Směrovací protokoly v počítačových sítích

Matúš Šimo

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Matúš Šimo**
Osobní číslo:	**A11062**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Směrovací protokoly v počítačových sítích**

Zásady pro vypracování:

1. **Zpracujte přehled směrovacích protokolů.**
2. **Vyhodnoťte použití jednotlivých protokolů.**
3. **Popište konfiguraci a metody zabezpečení vybraných protokolů.**
4. **Sestavte a nakonfigurujte v simulačním prostředí ukázkové topologie.**
5. **Porovnejte jednotlivé verze operačních systémů pro routery Cisco.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-80-251-2520-5.**
2. **HUCABY, Dave, Steve MCQUERRY a Andrew WHITAKER. Cisco router configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2010, xxii, 641 s. ISBN 978-1-58714-116-4.**
3. **SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.**
4. **DOYLE, Jeff a Jennifer DEHAVEN CARROLL. Routing TCP/IP. Indianapolis: Cisco Press, 2001, xxii, 945 s. ISBN 15-787-0089-2.**
5. **CISCO SYSTEMS, Inc. Internetworking Technology Handbook [online]. 2013 [cit. 2013-12-02]. Dostupné z: http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook**
6. **CISCO SYSTEMS, Inc. Routing Infrastructure [online]. 2013 [cit. 2013-12-02]. Dostupné z: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap3**

Vedoucí bakalářské práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalárska práca sa zaoberá dynamickými smerovacími protokolmi v počítačových sieťach. Teoretická časť popisuje základné informácie potrebné pre vniknutie do problematiky. Zoznamuje čitateľa s pojmami ako smerovač, smerovanie, Cisco IOS a popisom jednotlivých smerovacích protokolov a príkazov na ich konfiguráciu. Praktickú časť tvorí popis simulačného programu Cisco Packet Tracer a následná konfigurácia jednotlivých smerovacích protokolov.

Klíčová slova: smerovač, smerovací protokol, Cisco IOS, RIPv1, RIPv2, IGRP, OSPF, EIGRP.

ABSTRACT

Bachelor thesis deals with dynamic routing protocols in computer networks. Theoretical part of work describes basic information which is necessary for understanding problematics. Introduces reader with terms like router, routing, Cisco IOS and with description of individual routing protocols and commands for their configuration. Practical part consists from a description of simulation software Cisco Packet Tracer and following configuration of individual routing protocols.

Keywords: router, routing protocol, Cisco IOS, RIPv1, RIPv2, IGRP, OSPF, EIGRP.

Poďakovanie

Týmto by som sa chcel poďakovať svojmu vedúcemu Ing. Jiřímu Korbelovi Ph.D. za jeho vedenie, poskytnutý čas a cenné rady pri vypracovávaní mojej bakalárskej prace.

Takisto ďakujem mojím rodičom, priateľke a kamarátom za podporu počas celého štúdia.

Motto:

„Aj cesta dlhá 1000 míľ začína prvým krokom.“

Confucius.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Počítačové siete sú v dnešnej dobe Internetu neoddeliteľnou súčasťou veľkej časti populácie. Zjednodušujú komunikáciu, získavanie informácií, či bankové transakcie a tým uľahčujú život. Namiesto platenia faktúr na pošte, alebo hľadaní informácií v knihách nám stačí počítač pripojený na Internet a zrazu sa nám otvára virtuálny svet, kde stačí par stlačení klávesnice a kliknutí myšou a takmer všetko môžeme vykonať z pohodlia domova. Málo kto však vie, čo všetko sa za tým skrýva.

Najdôležitejšou súčasťou siete je zariadenie, ktoré sa nazýva smerovač(router). Ten má za úlohu rozposielať pakety podľa presne nadstavených parametrov. Tento proces sa nazýva smerovanie a delí sa na statické a dynamické. Táto práca sa zameriava na dynamické smerovanie pomocou smerovacích protokolov v interných sieťach a popis jednotlivých verzií operačných systémov smerovačov Cisco. V súčasnej dobe je minimum materiálov v slovenskom jazyku, ktorý popisuje túto problematiku. To je jedným z dôvodov pre vytvorenie uceleného dokumentu, ktorý môže byť prínosom pri konfigurovaní sietí aj pre menej jazykovo zdatných ľudí.

Teoretická časť bude zameraná na zoznámenie sa so základnými informáciami ohľadom smerovača, smerovania. Tie by mali byť základnou znalosťou každého, kto sa rozhodne s konfigurovaním sietí. To isté platí aj pre variabilné podsieťovanie. Ďalšia časť je tvorená popisom operačného systému Cisco IOS, ktorý má na starosti riadenie smerovačov od spoločnosti Cisco, ktorá je jednotkou na trhu v oblasti sieťových komponentov. Najväčšia časť však bude zameraná na samotné smerovacie protokoly a to konkrétne na RIPv1, RIPv2, IGRP, OSPF a EIGRP. U každého budú popísané jeho vlastnosti a príkazy na konfiguráciu.

Praktická časť bude robená v simulačnom prostredí Cisco Packet Tracer. Jedná sa o program spoločnosti Cisco, ktorý dokáže odsimulovať takmer všetky príkazy, ktoré sa používajú pri konfigurácii skutočného smerovača. V prvej časti sa bude nachádzať popis programu pre zoznámenie sa s prostredím a rozobratie jeho jednotlivých funkcií a druhá, ktorá je najdôležitejšia, bude tvorená ukážkovými topológiami. Tie budú vytvorené u každého protokolu tak, aby boli jasné a zrozumiteľné. Jednotlivé nenakonfigurované ako aj nakonfigurované simulácie v programe Cisco Packet Tracer sa budú takisto nachádzať aj v prílohe.

I. TEORETICKÁ ČÁST

1 ÚVOD DO SMEROVANIA

Pod pojmom smerovanie sa rozumie metóda pre výber trasy, ktorou budú dáta v sieti zasielané. Jeho vznik sa datuje do obdobia prvých počítačových sietí a postupne sa vyvíjalo až do súčasnej podoby. Zariadenie, ktoré v sieti smeruje pakety sa nazýva smerovač. [1]

1.1 Smerovač

Je sieťové zariadenie, ktoré má na starosti prepojovať aspoň dve siete. Jeho úlohou je rozdeľovať kolízne domény, filtrovať a blokovať všesmerové vysielanie a zaisťovať optimálnu trasu pre smerovanie paketov. Smerovače sú v skutočnosti veľmi silné počítače, prevádzajúce vysokú mieru spracovaných dát. Rozvoj priniesli 80. roky 20. storočia, kedy do Internetu vnikla komercia. Vtedy prišla na trh firma Cisco, ktorá premenila smerovače na hardwarové zariadenia a v súčasnosti na trhu dominuje. V ich zariadeniach je operačný systém IOS (Internetwork Operating System). Bol vyvinutý na smerovanie a prepínanie. Obsahuje riadkové rozhranie CLI. Medzi ďalších výrobcov patria JUNOS od Juniper Networks a XOS od Extreme Networks. [1]

1.1.1 Hardware smerovača

Smerovač je svojím spôsobom špecializovaný počítač s hardwarom a softwarom, ktorý plní funkcie, na ktoré je určený a to smerovanie paketov. Medzi hlavné hardwarové komponenty patria:

- **CPU** (The Central Processing Unit) - jedná sa o mikroprocesor, ktorý vykonáva inštrukcie,
- **RAM** (Random Access Memory) – pamäť, ktorá pri výpadku napájania stráca svoje informácie. Je používaná pre smerovacie tabuľky, smerovaciu konfiguráciu, vyrovnávajúca pamäť pre IOS,
- **FLASH –** slúži na uloženie Cisco IOS imidž, z ktorého si ho smerovač nahráva. Imidž môže byť komprimovaný alebo nekomprimovaný,
- **NVRAM** (Nonvolatile Random Access Memory) – používa sa na uloženie spúšťacej konfigurácie. Pri výpadku napájania sa nezmaže,
- **ROM** (Read Only Memory) – slúži na trvalé uloženie spúšťacieho diagnostického kódu. Má za úlohu hardwarovú diagnostiku počas spustenia smerovača a nahranie

IOS z FLASH do RAM. Môže byť použitá aj ako alternatívny bootovací zdroj. ROM sa nemaže,

- **zbernica –** rozdeľujú sa na systémovú a CPU. Systémová slúži na komunikáciu medzi CPU a rozhraniami. CPU zbernica komunikuje s pamäťami,
- **rozhrania –** LAN, Ethernet, Token Ring, sériové, ISDN, Console/AUX,
- **napájací zdroj –** má za úlohu napájať všetky komponenty smerovača. [2]

1.1.2 Cisco IOS

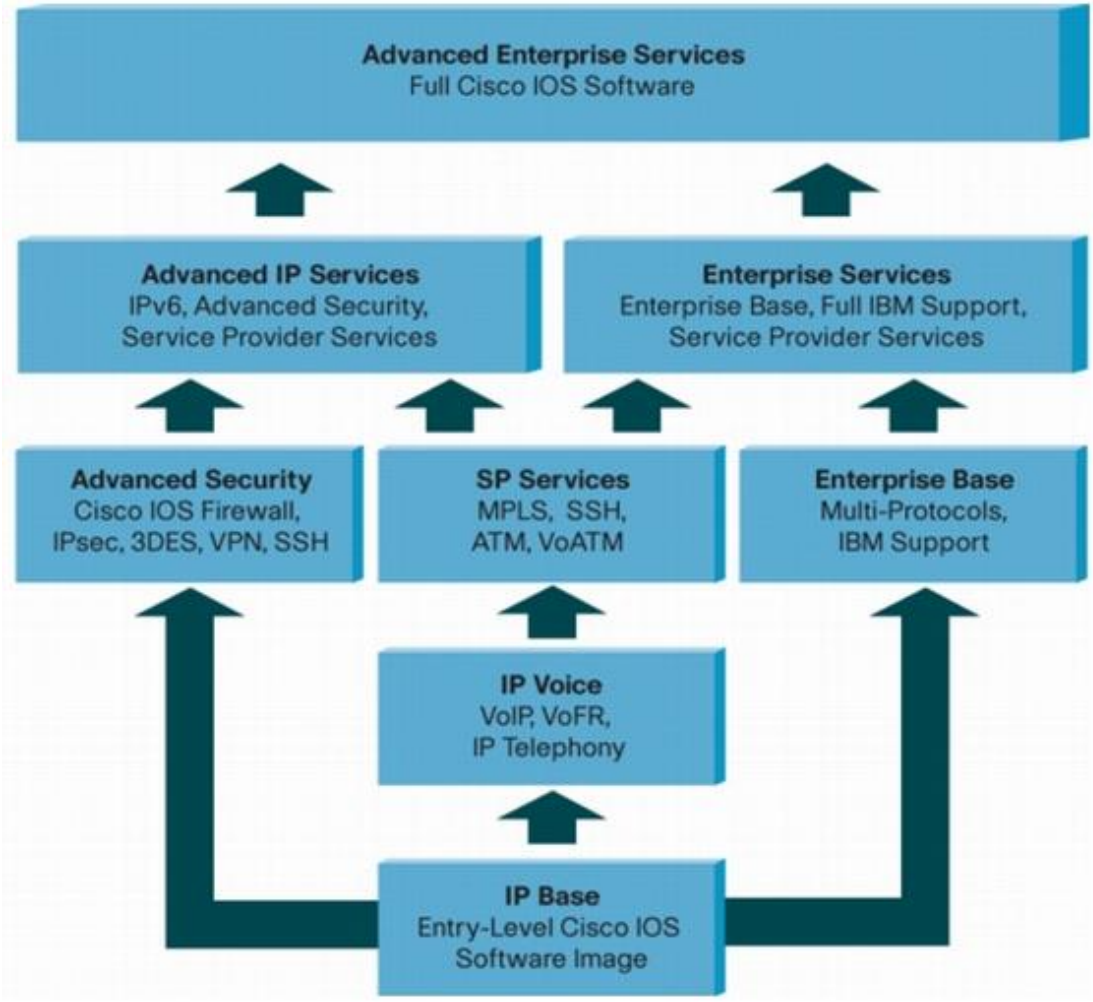
Jedná sa o systémové jadro vyvinuté firmou Cisco, ktorá poskytuje funkcie smerovania, prepínania, prepojenia sietí a telekomunikácií. Prvá verzia vznikla v roku 1986 a stojí za ňou vývojár William Yeager. [1]

Software IOS zaisťuje nasledovné úlohy:

- prenáša sieťové protokoly a ich funkcie,
- prepojuje vysokorýchlostné prenosy medzi zariadeniami v sieti,
- doplňuje bezpečnosť kvôli riadeniu prístupu a zamedzuje neoprávnenému použitiu siete ak nespĺňa určité požiadavky,
- poskytuje škálovateľnosť, hlavne za účelom zjednodušenia rastu siete a zaručenia redundancie,
- zaisťuje spoľahlivosť siete pri prepojovaní k jednotlivým sieťovým prostriedkom. [1]

Cisco IOS používa na konfiguráciu príkazový riadok CLI (Command Line Interface), ktorý obsahuje tri módy a to užívateľský, privilegovaný a konfiguračný, ktoré budú rozobraté v praktickej časti. [1]

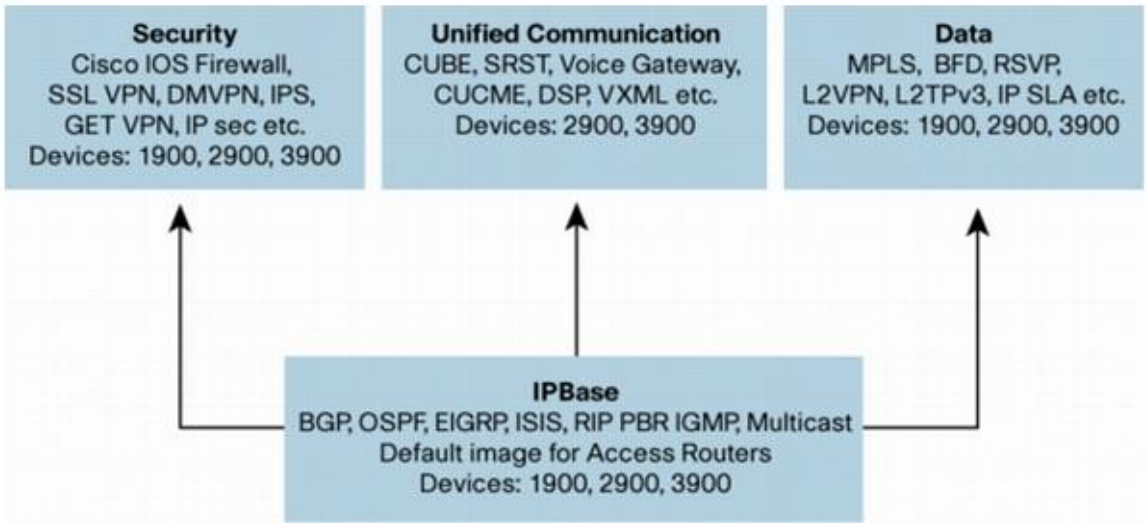
Delenie je tvorené dvoma spôsobmi a to starším, ktoré používali všetky verzie do 15.0. viď. obrázok 1. Je tvorené ôsmimi typmi.



Obrázok 1. Pôvodné delenie Cisco IOS [3]

Základná verzia sa nazýva IP Base, na ktorú sú nabaľované ďalšie funkcie ako VoIP, Firewall, šifrovanie, VPN, Novell, IPv6 a tak ďalej. Najvyššia verzia obsahuje všetky funkcie sa nazýva Advanced Enterprise Services. [3]

Od verzie 15.0 prešlo delenie z ôsmich častí na štyri viď. obrázok 2. Základná verzia je rovnako ako pri predchádzajúcom delení IP base, avšak podobná verzia ako bola Advanced Enterprise Services, ktorá obsahovala všetky funkcie už v novom delení nie je. [4]



Obrázok 2. Nové delenie Cisco IOS [4]

Na porovnanie bola vybraná verzia 12.3 na platforme 2691. Rozdiel medzi verziou IP Base a IP Voice sa nachádza v tabuľke 1, kde sú zobrazené pridané funkcie v IP Voice oproti základnému modelu IP Base. Nie sú zobrazené všetky, pretože rozdiel je až v 135 funkciách. [5]

Tabuľka 1. Pridané funkcie v Cisco IOS 12.3 IP Voice [5]

Pridané funkcie v IP Voice	
Mobile IP	Voice DSP Control Message Logger
Mobile IP - Dynamic DNS and Multiple DHCP Support	Voice Over IP (VoIP)
Mobile IP - Fastswitching Support on FA	Voice over ATM
Mobile IP - HA Policy Routing	Voice over ATM with AAL2 Trunking
Mobile IP - HMAC-MD5 support	Voice over Frame Relay (FRF.11)
Mobile IP - Mobile Networks	Voice over Frame Relay Configuration Updates
VoIP Call Admission Control using RSVP	Voice over IP Q.SIG Network Transparency
VoIP Gateway Trunk and Carrier Based Routing Enhancements	Voice Call Tuning
VoIP Outgoing Trunk Group Identification and Carrier ID for Gateways	Caller ID
Voice Busyout Enhancements	Cisco IOS Telephony Service (ITS) Version 2.1

Takisto boli porovnané aj dve najnovšej verzie 15.4T IP Base a Data, na platforme 2911. Rozdiel medzi verziami sa nachádza v tabuľke 2. Verzia Data má oproti IP Base 255 pridaných funkcií. V tabuľke preto nie sú zobrazené všetky. [5]

Tabuľka 2. Pridané funkcie v Cisco IOS 15.4T Data [5]

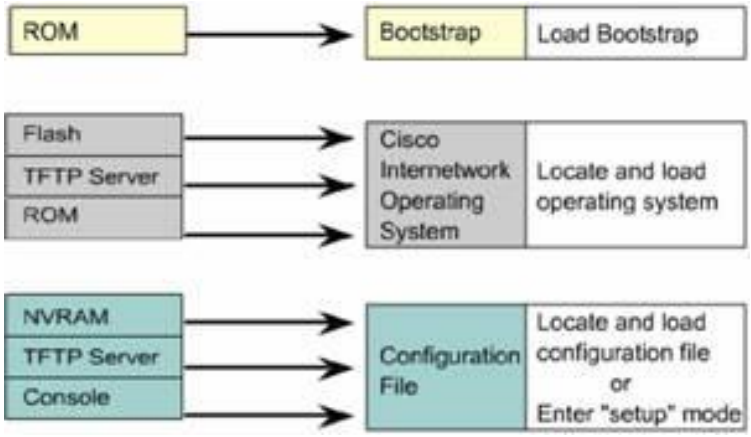
Pridané funkcie v Data	
ACL-based RBSCP	IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)
Frame Relay Access Support (FRAS) Border Access Node (BAN)	IPv6 Access Services: DHCPv6 Prefix Delegation
Frame Relay Access Support (FRAS) Boundary Network Node (BNN)	IPv6 over DMVPN
Frame Relay Access Support (FRAS) DLCI Backup	IPv6 transport for DMVPN
Frame Relay Access Support (FRAS) Dial Backup over DLSW+	Fast-Switched SRTLB
Frame Relay Access Support (FRAS) Host	Mobile IP - Challenge/Response Extestions
Frame Relay SVC Support (DTE)	Mobile IP - Dynamic DNS and Multiple DHCP Support
Frame Relay Tunnel Switching	Mobile IP - Dynamic Security Association and Key Distribution
VLAN id rewrite	Mobile IP - Fastswitching Support on FA
Virtual Templates for Protocol Translation	Tunneling of Asynchronous Security Protocols

1.1.3 Postupnosť pri spustení smerovača

Základnou a hlavnou úlohou smerovača je zabezpečiť smerovacie operácie. Po zapnutí sa vykonávajú nasledujúce operácie:

- test hardwaru,
- nájdenie a nahranie IOS,
- nájdenie a aplikovanie konfiguračných pravidiel. [6]

Pri hľadaní a nahrávaní Cisco IOS sa pozrie do boot systém commands uloženom v NVRAM. Nadstavenie konfiguračného registra umožňuje nasledovné alternatívy. Príkaz v boot system commands určí, ako postupovať pri hľadaní zdroja. Pri neprítomnosti príkazu sa využije IOS vo FLASH pamäti. Ak je prázdna pokúsi sa použiť TFTP na nahranie imidžu zo siete viď. obrázok 3. [6]



Obrázok 3. Postup pri spustení smerovača [6]

Bootovanie prebieha v nasledujúcich fázach:

a) **test hardwaru smerovača:**
    1) **POST** (Power On Self Test**)** – základný test funkcií smerovača (rozhrania, pamäť),
    2) **načítania bootstrap loadera** – má za úlohu inicializáciu bootovania a nahrania systému IOS.
b) **lokalizácia a načítanie softwaru Cisco IOS,**
c) **lokalizácia a načítanie štartovacej konfigurácia.** [7]

1.2 Smerovanie IP

Pod pojmom smerovanie rozumieme prenos paketu z jednej siete do druhej pomocou smerovača. Treba si vymedziť rozdiely medzi smerovaním a smerovacím protokolom.

