na IP protokole

EIGRP si vytvárajú topologickú databázu a databázu susedov, obidve sa využívajú pre DUAL. Pri výpadku linky DUAL hľadá alternatívnu cestu, alebo možného suseda v topologickej databáze. IP-EIGRP modul:

1. posiela a prijíma EIGRP pakety, ktoré nesú IP data
2. oznamuje DUAL o nových prijatých IP informáciách
3. spravuje smerovaciu tabuľku
4. redistribuuje smerovacie informáciu

### 2.7.3 Konfigurácia

Kroky pre konfigurovanie EIRGP v IP:

1. `router(config)#router eigrp autonomous-system-number`, povolí EIGRP. Číslo AS identifikuje všetky routre vnútri AS.
2. `router(config-router)#network network-number`, zadávajú sa siete, ktoré patria do AS a sú **priamo** pripojené k routru, kde bol príkaz `network` zadany.

3. router(config-if)#**bandwidth** kilobits, EIGRP routre vyžadujú zadanie šírky pásma
4. router(config-if)#**eigrp log-neighbor-changes**, doporučený príkaz CISCO, povoľuje logovanie zmien susedov

## ZÁVER

Cieľom práce bolo oboznámiť ako fungujú smerovacie protokoly, či už statické alebo dynamické. Statické smerovanie bolo stručnejšie, pretože nie je také rozšírené. V dynamickom smerovaní boli popísané jednotlivé protokoly od najstarších po najnovšie a od najpoužívanejších po menej používané. V protokoloch boli popísané ich vlastnosti, funkcie, princíp, výhody, nevýhody, konfigurácia a využitie.

O správny chod počítačových sietí sa starajú správcovia siete. Konfigurujú jednotlivé protokoly a v prípade nejakého problému ho musia vyriešiť čo najskôr, lebo správny beh počítačovej siete je v niektorých prípadoch veľmi dôležitý. Hlavne v podnikoch, ktoré sa bez správnej funkčnosti nemôžu ďalej pohnúť.

V tejto časti práce je len teória. Pre úplné pochopenie smerovania v počítačových sieťach je potrebné preštudovať aj praktickú časť, ktorá je uvedená na CD. Tam sú popísané a vysvetlené jednotlivé konfigurácie na konkrétnych príkladoch. Témy sú rozdelené do kapitol. Praktická časť taktiež obsahuje prezentácie ku kapitolám.



## CONCLUSION

The goal of this work was to know how the routing protocols, whether static or dynamic. Static routing was succinct, it is not so widespread. In a dynamic routing protocols have been reported each from oldest to newest and the most widely used for less. The logs were described their features, functions, principles, advantages, disadvantages, configuration and use.

The correct operation of computer networks, network administrators take care of. Configure different protocols in the case of a problem it must be resolved as soon as the correct running of the computer network, in some cases very important. Especially in companies, without proper function can no longer move. This part is only a theory. For a full understanding of routing in computer networks is necessary to study the practical part, which is included on the CD. There are described and explained the different configuration for specific examples. Topics are divided into chapters. The practical part also contains a presentations of the chapters.

**ZOZNAM POUŽITEJ LITERATÚRY**

- [1] Cisco Systems. Cisco Networking Academy: CCNA 2 Curriculum [online]. C2007 [cit. 2010-01-22]. Dostupný z WWW: <http://cisco.netacad.net/>.
- [2] STU v Bratislave: Cisco Networking academy [online]. [2008-01-01]. Dostupný z WWW: <<http://cisco-academy.aspone.cz/>>
- [3] O webu: O internetu, počítačích a webhostingu [online]. [cit. 2009-03-29]. Dostupný z WWW: <<http://owebu.bloger.cz/>>
- [4] FEI – Grygarek. Katedra informatiky, VŠB - TU Ostrava [online]. [cit. 2009-03-02]. Dostupný z WWW: <<http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html>>
- [5] Petr Bouška. Samuraj-cz [online]. [cit. 2009-09-04]. Dostupný z WWW: <<http://www.samuraj-cz.com/>>

**ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK**

(E)IGRP	(Enhanced) Interior Gateway Routing Protocol
BGP	Border Gateway Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
LAN	Local Area Network
MAC	Media Access Control
NIC	Network Interface Card
OSPF	Open Shortest Path First
RIP	Routing Information Protocol

**ZOZNAM OBRÁZKOV**

Obr. 1.	Formát IP paketu.....	11
Obr. 2.	Topológia.....	12
Obr. 3.	Rozdelenie dynamických protokolov.....	17
Obr. 4.	RIPv1 Formát správy.....	20
Obr. 5.	Topológia OSPF.....	24

## ZOZNAM PRÍLOH

P I Upravené materiály pre kurz CCNA2 v čestine. CD-ROM:\ materiály

P II Prezentácie pre kurz CCNA2. CD-ROM:\ prezentácie