Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 812 19 Bratislava

Simulátor komunikácie v počítačovej sieti

Tím č. 5
Red Dwarf

Odbor: Počítačové systémy a siete
Vedúci tímového projektu: Ing. Katarína Jelemnská, PhD

18. november 2005

Bc. Martin Hornáček
Bc. Michal Jánoš
Bc. Milan Melicherčík
Bc. Ján Václavik

Zadanie projektu

Navrhnite a zrealizujte programový systém pre simuláciu sieťovej komunikácie na druhej a tretej vrstve sieťovej architektúry RM OSI. Systém má umožňovať:

- definovanie topológie simulovanej siete,
- simuláciu rôznych prepájacích zariadení (napr. prepínač, smerovač, firewall ...),
- simuláciu komunikácie medzi prepájacími zariadeniami.

Funkčnosť navrhnutého systému overte v sieti so simulovanými zariadeniami pomocou komunikácie medzi koncovými zariadeniami.

OBSAH:

ZOZNAM OBRÁZKOV:

ZOZNAM TABULIEK:

1 Úvod

Predkladaný dokument je dokumentáciou k riešeniu projektu v rámci tímového projektu v školskom roku 2005/2006 tímom 19 – Red Dwarf. Našou úlohou bolo riešenie úlohy Simulátor komunikácie v počítačovej sieti. Dokument obsahuje analýzu, špecifikáciu a návrh riešenia.

1.1 Prehľad dokumentu

Analýza problému je popísaná v kapitole 2. Prehľadom problematiky a rozdelením základných sieťových technológií sa zaoberá kapitola 2.1. V kapitole 2.2 je analyzované riešenie podobného projektu iným tímom.

Špecifikácia požiadaviek sa nachádza v kapitole 3. V kapitole 3.1 je špecifikácia používateľského rozhrania, v kapitole 3.2 implementácia jednotlivých zariadení a v kapitole 3.2 sú prípady použitia.

Kapitola 4 obsahuje návrh systému.

1.2 Použité skratky

Táto kapitola obsahuje vysvetlenie skratiek použitých v tomto dokumente.

AS -	autonómny systém
BPDU -	dátová jednotka prepínacieho protokolu (*Bridge Protocol Data Unit).*
BDR -	záložný vyhradený smerovač (*Backup Designated Router*)
CIDR -	beztriedne smerovanie v rámci domény
CLI -	interfejs príkazového riadku
CRC -	kontrolný medzi súčet
CSMA/CD	metóda prístupu na linku a detekcie kolízií
DDP -	paket na komunikáciu s databázou
DR -	vyhradený smerovač (*Designated Router*)
DVA -	algoritmus na výpočet najkratšej cesty
FDDI -	optické rozhranie pre distribuované dáta
ID -	identifikátor
IGP -	protokol v rámci jednej domény

ISO -	medzinárodná štandardizačná organizácia
LAN -	lokálna sieť
LSA -	algoritmus na výpočet najkratšej cesty
MAC -	jedinečná adresa sieťového rozhrania
MAN -	miestna sieť
Mbps -	prenosová rýchlosť udávajúca počet mega bitov za sekundu
RFC -	odporúčania
RM-OSI -	simulačný model siete
STP -	protokol vetviaceho sa stromu
TCN -	upozornenie na zmenu topológie
VLSM -	variabilná dĺžka masky podsiete
WAN -	siete geografického rozsahu

1.3 Použitá notácia

Opis notácie použitej pri vytváraní diagramov uvedených v dokumente.

Diagram prípadov použitia a aktivít

Používateľ

Asociácia, väzba

Prípad použitia

2 Analýza

2.1 Úvod do problematiky

Počítačová sieť je systém vzájomne prepojených a spolupracujúcich počítačov. Medzi nimi možno prostredníctvom siete prenášať informácie.

2.1.1 Druhy počítačov v sieti

- **Pracovné stanice**- slúžia na spracovanie údajov používateľom. Je to samostatný počítať pripojený do siete, využívajúci jeho služby.
- **Server**- zabezpečuje chod siete. Realizuje funkcie siete a poskytuje ostatným používateľom svoje prostriedky (pamäť, tlačiareň...)

V sieti môže byť ľubovoľný počet serverov a pracovných staníc. Ak je serverov v sieti viac, môžu sa navzájom v poskytovaní služieb a prostriedkov doplňovať.

2.1.2 Základné časti siete

Sieť pozostáva z týchto základných častí:

- **Hardware** - zahrňuje všetky technické prostriedky počítača. Patria sem aj prostriedky, ktorými je realizované vlastné prepojenie siete (sieťové adaptéry...)
- **Software** - programové vybavenie, ktoré v spolupráci s hardware-om siete zabezpečuje funkcie siete. U niektorých operačných systémov sú tieto funkcie už jeho súčasťou.

2.1.3 Význam počítačových sietí

- **Zdieľanie údajov** - vďaka tomu, že dátové súbory sú uložené na serveroch siete a pripojení používatelia majú k nim prístup, môže potrebné dátové súbory spracovávať viac používateľov siete súčasne.
- **Zdieľanie prostriedkov** - umožňuje pracovným staniciam spoločne používať prostriedky siete, ktoré ponúkajú servery siete. Najčastejšie ide o zdieľanie diskov, keď lokálne disky pracovných staníc nemajú kapacitu a zdieľanie tlačiarní.

- **Zvýšenie spoľahlivosti systému** - v súvislosti so zdieľaním prostriedkov je možné v prípade poruchy zdieľaného prostriedku nahradiť tento prostriedok iným (tlačiareň...) a systém môže pracovať ďalej.

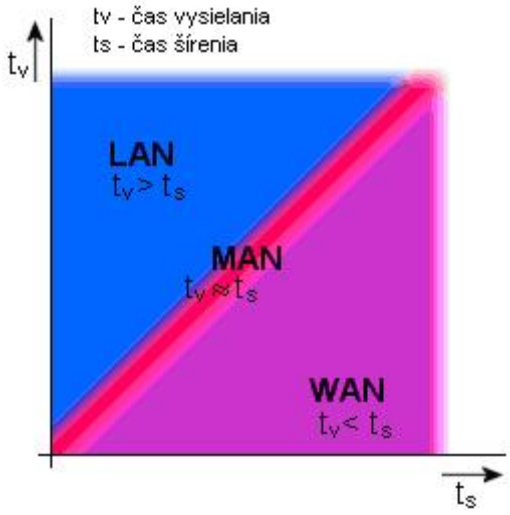
2.1.4 Rozdelenie podľa rozlohy

Siete sa rozdeľujú podľa pomeru doby vysielania a prijímania dát.

Local Area Network – **LAN –** Tieto siete sú rozsiahle od 10 m až do 1000 m. Sú to väčšinou siete v jednej budove alebo viacerých susediacich budovách. V rámci budovy sa používa štruktúrovaná kabeláž kombinujúca UTP a optické káble . Pre spojenie budov sa používajú optické káble alebo bezdrôtové spoje. Tieto siete môžu byť prepojené do ďalších väčších sietí. U LAN je doba vysielania **tv** vyššia ako doba šírenia signálu **ts** po prenosovom médiu (**tv > ts**).

Metropolitan Area Network – **MAN –** Verejná sieť pracujúca vysokou rýchlosťou a schopná prenášať dáta na vzdialenosť až 80 km. Tato sieť je menšia než WAN ale väčšia než LAN. Pre klasifikáciu pre ňu platí približne to isté čo v sieťach LAN. Sieť MAN má približne rovnakú dobu vysielania ako šírenia signálu (**tv = ts**).

Widea Area Network – WAN – S rastom geografického dosahu sietí pripojovanie užívateľov v rôznych mestách alebo štátoch prerastá sieť LAN a MAN do siete WAN (Wide Area Network). Počet užívateľov v takej sieti môže byť od desiatich do niekoľko tisíc užívateľov.
Doba vysielania je menšia než doba šírenia (**tv < ts**).



Obrázok č. 1: Rozdelenie sietí podľa rozlohy

2.1.5 Rozdelenie podľa topológie

Všetky návrhy siete vychádzajú z troch základných topológií:

- **Zbernicová topológia siete** - ak sú zapojené za sebou pozdĺž jediného kábla (segmentu).
- **Hviezdicová topológia siete** - ak sú počítače zapojené k segmentom, ktoré vychádzajú z jediného bodu (rozbočovača).
- **Prstencová topológia siete** - ak sú počítače zapojené ku káblu, ktorý tvorí prstenec.

2.1.6 Typy sietí podľa technológie

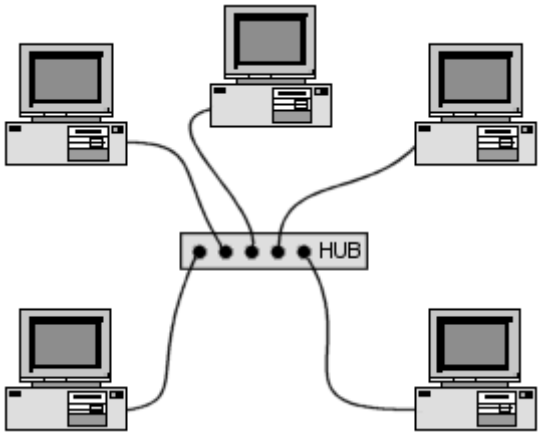
Siete sa dajú rozdeliť na 5 základných skupín, podľa použitej technológie:

- ArcNet
- Token-ring
- 100VG-AnyLAN
- FDDI
- Ethernet

ArcNet

Skratka slovného spojenia "Attached Resource Computer Network" (počítačová sieť s prepojenými prostriedkami). Ide o počítačovú sieť vyvinutou spoločnosťou Datapoint Corporation v roku 1977, ktorá umožňuje prepojiť množstvo osobných počítačov a pracovných staníc. Maximálny počet je 255.

Prenosovým médiom je koaxiálny kábel RG-62 A/U s impedanciou 93 ohmov. ArcNet je ale možno prevádzkovať aj na krútenej dvojlinke alebo optickom kábli. S použitím koaxiálneho kábla je maximálna dĺžka kábla od pracovnej stanice k rozbočovaču 610 metrov.



Obrázok č. 2: Sieť typu ArvNet

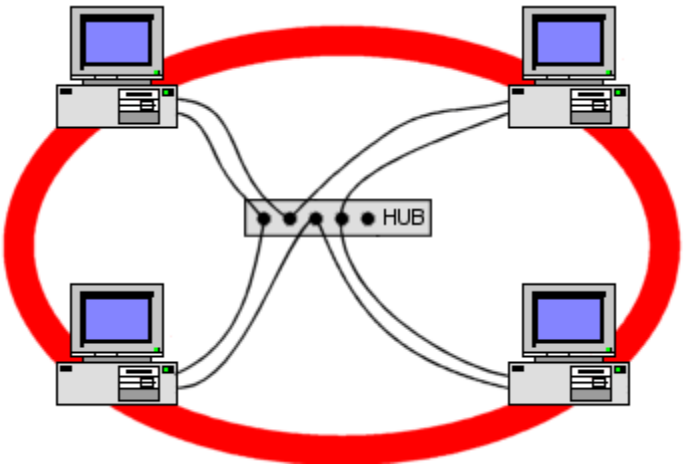
Predstavená sieť využíva prístupovú metódu založenú na predávaní známky a má prenosovú rýchlosť až 2,5 Mbps. Novšia verzia ArcNet Plus podporuje prenosovú rýchlosť až 20 Mbps. Maximálny priemer siete je 6,5 km. Fyzické zapojenie je hviezda, ale logická komunikácia je kruh.

Token-ring

Tato sieť bola v roku 1984 predstavená spoločnosťou IBM, ako súčasť riešenia prepojiteľnosti všetkých tried počítačov IBM.

V novších verziách bola prenosová rýchlosť 16Mb/s. Maximálna dĺžka závisí od počtu koncových zariadení, použitých káblov a zosilňovačov. V sieti token ring sú stanice prepojené do kruhu. Právo vysielať sa odovzdáva postupne v poradí pomocou špeciálneho rámca token. Aj keď je táto technológia založená na kruhové topologi, sieť Token-ring používa

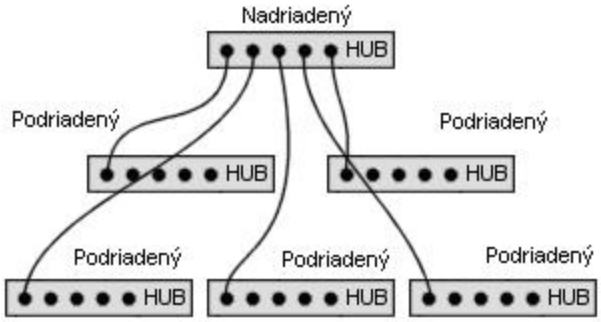
hviezdicové skupiny až ôsmich pracovných staníc, ktoré môžu byť napojené na hlavný kruh. Maximálny počet staníc je až 260 na jeden koncentrátor.



Obrázok č. 3: Sieť typu Token-ring

100VG-AnyLAN

Je to riešenie od firmy Hewlett-Packard. Rýchlosť tejto siete je minimálne 100 Mbps. Maximálny priemer siete je 7,7 km. Maximálny počet staníc nie je obmedzený, záleží od počtu rozbočovačov. Médiom je krútená dvojlinka a optický kábel. Je tu použitá bezkolízna prístupová metóda, umožňujúca dve úrovne priority (nízku a vysokú). Na 7,7 km je jeden rozbočovač. Za každý druhý rozbočovač sa musí odčítať 1,1 km.

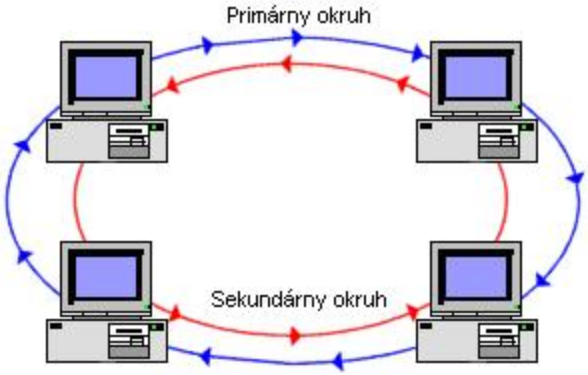


Obrázok č. 4: Sieť typu 100VG-AnyLAN

FDDI

Skratka slovného spojenia "Fiber Distributed Data Interface" (optické rozhranie pre distribuované dáta). Bola vytvorená v roku 1986.

Rýchlosť prenosu je 100 Mbps používajúca dvojitú protismernú kruhovú topológiu, podporujúcu až 500 počítačov. Jeden kruh sa označuje ako primárny a druhý ako sekundárny. Prenos dát prebieha väčšinou v primárnom okruhu. Pokiaľ nastane porucha v primárnom prstenci, FDDI automaticky prekonfiguruje sieť tak, aby mohli byť dáta posielané v druhom okruhu. Vďaka tejto redundancii je zaistená vysoká spoľahlivosť.

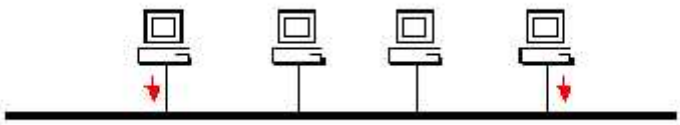


Obrázok č. 5:Sieť typu FDDI

Ethernet

Ethernet bol vyvinutý firmou Xerox v roku 1976. Ethernet používa prístupovú metódu CSMA/CD. Má svoj typ rámca. Pôvodne používal zbernicovú topológiu a umožňoval pripojiť na hlavný segmenty až 1024 počítačov a pracovných staníc. Jednotlivé stanice sú prepojené pomocou koaxiálneho kábla, optickým káblom či krútenou dvojlinkou.