Smerovací protokol dynamicky vyhľadáva všetky siete v dátovej sieti. Zabezpečuje rovnakú smerovaciu tabuľku u všetkých smerovačov, ktoré spolu komunikujú. Určuje nám trasu, ktorou je paket prenášaný. Medzi smerovacie protokoly patria napríklad RIP, RIPv2, IGRP, EIGRP, OSPF.

Ak majú všetky smerovače kompletné informácie o sieti, môžu pomocou smerovaného protokolu posielať pakety v rámci definovanej dátovej siete. Medzi smerované protokoly patria napríklad protokol IP a IPv6. [8]

1.3 Statické smerovanie

Pri statickom smerovaní musí administrátor ručne nadstaviť trasy do smerovacích tabuliek každého smerovača. Tento spôsob má svoje výhody aj nevýhody. [8]

Výhody:

- nespôsobuje žiadnu réžiu procesu smerovača. To má za výhodu možnosť kúpi lacnejšieho smerovača, než v prípade dynamického smerovania,
- medzi smerovačmi sa neopotrebováva šírka pásma dátovými prenosmi,
- zvyšuje sa bezpečnosť, keďže sa administrátor môže rozhodnúť, že povolí smerovanie iba do určitých sietí a ostatné zakáže. [8]

Nevýhody:

- administrátor musí dobre rozumieť sieti a prepojeniu jednotlivých smerovačov, aby ich dokázal správne nakonfigurovať,
- ak je pridaná nová sieť, musí administrátor doplniť trasu do všetkých ostatných smerovačov ručne,
- nemožno používať pri rozsiahlych sieťach, pretože konfigurácia a údržba by bola náročná a neprehľadná. [8]

1.4 Dynamické smerovanie

Používa sa v prípade, že sa pri hľadaní sietí a aktualizácií smerovacích tabuliek používajú špeciálne protokoly. Administrácia je jednoduchšia ako u statického smerovania, ale je tu kladení vyšší nárok na zaťaženie procesora a šírky pásma. Smerovací protokol definuje sadu pravidiel, pomocou ktorých sa smerovač riadi. [8]

1.4.1 Základné pojmy smerovacích protokol

Smerovacie protokoly boli prvý krát zjednotené v roku 1988 do štandardu RFC 1058. Pred tým, ako sa s nimi zoznámime, treba uviesť niektoré hlavné informácie. Je potrebné poznať pojmy ako autonómny systém, metrika, administratívna vzdialenosť, typy smerovacích protokolov a slučky v smerovaní. [8]

1.4.2 Autonómny systém

Pod pojmom autonómny systém skrátene AS, rozumieme sieť pod spoločnou administratívnou správou. V tomto systéme je rovnaká smerovacia stratégia a vonkajší svet je vnímaný ako jedna entita. Vznikol na základe toho, že smerovače by nedokázali udržiavať všetky smerovacie informácie v sieti Internet. Jednotlivé AS majú vlastné interné pravidlá, v ktorých môže byť jeden, alebo viac druhov interných smerovacích protokol a výmenu informácií medzi systémami zabezpečuje externý smerovací protokol. AS sa rozdeľujú na tri druhy a to:

- **single-homed** – jedná sa o AS, ktorý má jeden hraničný smerovač do ostatných sietí a často krát vôbec nepotrebuje externý smerovací protokol.
- **multihomed** – má oproti single-homed viacero hraničných smerovačov do ostatných sietí, avšak nedovoľuje, aby cez neho tiekla cudzia prevádzka.
- **transit** – AS, ktorý má taktiež viacero hraničných smerovačov a slúži na prenos tranzitnej prevádzky medzi inými systémami. [9]

1.4.3 Metrika

Jedná sa o hodnotu, ktorá nám uvádza, aká výhodná je cesta do cieľovej siete. Metriku chápeme ako vzdialenosť. Ak do cieľovej siete existuje viac ciest protokol vyberie trasu s najnižšou metrikou. [8]

Využívajú sa rôzne spôsoby na určenie metriky a medzi najčastejšie patri:

- rýchlosť,
- oneskorenie,
- spoľahlivosť,
- počet skokov,
- aktuálna záťaž. [8]

1.4.4 Administratívna vzdialenosť

Umožňuje pri konfigurácii oceniť dôveryhodnosť smerovacích informácií, ktoré smerovač príjma od susedného smerovača a udáva sa číslom od 0 po 255. Hodnota 0 je najdôveryhodnejšia a naopak hodnota 255 je najmenej dôveryhodná a nebude sa uskutočňovať žiadna prevádzka. Ak smerovač prijme dve rovnaké aktualizácie s rovnakou vzdialenosťou siete, najskôr skontroluje hodnotu administratívnej vzdialenosti a zvolí trasu s najnižšou hodnotou. Ak ju majú rovnakú, použije sa metrika smerovacích protokolov ako počet skokov, šírka pásma a podobne. Pokiaľ budú mať aj v tomto prípade rovnakú hodnotu, zaistí sa komunikácia vyvážene po obidvoch spojoch. Hodnoty administratívnej vzdialenosti sa nachádzajú v tabuľke 3. [8]

Tabuľka 3. Hodnoty administratívnej vzdialenosti [10]

Administratívna vzdialenosť	Predvolená vzdialenosť
Priame pripojenie	0
Statické smerovanie	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120

1.5 Variabilné podsieťovanie VLSM

Variabilné podsieťovanie vzniklo v polovici 90. rokov za účelom šetrenia adresného priestoru. IP adresa sa delí na 4.oktety. Triedy adries delíme do troch tried a to na triedu A, B a C. Trieda A používa prvý oktet na sieť a zvyšné tri oktety na hostiteľov. Trieda B používa dva oktety na sieť a dve na hostiteľov. Trieda C používa tri oktety na sieť a jeden oktet na hostiteľov. V tabuľke 4 je vidieť jednotlivé triedy a rozsahy pre sieť a hostiteľa. [11]

Tabuľka 4. Triedy a rozsah IP adries [11]

	1.oktet	2.oktet	3.oktet	4.oktet	maska podsiete
Trieda A	sieť	hostiteľ	Hostiteľ	hostiteľ	255.0.0.0
Trieda B	sieť	sieť	Hostiteľ	hostiteľ	255.255.0.0
Trieda C	sieť	sieť	Sieť	hostiteľ	255.255.255.0

	Rozsah prvého oktetu	Počet možných sietí	Počet hostiteľov na sieti
Trieda A	0-127	128	16,777,214
Trieda B	128-191	16,348	65,534
Trieda C	192-223	2,097,152	254

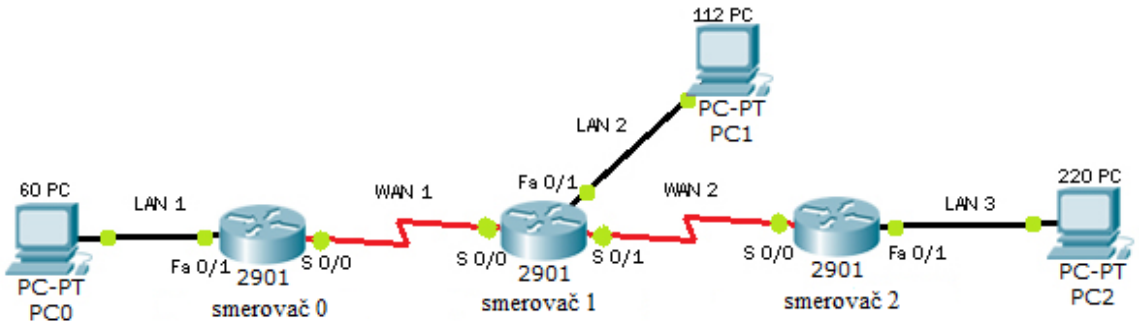
Pri variabilnom podsieťovaní VLSM je potrebné, aby si smerovacie protokoly medzi sebou vymieňali aj údaje o maske podsiete.

Pre určovanie počtu adries je používaná mocnina čísla 2. To vyplýva z dvojkovej sústavy. Ak je potrebný pre lokálnu sieť rozsah adries pre 25 počítačov, k tomuto číslu treba pripočítať adresu podsiete a adresu broadcastu. Z toho vyplýva, že bude potrebných 27 adries. Ako najbližšia mocnina dvojky je číslo 32. Ak by bolo v sieti 31 adries pre počítače, po pripočítaní adresy podsiete a broadcastu nám vyjde číslo 33, a tým pádom treba zväčšiť rozsah na ďalšiu mocninu dvojky a to je číslo 64. Pre lepšiu orientáciu je vytvorená tabuľka 5, po rozsah 2^10 s prehľadom počtu hostiteľov a másk. [11]

Tabuľka 5. Mocniny čísla 2 s počtom hostiteľov a masky podsiete [11]

mocnina čísla 2	Maximum hostiteľov	Dĺžka masky	Maska podsieťe
2^0	1	/32	255.255.255.255
2^1	2	/31	255.255.255.254
2^2	4	/30	255.255.255.252
2^3	8	/29	255.255.255.248
2^4	16	/28	255.255.255.240
2^5	32	/27	255.255.255.224
2^6	64	/26	255.255.255.192
2^7	128	/25	255.255.255.128
2^8	256	/24	255.255.255.0
2^9	512	/23	255.255.254.0
2^10	1024	/22	255.255.252.0

Najlepšie na vysvetlenie variabilného VLSM podsieťovania slúži jednoduchý príklad. Adresný rozsah pre sieť je 193.15.76.0 /23. Pomocou VLSM sa vytvoria adresy pre jednotlivé segmenty.



Obrázok 4. Vzorová sieť pre výpočet IP adries pomocou VLSM

Pre WAN 1 a WAN 2 postačia 4 adresy, a to pre sieť, prvú, poslednú a broadcastovú adresu.

Pre LAN 1 je treba rozsah väčší ako 60 adries plus dve adresy na sieť a broadcast. Ako najbližšia mocnina dvojky je číslo 64.

LAN 2 potrebuje minimálne 112 adries plus dve pre sieť a broadcast. Najbližšia mocnina je číslo 128.

Pri LAN 3 potrebuje až 220 adries plus ďalšie dve pre sieť a broadcast. Najbližšia mocnina je číslo 256.

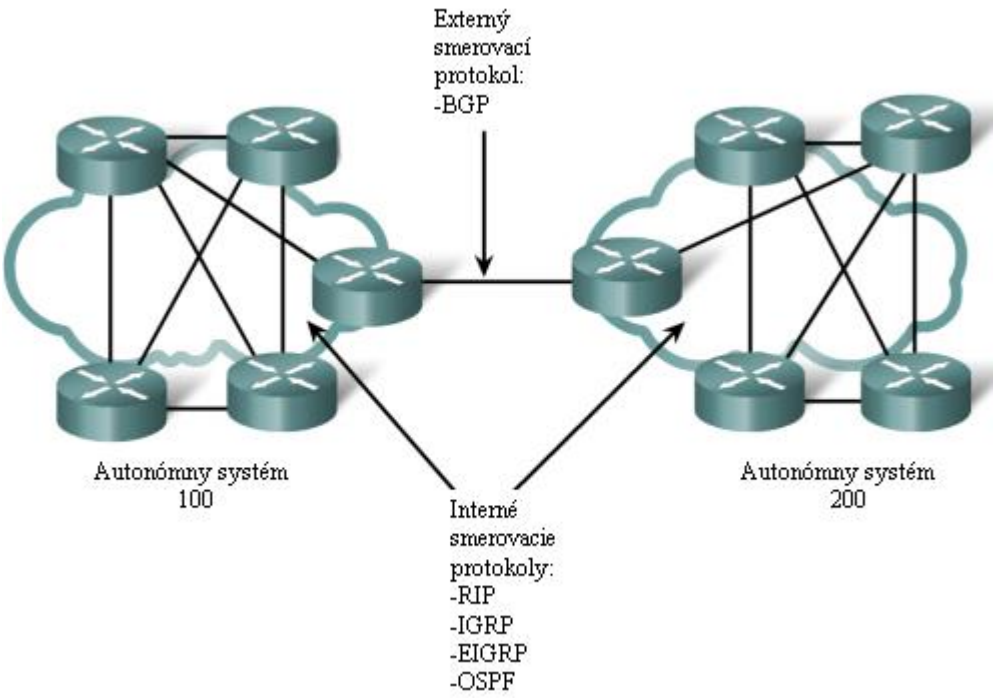
V tabuľke 6 je prehľadný popis adries, ktoré budú použité pre daný príklad.

Tabuľka 6. Výpočet IP adries pomocou VLSM

Sieť	Adresa siete	Maska podsiete	Prvá použiteľná adresa	Posledná použiteľná adresa	Broadcastová adresa
WAN 1	193.15.76.0	255.255.255.252	193.15.76.1	193.15.76.2	193.15.76.3
WAN 2	193.15.76.4	255.255.255.252	193.15.76.5	193.15.76.6	193.15.76.7
LAN 1	193.15.76.64	255.255.255.192	193.15.76.65	193.15.76.126	193.15.76.127
LAN 2	193.15.76.128	255.255.255.128	193.15.76.129	193.15.76.254	193.15.76.255
LAN 3	193.15.77.0	255.255.255.0	193.15.76.1	193.15.77.254	193.15.77.255

2 SMEROVACIE PROTOKOLY

Smerovacie protokoly sa rozdeľujú do dvoch hlavných skupín podľa toho, v akom prostredí pracujú, a to na interné, takzvané IGP(Interior Gateway Protocols), jedná sa o skupinu, ktorá pracuje vo vnútri autonómneho systému a externé EGP(Exterior Gateway Protocols), ktoré sa používajú medzi autonómnymi systémami viď. obrázok 4. [12]



Obrázok 5. Vnútorné a vonkajšie smerovacie protokoly [13]

Interné smerovacie protokoly sa delia do troch kategórií, a to s vektorom vzdialenosti, so stavom linky a hybridné. Treba poznať ich výhody a nevýhody pri administrácii siete.[8]

2.1 Smerovacie protokoly s vektorom vzdialenosti

Pod pojmom protokol s vektorom vzdialenosti rozumieme hľadanie najlepšiu trase do inej siete, na základe vzdialenosti. Tieto protokoly hľadajú linku s najnižším počtom skokov. Pod pojmom skok chápeme prechod paketu smerovačom. Algoritmus s vektorom vzdialenosti predáva susedným smerovačom kompletnú smerovaciu tabuľku, tí ju príjmu a už ju nijak neoverujú. Medzi tieto protokoly patrí protokol RIP, RIPv2, IGRP.[8]

Pred tým, ako budú rozobraté jednotlivé protokoly s vektorom vzdialenosti, treba sa zoznámiť s problematikou slučiek v smerovaní.

2.1.1 Slučky v smerovaní

Smerovacie protokoly s vektorom vzdialenosti sledujú zmeny v dátovej sieti. Pravidelne prevádzajú všesmerové vysielanie aktualizácií zo všetkých aktívnych rozhraniach a obsahuje úplnú smerovaciu tabuľku. Táto metóda úspešne funguje, avšak sú kladené veľké nároky na procesor a spotrebu šírky pásma. Problémy môžu nastať pri výpadku siete, čo môžu viesť k tomu, že smerovacie tabuľky nie sú aktuálne, a to má za následok posielanie paketov na smerovač, ktorý vypadol a nekomunikuje. Problém je v tom, že smerovač o chybe nevie, pretože ešte nemá aktuálnu smerovaciu tabuľku. Keďže odosielanie aktualizácií sa vykonáva každých 30 sekúnd, vznikne takzvaná slučka v smerovaní. [8]

Nato ako slučku prerušiť existuje viac možností.

