Нов Български Университет

департамент “Телекомуникации”

инж. Николай Петров Милованов

ТРАНСФОРМАЦИЯ НА МРЕЖИ И УСЛУГИ ОТ IPV4 КЪМ IPV6 В МРЕЖИТЕ ОТ СЛЕДВАЩО ПОКОЛЕНИЕ

АВТОРЕФЕРАТ

на дисертация за получаване на образователна и научна степен

“ДОКТОР НА НБУ“

по научна специалност: 5.3 **“Компютри и Телекомуникации”**

Нов Български Университет

департамент "Телекомуникации"

инж. Николай Петров Милованов

ТРАНСФОРМАЦИЯ НА МРЕЖИ И УСЛУГИ ОТ IPV4 КЪМ IPV6 В МРЕЖИТЕ ОТ СЛЕДВАЩО ПОКОЛЕНИЕ

АВТОРЕФЕРАТ

на дисертация за придобиване на образователна и научна степен

"ДОКТОР НА НБУ"

по научна специалност: 5.3 **"Компютри и Телекомуникации"**

Научен ръководител: **доц. д-р Иван Богомилов**

Обща характеристика на дисертационния труд

Актуалност на проблема

Еволюцията на телекомуникационните мрежи е процес, продиктуван от непрекъснато променящите се нужди на съвременното информационно общество. Процесът винаги е свързан с назряването на определени нужди, появата на нови технологии и приложението на технологиите в мрежите на различни по големина доставчици на съдържание и услуги. Процесът на преход от една технология към друга може да се случи стихийно, според дадена стратегия или в комбинация от двете. В съвременните телекомуникационни мрежи този процес не е непознат, често се случва да се мигрира от една технология към друга по-модерна, по-бърза и в крайна сметка по-добра. Примери за подобни миграции са подмяната на един вид релейни технологии с други, подмяната на медни кабели с оптични, замяната на множество преносни технологии от слой две на OSI (Open System Interconnection) модела с Ethernet. Общото между всички тези промени е, че са локални и винаги се отнасят до подмяната на една или друга технология под или над нивото на IP (Internet Protocol) протокола.

IP е възникнал като протокол, който да обедини създадените до този момент мрежи за данни. Целта е била да бъдат свързани мейнфрейм машините на водещи научни, военни и бизнес организации в САЩ (Съединените Американски Щати), за да може обединения им изчислителен ресурс да се използва за разработката на сложни научни експерименти. Постепенно мрежата, използвайки силните страни на IP протокола, е еволюирала до две отделни мрежи – Milnet и Internet. Millnet и до момента се използва за военни цели, а Internet е мрежата за глобална комуникация. През годините Internet и мрежите за данни, базирани върху IP са заели важна социално икономическа роля в съвременното общество. Повечето от нас едва ли биха могли да си представят живота без информационни услуги като email, google, www, facebook и skype. Бизнес корпорациите едва ли биха могли да функционират без мрежата, свързваща отделните им офиси или без мрежата, даваща достъп на милиони клиенти до услугите, предоставени от тях.

Силата на Интернет е пряко свързана с качествата на неговото най-силно звено – Интернет протокола. Основното технологично предимство на IP е възможността да работи

с всяка една преносна технология под него като в същото време може да пренася всякакъв вид полезна информация. Информацията, която може да бъде пренесена в един IP пакет, е практически неограничена и зависи само и единствено от максималния размер на сегмента на преносната среда.

Основният недостатък на протокола е свързан с един от неговите най-важни компоненти – адресното пространство. За разлика от информацията, адресите, използвани в Интернет, имат ограничен размер – 32 бита или четири байта. В началото на 70-те години това е било считано за огромно число, много по-голямо от бройката на супер-компютрите по онова време. Още с бума на модемните технологии през 80-те и най-вече през 90-те години става ясно, че това адресно пространство няма да е достатъчно за нуждите на бързо разрастващата се Интернет екосистема. В резултат на това се появяват няколко предложения за промяна на текущата версия четири на Интернет протокол. Надделява версия шест, специфицирана през 1995 в RFC 1883.

Новата версия на Интернет протокол предлага много по-голямо адресно пространство и редица други подобрения. Единственият проблем е, че новата версия не е съвместима със старата. Постепенно се появяват редица механизми за преход от IPv4 към IPv6, а също така и механизми, които да позволят многократното използване на IPv4 адресно пространство.

Въпреки наличието на множество механизми за преход такъв реално не се наблюдава. Редица водещи телекоми споменават наличието на желание и наличието на стратегия за преход, но такъв и до момента не е изпълнен.

Има няколко причини за това. Преходът би бил скъп и не носи директни ползи от бизнес гледна точка за оператора, който го извършва. Преходът е труден и изисква промени в технологията, на която се основава съществуващата мрежа. Изпълнението му без специализиран софтуер, който да подпомогне техническия персонал, изглежда като невъзможна задача в контекста на голям доставчик на мрежови услуги. Преходът е рискован и има реална опасност съществуващите услуги да бъдат засегнати и операторът да не успее да изпълни част от договорните клаузи с определени клиенти.

Анализирайки подобни причини може да се заключи, че е трудно да бъдат оценени бизнес и техническите критерии, които са предпоставка за избор на една или друга

стратегия за преход и че дори и да бъде избрана дадена стратегия е изключително трудно тя да бъде приложена.

Цел и задачи на дисертационния труд

Целта на настоящата дисертация е да бъде предложен формален подход за решаване на проблема по прехода от IPv4 към IPv6 и да бъдат създадени софтуерни средства за автоматизирано и контролирано изпълнение на прехода. За постигането на посочената цел трябва да бъдат изпълнени следните задачи:

1. Да се анализират основните мрежови технологии, имащи отношение към прехода от IPv4 към IPv6
2. Да се анализират основните софтуерни системи използвани за управление на процеси, ресурси и клиенти в съвременните телекомуникационни мрежи.
3. Да бъде предложен подход за формално решение на проблема по прехода от IPv4 към IPv6, което да може да бъде приложено върху контекста на даден мрежови оператор.
4. Да бъде демонстриран подхода върху контекста на оператор X. Да бъдат предложени стратегии за изпълнение на прехода и да бъде избрана най-подходящата спрямо контекста на оператор X.
5. Да бъде разработен прототип на софтуерна система, способен да изпълни стъпките от стратегията победител върху реална мрежова инфраструктура.

Научна новост

Авторът представя прехода от IPv4 към IPv6 като процес на еволюция на комуникационната мрежа от едно текущо състояние в друго желано. Всако едно от състоянията може да бъде представено като формален графовиден модел от данни. Еволюционният преход зависи от контекста на дадената мрежа и от разбиранията, и желанията на различните заинтересовани от дадената мрежа лица.

Преходът може да се изпълни чрез изпълнение на редица стъпки. Всяка една стъпка се състои от:

- технически ограничения, които трябва да бъдат налице, за да бъде възможно изпълнението ;
- бизнес ограничения, които служат за оценка на стъпката;
- действие, което променя текущото състояние на мрежата;
- ефект, който служи за проверка дали резултата от изпълнението на стъпката е този, който е очакван.

Стъпките могат да бъдат групирани в стратегии, а стратегиите могат да бъдат оценени на базата на бизнес и техническите ограничения на съставните им стъпки.

Трансформацията на мрежата от текущото към желаното състояние се извършва по стратегията, която отговаря изцяло на техническите ограничения и съвпада най-точно с бизнес интересите на различните заинтересовани лица.

Разкриването на текущото състояние на мрежата, генерирането на топологичен модел, визуализацията на дадено състояние, показването на разликите между две състояния и изпълнението на стъпките от стратегията могат да бъдат автоматизирани чрез прилагането на проектирания от автора специализиран софтуер.

Използване на резултатите (практическа приложимост)

Предложеният от авторът подход може да бъде използван не само за преход от IPv4 към IPv6, но и за преход от едно (първоначално) състояние към друго желано състояние на всяка една мрежова инфраструктура.

Разработеният прототип бе приложен в средите на мрежови оператори (Глобул), а също и от компании системни интегратори (Телелинк и Тест Солюшънс).

Апробация

Работата бе докладвана изцяло в департамент „Телекомуникации“, Нов Български Университет и частично в следните списания и научни конференции:

- списание „Инженерни Науки“, БАН
- годишник на Нов Български Университет департамент „Телекомуникации“,

- Научена конференция с международно участие „Телеком 2009“, гр. Варна, България
- Конференция с международно участие „Актуални проблеми на защитата на населението и инфраструктурата“, НВУ, гр. Велико Търново, 2009, 2012
- international conference ““Infusing Research and Knowledge in South-East Europe”, SEERC, гр. Солун, Гърция, 2011,
- international conference “MANAGEMENT OF TECHNOLOGY - STEP TO SUSTAINABLE PRODUCTION”, гр. Бол, Хърватска, 2011,
- international conference “Proceedings of International Conference for Entrepreneurship, Innovation and Regional Development”, гр. Охрид, Македония, 2011
- international conference “CompSysTech 2012”, гр. Русе, България, 2012.