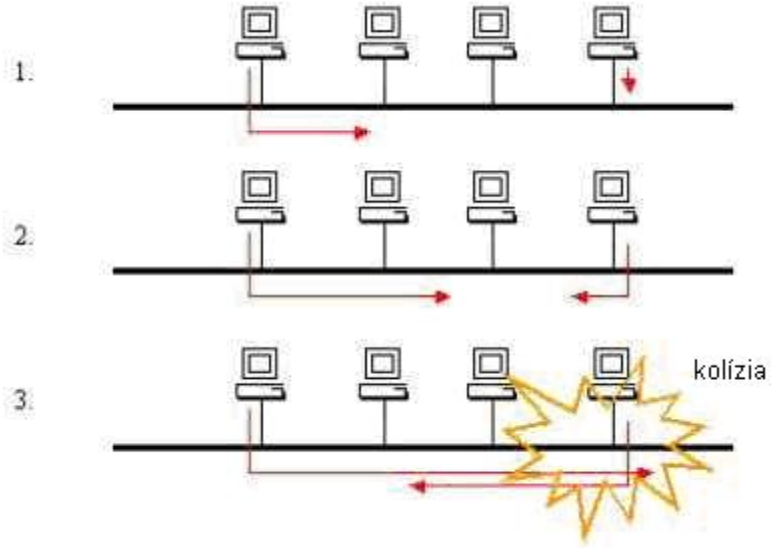
CSMA (Carrier Sense Multiple Access) - stanica pripravená vysielať dáta sleduje, či prenosové médium nepoužíva iná stanica. V prípade, že áno, stanica skúsi pristúpiť neskôr. Ak sa médium uvoľní začne stanica vysielať svoje dáta.



Obrázok č. 6: Metóda CSMA

CD (Collision Detection) – stanica počas vysielania sleduje, či je na médiu signál odpovedajúci vysielaným úrovniam. Prípad, kedy nastane interakcia signálov z viacerých staníc sa nazýva kolízia. V prípade detekcie kolízie stanica generuje signál JAM a všetky

stanice ktoré v danom okamžiku vysielali generujú náhodnou hodnotu času, po ktorej sa pokúsia vysielanie zopakovať.



Obrázok č. 7: Metóda CD

Vďaka tejto jednoduchosti boli dosiahnuté nízke ceny sieťových adaptérov a aktívnych prvkov, čo viedlo k značnému rozšíreniu Ethernetu. Jednoduchosť riešenia avšak priniesla aj jednu významnú nevýhodu – s narastajúcim počtom uzlov narastá aj počet kolízií a tým klesá teoretická priepustnosť siete. Súbor uzlov, ktorých vzájomná činnosť môže vygenerovať kolíziu sa nazýva kolízna doména.

Vedľa výrazu kolízna doména existuje výraz broadcastová doména. V počítačovej sieti sa vyskytujú principiálne dva typy paketov – tzv. unicasty a nonunicasty. Unicasty sú pakety, ktoré majú konkrétneho adresáta vyjadreného regulárnou sieťovou adresou. Nonunicasty používajú skupinovú adresu a sú určené, buď všetkým užívateľom (broadcasty) alebo vybranej skupine (multicasty). Problém je v tom, že nonunicastu sa musí počítač venovať aj keď nie je určený preň. S nárastom počtu uzlov v broadcastovej doméne narastá i množstvo nonunicastov. Z tohto dôvodu je nutné udržať veľkosť broadcastovej domény v rozumnej miere. Používané aktívne prvky majú k broadcastovej doméne rozdielny vzťah a preto ich voľbou sa dá priepustnosť siete ovplyvniť.

Formát paketu

Ako bolo už povedané, všetky rýchlostné modifikácie Ethernetu používajú rovnakú komunikačnú metódu CSMA/CD. Používajú však aj rovnaký formát a veľkosť paketu. Ethernetový paket je definovaný na 1. a 2. vrstve OSI.

Základnou častou paketu je hlavička linkovej vrstvy, ktorú nasledujú dáta (vrátane hlavičiek vyšších vrstiev). Hlavičky sú 4 typov a sú vzájomne nekompatibilné. Tieto typy sú :

- Ethernet_II
- Ethernet_802.3
- Ethernet_802.2
- Ethernet_SNAP

Formát – Ethernet_II.

Preambula	cieľová adresa (DA)	zdrojová adresa (SA)	typ paketu	dáta	CRC
8 byte	6 byte	6 byte	2 byte	46 až 1500 byte	4 byte

Každý paket je začína preambulou, ktorá slúži k synchronizácii vysielacej a prijímacej stanice. Nasleduje cieľová a zdrojová adresa MAC, číslo označujúce typ paketu, dátová časť a kontrolný súčet (CRC).

Používané média

Ethernet je dnes štandardizovaný v týchto verziách:

1. "Klasický" Ethernet s prenosovou kapacitou 10 Mbit/s:

10Base-2

– používa ako prenosové médium tienený koaxiálny kábel označovaný ako Thin Ethernet s impedanciou 50 ohm

- dĺžka segmentu môže byť maximálne 185 m
- na jednom segmentu môže byť maximálne 25 staníc
- segment musí byť na oboch koncoch ukončený pomocou tzv. terminátorov

10Base-5

– používa ako prenosové médium tienený koaxiálny kábel ozn. ako Thick Ethernet s impedanciou 50 ohm

- dĺžka segmentu môže byť maximálne 500 m
- segment musí byť na oboch koncoch ukončený pomocou tzv. terminátorov

10Base-T

– používa ako prenosové médium krútenú dvojlinku s impedanciou 100 ohm (min. Cat 3)
- dĺžka kábla medzi uzlom a aktívnym prvkom môže byť max. 100 m

10Base-FL

- používa ako prenosové médium optický kábel
- dĺžka medzi uzlami môže byť max. 2 km

2. Fast Ethernet s prenosovou kapacitou 100 Mbit/s:

100Base-TX

– používa ako prenosové médium krútenú dvojlinku s impedanciou 100 ohm (min. Cat 5)
– dĺžka kábla medzi uzlom a aktívnym prvkom môže byť max. 100 m

100Base-T4

– používa ako prenosové médium krútenú dvojlinku s impedanciou 100 ohm (min. Cat 3)
– dĺžka kábla medzi uzlom a aktívnym prvkom môže byť max. 100 m
– technológia nie je príliš rozšírená

100Base-FX

- používa ako prenosové médium optický kábel
- dĺžka medzi uzlami môže byť max. 2 km

3. Gigabit Ethernet s prenosovou kapacitou 1000 Mbit/s:

1000Base-SX

- používa ako prenosové médium optický kábel
- dĺžka medzi uzlami a aktívnym prvkom je ovplyvnená parametrami kábla

1000Base-LX

- používa ako prenosové médium optický kábel
- dĺžka medzi uzlami a aktívnym prvkom je ovplyvnená parametrami kábla

2.1.7 Model RM-OSI

Model RM-OSI je referenčný komunikačný model označený skratkou slovného spojenia "Open Systen Interconnection" (Prepojenie otvorených systémov). Je to doporučený

model siete definovaný organizáciou ISO v roku 1983, ktorý rozdeľuje vzájomnú komunikáciu medzi počítačmi do siedmich súvisiacich vrstiev.

Úlohou každej vrstvy je poskytovať služby nasledujúcim vyšším vrstvám a nezaťažovať vyššiu vrstvu detailmi o tom ako je služba v skutočnosti realizovaná. Uvedený model obsahuje nasledujúce vrstvy (každá vyššia vrstva využíva funkcie vrstvy nižšej).

1. Fyzická vrstva

Definuje prostriedky pre komunikáciu s prenosovým médiom a s technickými prostriedkami rozhrania. Ďalej definuje fyzické, elektrické, mechanické a funkčné parametre týkajúce sa fyzického spojenia jednotlivých zariadení. Je hardwarová.

2. Linková vrstva

Zaisťuje integritu toku dát z jedného uzlu siete na druhý. V rámci tejto činnosti je vykonávaná synchronizácia blokov dát a riadenia ich toku. Je hardwarová.

3. Sieťová vrstva

Definuje protokoly pre smerovanie dát, prostredníctvom ktorých je zaistený prenos informácií do požadovaného cieľového uzla.

4. Transportná vrstva

Definuje protokoly pre štruktúrované správy a zabezpečuje bezchybnosť prenosu. Rieši napríklad rozdelenie súboru na pakety a potvrdzovanie.

5. Relačná vrstva

Koordinuje komunikáciu a udržuje reláciu tak dlho, pokiaľ je potrebná. Ďalej zaisťuje zabezpečovacie, prihlasovacie funkcie.

5. Prezentačná vrstva

Špecifikuje spôsob, akým sú dáta formátované, prezentované, transformované a kódované. Rieši napríklad CRC, kompresiu a dekompresiu, šifrovanie dát.

6. Aplikačná vrstva

Je to v modeli najvyššia vrstva. Definuje spôsob, akým komunikujú so sieťou aplikácie, napríklad databázové systémy, elektronická pošta alebo programy pre emuláciu terminálov.

2.1.8 IP adresa

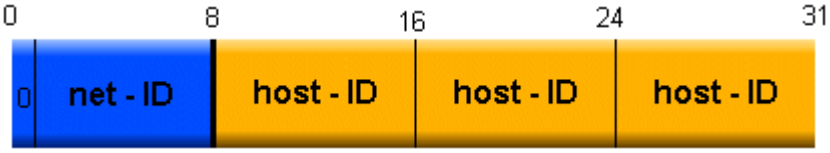
Ak chceme v rámci siete naviazať spojene s iným počítačom, musíme poznať jeho IP adresu. IP adresu musí mať každý počítač inú, pretože inak by nebolo možné rozlíšiť s akým počítačom chceme komunikovať.

IP adresy prideľuje je medzinárodná autorita poverená správou IP adries. V súčasnej dobe sa používa 32 bitová verzia IPv4 a verzia IPv6, ktorá je 128 bitová.

IPv4 adresa má veľkosť 4 byte = 32 bitov. Najčastejšie sa zapisuje v desiatkovej sústave, kde je jednotlivý byte oddelený bodkou. Každý byte môže nadobudnúť hodnotu od 0 - 255.

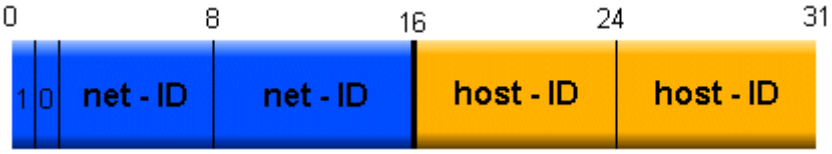
IP adresa sa skladá z dvoch častí net - ID (adresa siete) a host - ID (adresa počítača). Podľa toho ako sú jednotlivé siete rozľahlé rozlišujeme tri hlavné triedy IP adries - **A**, **B** a **C**.

Trieda A



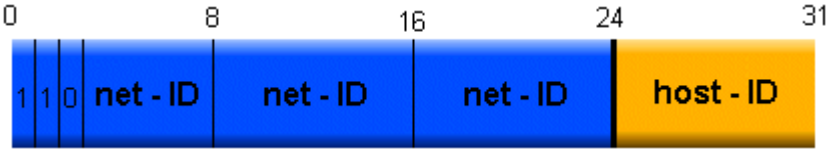
Dovoľuje adresovanie iba 126 sietí, ale v každej z nich maže byť až 16 miliónov počítačov. Rozsah hodnôt IP adries je: 0.0.0.0 až 127.255.255.255.

Trieda B



Trieda B umožňuje adresovať už 16 tisíc sietí a 65 tisíc počítačov v každej z nich. Prvé dva byte je adresa siete a ďalšie dva adresa počítače. Rozsah hodnôt v triede B je: 128.0.0.0 až do 191.255.255.255.

Trieda C



IP adresou triedy C dokážeme adresovať až 2 milióny sietí. V každej môže byť 254 počítačov. Prvé tri byte sú adresou siete a jeden byte adresou počítača. Rozsah je: 192.0.0.0. až 223.255.255.255

Špeciálne IP adresy

Niektoré IP adresy sú vyhradené pre špeciálne účely:

Rozsah od **224.0.0.0** do **239.255.255.255** je zaradený do triedy D. Tato trieda je využívaná pre multicasting.

Rozsah od **240.0.0.0** do **247.255.255.255** patrí do triedy E. Tieto hodnoty sú rezervované pre ďalšie použitie a pre experimentálne účely.

127.0.0.0 nebo **127.0.0.1** sú určené k testovacím účelom. Nazývajú sa tiež loopback adresy.

Broadcast adresa, **255.255.255.255** je určená všetkým počítačom v danej sieti. Používajú sa k hromadnému rozosielaniu paketov.

2.1.9 Aktívne prvky

Podľa počtu uzlov použitých v počítačovej sieti a v závislosti na jej topológii by mali byť volené aktívne prvky. V LAN sieťach sú používané nasledujúce typy aktívnych prvkov.

1. vrstva – fyzická vrstva

Opakovač (repeater) a **Rozbočovač** (hub) – aktívny prvok zaisťujúci spojenie dvoch a viacerých segmentov siete tím, že signál obdŕžaný na jednom porte zopakuje do ostatných portov, pričom signálu obnoví ostré vzostupné a zostupné hrany; rozširuje kolíznu i broadcastovú doménu.

Prevodník (Media Converter) – zariadenie, ktoré zaisťuje konverziu signálu z jedného typu média na iné

2. vrstva – linková vrstva

Most (bridge) – dvojportové zariadenie ktoré oddeľuje prevádzku na dvoch segmentoch siete na základe učenia fyzických (MAC) adries uzlov na oboch portoch. Na základe týchto adries most buď dáta na druhou stranu prepustí alebo neprepustí; most pracuje na druhej vrstve modelu OSI (linková vrstva) a preto je nezávislý od protokolu, ale je závislý na použitej sieťovej technológii. Most oddeľuje kolíznu doménu, ale rozširuje broadcastovú doménu; filtračná schopnosť sa vzťahuje len na Unicast pakety.

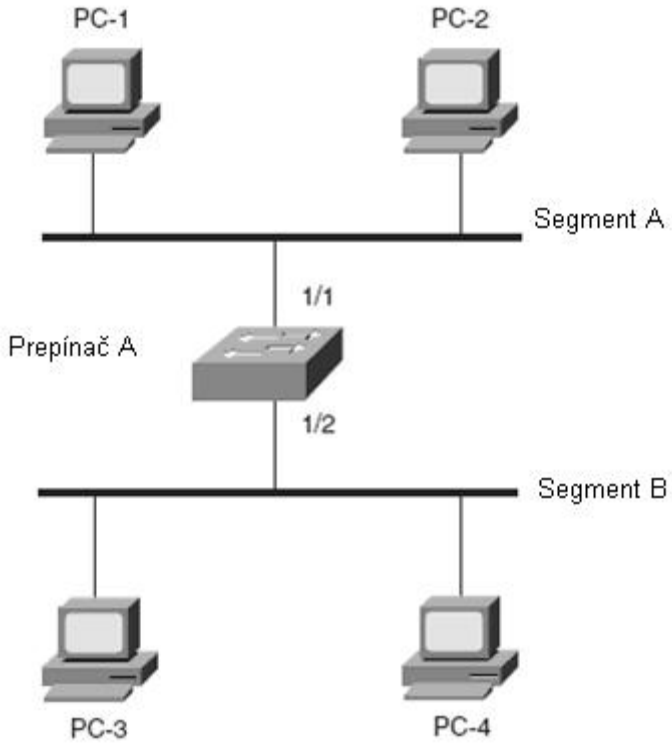
Prepínač (switch) – vysokorýchlostný multiportový most ktorý umožňuje:
– paralelnú komunikáciu medzi portami (tzn. napr. dvojice portov 2-3, 5-9, 6-4, … môžu komunikovať súčasne)
– popri štandardnej polovične duplexnej prevádzke prináša teoreticky dvakrát rýchlejší plne duplexní prenos

Prepínač oddeľuje kolíznu domény, ale rozširuje broadcastovú doménu.

2.1.10 Mechanizmus STP

Veľké siete nie sú navrhované len aby rýchlo a efektívne prenášali rámce alebo pakety, ale musia zvažovať ako sa rýchlo zotaviť z prípadnej chyby v sieti. Na tretej vrstve si smerovacie protokoly uchovávajú v tabuľke nadbytočné cesty do cieľovej siete, a tak sa môžu rýchlo zotaviť z poruchy, ak na primárnej ceste nastane chyba. Smerovanie tiež umožňuje využívať viaceré cesty, a tým rozdeľovať zaťaženie. Na druhej vrstve sa však žiadne smerovacie protokoly nepoužívajú a nadbytočné linkové spojenia nie sú dovolené, preto sa na druhej vrstve využíva „The Spanning-Tree Protocol“ (STP, protokol vetviaceho sa stromu), ktorý poskytuje nadbytočné linky a vyváženie záťaže, a tak sa môže zotaviť z poruchy bez včasného zásahu.