1) **Maximálny počet preskokov** - problém so slučkou v smerovaní má označenie ako počítanie do nekonečna a spôsobuje ich všesmerové vysielanie. Informácie, ktoré sú chybné sa šíria v sieti. Ak by nebolo vytvorené ošetrenie, počet skokov by mohol byť neobmedzený a pri každom prechode smerovača by narastal. Maximálny počet skokov je určený na čísle 15. Ak slučka spôsobí 15 preskokov, bude sieť považovaná za nefunkčnú a v smerovacej tabuľke bude označená ako neplatná. [8]

2) **Rozdelenie horizontu** - táto funkcia má za úlohu obmedziť rozsah neoprávnených informácií spojené so smerovaním v sieťach s vektorom vzdialenosti. Informácie o smerovaní sa nikdy neodosielajú späť v smere, v ktorom boli prijaté. Protokol rozlišuje, z ktorého rozhrania informácie o trase pochádzajú. [8]

3) **Znehodnotenie cesty** - ďalší spôsob akým sa zabraňuje problémom s aktualizáciou a predchádza sieťovým slučkám. Pri výpadku siete smerovač znehodnotí cestu tým, že nadstaví počet skokov na číslo 16 a to má za následok, že je považovaný za nedostupný. To spôsobí, že do siete nebudú vysielané nesprávne aktualizácie o trase. Najbližší smerovač príjme znehodnotenie cesty a pošle mu naspäť znehodnotenú spätnú aktualizáciu. To spôsobí, že všetky smerovače, ktoré využívajú nefunkčnú trasu budú mať o jej nefunkčnosti informácie. [8]

4) **Odstavenie** - Má za úlohu zabrániť tomu, aby boli nefunkčné trasy predčasne obnovené v tabuľkách iných smerovačov. Je určený čas na obnovenie funkčnosti prerušenej trasy, aby sa sieť mohla stabilizovať. Smerovače tak po určitú dobu nemôžu robiť zmeny. Táto situácia najčastejšie nastáva pri sériovom spojení, kde konektivita vypadáva a následne sa obnovuje. Ak by nebola možnosť takto stabilizovať sieť, mohlo by ju aj jedno kolísanie vyradiť z prevádzky. [8]

2.1.2 Protokol RIP

RIP (Routing Information Protocol) patrí do skupiny protokolov s vektorom vzdialenosti. Je určený hlavne pre malé siete, pretože vo veľkých sieťach nepracuje efektívne a je obmedzený počtom smerovačov kvôli maximálnemu počtu skokov. Je určený na čísle 15. Pri prekročení tohto čísla sa cieľ vzdialený 16 skokov považuje za nedosiahnuteľní. Smerovacia tabuľka je posielaná všetkým aktívnym rozhraniam každých 30 sekúnd. Protokol je rozdelený na dve verzie a to RIP verzia 1 a RIP verzia 2. Verzia 1 nám umožňuje iba triedne smerovanie, čo znamená, že všetky zariadenia v danej sieti musia mať rovnakú masku podsiete. Je to spôsobené tým, že sa v smerovacej tabuľke neodosielajú aj informácie o maske podsiete. Vylepšenie priniesol protokol RIP verzie 2, ktorý odstránil tento nedostatok. Používa funkciu smerovania podľa prefixu, čo má za dôsledok, že sa nemusí používať iba rovnaká maska podsiete. Jedná sa o funkciu beztriedneho smerovania. Protokol RIP má administratívnu vzdialenosť 120. Výhodou prečo použiť protokoly RIP je fakt, že sú založené na otvorenom štandarde, čo znamená, že ho podporujú všetky smerovače. Ako nevýhody treba považovať využitie príliš veľkej časti šírky pásma, čo má za následok veľké nároky na kapacitu siete, ako aj maximálny počet skokov, ktorý je obmedzený na čísle 15. Protokoly RIP a RIPv2 majú rozdielne formáty paketov. [14]

Paket protokolu RIP, viď. obrázok 5:

Obrázok 6. Paket protokolu RIPverzie 1 [14]

- **command –** určuje, či paket žiada alebo odpovedá. Ak je požiadavkový, tak zisťuje, či smerovač poslal všetky časti smerovacej tabuľky a ak je odpoveďový, tak sa jedná buď o nevyžiadanú pravidelnú aktualizáciu, alebo odpoveď na žiadosť. Odpovede obsahujú záznamy v smerovacej tabuľke. Viacnásobné RIP protokoly sa používajú na prenos informácií veľkých smerovacích tabuliek,
- **version number –** špecifikuje, o akú verziu protokolu RIP sa jedná. Toto pole môže signalizovať rôzne potenciálne nekompatibilné verzie,
- **zero –** toto pole nie je použité v norme RFC 1058, bolo pridané pre spätnú kompatibilitu s rôznymi predštandardizovanými RIP protokolmi. Predvolená hodnota je nadstavená na nulu,
- **AFI (Address Family Identifier) –** slúži na špecifikáciu použitej adresnej rodiny. RIP je navrhnutý na prenos informácií rôznych protokolov. Každá adresná rodina má svoj identifikátor, pre IP je to číslo 2.
- **address –** určuje IP adresu pre vstup,
- **metric –** udáva, koľko sietí bolo prekročených na ceste k cieľu. Hodnota 1 až 15 skokov sú určené pre platnú cestu a 16 pre nedostupnú sieť.[14]

Paket protokolu RIPv2 viď. obrázok 7:

Obrázok 7. Paket protokolu RIPverzie 1 [14]

Niektoré časti sú rovnaké ako pri predchádzajúcej verzii a to: command, version number a metric. Ďalšie časti sú:

- **unused –** nepoužitý, hodnota je nadstavená na nulu,
- **AFI (Address Family Identifier) –** funguje rovnako ako u predchádzajúcej verzii, avšak s jednou zmenou. Ak má pole pre prvý záznam nadstavenú hodnotu 0xFFFF, zvyšok obsahuje informácie o autentifikácii,
- **route tag –** poskytuje metódu na rozlišovanie medzi interným a externým smerovaním,
- **network address -** určuje IP adresu pre vstup,
- **subnet mask –** má za úlohu definovať masku. Ak je hodnota nadstavená na nulu, maska nie je definovaná,
- **next hope –** definuje IP adresu ďalšieho skoku, kde má byť paket preposlaný.[14]

Protokol reguluje svoj výkon pomocou štyroch časovačov:

- **časovač aktualizácie trasy –** nadstavuje na smerovači interval na pravidelnú aktualizáciu. Typicky sa jedná o hodnotu 30 sekúnd, kedy sa posiela všetkým svojím susedom kópia svojej smerovacej tabuľky,
- **časovač neplatnej trasy –** určuje sa doba, ktorá musí uplynúť, aby sa trasa označila za neplatnú. Jedná sa o čas 180 sekúnd. Ak za tento čas nedostane smerovač aktualizáciu trasy, pošle všetkým susedom aktualizáciu so správou, že daná trasa nie je funkčná,
- **časovač odstavenie –** nadstaví dobu, počas ktorej sú potlačené informácie o smerovaní. Dostanú sa do takzvaného odstavného stavu potom, čo dostanú informáciu, že trasa nie je dosiahnuteľná. Smerovač čaká, kým nedostane nový aktualizačný paket s lepšou metrikou alebo nevyprší čas odstavenia, kde je nadstavená predvolená hodnota 180 sekúnd,

- **časovač vymazania trasy –** nadstaví dobu medzi označením trasy za neplatnú po odstránenie so smerovacej tabuľky. Jedná sa o časový interval 240 sekúnd. Smerovač najprv oznámi všetkým svojím susedom, že sa chystá zrušiť trasu. Hodnota časovača neplatnej trasy však musí byť menšia ako interval časovača vymazania trasy, čo má za následok, že smerovač dostane dostatočnú dobu na informovanie susedov o neplatnej trase skôr, než aktualizuje lokálnu smerovaciu tabuľku. [8]

RIP protokol slepo dôveruje informáciám, ktoré dostáva od susedných smerovačov, preto vznikla forma ochrany a to autentifikácia.

1) **Ochrana autentifikáciou:**
    - plaintext,
    - MD5 hash. [15]
2) **Aktivácia autentifikácie:**
    - vytvorenie zoznamu kľúčov (kľúčenky),
    - aktivácia formy autentifikácia na konkrétnom rozhraní,
    - aktivácia konkrétnej kľúčenky na konkrétnom rozhraní. [15]

Názvy jednotlivých kľúčeniek sa od seba môžu líšiť, avšak čísla kľúčov musia byť identické, keďže sa číslo kľúča, ktorým sa podpisuje paket vkladá do tohto paketu, aby ho mohol príjemca overiť. Kľúčom sa podpisuje každý paket na danom rozhraní a ak je pripojené na multiaccess sieť musí každý smerovač na spoločnom segmente používať rovnaký kľúč. [9]

Každý jeden kľúč v kľúčenke má dvojicu časov platnosti, a to na podpísanie odchádzajúcej správy a overenie prijatej. Ak sa v kľúčenke nachádzajú viaceré platné pre odosielanie, tak bude použitý ten s najnižším číslom. [15]

2.1.2.1 Príkazy na konfiguráciu RIPv1 a RIPv2

Príkazy na konfiguráciu zadávame v konfiguračnom móde. Pri verzii RIP musíme mať na pamäti potrebu použiť triedne adresovanie z čoho vyplýva, že maska podsiete musí byť rovnaká na všetkých zariadeniach.

- *Konfigurácia RIP a RIPv2:*

Router (config) # router rip

Router (config-router) # network [sieť] / maska sa neudáva

- *Verzia RIP:*

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

- *Zrušenie siete:*

Router (config-router) # no network [sieť]

- *Manuálne nadstavenie autosumarizácie:*

Router (config) #interface [rozhranie]

Router (config-if) # ip summary-address rip [sieť] [maska]

- *Vypnutie autosumarizácie:*

Router (config-router) # no auto-summary

- *Vytvorenie kľúčenky:*

Router (config) # key chain [meno]

Router (config-keychain) # key [číslo]

Router (config-keychain-key) # key-string [heslo]

- *Aktivácia konkrétnej autentifikácie na rozhraní:*

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

- *Aktivácia kľúčenky na rozhraní:*

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

- *Redistribúcia do OSPF*

Router(config-router)# redistribute <protocol> [proces ID] [**match** route-type] [**metric** metric-value] [**route-map** map-tag]. [15]

2.1.3 Protokol IGRP

IGRP (Interior Gateway Routing Protocol) je vytvorený firmou Cisco. Jedná sa o protokol s vektorom vzdialenosti. Každý, kto chce využívať tento protokol, musí používať smerovače firmy Cisco. Bol vytvorený hlavne kvôli chybám, ktoré mal protokol RIP. Hlavný rozdiel oproti nemu je v tom, že sa počet skokov zvýšil z 15 až na 255. Protokol taktiež pracuje s inou metrikou, a to tak, že určuje optimálnu trasu v dátovej sieti na základe dvoch variant, a to šírky pásma a oneskorenie linky. Môžu sa však použiť aj spoľahlivosť, záťaž a taktiež maximálna prenosová jednotka, aj keď sa štandardne nepoužívajú. Posiela smerovaciu tabuľku každých 90 sekúnd. Možno ho použiť aj pri veľkých sieťach a pri jeho nadstavovaní sa uvádza aj číslo autonómneho systému. Administratívna vzdialenosť je 100. V súčasnej dobe však už Cisco IGRP nepodporuje, keďže vyvinuli vylepšenú verziu a to protokol EIGRP. [8]

2.1.3.1 Príkazy na konfigurácia IGRP

Keďže sa v súčasnej dobe protokol IGRP nepoužíva a bol nahradený protokolom EIGRP je ukázaných iba pár príkazov.

- *Konfigurácia IGRP:*

Router (config) # router igrp [číslo autonómneho systému]

Router (config-router) # network [sieť]

- *Zrušenie siete:*

Router (config-router) # no network [sieť]

- *Zrušenie IGRP s autonómnym systémom:*

Router (config-router) # no router igrp [číslo autonómneho systému]. [8]

2.2 Smerovacie protokoly so stavom linky

Protokoly so stavom linky sa označujú aj ako s algoritmom najkratšej trasy. Každý smerovač vytvára tri samostatné tabuľky. V prvej tabuľke sleduje priamo pripojené susedné smerovače. V druhej sa určuje topológia celej siete a tretia je smerovacia tabuľka. Smerovače pracujúce s protokolom stavu linky majú o celej sieti omnoho väčšie informácie ako smerovače s protokolom vektora vzdialenosti. [8]

2.2.1 Protokol OSPF

Protokol OSPF (Open Shortest Path First) patrí do kategórie s otvoreným štandardom, a preto sa môže používať na všetkých sieťových zariadeniach bez rozdielu značky. Oproti EIGRP má teda výhodu v tom, že je voľne šíriteľný a nie je vyhradený iba pre smerovače firmy CISCO. Patrí do skupiny smerovacích protokolov stavu linky. Je založený na Dijkstrovom algoritme, ktorý najskôr vytvorí strom najkratších ciest a následne sa do smerovacej tabuľky umiestnia optimálne trasy. V súčasnosti sa používajú dve verzie, a to OSPFv2 pre IPv4 a OSPFv3 pre IPv6. Tento protokol svojimi vlastnosťami možno použiť vo veľkých rozsiahlych sieťach kvôli deleniu na AS a oblasti. Toto rozdelenie sa nazýva hierarchická štruktúra a dôvody, ktoré k nej vedú sú zníženie réžie smerovania, urýchlenie konvergencie a obmedzenie nestability siete vďaka jej rozdeleniu na jednotlivé oblasti. Protokol OSPF musí mať oblasť nula, na ktorú sa pripájajú ostatné smerovače, jedná sa o takzvané chrbtové spojenie. Protokol pracuje v rámci autonómneho systému a taktiež dokáže spojovať viac autonómnych systémov. Smerovač, ktorý spojuje viac systémov sa nazýva hraničný smerovač autonómneho systému. Protokol OSPF nepoužíva štandardný typ masky podsiete, ale používa takzvanú wildcare masku. Podporuje variabilné podsieťovanie. [8,16]

2.2.1.1 Pojmy v OSPF

Priblíženie základných pojmov:

- **linka –** je rozhranie siete alebo smerovača,
- **ID smerovača –** je adresa IP, ktorá slúži na jeho identifikáciu. ID smerovača je vyberané ako najvyššia IP adresa zo všetkých nakonfigurovaných rozhraní a pokiaľ nie sú rozhranie nakonfigurované, tak zvolí protokol najvyššiu adresu zo všetkých fyzických rozhraní, ktoré sú aktívne. Jedná sa o 4 bajtové číslo,

- **priľahlosť –** dovoľuje priamu výmenu aktualizácií trás medzi dvoma smerovačmi. Protokol OSPF zdieľa trasy iba so susedmi, s ktorými nadstavil vzťah priľahlosti. Nemusia to byť všetci susedia, závisí to na type sieti a konfigurácii smerovača.
- **protokol Hello –** má za úlohu zaistiť dynamické zisťovanie susedov a udržovať vzťahy medzi nimi. Pakety sú odosielané na adresu 224.0.0.5,
- **paket LSA (Link State Advertisment) –** je dátový paket, ktorý v sebe obsahuje informácie o stave linky a smerovaní. Tento paket si vymieňajú len smerovače, ktoré medzi sebou ustanovili vzťah priľahlosti,
- **databáza susedov –** jedná sa o zoznam všetkých smerovačov, ktoré boli zistené protokolom Hello. Uchovávajú sa v nej podrobné informácie o každom smerovači,
- **topologická databáza** - v tejto databáze sú uložené informácie o všetkých paketoch LSA, ktoré boli pre danú oblasť prijaté. Informácie z tejto databázy sa používajú ako vstup Dijkstrovho algoritmu pre počítanie najkratšej ceste ku každej sieti. [8]

2.2.1.2 Výpočet stromu najkratšej cesty

Algoritmus najkratšej cesty počíta najlepšiu trasu do každej siete v rovnakej oblasti a je založený na dátach z topologickej databázy. Každý smerovač vytvára v oblasti takzvaný strom, ktorý sa podobá rodokmeňu. Sú to vlastne najkratšie cesty, pomocou ktorých smerovač vkladá do smerovacích tabuliek trasy. Strom obsahuje iba siete, ktoré sa nachádzajú v rovnakej oblasti. Ak sú v rôznych oblastiach, tak sú pre každú zostavené samostatné stromy. Protokol OSPF používa na výpočet najkratšej trasy metriku zvanú **náklady (cost)**. Náklady na cestu sú dané súčtom nákladov výstupných rozhraní pozdĺž celej cesty. [8]

2.2.1.3 Elegantný reštart

Protokol OSPF v stabilnom stave dokáže rýchlo reagovať na zmeny v smerovaní a rekonvergencii, čo robí z neho veľmi silný protokol. A nielen v stabilnom stave, ale aj v prípade, že niečo nie je v poriadku. Ak nastane reštart softwaru OSP, môže nastať problém s výskytom slučiek v smerovaní, preto sa zaviedol takzvaný elegantný reštart, ktorý bol štandardizovaný v RFC 3623.

Aj keď sa vykonáva reštart je možné pokračovať v zasielaní po splnení určitých podmienok a to:

- smerovač musí pri reštarte OSPF uvedomiť susedov pomocou paketu grace LSA,
- databáza LSA zostáva v priebehu reštartu stabilná,
- tento reštart podporujú všetci susedia a majú ho zapnutý v konfigurácii,
- reštart prebehne po zadanom intervale grace period,
- v priebehu reštartu musia susedné smerovače pracovať v pomocnom režime. [17]

2.2.1.4 Autentifikácia

Na garantovanie dôvery smerovačov používa protokol OSPF dva druhy autentifikácie, a to MD5 a plaintext. Jedná sa o rovnaké druhy autentifikácie, ktoré sa používajú pri protokole RIPv2. [16]

2.2.1.5 Konfigurácia OSPF

- *Nadstavenie OSPF:*

Router(config)# router ospf [číslo procesu]

Router(config-router)# network [sieť] [wildcard maska] oblasť [číslo oblasti]

- *Zapne autentifikáciu medzi smerovačmi na danom rozhraní:*

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

- *Nastaví heslo pre autentifikáciu medzi smerovačmi na danom rozhraní:*

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

- *Nastavenie priority:*

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

- *Nastavenie ceny cesty:*

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 smerovač považovaný za stratený:*

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

- *Konfigurácia plaintext autentifikácie:*

Router(config-if)#ip ospf authentication-key [heslo] – nadstaví heslo pre plaintext

Router(config-router)#area [číslo oblasti] authentication – druh autentifikácie pre oblasť

Router(config-if)# ip ospf authentication [null] – prepíše druh autentifikácie na konkrétnom rozhraní. Null deaktivuje autentifikáciu a bez argumentu sa aktivuje.