Публикации

Във връзка с тематиката на дисертационния труд са направени 10 научни публикации:

1. Milovanov, N., “Traffic optimization in the modern corporate WAN data network”, “Telecom 2009”, Varna, Bulgaria, pp. 328-334, Oct. 8-9, 2012
2. Milovanov, N. , “Service Fulfillment and Assurance in the NGN Networks”, Journal of NVU, Veliko Tarnovo, Bulgaria, 2009
3. Milovanov, N., From Static to Dynamic QoS”, Годишник на департамент "Телекомуникации", 2008 и 2009, НБУ, София, България
4. Slavinski A., Milovanov N., Georgieva V., “IPv4 TO IPv6 NETWORK TRANSFOMATION”, Годишник на департамент "Телекомуникации", 2008 и 2009, НБУ, София, България
5. Milovanov,N., Slavinki A., Georgieva V., “Service Oriented framework for IPv4 to IPv6 Network transformations”, **“**Infusing Research and Knowledge in South-East Europe”,5th Annual South-East European Doctoral Student Conference, SEERC, Thessaloniki, Greece, pp. 358-370, 2010

6. Milovanov N., Slavinski A., Bogomilov I., “Methodology for analyses and selection of Best Practices in the area of embedded systems and industrial informatics”, “Proceedings of International Conference for Entrepreneurship, Innovation and Regional Development ICEIRD 2011”, Ohrid, Macedonia, pp.1-6, 5-7 May 2011
7. Milovanov.N, Bogomilov I., Slavinski. A, 4TO6TRANS USE CASE - DYNAMIC NETWORK INVENTORY DATA POPULATION“, MANAGEMENT OF TECHNOLOGY - STEP TO SUSTAINABLE PRODUCTION“, Bol, Croatia, 2011
8. Милованов Н., Богомилов И. , “Сравнение между IPv4 и IPv6 виртуални частни IPSEC мрежи“, Списание „Инженерни Науки “, София, България, 09.2011
9. Milovanov N., Bogomilov I., “Case Study - IPv6 based building automation solution integration into an IPv4 Network Service Provider infrastructure“, N.Milovanov, I. Bogomilov, CompSysTech '12 Proceedings of the 13th International Conference on Computer Systems and Technologies, pp. 216-223, 2012
10. Богомилов И., Милованов Н., Славински А., Петров Г., „МЕХАНИЗМИ ЗА ПРЕХОД ОТ IPV4 КЪМ IPV6“, Сборник доклади от Юбилейна научна конференция по повод 10 години от създаването на Национален военен университет „Васил Левски”, гр. Велико Търново, 14-15 юни 2012 г
11. Петров Г., Стефанова Т., Богомилов И., Милованов Н., „Мениджмънт аспекти от прилагането на персонални системи за мониторинг на местоположението – аспекти на сигурността“ , Сборник доклади от научна конференция „Мениджмънт в динамично променяща се среда за сигурност“ на НВУ „Васил Левски“, Велико Търново, 30.11 - 01.12.2011, Том 5, стр. 142-150.

Кратко съдържание на дисертационния труд

Глава 1: Обзор – Мрежови технологии

В първа глава е представена кратка хронология на Интернет и основните личности, повлияли на развитието му. Целта на този текст е да покаже хората и технологиите повлияли на еволюционния процес на глобалната мрежа. В следващата част от главата е направен е литературен обзор на IPv4 и IPv6 и са анализирани приликите и разликите между тях. Представени са основните видовете адреси, разгледани са методите за автоматизиране на процеса на конфигурация на IPv6 адреси и са анализирани основните механизми за преход от IPv4 към IPv6. Главата е базирана основно на препоръки, стандарти и утвърдени технологии, поради факта, че целта на настоящата дисертация е да предложи реализируем подход за преход от IPv4 към IPv6, който да може да се следва без излишни тълкувания от организациите, които планират да внедрят новия протокол.

В заключение са изведени основните изводи от направения анализ и е направен преход към следващата глава.

1.1 Интернет - история и откриватели

Интернет е една от последните и най-важни стъпки в еволюцията на комуникационния процес в човешкото общество. Началото е поставено след края на втората световна война в Съединените Американски Щати от Vannevar Bush. Негова е идеята за създаването на “memex” машина за обработка и улеснен достъп до големи количества информация, и създаването на ARPA (Advanced Research Projects Agency). ARPA има за цел да даде технологично предимство на САЩ пред останалия свят чрез обединение на потенциала на военните с този на бизнеса и на научното общество. Последователи на идеите на Bush са J.C.R. Licklider, Bob Taylor и Paul Baran. Licklider е ученият, който първи изказва и защитава тезата, че компютърните системи могат да се използват за симулация на човешкото мислене. Bob Taylor е един от хората, възприели идеите на Licklider за мрежа между компютри и реално полага административното и финансово начало на проекта. Той назначава Lary Roberts за главен архитект и ръководител на екипа по създаване на мрежата. Архитектурата, използвана от Roberts, е

базирана на разработка на Paul Baran. Той предлага използването на пакетна комутация, голям брой мрежови възли и множество връзки между тях, т.е. това, което днес наричаме разпределена мрежа.

Не след дълго са започнали да се появяват и други мрежи подобно на ARPA - SATNET, ALOHANET. Появява се и идеята за обединение на различните мрежи в една обща, с което възниква и проблемът с унифициране на комуникационните протоколи. Технологията Ethernet, създадена от Bob Metcalfe и протоколният стек TCP/IP (Transmission Control Protocol/ Internet Protocol), създаден от Vint Cerf и Bob Kahn са такива унифицирани протоколи. Съвременните комуникации и Интернет са почти изцяло базирани на TCP/IP и по-специално на четвъртата версия на IP протокола.

1.2 Интернет протокол

Интернет протокол версия 4 (IPv4) е бил специфициран през далечната 1980 година в RFC 760. Следват нови спецификации, които добавят нови полета или въвеждат промени в съществуващите. Широкото приложение на Интернет мрежата и информацията предлагана в нея води до изчерпване на IPv4 адресното пространство. Този съществен проблем налага или използване на преобразуване на адреси, или създаване на нов протокол (IPv6).

RFC 1883 поставя началото на IPv6. Новата версия предлага много по-голямо адресно пространство, интегрира в себе си много от протоколите, свързани с IPv4 и предлага редица новости. IPv6 не предлага и не налага стратегията и средствата за преход от версия четири към версия шест. Една от основните причини вече повече от десет години след първоначалната поява на IPv6 все още по-малко от един процент от Интернет е преминал към новия протокол е липсата на първоначална стратегия и модел по-който да бъде извършен прехода.

DNS е протокол за определяне на адреса, отговарящ на дадено име, което потребителя изписва. Той играе важна роля при IPv4. DNS приложението при IPv6 ще е още по-важно тъй като адреса е по-дълъг и по-сложен за изписване от този при IPv4.

Съпоставка между IPv4 и IPv6 е направена в Глава1 част 1.3.4. Заглавната част на IPv6 дейтаграмата е по-малка от тази в IPv4 и е фиксирана на 40 байта. Добавянето на допълнителни етикети в IPv6 е една от основните разлики в сравнение с IPv4.

IPv6 адресът, независимо от вида си, е 128 битов (16 bytes). Адресът се представя в шестнадесетичен вид от 8 групи с по 4 числа. Групите са отделени една от друга с двоеточия. IPv6 поддържа три различни типа адреси, от които зависи как ще бъде доставен пакета - Unicast (индивидуален), Multicast (групов) и Anycast (селективен) адрес. При IPv6 липсват характерните за IPv4 Broadcast адреси.

NDP (Neighbor Discovery Protocol) е набор от механизми, използвани за откриване на съседни устройства. Част от механизмите в NDP присъстват и в IPv4, а други се появяват за пръв път в IPv6. Примери за представители на първата група са RDISC (Router Discovery), ARP (Address Resolution Protocol) и ICMPv4 (Internet Control Message Protocol версия 4), а на втората механизма за "stateless" конфигурация на IPv6 адреса.

1.3 Автоматизиране на процеса на конфигурация на IPv6 адреси

IP адресите може да бъдат конфигурирани ръчно или да бъдат зададени автоматично. При IPv4 автоматичната конфигурация на адреса на устройството може да стане по DHCP (Dynamic Host Configuration Protocol) или чрез PPP (Point to Point Protocol). При IPv6 адресът може да бъде зададен автоматизирано чрез следене на състоянието (по DHCPv6 или по PPP протокол) или "stateless", без да се следи състоянието от всеки един локален IPv6 маршрутизатор. В този случай адресът се задава на базата на префикс, конфигуриран на интерфейса на локалния маршрутизатор.

1.4 Механизми за преход от IPv4 към IPv6

През последните 10 години са разработени множество от механизми за преход от IP версия 4 към IP версия 6. Те могат да бъдат разделени най-общо на три групи. Механизми с превод на адреси, с тунелиране и с двоен IP стек.

Двойният IP стек се изразява в едновременната поддръжка на IPv4 и на IPv6 в мрежата. Най-доброто и пълно описание е дадено в RFC 4213. Препоръката специфицира

два основни механизъма за преход от IPv4 към IPv6 – изграждане на тунели и двоен IP стек.

Олекотеният двоен IP стек (Dual-Stack DS-lite) е технология, позволяваща на доставчик да мигрира опорната си мрежа към IPv6 и да продължи да използва досегашната IPv4 адресация, зададена на крайните клиентски устройства.

NAT-PT (Network Address Translation/Protocol Translation) е един от първите механизми за преобразуване на адреси и портове между IPv4 и IPv6. Той е дефиниран в RFC 2766. Основното му предназначение е да позволи двустранна, комуникация между IPv4 и IPv6 мрежови устройства. NAT-PT има две разновидности – статична и динамична.

NAT64/46 в комбинация с DNS64/46 са група механизми за преобразуване на мрежови адреси от IPv6 към IPv4 и обратно. Основната цел е да се осигури прозрачна комуникация между двата домейна и да бъдат избегнати недостатъците на NAT-PT. NAT64 поддържа два режима на работа: „stateless” и „statefull”.

Класическият Carrier Grade NAT444 е механизъм за двойно преобразуване на адреси, предоставящ възможност на доставчиците на услуги да отложат прехода към IPv6 за известен период от време. Механизмът се основава на възел (Large Scale NAT - LSN 444) за преобразуване частни IPv4 адреси към публични IPv4 такива в изключително голям мащаб. Целта е операторът да споделя едни и същи публични IPv4 адреси измежду голям брой абонати.

6in4 е статичен механизъм за свързване на отдалечени IPv6 зони през IPv4 среда. Механизмът използва изграждане на тунели между статично конфигурирани крайни точки.

