VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

KONFIGURACE SMĚROVACÍHO PROTOKOLU OPEN SHORTEST PATH FIRST

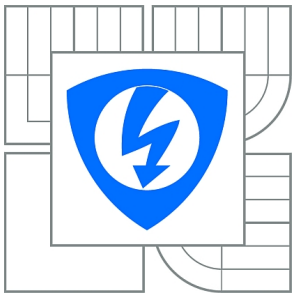
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Bc. JAKUB WOLF
AUTHOR

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

KONFIGURACE SMĚROVACÍHO PROTOKOLU OPEN SHORTEST PATH FIRST

CONFIGURATION OF OPEN SHORTEST PATH FIRST ROUTING PROTOCOL

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

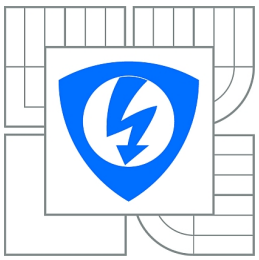
AUTOR PRÁCE — Bc. JAKUB WOLF

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. DAN KOMOSNÝ, Ph.D.

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Jakub Wolf	***ID:***	70305
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Konfigurace směrovacího protokolu Open Shortest Path First

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s dokumenty popisující činnost a zapojení laboratoře Cisco akademie FEKT, VUT v Brně. V programu Packet Tracer proveďte konfiguraci síťových prvků pro sadu laboratorních cvičení 2.6.2-9.8.3 kurzu CCNA1. Konfiguraci proveďte i pro všechny pracovní stanice v laboratoři a používaný výukový server. Dále v programu Packet Tracer vytvořte zadání samostatné úlohy pro konfiguraci směrovacího protokolu OSPF (Open Shortest Path First). Úlohu koncipujte tak, aby zahrnovala i problematiku adresace zařízení. Vytvořte systém automatické kontroly realizované úlohy. Při automatické kontrole hodnoťte dílčí úkoly podle obtížnosti zadání.

DOPORUČENÁ LITERATURA:

[1] GRAZIANI, R., JOHNSON, A. Routing Protocols and Concepts, CCNA Exploration Companion Guide. Cisco Press, USA, 2007. 606 s. ISBN 978-1-58713-206-3.
[2] NEMETH, E., SNYDER, G., HEIN T. Linux - Kompletní příručka administrátora. Computer Press, 2004. 880 s. ISBN: 80-722-6919-4.
[3] SPORTACK, A. Směrování v sítích IP [překlad Krásenský, D.]. 1. vydání. Brno : Computer Press, 2004. 351 s. ISBN 80-251-0127-4.

Termín zadání:	7.2.2011	***Termín odevzdání:***	26.5.2011

Vedoucí práce: doc. Ing. Dan Komosný, Ph.D.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Diplomová práca popisuje možnosti smerovacieho protokolu Open Short Path First (OSPF) v základnej konfigurácii a implementáciu do autonómneho systému. Teoretická časť rozoberá základny počítačových sietí a rozdelenie podľa rôznych kritérií. Ďalej popisuje spôsob adresovania v sieti Internet pomocou Internet Protocol (IP) adries a využívané princípy delenia rozsahov IP adries. Praktická časť pozostáva z dvoch projektov vytovrených v simulačnom programe. Prvý simuluje počítačovú učebňu so všetkými sieťovými zariadeniami a počítačovými stanica. Druhý projekt je úloha pre študentov, zameraná na simuláciu protokolu OSPF v autonómnom systéme. V úlohe je využité rozšírenie simlačného programu, ktoré umožňuje kooperatívnu prácu študentov na viacerých počítačoch pre realizáciu úlohy. V závere práce sú použité postupy zdokumentované. Súčasťou diplomovej práce je webová prezentácia.

KĽÚČOVÉ SLOVÁ

OSPF, simulácia , počítačová učebňa

ABSTRACT

A diploma thesis introduces possibilities of the routing protocol OSPF, basic configurations and implementation into an autonomous system. A Theoretical part shows computer networks fundamentals and divide them into several groups according to standarts. It also include a part about addressing scheme in the Internet network and the ways how to subneted networks. A practical part consists of two project, that are create in a simulation program. The first simulates classroom, all the network devices and the computers are included. The second is an exam made for student to introduce OSPF in the autonomous system. The Exam uses new type of an extension, that allow student cooperate together by solving the exam. A summary contains all technique disposed in both simulations and a web presentation.

KEYWORDS

OSPF, simulation, computer classroom

WOLF, Jakub *Konfigurace směrovacího protokolu Open Shortest Path First*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 74 s. Vedoucí práce byl doc. Ing. Dan Komosný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Konfigurace směrovacího protokolu Open Shortest Path First“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno ....

(podpis autora)

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

Internet v dnešnej dobe berieme ako samozrejmosť a vždy od neho očakávame maximálnu funkčnosť. Akékoľvek zdržanie pri sťahovaní súboru z webovej stránky, alebo nedostupnosť služby, berieme negatívne. Pretože sme v zamestnaní odrezaný od dôležitých dát, alebo doma si nemôžeme pozrieť najnovšie video. Aby k takýmto situáciám nedochádzalo, maly by sieti existovať mechanizmy, ktoré zabezpečia, aby sa informácia dostala zo serveru do nášho počítača čo najrýchlešie. Súčasne by mali zabezpečiť, že v prípade výpadku nejakej linky v sieti, nájdu nové cesty, ktorými dáta z firemného serveru, alebo najnovšie video môže doputovať až k nám. Mechanizmi, ktoré tieto funkcie zabezpečujú sú smerovacie protokoly a závisí na nich fungovanie Internetu.

Existuje niekoľko typov smerovacích protokolov no medzi najdôležitejšie a v súčasnosti najrozšírenejšie patrí protokol OSPF. Je to protokol zaisťujúci smerovanie paketov v segmentoch Internetu – autonómnych systémov Autonomous System (AS). Pretože každá sieť s prístupom k Internetu je súčasťou AS, je dôležité poznať schopnosti a možnosti, ktorými disponuje protokol OSPF a zvládať jeho nastavenie a implementáciu.

Diplomovu prácou sa snažím predviesť pricípy s akými OSPF pracuje a simulovať jeho nasadenie v niektorom z dostupných simulačných programov. Súčasne by simulácia mala splňovať požiadavku, aby bola vytvorený pre študentov, ktorý budú v nej mocť rozširovať a testovať svoje znalosti.

Program, ktorý som si vybral pre realizáciu simulácie a úlohy, je Packet tracer. Svojími parametrami vyhovoval mojím požiadavkám. V ňom som vytvoril úlohu, ktorá nielen že testuje študentov a poskytuje automatické vyhodnotenie, ale zároveň umožňuje vytvaráť rozsiahle siete spojením niekoľkých inštancií programu Packet tracer. Úloha poskytuje veľkú mieru interaktivity, pretože sieť, ktorú študenti nakonfigurujú môžu spájať so sieťami ostatných študentov.

Naviac som k tejto úlohe vytvoril simuláciu učebne Cisco akadémie, ktorá sa nachádza v budove Fakulty elektrotechniky a komunikačných technologií VUT v Brne. Rovnako je vytvorená v programe Packet tracer a vďaka nej je môžné riešiť akékoľvek úlohy z predmetov XCA1 až XCA5 vyučovaných na tejto fakulte.

Text diplomovej práce je rozdelený do siedmich kapitol. V prvých štyroch zrozumiteľným spôsobom vysvetľujem základy počítačových sietí. Kapitoly 1 a 2 obecne popisujú rozne typy sietí. Veľa priestoru venenujem adresovaniu v Internete, pretože uvedené princípy sú použité pri riešení úlohy. Kapitola 4 rozoberá problematiku smerovacieho protokolu OSPF.

Praktickú časť diplomovej práce popisujú kapitoly 7 a 8. V nich vysvetlujem metódy, ktorými som postupoval a spôsoby imlementácie smerovacie protokolu OSPF

do programu Packet tracer. Zároveň uvádzam spôsob využitia rozšírení programu, ktoré prispeli, k tvorbe zaujímavejšej úlohy.

Pre prezentáciu práce na stránkach Cisco akadémie som vytvoril webovú stránku s popisom jednotlivých úloh.

1 POČÍTAČOVÉ SIETE

Počítačová sieť je spojenie dvoch a viacerých počítačov komunikačným kanálom. Motiváciou je umožniť zariadeniam zdielať dáta, prostriedky (pamäťové, výpočtové) a aplikácie. Každá počítačová sieť obsahuje niekoľko dôležitých prvkov, bez ktorej nie je možné zabezpečiť správny chod. Prvky sú zodpovedné za funkčnosť, dohľad a bezpečnosť siete. V tejto kapitole sú opísané dôležité štandardy, architektúry a protokoly počítačových sietí. Ďalej charakteristika aktívnych prvkov a ich funkcia v počítačových sieťach.

1.1 Referenčný model OSI

Model Open Systems Interconnection (OSI) popisuje, ako je informácia z aplikácie bežiaca na jednom počítači, pomocou sieťového média, prenášaná do aplikácie v inom počítači. Účelom modelu je definovať logické postupy, bez detailnejšieho opisu jednotlivých krokov, pri premiestňovaní informácie a následne ich zatrieďovať do skupín — vrstiev. Model definuje sedem vrstiev, kde každá zastupuje práve jednu skupinu funkcií. Podrobnosti o každej vrstve sú ponechané vývojárom. Určená je najmä celková funkcia vrstvy a vzájomný vzťah s vyššími a nižšími vrstvami. Vrstvy medzi sebou komunikujú pomocou rozhrania, ale každá vrstva pracuje samostatne a nie je závislá od ostatných [1][2]. Komunikáciu medzi zariadeniami zabezpečujú protokoly, definujúce pravidlá, podľa ktorých sú informácie posielané. Protokoly implementujú funkciu jednej či viacerých vrstiev. Existuje mnoho rôznych protokolov. Napríklad smerovacie protokoly pracujú na tretej vrstve referenčného modelu. Oproti tomu protokoly druhej vrstvy majú na starosti formátovanie a adresovanie paketov pre konkrétne prenosové médium. Napriek tomu, že sú jednotlivé vrstvy navzájom odlišné, musia spolu kooperovať, aby bola informácia prenesená rýchlo, efektívne a bez chýb [2][3].

1.2 Delenie počítačových sietí

Delenie počítačových sietí je dôležitý nástroj pri návrhu, popise a administrácií. Ako hlavný deliaci faktor definujeme veľkosť siete z pohľadu jej geografickej a administratívnej rozlohy. Podľa týchto kritérií následne identifikujeme tri hlavné kategórie [1][5].

Wide Area Network (WAN) — je typ siete, ktorá sa rozpína na veľkej geografickom území. Príkladom je Internet, ktorý je rozšírený po celom svete.

Tab. 1.1: Vrstvy referenčného modelu OSI.

Aplikačná vrstva	Definuje spôsob akým spolu komunikujú aplikácie v sieti
Prezenčná vrstva	Rieši kompresiu, dekompresiu, kódovanie a šifrovanie dát
Relačná vrstva	Nadväzovanie a udržiavanie relácie medzi komunikujúcimi stranami; práva, heslá, obmedzenia
Transportná vrstva	Fragmentuje datá na pakety a skladá správy z frangmetov; zabezbečuje bezchybnosť prenosu
Sieťová vrstva	Zaisťuje adresovanie a smerovanie v sieti od zdroja k cieli
Linková vrstva	Stará sa o bezchybný prenos rámcov mezi dvomi priľahlými uzlami
Fyzická vrstva	Prenáša dáta fyzickým médiom, bez ohľadu na ich význam; definuje charakteristiku signálu, konektory a pod.

Metropolitan Area Network (MAN) – siete typu MAN svojou rozlohou zaberajú veľkosť väčšieho mesta — metropole.

Local Area Network (LAN) — sieť, priestorovo limitovaná na menšie miesto; počítače zapojené v sieti, sú fyzicky umiestnené blízko seba.

Nasledujúce podkapitoly sa budú týkať najmä sietí LAN a MAN, v ktorých smerovací protokol OSPF zohráva dôležitú úlohu.

1.3 Topológie lokálnych sietí

Topológia siete označuje spôsob, ako sú počítače a ďalšie zariadenia v sieti prepojené. Rozdelenie podľa topológie úzko súvisí s použitými prenosovými prostriedkami, technologickým vybavení siete a použitými protokolmi. Je nutné rozlišovať medzi fyzickou a logickou topológiou:

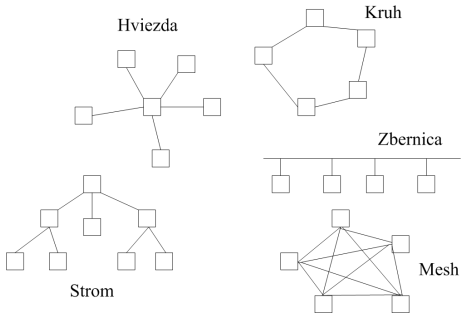
fyzická -– popisuje fyzické prepojenia, teda rozloženie prenosových prostriedkov a sieťových zariadení v miestnosti, budove alebo oblasti,

logická topológia -– popisuje prepojenia na vyšších vrstvách OSI.

Fyzické a logické topológie siete môžu byť identické, ale nie je to pravidlo. Napr. LAN ma fyzickú topológiu zodpovedajúcu hviezde a napriek tomu môže logicky spojovať

jednotlivé uzly ako kruh. V úlohe používam topológie typu hviezda a strom. Pri lokálnych sieťach sa stretávame s nasledujúcimi typmi topológii:

- hviezda – rozšírená v LAN; stanice sú spojené cez centrálny uzol,
- strom – hierarchický model s tranzitnými uzlami, ktoré zabezpečujú vetvenie,
- zbernica – bez centrálneho prvku; stanice pristupujú k jednému zdieľanému médiu,
- kruh – bez centrálneho prvku; každá stanica je uzol; komunikácie prebieha v kruhu,
- prepojená sieť – prepojenie každý s každým (full mesh); čiastočné prepojenie každý s každým (partial mesh) [1][5][4].



Obr. 1.1: Priestorová štruktúra hlavných typov topológií.

1.4 Architektúra lokálnych sietí

Architektúra sietí zahrňuje okrem špecifikácií definujúce fyzické a logické topológie aj použitý typ káblu, vzdialenostné obmedzenia, metódy prístupu, povolené veľkosti paketov, hlavičiek a ďalšie faktory.

Základná odlišnosť lokálnych od sietí MAN a WAN spočíva v komunikácií užívateľov na nižších vrstvách referenčného modelu. Predávanie správ medzi stanicami v lokálnej sieti eliminuje nutnosť smerovania na sieťovej vrstve. Väčšina LAN preto implementuje len najnižšie dve vrstvy — fyzickú a spojovú [6].

V obecnom povedomí — a najširšom používaní — sú predovšetkým dva typy lokálnych sietí Ethernet/IEEE 802.3 a Token Ring/IEEE 802.5, pričom silno prevažuje prvý menovaný. Dôvodom je najmä jednoduchá inštalácia, obsluha a zvyšovanie dostupných rýchlostí, ktoré je možné v niektorých prípadoch dosiahnuť bez nutnosti zásahu do stávajúcej infraštruktúry. Vývojová skupina pre architektúru 802.5 Token Ring je v súčasnej dobe neaktívna. Do popredia sa okrem už zmienených typov dostáva technológia bezdrôtových lokálnych sietí, ktoré predstavujú alternatívu ku klasickej kabeláži [7][8].

1.5 Hardware počítačových sietí

Sieť slúži na prepojovanie staníc poskytujúcich ostatným staniciam dáta, alebo služby. Požiadavky na prenos sú brané s ohľadom na rýchlosť, spoľahlivosť a náklady s ním spojené. Preto musí hardware počítačových sietí splňovať kritériá, ktoré zaručujú dodržanie týchto parametrov.

Medzi základný hardware bezosporu patria všetky typy kabeláže, ktoré sú často úzko zviazané s použitou sieťovou technológiou. Spojenie dvoch a viac počítačov je jednoducho realizovateľné pomocou jedného kábla a zapojenie do topológie zbernice. Takéto siete sa v dnešnej dobe takmer nevyskytujú z dôvodu ich nižšieho výkonu a slabých možnostiach administratívy. Aby bolo možné sieť aktívne riadiť a zabezpečiť, sú vytvorené spojovacie prvky: opakovače, rozbočovače, prepínače a smerovače, ktoré dokážu sieť rozdeliť na samostatné úseky. Jej funkciou je pre vytvorené úseky siete zaistiť funkčnosť, smerovať komunikáciu medzi nimi a vytvoriť redundantnú topológiu, pre väčšiu spoľahlivosť. Rozdelenie je dané podľa toho, na akej vrstve modelu OSI pracujú.

1.5.1 Opakovače a rozbočovače

Tieto zariadenia pracujú na posledných dvoch vrstvách. Opakovače sú veľmi jednoduché zariadenia, zosilňujúce signál na jednom fyzickom spoji. Rozbočovače fungujú na podobnom princípe ako opakovače s tým rozdielom, že zosilňujú signál na viacero výstupných portov.

V úlohe na simuláciu smerovacieho protokolu som tieto prvky nepoužil, pretože v dnešných návrhoch sietí sa už nevyskytujú. Sú nahradené modernejšími a inteligentnejšími zariadeniami. Dnes čiastočne nachádzajú uplatnenie pri testovaní a analyzovaní siete, keď je nutné zachytávať komunikáciu na dvoj, alebo viac-bodovom spoji [5].

1.5.2 Prepínače

Prepínač je aktívne zariadenie. V počítačových sieťach označenie prepínač – switch definuje aktívne zariadenie s väčším počtom portov, obyčajne 4 a viac, ku ktorým sa pripájajú najmä koncové stanice, ale aj ostatné sieťové prvky — rozbočovače, prepínače a smerovače.

Prepínač, pracuje na druhej vrstve modelu OSI. Dáta sú na tejto vrstve zabalené do rámca s hlavičkou. Obsahuje informácie o zdrojovej a cieľovej adrese, typu prenášaného protokolu, požiadavky na prenos a kontrolné súčty. Prepínač udržuje

tabuľku priradenia Media Access Control (MAC) adresy, alebo adries k portu. Databáza sa tvorí staticky – administrátorom vložený záznam, alebo dynamicky – záznamy prepínač automaticky pridáva podľa analýzy komunikácie v sieti [3].

Ako aktívne zariadenie druhej vrstvy, dokáže prepínač rozdeliť kolíznu doménu v jednom segmente na viacero menších. Medzi každým portom a stanicou, alebo iným zariadením, exituje nezávislá kolízna doména. Výhodou je fakt, že stanice už nezdieľajú jedno spoločné médium, ale o prístup sa delia s výrazne menším počtom zariadení — najčastejšie iba s prepínačom. Ďalšou nespornou výhodu je, že komunikácia, medzi prepínačom a zariadením, môže bežať oboma smermi — plný duplex . Rozdelenie jednej kolíznej domény na menšie nedelí sieť na menšie broadcast[1] domény, ale celá sieť ostáva súčasťou jednej domény [14].

1.5.3 Smerovače

Do skupiny zariadení, ktoré prepojuje dve a viac sietí patrí smerovač. Jejich úlohou je rozdeliť kolízne domény, filtrovať a blokovať broadcast vysielanie a zaisťovať optimálnu trasu pre smerovanie paketov k cieľu. Fungujú na sieťovej — tretej vrstve. Výkonné smerovače sú v skutočnosti veľmi silné počítače s vysokou mierou spracovania dát.

Na smerovače zaisťujúce spojenia v podnikových či metropolitných sieťach a na smerovače v chrbtovej sieti Internetu sú kladené vysoké výkonové a pamäťové nároky. K tomuto účelu slúžia dedikované zariadenia s špeciálnym hardvérom a softvérom.