- *Konfigurácia MD5 autentifikácie:*

Router(config)#interface <typ> <číslo>

Router(config-if)#ip ospf message-digest-key <kľúč-id> md5 <encryption-typ> <heslo>

Router(config-if)#exit

Router(config)#router ospf 1

Router(config-router)#area <oblasť-id> authentication message-digest

- *Redistribúcia do OSPF*

Router(config-router)# redistribute protocol [proces ID] [**metric** metric-value] [**metric-type** type-value] [**route-map** map-tag] [**subnets**] [**tag** tag-values]. [8,16,18]

2.3 Smerovacie protokoly hybridné

Hybridné protokoly sa využívajú, ak je potrebné vyhovieť požiadavkám konkrétnej situácie tak, aby spĺňali potreby každej organizácie. Každá konfigurácia je odlišná, a preto sa využívajú aspekty protokolov s vektorom vzdialenosti a stavom linky. Medzi hybridné protokoly môžeme zaradiť protokol EIGRP. [8]

2.3.1 Protokol EIGRP

EIGRP (Enchanced IGRP). Jedná sa o vylepšený protokol IGRP od spoločnosti Cisco. Je založený na princípe autonómneho systému. V aktualizácii ciest však protokol oproti svojmu predchodcovi zahŕňa aj masku podsiete. Protokol preto podporuje aj variabilné podsieťovanie VLSM. Radí sa medzi hybridné protokoly, pretože má vlastnosti aj ako protokol s vektorom vzdialenosti, tak aj protokol so stavom linky. Odosiela aktualizácie s vektorom vzdialenosti, čiže obsahujú informácie o sieťach spolu s nákladmi a ich dosiahnutie a má tiež vlastnosti protokolu so stavom linky, kde pri spustení synchronizuje smerovacie tabuľky medzi smerovačmi, ktoré so sebou susedia a potom odosiela aktualizácie až pri zmene topológie. Je preto vhodný do veľmi rozsiahlych sietí. Maximálny počet skokov je 255. Podporuje aj protokol IPv6. Efektívne zisťuje nových susedov a vyberá najlepšiu trasu pomocou difúzneho aktualizačného algoritmu. Smerovače budú susedia, ak sú v rovnakom autonómnom systéme, IP adresy rozhraní sú z tej istej podsiete a majú rovnaké K hodnoty. [8,19]

Aby sa mohli smerovače s protokolom EIGRP začať vymieňať svoje trasy, tak sa najprv musia stať susedmi. Aby sa tak stalo musia byť splnené tri podmienky, a to:

- *prijatie správy Hello alebo ACK,*
- *zhoda čísiel AS,*
- *identické metriky.* [8]

Protokoly so stavom linky obvykle neodosielajú aktualizácie pravidelne, avšak musí sa zaistiť, aby sa po pripojení nového zariadenia dozvedeli jeho susedia. Na toto nám slúži Hello paket. Tieto pakety sú vysielané trvale, aby zostali vzťahy medzi susednými smerovačmi zachovalé. Smerovače, ktoré nie sú v rovnakom autonómnom systéme nezdielajú informácie o smerovaní a nestavajú sa z nich susedia. Táto vlastnosť je veľmi výhodná vo veľkých sieťach, pretože sa tak obmedzuje objem informácií o trasách, ktoré sa šíria v jednotlivých autonómnych systémoch. Medzi jednotlivými autonómnymi systémami je potrebné zabezpečiť redistribúciu ručne. Celú smerovaciu tabuľku si smerovače posielajú iba v prípade, že do siete pribudlo nové zariadenie, aj to iba medzi susedmi. Ak sa každý z nich zoznámi s trasami suseda ďalej sa budú šíriť iba zmeny smerovacích tabuliek. Smerovač po prijatí trasy od svojich susedov uloží aktualizáciu do tabuľky lokálnej topológie. [8,17]

Smerovač pracujúci na princípe EIGRP udržuje 3 tabuľky:

- **tabuľka susedov** – má na starosti uchovávať informácie o susedných smerovačoch. Ak sa dozvie o novom susednom smerovači uloží si jeho adresu a rozhranie. Táto tabuľka sa uloží do pamäte RAM,
- **topologická tabuľka –** má za úlohu uchovávať všetky cieľové adresy spolu so zoznamom susedných smerovačov, ktoré ciele zverejnili a ukladá sa zverejnená metrika, ktorá pochádza zo smerovacích tabuliek susedného smerovača. Túto tabuľku využíva difúzny aktualizačný algoritmus. Tabuľka v sebe ukladá aj šesť pravdepodobných následníkov. Jedná sa o záložne trasy,
- **smerovacia tabuľka** – udržiava najlepšiu cestu do cieľa a má v sebe uložený aj následník. Je to jedna zo šiestych záložných trás z topologickej tabuľky ktorá má najlepšiu metriku. [20]

2.3.1.1 Protokol RTP

RTP (Reliable Transport Protocol) je firemný protokol spoločnosti Cisco, pomocou ktorého protokol EIGRP zaisťuje prenos medzi kompatibilnými smerovačmi. Pri viacsmerovom vysielaní používa protokol EIGRP adresu triedy D, 224.0.0.10 a udržuje zoznam susedných smerovačov, ktorí na ňu odpovedali. Ak niektorý zo susedov neodpovie, tak smerovač začne posielať jednosmerové vysielanie s rovnakými dátami a to až 16 krát. Ak ani na jednu žiadosť neodpovie, považuje svojho suseda za nefunkčného. [8]

2.3.1.2 Difúzny aktualizačný algoritmus DUAL

Tento algoritmus používa protokol EIGRP na udržovanie optimálnej cesty do vzdialenej siete a poskytuje nasledujúce funkcie:

- určenie záložnej trasy,
- VLSM podsieťovanie,
- obnovenie dynamických ciest,
- pýta sa na alternatívnu cestu, ak nemôže nájsť žiadnu trasu. [8]

Vďaka tomuto algoritmu má protokol EIGRP najrýchlejšiu konvergenciu ciest z pomedzi všetkých protokolov. Majú to na svedomí dva faktory a to, že smerovač udržuje kópie ciest všetkých susedných smerovačov, čo v prípade výpadku optimálnej trasy rieši preskúmaním

a vybraním náhradnej siete z tabuľky topológií a za druhé, ak neexistuje dobrá náhradná cesta, tak o ňu protokol EIGRP požiada susedné smerovače. [8]

2.3.1.3 Metrika EIGRP

Protokol EIGRP sa vyznačuje oproti iným tým, že namiesto jedného parametru využíva pri hľadaní optimálnej trasy kombináciu štyroch parametrov a to:

- šírka pásma,
- oneskorenie,
- záťaž linky,
- spoľahlivosť. [8]

Na výpočet metriky sa používa vzorec:

M= [K1 * šírka pásma + ((K2 * šírka pásma) / (256 – záťaž linky)) + K3 * oneskorenie].

Hodnoty K sú konštantné:

K = (K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0).[20]

2.3.1.4 Druhy EIGRP paketov

- **Update –** jeho úlohou je prenášať smerovaciu informáciu. Vždy ho dostanú len smerovače, ktorých sa informácia týka a môžu u príjemcu spustiť difúzny výpočet.
- **Query –** informácie sa posielajú všesmerovo a sú potvrdzované. Pomocou tohto paketu sa spúšťa alebo šíri difúzny výpočet, ktorý hľadá najkratšiu cestu do cieľa.
- **Reply -** tento paket sa posiela jednosmerovým vysielaním tomu smerovaču, ktorý sa pýtal. Je to odpoveď smerovača na Query paket. Prijatie tohto paketu zastavuje difúzny výpočet.
- **Ack-** sú to potvrdzovacie pakety na potvrdenie update, query a reply, adresované vždy jednosmerovo.
- **Hello –** majú za úlohu lokalizovať susedné smerovače. Vymieňajú čísla autonómnych systémov, timeout-ov a autentifikácií. Posielajú sa na IP adresu 224.0.0.10 a sú nepotvrdzované. [20]

2.3.1.5 Autentifikácia

Protokol EIGRP na rozdiel od RIPv2 podporuje iba MD5 autentifikáciu, kde obsah paketov nie je šifrovaný a neprenáša sa ani heslo. Prenáša sa však MD5 hash počítaný z čísla kľúča a hesla. Konfigurácia je úplne rovnaká ako u protokolu RIPv2, takže kľúče ako aj ich čísla musia byť zhodné. V kľúčenke je možné mať viaceré kľúče a ich platnosť je definovaná ľubovoľne podľa administrátora. Smerovač, ktorý odosiela, použije na počítanie hashu prvý platný kľúč od najnižšieho čísla a smerovač, ktorý ho prijíma, skúša všetky kľúče z kľúčenky až pokiaľ nenájde zhodu. [20]

2.3.1.6 Príkazy na konfigurácia EIGRP

- *Konfigurácia EIGRP:*

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

Router (config-router) # network [sieť]

- *Zapnutie a vypnutie autosumarizácie:*

Router (config-router) # auto-summary

Router (config-router) # no auto-summary

- *Autosumarizácia na rozhraní:*

Router (config-if) # ip summary-address eigrp [autonómny systém] [IP] [maska]

- *Zapnutie autentifikácie MD5 kľúčom:*

Router(config-if)# ip authentication mode eigrp [autonómny systém] md5

Router(config-if)# ip authentication key-chain eigrp [autonómny systém] [kľúč]

- *Konfigurácia kľúča:*

Router(config)# key chain [kľúč] md5

Router(config-keychain)# key [číslo]

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

- *Časová platnosť kľúča:*

Router(config-keychain-key)# accept-lifetime start-time {nekonečný | koncový čas | počet sekúnd}

- *Nadstavenie intervalu medzi Hallo paketmi:*

Router(config-if)# ip hello-interval eigrp [autonómny systém] [čas v sekundách]

- *Nadstavenie šírky pásma na danom rozhraní:*

router(config)#interface [typ] [číslo]

router(config-if)#bandwidth [kilobity]

- *Vyrovnávanie záťaže:*

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

Router (config-router) # maximum patch [1-6]

- *Nadstavenie počtu skokov:*

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

Router (config-router) # metric maximum-hops [1-255]

- *Redistribúcia do EIGRP:*

Router(config-router)# redistribute <protocol> [proces ID] [**match** route-type] [**metric** metric-value] [**route-map** map-tag]. [8,20]

2.4 Zhrnutie smerovacích protokolov

Každý smerovací protokol má určité výhody a nevýhody, a preto si treba vždy dobre zváži, aká smerovacia politika bude zvolená.

Z popísaných vnútorných protokolov sa najviac používajú RIPv2, OSPF a EIGRP. Zvyšné dva, RIPv1 a IGRP už nie sú využívané až tak často. Protokol RIPv2 s vektorom vzdialenosti je určený do malých sietí, kde je maximálny počet skokov 15. Ak sa toto číslo prekročí smerovač je nedosiahnuteľní. Používa variabilné podsieťovanie. Ako nevýhoda je hlavne pomalá konvergencia. Opak je protokol OSPF, ktorý pracuje na princípe stavu linky a nepoužíva metriku počtu skokov ale cenu linky, takže nie je obmedzený počtom smerovačov. Preto môže byť využívaný pre rozsiahle siete. Podporuje variabilné podsieťovanie a konvergencia je rýchla. Veľká výhoda tohto protokolu je, že je možné jeho použitie u smerovačov všetkých značiek a nie je zameraný na jednu konkrétnu na rozdiel od jeho veľkého konkurenta, protokolu EIGRP, ktorý vyvinula spoločnosť Cisco a jeho využitie je možné iba na smerovačoch tejto značky. Jedná sa o kombinovaný protokol, takže pracuje na princípe vektoru vzdialenosti, kde je oproti RIPv2 zvýšený počet skokov až na 255, tak aj na princípe stavu linky, kde sa používa metrika cena linky. Podporuje variabilné podsieťovanie. Použitie je možné aj pre rozsiahle siete a má veľmi rýchlu konvergenciu. Zhrnutie sa nachádza v tabuľke 7. [21]

Tabuľka 7. Porovnanie najpoužívanejších smerovacích protokolov. [21]

Charakteristika	RIPv1	RIPv2	EIGRP	OSPF
Vektor vzdialenosti	áno	áno	áno	nie
Stav linky	nie	nie	nie	áno
Beztriedne adresovanie	nie	áno	áno	áno
VLSM	nie	áno	áno	áno
Automatická sumarizácia	áno	áno	áno	nie
Manuálna sumarizácia	nie	áno	áno	áno
Hierarchická topológia	nie	nie	nie	áno
Veľkosť siete	malá	malá	veľká	veľká
Metrika	skoky	skoky	zložená metrika	cena
Rýchlosť konvergencie	pomalá	pomalá	veľmi rýchla	rýchla

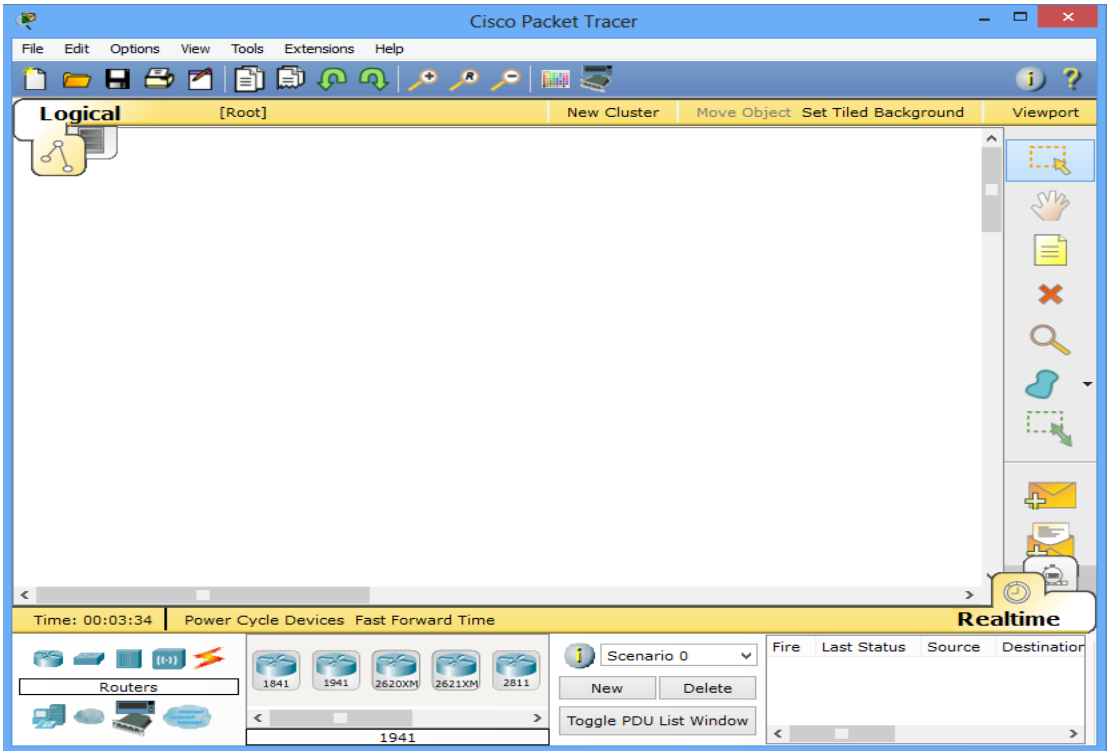
II. PRAKTICKÁ ČÁST

3 SIMULÁCIA UKÁŽKOVÝCH TOPOLÓGIÍ

Po zoznámení sa s teoretickými vlastnosťami vybraných smerovacích protokolov je potrebné na ukážkových topológiách odskúšať ich vlastnosti a funkčnosť. Ako simulačné prostredie je použitý Cisco Packet Tracer verzia 6.0.1.0011.

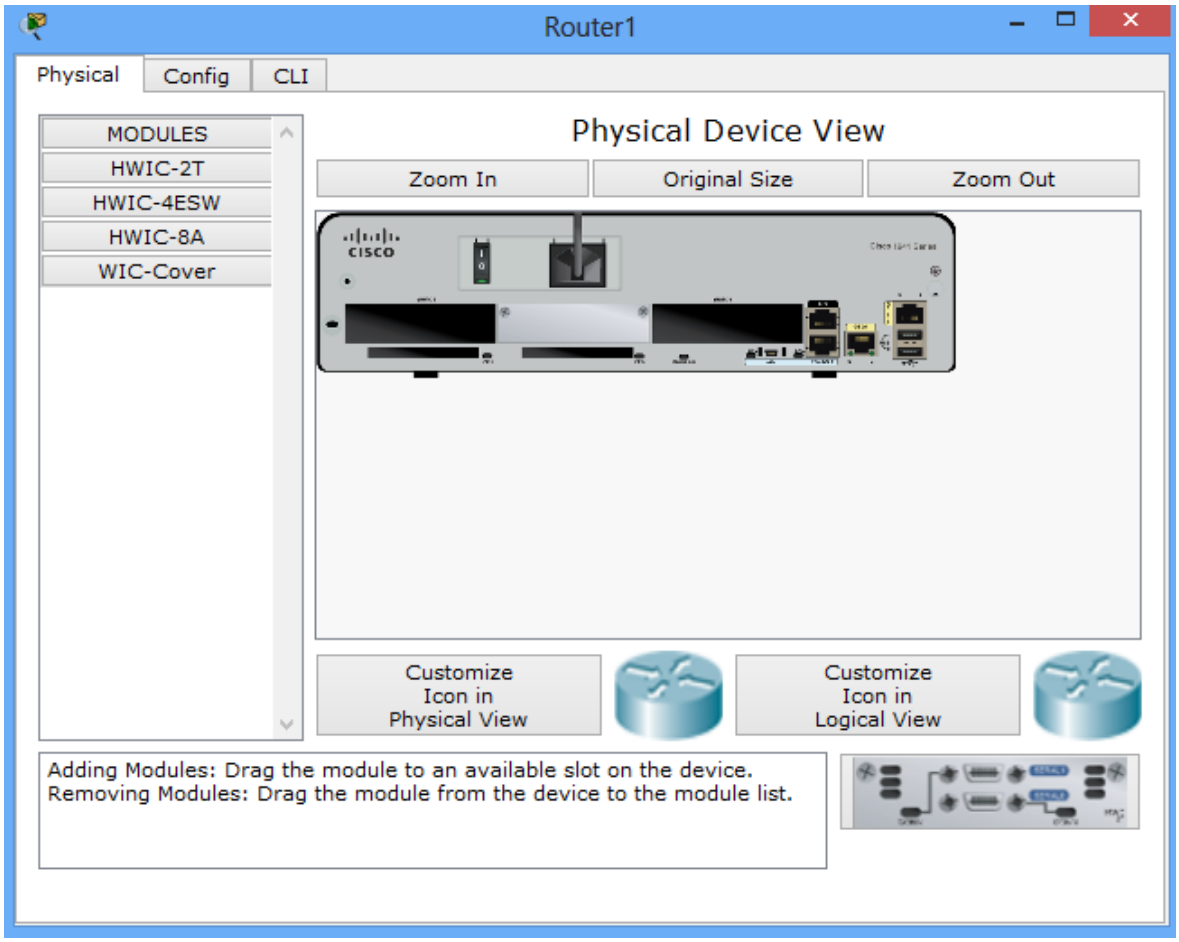
3.1 Zoznámenie sa s prostredím Cisco Packet Tracer

Cisco Packet Tracer je simulačné prostredie vyvinuté firmou Cisco a je možné s jeho pomocou odskúšať funkčnosť navrhnutej siete. Ako je vidieť na obrázku 8, prostredie je veľmi prehľadné. Skladá sa zo štyroch častí a to vrchnej, bočnej a spodnej lišty. Štvrtá časť je biela plocha, na ktorú sa vyberajú komponenty potrebné na simuláciu. Horná lišta obsahuje základne funkcie ako vybranie nového projektu, otvorenie staršieho, uloženie, tlač, kopírovanie, priblíženie a ďalšie možnosti. Na pravej lište sa nachádzajú ikony výber, posúvanie, písanie poznámok, vymazanie, prehliadanie, kreslenie útvarov, úprava útvarov a veľmi podstatné sú ikony v tvare obálky ktoré slúžia na odskúšanie funkčnosti nakonfigurovanej siete pomocou dátového paketu PDU. V spodnej lište je na ľavej strane výber komponentov a kabeláže. V strednej časti sú jednotlivé typy vybraného komponentu a v pravej časti je možne sledovať, či bol prenos PDU úspešný alebo neúspešný.