6to4 е механизъм за пренос на IPv6 трафик върху IPv4 среда, чрез автоматичното изграждане на 6to4 IPinIP тунели между IPv6 възлите. Механизмът предвижда уникален IPv6 префикс за всеки, който вече има IPv4 публичен адрес. Механизми, базирани на 6to4 са 6rd, 6over4, 4over6.

ISATAP е протокол за автоматично изграждане на тунели между възли с двоен IP стек върху IPv4 мрежова среда.

Teredo е протокол, разработен от Microsoft, за автоматизирано изграждане на тунели между IPv4 кандидат за IPv6 свързаност и IPv6 домейн.

6PE се основава на архитектура, при която PE маршрутизаторите са с двоен IP стек, а MPLS опорната мрежа е IPv4 базирана.

6VPE е базиран на MPLS L3 IPv4 VPN и позволява в един виртуален маршрутизиращ домейн VRF (Virtual Routing and Forwarding) да се поддържа както IPv4, така и IPv6.

Глава 2: Системи за управление на мрежата и бизнеса

2.1 Въведение

Системите за управление на мрежата и бизнеса са една от най-важните части в мрежата на всеки един съвременен доставчик на телекомуникационни услуги. Те се наричат OSS/ BSS системи и основните им сфери на приложение може да бъдат обобщени в три групи:

- Order Fulfillment – управление на поръчките, предоставяне на услуги и управление на ресурсите.
- Service Assurance – управление на повреди, производителност на мрежата, топология, конфигурация, планиране и тестване.
- Billing – системи за прилагане на тарифи, създаване на фактури, осигуряване събираемостта на приходите.

2.2 Препоръки на ITU-T

През 1996 ITU-T публикува стандарт M.3010, в който е представена концепция за управление на телекомуникационна мрежа TMN (Telecommunication Management Network). Тази концепция дефинира четири нива на управление - функционално, физическо, информационно, логическо. Логическото ниво на управление се състои от слой за управление на бизнеса BML (Business management layer), слой за управление на услугите SML (Service management layer), слой за управление на мрежата NML (Network management layer); слой за управление на елементите EML (Element management layer).

През 1997 към концепцията за логическото ниво се добавя допълнително разделение на процесите, характерни за комуникационния оператора в препоръка M.3400 - управление на процеси, свързани с повреди (Fault), управление на процеси, свързани с конфигурация (Configuration), управление на процеси, свързани с таксуване (Accounting), управление на процеси, свързани с оценка на ефективността (Performance), управление на процеси, свързани със сигурност (Security). Структурата на логическото ниво на TMN е представена в Глава 2 на Фигура 2-1 в дисертационния труд.

2.3 Стандарт NGOSS

NGOSS (New Generation Operations System and Software) представлява изчерпателна, интегрирана структура за разработване, осигуряване и имплементиране на OSS/BSS системи и софтуер. Структурата на NGOSS съдържа различните сфери и предлага няколко гледни точки – от страна на бизнеса, от страна на системите, от страна на разработчиците и от страна на клиентите (Глава 2, Фигура 2-2 от дисертационния труд). Основните сфери са SID, eTOM и TAM. SID предоставя бизнес ориентирана перспектива към модела на данните необходими, за да работи дадена организация. eTOM дефинира процесите, които ще използват данните, а TAM (Telecom Application Map) специфицира приложенията, които ще имплементират тези процеси.

2.3.1 eTOM

Организацията TM Forum създава модел наречен TOM (Telecom Operations Map). В периода 2000 – 2002г., този модел е допълнен до Enhanced TOM и публикуван от ITU-T като препоръка M.3050. Основната разлика между eTOM и TMN е в подхода, използван при управление. При TMN, водещи за управлението са мрежата и мрежовите елементи, докато eTOM е създаден с идеята за управление на всички процеси на доставчика на услуги.

Структурата на бизнес процесите в eTOM описва и анализира различни нива на процеси в зависимост от тяхната значимост и приоритети за бизнес процеса. Тази структура е дефинирана общо, като целта е да бъде независима от организации, технологии и услуги. Структурата на eTOM се състои от различни нива:

- Ниво 0 – Бизнес дейности, които разграничават процесите, свързани с клиентите от процесите за управление и стратегии.

- Ниво 1 – Процеси, които включват бизнес функции и стандартни процеси от край до край. Обхващат процесите по поддръжка на клиенти и управление на бизнеса.
- Ниво 2 – Основни процеси, които се комбинират помежду си за предоставяне на услуги и други процеси от край до край. Това ниво акцентира върху FAB (Fulfillment, Assurance and Billing) процесите, свързани със създаване и реализиране на услугите, осигуряване на качеството им и тяхното таксуване.
- Ниво 3 – Дейности и асоциирани утвърдени модели в бизнес процесите.
- Ниво 4 – Стъпки и асоциирани детайлни експлоатационни процеси.
- Ниво 5 – По-нататъшно разделяне на под-процеси, когато е необходимо.

2.3.1.1 Fulfillment (Изпълнение на процеса от поръчка до услуга)

Автоматизацията на процеса от поръчка до услуга започва със запитване от страна на клиента и завършва с доставка на работещ функциониращ продукт. Правилното протичане на този процес е една от най-важните задачи на всяка една компания с бизнес, свързан с доставката на услуги и реализацията на продукти. Автоматизацията на процеса позволява той да бъде реализиран за по-кратки срокове и с по-малко грешки.

Интерфейсът с клиента се управлява от системи за управление на взаимоотношенията с клиента CRM (Customer Relationship Management). CRM системите подават необходимата информация на система за активация на услугите, която на базата на входящата информация и текущото състояние на мрежата създава услуга за съответния клиент. Веднъж реализирала дадена услуга, системата за активация връща статус „Изпълнено“ на системата за управление на взаимоотношенията, а тя от своя страна уведомява клиента, че услугата му е реализирана и започва процесът по таксуване.

2.3.1.2 Service Assurance (Осигуряване на услугите)

Системите за Service Assurance имат за цел да осигурят оптимално използване на услуга от клиент, запазване на съществуващите клиенти, добавяне на нови и непрекъснато следене на предоставяното качество, така че да не се налага плащане на неустойки към клиент, в случай на понижено качество. Предоставяното качество на обслужване се дефинира под формата на договор, наречен SLA (Service Level Agreement). Основните системи, които се използват в Service Assurance са: Fault and Trouble management -

управление на повредите; Performance Management - управление на производителността на мрежата; Topology and Configuration Management – управление на топологията и конфигурациите.

2.3.1.3 Billing (Таксуване)

Системите за таксуване включват процеси по генериране и обработка на информация за таксуване, събиране на приходи за използвани мрежови ресурси или достъп до услуга. За получаване на данни за използваните ресурси се използват междинни системи (Mediation systems). Те събират информация от мрежовите елементи и я предават на процес, който прилага съответните тарифи и генерира съответната такса (Rating). Междинните системи получават записи за повиквания или сесии от данни, които включват информация за начало и край на сесията, участващи абонати, продължителност на сесията. Тези записи може да се изпратят и към други системи, например към отдела, който следи за измами.

Интегрираните системи за OSS/BSS улесняват ежедневната работа на телекомуникационните оператори и доставчици на услуги. Но съществен проблем е, че често поради своята сложност тези системи не могат да бъдат интегрирани напълно. Това води до необходимост от използване на оператори и извършване на някои от дейностите ръчно.

2.3.2 SID – Общ информационен модел

SID предоставя интегриран информационен модел за приложенията от NGOSS. Той е фокусиран върху логически елементи наречени “business entities” и дефинира техните характеристики чрез съвкупности от атрибути. “Business entity” е обект, който отговаря на определен бизнес интерес. SID е базиран на съвкупности от логически единици и взаимоотношения помежду им. Всяка една логическа единица се състои от определено количество данни, описани като атрибути и методи за манипулация на данните. SID е стандартизиран от ITU-T в препоръка M.3190. Моделът на данните в SID е разделен на няколко слоя, които разделят споделената информация в 8 домейна. Всеки един домейн отговаря на област от eTOM (Level 1). Всеки един от осемте домейна се състои от логически единици наречени ABE (Aggregate Business Entities). Те може да съдържат по-малки ABE, имащи отношение към по-малки зони от домейна. Моделът на данни в SID се използва в три големи групи стандарти, специфициращи интерфейси за

достъп до модела на данните – OSS/J (OSS through Java), MTOSI (Multi Technology Operation System Interface) и 3GPP.

2.3.3 Структура Приложения

Дефинираните по-горе процеси за частта „Експлоатация“ от eTOM трябва да бъдат реализирани в конкретни софтуерни продукти. Структура „Приложения“ дефинира именно съответствието между конкретните приложения и различните видове процеси. Приложенията може условно да се разделят на такива свързани с управлението на клиенти, услуги и процеси.

2.4 Стандарти, специфициращи как да бъде реализиран NGOSS

От реализирането на NGOSS са заинтересовани производители на софтуер, оператори и системни интегратори. Разнородната смесица от интереси на различните заинтересовани лица е довела до оформянето на три основни течения, определящи как трябва да бъде реализиран NGOSS – OSS/J, MTOSI и 3GPP.

OSS/J стартира паралелно с NGOSS като началото е поставено през 2000-та година. Целта на OSS/J е подобна на тази на NGOSS като разликите са, че NGOSS е фокусирана основно върху бизнес и системните аспекти на OSS/BSS, а OSS/J върху създаването и внедряването на отворен OSS на базата на основни Java базирани технологии. Развивайки се през годините става ясно, че двете програми взаимно се допълват. NGOSS създава унифициран модел на бизнес процесите, system framework и UML информационни модели. OSS/J следвайки принципите на NGOSS, редуцира SID модела до няколко референтни модела наречени – CBE (Core Business Entities), и създава референтни отворени API интерфейси. API интерфейсите реално предоставят достъп до CBE през SOAP (Simple Object Access Protocol) базирана уеб услуга. Достъпът позволява основните CRUD (Create, Read, Update, Delete) операции да бъдат изпълнени върху обектите създадени на база на CBE.