Smerovače sú charakterizované dvoma oddelenými funkčnými systémami.

Riadiaca úroveň je v nej zabudovaná podpora protokolov na spoluprácu s ostatnými zariadeniami v sieti, čoho výsledkom je tabuľka s trasami pre doručenie komunikácie — smerovacia tabuľka. Obsahuje tiež funkcie filtrácie, blokovania a zaistenia kvality služieb Quality of Service (QoS).

Doručovacia úroveň preveruje pakety na vstupnom rozhraní a podľa informácií získaných z riadiacej úrovne, prenáša na správny výstupný port. Hardware tvoria špecifické typy čipov a spojovacích polí.

Úlohou oboch je spoločnou spoluprácou prijať a spracovať paket, vybrať správny výstupný port a dáta v čo najkratšom čase odoslať [3][7].

[1] všeobecné vysielanie, ktoré sa šíri v celej doméne [14]

2 PROTOKOLOVÁ SADA TCP/IP

Protokoly použité v úlohe vytvorenej v praktickej časti sú súčasťou protokolovej sady Transmission Control Protocol / Internet Protocol (TCP/IP). Či už je to IP pre adresovanie staníc a smerovačov v topológii úlohy, alebo samotný smerovací protokol OSPF. Teória je zameraná na predstavenie princípov, ktoré som použil v úlohe na vypracovanie.

Označenie TCP/IP vznikla z názvu dvoch protokolov: Transmission Control Protocol (TCP) teda protokol riadenia prenosov a IP – internetový protokol. TCP/IP sada však neobsahuje iba dva, už zmienené protokoly, ale označuje oveľa širšiu skupinu komunikačných protokolov na všetkých vrstvách referenčného modelu. Preto označenie TCP/IP bude vždy popisovať celú sadu protokolov a štandardov a nie len protokoly TCP a IP (za kompletné označenie sa pokladá The TCP/IP Internet Protocol Suit, požívam však skátené TCP/IP)[3].

Architektúra, podobne ako referenčný model OSI, umožňuje oprostiť sa od závislosti na sieťovej infraštruktúre a vnímať siete prepojené smerovačmi ako jednu veľkú, virtuálnu sieť. Internet je súbor navzájom prepojených a spolupracujúcich sietí, ktorý funguje na základe dohodnutých procedúr pre prenos a univerzálnych identifikátorov, napr. IP adries. Bez ohľadu na vlastnosti siete — priepustnosť, oneskorenie, veľkosť, sa TCP/IP chová rovnako na všetkých sieťach.

2.1 Vrstvový model TCP/IP

Podobne ako referenčný model OSI vznikol vrstvový model TCP/IP, opisujúci úlohy jednotlivých vrstiev v procese komunikácie medzi dvomi entitami. TCP/IP má redukovaný počet vrstiev — štyri, oproti siedmim v prípade OSI. Napriek tomu, že si tieto dva modely nezodpovedajú, sú vo svojej štruktúre hraníc a komunikačných funkcií veľmi podobné. TCP/IP sa v žiadnom prípade nesnaží nahradiť model OSI. Model OSI je všeobecný popis komunikácie medzi dvoma zariadeniami a TCP/IP konkrétne opisuje správanie zariadení v počítačovej sieti Internet [4][5].

2.2 Internetový protokol

Je jeden z hlavných protokolov, ktoré poskytujú funkciu doručovania paketov v architektúre TCP/IP. Pracuje na sieťovej vrstve modelu TCP/IP a zavádza adresovanie koncových bodov v sieti pomocou smerovateľných logických adries. Protokol IP vytvára datagram — paket. Obsahujúce hlavičku s informáciami o adrese odosielateľa a príjemcu datagramu, type prenášaných dát a údaje upresňujúce chovanie

siete pri prechode datagramu . IP protokol je nezávislý na fyzickej vrstve a vďaka tomu funguje v celej rade rôznych typov sietí. Je navrhnutý ako protokol poskytujúci nespoľahlivú službu bez spojenia, ktorý neudržuje žiadne informácie o datagramoch [8][14].

V súčasnosti fungujú dve verzie protokolu IP. Populárny a signifikantne rozšírený protokol Internet Protocol version 4 (IPv4) a novší Internet Protocol version 6 (IPv6). Súčasný Internet funguje na protokole IPv4 a protokol IPv6, ktorý má v budúcnosti nahradiť protokol IPv4, je v tejto dobe vo fázy ladenia a testovania na menších úsekoch Internetu. Oboje protokoly sa líšia najmä veľkosťou adresného priestoru a vytváraním hlavičiek paketov [2].

2.3 Adresovanie v IPv4

Je najrozšírenejším protokolom z rodiny sieťových protokolov a figuruje ako hlavný protokol pre komunikáciu na Internete. Špecifikovaný je podľa RFC 761 STD5 [8].

Umožňuje adresovať zariadenie v lokálnej sieti, alebo Internete pomocou unikátneho 32-bitového identifikátoru. Teoreticky je možné adresovať 2^{32} zariadení, čo v dekadickom zápise reprezentuje 4 294 967 296 jedinečných adries. Reálne však nie je možné adresovať toľko zariadený z dôvodu delenia adresného rozsahu a definovanie špecifických typov adries, ktoré nie sú určené pre koncové zariadenie a sieťové uzly.

32 bitov IP adresy je zapisovaných po bytoch, ktoré sú medzi sebou oddelené bodkou. Rozoznávame viaceré formy zápisu:

- dvojkový – jednotlivé byty zapisujú po bitoch v dvojkovej sústave, napr: 10101010.11001100.11111111.00000011.
- Desiatkový – číslo v binárnej sústave sa po bytoch prevedie do dekadickej sústavy, 170.204.255.3.
- Hexadecimálny – jednotlivé byty adresy reprezentuje číslo v šestnástkovej sústave, aa.cc.ff.3 [5].

IP adresa sa skladá z dvoch častí.

- Adresa siete -– prvá časť adresy. Jednoznačne identifikuje sieť v LAN, alebo Internete. Slúži najmä pre účely smerovania.
- Adresa uzlu — druhá časť adresy identifikuje konkrétne zariadenie v sieti.

2.4 Rozdelenie adries podľa tried

S pribúdaním počtu inštitúcií a firiem pripojených do Internetu sa systém rozdelenia adresného priestoru stával nedostatočný a neefektívny. Z týchto dôvodov sa

zaviedla nová adresná schéma rozdeľujúca adresný priestor na triedy s rôznou dĺžkou identifikátoru siete. Výrazne sa rozšírili možnosti adresovania sietí, ktoré bolo možné efektívne prideliť na základe počtu koncových zariadený a uzlov v sieti. Adresa môže byť zaradená do jednej z piatich tried [4][7].

Tab. 2.1: Rozdelenie IP adries do tried.

Trieda	**Začiatočnébity**	**Počet bitovsiete**	**Počet zariadení**	**Začiatok rozsahu**	**Koniec rozsahu**
A	0	8	16 777 216	0.0.0.0	127.255.255.255
B	10	16	65 536	128.0.0.0	191.255.255.255
C	110	24	256	192.0.0.0	223.255.255.255
D (multicast)	1110	nedefinované	nedefinované	224.0.0.0	239.255.255.255
E (rezerva)	1111	nedefinované	nedefinované	240.0.0.0	255.255.255.255

2.5 Typy adries

V sieťach s podporou sieťového protokolu IPv4 je možné na základe cieľovej adresy a charakteru komunikácie rozdeliť spôsoby posielania paketov do následujúcich skupín.

- Jednosmerové (unicast) — pakety majú ako cieľovú adresu uvedenú unikátnu adresu priradenú práve jednému zariadeniu v LAN, alebo Internete. Tieto adresy sú definované v triedach A, B a C.
- Viac-smerové (multicast) — sú to adresy triedy D. Používajú sa na komunikáciu viacerých účastníkov v rôznych sieťach. Smerovače tieto pakety duplikujú na všetky rozhrania, z ktorých prišla požiadavka na prijímanie dát zo skupiny viacsmerového vysielania — multicastovej skupiny. z pravidla tieto pakety obsahujú multimediálne dáta, alebo riadiace informácie smerovacích protokolov (OSPF) a dohľadových protokolov vyšších vrstiev.
- Všeobecné lokálne (local broadcast) — používa sa na komunikáciu v rámci jednej siete pre prípad, keď je nutné rozoslať informácie všetkým zariadeniam v miestnej podsieti. Využívajú ho najmä služby zabezpečujúce správne fungovanie siete.
- Všeobecné (broadcast) — vysiela sa v prípade, keď zariadenie potrebuje osloviť všetky zariadenia v konkrétnej podsieti [2].

Medzi špeciálne adresy, ktorými však je možné jednoznačne určiť iba stanicu v lokálnej sieti, patria privátne adresy. Pre tieto adresy sú vyčlenené nasledujúce rozsahy:

- trieda A — 10.0.0.0,
- trieda B — 172.16.0.0 až 172.31.0.0,
- trieda C — 192.168.0.0 až 192.168.255.0.

Adresa z tohto rozsahu nesmie v Internete použitá ani smerovaná. Pakety prichádzajúce z adresy v rozsahu privátnych sietí, budú na internetových smerovačoch

zahodené. Privátne adresy sa používajú v absolútnej väčšie lokálnych sietí, pretože nemusia byť v rámci Internetu unikátne.

2.6 Podsiete a adresovanie v podsieťach

Do úlohy som začlenil techniku podsieťovania. Je samostatným zadaním a pre úspešné dokončenie úlohy je nevyhnutná. Študent by mal ovládať pricípy techniky variabilnej sieťovej mastky Variable Length Subnet Mask (VLSM) a jej smerovania Classless Inter-Domain Routing (CIDR), pretože sa využíva nie len v IPv4, ale aj v IPv6.

S postupným rozširovaním Internetu a zväčšujúcemu sa počtu pripojených zariadení, sa ukázalo, že rozdelenie adresného priestoru do sietí nie je efektívne. Nedostatok adries staníc pre triedy C a naopak nevyčerpateľnému prebytku v triede A, dalo v roku 1993 vzniknúť normám RFC 1517 až 1520. Definujú mechanizmus zvaný podsieťovanie –subnetting, teda keď viacero sietí zdiela rovnaký prefix. Systém podsieťovania výrazne optimalizuje využitie prefixov tým, že použitie prefixu nie je obmedzené na jednu lokálnu sieť, ale dáva vzniknúť väčšiemu počtu lokálnych sietí oddelených smerovačom [10].

2.6.1 Sieťová maska

Z dôvodu nového prístupu k deleniu adresného priestoru, ktorý už nie je založený na zoskupovanie do tried s rôznou dĺžkou prefixu, je nutné dôslednejšie rozlišovať časť IP adresy označujúca sieť a časť, ktorá označuje stanicu v danej sieti. Sieťová maska je nástroj, ktorý určuje, ktoré bity v IP adrese tvoria adresu siete. Sieťová maska je, podobne ako IP adresa, štyr-bytová. Na pozícii bitov označujúcich adresu siete a adresu podsiete, je hodnota bitov masky 1, na miestach bitov slúžiacich k identifikácii časti adresy pre stanice je hodnota 0. Vynásobenie IP adresy a príslušnej masky dostávame adresu siete.

Sieťovú masku je možné zapisovať viacerými spôsobmi. Najčastejšie sa maska zapisuje v dekadickej forme, podobne ako IP adresa. Teda štyri byty oddelené bodkou. Alebo skrátenou notáciou, ktorá udáva počet jednotkových bitov v maske. Toto číslo sa zapisuje spolu s IP adresou, napr. 192.168.3.0/24 [10][13].

2.6.2 Premenlivá dĺžka masky podsiete VLSM

Pôvodne sa predpokladalo, že diferenciácia na podsiete bude dostatočný mechanizmus na efektívneho využívania prideleného prefixu a tým ja celého adresného rozsahu. Preto sa v rámci jednej IP siete využívala rovnaká maska podsiete a teda

všetky segmenty lokálnej siete používali rovnakého počtu bitov pre adresovaniu zariadení a uzlov. Sieť sa však môže skladať zo segmentov, v ktorých je počet staníc výrazne odlišný. Dôvodom môže byť organizačná štruktúra siete, v jednom oddelení je viac počítačov ako v druhom, alebo použitá technológia, sériové rozhranie môže spojovať lem dve body. Zatiaľ čo technológia Ethernet dovoľuje spojovať desiatky staníc. Rozdelenie prefixu na niekoľko rovnakých podsietí je vo väčšine prípadov neefektívne a plytvá prideleným adresným priestorom.

Z tohto dôvodu sa zaviedlo technika nazývaná VLSM – variabilná dĺžka masky podsiete, definovaná v RFC 1812. Umožňuje využívať rôzneho počtu bitov pre adresovanie podsiete z prideleného prefixu podľa konkrétnych požiadavkou na podsieť – množstva staníc pripojených k segmentu [14][13].

2.6.3 Smerovanie bez použitia adresných tried CIDR

CIDR prekonáva obmedzenia kladené triedami adries na smerovanie v Internete a lokálnych sieťach. S rozširovaním Internetu sa ukázalo nevhodné budovať smerovanie tabuľky na základe tried IP adries. Využívanie mechanizmu smerovania podľa tried neumožňuje dostatočne agregovať záznamy v smerovacích tabuľkách smerovačov a tým výrazne narastajú pamäťové nároky a nároky na rýchle spracovanie paketov pri prechode smerovačom. Je nutné rýchlo nájsť odpovedajúcu cestu v smerovacej tabuľke.

CIDR umožňuje agregovať adresy na základe spoločného prefixu do väčších celkov — supersietí bez ohľadu na triedu adries. CIDR je protiklad systému podsietí a teda často označovaný ako nadsieťovanie – supernetting. Využíva však všetky techniky použité pri tvorbe podsietí. CIDR zmenšuje počet jedničiek v sieťovej maske a tým generalizuje záznam v smerovacej tabuľky, ktorý následne reprezentuje viacero IP sietí v Internete. Existencia konkrétnych sietí je pre smerovače Internetu skrytá vďaka supersieťam a smerovanie ku konkrétnym IP adresám zabezpečujú smerovače umiestnené bližšie jednotlivým sieťam. Takáto technika zmenšuje nároky na pamäť a výkon čím umožňujú sieťovým uzlom pracovať rýchlejšie [10][11].

2.7 Transportné protokoly

Transportná vrstva TCP/IP zodpovedá transportnej vrstve podľa referenčného modelu OSI, pretože poskytuje mechanizmus pre koncový prenos dát medzi dvomi stanicami. Služba, ktorú táto vrstva ponúka vyšším vrstvám, môže byť buď spoľahlivá, alebo nespoľahlivá, za použitia jedného z dvoch dostupných protokolov.

- TCP — transportný protokol poskytuje spoľahlivú, spojovo orientovanú službu. Vytvára obojsmerný logický komunikačný kanál medzi dvomi aplikáciami. Je transparentná pre aplikácie — prenáša ľubovolné dáta.
- User Datagram Protocol (UDP) — je na rozdiel od TCP veľmi jednoduchý protokol. Poskytuje nespoľahlivý prenos dát, pre aplikácie, ktoré nepožadujú zaistenie zabezpečenie prenosu proti chybám. Aplikácia kompletne preberá zodpovednosť za túto službu. UDP nenadväzuje spojene keď začína prenášať dáta.

Po tom čo sú dáta prenesené jedným z transportných protokolov k cieľovému uzlu, je dôležité určiť, ktorému procesu ich priradiť. Transportná vrstva rozbalí hlavičku datagramu a určí cieľový proces na základe číselného identifikátoru — portu. Port je pre daný uzol unikátne 16-bitové číslo identifikujúce proces. Po tom, čo transportná vrstva určí číslo portu, predá dáta konkrétnej aplikácii[3][14].

3 SMEROVANIE V IP SIEŤACH

Praktická časť diplomovej práce má ukázať fungovanie smerovacieho protokolu OSPF, ktorý patrí do skupiny smerovacích protokolov používajúcich stav linky. Na vysvetlenie, čo to smerovacie protokoly používajúce stav linky sú a aké iné typy existújú, som zaradiť túto kapitolu do teoretickej časti. Vysvetluje základy smerovania paketov v IP sieťach.

3.1 Základny smerovania paketov

V rozsiahlejších sieťach so smerovačmi, už nie je možné smerovať pakety medzi stanicami pomocou fyzických adries rozhraní. Preto sa využíva adresovania pomocou IP adresy siete a zariadenia. Pre zabezpečenie konektiviti medzi všetkými prvkami siete, vyžaduje vybaviť smerovače prostriedkami, s ktorými budú schopné správne určiť trasu k požadovanej sieti. Aby mohol smerovač správne fungovať, potrebuje poznať minimálne informácie k odoslaniu paketu do siete:

- cielovú adresu,
- susedné smerovače, ktorým môže prípadne preposlať paket,
- všetky trasy do siete,
- optimálne trasy do siete,
- spôsob kontroly a údržby smerovacích informácií.

Cieľovú adresu získa smerovač ľahko, analyzovaním hlavičky IP paketu. Ďalšie zmienené parametre už hlavička datagramu neobsahuje a potrebuje ich získať z iných zdrojov. Základnou možnosťou je priamo od správcu, alebo zložitejšou, ale zato efektívnejšou, nepriamo od vzdialených smerovačov cez smerovacie protokoly [11].

3.2 Statické smerovanie

O statické smerovanie sa jedná v prípade, že administrátor siete zadá všetky informácie o trase k sieti priamo do smerovacej tabuľky každého smerovača na plánovanej ceste [13].

3.3 Dynamické smerovanie

Optimálnu cestu v dynamickom smerovaní hľadajú smerovacie protokol. Pri hľadaní sietí a aktualizácii smerovacích tabuliek využívajú protokoly informácie získané zo susedných smerovačov. Údržba takéhoto systému je samozrejme výrazne jednoduchšia a najväčšie zásahy vyžaduje pri implementácii smerovacieho protokolu do

smerovačov v sieti. Systém sa už ďalej postará o výmenu informácií a udržovaní funkčných ciest medzi sieťami. Na výmenu záznamov o cestách a sieťach sa však využíva nezanedbateľná šírka pásma, s ktorou je nutné pri návrhu siete počítať [8].

3.3.1 Smerovacie protokoly s vektorom vzdialeností

Protokol s vektorom vzdialeností hľadá najlepšiu cestu do cieľovej siete na základe vektoru vzdialenosti. Vzdialenosť definuje počet preskokov — prechodov smerovačmi. Trasa do siete, ktorá obsahuje najnižší počet preskokov, je považovaná za optimálnu. Vektor označuje smer do vzdialenej siete Medzi protokoly s vektorom vzdialeností patria smerovacie protokoly Routing Information Protocol (RIP) a Interior Gateway Protocol (IGP). Systém preskokov používa aj smerovací protokol Internetu Border Gateway Protocol (BGP) [10].

3.3.2 Smerovacie protokoly používajúce stav linky

Smerovače s aktivovaných protokolom, ktorý ako relevantnú informáciu používa stav linky. Rozposiela informácie o sebe a pomocou prijatých informácií od ostatných smerovačov v sieti dokáže vytvoriť obraz topológie siete. Na takúto mapu následne aplikuje vhodný algoritmus, ktorého výstupom je najlepšia cesta k cieľu. Ak nastane zmena topológie, smerovač okamžite o tom informuje ostatné smerovače v sieti, ktoré okamžite prepočítajú cesty a aktuálne najlepšiu vložia do smerovacej tabuľky [8][11].