Obrázok 8. Užívateľské prostredie programu Cisco Packet Tracer

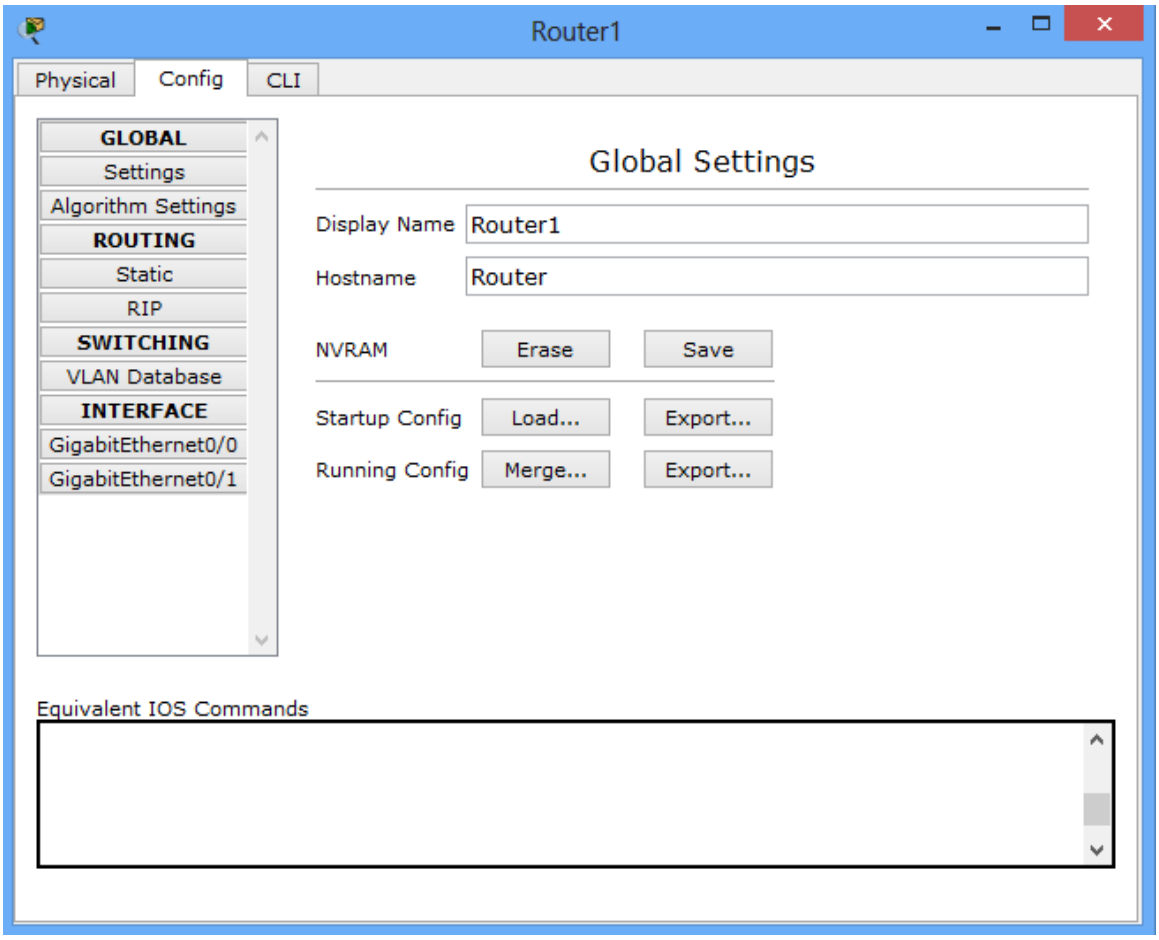
Po vybratí ľubovoľného smerovača a kliknutím naň kurzorom myši sa zobrazí nasledujúce prostredie, viď. obrázok 9.



Obrázok 9. Grafické prostredie smerovača, záložka Physical

Vo vrchnej časti sa nachádzajú tri záložky a to Physical, Config a CLI. Primárne sa zobrazí prostredie záložky Physical. Tu je vidieť, ako vyzerá vybraný typ smerovača v skutočnosti. Nachádzajú sa tu jednotlivé porty a taktiež vypínač. V ľavej lište sú umiestnené rozširujúce moduly s prídavnými portami.

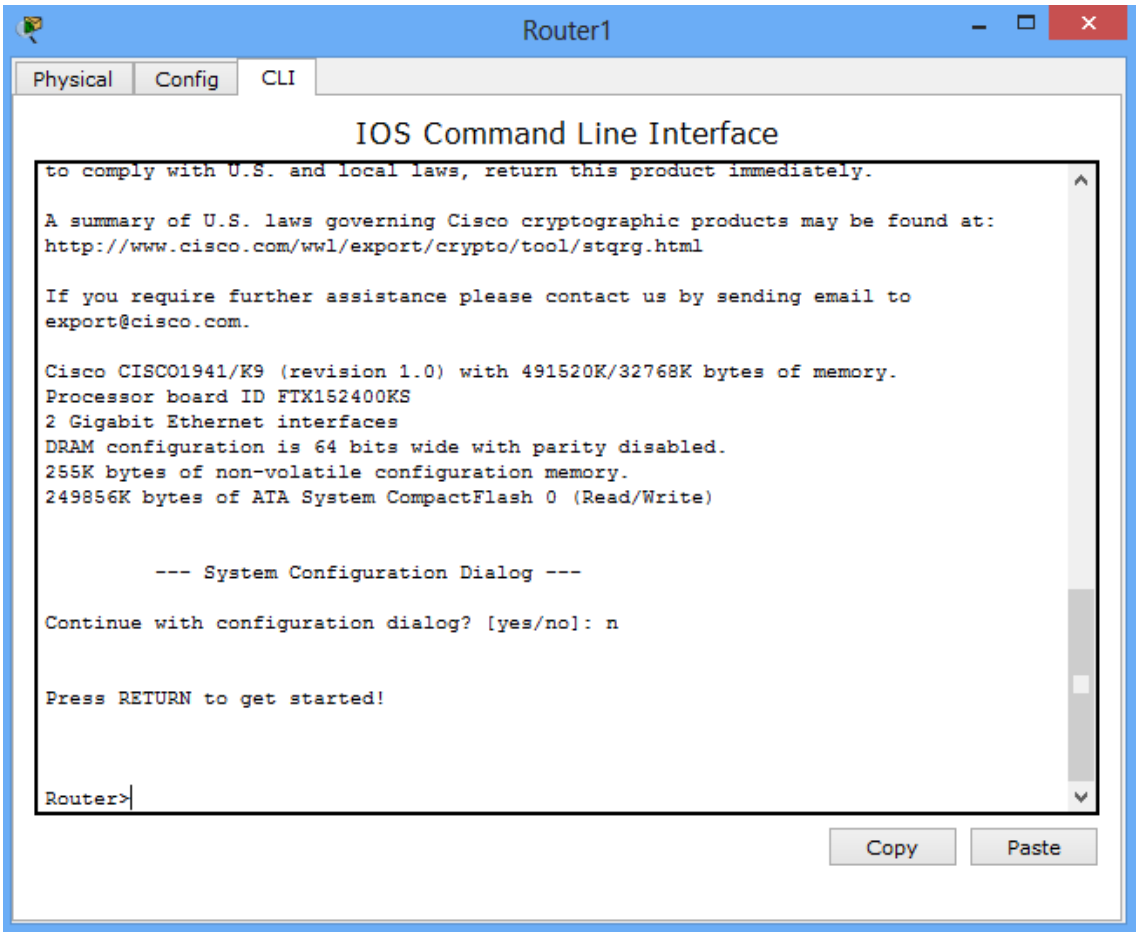
Ako druhá v poradí je záložka Config, viď. obrázok 10.



Obrázok 10. Grafické prostredie smerovača, záložka Config

Jedná sa o grafické prostredie, pomocou ktorého sa dajú nakonfigurovať základné funkcie smerovača. Je určené pre začínajúcich užívateľov, ktorí sa zoznamujú s konfiguráciou. Je tu možnosť vybrať meno, vymazať alebo uložiť konfiguráciu. Nadstaviť smerovanie pomocou statického smerovania, poprípade protokolu RIP a nadstavenie IP adresy a masky na rozhraní.

Ako tretia a najdôležitejšia časť je záložka CLI(Command Line Interface), ktorá dokonale simuluje prostredie pri konfigurácii skutočného smerovača, viď. obrázok 11.



Obrázok 11. Grafické prostredie smerovača, záložka CLI

Toto prostredie dokáže až na pár príkazov, ktoré fungujú iba na skutočnom smerovači presne nasimulovať potrebnú konfiguráciu bez potreby kupovať drahý hardware. Je vytvorené na pochopenie a odskúšanie topológií rôzneho druhu.

Cisco IOS obsahuje 3 rôzne módy, v ktorých má užívateľ povolené rôzne funkcie.

Ako prvý je **používateľský mód,** ktorý má za názvom smerovača znak >,

Napríklad: Router>.

Obsahuje iba obmedzený počet príkazov.

Ako druhý je **privilegovaný mód.** Na vstup je potrebné zadať príkaz **enable**. Zadáva sa v používateľskom mód a to nasledovne.

Router> enable

Router#

Privilegovaný mód má nasledujúci znak **#**. Prístup do tohto módu je potrebné zabezpečiť heslom, pretože už obsahuje veľké množstvo príkazov. V tomto režime sa ešte nedá upravovať konfigurácia. Na to slúži tretí mód, ktorý sa nazýva **konfiguračný**. Do neho dá dostať z privilegovaného módu príkazom **configure terminal,** poprípade aj skratkou **config t**.

Router > enable

Router #configure terminal

Router (config) #

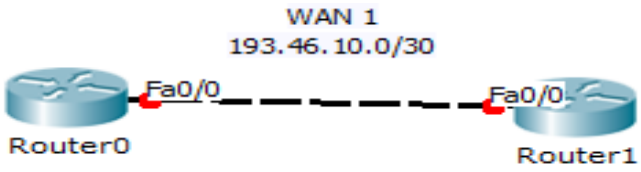
Jednotlivé módy bude možné lepšie pochopiť pri samotnej konfigurácii.

3.2 Konfigurácia

Na konfiguráciu budú použité ukážkové topológie, na ktorých budú odsimulované smerovacie protokoly RIP, RIPv2, OSPF a EIGRP. Protokol IGRP už nie je možné na smerovačoch spustiť, pretože nie je podporovaný. Na začiatok je však potrebné ukázať základnú konfiguráciu smerovačov, ktorá by mala byť nakonfigurovaná vždy kvôli bezpečnosti. Jedná sa hlavne o nadstavenie hesiel a rozhraní. Kompletné konfigurácie, ktoré chýbajú pri niektorých zadaniach sa nachádzajú v prílohe P I, na CD.

3.2.1 Základná konfigurácia smerovača

Pred tým, ako bude na smerovači použitý vybraný protokol je potrebné nakonfigurovanie mien, hesiel a IP adries portov. Vytvorené je jednoduché zapojenie dvoch smerovačov viď. obrázok 12 a následná základná konfigurácia v tabuľke 8.



Obrázok 12. Základná konfigurácia

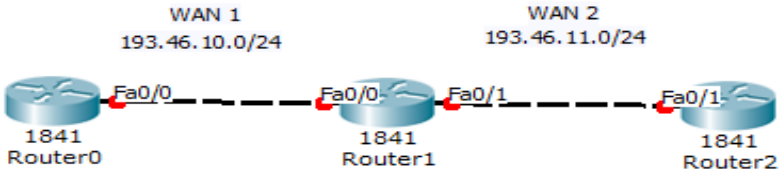
Tabuľka 8. Základná konfigurácia smerovačov Router0 a Router1

Príkazy	Router0	Router1
privilegovaný mód	Router>enable	Router>enable
konfiguračný mód	Router#config t	Router#config t
nadstavenie mena	Router(config)#hostname skola	Router(config)#hostname dom
nadstavenie hesla pre privilegovaný mód, md5 hash	skola(config)#enable secret cisco	dom(config)#enable secret cisco
nadstavenie hesla pre telnet	skola(config)#line vty 0 4	dom(config)#line vty 0 4
	skola(config-line)#password class	dom(config-line)#password class
	skola(config-line)#login	dom(config-line)#login
odchod z rozhrania	skola(config-line)#exit	dom(config-line)#exit
nadstavenie hesla pre konzolu	skola(config)#line con 0	dom(config)#line con 0
	skola(config-line)#password class	dom(config-line)#password class
	skola(config-line)#login	dom(config-line)#login
odchod z rozhrania	skola(config-line)#exit	dom(config-line)#exit
nadstavenie hesla pre AUX port	skola(config)#line aux 0	dom(config)#line aux 0
	skola(config-line)#password class	dom(config-line)#password class
	skola(config-line)#login	dom(config-line)#login
odchod z rozhrania	skola(config-line)#exit	dom(config-line)#exit
zahashovanie hesiel pomocou md5	skola(config)#service password-encryption	dom(config)#service password-encryption
nadstavenie IP adresy a masky na rozhraní	skola(config)#interface fastEthernet 0/0	dom(config)#interface fastEthernet 0/0
	skola(config-if)#ip address 193.46.10.1 255.255.255.252	dom(config-if)#ip address 193.46.10.2 255.255.255.252
zapnutie rozhranie	skola(config-if)#no shutdown	dom(config-if)#no shutdown

Základná konfigurácia bola úspešne nakonfigurovaná. Jej hlavnou úlohou bolo zaheslovanie a nadstavenie IP adries a másk rozhraní. Na smerovačoch však ešte nebol nadstavený žiadny zo smerovacích protokolov. To prichádza na radu v nasledujúcej časti.

3.2.2 Protokol RIP

Ako prvý bude nakonfigurovaný protokol RIP. Jedná sa o staršiu verziu, ktorá podporuje iba triedne podsieťovanie. Vzorové zapojenie je zobrazené na obrázku 13.



Obrázok 13. Ukážkové zapojenie pre RIPv1

Ako prvý krok je vytvorenie základnej konfigurácie.

Router0

Router>enable

Router#config t

Router(config)#hostname smerovac0

smerovac0(config)#enable secret cisco

smerovac0(config)#line vty 0 4

smerovac0(config-line)#password class

smerovac0(config-line)#login

smerovac0(config-line)#exit

smerovac0(config)#line con 0

smerovac0(config-line)#password class

smerovac0(config-line)#login

smerovac0(config-line)#exit

smerovac0(config)#line aux 0

smerovac0(config-line)#password class

smerovac0(config-line)#login

smerovac0(config-line)#exit

smerovac0(config)#service password-encryption

Router1

Router>enable

Router#config t

Router(config)#hostname smerovac1

smerovac1(config)#enable secret Cisco

smerovac1(config)#line vty 0 4

smerovac1(config-line)#password class

smerovac1(config-line)#login

smerovac1(config-line)#exit

smerovac1(config)#line con 0

smerovac1(config-line)#password class

smerovac1(config-line)#login

smerovac1(config-line)#exit

smerovac1(config)#line aux 0

smerovac1(config-line)#password class

smerovac1(config-line)#login

smerovac1(config-line)#exit

smerovac1(config)#service password-encryption

Router2

Router>enable

Router#config t

Router(config)#hostname smerovac2

smerovac2(config)#enable secret cisco

smerovac2(config)#line vty 0 4

smerovac2(config-line)#password class

smerovac2(config-line)#login

smerovac2(config-line)#exit

smerovac2(config)#line con 0

smerovac2(config-line)#password class

smerovac2(config-line)#login

smerovac2(config-line)#exit

smerovac2(config)#line aux 0

smerovac2(config-line)#password class

smerovac2(config-line)#login

smerovac2(config-line)#exit

smerovac2(config)#service password-encryption

Ako druhý krok je nakonfigurovanie rozhraní jednotlivých smerovačov.

Router0

smerovac0(config)#interface fastEthernet 0/0

smerovac0(config-if)#ip address 193.46.10.1 255.255.255.0

smerovac0(config-if)#no shutdown

smerovac0(config-if)#exit

Router1

smerovac1(config)#interface fastEthernet 0/0

smerovac1(config-if)#ip address 193.46.10.2 255.255.255.0

smerovac1(config-if)#no shutdown

smerovac1(config-if)#exit

smerovac1(config)#interface fastEthernet 0/1

smerovac1(config-if)#ip address 193.46.11.1 255.255.255.0

smerovac1(config-if)#no shutdown

smerovac1(config-if)#exit

Router2

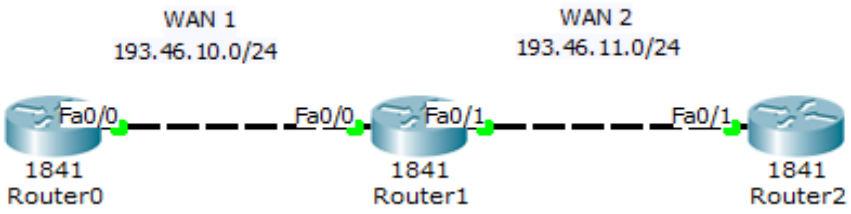
smerovac2(config)#interface fastEthernet 0/1

smerovac2(config-if)#ip address 193.46.11.2 255.255.255.0

smerovac2(config-if)#no shutdown

smerovac2(config-if)#exit

Ako vidieť na obrázku 14, porty sú nakonfigurované čo signalizuje ich zelená farba.



Obrázok 14. Nakonfigurované porty

Ako tretí a posledný krok je spustenie a nadstavenie samotného protokolu RIPv1.

Router0

smerovac0(config)#router rip

smerovac0(config-router)#version 1

smerovac0(config-router)#network 193.46.10.0

smerovac0(config-router)#no auto-summary

smerovac0(config-router)#exit

Router1

smerovac1(config)#router rip

smerovac1(config-router)#version 1

smerovac1(config-router)#network 193.46.10.0

smerovac1(config-router)#network 193.46.11.0

smerovac1(config-router)#no auto-summary

smerovac1(config-router)#exit

Router2

smerovac2(config)#router rip

smerovac2(config-router)#version 1

smerovac2(config-router)#network 193.46.11.0

smerovac2(config-router)#no auto-summary

smerovac2(config-router)#exit

Zapojenie s protokolom RIPv1 bolo úspešne odskúšané. Paket zo smerovača Router0 prišiel na smerovač Router2 a opačne, o čom svedčí aj výstup z Cisco Packet Tracera, viď. obrázok 15.