MTOSI предоставя набор от интерфейси за достъп до моделите на данните, специфицирани в MTNM. MTNM е технологично ориентиран модел повлиян основно от експерти с опит в мрежовите транспортни технологии. Основната цел е била да се създаде интерфейс от OS (Operation System) към OS и от NML (Network Management Layer) към EML (Element Management Layer) за управление на мрежи, използващи една или повече от

една технология за пренос (SONET, SDH, PDH, ATM, FR, DSL, Ethernet). Интерфейсите са различни в зависимост от зоната на приложение. Приложения са управление на връзките, управление на конфигурацията и др.

MTOSI е фокусиран в предоставянето на интерфейси на ниво услуга, мрежа и устройство. OSS/J от друга страна цели да предостави отворени интерфейси в целия OSS/BSS спектър. OSS/J интерфейсите не зависят от мрежовите технологии, докато тези предоставени от MTOSI зависят. През последните години тенденцията е OSS/J и MTOSI да бъдат обединени в един общ стандарт, но това все още не е факт.

2.5 Адаптиране на системите за управление на мрежата и бизнеса към IPv6

От гледна точка на прехода от IPv4 към IPv6 промените ще бъдат основно в eTOM ниво 2 или така наречения FAB модел. Слоят за осъществяване на поръчките ще трябва да започне да създава услуги за клиенти, базирани на IPv6. Системите за инвентаризация на мрежата ще трябва да бъдат променени, така че IPv6 да бъде включен по начин, подобен на сегашното представяне на IPv4. Системите за наблюдение на мрежовия трафик ще трябва да започнат да наблюдават и трафика, генериран от услуги и абонати в IPv6, а системите за таксуване ще се наложи да започнат да таксуват и услугите, свързани с IPv6. Адаптацията на бизнес процеса към новия протокол вероятно ще бъде по-трудна и бавна от адаптацията на съществуващите мрежи към IPv6. Процесът ще отнеме време и ще се отрази и на съществуващите системи в частта на системи за управление на бизнес процеса. За да станат реалност подобни предложения, от една страна ще трябва да еволюират не само мрежата на доставчиците, но и използваните системи за управление, а също и системите за управление на бизнеса.

Основната цел на настоящата дисертация е да предложи методология и прототип на софтуерна система за еволюция на мрежите от IPv4 до IPv6. Най–подходящата точката за интеграция със съществуващия OSS/BSS чрез попълване на SID модела. По този начин данните генерирани от система за трансформация на мрежи може да бъдат използвани от голяма част от останалите OSS/BSS приложения.

Глава 3: Подход и предложение за решаване на проблема

3.1 Въведение

В настоящата глава е представен подходът на автора за решаване на проблема по трансформация на мрежи и услуги от IPv4 към IPv6.

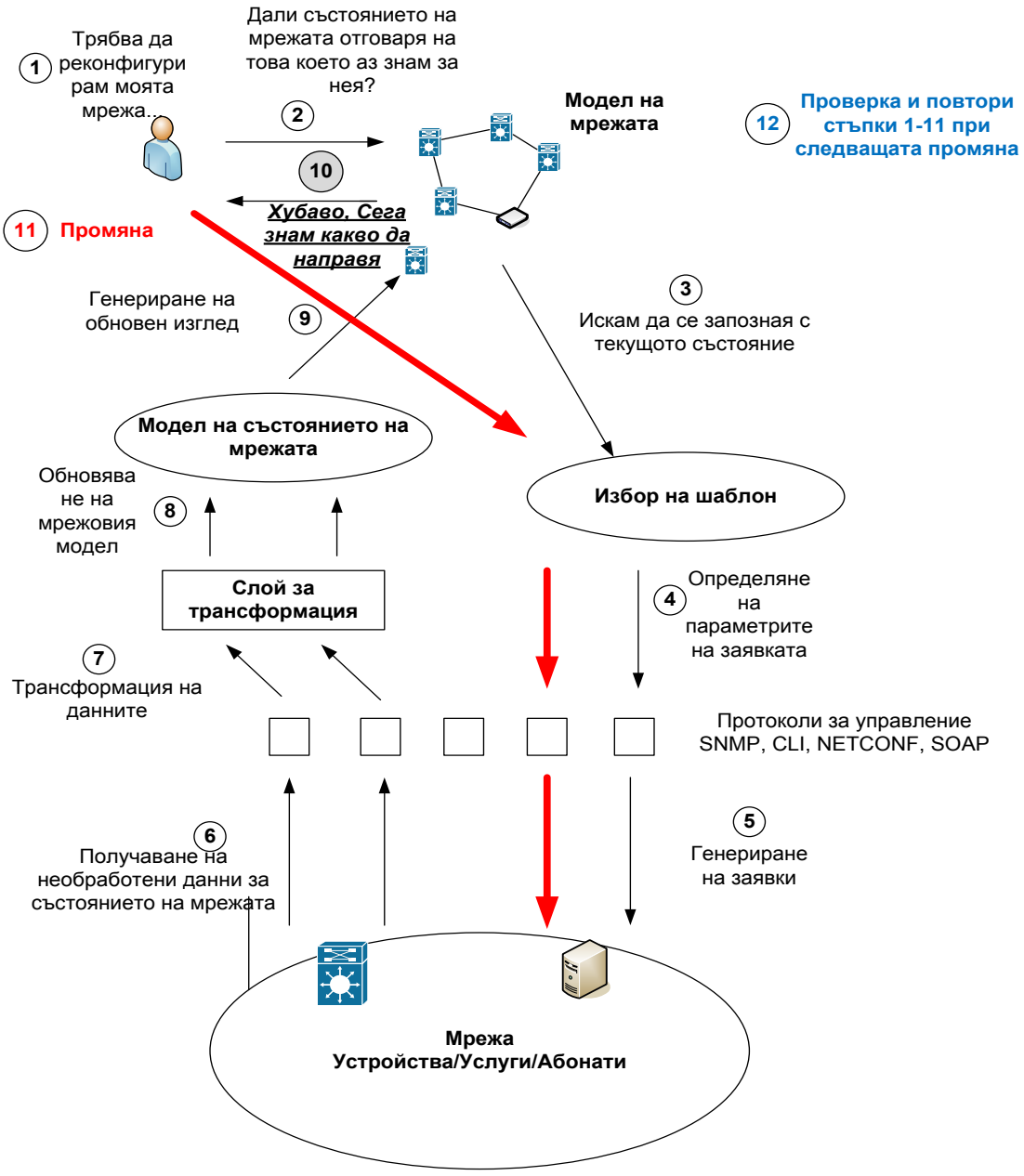
3.2 Основна идея

Основната идея, на базата, на която в последствие са дефинирани функционалните изисквания към прототипа за преход от IPv4 към IPv6 е представена като поредица от логически действия (1 – 12) на **Error! Reference source not found.**.

1. Мрежата трябва да отговори на дадена промяна в заобикалящата я среда. Промяната може да бъде въвеждане на нова услуга, добавяне на нов абонат или реакция в резултат от настъпването на дадена повреда. В голяма част от случаите промяната се изразява в конфигурация на ново или съществуващо устройство или пък в добавяне или подмяна на оборудване.
2. Преди да бъде направена каквато и да е промяна в „жива“ мрежа е добре да бъде зададен въпроса дали познанията на инженера за нея са актуални. Познанието в голяма част от случаите се свързва с визията за дадена топология. За да бъде изградена топологията, е необходимо да бъде извлечена информация от мрежата по даден протокол.
3. Командите за извличане на информация или за промяна състоянието на мрежата могат да бъдат описани в шаблони. Шаблоните съдържат комбинации от заявки и се използват за описване на поредиците от заявки, които инженерите изпълняват.
4. За да бъдат изпълнени командите от шаблона, трябва да им бъдат подадени набор от входящи параметри.
5. Изпълнението на заявките става чрез протоколи за управление на мрежови устройства като SNMP, NETCONF, CLI (Telnet/SSH).
6. Мрежата връща необработени данни в отговор на заявките. Необработените данни трябва да бъдат нормализирани.

7. Нормализацията става чрез трансформация на необработените данни във формат, удобен за визуализация на мрежовата топология.
8. Новите данни обновяват модела на мрежата.

Фигура 3.1Основнаидея



9. На базата на обновения модел се визуализира обновената топология на мрежата.
10. Топологията и промените в нея биват анализирани.
11. Вече може да бъде взето решение какво и как да бъде променено в мрежовата инфраструктура.
12. Провери резултата и ако е успешен повтори стъпки от 1 до 11 за следващата промяна

Основнта идея надгражда съществуващото състояние, при което мрежите се конфигурират основно или ръчно или от системи за упрвление на мрежи спсобни да управляват единственно конкретни техни състояния.

В течение на работата по настоящата теза бе установено, че описаната поредица от действия се повтаря ден след ден във всяка една мрежа. Независимо дали се извършва миграция към IPv6 или се въвежда в експлоатация нова услуга поредицата от действия си остава реално една и съща. Тя винаги се състои от някакво действие, което може да бъде изпълнено при определени условия и което ще има определен ефект върху инфраструктурата. Действието винаги носи определен риск, отнема време и си има цена. Комбинацията от всичките тези елементи може да се определи като стъпка, която променя текущото състояние на мрежата.

Възниква въпросът дали процесът на непрекъсната промяна на състоянието на мрежата не може да бъде систематизиран, така че да обедини техническите действия с изискванията на бизнеса. Бизнес изискванията се превръщат в стратегия за развитие на дадената компания. Стратегията отговаря на изискванията на редица вътрешни и външни за дадената компания заинтересовани лица. Тези изисквания биват породени от редица обстоятелства свързани с екосистемата, в която се развива дадения бизнес. В крайна сметка изискванията на бизнеса могат да бъдат реализирани чрез поредици от множество технически стъпки. Стъпките могат да бъдат групирани в стратегии. Заинтересованите лица трябва да имат начин да оценят отделните стратегии за развитие и да изберат най-подходящата за развитие на техния бизнес.