3.4 Administratívna vzdialenosť AD

Oceňuje dôveryhodnosť smerovacej informácie, ktoré smerovač získal z rôznych zdrojov. Administratívna vzdialenosť sa udáva celým číslom od 0 do 255, kde hodnota 0 identifikuje najdôveryhodnejší záznam. Pokiaľ má smerovač viac záznamov o ceste k cieli, najskôr skontroluje hodnotu Administrative Distance (AD). A ďalej bude preferovať trasu s najnižšou hodnotou AD [4].

4 SMEROVACÍ PROTOKOL OSPF

Nasledujúce kapitoly popisujú smerovací protokol OSPF a to ako základnú konfiguráciu, tak i zložitejšie implementačné techniky, ktorými je možno optimalizovať smerovanie v autonómnych systémoch[1]. Praktická časť diplomovej práce implementuje veľkú väčšinu popísaných techník a vlasntostí, o ktorých sa v naslednujúcich podkapitolách zmienim.

4.1 Základy smerovacieho protokolu OSPF

OSPF je smerovací protokol otvoreného štandardu, ktorý implementuje mnoho dodávateľov aktívnych prvkov siete. Problematiku výberu najlepšej cesty rieši na základe stavu liniek. V Internete a v mnoho ďalších prípadoch hraje veľmi často úlohu interného smerovacieho protokolu pre autonómny systém – AS. No dokáže prijať a spracovať informácie aj z iných AS. Najdôležitejšie charakteristiky protokolu OSPF:

- používa hierarchický model oblastí,
- minimalizuje réžiu,
- umožňuje škálovateľnosť,
- podporuje VLSM/CIDR,
- neobmedzuje počet preskokov.

Fungovanie protokolou je založené na Dijkstrovom algoritme. Protokolo OSPF konverguje rýchlo a podporuje viac trás s rovnakými nákladmi do jedného cieľa. Najnovšia verzia Open Short Path First version 3 (OSPFv3) obsahuje podporu nového štandardu IPv6 no v súčasnosti najrozšírenejšou ostáva Open Short Path First version 2 (OSPFv2) pre IPv4 [8][11][13].

4.2 Výmena databáze komunikácia medzi smerovačmi

4.2.1 Identifikátor smerovačov

Kým začne smerovač odosielať zprávy ostatným smerovačom v sieti, musí si zvoliť jedinečný 32-bitový identifikátor – Router Identifier (RID). Najčastejšie sa zapisuje po bajtoch v desiatkovej sústave, podobne ako adresa IPv4. Identifikátor smerovača v OSPF, RID, si volia zariadenia podľa následujúceho postupu. K ďalšiemu kroku dochádza iba vtedy, pokiaľ sa nepodarilo identifikátor určiť v kroku predchádzajúcom.

[1]Časť internetu s rovnakým IP prefixom, smerovacím protokolom a najčastešie pod správou jednej organizácie, alebo Internet service provider – poskytovateľ Internetového pripojenia (ISP)

1. Identifikátor smerovača, zadaný príkazom **router-id** v konfiguračnom režime protokolu OSPF.
2. Najvyššia IP adresa aktívnej lokálnej slučky — loopback[2] rozhrania.
3. Použije sa najvyššia IP adresa na akomkoľvek aktívnom rozhraní, ktoré je v stave „*up up*“.

Nastavovanie RID má presne dané pravidlá. Pre prehľadnosť a jednoduchú administráciu je vhodné explicitne zadávať IP a to buď pomocou príkazu **router-id**, alebo konfiguráciou lokálnej slučky, ktorá môže byť rozhlasovaná do OSPF. Následne je možné pomocou Internet Control Message Protocol (ICMP)[3] správ testovať spojenie medzi na konkrétny smerovač. Pre logiku nastavenia RID platí niekoľko zásad.

- Rozhranie z ktorého si smerovač preberá RID nemusí byť súčasťou OSPF domény.
- Identifikátor RID nemusí byť dosiahnuteľný cez smerovacie tabuľky.
- V krokoch dva a tri sa RID volí podľa rozhraní, ktoré boli aktuálne v okamžiku spustenia procesu OSPF.
- OSPF sa môže zmeniť pri reštarte procesu OSPF, alebo explicitne zmenou RID v konfigurácii [9].

4.2.2 Prenos správ OSPF medzi smerovačmi

Smerovací protokol OSPF komunikuje so svojimi susedmi pomocou piatich typov správ. Každý typ je charakteristický obsahom, ktorý prenáša. OSPF komunikuje na transportnej vrstve TCP/IP a v IP záhlaví, v položke Protocol, je vedený pod číslom 89 [14].

Komunikáciu medzi smerovačmi je môžné rozdeliť do troch častí: naväzovanie susedstva medzi smerovačmi, výmena databáze, udržiavanie a aktualizovanie databáze.

4.2.3 Naviazanie susedstva medzi smerovačmi

Tato časť je prvou a veľmi dôležitou súčasťou celej komunikácie medzi smerovačmi v OSPF doméne. Pokiaľ sa nepodarí naviazať susedstvo, žiadne ďalšie informácie sa neprenášajú a smerovanie v sieti môže byť výrazne obmedzené, alebo celkom nefunkčné.

Smerovače používajú na naviazanie susedstva správy Hello. Zprávy Hello začínajú komunikáciu medzi smerovačmi a súčasne plnia funkciu sledovania susedov. Tri hlavné účely správ Hello sú:

[2] Virtuálne rozhranie na sieťových zariadeniach, ktoré ma vlastnú IP adresu.
[3] Protokol pre administráciu počítačových sietí.

- rozpoznanie smerovačov OSPF v spoločnej sieti,
- autentifikácia (voliteľná) a kontrola zhody nastavených parametrov,
- sledovanie a vyhodnocovanie stavu susedov a detekcia prípadného výpadku.

Akonáhle je OSPF proces aktívny, smerovač začne počúvať na viacsmerovej adrese 224.0.0.5 zprávy Hello a to na všetkých rozhraniach so zapnutým protokolom OSPF. Ako zdrojový adresa paketu je uvedená IP adresa z výstupného rozhrania smerovača. Akonáhle obdrží smerovač správu Hello, začne analyzovať uvedené údaje a vyhodnotí, či je, alebo nie je možné naviazať susedstvo so smerovačom, ktorý Hello správu odoslal. Hello správa prejde následujúcimi kontrolami:

- autentizačný proces (pokiaľ je vyžadovaná autentizácia),
- musia sa nachádzať v rovnakej podsieti s totožnou maskou siete,
- rozhranie ktoré prijalo Hello správu je v rovnakej OSPF oblasti (identifikátor aj typ),
- nesmie mať duplicitné RID,
- zhodné hodnoty časovačov Hello a Dead.

Pokiaľ akákoľvek z vyššie uvedených podmienok je vyhodnotená ako nesplnená, smerovače medzi sebou nevytvoria žiadnu reláciu — susedstvo. Čísla procesov nie sú súčasťou kontroly a teda nevyžaduje sa zhoda.

Po procese naviazania susedstva, plnia Hello správy tretiu funkciu a to udržiavanie už naviazanej relácie medzi smerovačmi. OSPF vyžaduje, aby Hello správy prichádzali od susedov periodicky, teda ide o systém neustáleho oživovania spojenia — keepalive. Implicitné hodnota časovaču Hello na Cisco zariadeniach je 10 s. Pokaľ smerovač neprijme paket so správou Hello do uplynutí časovaču Dead, považuje suseda za neaktívneho a neustále vyčkáva na Hello správu. Zároveň rozhlási správu o nefunkčnom susedovi ostatným smerovačom. Nastavenie intervalov je možné meniť. Východzia hodnota Dead sa rovný štvornásobku hodnote Hello intervalu [3][9][8][13].

4.2.4 Výmena databáz

Akonáhle naviažu cez Hello zprávy smerovače susedstvo, začnú proces výmeny informácií. Synchronizácia databáz prebieha v niekoľkých krokoch.

1. Smerovač si navzájom vymenia tabuľku Database Description (DBD). Tá obsahuje hlavičky záznamov Link State Advertisment (LSA) ktoré sú súčasťou Link-State Database (LSDB). Hlavička dáva informáciu smerovaču, podľa ktorej dokáže každé LSA jednoznačne identifikovať: type, adresu smerovača, ktorý LSA rozhlasoval, metriku a sekvenčné číslo. LSA môže prenášať informáciu o stave linky, aj informáciu o sieti.

2. V tejto chvíli ma každý smerovač zoznam LSA, ktoré sú známe susedovi. Porovná záznamy s prijatej DBD so svojou LSDB databázou a vyhodnotí vysledok. Pri porovnaní môže nastať jedna z troch situácií:

   nenašla sa žiadna zhoda medzi lokálnou LSDB a DBD,

   našiel sa rovnaký záznam LSA, ale sekvenčné v LSDBje menšie ako v DBD,

   našla sa zhoda v LSA medzi LSDB a DBD, ale lokálne sekvenčné číslo je rovnaké, ako to zo susedovej tabuľky.
3. V prípade, že smerovač vyhodnotí, že nemá konkrétne LSA, alebo záznam nie je aktuálny a existuje iný s vyšším sekvenčným číslom, vyšle Link State Request (LSR) susedovi, ktorý vo svojej DBD ohlasoval aktuálnejšie LSA. Ten mu odpovie správou Link State Update (LSU), ktorá obsahuje jeden alebo viacej kompletných LSA. Ak sa sekvenčné čísla zhodujú smerovač nežiada žiadne ďalšie informácie. Počas celého procesu výmeny sú smerovače v stave Loading až do doby, kedy si obaja nevymenili a synchronizovali LSDB. Vtedy prechádzajú zo stavu Loading do stavu Full [7].

Proces zasielania LSU používa spoľahlivý prenos, kedy hneď ako smerovač prijme a vyhodnotí, či nedošlo pri prenose k chybe, pošle potvrdenie Link State Acknowledgement (LSAck) s hlavičkami, ktoré LSA obsahovalo. V tomto okamžiku, kedy sú LSDB plne synchronizované, môžu nezávisle na sebe spustiť výpočet algoritmu a vypočítať zo svojho pohľadu najlepšie cesty k cieľovým sieťam.

4.2.5 Udržiavanie synchronizácie a činnosti v stabilnom stave

Ani po výmene záznamov, prechode do stavu Full a výpočte najlepších ciest, neprestane smerovač komunikovať s okolím. Každý smerovač odosiela správy Hello a informuje suseda o svojom stave. Súčasne očakáva, že dostane od suseda Hello správu do vypršania časovaču Dead; v opačnom prípade je považovaný za neaktívneho. Ak zistí zmenu v stave linky alebo siete — link-state, okamžite vyšle LSU, ktoré obsahuje aktuálny stav LSA s inkrementovaným sekvenčným číslom. LSU zaplaví celú sieť, tak aby každý smerovač mohol synchronizovať svoju LSDB a prepočítať cesty.

Každých 30 minút rozposiela do siete LSU Refresh so záznamom LSA, ktoré sám spravuje (nie, ktoré sa naučil do ostatných smerovačov) s inkrementovaným sekvenčným číslom. Každý záznam na svoj vlastný časovač, podľa ktorého sa rozhoduje, kedy je potrebné poslať LSU Refresh. Zároveň sám očakáva obnovovacie LSU pre naučené LSA a pokial žiadny nedostane do 60 minút, vymaže ho z LSDB [10]

4.3 Voľba referenčného a záložného referenčného smerovača

Lokálne siete typom komunikácie zapadajú do triedy s všeobecným vysielaním. Teda siete v ktorých technológie na fyzickej vrstve a linkovej vrstve podporujú šírenie všeobecnej komunikácie a pripojenie viac staníc do jedného segmentu. Príkladom je najrozšírenejší Ethernet.

Protokol OSPF používa pre optimálizáciu procesu a zníženie réžie na dátových linkách s viac-násobným prístupom, princíp voľby Designated Router – referenčný router (DR) – referenčného a Backup Designated Router (BDR) – záložného referenčného smerovača. Bez centralizovaného prvku by totiž každé dva smerovače museli naviazať susedstvo s každým, čím by vznikla full mesh topológia čo by pri výmene LSU výrazne zaťažovalo sieť. Na sieťach LAN a ostatných s viacnásobným prístupom, naväzujú smerovače susedstvo jedine s DR alebo BDR. Akékoľvek plošné rozosielanie dát prechádza cez DR, ktorý sa stará o distribúciu ostatným smerovačom. Výrazne sa znižuje objem OSPF správ prenesených v sieti.

Proces voľby určeného a záložného smerovača prebieha iba v segmentoch, ktoré používajú broadcast komunikáciu a iných sietí s viacnásobným prístupom. U dvojbodových spojení (sériové spojenie), k voľbám DR a BDR nedochádza [5][13].

4.3.1 Proces voľby

Pri voľbe centrálneho smerovača a záložného sa využíva, tak ako pri naviazaní susedstva, správa Hello. V každom segmente sa pomocou multicast paketov posiela Hello. Voľba DR a BDR sa riadi následujúcimi pravidlami.

- Každý smerovač s prioritou z intervalu 1–255 sa pokúša stať sa DR, pokial do poľa DR odosielaných správ zapíše svoje RID.
- Ak je priorita nastavená na 0, smerovač sa nezúčastňuje voľby.
- Smerovače kontrolujú hodnotu priority a RID v priatých správach Hello.
- Pokial sa v Hello objaví potencionálne lepší referenčný smerovač; prestane sa smerovač usilovať o pozíciu DR.
- Prvým kritériom je priorita, čím väčšia tým má smerovač väčšiu šancu stať sa DR.
- Druhým kritériom pri zhode priorít je RID, volený je smerovač s najvyšším RID.
- Smerovač, ktorý skončil „druhý“ sa stáva BDR.
- Pokial sa po skončení voľby objaví nový smerovač, alebo niektorý zo stávajúcich zmení prioritu, nemôže rolu DR ani BDR prevziať.
- Ak nastane výpadok DR, funkciu preberá BDR a opakuje sa voľba BDR [13].

4.3.2 Rozosielanie správ v sieti s DR a BDR

Smerovače, ktoré nie sú referenčný alebo záložným referenčný smerovač a potrebujú odoslať správu ostatným; využijú viac-smerovou adresou 224.0.0.6. DR potvrdí prijatie a plošne prepošle ostatným smerovačom v broadcast sieti na viac-smerovú adresu 224.0.0.5, štandardná adresa pre výmenu dát v OSPF. Ostatné smerovače jednotlivo potvrdia prijatie správy.

BDR podobne ako DR neustále počúva na viac-smerovej adrese 224.0.0.6 a spracováva správy z ostatných smerovačov no na rozdiel do BDR neposiela potvrdenia ani aktualizácie. Pri výpadku DR okamžite preberá funkciu BDR a prebieha voľba nového DR [9].

4.3.3 Susedstvo medzi smerovačmi

Smerovače, ktoré nie sú DR ani BDR označujeme ako DROTHER. Ako už bolo zmienené, smerovače komunikujú výhradne cez DR. Preto musia mať medzi sebou vytvorenú reláciu — susedstvo, ktoré je v stave Full a teda obsahujú identické LSDB. DROTHERs smerovače sa však susedmi nestanú, napriek tomu, že všetky parametre v Hello správach sú zhodné a teda splňujú podmienku vytvorenia susedstva. Pretože si DROTHERS priamo medzi sebou nevymieňajú žiadne OSPF dáta uvádza sa, že sú v stave priľahlé.

4.4 Hľadanie najlepšej cesty

Akonáhle získa smerovač všetky informácie o sieti, synchronizovaná LSDB, potrebuje zistiť, ktorá cesta je k jednotlivým sieťam najvýhodnejšia. Z LSU dokáže zistiť metriku a pomocou algoritmu vypočítať ideálne smerovanie paketov k cieli.

4.4.1 Metrika linky

Hodnotenie výhodnosti linky je založené na jednej bez rozmernej veličine — metrike, obecne označovanej ako cena. Definuje aké sú „náklady“ sú spojené s prenosom paketu po spoji. Náklady na celú cestu sú dané súčtom cien výstupných rozhraní pozdĺž celej cesty. Na akých parametroch závisia náklady je podľa štandardu RFC 2338 možné voliť ľubovoľne. Smerovače Cisco definujú výpočet nákladov, na všetkých rozhraniach s podporou protokolu OSPF, podľa jednoduchej rovnice.

$$cena = 100000000/ < rychlostlinky > [b/s][11]. \tag{4.1}$$

Šírka pásma zodpovedá konfigurovanej šírke pásma rozhrania, napr. Fast Ethernet s rýchlosťou 100 Mb/s bude mať cenu 1. Cenu linky je možné zmeniť aj príkazom

ip cost v konfiguračnom režime rozhrania. V prípade nasadenia technológie, ktorá má šírku pásma väčšiu, ako je referenčná hodnota 100 000 000, je vhodné zväčšiť referenčnú hodnotu.

4.4.2 Výpočet stromu najkratších ciest

Smerovač počíta pre každú oblasť najkratšiu cestu do sietí v danej oblasti. K výpočtu používa dáta zhromaždené v LSDB a algoritmus, označovaný ako Dijkstrov algoritmus najkratšej cesty Shortest Path First (SPF). Výsledkom je matematický model siete — strom. Najkratšie cesty sú vybraté zo stromu a vložené ako záznam do smerovacej tabuľky. Strom je nutné prepočítať vždy, keď smerovač získa novú, alebo aktuálnejšiu informáciu o linke [13][14].

4.5 Delenie OSPF domény na oblasti

Topologické tabuľky — LSDB smerovačov obsahujú informácie o celej sieti, čo sa premieta do pamäťovej a výpočtovej náročnosti OSPF. V komplexnejších sieťach môže nastať niekoľko problémov spojených so smerovacím protokolom.

- Častý výpočet SPF algoritmu – veľká sieť obsahuje množstvo liniek ktoré sú musia byť pravidelne aktualizované a zvyšuje sa frekvencia náhodných zmien v topológii (poruchy, pripojenie novej siete a pod.). Pri každej takejto zmene sa musí prepočítať strom z ktorého sú vyberané najlepšie cesty.
- Veľké smerovacie tabuľky — OSPF automaticky nesumarizuje siet, takže jedna sieť znamená jeden záznam v smerovacej tabuľke.
- Pamäťová náročnosť LSDB — smerovač musí uchovávať stavy všetkých liniek v sieti [8].

OSPF dokáže sieť rozdeliť na menšie celky, ktoré sú známe ako oblasti a identifikované 32-bitovým číslom najčastejšie zapisovaným v desiatkovej sústave. Oblasti majú hierarchické delenie do dvoch úrovní. V prvej úrovni je oblasť 0, ktorá je základná — tranzitná a všetky smerovače vo východzej konfigurácii patria práve do nej. Druhú úroveň tvoria všetky ostatné oblasti, ktoré musia priamo susediť s tranzitnou oblasťou[4]. Používanie oblastí v rozsiahlych sieťach odstraňuje nežiadúce faktory.

- Redukuje frekvenciu výpočtu SPF – algoritmus počíta cesty pre menší počet liniek.
- Znižuje počet záznamov v smerovacej tabuľke — pri správnom návrhu je možné jednoducho

[4]Exituje využite virtuálneho spojenia cez okrajovú oblasť s tranzitnou cez inú okrajovú oblasť. Používanie sa neodporúča

- sumarizovať[5].
- Menej záplavových LSU — menšie množstvo liniek znamená menší počet LSU v sieti.

Hranice oblastí sú vždy na smerovači a nie na linke. Oblasť sa definuje na rozhraní a preto sa môže smerovač nachádzať zároveň v transportnej aj okrajovej oblasti. Podľa toho, do akej oblasti sú rozhrania priradene, delíme smerovače do skupín.

Vnútorné smerovače : všetky rozhrania majú pridelený rovnaký identifikátor oblasti; rozposielajú všetky LSA, ktoré príjmu.