Fire	Last Status	Source	Destination	Type
	Successful	Router2	Router0	ICMP
	Successful	Router0	Router2	ICMP

Obrázok 15 – Funkčnosť zapojenia

Takisto bolo spojenie potvrdené aj príkazom ping. Ten sa spúšťa v privilegovanom móde a po zadaní IP adresy portu zobrazí koľko paketov bolo úspešne prijatých viď. obrázok 16.

```
smerovac2#ping
Protocol [ip]:
Target IP address: 193.46.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.46.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Obrázok 16. Použitie príkazu ping na odskúšanie spojenia

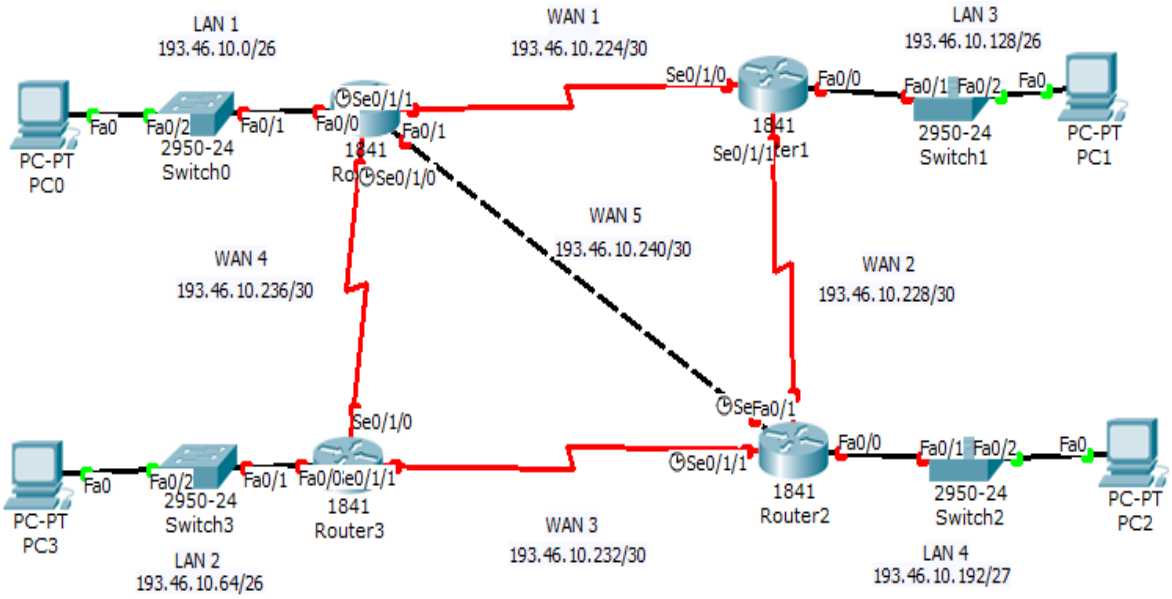
Protokol RIPv1 ma jednoduchú konfiguráciu. Treba si hlavne uvedomiť, že podporuje iba triedne podsieťovanie. Je určený do malých sietí a v súčasnosti je skôr využívaná jeho novšia verzia a to RIPv2.

3.2.3 Protokol RIPv2

Jedná sa o vylepšenú verziu protokolu RIP. Najväčšia výhoda oproti jeho predchodcovi je možnosť použitia variabilného podsieťovania. Keďže sa jedná o používanejšiu verziu zapojenie už je zložitejšie, a taktiež je nasimulovaná aj najväčšia slabina a to počet skokov, ktorý je obmedzený na číslo 15, a ďalej už komunikácia nie je možná.

Vo všetkých ďalších zapojeniach bude vynechaná základná konfigurácia mien a hesiel, keďže sa jedná vždy o rovnaký proces. Simulácie budú skôr zamerané na jednotlivé smerovacie protokoly.

Prvé zapojenie pomocou protokolu RIPv2 je tvorené štvoricou smerovačov, prepínačov a PC. Obsahuje päť WAN a štyri LAN siete ako je vidieť na obrázku 17.



Obrázok 17 - Ukážkové zapojenie pre RIPv2

Keďže zapojenie obsahuje sériové rozhranie musí sa na rozhraní DCE (rozhranie s hodinami), nadstaviť clock rate. Jedná sa o hodinový signál, ktorý synchronizuje komunikáciu. Má za úlohu spúšťať časovač a definuje rýchlosť. [19]

Konfigurácia je nasledovná: Router(config-if)#clock rate <hodnota>, (1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000). [19]

Ako prvý krok je potrebné nadstaviť každému rozhraniu smerovača, ktoré bude využívané IP adresu, masku a pri sériovom rozhraní DCE aj clock rate .

Router0

Router(config)#interface serial 0/1/1

Router(config-if)#ip address 193.46.10.225 255.255.255.252

Router(config-if)#clock rate 9600

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial 0/1/0

Router(config-if)#ip address 193.46.10.237 255.255.255.252

Router(config-if)#clock rate 9600

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 193.46.10.1 255.255.255.192

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 193.46.10.241 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router1

Router(config)#interface serial 0/1/1

Router(config-if)#ip address 193.46.10.229 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial 0/1/0

Router(config-if)#ip address 193.46.10.226 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 193.46.10.129 255.255.255.192

Router(config-if)#no shutdown

Router2

Router(config)#interface serial 0/1/1

Router(config-if)#ip address 193.46.10.233 255.255.255.252

Router(config-if)#clock rate 9600

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial 0/1/0

Router(config-if)#ip address 193.46.10.230 255.255.255.252

Router(config-if)#clock rate 9600

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 193.46.10.193 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 193.46.10.242 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router3

Router(config)#interface serial 0/1/1

Router(config-if)#ip address 193.46.10.234 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial 0/1/0

Router(config-if)#ip address 193.46.10.238 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 193.46.10.65 255.255.255.192

Router(config-if)#no shutdown

Router(config-if)#exit

V druhom kroku je nakonfigurovanie protokolu RIPv2. Smerovače Router0 a Router2 smerujú do štyroch sietí a Router1 a Router3 do troch sietí.

Router0

Router(config)#router rip

Router(config-router) #version 2

Router(config-router) #network 193.46.10.224

Router(config-router) #network 193.46.10.236

Router(config-router) #network 193.46.10.240

Router(config-router) #network 193.46.10.0

Router(config-router) #no auto-summary

Router(config-router) #exit

Router1

Router(config)#router rip

Router(config-router) #version 2

Router(config-router) #network 193.46.10.224

Router(config-router) #network 193.46.10.228

Router(config-router) #network 193.46.10.128

Router(config-router) #no auto-summary

Router(config-router) #exit

Router2

Router(config)#router rip

Router(config-router) #version 2

Router(config-router) #network 193.46.10.228

Router(config-router) #network 193.46.10.232

Router(config-router) #network 193.46.10.240

Router(config-router) #network 193.46.10.192

Router(config-router) #no auto-summary

Router(config-router) #exit

Router3

Router(config)#router rip

Router(config-router) #version 2

Router(config-router) #network 193.46.10.232

Router(config-router) #network 193.46.10.236

Router(config-router) #network 193.46.10.64

Router(config-router) #no auto-summary

Router(config-router) #exit

Po nadstavení protokolu RIPv2 na všetkých smerovačoch je možné v privilegovanom móde, príkazom **show ip route** zobraziť smerovaciu tabuľku. Ako príklad je použitá smerovacia tabuľka zo smerovača Router0 viď. obrázok 18.