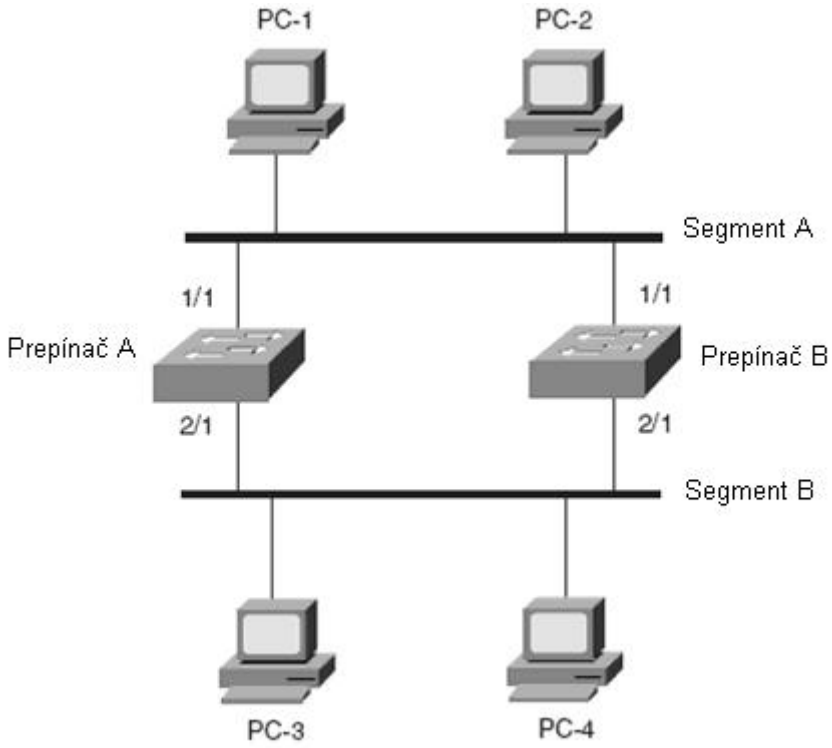
Na obrázku č. 8 je znázornená jednoduchá sieť, kde prepínač funguje ako most. Táto sieť ale neposkytuje žiadne nadbytočné linky a v prípade, ak by prepínač alebo jedna z jeho liniek zlyhala, bola by sieť nefunkčná.



Obrázok č. 8: Sieť s jedným prepínačom

Spoľahlivosť a odolnosť siete môžeme zvýšiť pridaním viacero liniek a ďalšieho prepínača, ako vidíme na obrázku č. 9. Ale z dôvodu, že o sebe prepínače nevedia, vznikajú

tzv. „*bridging loop*“ (premosťovacie slučky), kedy duplikujú rámce a preposielajú si ich stále medzi sebou.



Obrázok č. 9: Sieť s dvomi prepínačmi

Riešením tohto problému je fyzické prerušenie liniek a vypnutie prepínača alebo použitie STP protokolu, ktorý zabraňuje vytvoreniu týchto slučiek, a tým môžeme využívať výhody nadbytočných liniek a prepínačov v sieti.

Pomocou STP protokolu prepínače medzi sebou komunikujú, vyjednávajú medzi sebou bezslučkové cesty do jednotlivých segmentov v sieti. Slučky sú objavené skôr ako sú cez linky vysielané dáta a nadbytočné linky sú vypnuté. V prípade zlyhania jednej linky, prepínač pohotovo zareaguje a zapne jej záložnú (nadbytočnú) linku.

Vďaka STP komunikujú všetky prepínače zapojené v sieti a na základe informácií, ktoré si medzi sebou vymieňajú, každý prepínač vykonáva „Spanning-Tree“ algoritmus. Algoritmus zvolí referenčný bod v sieti a k nemu vypočítava cenu cesty každej linky. Ak algoritmus nájde nadbytočné linky, cez jednu posiela rámce a druhú vypne. Algoritmus spája prepínače do stromovej štruktúry a zabraňuje tak vytváraniu slučiek. Ak jedna z aktívnych liniek zlyhá, prepočíta sa celý strom znova, aby mohla byť jedna nadbytočná linka aktivovaná.

Spanning Tree algoritmus a protokol 802.1D

Komunikácia

Prepínače komunikujú medzi sebou a vymieňajú si dáta pomocou *Bridge Protocol Data Units (BPDUs, dátová jednotka prepínacieho protokolu).* Prepínač vysiela BPDU rámec cez každý port, kde zdrojová MAC adresa je jedinečná MAC adresa portu a cieľová adresa je multicastová adresa 01-80-c2-00-00-00, na ktorej počúvajú všetky prepínače v sieti.

Existujú dva typy BPDU:

- Konfiguračná BPDU, ktorá slúži na výpočet stromu,
- TCN (*Topology Change Notification, oznámenie zmeny topológie)* BPDU, ktorou sa upozorňuje na zmenu topológie siete

Cieľom výmeny BPDU je vytvorenie jednotného a stabilného stromu topológie. Konfiguračné BPDU obsahujú informácie o identifikácii prepínača, cenu cesty a nastavenia časovačov. Všetky tieto údaje sa používajú pri výpočte všeobecného stromu a zvolenia referenčného bodu v sieti tzv. *Root Bridge (koreňový prepínač).*

Popis	Veľkosť v bajtoch
ID protokolu	2
Verzia	1
Typ správy	1
Príznak	1
ID koreňového prepínača	8
Cena cesty ku koreňu	4
ID odosielateľa (prepínača)	8
ID portu na prepínači	2
Vek správy	2
Maximálny vek správy	2
Interval vysielania BPDU	2
Oneskorenie	2

Tabuľka č. 1: Obsah konfiguračného BPDU

Voľba koreňového prepínača

Aby sa všetky prepínače v sieti dohodli na bezslučkovej typológii, musia si zvoliť referenčný bod v sieti. Na voľbe tohto bodu sa podieľajú všetky pripojené prepínače. Každý prepínač má svoje jedinečné identifikačné číslo – ID, ktorého veľkosť je dva bajty a pozostáva z nasledujúcich častí:

• **Priorita prepínača (2 bajty) -** môže nadobúdať hodnotu od 0 do 65 535. Prednastavená hodnota je 32 768.

• **MAC Adresa (6 bajty) –** jedinečná adresa prepínača

Na začiatku, pri zapnutí prepínača, nevie nič o okolitých prepínačoch a za koreňový prepínač si zvolí sám seba. Voľba prebieha nasledovne:

- Každý prepínač vysiela BPDU, kde ID koreňového prepínača a ID odosielateľa je jeho vlastné ID.
- Prijaté BPDU ja analyzované a ak hodnota ID koreňového prepínača je menšia ako jeho aktuálna, nahradí svoju vlastnú hodnotu ID koreňového prepínača prijatou.
- Prepínač opäť preposiela BPDU, ale už so zmenenou hodnotou ID koreňového prepínača.
- Prepínače sa skôr či neskôr dohodnú a za referenčný bod siete si zvolia prepínač s najnižšou prioritou.

Voľba koreňového prepínača je pretrvávajúci proces, ktorý sa spúšťa zmenou ID koreňového prepínača každé dve sekundy.

Voľba koreňových portov

Po voľbe koreňového prepínača musí každý prepínač definovať svoj vzťah k nemu. Tento proces sa tiež nazýva voľba koreňového portu. Tento port sa vyberá na základe najmenšej ceny cesty ku koreňu. Cenu cesty tvorí súčet cien jednotlivých liniek, ktoré vedú ku koreňu stromu. Jej predvolené hodnoty sú vypísané v tabuľke č. 2. Všeobecne platí, čím väčšia priepustnosť linky, tým je menšia jej cena. Pôvodná norma IEEE 802.1D definovala cenu cesty ako podiel 1000 Mbps / priepustnosť linky v Mbps, ale z dôvodu rozvoja

moderných technológií a používania gigabitového ethernetu zaviedla IEEE novú nelineárnu škálu pre cenu cesty. Porovnanie je znázornenie v tabuľke č. 2.

Priepustnosť linky	Stará norma	Nová norma
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

Tabuľka č. 2: Cena cesty

Voľba portov na posielanie dát

V tomto stave sú zatiaľ všetky linky aktívne a STP algoritmus musí zvoliť jeden port na posielanie dát pre každý segment siete tzv. *Designated Port*. Algoritmus vyberá port na základe najmenšej ceny cesty ku koreňovému prepínaču. Ak má susediaci prepínač na zdieľanom segmente siete rovnakú cenu cesty, berie sa ďalej do úvahy najnižšie ID prepínača na segmente a potom najmenšie ID portu prepínača.

Typy časovačov

STP protokol používa tri typy časovačov, aby sa uistil, že strom bol vytvorený správne a nevznikli žiadne slučky

• „**Hello Time“** – Interval posielania konfiguračných BPDU
• „**Forward Delay“ –** Čas, ktorý strávi port v stavoch počúvajúci a učiaci. Predvolená hodnota je 15 sekúnd.

• „**Maximum (max) Age“ –** Čas, ako dlho prepínač udržiava informácie o prijatom BPDU v pamäti. Po uplynutí tejto doby , prepínač informuje o zmene topológie v sieti. Predvolená hodnota je 20 sekúnd.

Tieto hodnoty môžu byť zmenené len na koreňovom prepínači a sú ďalej preposielané pomocou konfiguračných BPDU. Takto sa zaisťuje jednotná hodnota časovačov v celej sieti.

Zmena topológie

Ak nastane zmena v topológii, prepínač, ktorý túto zmenu zistí, posiela cez koreňové porty TCN BPDU, pokiaľ nedostane potvrdenie od koreňového prepínača. Ten nastaví v nasledujúcich správach príznak o zmene v topológii. Každý prepínač, ktorý prijme taký príznak, skráti čas uloženia MAC adries vo svojej tabuľke z 300 sekúnd na 15. Vďaka tomu, zostávajú prepínacie tabuľky aktuálne, lebo v nej zostanú len aktívne stanice.

Popis	Veľkosť v bajtoch
ID protokolu	2
Verzia	1
Typ správy	1

Tabuľka č. 3: Obsah TCN BPDU

Stav portu

V procese výpočtu stromu, musí každý port prechádzať niekoľkými stavmi aby sa stal aktívnym a mohol preposielať dáta. Protokol definuje nesledujúce stavy:

Blokujúci

Po inicializácii portu, sa nachádza port v blokujúcom stave, a preto nemôžu vznikať žiadne prepínacie slučky. V tomto stave port nemôže prijímať, vysielať dáta a ani vytvárať prepínaciu tabuľku na základe prijatých rámcov. Portu je dovolené len prijímať BPDU rámce od susediacich prepínačov.

Počúvajúci

Port prechádza do tohto stavu ak ho prepínač môže určiť za koreňový port alebo port na posielanie dát. V tomto stave port stále nemôže posielať a prijímať dátové rámce, ale má dovolené prijímať a posielať BPDU, a tak sa aktívne zúčastniť na tvorbe stromu topológie. Až teraz sa určuje, či daný port bude prenášať dáta alebo sa vráti späť do blokujúceho stavu.

Učiaci

Po čase strávenom v stavoch blokujúci a počúvajúci, ktorý určuje časovač „Forward Delay“, môže prejsť do stavu učiaci. V tomto stave si tvorí MAC tabuľku pre daný port.

Preposielajúci

Po ďalšom čase „Forward Delay“ port môže preposielať dátové rámce, tvorí MAC tabuľku a prijíma a posiela BPDU. Port je teraz plne funkčný v rámci topológie

3. vrstva – sieťová vrstva

Smerovač (router) – je to dva a viac portové zariadenie, ktoré pracuje na podobnom princípe ako prepínač, ale na tretej vrstve modelu OSI – pracuje teda s logickými adresami a je protokolovo závislý, ale relatívne nezávislý na použitej sitovej technológii (pre každú technológiu musí mať patričný adaptér). Smerovače sú v LAN sieťach používané prevažné pre oddelenie broadcastových domén – túto oblasť však opúšťajú lebo začínajú byť nahradzované smerovacími prepínačmi. Vedľa použitia v sieťach LAN, našli smerovače dôležité uplatnenie vo WAN sieťach, kde sú používané pre prepojovanie vzdialených lokalít

Prepínač pracuje s jednou tabuľkou a to s tabuľkou, kde sú relácie medzi MAC adresou a portom zariadenia. Smerovač pracuje s dvomi tabuľkami. V prvej je relácia medzi MAC adresou, logickou adresou a portom (tabuľka obsahuje údaje iba o priamo pripojených uzloch). V druhej tabuľke je zoznam sietí (častí logických adries) s portom kadiaľ vedie najlepšia cesta do danej siete.

Smerovací prepínač (routing switch) – je to relatívne nové zariadenie, ktoré pracuje s rýchlosťami obvyklými pre druhú vrstvu i s informáciami tretej vrstvy.

2.1.11 Základy smerovania v IP prostredí

Stanice v rámci jednej logickej siete komunikujú priamo (s použitím mechanizmu ARP). Pokiaľ však chce komunikovať stanica z jednej siete (napr. 192.168.1.x) s uzlom z inej siete (napr. 192.168.2.x), je potrebné siete prepojiť zariadením pracujúcim na 3. vrstve OSI.

Smerovače si udržiavajú prehľad o tom, na ktorom porte je aká sieť. Tieto informácie sú do zariadenia zadávané staticky alebo je používaný určitý mechanizmus pre ich dynamickú výmenu. Dynamických smerovacích protokolov je pomerne veľa napr. RIP, IGRP EIGRP, OSPF, BGP, EGP, ...

V závislosti na implementácii môžu byť súčasťou smerovacej tabuľky i masky cieľových sietí a typ protokolu, pomocou ktorého sa smerovač o sieti dozvedel.

Smerovacie protokoly

RIP

Smerovací protokol, ktorý využíva DVA algoritmus a ako metriku cesty používa počet skokov. Slúži na smerovanie v rámci autonómneho systému. RIP si vymieňa aktualizácie v pravidelných intervaloch a ak nastane zmena v sieti.

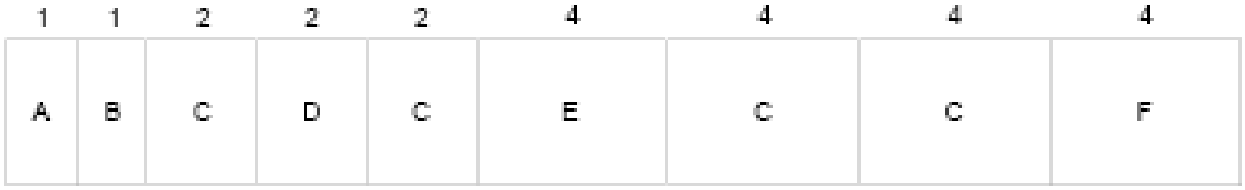
Metrika

Ak prijatá aktualizácia obsahuje nové informácie o novej ceste, priradí ju do svojej tabuľky a zahrnie ju do svojich aktualizácii, pričom jej zvýši metriku o jedna. Ako adresa ďalšieho skoku sa použije IP adresa odosielateľa danej aktualizácie. RIP uchováva len cestu s najlepšou metrikou do danej siete. Rip využíva počet skokov na meranie vzdialenosti medzi zdrojovou a cieľovou sieťou. Každý smerovač na ceste od zdroja k cieľu má priradenú hodnotu skoku, ktorá je väčšinou 1. Aby sa RIP vyhol smerovacím slučkám, používa maximálny počet skokov 15. Ak po zvýšení metriky je hodnota 16, označí danú sieť za nedosiahnuteľnú.

RIP vo všeobecnosti posiela aktualizácie každých 30 sekúnd. Každá cesta má svoj časovač, ktorý ak uplynie, vyhlási ju za nedosiahnuteľnú.

Formát paketu

RIP je enkapsulovaný v IP protokole. Jeho formát je zobrazený na obrázku č. .



Obrázok č. 10: Formát dátovej časti IP - RIP paketu

A – požiadavka / odpoveď, určuje typ správy.
B – verzia
C – nevyužíva sa
D – obsahuje informácie o smerovanom protokole, pre IP má hodnotu 2
E – IP adresa
D – metrika danej adresy

RIP podporuje „load balancing“ až cez 6 ciest s rovnakou metrikou. Prednastavené je použitie 4 ciest a ich výber sa vykonáva na základe algoritmu „round robin“.