Hraničné smerovače oblastí Area Border Router (ABR) : ak sú rozhrania s aktívnym protokolom OSPF, pridelené do rôznych oblastí — jedna z nich je vždy tranzitná, potom slúži smerovač ako most medzi oblasťami a okrem štandardných funkcií rieši filtráciu LSA správ a rozposielanie defaultných ciest.

Hraničné smerovače autonómneho systému Autonomous System Border Router (ASBR) : smerovače nemajú obmedzenie na umiestnenie v logickej topológii. Spojujú autonómny systém s iným, alebo sprostredkovávajú spojenie do sietí s odlišným smerovacím protokolom [10].

4.6 Typy LSA správ

LSAs sú stavebné bloky OSPF topologickej databáze — LSDB. Samostatne sa chovajú ako záznamy a v kombinácii popisujú celú OSPF sieť, alebo oblasť. LSA je dátová štruktúra, ktorá obsahuje hlavičku s informáciami (pôvodca LSA, identifikátor LSA, sekvenčné číslo, typ a iné) a dáta. LSA je možné rozdeliť podľa typu do 11 skupín.

4.6.1 Oznámenia LSA typu 1 a 2

Každý smerovač generuje LSA s informácie o seba, priamo pripojených linkách s aktuálnymi stavom a zoznam susedných smerovačov. Udaje sú platné pre oblasť v ktorej má smerovač aktívne rozhranie a pre každú oblasť vytvára samostatné LSA typu 1, a rozposiela do konkrétnej oblasti — rozhrania.

LSA druhého typu je vytváraný v sieti s všeobecným vysielaním (Ethernet) a Non–Broadcast Multiple Access (NBMA)[6] (Frame Relay) vo vnútri oblasti. Referenčný smerovač DR je zodpovedný za rozhlasovanie LSA. Typ 2 obsahuje zoznam všetkých smerovačov (aj DR a BDR), ktoré zdieľajú jednu podsieť spolu s maskou podsiete.

[5] Generalizácia viacerých záznamov v smerovacej tabuľke do jedného na základe IP adresy.

[6] Siete bez všeobecného vysialnia, ktoré je však často simulované inými spôsobmi.

Správy typu 1 a 2 sú zahodené na hraničnom smerovači a nikdy sa nedostanú za hranice oblasti.

Pokiaľ smerovač obdrží všetky LSA 1 a 2 rozposielaných v danej oblasti, može na LSDB aplikovať algoritmus SPF a vypočítať strom ciest, z ktorého dokáže určiť najkratšie cesty v rámci oblasti.

4.6.2 Oznámenia LSA typu 3

Hraničné smerovače ABR neprepúšťajú oznámenia LSA typu 1 a 2 z jednej oblasti do druhej. Namiesto toho oznamujú LSA typu 3, ktoré obsahujú informáciu o všetkých sieťach v oblasti. Identifikátor linky v hlavičke LSA je nastavený na číslo oblasti, ktorú smerovač rozhlasuje do autonómneho systému. v bližšie nešpecifikovaných krajových sieťach, nepodliehajú LSA typu 3 filtrovaniu na ABR. Takže do okrajovej oblasti sa dostanú informácie o sieťach v ostatných oblastiach a vnútorné smerovače pre každú z nich vytvoria samostatný strom ciest a vyberú najlepšiu.

4.6.3 Oznámenia typu 4 a 5

LSA typu 4 a 5 oznamujú externé cesty v autonómneho systému s OSPF smerovacím protokolom.

Typ 4 generuje smerovač ABR, ale iba v prípade, že v okrajovej oblasti, ku ktorej má ABR pripojené rozhranie exituje ASBR smerovač. LSA identifikuje tento smerovač a poskytuje ostatným oblastiam informáciu o ceste k nemu. Smerovač, ktorý má pripojenie k externej ceste sa v LSA identifikuje externým bitom nastaveným na 1. ASBR posiela informácie o stave linky ako LSA typ 1. Keď ABR prijme správu, ktorá ma externý bit nastavený na 1, zmení typ na 4 a rozpošle údaj do autonómneho systému.

Typ 5 je na rozdiel od LSA typu 4 vytváraný na ASBR smerovači a nezmenený putuje celým autonómnym systémom. Identifikátor linky — link-state ID je číslo externej siete. Sietí, ktoré ASBR rozhlasuje môže byť mnoho, preto vždy mala aplikovať sumarizácia priamo na ASBR [7][8].

4.7 Cena externej cesty

Externé cesty ohlasované do OSPF smerovacej domény môžu mať rôznu cenu, podľa toho, aký ju rozhlasujú ASBR smerovače. Rozlišujeme dva typy externých ciest

E1 : cena cesty je súčet ceny, ktorú ohlasuje ASBR a hodnoty cien liniek, ktorými paket cielený mimo autonómny systém, musí prejsť. Riešenie je vhodné pokiaľ

existuje viacero ASBR oznamujúcich cestu do rovnakého AS, aby sa vyhlo suboptimálnemu smerovaniu v sieti.

E2 : smerovače, ktoré príjmu externú cestu s typom metriky E2, nastavuje ju ASBR keď ohlasuje cestu, prevezmú cenu ako pevnú a nepripočítavajú cenu cesty k ASBR. Cena cesty k externej sieti je v celom autonómnom systéme rovnaká. E2 metrika sa používa, pokiaľ je len jeden ASBR, ktorý má prístup k tejto sieti [8].

4.8 Rozdelenie koncový oblastí

Hierarchická štruktúra oblastí protokolu OSPF definuje dve úrovne, do ktorej môžu oblasti zapadať: tranzitná — má identifikátor 0 a okrajová — všetky ostatné. Okrajové siete OSPF ďalej, už bez hierarchickej štruktúry, delí na štyri typy. Všetky typy určitým spôsobom zlepšujú výkon celej smerovacej domény, pretože zjednodušujú LSDB databáze čim aj smerovacie tabuľky a zmenšujú množstvo záplavových LSA. Detailne spomeniem dve, ktoré sú použité v praktickej časti [10].

4.8.1 Koncová oblasť

ABR v koncovej – stubby oblasti, ktorá je nastavená ako koncová transformuje všetky LSA typu 4 a 5, ktoré mu prídu z transportnej oblasti na typ 3. Všetky cesty z typu 4 a 5 sa transformujú na jeden záznam s predvolenou — default cestou. Keď vnútorný smerovač potrebuje poslať paket do siete mimo OSPF, použije predvolenú cestu a pošle paket ABR, ktorý už má informácie o tom, kam smerovať ďalej. Koncová oblasť nemôže obsahovať ASBR smerovač, s výnimkou, keď ABR je zároveň ASBR. Všetky vnútorné aj hraničný smerovač musia mať pred naviazaním susedstva explicitne nastavené, že sú súčasťou koncovej oblasti [10].

4.8.2 Plne koncová oblasť

Jedná sa o proprietárne riešenie Cisco. Hraničný smerovač plne koncovej oblasti — totally stubby, okem LSA typu 4 a 5, neoznamuje ani typ 3, ktorý získal z tranzitnej oblasti od ostatných ABR smerovačov. Namiesto toho rozposielajú jediné LSA typu 3 s predvolenou cestou. Jediné informácie uložené v LSDB vnútorných smerovačov sú o linkách v oblasti. Ak smerujú paket do siete, ktoré nie je oznamovaná v oblasti, využijú predvolenú cestu. Podobne ako v koncovej, sú všetky smerovače konfigurované ako stub a iba ABR vie o tom, že rozhranie patrí k totálne koncovej. V oblasti sa nesmú nachádzať ASBR, iba ak ABR je súčasne ASBR [10].

4.9 Bezpečnosť v protokole OSPF

Všetky správy sú sieťou prenášane nešifrovane a zdroj informácii nie je žiadnym spôsobom autentizovaný. V protokole OSPF nie je možné zaručiť dôvernosť správ, ale je možné overiť zdroj, z ktorého smerovač prijal informáciu. Pokiaľ dokáže smerovač určiť pôvodcu správy, nedovolí prípadnému útočníkovi podvrhnúť informácie, ktoré dokážu vyradiť sieť z prevádzky. OSPF protokol implementuje dva spôsoby autentifikácie.

- Jednoduchú pomocou otvoreného hesla – vzhľadom na to, že sa heslo prenáša v otvorenej podobne, nemá takýto spôsob autentifikácie veľký význam. Cisco smerovače podporujú heslo, ktoré má dĺžku maximálne 8 znakov.
- Pomocou Message-Digest algorithm (MD5) hašovacej funkcie -– autentifikácia prebieha pomocou výzvy a odpovede. V oboch prípadoch musí na smerovačoch v rovnakej sieti nastavená identická forma autentifikácie a zhodný kľúč. Pokiaľ nie je podmienka splnený, smerovače nenadviažu susedstvo, bez ktorého je výmena informácií nemožná [13].

5 OPERAČNÝ SYSTÉM ZARIADENÍ CISCO

Pre simuláciu smerovacieho protokolu OSPF som použil zariadenia firmy Cisco, podobne ako v kurzoch Cisco Akadémie. Kapitolou popisujem vlastnosti operačného systému Cisco.

Operačného systém, prideľuje prostriedky a spravuje funkcie typu nízko úrovňových hardvérových rozhraní. Ten v smerovačoch a väčšiny prepínačoch firmy Cisco tvorí operačný systém Cisco Internetwork Operation System (IOS).

Cisco IOS je systémové jadro vyvinuté v spoločnosti Cisco, ktoré poskytuje funkcie smerovania, prepínania, prepojenia sietí a telekomunikačných technológií. V zariadeniach Cisco sa vyskytujú v rôznych verziách a modifikáciách, podľa typu zariadenia, do ktorého sú implementované. Odlišujú sa najmä v podpore technológií, protokolov a dostupných funkciách. IOS zaisťuje následujúce dôležité úlohy:

- podporu sieťových protokolov,
- bezpečnosť, riadenie prístupu — zamedzenie prístupu neoprávnenému užívateľovi,
- poskytovať škálovatelnosť za účelom zjednodušenia rozšírenia siete a zaručenie dostatočnej redundancie.

5.1 Možnosti prístupu

Cez pripojenie je možné upravovať a overovať konfiguráciu, kontrolovať funkčnosť a detektovať chyby na zariadení, alebo v sieti. Využiť je možné viacero spôsobov, pričom každý je charakteristický a vhodný pre iné situácie a podmienky. Existujú tri typy prístupu: prístup cez konzolu, Telnet[1]/Secure Shell (SSH)[2] a vytáčané pripojenie.

5.1.1 Prístup cez konzolu

Ako základný spôsob ho podporujú všetky zariadenia. Funguje ako lokálny terminál smerovačov, alebo prepínačov. Pripojenie je realizované cez sériovú linku. Lokálny terminál sa uplatňuje pri zadávaní počiatočných nastavení zariadenia, odstraňovaní vážnejších porúch a v neposlednej rade pri obnove hesla. Pristupovanie je možné obmedziť a povoliť prácu so systémom iba autentizovaným užívateľom pomocou heslo.

[1]Protokol pracujúci na aplikačnej vrstve. Ovláda zariadenia v sieti cez terminál s príkazovým riadkom [8].

[2]Protokol umoľňujúci bezpečnú komunikáciu medzi počítačmi pomocou ąifrovania [6].

5.1.2 Vzdialené terminály integrovanej správy

Pokiaľ je prenos informácií, medzi vzdialených zariadením a emulovaným terminálom na lokálnej stanici, cez sieť, označujeme spôsob konfigurácie ako integrovaná – in-band, administrácia. Aplikuje sa na už bežiace zariadenia, ktoré majú funkčnú tretiu vrstvu.

Cisco smerovače a prepínače používajú dva protokoly aplikačnej vrstvy. Prvý, nezabezpečený, Telnet a novší a bezpečnejší SSH.

5.1.3 Pripojenie pomocou pomocného portu AUX

Auxiliary – pomocný port (AUX) port pracuje podobne ako port lokálneho terminálu, no dovoľuje konfigurovať príkazy modemu. To znamená, že je možné k zariadeniu pripojiť modem vytáčaného spojenia. Fungovanie nie je závislé na počítačovej sieti — out-of-band, tzn. mimo vlastnú sieť. Teda AUX port je vhodné použiť ako zálohu in-band spojenia SSH, alebo Telnet.

5.2 Administrácia systému

5.2.1 Konfiguračné režimy

Cisco zariadenia sú konfigurované cez Command-line interface (CLI), teda zadávaním textovým príkazov do konzole. Celý systém ma hierarchické delenie do vrstiev a každá z nich obsahuje rozdielnu sadu príkazov a funkcií.

Vstupnou bránou do systému je globálny neprivilegovaný užívateľský režime. V tomto režime je možné použiť veľmi obmedzený počet príkazov a aj tie slúžia na kontrolu základných parametrov systému.

Vyššiu vrstvu reprezentuje privilegovaný užívateľský režim. Príkazy zadané do CLI dokážu čiastočne upraviť krátkodobé parametre systému no nedokážu zmeniť konfiguráciu. Ďalej rozširujú možnosti zobrazenia aktuálnych štatistík a nastavení. Najdôležitejší režim — konfiguračný, obsahuje príkazy priamo zasahujúce do konfigurácie. Je ďalej delený podľa častí systému, ktorých nastavenia je možné zmeniť — nastavovanie portov, prístupové metódy, smerovacie protokoly, riadenie prístupu a pod. Každý zadaný príkaz sa okamžite stáva súčasťou platnej konfigurácie.

Jednotlivé vrstvy je možné samostatne zabezpečiť prístupovým heslo a zabrániť tak neautorizovanému prístupu do systému.

5.2.2 Zadávanie príkazov

Ako už bolo spomenuté, príkazy sa do systému sa zadávajú v textovej podobe. Na každej úrovni je možné pomocou otázniku vypísať zoznam podporovaných príkazov a tak isto je možné vypísať očakávané parametre a ich formát. Terminály podporujú automatické dokončovanie, čo v praxi znamená, že do CLI stačí vypísať začiatočné písmená požadovaného príkazu a pokiaľ je podľa týchto písmen identifikovaný práve jeden príkaz, systém doplní zbytok písmen, alebo slov. Funkcia výrazne urýchľuje a zjednodušuje prácu vo všetkých typoch režimov. V nižších úrovniach nie je možné zadávať príkazy vyššieho konfiguračného režimu, no príkazy privilegovaného režimu sú v správnej syntaxe dostupná aj v konfiguračnom režime.

Všetky príkazy sú potvrdzované klávesou Enter a naposledny potvrdené sú uložené v pamäti, ktorá má štruktúru lineárne viazaného zoznamu ktorým je možné listovať.

5.3 Kontrola a uloženie konfigurácie

Koonfigurácie je uložená v samostatnom súbore ako text. Riadky sú zadané konfiguračné príkazy a zoskupené do častí hierarchicky, tak ako ich nájdeme v systéme. Aktuálna konfigurácia, podľa ktorej zariadenie pracuje, je uložená v súbore running-config. Zobraziť ho môžeme cez príkaz v privilegovanom režime **show running-config**. Súbor sa pri vypnutí, alebo reštarte smerovača (ale aj prepínača) nenávratne vymaže a pre inicializácii je použitý súbor startup-config, s uloženou konfiguráciou. Implicitne obsahuje nastavenie výrobcu, ale pokiaľ je konfigurácia z running-conf prekopírovaná do startup-conf, systém použije príkazy z nej. Uloženie aktuálnej konfigurácie je možné príkazom **copy running-config startup-config** [4][6][8].

6 SIMULAČNÝ PROGRAM PACKET TRACER

Na realizáciu simulácie som si vybral program Packet tracer. Výber ovplivnila viazanosť na Cisco Akadémiu a výborná podpora zariadení Cisco. Ako program funguje a aké funkcie ponúka opisujem v nasledujúcej kapitole.

Spoločnosť Cisco vyvinula pre účely Cisco akadémie program, ktorý dokáže simulovať reálnu sieť. Motiváciou bolo sprístupniť študentom praktické ukážky implementácie Cisco zariadení do počítačovej sieti. Často vznikajú praktické prekážky pri testovaní vedomostí a simulácii na reálnych zariadeniach — časové obmedzenia, počet študentov na dané množstvo zariadení a iné. Packet tracer tieto bariéry odbúrava, pretože zadané úlohy je možné vypracovať rovnako ako na fyzických prvkoch a tak isto jednoducho aj simulovať konfigurácie, alebo sledovať prenos dát v sieti. Napriek tomu, že primárne plní účel ako výukový program, vlastnosti, ktorými disponuje, ho robia vhodným aj pre praktické simulácie a testovania konfigurácii pred implementáciou do skutočnej siete.

V súčastnosti vychádza vo verzii 5.3 pre všetky najrozšírenejšie operačné systémy (Windows, Linux, MacOS).

6.1 Užívateľské rozhranie

Rozhranie programu Packet tracer je plne grafické. Obsahuje ovládacie prvky delené podľa významu do skupín, katalóg použiteľných zariadení a kabeláže, ďalej prepínanie medzi topológiami a nastavovanie simulácie.

Packet tracer podporuje fyzické a logické zobrazenie topológie. Logická zobrazuje prvky siete nezávisle na ich umiestnení v stojane, miestnosti či budove a prakticky všetky siete sa sú vytvárané ako logická topológia.

Druhou možnosťou je simulovať fyzickú topológiu, tak ako sú smerovače, prepínače a stanice lokalizované v objekte alebo väčšej geografickej oblasti. Zobrazenie je skôr informatívneho charakteru a umiestnenie prvkov nemá na simuláciu vplyv.

Každé zariadenie má vlastné konfiguračné okno, ktoré je delené do sekcií. Význam a počet sekcií je vo všetkých zariadenia podobný. Smerovače, prepínače po prípade iné aktívne prvky Cisco majú sekciu s konzolovým terminálom, do ktorej sa zadávajú príkazy a prakticky celá konfigurácia prebieha cez tento terminálu.

Stanice, servery ponúkajú sekciu podobnú pracovnej ploche počítača. V nej sú umiestnené najpoužívanejšie užívateľské aplikácie sieťových služieb (jednoduchý webový prehliadač, elektronickú poštu) a programy pre administráciu a analýzu siete a sieťových zariadení. Packet tracer dokáže pracovať v dvoch simulačných režimoch.

- Mód s reálnym časom — real-time mode: zariadenia a sieť ma okamžitú odozvu na zmenu parametrov a viac zodpovedá skutočnej sieti.

- Simulačný mód — simulation mode: v tomto režime je možno kontrolovať časové intervaly medzi odoslanými paketami, čo detailnejšie odkrýva tok dát sieťou. Pomáha pochopiť podstatu výmeny správ rôznych protokolov.

6.2 Podporované technológie

Simulačný program Packet Tracer podporuje najdôležitejšie protokoly všetkých vrstiev modelu TCP/IP. Každou verziou pravidelne pribúdajú ďalšie, alebo sa zlepšuje implementácia stávajúcich. Samozrejmosťou je podpora zariadení Cisco. Katalóg všetkých zariadení je rozdelený do sekcii:

- smerovače, prepínače, huby — obsahuje niektoré modelové rady Cisco,
- bezdrôtové prístupové body — najme zariadenia divízie LinkSys,
- koncové zariadenia — stanice, servery, Voice over Internet Protocol (VoIP)[1] telefóny, tlačiarne a iné.

Okrem základných kategórii exituje ešte sekcia s užívateľsky definovanými zariadeniami. Packet tracer umožňuje vytvárať vlastné zariadenia, pretože podobne ako skutočné Cisco prvky, je možné smerovače (a aj niektoré iné zariadenia) rozširovať pomocou zásuvných modulov. Moduly zväčšujú počet portov, alebo pridávajú podporu pre prenosové technológie.

6.3 Rozšírenia programu

Okrem základných funkcií, medzi ktoré bezpochyby patrí simulácia, podporuje Packet tracer aj rozšírenia, ktoré zväčšujú variabilitu a atraktivitu.