```
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

     193.46.10.0/24 is variably subnetted, 9 subnets, 3 masks
C       193.46.10.0/26 is directly connected, FastEthernet0/0
R       193.46.10.64/26 [120/1] via 193.46.10.238, 00:00:12, Serial0/1/0
R       193.46.10.128/26 [120/1] via 193.46.10.226, 00:00:14, Serial0/1/1
R       193.46.10.192/27 [120/1] via 193.46.10.242, 00:00:14, FastEthernet0/1
C       193.46.10.224/30 is directly connected, Serial0/1/1
R       193.46.10.228/30 [120/1] via 193.46.10.242, 00:00:14, FastEthernet0/1
                         [120/1] via 193.46.10.226, 00:00:14, Serial0/1/1
R       193.46.10.232/30 [120/1] via 193.46.10.242, 00:00:14, FastEthernet0/1
                         [120/1] via 193.46.10.238, 00:00:12, Serial0/1/0
C       193.46.10.236/30 is directly connected, Serial0/1/0
C       193.46.10.240/30 is directly connected, FastEthernet0/1
```

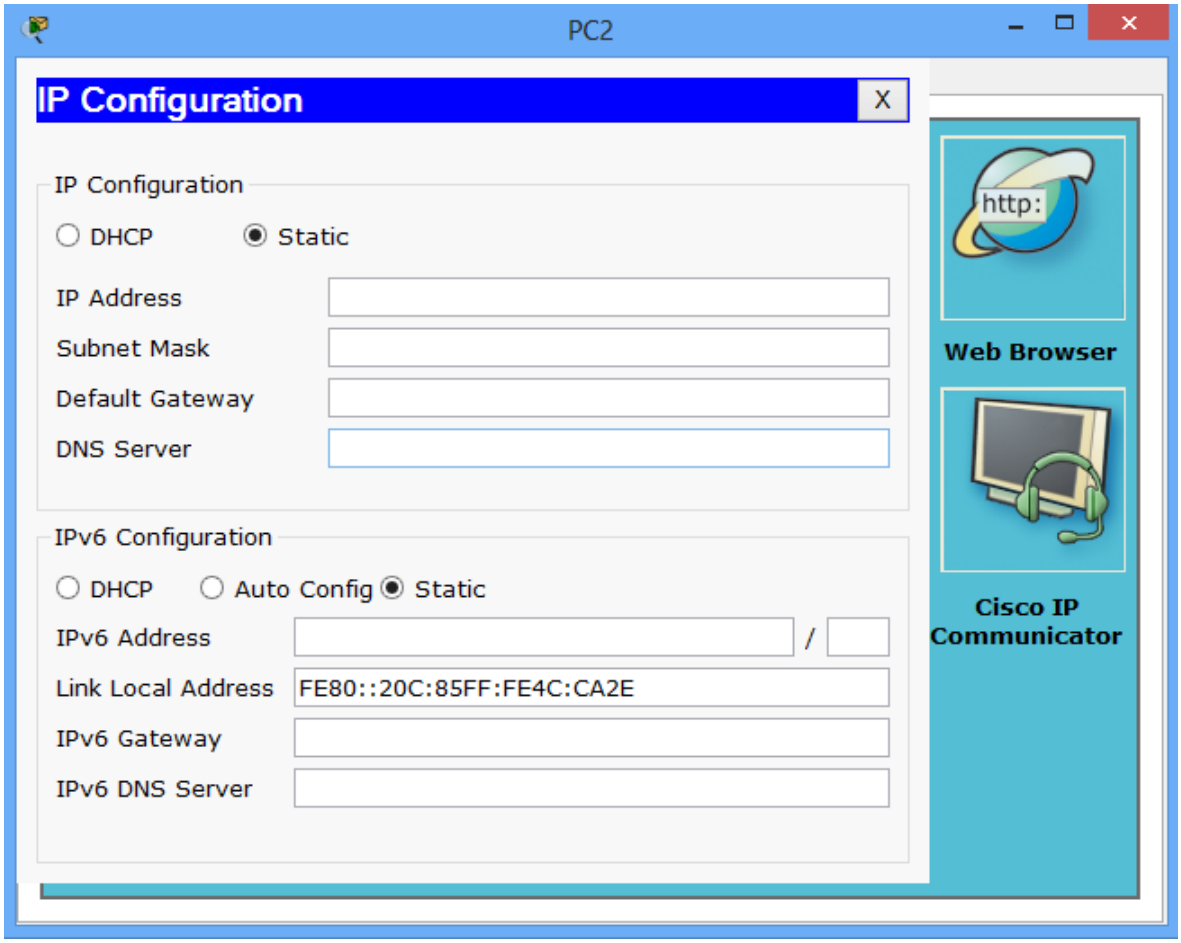
Obrázok 18. Smerovacia tabuľka smerovača Router0

Jednotlivé PC majú nasledujúce IP adresy, viď. tabuľka 9.

Tabuľka 9. Rozsah adries pre nakonfigurovanie PC

	IP adresa	Maska podsieťe	Default Gateway
PC0	193.46.10.2	255.255.255.192	193.46.10.1
PC1	193.46.10.130	255.255.255.192	193.46.10.129
PC2	193.46.10.194	255.255.255.224	193.46.10.193
PC3	193.46.10.66	255.255.255.192	193.46.10.65

Ako posledný krok je nakonfigurovanie IP adries PC. To je možné kliknutím kurzorom myši na vybrané zariadenie, v ňom na záložku deskop, vybrať IP configuration a zobrazí sa nasledujúce prostredie, viď. obrázok 19.



Obrázok 19. Nadstavenie IP adresy, masky a default gateway

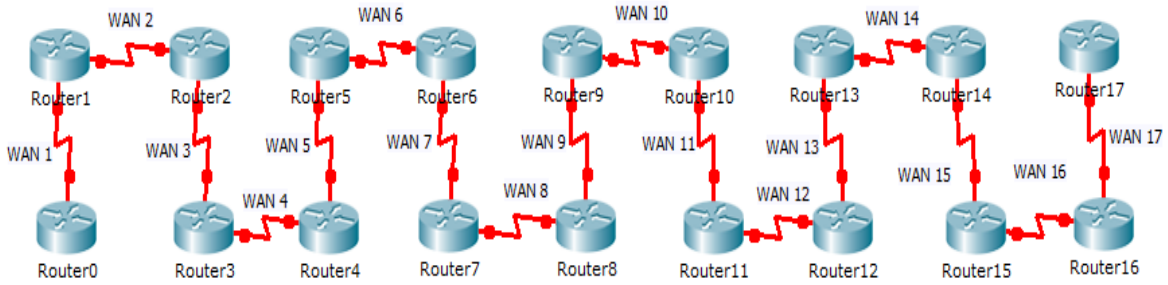
Do políčka IP Address zvolíme IP adresu z rozsahu pre danú sieť. Políčko Subnet Mask slúži na zadanie masky podsieťe a Default Gateway je IP adresa rozhrania smerovača pre LAN.

Po nakonfigurovaní sa pomocou poslania dátového paketu odskúšala funkčnosť siete, viď obrázok 20.

Fire	Last Status	Source	Destination	Type
	Successful	PC3	PC1	ICMP
	Successful	PC0	PC2	ICMP
	Successful	PC1	PC0	ICMP

Obrázok 20 - Funkčnosť zapojenia

Protokol RIP je určený iba do menších sietí, keďže má obmedzený počet skokov. Nasledujúci rozsah demonštruje, že už po pätnástom paket nie je možné doručiť a stáva sa zahodením. Vzhľadom k veľkému rozsahu IP adries rozhraní a sietí je ukážka iba grafická viď. obrázok 21.



Obrázok 21. Zapojenie pre odskúšanie maximálneho počtu skokov

Použité IP adresy pre jednotlivé siete WAN sa nachádzajú v tabuľke č 10.

Tabuľka 10. Rozsah IP adries pre jednotlivé WAN siete.

WAN1	193.46.10.0/30	WAN10	193.46.10.36/30
WAN2	193.46.10.4/30	WAN11	193.46.10.40/30
WAN3	193.46.10.8/30	WAN12	193.46.10.44/30
WAN4	193.46.10.12/30	WAN13	193.46.10.48/30
WAN5	193.46.10.16/30	WAN14	193.46.10.52/30
WAN6	193.46.10.20/30	WAN15	193.46.10.56/30
WAN7	193.46.10.24/30	WAN16	193.46.10.60/30
WAN8	193.46.10.28/30	WAN17	193.46.10.64/30
WAN9	193.46.10.32/30		

Kompletná konfigurácia sa nachádza v prílohe P I kvôli jej rozsiahlosti.

Demonštrácia maximálne pätnástich skokov je uvedená v nasledujúcom obrázku 22.

Fire	Last Status	Source	Destination	Type
	Successful	Router0	Router16	ICMP
	Failed	Router0	Router17	ICMP
	Successful	Router17	Router16	ICMP

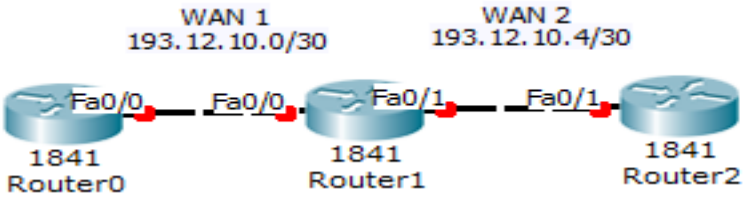
Obrázok 22. Funkčnosť zapojenia

Medzi smerovačmi Router0 a Router16 nepresiahol počet skokov povolenú hranicu, a tak bol dátový paket prijatý úspešne. Avšak problém nastal pri pakete, ktorý smeroval zo smerovača Router0 na Router17, kedy spojenie zlyhalo, keďže bola prekročená hranica pätnástich skokov. Ako dôkaz, že chyba nie je v spojení bol paket medzi smerovačmi Router17 a Router16 prenesení bez problémov.

3.2.4 Protokol OSPF

Na rozdiel od RIPv1 a RIPv2, ktoré používajú vektorovú metriku a majú obmedzený počet skokov. Protokol OSPF má metriku so stavom linky a nie je obmedzený počtom pätnástich skokov. Preto je možné jeho využitie aj v rozsiahlych sieťach. Zmena je aj v maske, ktorá je pri OSPF wildcare.

Ako prvé je realizované jednoduché zapojenie troch smerovačov viď. obrázok 23.



Obrázok 23. Ukážkové zapojenie pre OSPF

Konfigurácia rozhraní je robená rovnakými ako pri predchádzajúcich zapojeniach príkazmi:

- Router(config)# interface [typ rozhrania] [slot/port],
- Router(config-if)# ip address [adresa] [maska].

Preto už nebude v nasledujúcich zapojeniach popisované, ale zameranie bude hlavne na samotný protokol OSPF.

Rozsah použitých IP pre rozhrania a PC sa nachádza v tabuľke 11.

Tabuľka 11. Rozsah IP adries pre rozhrania.

	Router0	Router1	Router2
Fa0/0	193.12.10.1/30	193.12.10.2/30	
Fa0/1		193.12.10.5/30	192.168.10.6/30

Konfigurácia OSPF na jednotlivých smerovačoch.

Router0

Router(config)#router ospf 1

Router(config-router) #network 193.12.10.0 0.0.0.3 area 1

Router(config-router)#exit

Router1

Router(config)#router ospf 1

Router(config-router) #network 193.12.10.0 0.0.0.3 area 1

Router(config-router) #network 193.12.10.4 0.0.0.3 area 1

Router(config-router)#exit

Router2

Router(config)#router ospf 1

Router(config-router) #network 193.12.10.4 0.0.0.3 area 1

Router(config-router)#exit

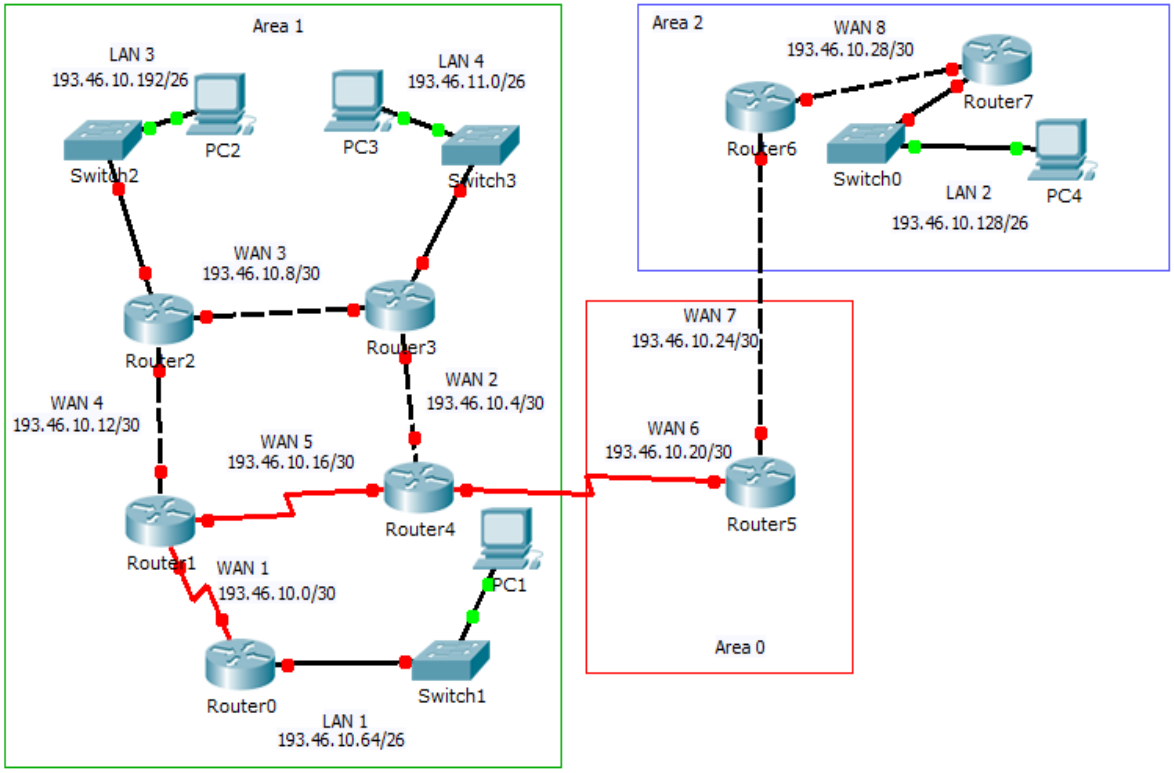
Konfigurácia bola úspešná, o čom svedčí aj príchod dátového paketu z Router0 na Router2 a opačne, viď. obrázok 24.

Fire	Last Status	Source	Destination	Type
	Successful	Router2	Router0	ICMP
	Successful	Router0	Router2	ICMP

Obrázok 24. Funkčnosť zapojenia

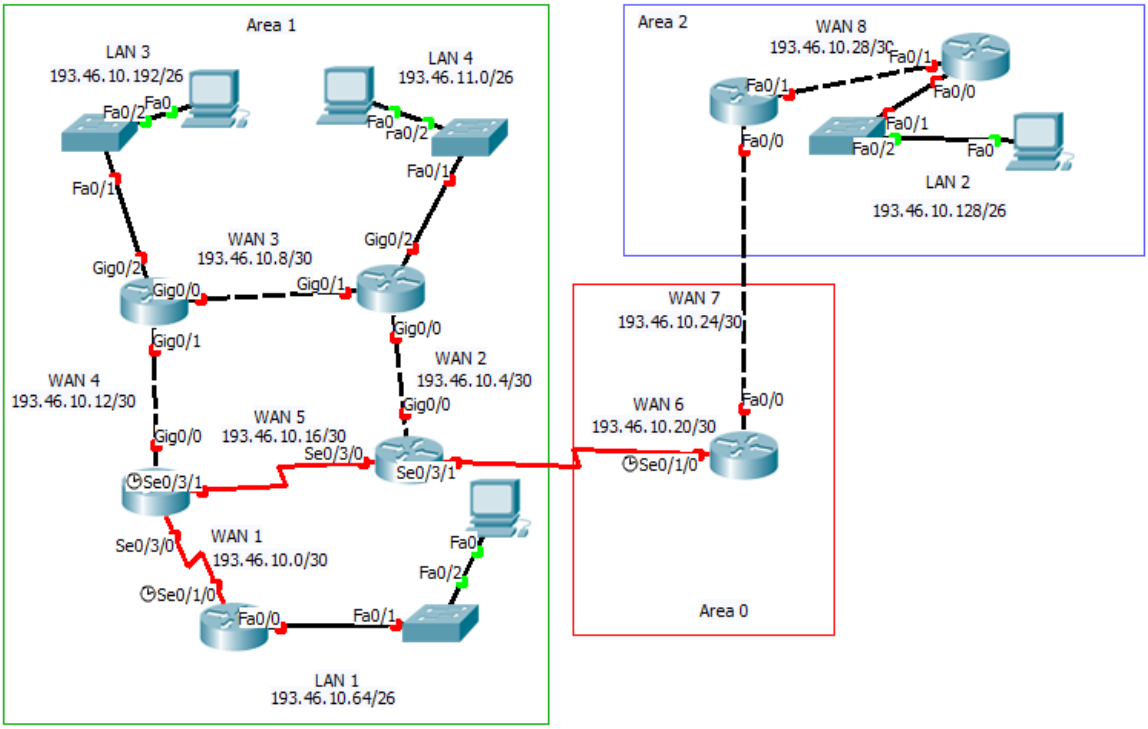
Jednoduchá konfigurácia protokolu OSPF bola úspešne zrealizovaná. Treba si hlavne dávať pozor na wildcare masku, číslo AS a oblasti.

V ďalšom zapojení sa jedná o zložitejšiu konfiguráciu až ôsmich smerovačov, štyroch prepínačov a štyroch PC. Skladá sa z troch oblastí, (Area1, 2, 3). Taktiež obsahuje autentifikáciu OSPF. Popis rozhraní na obrázku 25 je vypnutý pre lepší prehľad.



Obrázok 25. Zapojenie OSPF bez popisu portov

Popis jednotlivých portov sa nachádza na obrázku 26. Názvy zariadení sú vypnuté kvôli lepšej prehľadnosti.



Obrázok 26. Zapojenie OSPF s popisom portov

Konfigurácia rozhraní už nie je rozobratá. V tabuľke č.12 sa nachádzajú iba IP adresy jednotlivých portov.

Tabuľka 12. Rozsah IP adries pre rozhrania

	Router0	Router1	Router2	Router3
Fa0/0	193.46.10.65/26			
Se0/1/0	193.46.10.2/30			
Se0/3/0		193.46.10.1/30		
Se0/3/1		193.46.10.17/30		
Gig0/0		193.46.10.13/30	193.46.10.10/30	193.46.10.5/30
Gig0/1			193.46.10.14/30	193.46.10.9/30
Gig0/2			193.46.10.193/26	193.46.11.1/26
	Router4	Router5	Router6	Router7
Gig0/0	193.46.10.6/30			
Se0/3/0	193.46.10.18/30			
Se0/3/1	193.46.10.21/30			
Se0/1/0		193.46.10.22/30		
Fa0/0		193.46.10.25/30	193.46.10.26/30	193.46.10.129/26
Fa0/1			193.46.10.29/30	193.46.10.30/30

Nadstavenie protokolu OSPF pre všetky smerovače v sieti.

Router0

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.0 0.0.0.3 area 1

Router(config-router) #network 193.46.10.64 0.0.0.63 area 1

Router1

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.0 0.0.0.3 area 1

Router(config-router) #network 193.46.10.12 0.0.0.3 area 1

Router(config-router) #network 193.46.10.16 0.0.0.3 area 1

Router2

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.12 0.0.0.3 area 1

Router(config-router) #network 193.46.10.8 0.0.0.3 area 1

Router(config-router) #network 193.46.10.192 0.0.0.63 area 1

Router3

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.8 0.0.0.3 area 1

Router(config-router) #network 193.46.10.4 0.0.0.3 area 1

Router(config-router) #network 193.46.11.0 0.0.0.63 area 1

Router4

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.4 0.0.0.3 area 1

Router(config-router) #network 193.46.10.16 0.0.0.3 area 1

Router(config-router) #network 193.46.10.20 0.0.0.3 area 0

Router5

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.20 0.0.0.3 area 0

Router(config-router) #network 193.46.10.24 0.0.0.3 area 0

Router6

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.24 0.0.0.3 area 0

Router(config-router) #network 193.46.10.28 0.0.0.3 area 2

Router7

Router(config)#router ospf 1

Router(config-router) #network 193.46.10.28 0.0.0.3 area 2

Router(config-router) #network 193.46.10.128 0.0.0.63 area 2

Nato, aby jednotlivé oblasti (Area) medzi sebou komunikovali, musia byť prepojené cez oblasť 0. Keďže sa jedná o zložitejšie zapojenie, v ďalšom kroku je nadstavená autentifikácia OSPF tak, aby medzi sebou komunikovali PC2 s PC3 cez smerovače Router2 a Router3 a PC0 s PC1 cez smerovače Router0, Router1, Router4, Router5, Router6 a Router7. Vzájomná komunikácia nie je možná kvôli nadstaveniu dvoch rôznych autentifikácií.

Kvôli veľkému rozsahu nakonfigurovania autentifikácie pre každé rozhranie je zobrazená iba ukážka pre smerovače Router0 a Router2, keďže majú rozdielne heslo a preto medzi sebou nekomunikujú. Je použitá md5 autentifikácia.

Router0

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip ospf message-digest-key 1 md5 cisco

Router(config-if)#ip ospf authentication message-digest

Router(config-if)#exit

Router(config)# interface serial 0/1/0

Router(config-if)#ip ospf message-digest-key 1 md5 cisco

Router(config-if)#ip ospf authentication message-digest

Router(config-if)#exit

Router(config)#router ospf 1

Router(config-router)# area 1 authentication message-digest

Router2

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#ip ospf message-digest-key 1 md5 class

Router(config-if)#ip ospf authentication message-digest

Router(config-if)#exit

Router(config)# interface gigabitEthernet 0/1

Router(config-if)#ip ospf message-digest-key 1 md5 class

Router(config-if)#ip ospf authentication message-digest

Router(config-if)#exit

Router(config)# interface gigabitEthernet 0/2

Router(config-if)#ip ospf message-digest-key 1 md5 class

Router(config-if)#ip ospf authentication message-digest

Router(config-if)#exit

Router(config)#router ospf 1

Router(config-router)# area 1 authentication message-digest

Týmto spôsobom sa nakonfiguruje každý smerovač a rozhranie, na ktorých je zapnutá autentifikácia.

Ďalší krok je nadstavenie IP adries na štyroch PC. Použité sú adresy, viď. tabuľka 13.

Tabuľka 13. Rozsah IP adries pre rozhrania.

	IP adresa	Maska podsieťe	Default Gateway
PC1	193.46.10.66	255.255.255.192	193.46.10.65
PC2	193.46.10.130	255.255.255.192	193.46.10.129
PC3	193.46.10.194	255.255.255.192	193.46.10.193
PC4	193.46.11.2	255.255.255.192	193.46.11.1

Zapojenie je kompletne zrealizované a ako posledný krok je odskúšanie jeho funkčnosti. Kvôli realizácii autentifikácie budú medzi sebou komunikovať iba zariadenia, ktoré ju majú nadstavenú rovnako, viď. obrázok 27.

Fire	Last Status	Source	Destination	Type
	Successful	PC1	PC4	ICMP
	Successful	PC2	PC3	ICMP
	Failed	PC2	PC1	ICMP
	Failed	PC3	PC1	ICMP
	Failed	PC2	PC4	ICMP
	Failed	PC2	PC4	ICMP

Obrázok 27. Funkčnosť zapojenia

Komunikujú medzi sebou iba PC1 s PC4 a PC2 s PC3. Autentifikácia bola nadstavená správne a zapojenie funguje.

Smerovacia tabuľka smerovača Router5 z oblasti Area0 obsahuje nasledujúce spojenia, viď .obrázok 28.

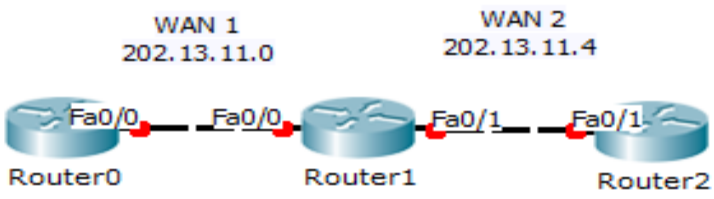
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     193.46.10.0/24 is variably subnetted, 9 subnets, 2 masks
O IA    193.46.10.0/30 [110/192] via 193.46.10.21, 00:54:19, Serial0/1/0
O IA    193.46.10.4/30 [110/65] via 193.46.10.21, 00:54:19, Serial0/1/0
O IA    193.46.10.12/30 [110/129] via 193.46.10.21, 00:54:19, Serial0/1/0
O IA    193.46.10.16/30 [110/128] via 193.46.10.21, 00:54:19, Serial0/1/0
C       193.46.10.20/30 is directly connected, Serial0/1/0
C       193.46.10.24/30 is directly connected, FastEthernet0/0
O IA    193.46.10.28/30 [110/2] via 193.46.10.26, 02:57:30, FastEthernet0/0
O IA    193.46.10.64/26 [110/193] via 193.46.10.21, 00:54:19, Serial0/1/0
O IA    193.46.10.128/26 [110/3] via 193.46.10.26, 02:57:30, FastEthernet0/0
```

Obrázok 28. Smerovacia tabuľka smerovača Router5

3.2.5 Protokol EIGRP

Posledný z rady smerovacích protokol je firemný protokol spoločnosti Cisco a to EIGRP. Jeho použitie je možné iba na smerovačoch tejto značky.

Ako prvé je realizované zapojenie troch smerovačov na zoznámenie sa so základnou konfiguráciou EIGRP, viď obrázok 29.



Obrázok 29. Zapojenie pre EIGRP

Konfigurácia rozhraní už nie je rozpísaná. V tabuľke 14 sa nachádzajú IP adresy pre konkrétne porty zapojenia.

Tabuľka 14. Rozsah IP adries pre rozhrania.

	Router0	Router1	Router2
Fa0/0	202.13.11.1/30	202.13.11.2/30	
Fa0/1		202.13.11.5/30	202.13.11.6/30

Druhý krok je nadstavenie EIGRP na všetkých troch smerovačoch.

Router0

Router(config)#router eigrp 1

Router(config-router)# network 202.13.11.0 0.0.0.3

Router(config-router)# no auto-summary

Router1

Router(config)#router eigrp 1

Router(config-router)# network 202.13.11.0 0.0.0.3

Router(config-router)# network 202.13.11.4 0.0.0.3

Router(config-router)# no auto-summary

Router2

Router(config)#router eigrp 1

Router(config-router)# network 202.13.11.4 0.0.0.3

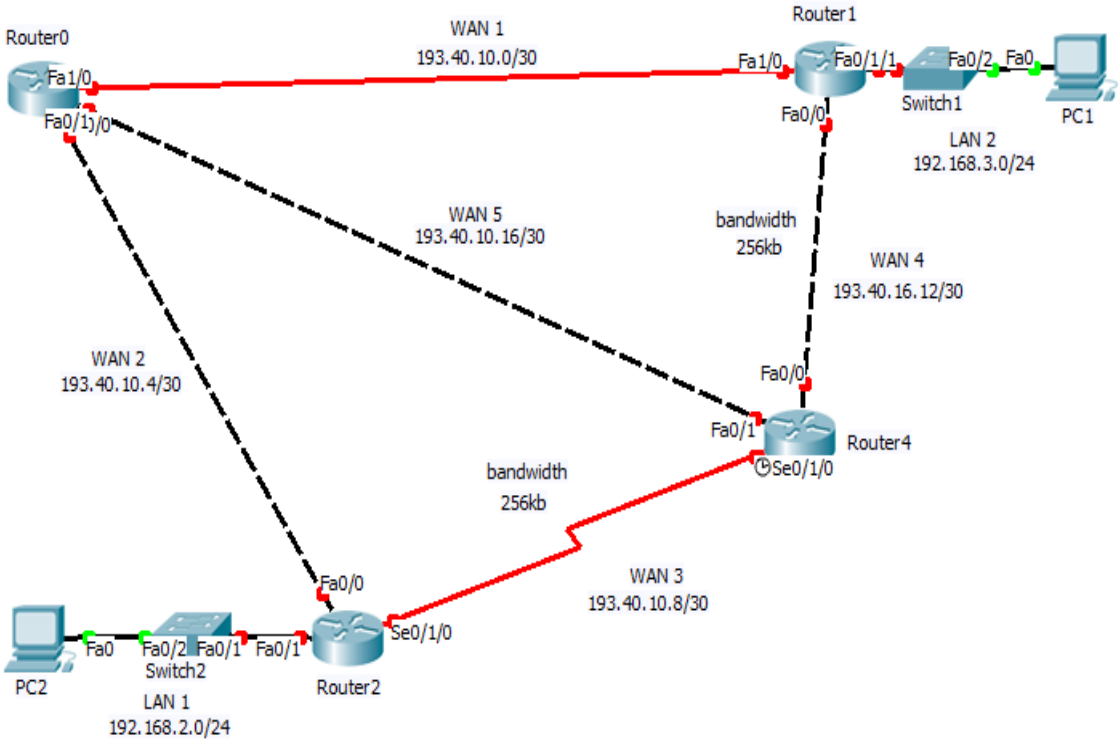
Router(config-router)# no auto-summary

Zapojenie bolo úspešne zrealizované a jeho funkčnosť bola odskúšaná dátovým paketom, ktorý prešiel z Router0 na Router2 a naopak, viď. obrázok 30.

Fire	Last Status	Source	Destination	Type
	Successful	Router0	Router2	ICMP
	Successful	Router2	Router0	ICMP

Obrázok 30. Funkčnosť zapojenia

Druhé zapojenie je realizované pomocou štyroch smerovačov, dvoch prepínačov a PC, viď. obrázok 31.



Obrázok 31. Rozsiahlejšie ukážkové zapojenie EIGRP

IP adresy pre konkrétne porty smerovačov a PC sa nachádzajú v tabuľke č. 15.

Tabuľka 15. IP adresy pre jednotlivé rozhrania smerovačov.

	Router0	Router1	Router2	Router3
Fa0/0	193.40.10.5/30	193.40.10.14/30	193.40.10.6/30	193.40.10.13/30
Fa0/1	193.40.10.17/30	192.168.3.1/24	192.168.2.1/24	193.40.10.18/30
Fa1/0	193.40.10.1/30	193.40.10.2/30		
Se0/1/0			193.40.10.9/30	193.40.10.10/30
	IP adresa	Maska podsiete	Default Gateway	
PC1	192.168.3.2	255.255.255.0	192.168.3.1	

Nadstavenie EIGRP na všetkých smerovačoch.