За да може да бъде даден отговор на този въпрос, ще бъде разгледан конкретния бизнес контекст на един виртуален мрежови оператор.

3.3 Контекст на виртуален мрежови оператор

За да се дефинира проблема, ще бъде представен конкретен хипотетичен пример с доставчика на Интернет услуги X.

Операторът X е среден по размер доставчик на Интернет услуги с около 500 бизнес клиенти и 50000 домашни абонати. X предоставя на корпоративните си клиенти, мрежови услуги като L2 и L3 MPLS VPN мрежи, хостинг, Интернет, телефония и редица други услуги с добавена стойност. През годините този оператор се е справял успешно на конкурентния пазар и търси начин да защити позициите си като за целта усилия полагат различни отдели - „Маркетинг“, „Продажби“, „Развитие на мрежата“, „Поддръжка на мрежата“.

Предложенията на отдел „Маркетинг“ се свеждат до въвеждането на две нови технологии - Internet of Things и Cloud.

Съвместно с реализиране на новите технологии, операторът X трябва да осигури качествени мрежови услуги на своите клиенти. Качеството обикновено означава гарантиране на определени трафични параметри за определени видове трафик и определена надеждност. Освен това мрежовите промени се извършват във времеви интервали договорени най-вече с корпоративните клиенти. Качеството, надеждността и времевите интервалите за реализиране на промените представляват ограничения и качествени характеристики при реализацията на новите технологии.

Изискванията, свързани с въвеждането на новите технологии във виртуалния мрежови оператор X, са актуални за редица реални компании. Анализът на изискванията и подготвянето на стратегии за реализиране на новите технологии се извършва от мрежови архитект или дори екипи от такива. Ръководителите на компанията от своя страна избират коя стратегия е най-подходяща спрямо целите и ограниченията, с които трябва да се съобразява дадената компания. Обикновено ограниченията може да бъдат най-просто изразени като време, цена и риск. Важното е решенията да са резултат от добре анализирани и аргументирани стратегии, предложени от мрежовия архитект.

3.4 Подход на автора

Преходът на дадена мрежова инфраструктура от IPv4 към IPv6, може да бъде описан като преход от едно текущо (IPv4) състояние на мрежата към друго желано (IPv6). За да бъде достигнато желаното състояние, мрежата ще трябва да премине през едно или повече от едно преходни състояния. Преходите между тези състояния може да се определят като стъпки, които мрежата би преминала, за да се реализират дадени промени. Стъпките може да бъдат групирани в стратегии. Достигането на желаното състояние може да стане чрез изпълнението на една или друга стратегия. Изборът на стратегия, по която да еволюира мрежата се извършва на база на оценка на техническите и бизнес еволюционни критерии, наложени от основните заинтересовани лица в дадената мрежа. Пътят, по който желаното състояние ще бъде достигнато, ще се нарича еволюционен.

Всяка мрежа във всеки даден момент е в дадено **състояние**. Състоянието може да бъде описано на базата на множество статични и динамични параметри.

Допускане 1: Текущото състояние може да бъде представено като граф, състоящ се от възли и ребра с дадени параметри, изразяващи статичните или динамични свойства на дадена мрежа.

Всеки граф може да бъде изразен като G = (V,E), където V = {v1, . . . , vn} е множество от възли и E = {e1, . . . , em}, множество от ребра (връзки) между възлите.

Всяко едно устройство, налично в дадената мрежа е възел. Всеки възел има уникален идентификатор (ID) и се характеризира с множество от свойства.

Всяка връзка между два възела е ребро. Всяко ребро има уникален идентификатор (ID), връх, от който излиза (source) и връх, до който достига (target). Всяко едно ребро се характеризира с множество от свойства.

Графът, отговарящ на дадено състояние на мрежата може да бъде съхраняван в различни модели от данни. Форматът използван от автора е Graphml.

По отношение на трансформация на мрежата от едно състояние в друго, авторът прави следното допускане:

Допускане 2: Процесът на мрежова трансформация може да бъде формално изразен и описан като промяна на модела на мрежовия граф от текущо състояние към бъдещо „желано“ състояние.

Всяко едно от състоянията може да бъде формално описано в Graphml.

Допускане 3: Промяната на свойствата ще става на базата на действия. Действията може да съдържат една или повече команди. Командите може да бъдат групирани в шаблони.

Шаблонът дефинира последователност от команди, условията, при които те трябва да се изпълнят и нужните им параметри.

Допускане 4: Процесът на трансформация ще се случи на определен брой „архитектурно значими“ стъпки, докато бъде достигнато желаното състояние.

Всяка една стъпка може да се опише като действие в дадена мрежа. Преди да се случи дадено действие в мрежата, трябва да са изпълнени определени условия. Условията ще се наричат **технически ограничения**. Техническите ограничения обикновено определят възможните последователности от стъпки до достигане на желаното състояние. Освен технически, стъпката може да бъде асоциирана и с определени **бизнес ограничения** (например време за изпълнение, риск, цена). Накрая е добре да се знае дали дадената стъпка е изпълнена успешно или не, т.е. необходима е допълнителна проверка дали мрежата наистина е в това състояние, в което се очаква да бъде.

Допускане 5: Всяка една стъпка се състои от технически и бизнес ограничения, действия, които ще се изпълнят за дадено мрежово устройство и механизми за проверка дали действието реално е довело до очакваното състояние.

Техническите ограничения може формално да се изразят като предварителни условия, на които трябва да отговаря модела на мрежата преди да бъде предприето дадено действие в нея. Те предпазват мрежата от изпълнението на неправилни действия. Синтаксисът на език от команди и проверки, които трябва да бъдат направени преди тяхното изпълнение е дефиниран от Едгар Дийкстра. Дийкстра дефинира “Guarded Command Languadge” език, според който задължителното условие – “guard” е твърдение, което трябва да е истина преди да бъде изпълнена дадена команда/ команди. В системата

за трансформация на мрежи от IPv4 към IPv6 “guard” е проверка по отношение на текущия модел на графа, която трябва да даде верен резултат.

Може да има различни видове ограничения, свързани с бизнеса и организацията, които да бъдат асоциирани с дадена стъпка. Три от най-често срещаните такива са риск, цена и време. Те са дефинирани в Глава 3, част 3.3.9.2.

Действието се изразява в прилагането на даден шаблон или команда върху конкретно мрежово устройство, връзка или група от такива.

Практиката показва, че няма оператор, който да не държи на **механизъм за проверка** дали дадено действие в мрежата е успешно или не. Според подхода на автора проверката може да бъде два типа:

- Проверка дали обновения мрежови модел наистина се намира в очакваното състояние. Това се изразява в намиране на разликите между достигнатото състояние и предишното състояние и проверка дали в разликите се съдържат очакваните промени.
- Проверка в реалната мрежа - пример за това е изпълнението на команди за проверка на свързаността като ping и traceroute.

Практиката е показала, че ако нещо ще се променя в реална мрежа, винаги трябва да се знае в случай на неуспех, как да се подходи. Трябва да бъде дефинирана и стъпка, която би върнала мрежата в предходното ѝ състояние.

Допускане 6: Стъпките могат да се групират в стратегии. Стратегиите се отличават една от друга по стъпките, от които се състоят и по междинните състояния, през които ще премине мрежата при изпълнение на стратегията. Всяка една стратегия се характеризира с конкретни технически и бизнес ограничения според стъпките, от които е съставена.

Подборът на стъпките в дадена стратегия зависят основно от техническите и бизнес ограничения.

Бизнес ограниченията влияят на основната цел на стратегията и в общия случай, заедно с техническите ограничения, предопределят стъпките, от които тя ще се състои. Бизнес ограниченията влияят и генерално на подредбата на самите стъпки.

Техническите ограниченият оказват влияние върху конкретните стъпки, които биха били използвани в конкретна стратегия. Те също така оказват влияние върху точната последователност от стъпки в дадена стратегия. От тях зависи дали една стъпка може да се изпълни или не. Поради това стъпките в стратегията трябва да бъдат подредени в такъв ред, че тяхната изпълнимост да бъде предварително гарантирана.

Допускане 7: Еволюционният път е стратегията, отговаряща най-добре на изискванията на различните заинтересовани лица. По него мрежата еволюира от първоначалното си състояние до желаното такова.

Пътят от текущото (Initial State) до желаното (Desired state) състояние преминава през множество от междинни състояния. Преходът между състоянията се определя от стъпките, част от одобрената стратегията. Мрежата еволюира по графовиден път. Пътят се състои от първоначалното, крайното и множество от междинни състояния. Преходът между едно и друго състояние се извършва според стъпките, от които се състои еволюционния път.

Еволюционният път бива избран на база на оценка на ограниченията наложени от заинтересованите лица и условията наложени от средата, в която оперира даденият оператор, в съответствие с ограниченията, асоциирани с конкретните стъпки. Критериите за избор на еволюционен път се изразяват формално спрямо ограниченията, асоциирани с всяка една стъпка. Критериите могат да бъдат разделени на две основни групи – технически и бизнес. Техническите са наложени от околната среда, т.е. те се асоциират със задължителни ограничения, наложени от текущата мрежа и поддържаните от нея услуги. Бизнес ограниченията са наложени от различните заинтересовани лица. Техническите критерии трябва да бъдат задължително изпълнени, а бизнес критериите да бъдат подредени по приоритет. Еволюционният път е стратегия, отговаряща напълно на техническите критерии и максимално на бизнес критериите.

В дисертационния труд в Глава 3, част 3.3 на Фигура 3-9 е предложен алгоритъм за избор на еволюционен път. Изборът на еволюционен път може да бъде извършен по него

по алгоритъм разработен от доставчика на мрежата или по някой от много алгоритми за избор на решение на базата на многокритериален анализ. Фокусът на настоящата теза е върху разработката на подход за предоставяне на формални критерии за избор, на базата на които да бъде взето решение независимо от използвания алгоритъм.