RIP v1 má nasledujúce obmedzenia:

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

IGRP

Smerovací protokol vyvinutý firmou CISCO. Využíva DVA algoritmus, každému susediacemu smerovaču posiela celú a lebo časť svojej smerovacej tabuľky. Pri výpočte metriky zohľadňuje priepustnosť, záťaž, oneskorenie a spoľahlivosť linky, pričom správca siete môže určiť váhu jednotlivých parametrov. Metrika nadobúda hodnoty od 1 po 255. Slúži na smerovanie v rámci autonómneho systému.

Aktualizácie sa posielajú broadcastom každých 90 sekúnd

OSPF

- Ide o beztriedny smerovací protokol vnorený do IP protokolu
- Používa sa na IGP (Interior gateway protocol) smerovanie v rámci jedného autonómneho systému (AS)
- Veľké prepojovacie siete umožňuje rozdeliť do viacerých samostatných AS pripojených na chrbticový AS (zníženie záťaže smerovačov a prenosu medzi nimi)
- Na určenie cesty využíva metódu LSA (Link State Algorithm)
- Výberové kritériá: oneskorenie, priepustnosť, pripojiteľnosť
- Smerovaciu tabuľku generuje pomocou Dijkstrovho algoritmu

Smerovače používajúce OSPF smerovací protokol môžeme rozdeliť do 4 kategórií:

- Internal router – smerovač vnútri AS
- Area border router – smerovač na hranici AS a chrbticového AS
- Backbone router – smerovač patriaci iba do chrbticového AS
- AS boundary router – router vnútri AS, ktorý zdieľa smerovacie informácie s inými smerovačmi v iných AS

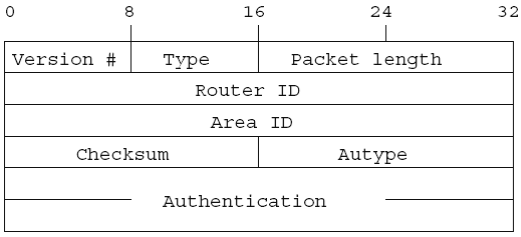
Vlastnosti smerovačov:

- V každej oblasti je jeden určený DR (designated router) prípadne jeden záložný BDR (backup DR), ktoré sa určia pre každý AS automaticky na základe vyššej priority a vyššieho ID routra (ID je vlastne IP adresa routra v AS)
- DR a BDR je logicky priľahlý ku všetkým smerovačom v rámci AS, ale vo všeobecnosti priľahlý smerovač je iba priamo susediaci smerovač
- Každý smerovač má jednu tabuľku priľahlých smerovačov a jednu smerovaciu tabuľku, ale area border router a AS boundary router má pre každý AS má samostatné pre každý AS. Každý si ešte udržiava vlastnú tabuľku (LSD) opisujúcu topológiu AS.
- Informácie medzi smerovačmi sa šíria hromadne záplavou „flood“ pomocou multicast adries (adresou 224.0.0.5 medzi priľahlými smerovačmi a adresou 224.0.0.6 medzi DR a BDR smerovačmi)
- OSPF protokol implementuje 5 typov paketov:
  - HELLO pakety
  - DDP pakety – Database Description packet
  - LSR – Link State Request

- LSU – Link State Update
- LSAck – Link State Acknowledge

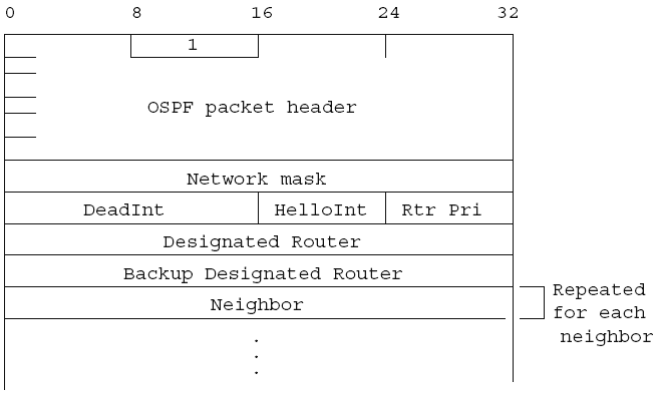
Pakety OSPF protokolu:

Pakety protokolu sú zapuzdrené do IP protokolu (pole protokol IP protokolu obsahuje hodnotu 89). Hello pakety sa slúžia na objavovanie a udržiavanie spojenia so susedmi. DDR a LSR pakety sa používajú na formovanie priľahlostí. LSU a LSAck pakety zabezpečujú obnovu LSD databázy. Každý LSU paket nesie niekoľko nových LSA (Link State Advertisements) informácií o jeden skok ďalej od ich bodu vzniku. Každá LSA obsahuje identifikátor smerovača, ktorý ju vytvoril a kontrolnú sumu. Všetky typy protokolu majú rovnaký formát hlavičky. Jeho podobu môžeme vidieť na nasledujúcom obrázku.

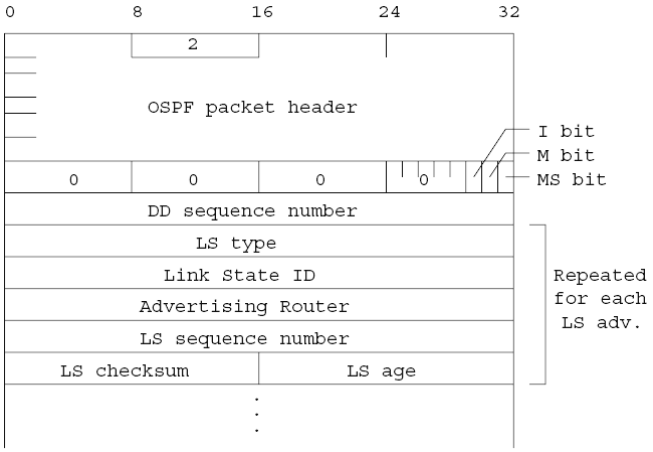


Obrázok č. 11: Formát hlavičky OSPF paketu

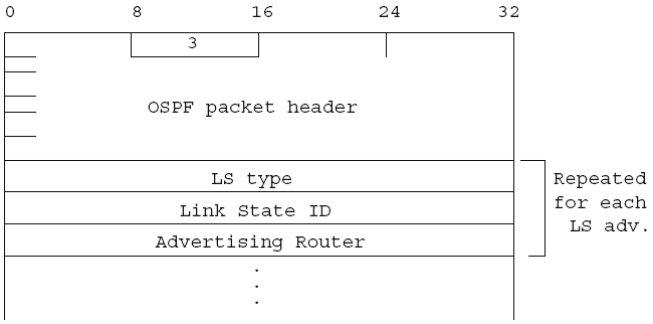
Jednotlivé typy OSPF paketu sa rozlišujú na základe poľa Type v spoločnej hlavičke. Podrobný formát zvyšných častí OSPF paketu je možné vidieť na nasledujúcich obrázkoch. Popis jednotlivých polí, ako aj ostatné informácie je možné získať z RFC dokumentácie OSPF protokolu (RFC 1131).



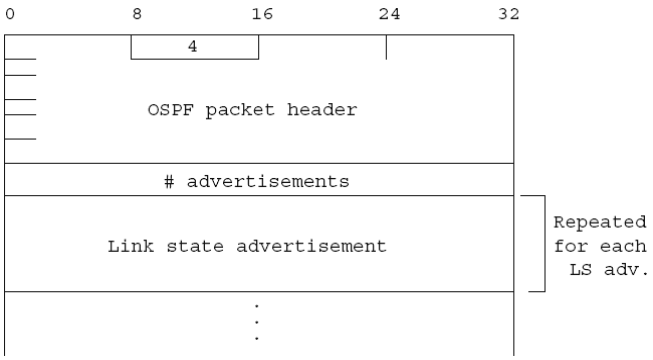
Obrázok č. 12: Formát HELLO paketu



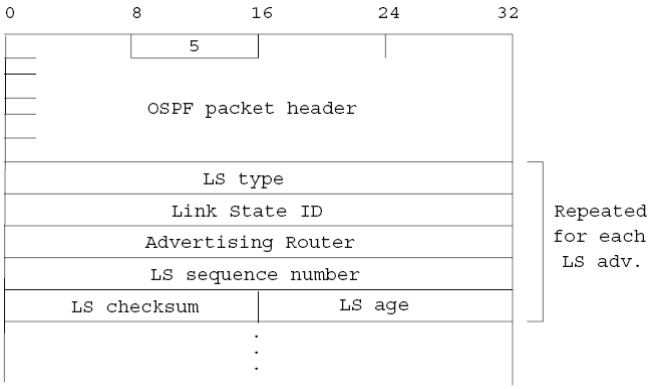
Obrázok č. 13: Formát DDR paketu



Obrázok č. 14: Formát LSR paketu



Obrázok č. 15: **Formát LSU paketu**



Obrázok č. 16: **Formát LSAck paketu**

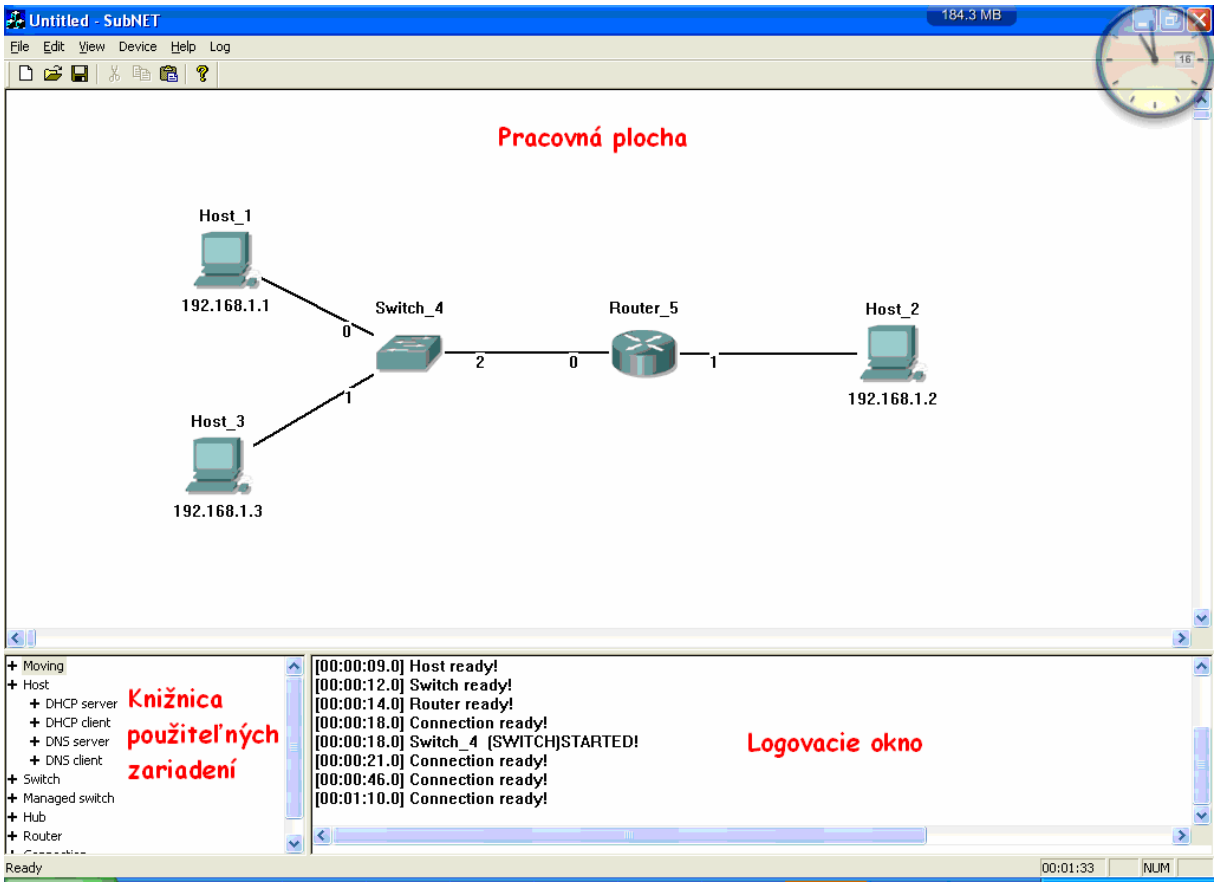
2.2 Analýza konkurenčných produktov

Pri príprave na projekt sme sa nevyhli ani štúdiu už existujúcich riešení. Jednalo sa o riešenie od tímu, ktorý riešil podobný problém minulý rok na predmete Tímový projekt na FIIT STU, ako aj o riešenia od komerčných subjektov.

2.2.1 SUBNET

SUBNET je výtvorom tímu, ktorého zadanie projektu bolo totožné s našim. Aplikácia je použiteľná pre výukový proces a pre simuláciu počítačovej siete.

2.2.1.1 Používateľské rozhranie



Obrázok č. 17: Používateľské rozhranie tímu SubNet

Na prvý pohľad je aplikácia používateľsky príjemná, avšak počas práce s ňou sa vyskytujú určité nedostatky:

Pre vytváranie topológie je na ľavej časti obrazovky strom, ktorý obsahuje jednotlivé prvky siete. Veľkosť tohto stromu je nedostatočná a je nutné ho posúvať, čo spomaľuje tvorbu topológie.

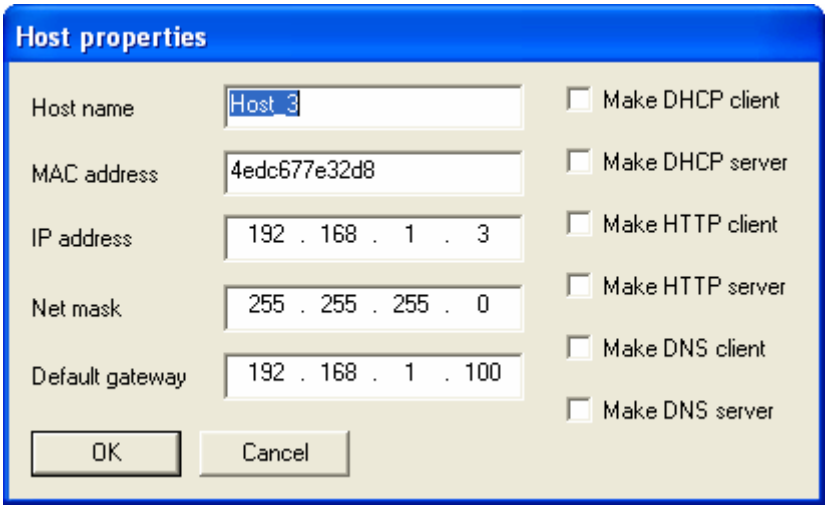
Rýchlosť kreslenia stromu siete je obmedzená a po pridaní nejakého prvku siete je nutné čakať asi 1 sekundu, kým je možné pridať ďalší prvok (dôvod je popísaný v časti implementácia).

Aplikácia umožňuje pridávanie rôznych typov sieťových zariadení ako opakovač, prepínač, smerovač a linkové spojenie. Umožňuje tiež vytvárať užívateľské prvky siete odvodené od základných prvkov a tiež ukladanie a načítanie topológie do / zo súboru.