Router0

Router(config)#router eigrp 1

Router(config-router)# network 193.40.10.0 0.0.0.3

Router(config-router)# network 193.40.10.4 0.0.0.3

Router(config-router)# network 193.40.10.16 0.0.0.3

Router(config-router)# no auto-summary

Router1

Router(config)#router eigrp 1

Router(config-router)# network 193.40.10.0 0.0.0.3

Router(config-router)# network 193.40.10.12 0.0.0.3

Router(config-router)# network 192.168.3.0 0.0.0.255

Router(config-router)# no auto-summary

Router2

Router(config)#router eigrp 1

Router(config-router)# network 193.40.10.4 0.0.0.3

Router(config-router)# network 193.40.10.8 0.0.0.3

Router(config-router)# network 192.168.2.0 0.0.0.255

Router(config-router)# no auto-summary

Router3

Router(config)#router eigrp 1

Router(config-router)# network 193.40.10.4 0.0.0.3

Router(config-router)# network 193.40.10.8 0.0.0.3

Router(config-router)# network 192.168.2.0 0.0.0.255

Router(config-router)# no auto-summary

V tomto zapojení je pomocou príkazu: **Router(config-if)# bandwidth [hodnota v kb]**, na konkrétnych rozhraniach ukázané, ako veľkosť šírky pásma zmení trasy pri posielaní paketov.

Nadstavenie šírky pásma na rozhraní smerovačov:

Router1

Router(config)#interface fastEthernet 0/0

Router(config-if)#bandwidth 256

Router2

Router(config)# interface serial 0/1/0

Router(config-if)#bandwidth 256

Router3

Router(config)#interface fastEthernet 0/0

Router(config-if)#bandwidth 256

Router(config-if)#exit

Router(config)#interface serial 0/1/0

Router(config-if)# bandwidth 256

Po zmene rýchlosti na 256 kb smerovač Router3 neodosiela pakety na Router1 priamo, ale cez smerovač Router0. To isté platí aj pre komunikáciu so smerovačom Router2. Trasy protokolu EIGRP je možné získať príkazom: **Router# show ip eigrp topology**, viď obrázok 32, na ktorom je smerovač Router3.

```
Router#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 193.40.10.12/30, 1 successors, FD is 10002432
         via Connected, FastEthernet0/0
P 193.40.10.16/30, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 193.40.10.8/30, 1 successors, FD is 10511872
         via Connected, Serial0/1/0
P 193.40.10.0/30, 1 successors, FD is 30720
         via 193.40.10.17 (30720/28160), FastEthernet0/1
         via 193.40.10.14 (10004992/28160), FastEthernet0/0
P 192.168.3.0/24, 1 successors, FD is 33280
         via 193.40.10.17 (33280/30720), FastEthernet0/1
         via 193.40.10.14 (10004992/28160), FastEthernet0/0
P 193.40.10.4/30, 1 successors, FD is 30720
         via 193.40.10.17 (30720/28160), FastEthernet0/1
         via 193.40.10.9 (10514432/28160), Serial0/1/0
P 192.168.2.0/24, 1 successors, FD is 33280
         via 193.40.10.17 (33280/30720), FastEthernet0/1
         via 193.40.10.9 (10514432/28160), Serial0/1/0
```

Obrázok 32. Topologická tabuľka EIGRP na smerovači Router3

Odskúšanie nakonfigurovaného zapojenia prebehlo úspešne. Dátový paket s PC1 prišiel na PC2 a opačne, viď obrázok 33.

Fire	Last Status	Source	Destination	Type
	Successful	PC1	PC2	ICMP
	Successful	PC2	PC1	ICMP

Obrázok 33. Funkčnosť zapojenia

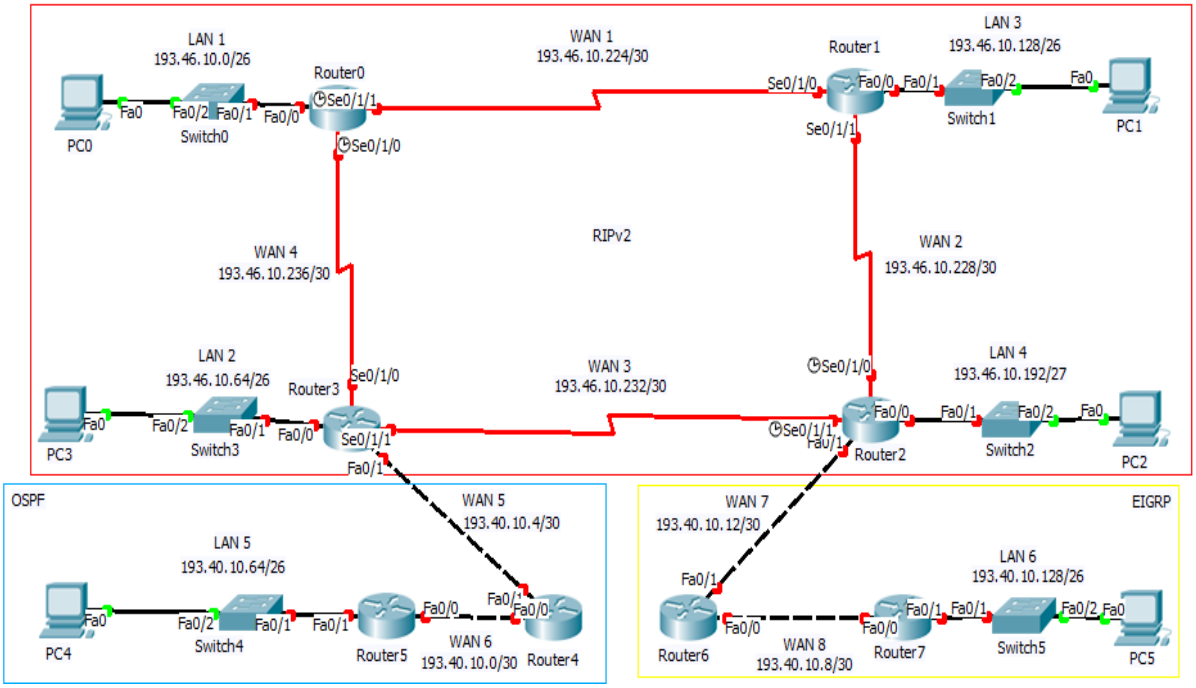
Zobrazenie smerovacej tabuľky smerovača Router 3, viď. obrázok 34.

```
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

D    192.168.2.0/24 [90/33280] via 193.40.10.17, 01:26:02, FastEthernet0/1
D    192.168.3.0/24 [90/33280] via 193.40.10.17, 01:26:02, FastEthernet0/1
     193.40.10.0/30 is subnetted, 5 subnets
D       193.40.10.0 [90/30720] via 193.40.10.17, 01:26:03, FastEthernet0/1
D       193.40.10.4 [90/30720] via 193.40.10.17, 01:26:03, FastEthernet0/1
C       193.40.10.8 is directly connected, Serial0/1/0
C       193.40.10.12 is directly connected, FastEthernet0/0
C       193.40.10.16 is directly connected, FastEthernet0/1
```

Obrázok 34. Smerovacia tabuľka smerovača Router3

3.2.6 Konfigurácia RIPv2, OSPF, EIGRP

Nie vždy sa v sieti nachádza iba jeden druh smerovacieho protokolu. Preto sa v poslednom zapojení vyskytujú hneď tri a to RIPv2, OSPF a EIGRP. Na to, aby medzi sebou komunikovali, musí byť na hraničných smerovačoch nadstavená redistribúcia. Zapojenie obsahuje osem smerovačov, šesť prepínačov a PC, viď. obrázok 35.



Obrázok 35. Ukážkové zapojenie RIPv2, OSPF, EIGRP

Konfigurácia smerovacích protokolov už nie je rozobratá pre veľký rozsah konfigurácie. V tabuľke 16 sa nachádzajú adresy sietí pre jednotlivé smerovače a smerovacie protokoly.

Tabuľka 16. Rozsah IP adries pre smerovače a smerovacie pretokoly

RIPv2	Router0	Router1	Router2	Router3
	193.46.10.0/26	193.46.10.128/26	193.46.10.192/27	193.46.10.64/26
	193.46.10.236/30	193.46.10.224/30	193.46.10.228/30	193.46.10.236/30
	193.46.10.224/30	193.46.10.228/30	193.46.10.232/30	193.46.10.232/30
			193.40.10.12/30	193.40.10.4/30
	Router4	Router5	Router6	Router7
OSPF	193.40.10.0/30	193.40.10.0/30		
	193.40.10.4/30	193.40.10.64/26		
EIGRP			193.40.10.8/30	193.40.10.8/30
			193.40.10.12/30	193.40.10.128/26

IP adresy rozhraní a PC sa nachádzajú v tabuľke 17.

Tabuľka 17. Rozsah IP adries pre rozhrania a PC

	Router0	Router1	Router2	Router3
Fa0/0	193.46.10.1/26	193.46.10.129/26	193.46.10.193/27	193.46.10.65/26
Fa0/1			193.40.10.14/30	193.40.10.6/30
Se0/1/0	193.46.10.237/30	193.46.10.226/30	193.46.10.230/30	193.46.10.238/30
Se0/1/1	193.46.10.225/30	193.46.10.229/30	193.46.10.234/30	193.46.10.233/30
	Router4	Router5	Router6	Router7
Fa0/0	193.40.10.2/30	193.40.10.1/30	193.40.10.9/30	193.40.10.10/30
Fa0/1	193.40.10.5/30	193.40.10.65/26	193.40.10.13/30	193.40.10.129/26
	IP adresa	Maska podsiete	Default Gateway	
PC0	193.46.10.2	255.255.255.192	193.46.10.1	
PC1	193.46.10.130	255.255.255.192	193.46.10.129	
PC2	193.46.10.194	255.255.255.224	193.46.10.193	
PC3	193.46.10.66	255.255.255.192	193.46.10.65	
PC4	193.40.10.66	255.255.255.192	193.40.10.65	
PC5	193.40.10.130	255.255.255.192	193.40.10.129	

Na to, aby medzi sebou jednotlivé smerovacie protokoly komunikovali je treba nadstaviť redistribúciu.

Router2

Router(config)#router eigrp 1

Router(config-router)# redistribute rip metric 10000 100 255 1 1500

Router(config-router)# exit

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# redistribute eigrp 1 metric 3

Router3

Router(config)# router ospf 1

Router(config-router)# redistribute rip subnets

Router(config-router)# exit

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# redistribute ospf 1 metric 3

Pri redistribúcii do RIP je treba nadstaviť metriku. V OSPF je potrebné zadať príkaz subnets, aby sa preposlali aj podsiete. Pri EIGRP sa nadstavuje najviac parametrov a to priepustnosť siete, oneskorenie, spoľahlivosť, zaťaženie a maximálna veľkosť paketu na trase v bajtoch.

Konfigurácia bola správna, o čom svedčí obrázok 36, na ktorom je úspešne prenesený dátový paket z OSPF cez RIPv2 až do EIGRP a opačne.

Fire	Last Status	Source	Destination	Type
	Successful	PC4	PC5	ICMP
	Successful	PC5	PC4	ICMP

Obrázok 36. Funkčnosť zapojenia

3.2.7 Zhrnutie praktickej časti

Všetky zapojenia konfigurácií od základnej cez jednotlivé protokoly RIPv1, RIPv2, OSPF, EIGRP ako je spojenie RIPv2,OSPF a EIGRP v jednom zapojení boli úspešne nakonfigurované, o čom svedčí odskúšanie pomocou dátového paketu. V prílohe sa nachádzajú dve verzie každého zapojenia, a to nenakonfigurované a nakonfigurované simulácie vytvorené v programe Cisco Packet Tracer.

ZÁVĚR

Cieľom bakalárskej práce bolo vytvoriť ucelený dokument s problematikou smerovania pomocou dynamických smerovacích protokolov a simulácií ukážkových topológií v prostredí Cisco Packet Tracer od spoločnosti Cisco.

Pre vniknutie do problematiky bolo veľmi dôležité zoznámiť sa s teoretickými vlastnosťami, ktoré sú uvedené v teoretickej časti práce. V nej boli popísané základné pojmy ako smerovač, smerovací protokol, smerovaný protokol, Cisco IOS, statické a dynamické smerovanie. Tieto sú potrebné na vniknutie do témy. Dôležitá časť je takisto variabilné podsieťovanie, ktoré využíva väčšina smerovacích protokolov a jeho veľkou výhodou je šetrenie adresného miesta. Najdôležitejšou časťou však bol popis jednotlivých protokolov. V práci ich je popísaných päť a to RIPv1, RIPv2 a IGRP, ktoré patria do skupiny s vektorom vzdialenosti. OSPF do skupiny so stavom linky a ako posledný EIGRP, ktorý má vlastnosti obidvoch skupín, a preto sa nazýva hybridný. Taktiež je popísaná aj autentifikácia, ktorá slúži na zabezpečenie smerovania.

Praktická časť bola robená v simulačnom prostredí Cisco Packet Tracer. V úvode sa nachádza popis jednotlivých častí tohto programu pre lepšiu orientáciu. Ako ďalšie sú vytvorené ukážkové topológie. Prvé jednoduché zapojenie je zamerané na základnú konfiguráciu smerovača, ktorá by nemala nikdy chýbať. Je v nej popísaná bezpečnosť pomocou hesiel pre jednotlivé porty a vstupy do módou príkazového riadku smerovača. Takisto sú jednotlivé heslá zahashované pomocou md5 hashu kvôli väčšej bezpečnosti. Ďalej sa v nej nachádza zmena mena smerovača a nadstavenie IP adries a másk pre jednotlivé porty. Po tejto konfigurácii prichádzajú na rad samotné smerovacie protokoly. Vždy sa jedná o základnú konfigurácie a zložitejšiu konfiguráciu, okrem RIPv1, ktorá obsahuje iba jednu a IGRP, ktorá nie je vytvorená vôbec kvôli zrušeniu podpory na smerovačoch z dôvodu jeho vylepšenia na protokol EIGRP. Protokol RIPv2 obsahuje aj konfiguráciu maximálneho počtu skokov. Ako posledné zapojenie je spojenie troch najviac používaných protokol RIPv2, EIGRP a OSPF v jednej sieti, kde musela byť použitá redistribúcia, keďže nie je možné posielať pakety cez rôzne smerovacie protokoly. Zapojenie vytvorené v Cisco Packet Tracer sa nachádzajú v prílohe.

SEZNAM POUŽITÉ LITERATURY

[1] SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.

[2] WANs a rútre: Vnútorné komponenty routra. In: *CISCO Networking Academy* [online]. [cit. 2014-04-02]. Dostupné z: http://cisco-academy.aspone.cz/wans-a-rutre.html

[3] Cisco IOS Packaging, Product Bulletin No. 2160: New Packaging Feature Inheritance Principle.In:*www.cisco.com* [online].[cit.2014-05-16]. Dostupné z: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-packaging/prod_bulletin09186a00801af451.html

[4] Cisco IOS Release 15.0 Feature Sets and Memory Recommendations for Cisco 1900, 2900 and 3900 Series Routers: Cisco IOS Software Release 15.0 Features Sets and Universal IOS Images. In: *www.cisco.com*[online]. [cit. 2014-05-16]. Dostupné z: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-packaging/product_bulletin_c25-566278.html

[5] Cisco Feature Navigator. In: *www.cisco.com* [online]. [cit. 2014-05-16]. Dostupné z:http://tools.cisco.com/ITDIT/CFN/jsp/compareImages.jsp

[6] Cisco IOS softver: Postupnosť sekvencií pri zapnutí routra. In: CISCO Networking Academy [online]. [cit.2014-04-02]. Dostupné z: http://cisco-academy.aspone.cz/cisco-ios-softver.html

[7] Úvod k smerovaniu: Routing Protocols and Concepts – Chapter 1. In: [online]. [cit. 2014-04-02].Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccna2/Ch1-Routing.pdf

[8] LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.

[9] Border Gateway Protocol (BGP): ROUTE Module 6. In: [online]. [cit. 2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccnp-route-v6/BSCI%20M6.pdf

[10] Distančné vektorové smerovacie protokoly: Vyrovnávanie záťaže cez viacnásobné cesty. In: *CISCO Networking Academy* [online]. [cit.2014-04-02]. Dostupné z: http://cisco-academy.aspone.cz/distancne-vektorove-smerovacie-protokoly.html

[11] VLSM a CIDR: CCNA2 – Kapitola 6. In: [online]. [cit. 2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccna2/Ch6-VLSM%20a%20CIDR.pdf

[12] Smerovanie a smerovacie protokoly: Autonómny systém a IGP verzus EGP. In: *CISCO Networking Academy*[online]. [cit. 2014-04-02]. Dostupné z: http://cisco-academy.aspone.cz/smerovanie-a-smerovacie-protokoly.html

[13] Úvod do dynamických smerovacích protokolov. In: [online]. [cit. 2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccna2/Ch3-Intro-Dynamic_routing.pdf

[14] Routing Information Protocol: RIP Packet Format. In: *DocWiki* [online]. [cit. 2014-04-02]. Dostupné z: http://docwiki.cisco.com/wiki/Routing_Information_Protocol

[15] RIPv2: CCNA2 – Kapitola 9. In: *CISCO Networking Academy* [online]. [cit. 2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccna2/Ch7-RIPv2.pdf

[16] Stretnutie 3: Smerovací protokol OSPF: ROUTE Module 3. In: *CISCO Networking Academy* [online]. [cit. 2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccnp-route-v6/BSCI%20M3-v2.pdf

[17] ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-80-251-2520-5.

[18] HUCABY, Dave, Steve MCQUERRY a Andrew WHITAKER. Cisco router configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2010, xxii, 641 s. ISBN 978-1-58714-116-4.

[19] DOYLE, Jeff a Jennifer DEHAVEN CARROLL. Routing TCP/IP. Indianapolis: Cisco Press, 2001, xxii, 945 s. ISBN 15-787-0089-2.

[20] Stretnutie 2: Smerovací protokol EIGRP: BSCI/ROUTE Module 2. In: *CISCO Networking Academy* [online].[cit.2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccnp-route-v6/BSCI%20M2.pdf

[21] Distance vector routing protokoly: CCNA2 – Kapitola 4. In: *CISCO Networking Academy* [online]. [cit. 2014-04-02]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/Netacad/LST/ccna2/Ch4-Distance%20vector.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACK	Acknowledgment
AFI	Address Family Identifier
AS	Autonomous System
AUX	Auxiliary
CLI	Command Line Interface.
CPU	Central Processing Unit
EIGRP	Enchanced Interior Gateway Routing Protocol.
ID	Identification
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol.
IOS	Internetwork Operating System.
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MD5	Message Diggest algorithm 5
NVRAM	Non Volatile Random Access Memory
OSPF	Open Shortest Path First.
PDU	Protocol Data Unit
POST	Power On Self Test
RAM	Random Access Memory
RFC	Request For Comments
RIP	Routing Information Protocol
ROM	Read Only Memory
RTP	Reliable Transport Protocol
Viď.	Vidieť.

VLSM	Variable Length Subnet Masking
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
XOS	Xerox Operating System

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CD S NAKONFIGUROVANÝMI ZADANIAMI

Na CD sa nachádzajú nenakonfigurované a nakonfigurované zadania jednotlivých protokolov.