Prvou je Activity wizard. Funkcia, ktorá umožňuje vytvárať úlohy. Úloha obsahuje štartovaciu topológiu, samostatné okno s informáciami a často aj postupom. Za všetkým sa skrýva mechanizmus, ktorý kontroluje správnosť konfigurácie zariadení a funkcionalitu siete. V reálnom čase dokáže dať užívateľovi informáciu o správnosti prevedeného kroku. Na záver vyhodnotí výsledok. Parametre, topológiu a váhu jednotlivých krokov nastavuje zadávateľ, teda ten kto úlohu vytvára. Activity wizard môže slúžiť ako prostriedok testovania študentov, alebo ako sprostredkovateľ informácii pre výukovú topológiu.

Ďalším prvkom, ktorý zvyšuje atraktivitu programu Packet tracer je viac-užívateľská — multiuser podpora. Znamená to, že do topológie sa vloží, ako bežné zariadenie, prvok, ktorý v LAN (ale aj v Internete) dokáže viacero inštancií programu bežiacich na rôznych počítačoch spolu prepojiť. Prenosy v simulovanej sieti sú tunelované cez

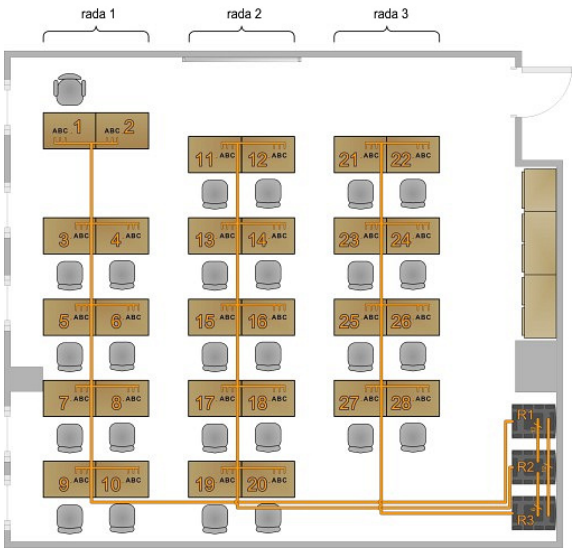
[1] Súbor protokolov pre prenos hlasu paketovou sieťou[17].

skutočnú sieť. Cez multiuser rozhranie je možné budovať rozsiahle systémy sietí a zároveň vytvárať interakciu medzi užívateľmi [16].

7 SIMULÁCIA UČEBNE CISCO AKADÉMIE

Ako súčasť diplomovej práce som vytvoril projekt simulácie učebne, v ktorej sa vyučujú predmety Cisco akadémie. Projekt som vytvoril v simulačnom nástroji Packet tracer. Cieľom je dať možnosť testovať implementáciu smerovacieho protokolu OSPF v podobných podmienkach ako ponúka učebňa.

Práca na prenesení Cisco učebne do programu spočíva v analýze možností, ktorými Packet tracer disponuje, a ich zúžitkovaní pri tvorbe úlohy zameranej na smerovací protokol OSPF. Simulácia okrem iného demonštruje výhody, ktoré testovanie na virtuálnej sieti a až následná implementácia do reálnej prináša.



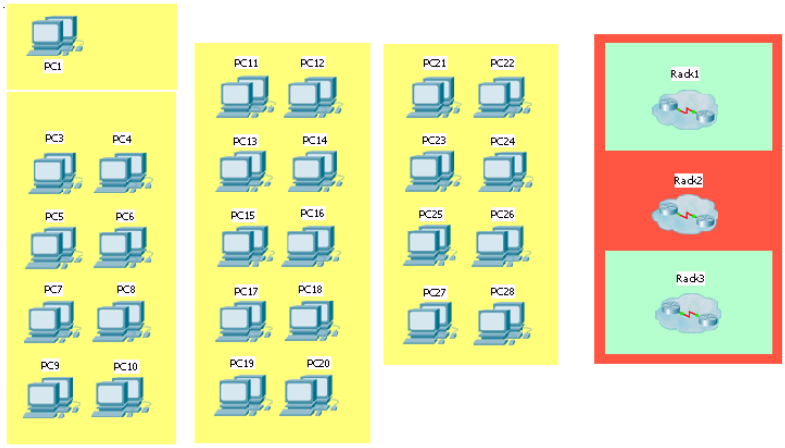
Obr. 7.1: Pôdoris učebne Cisco akadémie.

7.1 Realizácia učebne v simulačnom programe

Ako som sa už zmienil, projekt som vytvoril v programe Paceket tracer pomocou súčasti Activity wizard. Dôvod realizácie učebne pomocou tohto nástroja je, že oproti obyčajnej simulácii dokáže zakázať fyzickú manipuláciu so zariadeniami a zobrazovať informačné popisky, ktoré uľahčujú orientáciu v simulovanej učebni.

Vďaka blokovaní posúvania zaradení, odpadá starosť o rozhádzanie rozloženia a tým aj prehľadu. Samozrejme niekomu preddefinované rozloženie nemusí vyhovovať, prípadne sa môže stať, že uzamknutý prvok prekáža. Preto som sa snažil topológiu po fyzickej stránke optimalizovať a vyhnúť sa tak spomínaným problémom. Učebňa v simulácii zachycuje pohľad na pôdorys tej reálnej. Orientácia korešponduje s prezentovanými obrázkami na stránkach predmetu.

Učebňa je rozložená do farebných blokov. Bloky s žltým pozadím reprezentujú celkovo tri rady s počítačmi plus jeden blok figuruje ako stôl učiteľa. Červený blok ,v pravej časti, je oblasť, v ktorej sa nachádzajú sieťové zariadenia – smerovače a prepínače. Farebné bloky sú použité najmä kvôli prehľadnosti. Celkovo je v miestnosti 28 počítačov z toho dva slúžia vyučujúcemu. Z týchto dvoch je využívaný iba jeden. Počty počítačov v radách simulovanej učebne korešpondujú s počtami v reálnej učebni [15].



Obr. 7.2: Topológia Cisco učebne s 28 počítačmi a 3 dátovými rozvádzačmi.

7.2 Simulovanie počítača

V reále obsahujú počítače dve sieťové karty a jeden sérievoý port. Takáto konfigurácia v Packet tracer nie je bohužiaľ možná. Problém sa nachádza v počte kariet ktoré može jedno koncové zariadenie obsahovať. V simulačnom prostredí je to iba jedna karta, respektíve jeden slot. V slote môže byť iba jeden modul. Na výber sú dva: ethernetový port a bezdrôtový adaptér.

Použitie iba jedného modulu by nezodpovedalo skutočnosti. Preto sú všetky koncové stanice duplikované. To znamená, že jednu reálnu stanicu v simulácii reprezentujú dve s podobnou konfiguráciou.

V prostredí som sa snažil zariadenia, ktoré sú spolu brané ako jeden počítač, umiestniť navzájom čo najbližšie, však tak, aby si nezavadzali. Počítače ležia jeden na druhom. Vrchný počítač figuruje ako ethernetová sieťová karta do ostrej – VUT siete.

7.3 Prepínače a smerovače v simulácii

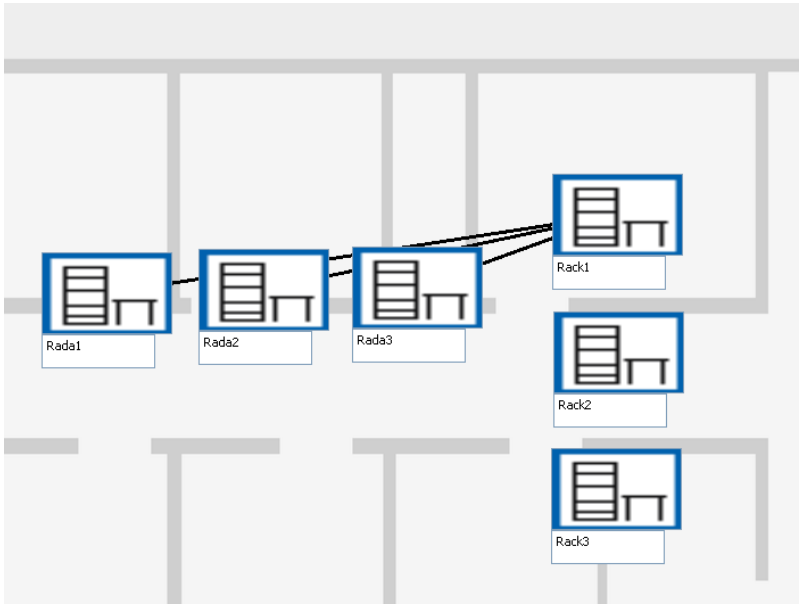
Do červenej oblasti som umiestnil sieťové zariadenia. Aby ostala previazanosť so skutočnou miestnosťou, triedenie smerovačov a prepínačov podlieha rovnakému systému, čo znamená umiestnenie zariadení do troch dátových rozvádzačov. V simulácii sa na združovanie zariadení používajú oblaky – clustre. Ide o nástroj vytvarajúci prostredie so stromovou štruktúrov. Použitie sa vyplatí najmä v topológii s veľkým množstvom zariadení, čo topológia Cisco akadémie je. Každý oblak je pomenovaný podľa dátového rozvádzača, ktorý reprezentuje. Po rozklikuntí sa zobrazí obsah oblaku a teda aj vstúpi do nižšej úrovne. Oblak zahŕňajú práve toľko sieťových prvkov koľko je dátových rozvádzačov v učebni.

Prvý oblak okrem klasickej výbavy, v podobe smerovačov a prepínačov, obsahuje server a ďalší oblak. Server disponuje funkciou Dynamic Host Configuration Protocol (DHCP)[1]. Priraďuje IP adresy staniciam pripojeným do ostrej siete z rozsahu adries 147.229.0.0/16 tak, ako v skutočnosti. Ďalšie služby typu Hypertext Transfer Protocol (HTTP)[2] server, alebo Trivial File Transfer Protocol (TFTP)[3] server sa v cvičeniach veľmi nepoužívaju, avšak konfigurácia nie je problém a je povolená. Druhým zvláštnym prvkom nachádzajúcim sa v prvom dátovom rozvádzači je oblak s názvom HP ProCurve. Funkcia zariadenia spočíva v spojení všetkých staníc označených „PCx realNet“ do jednej siete, ktorú obsluhuje DHCP server. Oblak maskuje dva prepínače, aby figurovali ako jeden veľký.

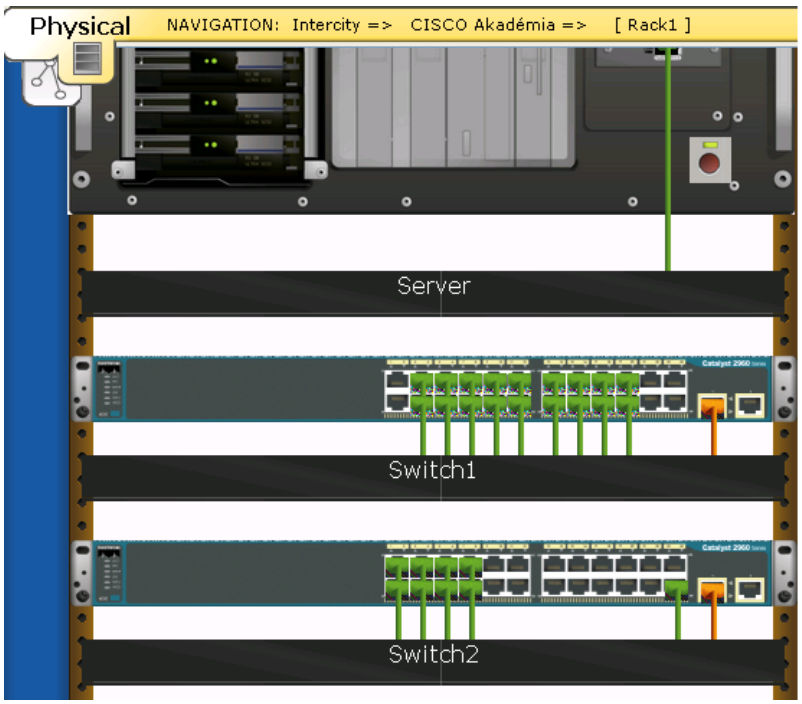
7.4 Fyzické rozloženie zariadení v prostredí programu

Cisco učebňu som súčasne preniesol aj do fyzickej štruktúry. Napriek tomu, že sú veľmi podobné. Vo fyzickej zobrazení učebne je možné vidieť zariadenia umiestnené v dátovom rozvádzači a manipulovať s nimi. Prepínanie medzi zobrazeniami prebieha cez menu v hornej časti obrazovky. Fyzická topológia má podobne ako logická hierarchickú štruktúru. Najvyššiu úroveň reprezentuje učebňa Cisco akadémie. V nižšej úrovni sa už dostávame na stupeň v ktorom už figurujú rady s počítačmi a dátové rozvádzače. Po kliknutí prvok sa zobrazia samotné zariadenia. Samozrejme, že podľa prvku dostaneme zariadenia náležiac k dátovému rozvádzaču či rade. Kliknutie na racku názorne vyobrazí sieťové prvky ako v reálnej situácii a to i s kabelážou. Operácie spracovávané na tejto úrovni sú mierené najmä na správu napájania a sieťovej kabeláže.

[1] Protokol automatickej konfigurácie zariadení v sieti[12].
[2] Protokol na prenášianie webových prezentácií[3].
[3] Zjednodušený protokol pre prenos dát sieťou[5].



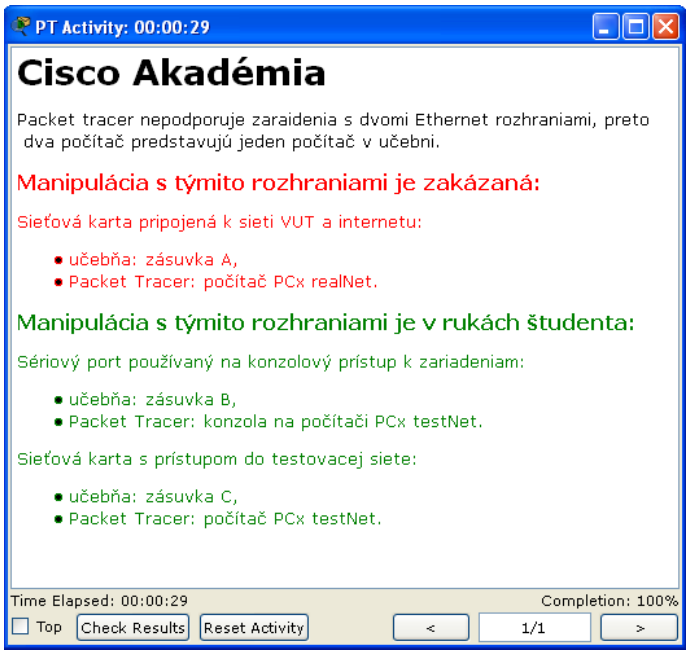
Obr. 7.3: Uroveň v ktorej vidieť racky a rady.



Obr. 7.4: Grafické znázornenie zariadení a ich zapojenia.

7.5 Doplkové informácie

Súčasťou simulácie je aj informačné okno. Publikované informácie som editoval HyperText Markup Language (HTML) značkami – tagmi. Do informácii som zahrnul základné inštrukcie a pokyny analogické s direktívami platnými v Cisco učebni. Súbor so simulovanou učebňou je stiahnuteľný zo stránok Cisco akadémie FEKT



Obr. 7.5: Informácie zobrazované pri každom spustení úlohy.

VUT v Brne. Súčasťou je i webová prezentácia, ktorá informuje o základnom ovládaní a navigácii v programe Packet tracer a simulácii.

8 SIMULÁCIE PROTOKOLU OSPF A VYTVORENIE ÚLOHY

Cieľom diplomovej práce je simulovanie smerovacieho protokolu OSPF. Predvedenie možností ktoré ponúka a súčasne vytvoriť úlohu pre študetov s témou protokolu OSPF. V teoretickej časti som popísal hlavné rysy OSPF, ktoré následne simulujem a sú súčasťou zadania ulohy pre študentov. Ako simulačný program som si vybral nástroj Packet tracer. Dôvodom môjho výberu, je skutočnosť, že zmienený program používa často Cisco akadémia ako súčasť výuky. Čím majú študenti ovládanie a základné techniky v povedomí. Zároveň je vhodný na tvorenie úloh, pretože obsahuje moduly, ktorými je možné kontrolovať priebeh vypracovania podľa vopred definovaných parametrov.

Výstupom je teda úloha v ktorej môže študent testovať konfigurácie bez prístupu k fyzickým sieťovým prvkom a mimo laboratória. Čo úlohu predurčuje byť súčasťou individuálnej prípravi a s rozšírením multiuser aj súčasťou skupinovej prípravy s ďalšími študentami. Zoznamuje študentov so základnými princípmi smerovacích protokolov zohľadňujúce stav linky a najmä s protokolom OSPF. Súčasne ponúka pohľad na zložitejšie princípi a konfigurácie OSPF. Medzi tie najdôležitejšie patrí rozdelenie autonónmneho systému do hierarchickej štruktúry oblastí a aplikovanie roznych špecifikácií pre okrajové oblasti v OSPF doméne. Počas celej úlohy som zaistil kontrolu zadaných príkazov a parametrov. Výstupným protokolom je priebežne aktualizovaý list informujúci o tom, ktoré nastavenia študent volil správne podľa zadania a ktoré príkazy zadal chybne.

Úlohu som koncipoval tak, aby študent okrem praktických poznatkov z implementácie smerovacieho protokolu OSPF, mal možnosť pracovať aj po úspešnom dokončení na atraktívnej topológii, v ktorej môže pokračovať v nasadzovaní niektorých ďalších nastavení podľa vlastných preferencií. Túto vlastnosť zaručuje najmä rozšírenie multiuser.

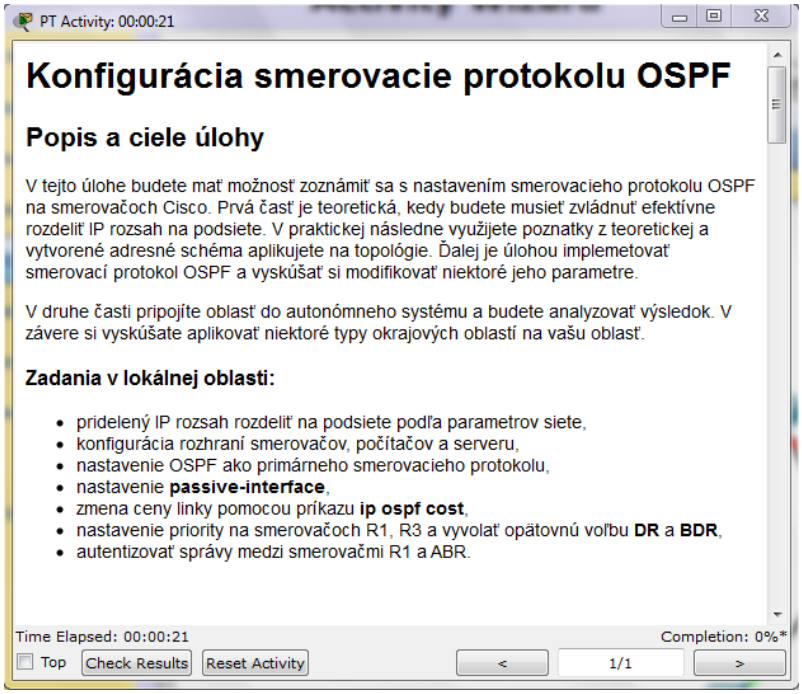
8.1 Použie rozšírení programu

Pri vytváraní úlohy som hľadal postupy a funkcie, ktorými dokážem splniť požiadavky položené v zadaní a prípadne začleniť inovatívne prvky pre zvýšenie atraktivity. Vhodné riešenia ponúkli dve rozšírenia simulačného programu Packet Tracer:

- Activity wizard,
- multiuser topológia.