Klady a zápory jednotlivých prvkov siete:

Connection : + Dá sa spustiť „Sniffer“ na každom spojení
– Neumožňuje žiadne nastavenia pre dané spojenie
– Nedá sa spustiť na dvoch a viacerých spojeniach súčasne

Host: + Každý host má konzolu, kde si môžeme otestovať základné príkazy: ping, ipconfig, arp, tracert
– Možnosti DHCP klient server, DNS klient server, HTTP klient server boli nefunkčné a spôsobovali pád aplikácie



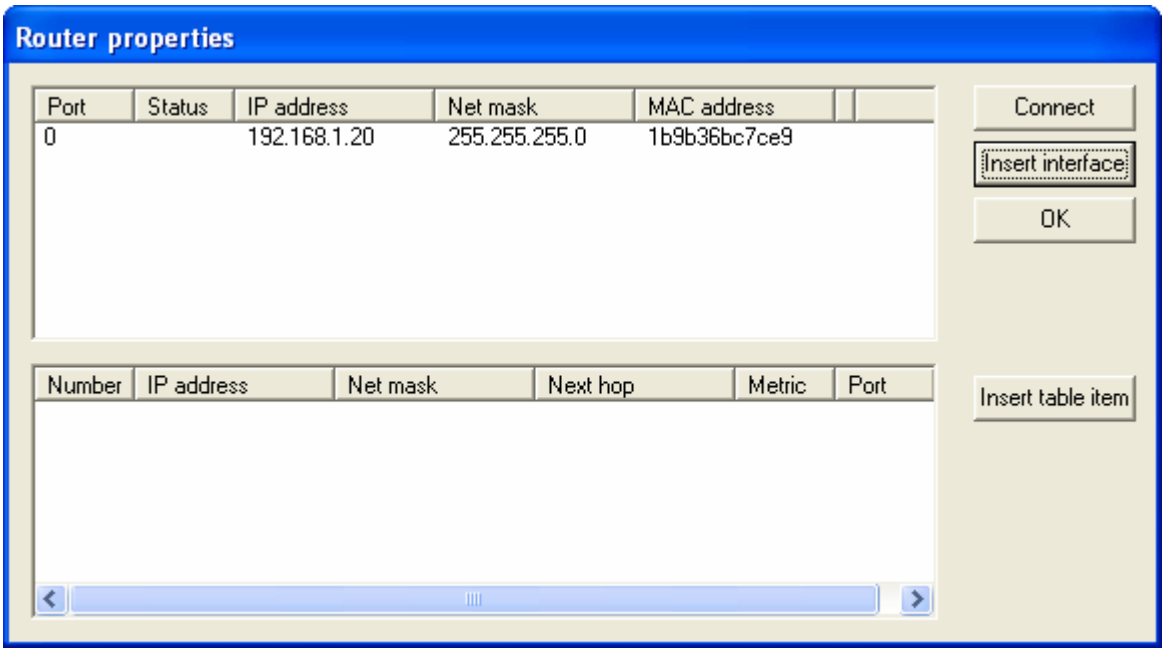
Obrázok č. 18: Nastavenie stanice

Switch: – Možnosť nastavenia len MAC adresy, žiadny rozdiel medzi manažovateľným a obyčajným switchom
– Nedokážu zobraziť tabuľku MAC adries a portov

Router: + Dá sa zmeniť metrika ale vzhľadom na RIP je to zbytočné
+ Príkazy konzoly: enable, helo, ping, show (history, route), tracert
– Nutnosť manuálneho pridania interfejsu s MAC, IP, maskou, portom

– Smerovacia tabuľka je len statická

– Čo sa raz vytvorí, nedá sa odstrániť (položka smerovacej tabuľky, interfejs)



Obrázok č. 19: Nastavenie smerovacej tabuľky smerovača

Použité protokoly:

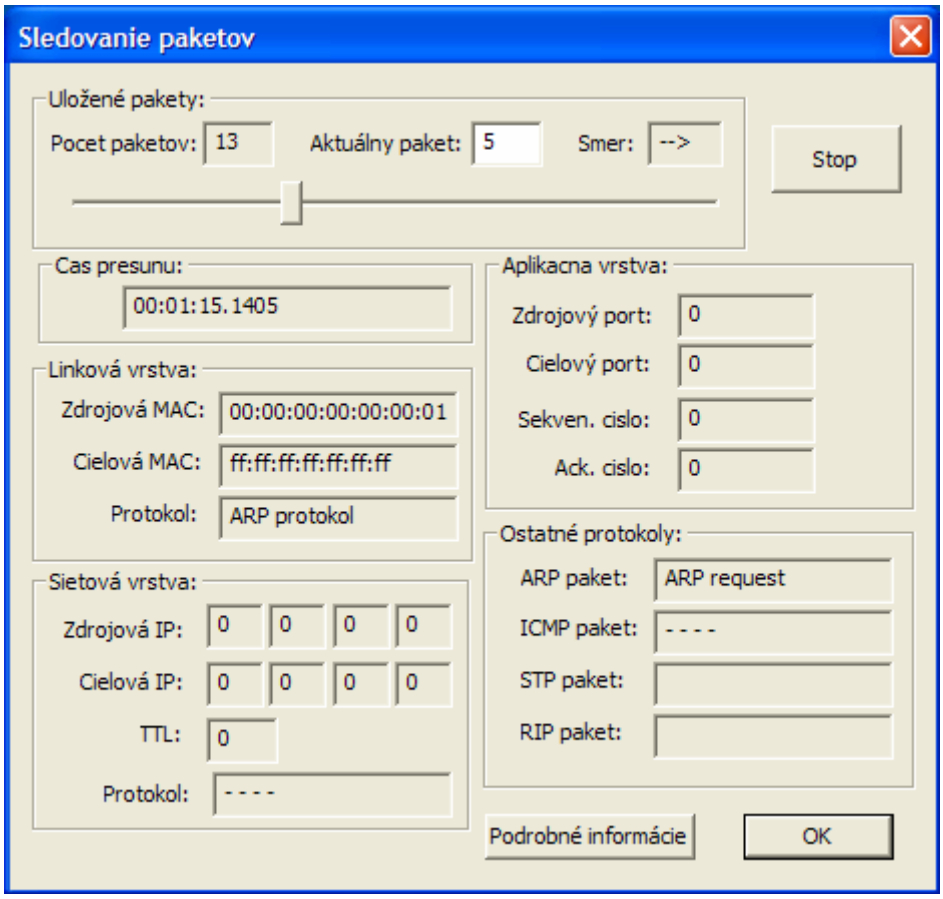
STP	-	nefunkčné
ARP	+	funkčné
ICMP	+	funkčné
RIP	-	nie celkom funkčné

Konzola:

Na každom zariadení je možné spustiť konzolu s príkazovým riadkom, kde je možné zadávať vopred definované príkazy. Vzhľadom na to že niektoré funkcie aplikácie nie sú funkčné, tak ani tieto príkazy konzola nerozoznáva.

Ďalšie vlastnosti:

V analyzátore paketov sa pri icmp paketoch nezobrazuje zdrojová a cieľová IP adresa. Pri vytvorení viacerých spojení medzi dvomi rovnakými zariadeniami nie je vidieť, či to predchádzajúce spojenie sa odstránilo alebo ostalo zapojené. Aplikácia neumožňuje zobrazovanie akýchkoľvek štatistík.



Obrázok č. 20: Analyzátor paketov

Pretože sme sa rozhodli pokračovať v zdokonaľovaní tejto aplikácie, ktorej základ tvorí silný a prepracovaný model simulovania siete, uvádzame analýzu implementačnej časti tejto aplikácie.

2.2.1.2 Analýza Implementácie

Použité knižnice

Tvorcovia tohto programu použili knižnicu TINY na modelovanie procesných udalostí. Táto knižnica obsahuje rôzne generátory náhodných čísel. Umožňuje výpisy štatistík a má v sebe implementované rôzne typy dátových zásobníkov ako FIFO rady a obslužné miesta.

Táto knižnica je primárne určená na modelovanie systémov pomocou udalostí avšak disponuje aj podporou procesného modelovania. V plnej miere implementuje model simulačného času ako aj programátorské rozhranie (API) v jazyku C++. Je použiteľná na platforme UNIX aj MS Windows. Disponuje aj generátormi náhodných čísel s rôznym typom

rozdelení, ktoré autori použili na implementáciu stochastických udalostí (chyby pri prenose). Ďalej umožňuje zbierať z odsimulovaného systému rôzne štatistické údaje, potrebné pre ďalšiu analýzu správania sa systému.

Na implementovanie CLI využívajú autori knižnicu Readline. Táto umožňuje programátorom vytvárať funkcie na dopĺňanie ľubovoľných informácií nielen názvov súborov. Knižnica Readline obsahuje viaceré funkcie, ktoré boli pre tento projekt potrebné. Zahŕňa prácu s rôznymi terminálmi, nízko úrovňovú správu prijímaných znakov a umožňuje programátorovi vytvárať" vlastné funkcie na doplňovanie príkazov a prácu s históriou príkazov.
Túto knižnicu autor využil na :

- vytvorenie' funkcie na doplňovanie príkazov,
- kontextovú nápovedu a prácu s históriou.

Vo všeobecnosti knižnica Readline ponúka sadu príkazov pre manipuláciu s textom, ktorý je vpísaný do príkazového riadku, umožňujúc jeho opravu v prípade chyby, namiesto celého prepísania riadku.

V knižnici sú implementované funkcie pre:

- pohyb po riadku – k týmto príkazom patria aj prislúchajúce klávesové skratky. Napr. presun na začiatok riadku – Ctrl + a. Presun na koniec riadku – Ctrl + e atď.
- tzv. killing príkazy – tie umožňujú zmazanie textu z riadku s tým, že sa uloží a neskôr môže opäť vložiť. Čiže metóda – copy paste. Taktiež sú nadefinované klávesové skratky napr. Ctrl+k znamená kopírovanie a Ctrl + y je vloženie textu.
- príkazy pre hľadanie histórie
- príkazy pre menenie textu
- príkazy pre dopĺňanie – pomocou tlačidla TAB
- je možné posielať do príkazov numerické argumenty, ktoré špecifikujú zopakovanie príkazu
- vytvorenie tzv. inicializačného súboru, ktorým sa nadefinujú určité vlastnosti správania sa knižnice

Triedy

Kvôli prehľadu použitých tried uvádzame diagram tried, z ktorého budeme vychádzať. Z diagramu je vidieť, že boli implementované knižnice pre prácu s protokolmi Ethernet, IP, ARP, ICMP, UDP, TCP smerovací protokol RIP a protokol STP.

Sú to triedy :

C_Protocol - abstraktná trieda, zahrňuje potrebné atribúty a metódy pre všetky protokoly

C_ProtSTP - umožní používanie spanning-tree algoritmu pre switch-e

C_ProtIP - trieda zabezpečujúca komunikáciu pomocou IP protokolu

C_ProtICMP - trieda zabezpečujúca komunikáciu pre službu ping

C_ProtRIP - každý router môže túto triedu používať na realizáciu RIP protokolu

C_ProtARP - trieda, pomocou ktorej je možné používať ARP protokol

C_ProtTCP - trieda zabezpečujúca komunikáciu pomocou TCP protokolu

C_ProtUDP - trieda zabezpečujúca komunikáciu pomocou UDP protokolu

C_Packet - trieda ktorá definuje paket, jeho dĺžku a dáta

C_ProtEthernet - objekt protokolu ethernet poskytuje rozhranie pre prácu s ethernetovým rámcom

V týchto triedach sú implementované metódy pre jednoduchú prácu s paketmi jednotlivých protokolov, pre získavanie konkrétnych dát z týchto paketov a pre vytváranie paketov s konkrétnymi dátami a parametrami. Veľmi dobre je implementované vytváranie rámcov od horných vrstiev k nižším a tiež naopak.

Pre zariadenia boli navrhnuté tieto triedy:

C_ArpCache - objekt C_ArpCache poskytuje metódy pre prácu s tabuľkou Arp

C_CPU - objekt spracovania - facility

C_Device - všeobecná trieda pre zariadenia:

C_Host

C_Hub

C_Router

C_ManagedSwitch

C_Switch

Zariadenia odvodené od všeobecnej triedy **C_Device**. Každé zariadenie má svoje konkrétne parametre ako počet portov, interfejsov ,svoje obslužné miesto **CFacilty** a svoje služby. Obslužné miesto je proces, ktorý je budený iným procesom, napríklad procesom z interfejsu ak naň prišli nejaké pakety. Tento zobudený proces potom môže napr. vybrať všetky pakety z interfejsov, ktoré mali niečo vo vstupných FIFO radoch svojich potov a poslať ich po spracovaní na iné interfesjsi (výstupné FIFO rady portov pre dané interfejsi).

C_Interface - všeobecná trieda pre rozhranie na niektorom zariadení :

C_InterfaceHost

C_InterfaceHub

C_InterfaceMSwitch

C_InterfaceRouter

C_InterfaceSwitch

Každé zariadenie má svoj vlastný typ interfejsu odvodený od jedného typu C_Interface. Interfejs má svoj port CPort, svoje vlastné obslužné miesto CFacility, ktoré vykonáva určitú činnosť ak do vstupných FIFO radov jeho portov prišli nejaké pakety. (Napr. zobudí obslužný proces zariadenia). Každý interfejs má tiež FIFO rad pre pakety prichádzajúce z IP vrstvy.

C_Port - miesto pre pripojenie spojenia

C_RouteTable - poskytuje metódy pre prácu so smerovacou tabuľkou

Príkazy pre konzolu:

C_Tracert

C_Ping

Pre služby boli navrhnuté tieto triedy:

C_AppService - všeobecná trieda pre aplikačné služby

C_Service - všeobecná trieda pre služby:

C_ServiceDHCP

C_ServiceDNS

C_ServiceHTTP

C_ServiceICMP

C_ServiceIPHost

C_ServiceIPRouter

C_ServiceRIP

C_ServiceSTP

C_ServiceTCP

C_ServiceUDP

C_TcpSession

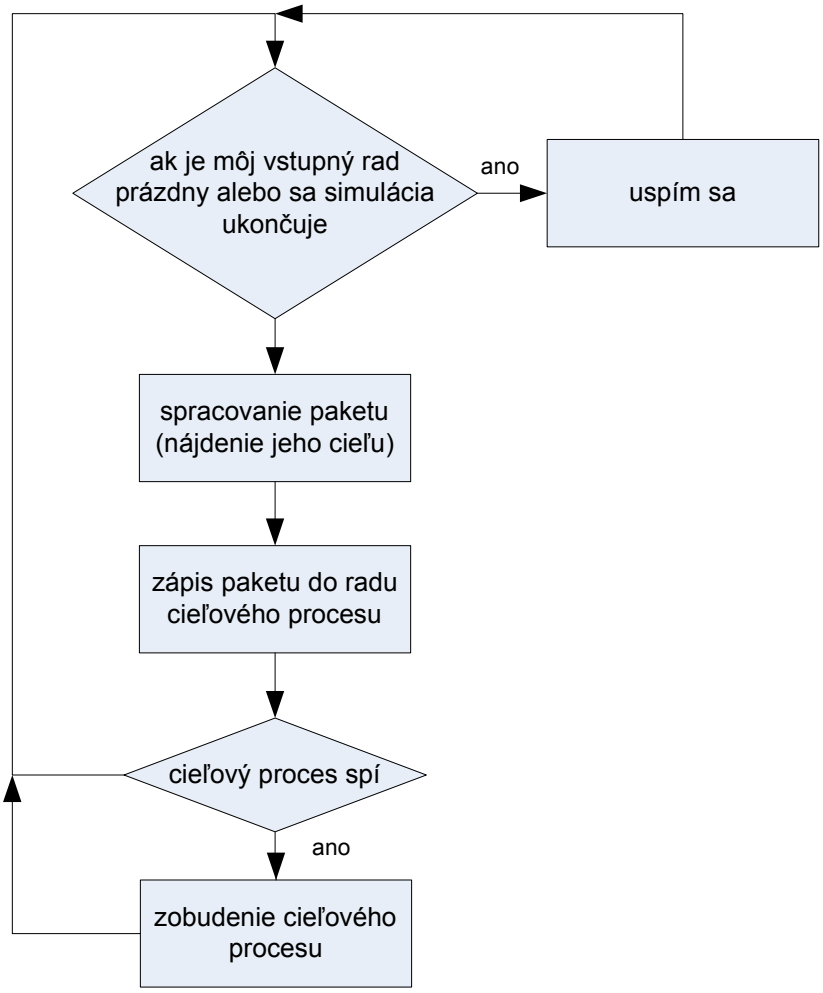
Služby sú odvodené od všeobecnej triedy **C_Service.** Každá služba má jedno obslužné miesto **CFacility,** jeden proces spracovania, a dva rady jeden, do ktorého procesy dávajú pakety na výstup a jeden, do ktorého procesy dávajú pakety na vstup. Obslužný proces vyberá pakety zo vstupného radu, vykonáva potrebné činnosti ako napr. smerovanie a posiela vytvorený paket do výstupného radu. (ak je nutné tak budí niektorý iný obslužný proces napr. IP proces).