Глава 4: Приложение на подхода върху контекста на оператор X

В глава 4 авторът демонстрира описания в глава 3 подход върху контекста на оператор X. За целта са моделирани първоначалното и желаното състояние на мрежата X, групи от стъпки за изпълнение на механизмите за преход от IPv4 към IPv6 и четири стратегии за цялостен преход между двете състояния.

Стратегиите са оценени по алгоритъма от глава 3 според критериите валидни за контекста на оператор X и е избрана най-подходящата стратегия за еволюция на мрежата.

4.1 Състояния

Състоянията на мрежата пресъздават първоначалното и желаното състояние на мрежата на оператор X.

4.2 Допускания

- Възлите, изпълняващи ролята на CE, поддържат IPv4, IPv6, NAT-PT и изграждане на тунели 6to4.
- P е обявено от производителя на техника в състояние “End-of-Live”, което не поддържа IPv6. Това устройство трябва да бъде заменено рано или късно с по-нов модел.
- Многофункционалното устройство DC изпълнява ролята на маршрутизатор, loadbalancer (възел, преразпределящ трафичните потоци към останалите машини в центъра за данни) и поддържа IPv6.
- По план мрежата трябва да бъде разширена с две допълнителни устройства на слоя за обединява на трафичните потоци – PE1, PE2.

- X използва OSPFv2 за IPv4 маршрутизиращ протокол и OSPFv3 за IPv6 маршрутизиращ протокол.
- Всички възли на мрежата без Srv и HG са представени чрез реални модели на производителя на мрежово оборудване Cisco Systems.
- Командите, използвани в действията също са според синтаксиса на операционните системи IOS (Internetwork Operating System) и IOS-XR (IOS for High End Routers).

Метаданни

Метаданните са характеристиките на елементите на графа - връзки и възли. В показаните по-долу модели са демонстрирани само метаданните, имащи пряко отношение към прехода от IPv4 към IPv6.

4.2.1.1 Първоначално състояние

Метаданните, с които се характеризират възлите в първоначалното състояние на мрежа са:

- deviceModel - Идентификатор на модела на устройството.
- ManagementIPv4Address - IPv4 Адрес, който се използва за комуникация с устройството от системите за управление на мрежата.
- Port - Идентификатор на порта. Едно устройство може да има повече от един вид порт.
- Ipv4Forwarding - Идентификатор за това дали версия 4 на IP протокола работи на даденото устройство.
- bgpLoacalAS - Идентификатор на BGP автономна системата.

Метаданните, с които се характеризират връзките в първоначалното състояние на мрежа са:

- ipv4Forwarding - Идентификатор за това дали версия 4 на IP протокола работи на дадения интерфейс.
- bgp4Forwarding - Идентификатор за това дали на съответната връзка се използва за IPv4 eBGP peering

- localIPv4Address - Идентификатор на локалния IPv4 адрес на входящия порт (sourceport).
- remoteIPv4Address - Идентификатор на IPv4 адреса на порта на устройството на другия край на връзката (targetport).
- ipv4Routing - Идентификатор на типа на IPv4 маршрутизиращия протокол
- mediaType - Идентификатор на типа на средата на връзката.

4.2.1.2 Желано състояние

- deviceModel - Идентификатор на модела на устройството.
- ManagementIPv6Address - IPv6 Адрес, който се използва за комуникация с устройството от системите за управление на мрежата.
- Port - Идентификатор на порта. Едно устройство може да има повече от един вид порт.
- ipv6Forwarding - Идентификатор за това дали версия 6 на IP протокола работи на даденото устройство
- bgpLoacalAS - Идентификатор на BGP автономна системата.

Метаданните, с които се характеризират връзките в желаната мрежа са:

- ipv6Forwarding - Версия за това дали версия 6 на IP протокола, работи на порта на даденото устройство.
- bgp6Forwarding - Идентификатор за това дали на съответната връзка се използва за IPv6 eBGP peering.
- localIPv6Address - Идентификатор на локалния IPv6 адрес на входящия порт (sourceport).
- remoteIPv6Address - Идентификатор на IPv6 адреса на порта на устройството на другия край на връзката (targetport).
- Ipv6Routing - Идентификатор на типа на IPv6 маршрутизиращия протокол
- mediaType - Идентификатор на типа на средата на връзката.

4.2.2 Списък със съкращения

- CE (Customer Edge) – маршрутизатор, изграждащ и участващ в слоя за достъп в мрежата на оператора.

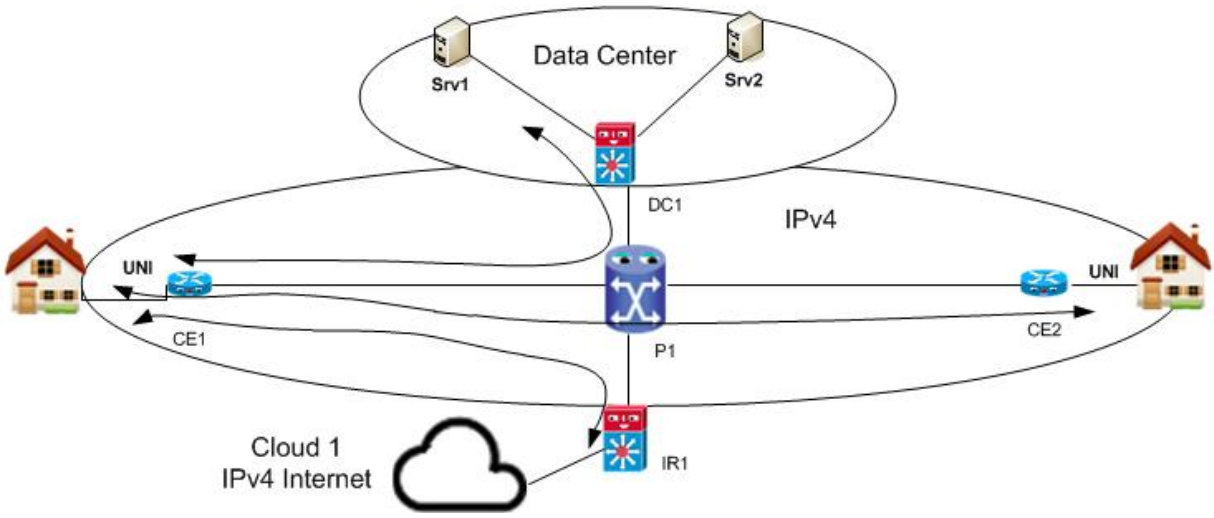
- P (Provider Core Router) – маршрутизатор, изграждащ опорната мрежа.
- DC (Data Center) – многофункционално устройство, свързващо центъра за данни с останалата мрежа.
- IR (Internet Router) - граничен маршрутизатор, свързващ оператора с IPv4 и IPv6 Интернет.
- Srv (Server) – сървър, разположен в центъра за данни. Може да е реална физическа машина или виртуална такава.
- HG (Home Gateway) – домашен шлюз. Свързва компонентите на услугата „Интелигентен дом" с останалата мрежа на оператора.
- PE (Provider Edge) – играе ролята на устройство, което обединява трафика от множеството устройства в слоя за достъп.
- UNI (User Network Interface) - интерфейсът между CE и HG.
- Clould$_1$- Сборен възел, играещ ролята на IPv4 Интернет.
- Clould$_2$ – Сборен възел, играещ ролята на IPv6 Интернет.

4.2.3 Модели на първоначално и крайното състояние на мрежата

В авторефератът към дисертацията са демонстрирани само част от възлите и връзките в моделите на първоначалното и желаното състояния. Пълните модели са демонстрирани в дисертацията на Фигури 4.2 и Фигура 4.4.

Моделът на първоначалното състояние на мрежата се състои от един P, две CE, един DC и един IR маршрутизатор. В центъра за данни се намират сървъри Srv1 и Srv2.

Фигура 4.1 Първоначално състояние на мрежата



Според предложения подход, моделът на това състояние ще бъде изразен в Graphml формат (Фигура 4.2).