8.1.1 Využite rozšírenia pre vytváranie úloh v simulačnom programe

Úlohu som vytvoril v simulačnom programe Packet tracer pomocou rozšírenia Activity wizard. Túto variantu som si vybral najmä preto, pretože vďaka Activity wizard som mohol implementovať informáčné okno, ktoré obsahuje rozpísané zadania úlohy, vhodné postupy a ďalšie dôležité informácie o úlohe 8.1. Okno je neoddeliteľnou súčasťou úlohy. Otvára sa šúčasne so spustením úlohy, bez nutnosti zásahu študenta. Počas simulácie ho nie je možné zavrieť, iba minimalizovať. Okrem informácie aké doporučené adresy má študent použiť obsahuje časovač. Ten počíta čas od začatia riešenia až po jej úspešné dokončenie. Ďalej obsahuje voľbu vyhodnotenia úlohy, ktorú je možné aktivovať kedykoľvek v priebehu riešenia. Rovnako ako pre



Obr. 8.1: Informačné okno obsahuje údaje potrebné k vypracovaniu.

informačné okno, som pre potreby kontoroly a vyhodnotenia úlohy využil možností rozšírenia Activity wizard. Vyhodntil som, aké parametre je potrebné sledovať. Volil som podľa ich dôležitosti vo výslednej konfigurácii. Teda napríklad, či keď študent nastaví na rozhraní vnútorného smerovača oblasti nevhodnú IP adresu, alebo adresu z nesprávnou maskou, aký dopad bude mať chyba na fungovanie smerovacieho protokolu OPSF. V tomto prípade by to malo závažné následky, pretože súčasťou úlohy je aj správne navrhnúť rozdelenie IP adries. Postupným analyzovaním všetkých funkčných parametrov v topológii siete som dospel k kontrolnému listu. Ten obsahuje vybrané nastavenie s prideleným množstvom bodov. Čím výšší počet bodov, tým je

zadanie v úlohe dôležitejšie. Rozšírenie Activity wizard podľa listu kontrol neustále sleduje prácu študenta v simulácii. Študent získa aktuálne informácie o správnosti svojho postupu, pri zhliadnutí tohto listu. Spôsob neustáleho informovania o správnosti zadaných príkazov je vhodný, pretože dáva študentovi spätnú väzbu a dokáže ho včas upozorniť na nevhodne zadané parametre.

8.1.2 Význam rozšírenia pre kooperáciu študentov v úlohe

Druhým rozšírením, ktoré som do úlohy vložil, je rozhranie multiuser. Študent v závere úlohy, keď sú smerovače v topológii správne nastavené a smerovací protokolo OSPF informuje ostatné smerovače o sieťach v oblasti, pripojí cez multiuser sieť do väčšiaho systému. Ten obsahuje ako siete ostatných študentov, ktorý už majú funkčnú doménu OSPF a pripojili ju do systému, tak aj podpornú sieť. Podpornú sieť som vytvoril, aby prvky a procesy, ktoré v nej bežia napomáhali k pochopeniu protokolu OSPF vo svete autonómneho systému. Cez multiuser si siete študetov vymieňajú dáta, komunikujú a celý systém sa dostáva do stavu, kedy je nutná kooperácia a komunikácia medzi študetami pre správne fungovanie autonómneho systému. Preto sa úloha, alebo úlohy viac približujú realite, ako simulácii.

8.2 Návrh úlohy a vytvorenie topológie

Po formulovaní všetkých požiadavkov a otestovaní rozšírenia Activity wizard na simulácii učebne Cisco akadémie som pristúpil k samotnému nárhu úlohy. Podľa podmienok, ktoré má úloha splňovať som počas návrhu zohľadnil naslednujúce body:

- veľkosť úlohy,
- schopnosti OSPF,
- tvar topológie,
- počet a typ zariadení v topológii,
- náväznosť na multiuser rozhranie.

Faktor veľkosť úlohy som zohľadnil pri návrhu času, za ktorú bude možné úlohu dokončiť. Pretože za cieľ úlohy som si stanovil predstaviť smerovací protokol OSPF v čo najväčšej miere, musel som navrhnúť topológiu, ktorá zodpovedá ako aj podmienkam v laboratóriu, tak čiastočne aj reálnym situaciám. Topológia obsahuje viacero typov prenosových technológií v lokálnych a metropolitných sietí.

- Viac-prístupová sieť (multiaccess); segment siete s broadcast vysielaním. Použitá je technológia Ethernet.
- Spojenie bod-bod (point-to-point); linka vytvorená medzi dvomi smerovačmi.

Tieto typy prepojení majú význam pri nastavovaní a úprave základných parametrov protokolu OSPF. V úlohe sú napríklad použité na demoštráciu voľby referenčného

smerovača a záložného referenčného smerovača v segmente siete s prístupom k zdieľanému médiu a broadcast vysielaním.

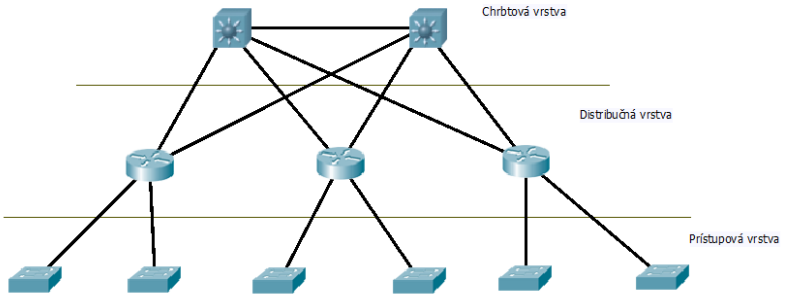
Ďalej som sa pri vytváraní topológie snažil využiť trojvrstvový hierarchický model Cisco. Jedná sa o doporučenie firmy Cisco, ktoré pomáha pri návrhu, implementácii a údržbe, spoľahlivej a cenovo efektívnej hierarchickej paketovej siete. Vzhľadom na to, že sa jedná o logickú štruktúru, nie je nutné zabezpečiť rovnakú fyzickú topológiu. Model využíva podobných princípov, ako štandard OSI. Teda každá úroveň — vrstva má určité povinnosti a každej dokážeme priradiť sieťový hardware. Hierarchický model tvoria tri vrstvy.

Core layer – jadro siete, chrbtová časť: nachádza sa na vrchole modelu a je zodpovedná za rýchly a spoľahlivý prenos veľkých objemov dát. Dáta prenášaná v chrbtovej sieti sú spoločné pre väčšinu užívateľov a preto prípadný výpadok či závada ovplyvní takmer všetky služby. Preto má prepojenie zariadené v jadre výrazne redundantný charakter.

Distribution layer – distribučná vrstva: tvorý centrum komunikácie medzi prístupovou vrstvou — užívateľmi a jadrom. Hlavnými funkciami je zaisťovať smerovanie v sieti do WAN aj medzi VLAN, riadiť prístup k WAN, zaisťovať obojstrannú bezpečnosť a definovať všesmerové a viacsmerové domény.

Access layer – prístupová vrstva: k tejto vrstve sú už pripojené pracovné stanice, servery a periférie.

Dôvod prečo som pri návrhu využil Cisco model je, že v predmetoch Cisco akadémie sa často používa a zároveň je vhodný pre túto úlohu. Packet tracer vyvíja spoločnosč



Obr. 8.2: Hierarchický model návrhu siete použitý v úlohe.

Cisco, preto aj zariadenia, ktoré možno v simulácii použiť pochádzajú výhradne od firmy Cisco. V úlohe sú použité:

- smerovače – upravené typ 2811,
- prepínače – typy 2960 a 3560-24PS,
- koncové zariadenia – servery a počítačové stanice.

Pre potreby multiuser rozšírenia som musel vytvoriť systém viacerých úloh, ktoré by bolo možné efektívne spájať. Ako najlepšie riešenie sa javilo využitie dvoch úloh:

- koncová úloha;
- centrálna úloha.

Každá z nich má vlastnú topológiu a špecifické služny, ktoré zabezpečuje. Prvá úloha je určená pre študentov. Prvky v tejto sieti sú rozložené tak, aby bol smerovací protokol vhodne aplikovateľný. Druhá obsahuje zariadenia, ktoré spájajú koncové úlohy a zabezpečujú ich vzájomnú komunikáciu. Používať ju môžu ako študenty, tak aj vyučujúci, o výbere rozhoduje spôsob využitia úlohy. Ak je cieľom vyučujúceho mať dohľad na autonómnym systémom, spustí si centrálnu úlohu na svojej pracovnej stanici. Pokiaľ však simuláciu OSPF testujú študenti samostatne, môže centrálna úloha bežať na niektorom z študentských počítačov. Tymto návrhom som dal možnosť používať úlohy mimo školských priestorov a s využitím menšieho počtu počítačov.

Oboje súčasne implementujú multiuser rozhranie, cez ktoré sa navzájom spájajú do jedného autonómneho systému. Okrem konektivity medzi koncovými úlohami poskytuje podporné služby výšších vrstiev, internetového referenčného modelu TCP/IP, pre celú sieť.

8.3 Koncová úloha

Nosným prvkom praktickej časti je koncová úloha, pretože práve v nej sa konfiguruje smerovací protokol OSPF. Úloha dokáže pracovať samostatne bez podpori centrálnej úlohy, no následnej nie je možné zariadiť jedodnuché prepojenie viacerých koncových úloh. Študent teda nemôže využívať funkcie multiuser, aby bol schopný zaradiť svoju sieť do autonómneho systému a vytváral komunikáciu medzi ostatnými koncovými úloha a súčasne využíval služieb centrálnej siete. Topológia obsahuje päť upravených smerovačov Cisco 2811. Smerovače ABR, R1 a R4 sú rozšírené o dva sériové porty — modul WIC-2T. Dôvodom rozšírenia je fakt, že prepojenie dvoch smerovačov v laboratórii Cisco akadémie je typu bod-bod vytvoreného sériovou linkou. Rozšírenie modulom prinieslo priblíženie simulácie reálnym podmienkam v učebni.

Smerovač R2 sa odlišuje od štandardných modelov použitím rozširujúcich modulov a na rozdiel od ostatných smerovačov v sieti som nepoužil moduly so sériovými portami, ale moduly s ethernetovými rozhraniami, ktoré rozširujú smerovač o vlasntosti prepínača na týchto portoch. Tým je možné pre segmety v prístupovej vrstve s menším počtom koncových staníc ušetriť prepínač a namiesto toho rozšíriť priľahlí smerovač.

Ďalej topológia obsahuje tri Cisco prepínače typu 2960. Sú to štandardné prepínače bez prídavných modulov, alebo iných rozšírení. SW2 a SW3 patria v topológii do prístupovej vrstvy. A prepínač SW1 je súčasťou distribučnej vrstvy hierarchického modelu Cisco. Do tejto časti topológie je vložený preto, aby vytvoril viacprístupovú sieť s všeobecným vysielaním. Smerovače pripojené k tomuto segmetu musia pre správne fungovanie OSPF smerovacieho protokolu zvloliť DR a BDR smerovače, s ktorými v tomto type siete výhradne komunikujú. Študent pri vypracovaní úlohy bude musieť meniť niekoré parametre OSPF, aby zaručil, že DR smerovač sa stane ten, ktorý je požadovaný v zadaní.

Na overenie funkčnosti a vizualizácie komunikácie v sieti som do topológie koncovej úlohy vložil tri počítače a jeden server. Sprostredkovávajú prístup k protokolom vyšších vrstiev, napr: HTTP, Domain Name System (DNS)[1] a pod. Niektoré z týchto služieb sú implementované ako v koncovej úlohe, tak aj v centrálnej úlohe. Študent má možnosť v koncovej úlohe využiť DNS server a HTTP server. Oboje služby prispievajú najma k overeniu funkčnosti siete vo vyšších vrstvách internetového modelu TCP/IP a interakcii medzi študentami zdielajúcich jednu centrálnu úlohu. Cez webový prehliadač je možné pristupovať na prezentácie umiestnené na HTTP serveroch nachádzajúcich sa v rôznych oblastiach, ktoré sú pod správou ostatných študentov.

Každá koncová úloha obsahuje multiuser rozhranie, pomocou ktorého sa pripája do centrálnej úlohy. Pokiaľ nie je pripojený do centrálnej úlohy nemá pre smerovanie v lokálnej oblasti OSPF žiadny význam. Roozhranie naberá na význame až vtedy, keď sú všetky podstatné nastavenia smerovacieho protokolu aplikované a oblasť je pripravená zaradiť sa do autonómneho systému.

Verzie koncovej úlohy sú rovnaké pre všetky zadania, teda pre všetky rozsahy IP adries. Takéto riešenie som volil preto, aby bola úloha dostatočne variabilna a umožňovala pripojiť teoreticky neobmedzený počet koncových úloh do centrálnej. Prakticky je toto číslo obmedzené výkonom počítača, na ktorom beží centrálna úloha. Distribúcia spočíva v stiahnutý jedného súboru spustiteľného v Packet tracer. Ten obsahuje ako topológiu tak aj informačné okno a všetky potrebné rozšírenia.

8.4 Centrálna úloha

Druhou časťou úlohy zameranej na smerovací protokol OSPF je centrálna úloha. Centrálna úloha nie je nevyhnutnou pre pochopenie základných princípov OSPF, ale prispieva k pochopeniu a osvojeniu si komplexnejších štruktúr smerovecej domény.

[1]Systém prekladu IP adries na doménové mená a naopak [14].

Medzi tieto zložitejšie nastavenia radím delenie autonómneho systému do oblastí a aplikovanie rôznych typov okrajových oblastí na siete v koncových úlohách.

Princíp úlohy som koncipoval tak, aby v tento časti nemusel študent nastavovať žiadne parametre spojené s funkciou siete a bral sieť centrálnej úlohy ako podpornú. Všetky parametre som vopred nakonfiguroval, takže k spusteniu úlohy nie sú nutné žiadne ďalšie výpočty adries, nastavovanie rozhraní alebo prepojenie zariadení medzi sebou. Centrálna úloha slúži iba ako prostredník medzi koncovými úlohami v ktorých pracujú študenti a v hierarchickom návrhom modele siete figuruje ako chrbtová sieť. Teda zaisťuje vysokorýchlostné spojenie medzi smerovačmi distribučnej vrsty, ktoré sú už samozrejme súčasťou topológie v koncových úlohách.

Do hlavnej siete centrálnej úlohy som vybral dva prepínače 3560-24PS. Sú to vysokovýkonné prepínače a preto sú použité na v chrbtovej časti simulovaného autonómneho systému, ktorá prenáša veľké množstvo dát z okrajových oblastí. Spojenie medzi prepínačmi zaisťuje dvojica priamych krútených dvojliniek, aj napriek tomu, že by v prípade spájania rovnakých zariadení mal byť použitý krížený kábel. Proti týmto chybám sú však prepínače obránené a dokážu sami detekovať vysielací a príjmací pár a podľa toho upraviť konfiguráciu na lokálnom rozhraní. Na rozhraniach je použitá technológia Gigabit ethernet s prenosovou rýchlosťou 1 Gb plného duplexu1.5.2. Ak však existuje duplicitné spojenie medzi prepínačmi, tie to vyhodnotia a protokolom Spanning Tree Protocol (STP)[2] vyberú len jedno a druhá linka sa okamžite stane nefunkčnou, aby v sieti nevznikali logické slučky. Pre zlepšenie výkonu spoju, medzi prepínačmi, som aplikoval technológiu Etherchannel. Vytvára z viacerých fyzických spojení medzi prepínačmi jedno logické, takže výsledná dostupná šírka pásma medzi nimi je suma liniek, zahrnutých do spoločného kanálu.

V OSPF smerovacej doméme sú rozhrania smerovačov propojených k tejto sieti súčasťou oblasti 0 a teda tranzitnej oblasti. Bez použitia virtuálnych liniek musí byť každá okrajová oblasť pre komunikáciu s ostatnými, pripojená minimálne jedným smerovačom práve do tranzitnej oblasti, cez ktorú hraničné smerovače posielajú všetky dáta. Súčasťou centrálnej úlohy je pomocná časť siete. V smerovacom protokole OSPF vystupuje ako samostatná oblasť s identifikátorom 100. Navrhol som ju tak, aby obsahovala server a niekoľko smerovačov. Server sa nachádza v sieti, ktorú však neobsluhuje OSPF, ale je pod administratívou smerovacieho protokolu Routing Information Protocol version 2 (RIPv2)[3]. Dôvodom tejto zmeny je, aby sa do autonómneho systému mohli cez hraničný smerovač ASBR dostať LSA oznamujúci externú cestu. Externé cesty v okrajových oblastiach sa ďalej môžu filtrovať. Nastavenie filtrácie je súčasťou zadania v koncovej úlohe a preto sa o implementáciu

[2]Protokol na datovej vrstve pre prevenciu vzniku sľučiek v topológiach s technológiu Ethernet [8].

[3]Novšia verzia protokolu RIP s podporou CIDR [13].

starajú študenti. Ak správne nastavia správania svoji hraničných smerovačov k externej ceste, bude mať ich oblasť prístup k službám vyšších vrstiev k už spomýnanej službe DNS a HTTP.

Samozrejmosťou je informačné okno s údajmi o nastaveniach smerovačoch, adresnom pláne a podobných dôležitých parametrov.

Multiuser rozhrania nie sú súčasťou topológie, ale akonáhle príde požiadavka na vytvorenie spojenia z koncovej úlohy, dynamicky sa vytvorí a administrátor centrálnej úlohy ho môže spravovať a ďalej s ním manipulovať. Maximálne doporučené množstvo multiuser rozhraní nie je v špecifikáci udávané, ale doporučuje neprekračovať počet 12 na jednu centrálnu úlohu. Každé rozhranie by malo mať názov odvodený z oblasti, ktorej zaručuje konektivitu. Disturibúcia centrálnej úlohy prebieha podobne ako koncovej, teda v jednom súbore, ktorý obsahuje všetky potrebné informácie a nakonfigurovanú topológiu.

8.5 Postup vypracovania

Úlohy sa študentovi dostanú v podobe dvoch súborov: koncová úloha a centrálna úloha. Pokiaľ existuje už niekde v sieti spustená centrálna úloha, nie je nutné ju na strane študenta používať a ďalej pracuje iba s koncovou úlohou.

Ak však študent pracuje na úlohe samostatne a stále má záujem simulovať smerovací protokol OSPF s podporou oblastí. Môže spustiť centrálnu úlohu na rovnakom počítači ako koncovú úlohu. Centrálna úloha pracuje ako samostatná inštancia programu Pakcet tracer, nezávisle na ostatných. Pretože som koncové úlohy navrhol s vysokou mierov variability, môže študent využívať viacero koncových úloh na jednom počítači a tým testovať protokol v systéme s viacerými oblasťami. Čo úlohy neobmedzuje na použitie v týme, ale môže byť súčasťou individuálnej prípravy študenta.

Vypracovanie úlohy som rozdelil do troch samostatných krokov.

1. Príprava – výpočet adries, základné nastavenia rozhraní smerovačov, staníc a serveru.
2. OSPF v lokálnej oblasti – implementovanie smerovacieho protokolu OSPF do lokálnej oblasti; modifkácia niektorých parametrov.
3. Začlenie oblasti do AS – príprava na pripojenie pomocou multiuser rozhrania; testovanie rôznych typov koncových sietí.