Procesy

Pre potreby aplikácie sú vytvorené dva procesy Refresher a Loader. Úlohou Refreshera je každú sekundu kontrolovať, či neboli pridané nejaké zariadenia a ak boli tak ich inicializuje pridá ich stromu. Po tom ako skontroloval prítomnosť nových zariadení, pozdrží vykonávanie samého seba na 1 sek. a potom pokračuje v nekonečnom cykle dokola.Úlohou Loadera je uskutočnenie zmeny v prípade pridania interfejsu nejakého zariadenia, pridaním smerovacieho pravidla poprípade pri zmene nejakej služby.

Skelet procesu

Na obrázku č 10 je vidieť kostru, z ktorej pozostáva každý proces (s výnimkou procesu Refresh). Ide o „nekonečnú“ slučku, v ktorej proces kontroluje svoje vstupné rady, spracováva požiadavky a zapisuje odpovede do radov iných procesov, ktoré následne aj „budí“ ak je to potrebné.



Obrázok č. 21: Skelet procesu

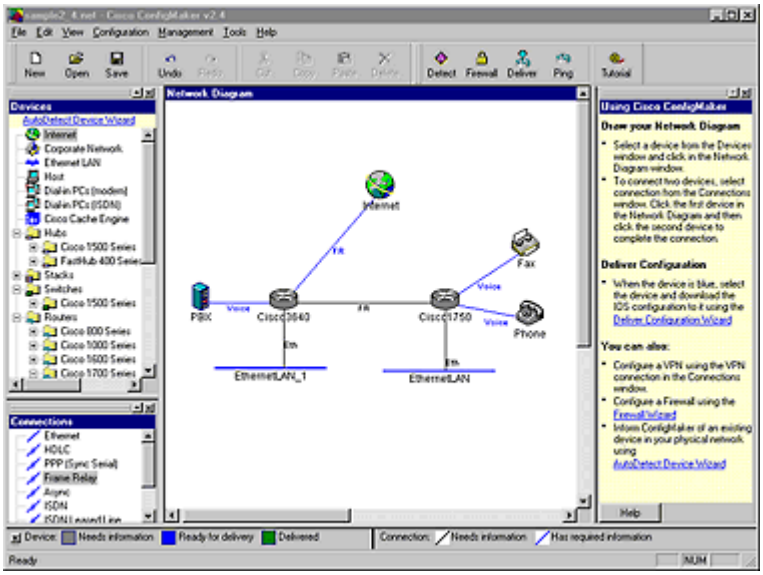
2.3 Komerčné riešenia

Komerčné riešenia, ktoré sme analyzovali mali rôzne zameranie. Niektoré z nich boli voľne prístupné (aj keď po registrácii na stránke firmy, ktorá ich produkuje), iné mali dostupné len demo verziu a z iných bol k dispozícii len produktový list. Tak isto bolo rôzne zameranie produktov – niektoré z nich sú zamerané na konfiguráciu siete, pričom neumožňujú jej simuláciu, kým iné nemajú také možnosti konfigurácie zariadení, ale umožňujú simuláciu. Testované produkty boli: Cisco ConfigMaker, Cisco Network Assistant, Gambit Virtual Lab a RouterSim Network Visualizer.

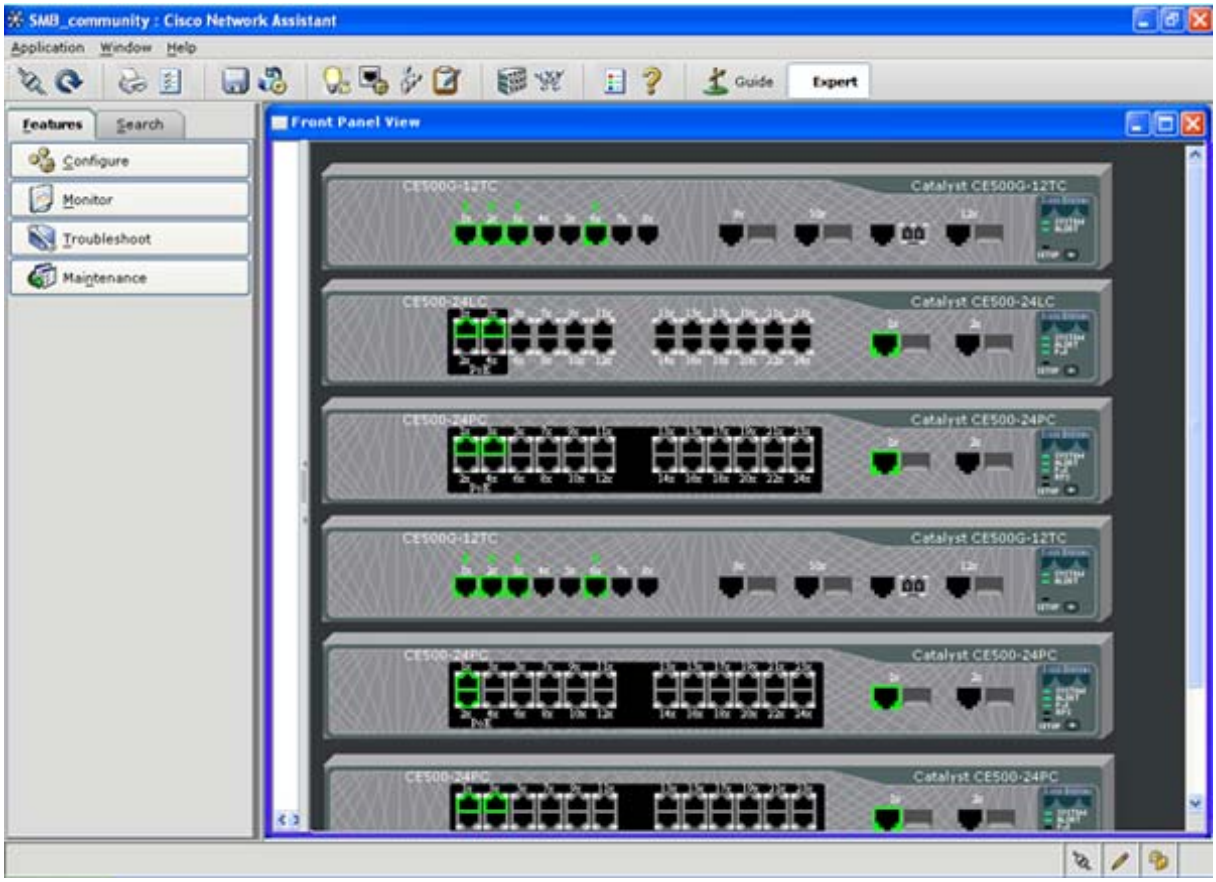
2.3.1 Cisco ConfigMaker a Cisco Network Assistant

Oba tieto produkty pochádzajúce od jednej firmy (Cisco Systems, Inc.) majú veľmi podobné zameranie, a preto sú popísane spolu. Obe aplikácie sú dostupné po registrácii na firemnej stránke a sú zamerané na podporu vytvorenia a konfigurácie malých až stredných sietí vybudovaných za použitia Cisco zariadení. V programoch sa dá (za použitia grafického

užívateľského prostredia) vybudovať požadovaný model siete pozostávajúci z počítačov, opakovačov, prepínačov a smerovačov (podporované sú Cisco zariadenia zo sérií 800, 1000, 1600, 1700, 2500, 2600, 3600 a 4000). Programy umožňujú vytvorenú konfiguráciu zariadení uložiť do súboru a následne načítať do Cisco zariadenia (čo uľahčí následnú konfiguráciu zariadení), resp. v prípade Cisco Network Assistant rovno nahrať po sieti do zariadenia.



Obrázok č. 22: Ukážková obrazovka programu Cisco ConfigMaker. Program pozostáva z hlavného okna, v ktorom sa nachádza model siete. V ľavo od neho sú dve okná v ktorých sa nachádzajú rôzne typy zariadení, ktoré sa dajú pridať do modelu siete a taktiež rôzne druhy spojení.



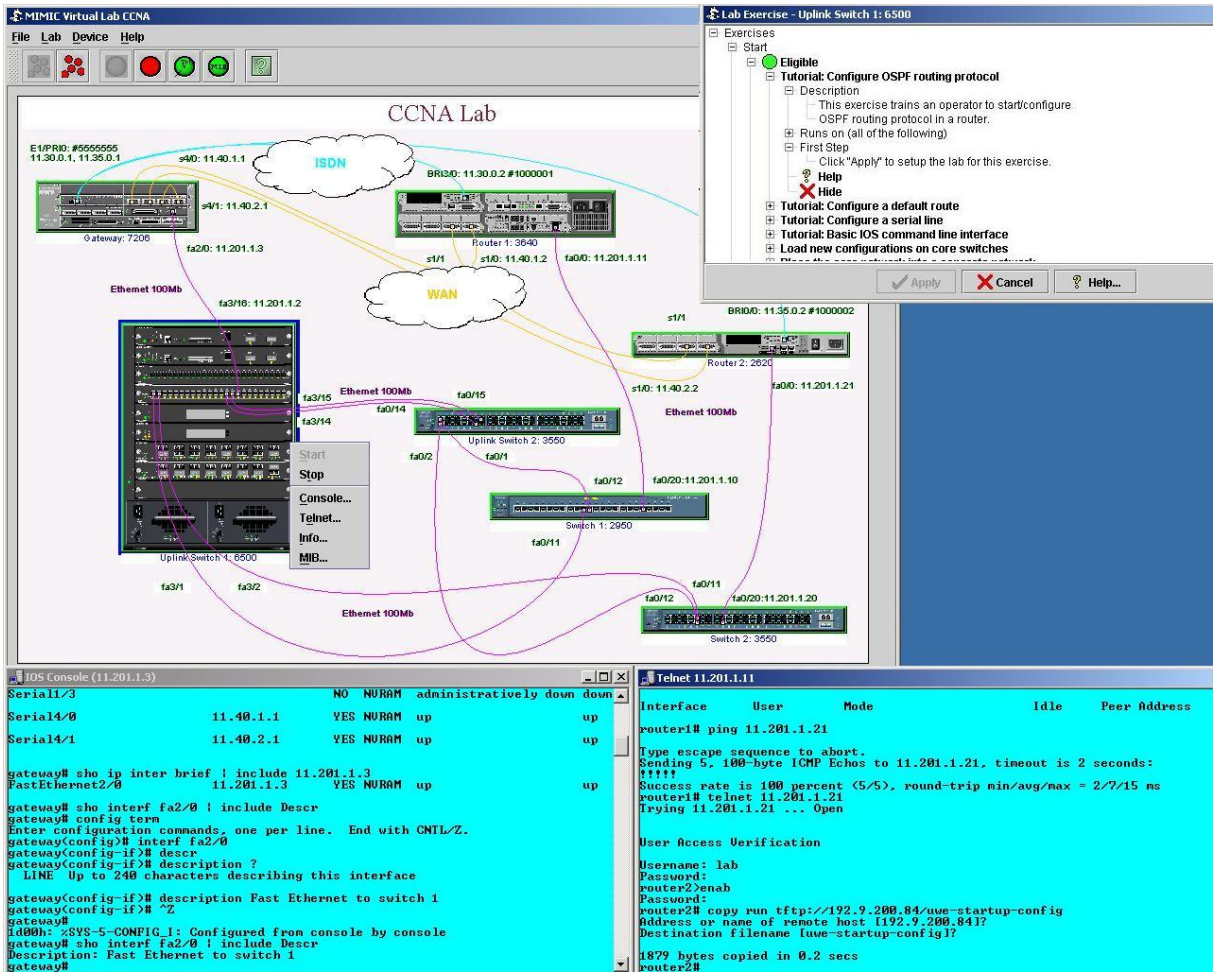
Obrázok č. 23: Ukážková obrazovka programu Cisco Network Assistant.

2.3.2 Gambit Virtual Lab

Tento produkt je určený na výuku v programe Cisco Network Academy (CCNA), a preto sa snaží maximálnej miere zachovávať správanie Cisco produktov. Umožňuje vytvorenie modelu siete pozostávajúcej z maximálne 7 sieťových zariadení (Cisco smerovače (2620, 3640 a 7206) a prepínače (2950, 3550 a 6500), ktoré môžu byť navzájom pospájané spojeniami používanými v LAN, WAN a ISDN. V demo verzii nie je možné si vytvárať vlastné modely sietí, ale len načítať niektorý z predpripravených modelov dodávaných spolu s produktom. Konfigurácia zariadení sa uskutočňuje pomocou konzolového rozhrania, pričom simulátor podporuje plnú sadu príkazov Cisco IOS. Produkt umožňuje nasledovné operácie:

- práca v rôznych módoch – užívateľský, privilegovaný, configuračný a mód nastavovania rozhraní
- nastavenie hesla, IP adries, meno, šírka prenosového pásma
- nastavenie smerovacích protokolov – RIP, IGRP, EIGRP, BGP, OSPF, IS-IS
- „ping“-ovanie zariadení v sieti
- uloženie/načítanie konfigurácie
- štartovanie zariadenia z „flash“ pamäte alebo z TFTP serveru

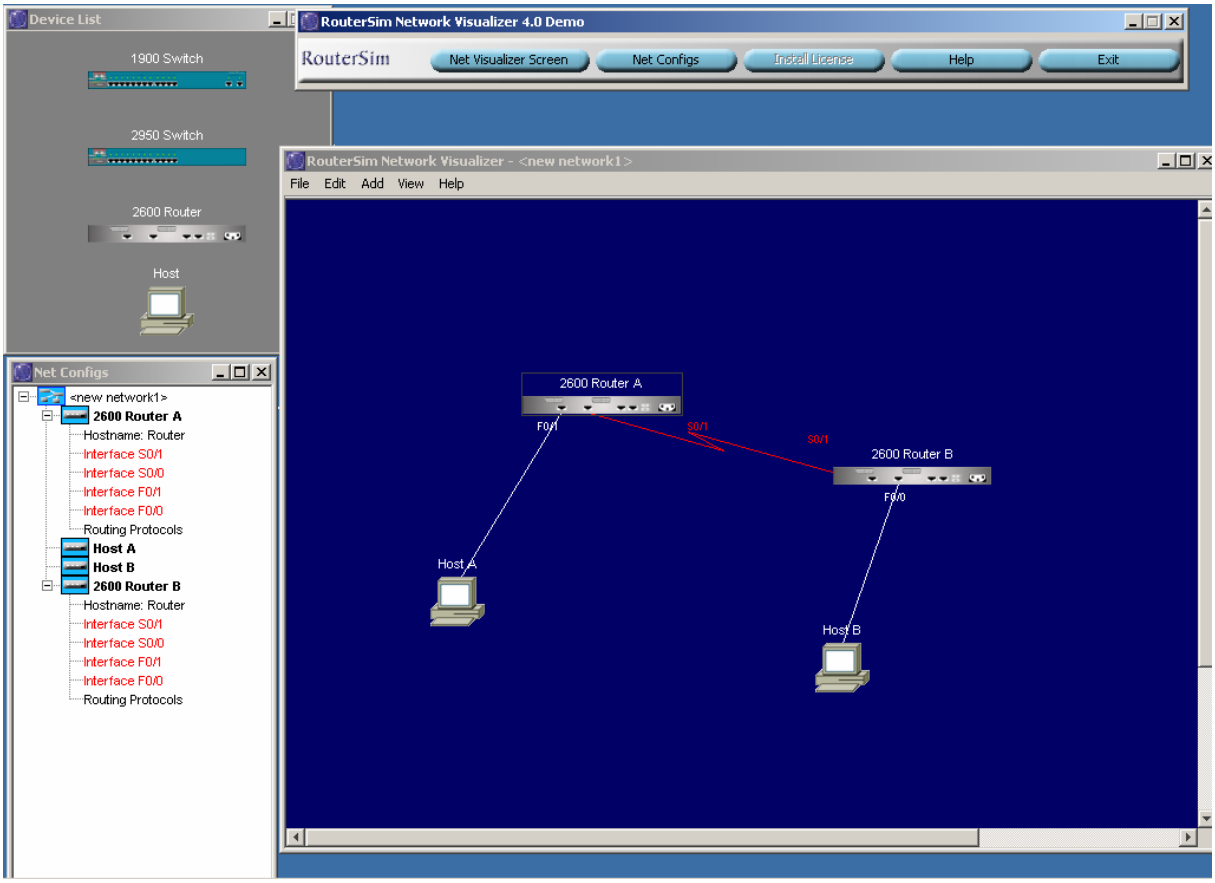
- vzdialené „logovanie“ cez SNMP
- konfigurácia ISDN, CDP, PPP, Frame Relay, ACL a NAT



Obrázok č. 24: Ukážková obrazovka programu znázorňujúca model siete a konzoly prepínačov.