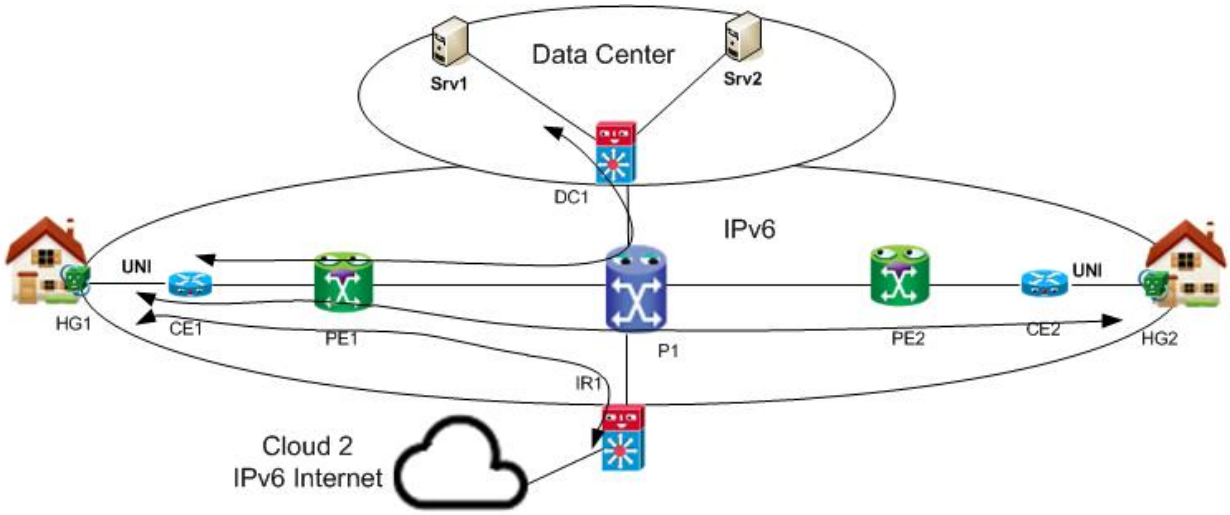
Фигура 4.2 Модел на състоянието на първоначалната мрежа

```
<graphml>
  <graph edgedefault="undirected">
    <key id="deviceModel" for="node" attr.name="deviceModel" attr.type="string"/>
    <key id="ManagementIPv4Address" for="node" attr.name="ManagementIPv4Address"
attr.type="string"/>
    <key id="port" for="node" attr.name="port" attr.type="string"/>
    <key id="ipv4Forwarding" for="node" attr.name="ipv6Forwarding" attr.type="string"/>
    <key id="bgp4Forwarding" for="edge" attr.name="bgp4Forwarding" attr.type="string"/>
    <key id="localIPv4Address" for="edge" attr.name="localIPv4Address" attr.type="string"/>
    <key id="remoteIPv4Address" for="edge" attr.name="remoteIPv4Address" attr.type="string"/>
    <key id="ipv4Routing" for="edge" attr.name="ipv4Routing" attr.type="string"/>
……<key id="bgpLoacalAS" for="node" attr.name=" bgpLoacalAS " attr.type="string"/>
……<key id="mediaType" for="edge" attr.name=" mediaType" attr.type="string"/>
    <node id="P1">
      <data key="port">Gig1/0</data>
      <data key="port">Gig0/0</data>
      <data key="port">Gig1/1</data>
      <data key="port">Gig2/1</data>
      <data key="deviceModel">cisco12810</data>
      <data key="ManagementIPv4Address">10.10.13.22</data>
      <data key="ipv4Forwarding">YES</data>
```

```
        </node>
         <node id="DC1">
           <data key="deviceModel">cisco7606</data>
           <data key="ManagementIPv4Address">10.10.14.2</data>
           <data key="ipv4Forwarding">YES</data>
           <data key="port">Gig1/0</data>
            <data key="port">Gig1/1</data>
            <data key="port">Gig1/2</data>
        </node>
       …..
        <edge id="P1DC1" source="P1" target="DC1" sourceport="Gig1/1" targetport="Gig1/0">
           <data key="localIPv4Address">10.10.14.1</data>
           <data key="remoteIPv4Address">10.10.14.2</data>
           <data key="ipv4Forwarding">YES</data>
           <data key="ipv4Routing">OSPF</data>
……..<data key="mediaType">GigabitEthernet</data>
        </edge>

      </graph>
</graphml>
```

Фигура 4.3 Желана мрежа



Фигура 4.4 Модел на състоянието на желаната мрежа

```
<graphml xmlns:cmp="http://xsltsl.org/cmp">
  <graph edgedefault="undirected">
    <key id="deviceModel" for="node" attr.name="deviceModel" attr.type="string"/>
    <key id="ManagementIPv6Address" for="node" attr.name="ManagementIPv6Address"
attr.type="string"/>
    <key id="port" for="node" attr.name="port" attr.type="string"/>
    <key id="ipv6Forwarding" for="node" attr.name="ipv6Forwarding" attr.type="string"/>
    <key id="ipv6Forwarding" for="edge" attr.name="ipv6Forwarding" attr.type="string"/>
    <key id="bgp6Forwarding" for="edge" attr.name="bgp6Forwarding" attr.type="string"/>
    <key id="localIPv6Address" for="edge" attr.name="localIPv6Address" attr.type="string"/>
    <key id="remoteIPv6Address" for="edge" attr.name="remoteIPv6Address" attr.type="string"/>
    <key id="ipv6Routing" for="edge" attr.name="ipv6Routing" attr.type="string"/>
……<key id="bgpLoacalAS" for="node" attr.name=" bgpLoacalAS " attr.type="string"/>
……<key id="mediaType" for="edge" attr.name=" mediaType" attr.type="string"/>
    <node id="P1">
      <data key="port">Gig0/0</data>
      <data key="port">Gig1/0</data>
      <data key="port">Gig1/1</data>
      <data key="port">Gig2/1</data>
      <data key="deviceModel">CRS1</data>
      <data key="ManagementIPv6Address">FEC0:10:10:13::22</data>
      <data key="ipv6Forwarding">YES</data>
    </node>
```

```
        <node id="DC1">
          <data key="deviceModel">cisco7606</data>
          <data key="ManagementIPv6Address">FEC0:10:10:14::2</data>
          <data key="ipv6Forwarding">YES</data>
            <data key="port">Gig1/0</data>
           <data key="port">Gig1/1</data>
            <data key="port">Gig1/2</data>
        </node>
        <edge id=" P1DC1" source="P1" target="DC1" sourceport="Gig1/1" targetport="Gig1/0">
          <data key="localIPv6Address">FEC0:10:10:14::1</data>
          <data key="remoteIPv6Address">FEC0:10:10:14::2</data>
          <data key="ipv6Forwarding">YES</data>
          <data key="ipv6Routing">OSPFv3</data>
……..<data key="mediaType">GigabitEthernet</data>
        </edge>
      </graph>
    </graphml>
```

4.3 Еволюция на модела

Преходът от IPv4 към IPv6 се изразява в множество еволюционни промени на мрежовата инфраструктура. Промените могат да бъдат изразени формално чрез разлики в топологията на мрежата и в разлики между елементите и метаданните на графа, представящ крайното (желано) и първоначално състояние на мрежата.

4.3.1 Прилики и разлики в топологията на мрежата

Топологичните прилики между двете състояния са:

- Възли CE1, CE2, House1, House2, IR1, DC1, Srv1, Srv2, P1 съществуват и в двете топологии.
- Връзки CE1-House1, CE2-House2, P1-DC1, P1-IR1, DC1-Srv1, DC2-Srv2 съществуват и в двете състояния.

Топологичните разлики между желаното и първоначалното състояние са:

Възли:

- Появили са се четири нови възли HG1, HG2, PE1, PE2, Internet Cloud2;

- Изчезнал е възел Internet Cloud1.

Връзки:

- Появили са се нови връзки: HG1-House1, HG2-House2, CE1-PE1, CE2-PE2, P-PE1, P-PE2.
- Изчезнали са връзки: CE1-P1, CE2-P2, IR1-Cloud1;

4.3.2 Прилики и разлики в метаданните на графа, възлите и връзките

Свойства ManagementIPv4Address и ipv4Forwarding, съществуващи на всеки един възел в първоначалната топология са изчезнали от модела и са заменени с ManagementIPv6Address и ipv6Forwarding.

Свойство deviceModel на възел P1 се е променило от 12810 на CRS1.

Свойства localIPv4Address, remoteIPv4Address, ipv4Forwarding, ipv4Routing, съществуващи на всяка една връзка в първоначалната топология са изчезнали от модела и са заменени с localIPv6Address, remoteIPv6Address, ipv6Forwarding, ipv6Routing.

Появило се е ново свойството bgp6Forwarding на връзката между IR1 и InternetCloud2

Запазило се е свойството mediaType.

4.3.3 Анализ на приликите и разликите

Еволюцията на мрежата от IPv4 към IPv6 се е отразила на топологията на мрежата по следните начини:

- С внедряването на услугата Интелигентен Дом се появил нов микро слой за достъп в къщата на крайния клиент. Появили са се нови устройства и нови връзки.
- По-време на прехода опорната инфраструктура на мрежата се е разширила с нов слой от PE устройства. Това е пряк резултат от политиката на оператора за експанзия в нови зони, но и като мярка спрямо нарасналия потребителски трафик от новопоявилите се услуги (в случая Интелигентен дом).
- IPv6 е въведен на всеки един възел от мрежовата инфраструктура Това се е изразява в нова адресна схема и в промени на метаданните на всеки един

възел и връзка. Промените се изразяват в подмяна на версия 4 с версия 6 на IP протокола на всяко едно устройство и на всеки един негов интерфейс. В подмяна на IPv4 адреса с IPv6 такъв и в подмяна на маршрутизиращия протокол. В опорната мрежа OSPFv2 е заменен с OSPFv3. По останалите устройства се е запазил типът на маршрутизацията - статичен, но вече е статична IPv6 вместо статична IPv4 маршрутизация.

- Типът на средата на протокола под IP се е запазил непроменен.
- Интернет BGP peering се е променил и доставчикът вече няма свързаност към остарелия IPv4 Интернет.

Подобна еволюционна промяна не може да стане с „магическа пръчка“ тя трябва да се случи на малки стъпки групирани в определена стратегия и чрез прилагане на някой от механизмите за преход, описани в глава 1.

4.4 Стъпки

Преходите между отделните състояния ще се извършат на “стъпки”. Стъпките биват различни видове. Може да има стъпки, свързани с разширения на мрежата и добавяне на нови устройства и връзки. Друг тип стъпка е подмяна на съществуващо устройство или промяна на съществуваща връзка. Третият и най-често срещан вид стъпка е свързана с промяна на параметрите (метаданните) на съществуващи устройства и връзки. Всяка една стъпка, т.е. преход между две състояния, се състои от действие, ефект върху мрежата и може да бъде обвързана с определени технически и бизнес ограничения. Понякога ефекта от дадено действие може да се различава от предварително очаквания такъв. Ако това е така, се изпълнява “rollback” стъпка, съдържаща действие обратно на предишното или команда, с която дадено устройство да бъде върнато към последната му работеща конфигурация.

Стъпките са дефинирани според шаблона в подточка и са разделени в няколко основни групи. Всяка една група съдържа стъпки с подобна функционалност, но дефинирани за устройства на различни слоеве от мрежата.

Синтаксисът, използван за дефиниране на действието, ефекта, техническите и бизнес ограниченията следва дефинициите и допусканията, направени в подточка 4.2.1.