Prvé dve som navrhol tak, aby overovali základné znalostí z VLSM štandardu, Cisco IOS a smerovacieho protokolu OSPF. Po úspešnom dokončený má študent oblasť, kde všetky zariadenia majú nakonfigurovanú IP adresu a smerovače medzi sebou komunikujú a vymieňajú si LSU správy. Treti časť už využíva multiuser rozhranie a

prípaja oblasť do autonómneho systému, v ktorom už môžu, ale nemusia byť pripojené koncové úlohy ostatných študentov. V tento časti úlohy overujem a precvičujem znalosti z vyšších konfiguračných techník OSPF protokolu. Po dokončený poslednej časti môže študent ďalaj pokračovať v simulovaní siete, využívať služieb vyšších vrstiev, alebo implementovať nové protokoly a technológie.

8.5.1 Príprava a základné nastavenie

Po otvorení súboru s koncovou úlohou v Packet tracer sa spolu s hlavným oknom programu spustí vedľajšie – informačné. Obsahuje všetky údaje potrebné k úspešnému dokončeniu.

Pred samotným vypracovaním dostane študent pridelený rozsah IP adries triedy C a identifikačné číslo OSPF oblasti podľa tabulky 8.1. Rozhodnovanie o tom kto dostane aký rozsah a idetifikátor oblasti môže dať vyučujúci, alebo si to študenti, ktorých koncové úlohy budú súčasťou jedného autonómneho systému, rozdelia sami. Prvým zadaním je pridelený rozsah IP adries rozdeliť na podsiete, tak aby odzrkadľovali požiadavky kladené na jednotlivé segmenty siete. Segmenty sa od seba líšia počtom zariadení, ktoré sa v ňom nachádzajú. Teda študent musí aplikovať metódu variabilnej masky podsiete VLSM aby efektívne využil pridelené IP adresy.

Výsledok delenia študent aplikuje na sieť a vhodne priradí IP adresy zariadeniam v sieti. Ako rozhraniam smerovačov, tak aj sieťovým kartám pracovných staníc a serveru. Rozhrania smerovačov sa nastavujú cez príkazový riadok. Počítače s servery používajú nastavenie cez grafické rozhranie 8.6. Okrem IP adresy a masky môže študent špecifikovať adresu DNS servera. Vyberie si z dvoch možností.

- DNS server v lokálnej oblasti – využívanie domenových mien je možné, akonáhle bude smerovací protokol OSPF funkčný a smerovače budú poznať cestu k sieti, ktorá obsahuje server.
- DNS server v podpornej sieti – podporná sieť sa nachádza v cetntrálnej úlohe. Vyžadované je pripojenie cez multiuser rozhranie a správna distribúcia externej cesty v lokálnej oblasti.

Úloha automaticky vyhodnotí, či študent zadal masky podsietí v súlade s požiadavkami uvedenými v informačnom okne.

V tomto bode je dôležité overiť správne nastavenie rozhraní jednotlivých zariadení, pretože práve chyby zlého priradenia IP adries rozhraniu sú častým dôvodom nefunkčnej siete. Odporúčam využiť základný nástroj na analýzu sieťo ako ping. Zariadenia v jednom sieťovom segmente by mali medzi sebou posielať ICMP správy typu ECHO a REPLY.

Tab. 8.1: Rozdelenie rozsahov IP adries podľa oblastí.

Oblasť	Prvá IP adresa	Posledná IP adresa	Adresa ABR
Area 1	192.168.1.0	192.168.1.255	10.0.0.1
Area 2	192.168.2.0	192.168.2.255	10.0.0.2
Area 3	192.168.3.0	192.168.3.255	10.0.0.3
Area 4	192.168.4.0	192.168.4.255	10.0.0.4
Area 5	192.168.5.0	192.168.5.255	10.0.0.5
Area 6	192.168.6.0	192.168.6.255	10.0.0.6
Area 100	192.168.100.0	192.168.100.255	10.0.0.100

8.5.2 Základná konfigurácia OSPF v rámci jednej oblasti

Akonáhle je overená funkčnosť liniek medzi smerovačmi a smerovačmi a stanicami, dostáva sa študent k samotnej implementácii smerovacieho protokolu OSPF do siete. Konfigurácia prebieha podľa návodu v informačnom okne a súčasne je treba dodržiavať pridelený identifikátor oblasti. Ten sa priraďuje na všetkých rozhraniach smerovačov v lokálnej oblasti. Výnimku tvorí jedno rozhranie na ABR, ktoré bude slúžiť ako prístup do centrálnej siete cez multiuser rozhranie. Priradené bude do tranzitnej oblasti, ktorá má štandardný indetifikátor 0.

Pokiaľ základné nastavenie smerovacieho protokolu OSPF prebehlo v poriadku, komunikácia by medzi akýmikoľvek dvoma zariadeniami mala fungovať bez problémov. Možností ako overiť funkčnosť je viacero, od základných ako ping (smerovače aj stanice) až po protokoly vyšších vrstiev: HTTP, DNS (stanice a čiastočne smerovače). V návode však výrazne odporúčam sledovať zmeny cez smerovacie tabuľky a ich analýzov zistiť, či sú všetky siete v lokálnej oblasti dostupné.

Zmena ceny liniek

Nasleduje časť zameraná na doladenie fungujúceho systému. Ďalšou sadou príkazov zmení študent cenu liniek medzi vnútornými smerovačmi podľa zadania. Takáto situácia môže nastať, keď potrebuje administrátor operatívne zmeniť trasu paketov, ale zároveň potrebuje, aby bola linka funkčná. Smerovače ktoré zmenu zaznamenajú okamžite zaplavia sieť aktuálnymi LSU, ktoré iniciujú prepočítanie stromu najkratších ciest na ostatnýc zariadenia s aktivovaným protokolol OSPF. Ak smerovač vyhodnotí, že po prepočítaní stromu existuje kratšia cesta pre danú cieľovú IP adresu, ako má uloženú v smerovacej tabuľke, záznam nahradím aktuálne platným. Takýmto spôsobom je možné nepriamo riadiť smerovanie v okrajovej oblasti.

Nastavenie autentizácie OSPF správ

Významnú súčasť úlohy predstavuje nastavenie autentizácie medzi dvomi smerovačmi. Smerovače v simulačnom programe Packet tracer podporujú dva spôsoby autentizácie OSPF správ.

- Heslom prenášaným v otvorenej podobe.
- Algoritmom s využitím hašovacej funkcie MD5.

Pretože autentizáciu heslom, ktoré je navyše prenášané na linke v nezabezpečenej podobe, považujem za nedostatočné. Študent má za úlohu implementovať zabezpečenie typu MD5. Zaisťuje vyššie požiadavky na bezpečnosť čím je vhodnejšie pre využitie v reálnych situáciách. Sadou príkazov, ktoré sú popísane v postupe, študent zaručí, že smerovač môže overiť zdroj z ktorého informácie prišla. Ak sú kľúče na oboch komunikujúcich stranách správne nastavené, smerovače nadviažu susedstvo a budú si môcť vymeniť LSU správy.

Upravenie voľby DR a BDR smerovačov

Poslednou dôležitú úpravu v smerovacej doméme OSPF, ktorú musí študent zvládnuť, je dosiahnuť zmenu DR a BDR v segmente s broadcast vysielaním — časť, kde sú smerovače R1, R2, R3 prepojené prepínačom SW1. Pretože voľba zvolených smerovačov je na začiatku úlohy silne závisla na tom, v akom poradí boli rozhrania smerovačov konfigurované. To v niektorých situáciách považujem za nedostantočné a pokiaľ administrátor systému chce jasne definovať vybrané smerovače, musí zasiahnuť do voľby a zmeniť aktuálne rozdelenie.

Podľa požiadaviek, ktoré som umiestnil do zadania, má študent za úlohu prinútiť smerovač R1 prebrať úlohu DR a R2 funkciu BDR. Výsledok je možné dosiahnuť dvomi spôsobmi:

- zmena priority,
- zmena RID.

Samozrejeme na dosiahnutie cieľu môže použiť oboje no v návode odporúčam prvú variatu, ktorá nerobí zásah do identifikácie smerovača v sieti. Študent ďalej reštartom OSPF procesu znovu zariadiť voľby DR a BDR.

Celý proces je sledovaný úlohou, podľa kritérií, ktoré som definoval a aplikoval do úlohy.

8.5.3 Pripojenie OSPF oblasti do autonómneho systému

Pokiaľ je OSPF smerovací protokol v oblasti správne nastavený, je možné pripojiť túto okrajovú oblasť pomocou ABR do tranzitnej oblasti. K tomu slúži multiuser rozhranie umiestnené v topológii. Študent vloží parametre do nastavenia multiuser

rozhrania medzi koncovou a centrálnou úlohou. Základný údaj je socket: IP adresa + číslo portu. IP adresa môže byť zároveň adresa lokálnej sľučky, pokial centrálna úloha beží na rovnakom počítači ako koncová. Štandardný port je tcp:38000.

Po úspešnom pripojení sa zmení symbol pre multiuser rozhranie a spojenie medzi centrálnou a konečnou úlohou je naviazane. Následne už je možne spojiť ABR smerovač s prepínačom v centrálnej úlohe. Na fyzickej vrstve je použitý priamy kábel a technológia Ethernet. Študent jednoduchým spôsobom chyť-a-pusť (drag-and-drop) spojí ABR s Multiuser, kde sa mu zobrazí výber všetkých portov, ktoré prepínače v centrálnej úlohe ponúkajú. Voľba na ktorý port bude ABR pripojený nemá na výsledok žiadny vplyv.

Akonáhle sa vytvorí spojenie medzi prepínačom v centrálnej úlohe a smerovačov v koncovej, prejde rozhranie na smerovači zo stavu down do stavu up. Začne nadväzovať susedstvo s DR v transportnej oblasti. Porovná všetky kritériá, ktoré sú nutné k úspešnému založeniu susedstva. Akonáhle ho úspešne nadviažu začnú si medzi sebou vymieňať LSA. Vnútorné smerovače v okrajovej oblasti sa začnú dozvedať o ostatných sieťach pripojených k centrálnej. Študent sleduje tento proces ako zmenu v smerovacích tabuľkách. Štandardnými testovacími nástrojmi si môžu študenti overiť vzájomné spojenie.

Týmto posledným krokom je OSPF okrajová oblasť úspešne pripojená do autonómneho systému. Pokiaľ existuje aspoň jedna okrajová oblasť, ktorá má úspešne naviazané spojenie s tranzitnou. Môže študent testovať spojenie s nimi a to buď na nižších vrstvách alebo počítačom sa pripojiť na niektorý z dostupných HTTP serverov.

Ďalšie zadanie spočíva v úprave typu okrajovej oblasti, tak aby sa do nej dostali iba určité typy LSA. To znamená nakonfigurovať ABR a vnútorné smerovače pre okrajovú oblasť typu stub a totaly stubby. Nastavenia majú za následok redukciu záznamov v smerovacích tabuľkách vnútorných smerovačov, pretože sa do oblasti oznamuje iba predvolená cesta.

V prvom prípade sa do oblasti nedostane LSA od ASBR smerovača, ktorý ohlasuje sieť s aktívny smerovacím protokolom RIPv2 ako externú cestu. V druhom prípade bude ABR totaly stubby oblasti blokovať LSA typ 3, vytváraný ABR smerovačmi v koncových úlohách ostatných študentov.

Súčasná verzia simulačného programu Packet tracer nepodporuje sumarizáciu, preto nie je možné zmenšovať počet záznamov v smerovacích tabuľkách koncentráciou do jedného záznamu. Napriek tomu je vhodné využívať pridelený adresný priestor tak, aby bola sumarizácia v budúcnosti možná.

Tým je celá úloha ukončená. No napriek tomu môže študent pokračovať v používaní a prípadom využití nový protokolov, technológií a služieb.

8.6 Služby ponúkané centrálnou úlohou

Okrem hlavnej úlohy, tranzitná oblasť pre OSPF doménu, ponúka centrálna úloha služby protokolov vyšších vrstiev. Do topológie centrálnej úlohy som vložil server s viacerými službami Internetu, ale aj intranetu väčšiny organizácii. Server ukrytý pred OSPF v doméne smerovacieho protokolu RIPv2, takže do OSPF domény je rozhlasovaný v externej ceste. Na servery som spustil služby DNS a HTTP.

8.6.1 Využite služby DNS v úlohe

DNS v úlohách funguje, tak, že server v centrálnej úlohe funguje ako DNS server pre celý autonómny systém. Databáza doménových mien obsahuje asociácie IP adresy a mena stáníc PC1, PC2 a servera pre prvých šesť oblastí 8.2. Aby systém správne fungoval, je nutné, aby sa študent pri plánovaní rozloženia adries v okrajovej oblasti dodržali niekoľkých pravidiel:

- IP adresa servera SERV: 192.168.X.1,
- IP adresa stanice PC1: 192.168.X.2,
- IP adresa stanice PC2: 192.168.X.33,

kde X označuje posledných 8 bitov, z celkového počtu určených pre adresovanie siete. Tieto pravidlá nie je, pri správnom návrh rozdelenia adresného priestoru, ťažké dodržať. Implementoval som kontrolu, ktorá vyhodnotí, či boli masky a IP adresy týchto troch zariadení nakonfigurované správne.

Ak sú všetky stanice a server nastavené odpovedajúcou IP adresou, je môžné na ne pristupovať pomocou doménového mena. Využívať sa dá pri zadávaní príkazu ping na smerovačoch, alebo príkazovom riadku akejkoľvek stanice v AS. Ako stanice, tak aj smerovače musia mať nakonfigurovaný IP adresu názvového serveru.

8.6.2 Webové služba v koncovej a cetrálnej úlohe

Okrem serverov v okrajových oblastiach, ktoré sú sučasťou koncových úloh som do AS zaradil aj HTTP server v oblasti 100 v centálnej úlohe. Záznam je funkčný stále bez ohľadu na rozdelenie IP adres v autonómnom systéme. HTTP server som nastavil tak, aby vyčkával na prichádzajúce požiadavky na štandradnom porte tcp:80. Ak študent zadá adresu, buď IP, alebo doménový názov, do prehliadača v koncovom zariadení, zobrazí sa mu webová prezentácia, ktorú som vytvoril. Webová stránka je formátovaná základnými html značkami, ktoré Packet tracer podporuje.

Tým, že som do úlohy na smerovací protokol OSPF integroval služby vyšších vrstiev referenčného modelu TCP/IP, sa sieť priblížila fungovaniu reálneho autonómneho systému. Zároveň je server, ktorý poskytuje DNS a HTTP, umiestnený

Tab. 8.2: Záznamov DNS v autonómnom systéme.

Oblasť	Zariadenie	IP adresa	Doménové meno
Area 1	PC1	192.168.1.2	pc1.area1
	PC2	192.168.1.33	pc2.area1
	SERV	192.168.1.1	server.area1
Area 2	PC1	192.168.2.2	pc1.area2
	PC2	192.168.2.33	pc2.area2
	SERV	192.168.2.1	server.area2
Area 3	PC1	192.168.3.2	pc1.area3
	PC2	192.168.3.33	pc2.area3
	SERV	192.168.3.1	server.area3
Area 4	PC1	192.168.4.2	pc1.area4
	PC2	192.168.4.33	pc2.area4
	SERV	192.168.4.1	server.area4
Area 5	PC1	192.168.5.2	pc1.area5
	PC2	192.168.5.33	pc2.area5
	SERV	192.168.5.1	server.area5
Area 6	PC1	192.168.6.2	pc1.area6
	PC2	192.168.6.33	pc2.area6
	SERV	192.168.6.1	server.area6
RIPv2	SERV	172.16.0.1	server.rip

mimo OSPF domény čo simuluje prípad Internetu, kedy je väčšina týchto serverov umiestná mimo lokálny AS.

8.7 Využitie simulačného módu v konečnej úlohe

Súčasťou úlohy je aj simuláčný mód, ktorý vizualizuje pakety prenášané medzi zariadeniami. Prepnutie do módu simulácie zastavý čas a pakety sú posielané dvomi spôsobmi:

- pošli a čakaj – po tom čo sa paket pošle musí študent potvrdiť poslanie ďalšieho paketu,
- posielaj postupne – pakety sa posielajú postupne a doba medzi prijatím jedného a vyslaním ďalšieho je nastaviteľná posuvníkom.

Doporučujem použiť oboje, pretože každý z nich je vhodný na iné účely. Študent počas konfigurácie smerovacieho protokolou OSPF prepne program Packet tracer do režimu simulácie. Za pomoci filtru vyberie pakety, ktoré ho zaujímajú, v tomto prípade OSPF, a použije jeden z módov simulácie. Prakticky stále si smerovače v sieti vymieňajú HELLO zprávy, takže vždy je možné zachytiť tento druh komunikácie.

V situáciách ako zmena ceny liniek študent uvidí zaplavovanie siete LSU správami s aktuálnym LSA informujúcim o zmene v stavu linky.

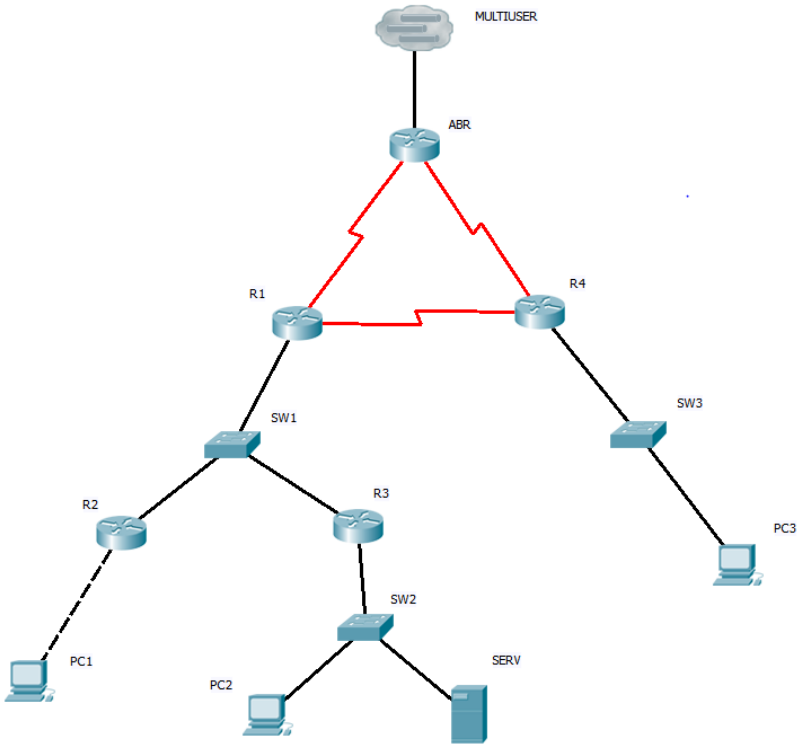
Mód umožňuje nahliadnuť do ramca, paketu a zprávy prenášanej na linke. Vo výpise prenesených rámcov si môže vybrať jeden z nich a pozrieť si informácie v hlavičkách na jendnotlivých vrstvách modelu OSI. Na linkovej to je hlavička ethernetu s MAC adresami. Sieťová obsahuje IP hlavičku obsahujúca IP adresy, číslo protokolu vyššej vrstvy a ďalšie štandardné parametre. Vo vyšších vrstách už študent vidí OSPF správy rozpísané do tabuľky. Može si prezrieť obsah a formu a lepšie pochopiť štruktúru dát. Súčasne som vytvoril niekoľko ICMP paketov, ktoré sú súčasťou scenára a študent spustením scenára uvidí paket ako cestuje medzi zariadeniami v sieti. Simulačný mód funguje v koncovej úlohe a centrálnej úlohe, iba ak nie je aktívne rozhranie multiuser. Takže ak študent pripojený do autonómneho systému a chce využiť simulačného módu, musí odpojiť multiuser rozhranie. Napriek tomu je simulačný mód prínosný a pomáha k pochopeniu princípov komunikácie smerovacieho protokolu OSPF.