2.3.3 RouterSim Network Visualizer

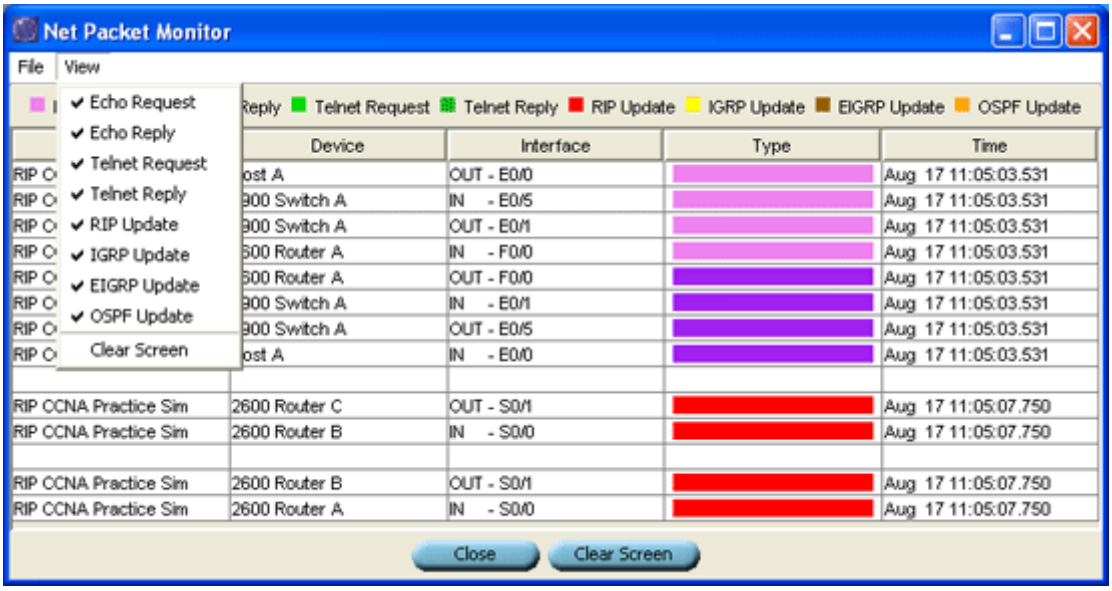
Tento program je dostupný v podobe demo verzie a je zameraný taktiež na výuku v CCNA kurzoch. V tejto demo verzii je k dispozícii len možnosť pridania dvoch smerovačov (dve sériové a 2 ethernet rozhrania) a dvoch počítačov, ktoré je možné konfigurovať pomocou konzoly (pričom sa ale konfigurácia zobrazuje aj v špeciálnom okne).



Obrázok č. 25: Ukážkové okno z programu RouterSim Network Visualizer 4.0 Demo s pridaným maximálnym počtom zariadení.

Pri zakúpení je k dispozícii už verzia 5.0, ktorá má podľa výrobcu množstvo vylepšení a má nasledovné vlastnosti:

- neobmedzený počet modelov sietí ako aj zariadení v modeli (obmedzené len dostupnými zdrojmi počítača)
- podporované zariadenia: Cisco 2621 smerovač s Enterprise edition 12.x softwéru; Cisco 2950 prepínač s 12 10/100 portami; Cisco Catalyst 1912EN prepínač s Enterprise edition softwéru; Cisco 3550 prepínač s 10 10/100 portami; koncové počítače
- umožňuje sledovať komunikáciu zariadení po sieti – pomocou Net Packet Monitoru (viď nasledujúci obrázok)



Obrázok č. 26: Zobrazenie zachytených paketov

- plná emulácia IOS-u simulovaných Cisco zariadení (napr. podpora smerovacích protokolov RIP, RIP v.2, OSPF, EIGRP), podpora NAT, …)

2.3.4 Zhrnutie

Program RouterSim Network Visualizer (spolu s programom Gambit MIMIC Simulator Suite, čo je rozšírená verzia programu Virtual Lab, ku ktorému ale bol k dispozícii len produktový list, a preto je veľmi ťažké hodnotiť jeho funkcie) spĺňajú požiadavky kaldené na simulátor siete (použiteľný napr. pri výučbe). Ale ich zásadná nevýhoda je značná cena, ktorú je potrebné zaplatiť za licencie.

3 Špecifikácia požiadaviek

Na základe vyhotovenej komplexnej analýzy a analýzy predchádzajúceho riešenia tímu SUBNET z minulého roku, sme si stanovili zoznam požiadaviek, ktoré sa budeme snažiť splniť podľa možností v čo najväčšej miere. Vo všeobecnosti ide o dopracovanie a prípadné rozšírenie predchádzajúceho riešenia. Nasledovná špecifikácia preto vychádza zo špecifikácie aplikácie SUBNET a obsahuje iba body, ktoré je podľa nás vhodné oproti pôvodnému projektu doriešiť, pozmeniť alebo doplniť, ako aj body, o ktoré plánujeme predchádzajúce riešenie rozšíriť. Stanovené požiadavky sú rozdelené do nasledovných kategórií:

3.1 Používateľské prostredie

- Ošetrenie uloženia a načítania modelu do a zo súboru
- Pridanie stromu aktuálne použitých zariadení v sieťovom modeli
- Vytvorenie rýchleho konfiguračného bloku
- Optimalizácia užívateľského prostredia a jeho ovládania
- Predvolená automatická konfigurácia zariadení pridávaných do modelu siete

3.2 Implementácia zariadení

Spojenie:

- Nastavenie parametrov prenosu prepojenia (chybovosť – BER, typ – serial, ethernet)
- Sniffovací dialóg – prepracovanie obsahu okna
- Sniffovací dialóg – ošetriť možnosť sledovať viaceré spojenia súčasne
- Vyznačenie prenosovej trasy sledovaných paketov
- QOS štatistiky prenosovej linky

Koncové zariadenie (host):

- Implementácia telnet spojenia medzi hostami (server a klient)

Prepínač (switch):

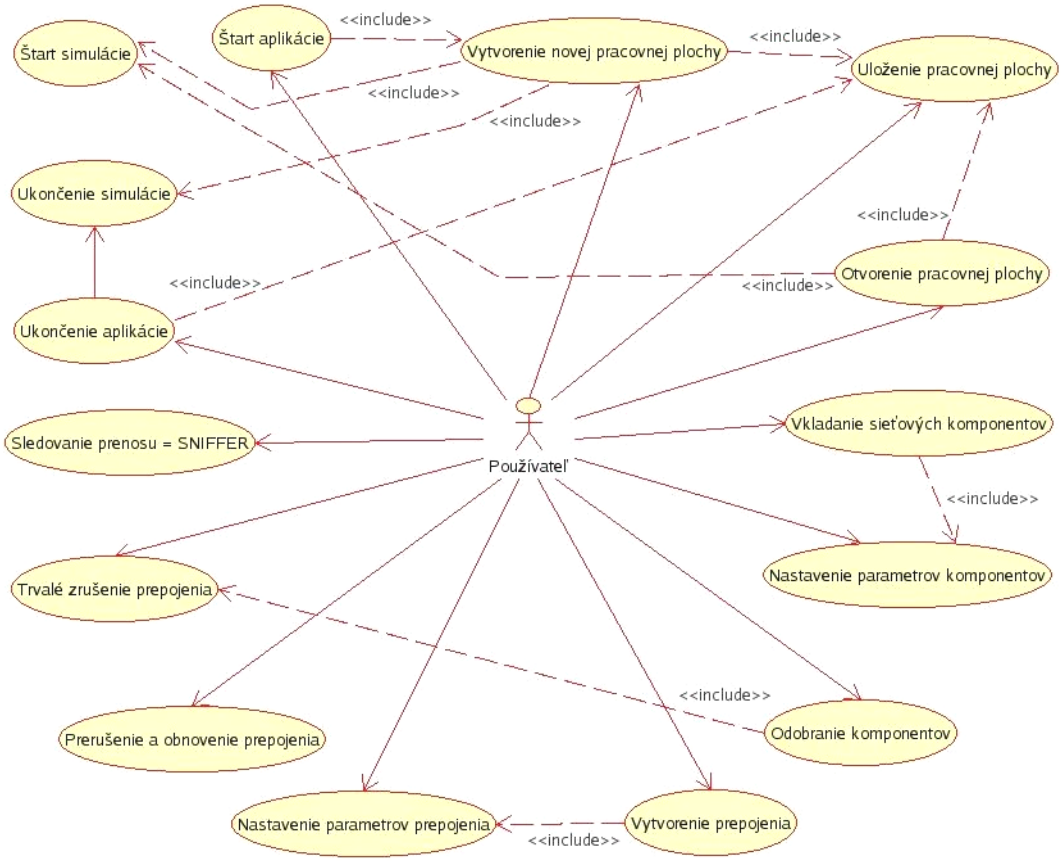
- Zobrazenie smerovacej tabuľky
- Implementácia manažovateľného prepínača (VLANy, port security)
- Implementácia STP protokolu

Smerovače (router):

- Ošetrenie sieťových rozhraní smerovačov – preddefinovanie počtu rozhraní
- Implementácia smerovacích protokolov RIP, IGRP, OSPF

3.3 Prípady použitia

Diagram prípadov použitia ako aj samotné prípady použitia sa od pôvodne navrhovanej špecifikácii líšia z dvoch dôvodov. Prvý dôvod je, že predchádzajúca implementácia obsahuje rozdiely oproti pôvodnej špecifikácii a druhý je doplnenie a aplikácia nami navrhovaných zmien do funkcionálnych vlastností programu. Výsledná podoba diagramu prípadov použitia je zobrazená na obrázku č. 26.



Obrázok č. 27: **Aktualizovaný a upravený diagram prípadov použitia**

Keďže sa jednotlivé prípady použitia viac či menej líšia od pôvodných a niektoré boli vypustené, uvádzame podrobný popis jednotlivých udalostí s ich fungovaním.

3.3.1 Štart aplikácie

Spustením aplikácie sa vykoná proces štartu aplikácie. Ten v sebe zahŕňa načítanie a spustenie programu a následné vytvorenie novej pracovnej plochy (viď Vytvorenie novej pracovnej plochy). Tým sa zároveň spustí simulácia pre aktuálnu pracovnú plochu.

3.3.2 Vytvorenie novej pracovnej plochy

Zvolením možnosti „Nový“ v časti „Súbor“ hlavného menu sa vytvorí nové pracovné prostredie, v ktorom je možné vytvoriť model siete, ktorý bude simulovať sieťový prenos. Táto možnosť automaticky zahŕňa funkciu spustenia simulácie (viď Štart simulácie). Ak v aktuálna pracovná plocha obsahovala nejaký vytvorený, alebo otvorený sieťový model, pred vytvorením prázdnej pracovnej plochy sa vykonajú prípady použitia Ukončenie simulácie a Uloženie pracovnej plochy.

3.3.3 Štart simulácie

V tomto prípade sa v pozadí aplikácie vytvorí nová simulácia, ktorá bude obsahovať modely zariadení a spojení z aktuálne otvoreného sieťového modelu v pracovnom prostredí aplikácie a následne sa začne jej vykonávanie.

3.3.4 Uloženie pracovnej plochy

Tento prípad môže nastať dvomi spôsobmi. V prvom sa predpokladá, že ho vyvolá samotný používateľ zvolením možnosti „Uložiť“ v časti „Súbor“ hlavného menu aplikácie. V druhom prípade je vyvolaný iným prípadom použitia, kedy po jeho aktivácii sa používateľ upozorní na fakt, že pracovná plocha bola zmenená a ponúkne sa mu možnosť, či ju chce používateľ uložiť, alebo zahodiť zmeny. Ak užívateľ ignoruje zmeny, pokračuje vykonávanie situácie, ktorá tento prípad vyvolala. Ak používateľ si zvolí uloženie, prípad pokračuje spoločne tým, že sa otvorí okno so stromovou štruktúrou, kde si užívateľ zvolí miesto a názov súboru, do ktorého sa uloží pracovná plocha. Ak pracovná plocha bola už vopred uložená, používateľovi sa neotvorí možnosť zvoliť miesto, kde sa plocha uloží, ale automaticky sa uloží do súboru s pôvodným názvom a umiestnením na disku.

3.3.5 Otvorenie pracovnej plochy

Používateľ si v hlavnom menu aplikácie v časti „Súbor“ zvolí možnosť „Otvoriť“, čím sa začne proces otvárania uloženej pracovnej plochy. V rámci neho sa testuje obsah aktuálnej

pracovnej plochy. Ak aktuálna plocha obsahuje nejaký model, aktivuje sa prípad Uloženie pracovnej plochy. Po prípadnom uložení sa otvorí dialógové okno, v ktorom si používateľ v súborovej štruktúre nájde súbor s uloženou pracovnou plochou. Po výbere a stlačení tlačidla „Otvoriť“ sa v pracovnej ploche zobrazí načítaný model a aktivuje prípad Štart simulácie.

3.3.6 Ukončenie simulácie

V tomto prípade sa ukončia všetky simulačné procesy, prípadne vyhodnotia globálne štatistiky. Zároveň sa zo simulácie odstránia všetky mechanizmy používané pri simulácii sieťového modelu.

3.3.7 Ukončenie aplikácie

Tento prípad nastane, keď používateľ ukončí beh samotnej aplikácie. Jeho úlohou je zastavenie simulácie a v prípade, že aplikácia obsahuje vytvorený model siete, ponúkne používateľovi možnosť uložiť sieťový model do súboru.

3.3.8 Vkladanie sieťových komponentov

Výberom sieťového komponentu v bloku knižnice sieťových komponentov má používateľ možnosť pridať rôzne druhy sieťových zariadení do modelu siete, ktorý slúži na simulovanie prenosu. Pridaním komponentu do modelu sa zároveň vytvoria údajové štruktúry slúžiace na simuláciu prenosu a uloženie nastavení. Pridaným zariadeniam sa automaticky nastavia preddefinované nastavenia podľa svojho druhu aktiváciou prípadu použitia Nastavenie parametrov komponentu.

3.3.9 Nastavenie parametrov komponentu

Ak tento prípad použitia vyvolal prípad použitia Vkladanie sieťových komponentov, nastavenia sa aplikujú automaticky podľa preddefinovaných možností. Ak tento prípad vyvolal používateľ kliknutím pravého tlačidla myši, pre zariadenia manažovateľný prepínač alebo smerovač sa otvorí konzola pre podrobné nastavenie zariadení, inak sa otvorí dialógové okno, v ktorom sa nastavia základné nastavenia zariadenia. Tento prípad zároveň zastrešuje možnosť otvorenia konzoly na zariadení, v ktorej sa zadávajú príkazy sieťovej komunikácie.

3.3.10 Odobratie komponentu

Týmto prípadom použitia sa zastrešuje operácia odobratia sieťového prvku z modelu siete. Tým sa zo simulačného modelu odstránia všetky štruktúry vlastné odstraňovanému modelu. Ak bolo na komponent napojené sieťové spojenie, pre toto spojenie sa zároveň vyvolá prípad použitia Trvalé zrušenie prepojenia.

3.3.11 Vytvorenie prepojenia

Výberom sieťového prepojenia v bloku knižnice sieťových komponentov má používateľ možnosť prepojiť dve sieťové zariadenia. Typ prepojenia sa detekuje automaticky. Tento prípad zároveň aktivuje prípad použitia Nastavenie parametrov prepojenia pre aktuálne vytvárané prepojenie.

3.3.12 Nastavenie parametrov prepojenia

Ak tento prípad použitia vyvolal prípad použitia Vytvorenie prepojenia, nastavenia sa aplikujú automaticky podľa preddefinovaných možností. Ak tento prípad vyvolal používateľ kliknutím pravého tlačidla myši na sieťovom spojení, otvorí sa dialógové okno, v ktorom užívateľ nastaví základné vlastnosti prenosu cez dané spojenie.

3.3.13 Prerušenie a obnovenie prepojenia

Tento prípad zastrešuje dve operácie nad sieťovým prepojením. Po kliknutí pravého tlačidla myši má používateľ možnosť prerušiť fungujúce prepojenie a tým pozastaviť na ňom prenos, resp. obnoviť prenos na tomto spojení. Deaktiváciou prepojenia ostane prepojenie pripojené, avšak žiadna komunikácia ním nebude prechádzať.

3.3.14 Trvalé zrušenie prepojenia

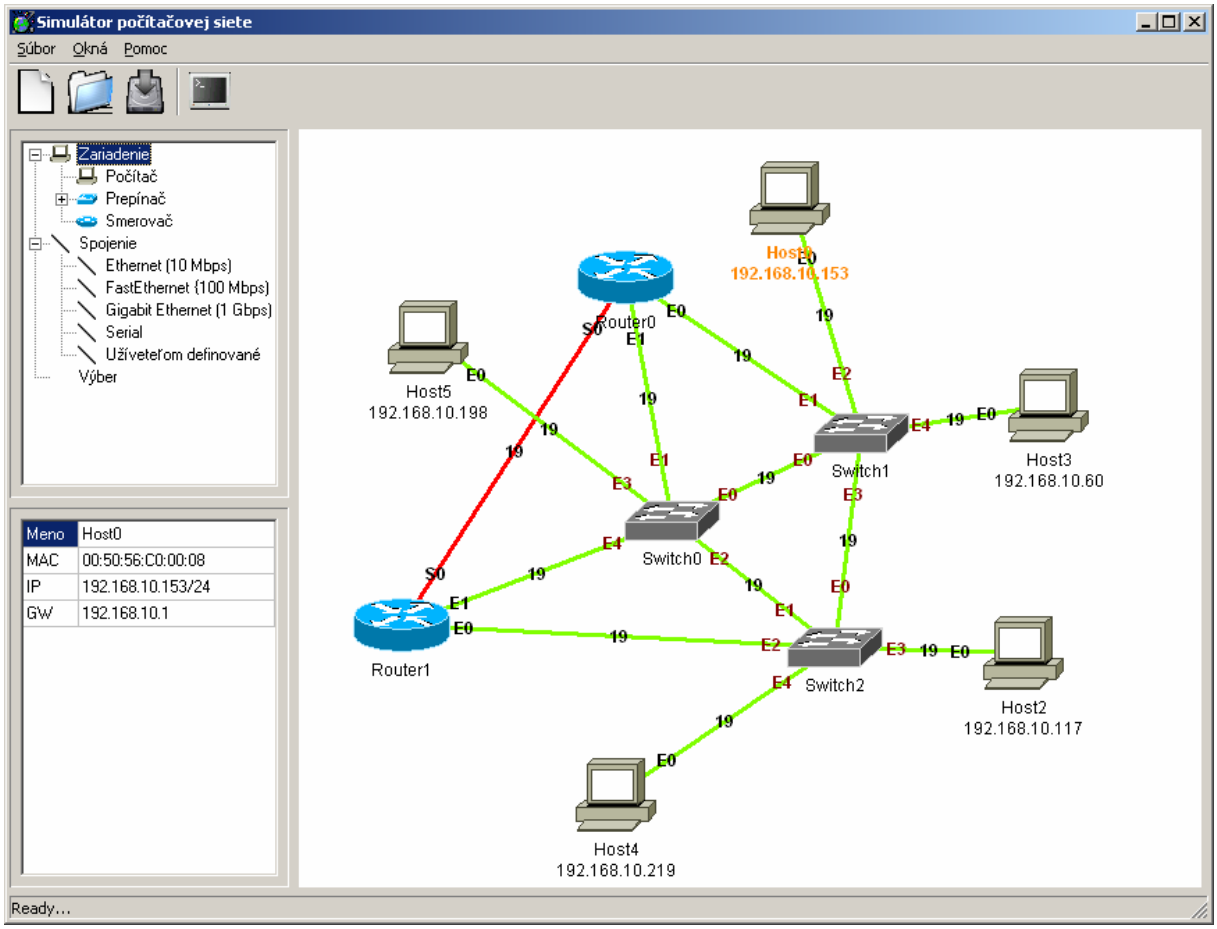
Operáciu úplného zrušenia prepojenia dvoch zariadení zastrešuje tento prípad použitia. Kliknutím pravého tlačidla myši na spojenie má používateľ možnosť v zobrazenom menu zrušiť celé prepojenie a tým aj všetky údajové štruktúry slúžiace na simuláciu prenosu. Po úplnom zrušení prepojenia nebude možné zobraziť trasu prenosov, ktoré boli prenášané týmto prepojením.

3.3.15 Sledovanie prenosu – SNIFFER

Sledovanie prenosu je možné aktivovať na existujúce prepojenia dvoch sieťových komponentov. Funkcia sniffera je rozdelená na niekoľko častí. Prvá obsahuje časovo usporiadaný zoznam prenášanej komunikácie. Označením konkrétneho preneseného údajového rámca je možné v časti s detailmi zobraziť hlbšiu analýzu rámca. V bloku štatistík sú zobrazené rozličné štatistické informácie získané z prenosu, ako aj parametre linky hovoriace o kvality prenosu (QoS).

4 Návrh

4.1 Návrh GUI



Obrázok č. 28: Návrh obrazovky

Hlavné okno aplikácie sa skladá z dvoch častí – v ľavej časti sú to zariadenia, ktoré je možné pridať do modelu siete (vľavo hore) a nastavené parametre jednotlivých existujúcich zariadení (vľavo dole). Najväčšiu časť obrazovky zaberá plocha zobrazujúca model siete. Okrem toho je možné si zobraziť konzolu zariadenia (na konfiguračné alebo testovanie účely) a okno zobrazujúce rámce prenesené sieťou (a z nich následne vypočítané štatistiky).

4.2 Hrubý návrh

Keďže náš návrh vychádza z už hotového systému, musíme pri návrhu zohľadniť jeho doterajšiu implementáciu. Preto uvádzame diagramy tried, v ktorých sú doplnené nami navrhované triedy.

4.2.1 Diagram tried

Diagram tried predstavuje celkový pohľad na architektúru navrhovaného systému. Pozostáva z dvoch častí:

- Funkcionálny diagram tried – predstavuje triedy vykonávajúce základné funkcie systému a reprezentujú základne objekty systému.
- Diagram tried pre služby – triedy, ktoré sú využívané funkcionálnymi triedami

Vo funkcionálnom grafe sú zobrazené (normálnym písmom) základné triedy, ktoré už sú implementované a sú celkovo funkčné. Hrubým písmom sú vyznačené triedy, ktoré neboli plne funkčné, alebo ktoré neboli vôbec implementované.

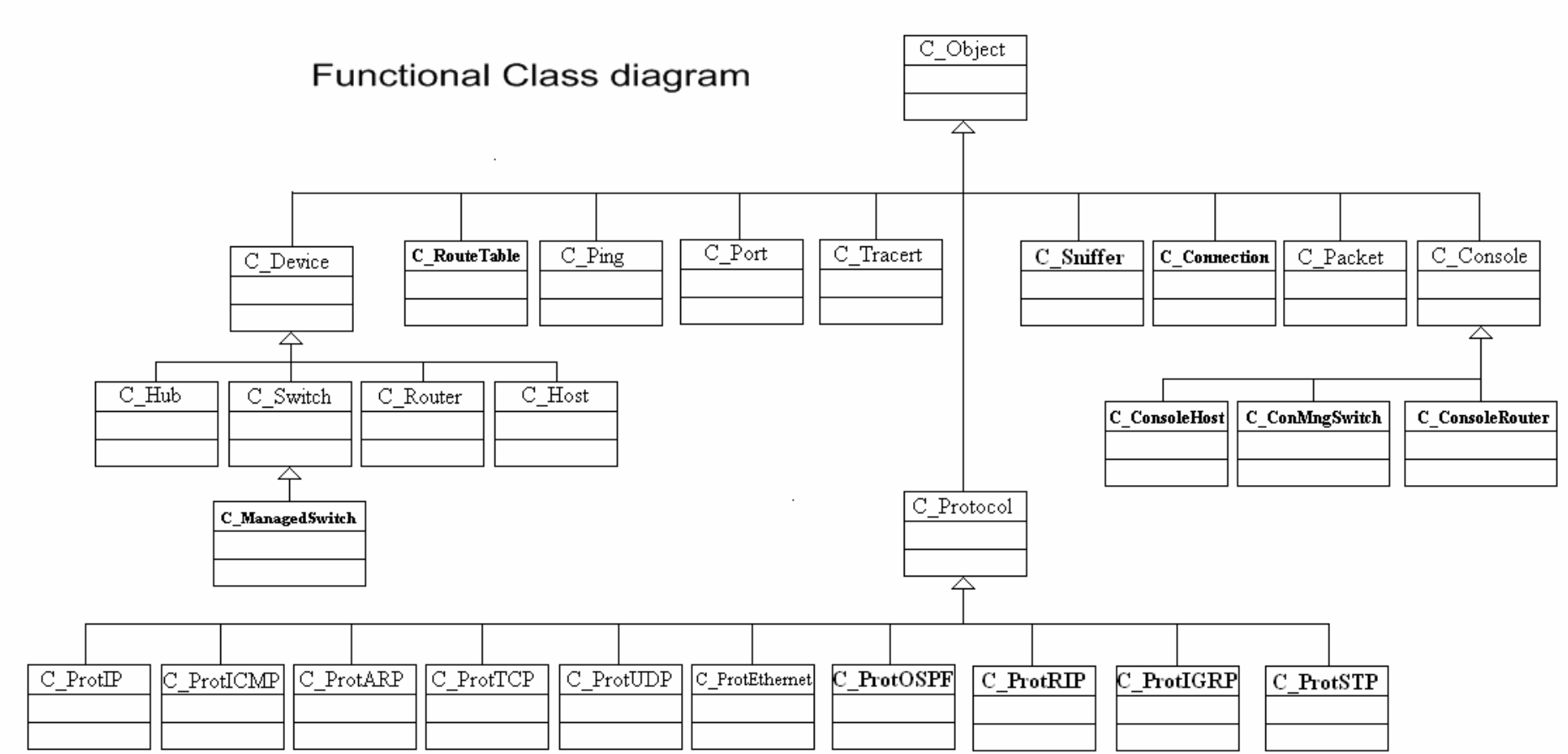
Medzi ne patria:

C_ProtSTP - trieda bude implementovať základné funkcie pre prácu s paketmi STP protokolu, vytváranie paketu, získavanie dát z paketu.

C_ProtIGRP - trieda bude implementovať základné funkcie pre prácu s paketmi IGRP protokolu, vytváranie paketu, získavanie dát z paketu.

C_PrtoOSPF - trieda bude implementovať základné funkcie pre prácu s paketmi OSPF protokolu, vytváranie paketu, získavanie dát z paketu.

C_ProtRIP - trieda bude implementovať základné funkcie pre prácu s paketmi RIP protokolu, vytváranie paketu, získavanie dát z paketu.



Obrázok č. 29: Funkcionálny diagram tried

C_ManagedSwitch - trieda odvodená od triedy C_Switch, ide o zariadenie konfigurovateľného prepínača, na ktorom sa budú dať nastaviť vlan-y a switch port security.

C_Sniffer - trieda, v ktorej je implementovaný sniffer, ktorý je možné súčasne spustiť na viacerých linkách

C_Connection - implementácia spojenia medzi zriadeniami, umožňuje rôzne typy káblov a rýchlostí, half a full duplex.

C_RouteTable - implementácia dynamickej a statickej smerovacej tabuľky pre router

C_ConsoleHost -

C_ConMngSwitch -

C_ConsoleRouter - implementovaná konzola pre zadávanie príkazov ako iná alternatíva k nastavovaniu cez grafické rozhranie.

V diagrame služieb sú tak isto hrubým písmom vyznačené služby, ktoré musíme upraviť alebo vytvoriť.

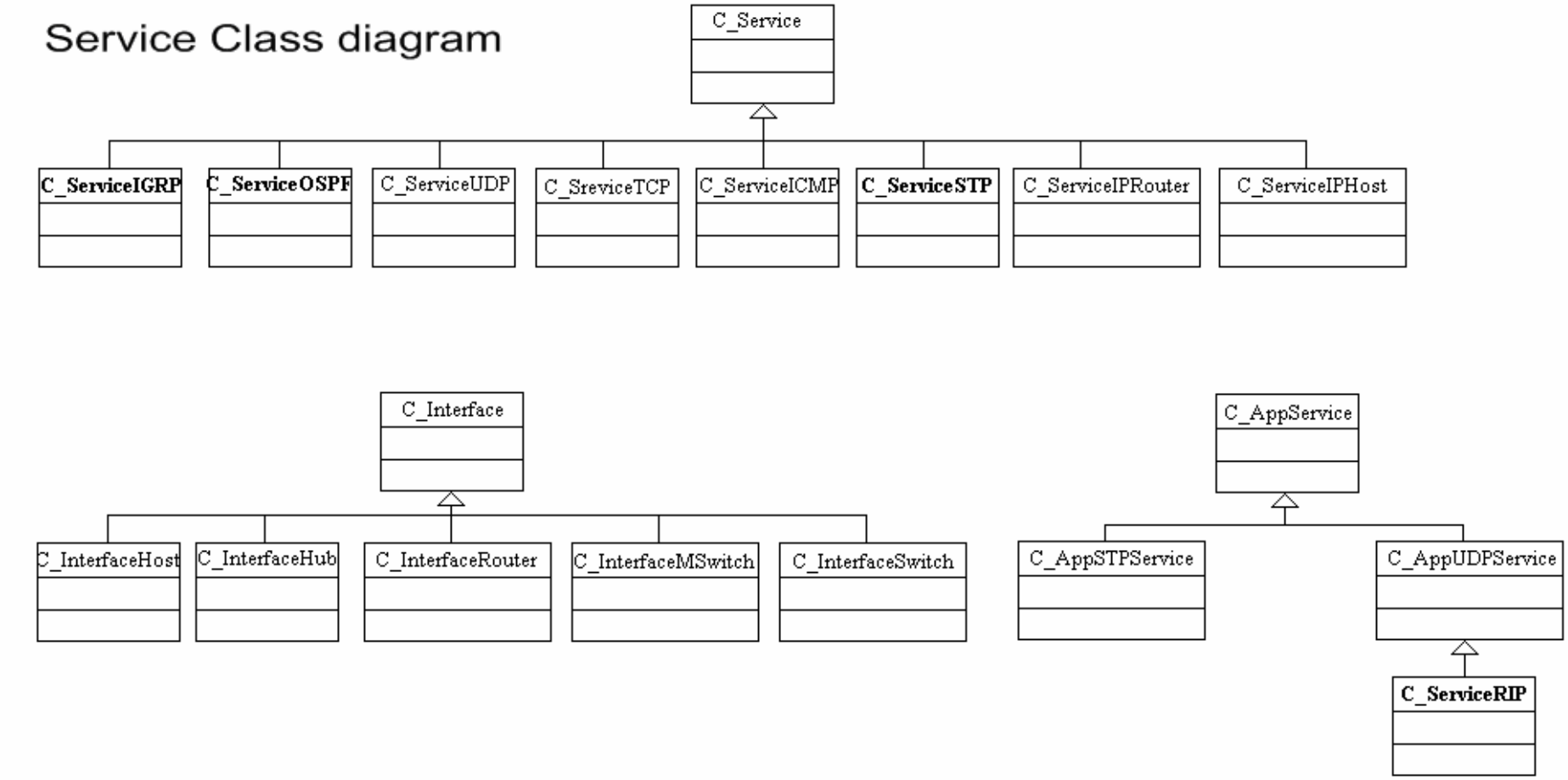
Medzi ne patria:

C_ServiceSTP - služba zabezpečí chod spanning tree algoritmu a teda odstránenie logických slučiek v topológii.

C_ServiceOSPF - služba zabezpečí fungovanie smerovacieho protokolu OSPF

C_ServiceIGRP - služba zabezpečí fungovanie smerovacieho protokolu IGRP

C_ServiceRIP - služba zabezpečí fungovanie smerovacieho protokolu RIP



Obrázok č. 30: Diagram tried pre služby

5 Použitá literatúra:

[1] Timovy projekt 2004/2005, tim SubNet

[2] Počítačová sieť
http://sk.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_sie%C5%A5

[3] Understanding Spanning-Tree Protocol
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm

[4] Routing Information Protocol
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm

[5] Interior Gateway Routing Protocol
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

[6] OSPF Design Guide
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm

[7] The OSPF Specification
http://www.rfc.net/rfc1131.html