8.8 Vyhodnotenie a kontrola správnosti

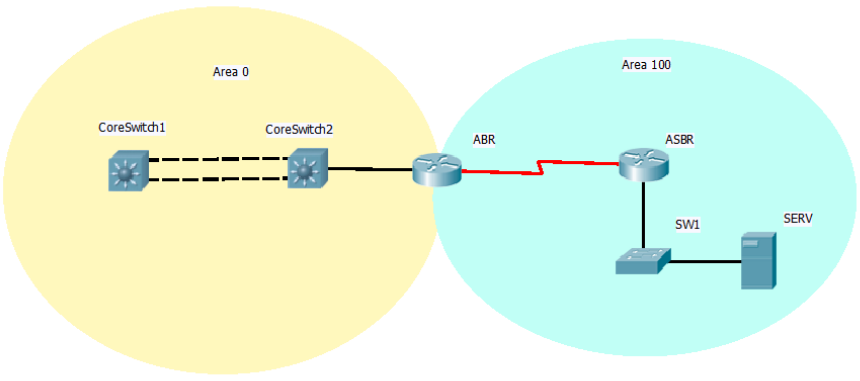
Úlohu som nakonfiguroval tak, aby kontrolovala správnosť zadaných príkazov a nastavení. Každé dielčie zadanie je ohodnotené bodmi a na výslednom bodovom zisku sa podieľajú podľa ich náročnosti a dôležitosti pre funckiu siete.

V dolnej časti informačného okna sa zobrazuje aktuálne percento, ktoré značí aké množstvo bodov z celkového počtu už bolo dosiahnuté, teda koľko zadaní študent dokončil správne.

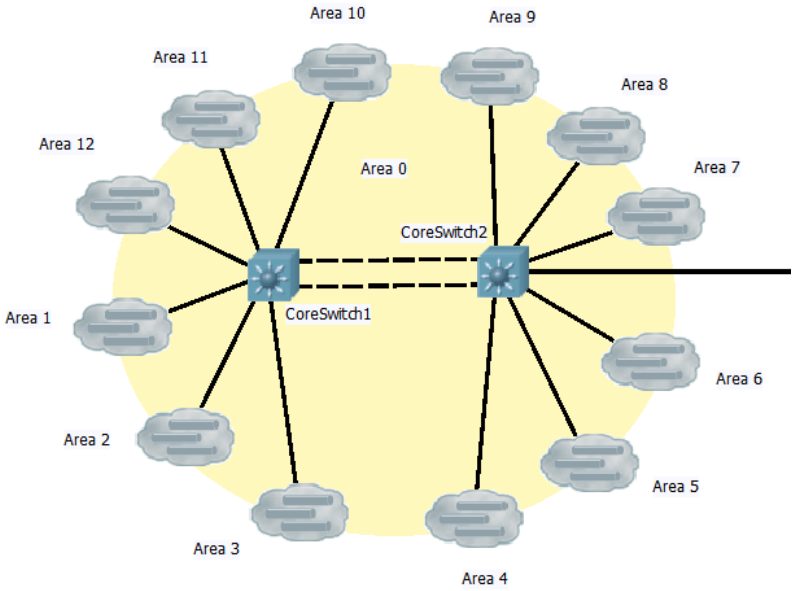
Počas práce na úlohe môže kontrolovať, ktoré časti už sú hotové a ktoré nie. Čiastočné vyhodnotenie sa vyvolá tlačidlom ukončenia, z ktorého je možne sa späť vrátiť do simulácie a pokračovať v práci. Čím som zaručil, aby mohol študent kontorolovať splnenie požiadavkov.



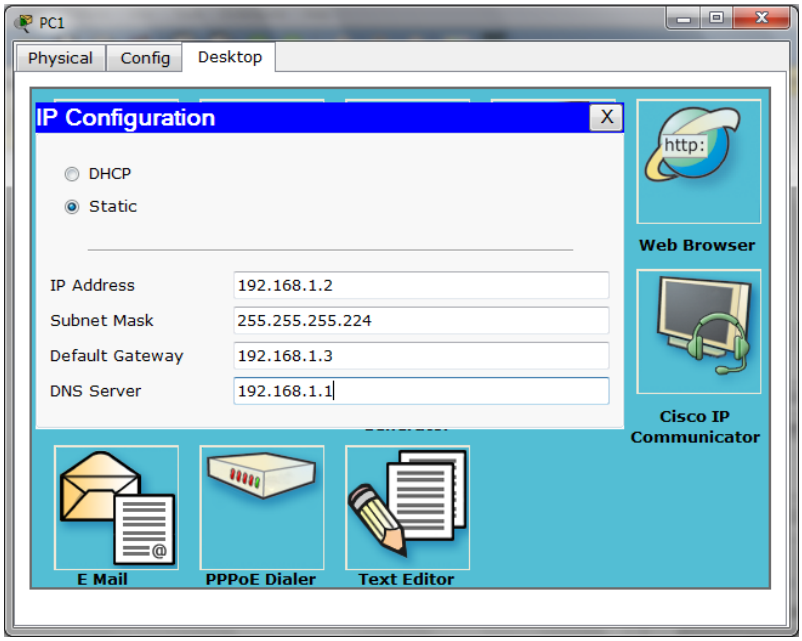
Obr. 8.3: Topológia siete v koncovej úlohe.



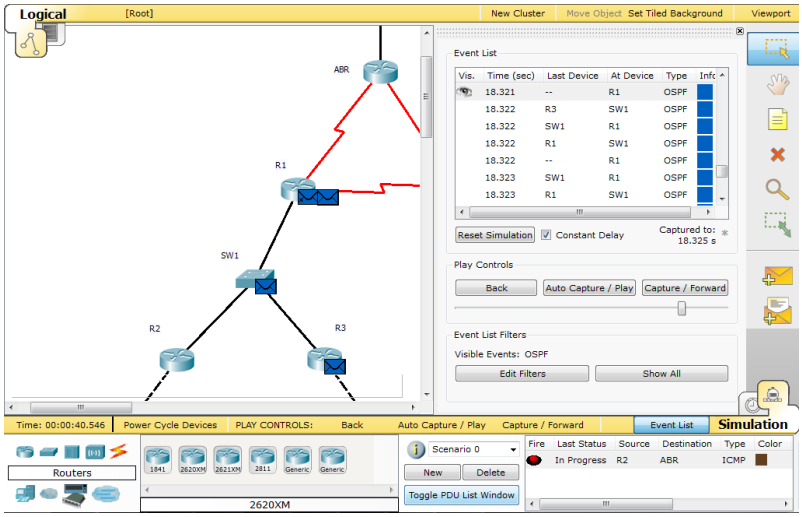
Obr. 8.4: Topológia siete v koncovej úlohe.



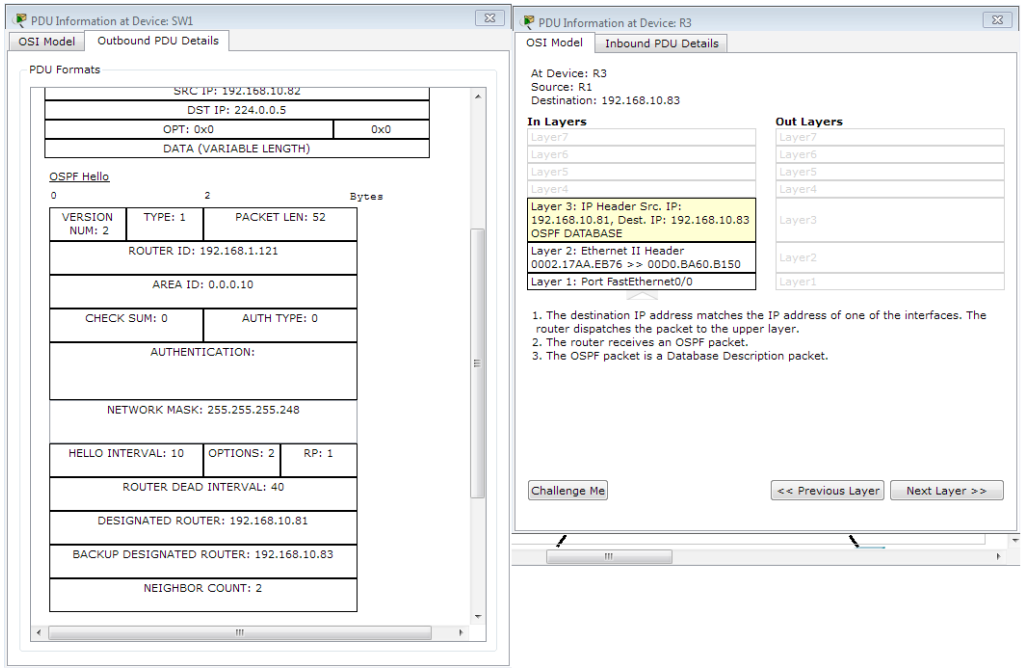
Obr. 8.5: Topológia siete v koncovej úlohe.



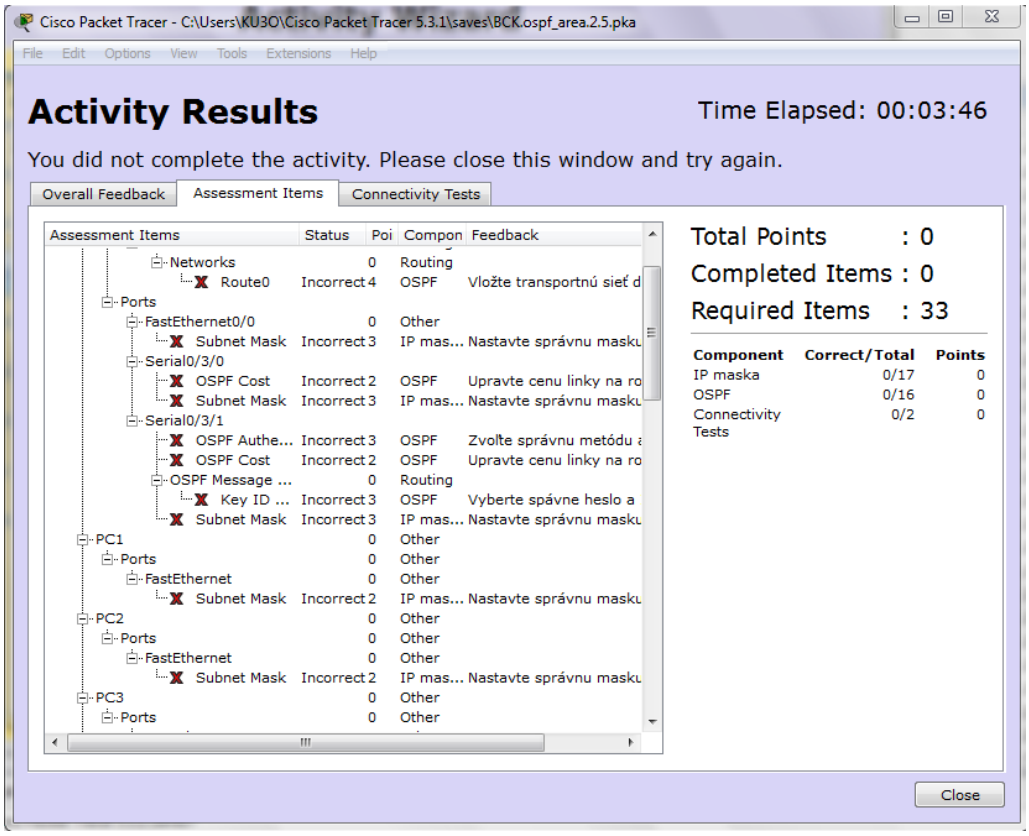
Obr. 8.6: Grafické rozhranie dialógu nastavenia IP adresy na počítači.



Obr. 8.7: Simulačný režim so zapnutou filtráciou OSPF správ.



Obr. 8.8: Zobrazenie obsahu rámca vo vrstvách referenčného modelu OSI a správy OSPF v bitovej tabuľke.



Obr. 8.9: Vyhodnotie úlohy s výpisom splnených a nesplnených zadaní.

9 ZÁVER

Behom simulácie a práce na úlohe, som si uvedomil význam smerovacieho protokolu OSPF. Tým, že som vytvoril úlohu pre študentov, môžem tieto poznatky sprístupniť v zaujímavej a zároveň dostatočne odbornej forme. Úloha využíva teóriu, ktorú som spracoval v kapitolách 2 a 4 a s jej pomocou som sa snažil prezentovať vlastnosti, ktorými smerovací protokol OSPF disponuje.

Ako simulačný nástroj, ktorý som neskôr použil aj pri tvorbe úlohy, som si vybral Packet tracer. Vďaka funkciám a rozšíreniam, ktoré som popísal v kapitole 6, som mohol do úlohy vložiť niekoľko atraktívnych prvkov. Za najzaujímavejšie považujem rozšírenie, ktoré umožnuje študentom spájať svoje siete do jednej veľkej a vytvárať tak komplexné systémy. Vďaka nemu môžu študenti pracovať ako tým a každý člen zodpovedá za svoju sieť. No zároveň musia spoločnými silami zabezpečiť bezchybný chod autonómneho systému.

Okrem úlohy som naviac preniesol učebňu Cisco akadémie do simulácie v programe Packet tracer. Zobrazenie prvkov v simulácii je takmer totožné s rozložením smerovačov, prepínačov a staníc v učebni. Čím sa mi podarilo verne napodobiť reálne podmienky. Študent môže využiť učebňu Cisco akadémie v programe Packet tracer na riešenie úloh, bez nutnej prítomnosti v učebni.

Myslím že ako úloha na smerovací protokol OSPF, tak aj simulácia učebne, majú potenciál stať sa súčasťou výuky či už premetov Cisco akadémie, alebo iných, zameraných na problematiku smerovania v IP sieťach.

LITERATÚRA

[1] PRITSKY, T., MOORE, M., SOUTHWICK, P., RIGGS, C. *Telecommunications: a beginner's guide*. McGraw-Hill Professional, 2001. 507 s. ISBN 978-00-721-9356-5

[2] SOSINSKY, B. *Mistrovství – počítačové sítě*. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7

[3] PUŽMANOVÁ, R. *TCP/IP v kostce*. České Budějovice : Kopp, 2004. 607 s. ISBN 80-7232-236-2

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

[5] EMPSON, S. *CCNA : kompletní přehled příkazů : autorizovaný výukový průvodce* [preklad Krásenský, D.]. 1. vydanie. Brno : Computer Press, 2009. 336 s. ISBN 978-80-251-2286-0.

[6] KRČMÁŘ, P. *Linux : postavte si počítačovou síť* 1. vydanie. Praha : Grada, 2008. 182 s. ISBN 978-80-247-1290-1

[7] TEARE, D. *Návrh a realizace sítí Cisco*. Brno : Computer Press, 2003. 758 s. ISBN 80-251-0022-7

[8] VELTE, J., VELTE, T. *Síťové technologie Cisco : velký průvodce*. Brno: Computer Press, 2003. 759 s. ISBN 80-7226-857-0

[9] *Směrovací protokol OSPF* [online]. 2004 [cit. 4. 5. 2011] Dostupný z WWW: <http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html>.

[10] HUCABY, D., MCQUERRY, S. *Konfigurace směrovačů Cisco*. [preklad Veselký, J.]. Computer press, 2004. 632 s. ISBN 80-722-6951-8.

[11] GRAZIANI, R., JOHNSON, A. *Routing Protocols and Concepts, CCNA Exploration Companion Guide*. Cisco Press, USA, 2007. 606 s. ISBN 978-1-58713-206-3.

[12] DROMS, R., LEMON, T. *DHCP Příručka administrátora* [preklad Blažík, M., Černý, J.]. 1. vydanie. Brno : Computer Press, 2004. 490 s. ISBN 80-251-0130-4

[13] SPORTACK, MARK A. *Směrování v sítích IP* [preklad Krásenský, D.]. 1. vydanie. Brno : Computer Press, 2004. 351 s. ISBN 80-251-0127-4.

[14] KABELOVÁ, A., DOSTÁLEK, L. *Velký průvodce protokoly TCP/IP a systémem DNS*. Praha : Computer Press, 2002. 542 s. ISBN 80-7226-675-6

[15] *Cisco Akademie* [online]. 2011 [cit. 4.5. 2011]. Český. Dostupný z WWW: <http://adela.utko.feec.vutbr.cz/cisco_akademie/>.

[16] *Packet Tracer 5.0 Data Sheet* [online]. ©2008 [cit. 4. 5. 2011]. Angličtina. Dostupný z WWW: <http://www.cisco.com/web/learning/netacad/downloads/pdf/PacketTracer5_0_DS_0703.pd

[17] WALLACE, K. *Cisco VoIP : autorizovaný výukový průvodce*. Brno : Computer Press, 2009. 527 s. ISBN 978-80-251-2228-0

ZOZNAM SKRATEK

ABR Area Border Router

AD Administrative Distance

AS Autonomous System

ASBR Autonomous System Border Router

AUX Auxiliary – pomocný port

BDR Backup Designated Router

BGP Border Gateway Protocol

CIDR Classless Inter-Domain Routing

CLI Command-line interface

DBD Database Description

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DR Designated Router – referenčný router

FEKT Fakulta elektrotechniky a komunikačních technologií

HTML HyperText Markup Language

HTTP Hypertext Transfer Protocol

ICMP Internet Control Message Protocol

IGP Interior Gateway Protocol

IOS Internetwork Operation System

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

ISP Internet service provider – poskytovateľ Internetového pripojenia

LAN Local Area Network

LSA Link State Advertisment

LSAck Link State Acknowledgement

LSDB Link-State Database

LSR Link State Request

LSU Link State Update

MAC Media Access Control

MAN Metropolitan Area Network

MD5 Message-Digest algorithm

NBMA Non–Broadcast Multiple Access

OSI Open Systems Interconnection

OSPF Open Short Path First

OSPFv2 Open Short Path First version 2

OSPFv3 Open Short Path First version 3

QoS Quality of Service

RID Router Identifier

RIP Routing Information Protocol

RIPv2 Routing Information Protocol version 2

SPF Shortest Path First

SSH Secure Shell

STP Spanning Tree Protocol

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol / Internet Protocol

TFTP Trivial File Transfer Protocol

UDP User Datagram Protocol

VLSM Variable Length Subnet Mask

VoIP Voice over Internet Protocol

VUT Vysoké učení technické

WAN Wide Area Network

ZOZNAM PRÍLOH

A CD-ROM

A.1 xwolfj01.pdf

Elektronická verzia diplomovej práce vo formáte PDF.

A.2 ciscoClass.pka

Súbor programu Packet tracer obsahujúci simuláciu Cisco akadémie. Vytvorené a testované na verzii 5.1. Otvorenie súboru prebieha štandardným spôsobom cez menu v okne programu.

A.3 examEdge.pka

Súbor programu Packet tracer obsahujúci Koncovú úlohu. Vytvorené a testované na verzii 5.1. Otvorenie súboru prebieha štandartným spôsobom cez menu v okne programu.

A.4 examCentral.pka

Súbor programu Packet tracer obsahujúci Centrálnu úlohu. Vytvorené a testované na verzii 5.1. Otvorenie súboru prebieha štandartným spôsobom cez menu v okne programu.

A.5 classWeb.html

Webová prezentácia pre simuláciu učebne Cisco akadémie vo formáte HTML.

A.6 examWeb.html

Webová prezentácia pre vypracovateľnú úlohu s OSPF smerovací protokolom vo formáte HTML.

A.7 styles.css

Štýlový css súbor pre HTML prezentácie.

A.8 Zložka: pic

Zložka obsahujúca obrázky k webovým prezentáciám.