4.4.1 Шаблон за дефиниране на стъпки

Всяка една от стъпките е структурирана в следния шаблон (Таблица: 4-1).

Таблица: 4-1 Шаблон за описване на стъпка

Номер: S - Уникален идентификационен номер на стъпката
Име: Име на стъпката
Контекст: Контекст, в който стъпката ще бъде приложена.
Технически ограничения: Техническите ограничения, които са задължителни за изпълнението на стъпката. Входящи параметри – входящите параметри, необходими за изпълнението на условията в проверката. Проверка – проверка спрямо текущото състояние.
Бизнес ограничения : Бизнес ограниченията, асоциирани с дадената стъпка. В най-общия случай това е цената, на която може да се изпълни стъпката, рискът при изпълнението на стъпката и времето, за което може да бъде осъществена дадената стъпка.
Действие: Входящи параметри - входящите параметри, необходими за изпълнение на действието. Действие – действието, с което се характеризира дадената стъпка. Често действието се изразява в изпълнение на шаблон с команди.
Ефект : Входящи параметри - входящите параметри, необходими за проверка на ефекта. Проверка – проверка, удостоверяваща дали даденото действие е донесло нужния

ефект върху мрежата.

В настоящата дисертация са разгледани множество стъпки, свързани с различни механизми за преход от IPv4 към IPv6, а също и с фундаментални дейности като подмяна на мрежово оборудване и нова конфигурация на мрежово оборудване според контекста на оператор X. Описанието на стъпките е в отделен документ – Приложение 1 към дисертацията.

Стъпките от Приложение 1 са разработени според контекста на оператор X, но могат да се използват със сравнително малки изменения за преход на коя да е мрежа на друг оператор от IPv4 към IPv6. Не случайно в стъпките не се споменават индексите на конкретните устройствата. Например, ако в модела на мрежата на X има устройство P1, то в стъпките е дадено просто P_i; ако в модела има PE1 и PE2, в стъпките и стратегиите се споменава само за PE и PE_i. По аналогия, ако става дума за DC1, IR1, CE1 и Srv1,2, то се използват DCi, IR_i, CE_i и Srv_i. Това е направено с цел да бъде демонстрирано, че стъпката или стратегията засяга всички устройства, намиращи се в дадения слой на мрежата или изпълняващи дадена роля в нея. Пример за изцяло дефинирана стъпка е демонстриран в Таблица: 4-2. В Приложение 1 са обобщени предложените стъпки за мигриране на мрежата от текущото към желаното състояние.

Таблица: 4-2 Пример за напълно описана стъпка

Номер: S13
Име: Enable NAT-PT (Добавяне на NAT-PT)
Контекст: Добавянето на механизъм за превод на адреси от IPv4 към IPv6 има приложение основно на слой CE. Той би играл важна роля при въвеждане в експлоатация на услугата „Интелигентен дом“. Стъпката има смисъл в стратегии, при които центърът за данни, опорната мрежа и Интернет са все още изцяло IPv4, а интелигентният дом е IPv6 базиран.
Технически ограничения:

Входящи параметри:

$id**= ‘$CE_i$’, **$model=’cisco2821’;

Проверки:

1. Проверка дали IPv6 е конфигуриран на устройство CE_i:

   count(//graphml/graph/node[contains(@id,$id)]/data[@key='ipv6Forwarding' and . =’YES’]) = 1

2. Проверка дали IPv6 е конфигуриран на интерфейса, сочещ към клиента:

   count(//graphml/graph/edge[contains(@source,$id)]/data[@key='ipv6Forwarding' and .=’YES’]) = 1

Бизнес ограничения :

Likelihood = Medium, IMPACT=Low =>Risk=LOW

Cost = $2280 - Цената включва разходи само за труд (57 човеко часа по $40 на час) и е определена на база на допускането, че IR устройствата поддържат NAT46/ NAT64 и няма допълнителни разходи, свързани с подмяна на устройства или обновяване на софтуера на съществуващите.

Preparation Time = 40h, Lab Testing Time = 16 h, Maintenance Window Time = 1h – стъпката не отнема много време, ако бъде изпълнена за едно устройство. Разбира се очакванията са това да не бъде така и тя да бъде изпълнена върху много устройства. В такъв случай времето за изпълнение в живата мрежа (Maintenance Window Time) следва да се умножи по броя на устройствата.

Действие:

Входящи параметри:

###vars: username=user, password=pass, $ipv6prefix=’ 2001:DB8::/96’, $ipv4prefix=’ 11.11.11.11’, $NNI=’Fa1/0’, $UNI=’Fa1/1’;

Шаблон:

read_until('(login:|user:|Username:)',3)

$username

read_until('(Password:|password:)',3)

```
$password
### start read_until('.*#',3)
set cli  screen-length 0
configure terminal
ipv6 nat v6v4 source $ipv6prefix $ipv4prefix
interface $UNI
ipv6 nat
interface $NNI
ipv6 nat
### stop read_until
exit
### exit
```

Ефект:

Ефектът се състои в две проверки спрямо преходното състояние. Първият ред проверява дали NAT-PT работи на ниво устройство, а вторият дали NAT-PT е конфигуриран на ниво интерфейс.

Входящи параметри:

$id= ‘$CE_i$’

Проверка:

```
count(//graphml/graph/node[contains(@id,$id)]/data[@key='ipv6NatPt' and . =’YES’]) = 1
count(//graphml/graph/edge[contains(@source,$id)]/data[@key='ipv6NatPt' and .=’YES’]) = 2
```

4.5 Стратегии за преход от IPv4 към IPv6 чрез преминаване през междинно състояние “Building Automation in Production"

Всяка една от изложените стратегии цели да постигне пълен преход от IPv4 към IPv6 чрез преминаване на междинно състояние „Building Automation in Production”, съответстващо на осъществяването на услугата „Интелигентен дом“ в мрежата на оператор X.

4.5.1 Допускания:

- Цената на хардуера за подмяната на P е $500000.

- Общата цена на хардуера за добавянето на един PE маршрутизатор е $160000.

4.5.2 Определяне на бизнес ограниченията на база на анкета

Един от основните проблеми, свързани с прехода от IPv4 към IPv6 е липсата на ясен механизъм за оценка на бизнес ограниченията, свързани с изпълнението на всяка една от стъпките в дадена стратегия. Проблемът донякъде се състои във факта, че за да бъде дадена достатъчно точно определение, трябва да е ясен контекста, в който ще бъде изпълнена дадена стратегия.

За определяне на бизнес критериите за всяка една от стратегиите, част от настоящата теза, бе направена анкета с експерти от различни представители на бизнеса, свързани с мрежовите технологии. Анкетата се състоеше данни за от:

- Контекста на оператор X;
- Диаграми на първоначалното и желаното състояние на мрежата;
- Описание и диаграми на стратегиите за преход.

Всеки един от анкетираните трябваше да попълни таблица с бизнес ограниченията за всяка една от стъпките на стратегиите. Бизнес ограниченията бяха дефинирани като риск, цена и време.

Цената бе изразена в щатски долари.

Рискът в числови стойности, а именно:

- Note = 0;
- Low = 1;
- Medium = 2;
- High = 3;
- Critical = 4.

Времето е разделено на периоди за:

- подготовка (Time for Preparation);
- тестване в лаборатория (Time for lab testing);
- изпълнение на стъпката върху живата мрежа (Maintenance Window).

Сред анкетираните имаше хора на инженерни позиции в телеком оператори и доставчици на услуги, представители на системните интегратори и на производителите на оборудване. Сред инженерите по Телекомуникации, които попълниха анкетата са:

инж. Тодор Емануилов – Началник отдел „Service IP and Corporate Solutions" в Cosmo Bulgaria Mobile, България

инж. Сезен Анефи – Sr. IT Consultant в „Intracom Svyaz", Русия

инж. Георги Рибарски – Senior Expert Analysis and Design в „Telelink", България

eng. Jovica Djordjevic – Solution & Product Manager IP в „Huawei Technologies", Германия

инж.Николай Манолов – Princial Engineer в „Juniper Networks", Великобритания

инж. Злати Петров – Инженер по телекомуникации и изпълнителен Директор SNT Bulgaria

инж. Мартин Колев – Инженер по телекомуникации и Изпълнителен Директор TFN-T

Множество мнения бяха събрани и чрез публикуването на анкетата в социалната мрежа Linkedin и по специално в професиналните групи, свързани с прехода към IPv6.

4.6 Стратегии

Стратегиите са последователности от стъпки, отговарящи на конкретни бизнес и технически ограничения.

4.6.1 Преход към IPv6 чрез stateless NAT64 и пълна подмяна на IPv4

Това е стратегия, позволяваща бърз, цялостен преход към IPv6 на цялата IPv4 инфраструктура. В стратегията е заложена първоначална подмяна на оборудването, което не "говори" IPv6, цялостна трансформация на обновената инфраструктура към IPv6, въвеждане на "stateless" IP, ICMP NAT64 механизъм за комуникация със съществуващите IPv4 мрежи. След като мрежата бъде мигрирана и свързана със съществуващия IPv4 Интернет, следва въвеждането в експлоатация на услугата "Интелигентен дом". Последната стъпка на стратегията е изместена далеч в бъдещето и ще се състои в

отстраняване на механизъма за превод на адреси към/ от IPv4 в момент, когато мрежите бъдат само IPv6. След изпълнението и на тази стъпка мрежата ще достигне желаното състояние “IPv6 - IPv6 Only”.

Стъпките и състоянията на тази стратегия са представени подробно в точка 4.4.1 в Глава 4 от настоящата дисертация.

Таблица: 4-3 Бизнес ограничения (Business Constraints) на стратегията за преход към IPv6 без двоен IP стек

Step	Target State	Risk	Cost	Time periods		
				Preparation	Lab testing	Maintenance window
Replace P	Network IPv6 Capable	3	523750	110	31	7
Add 2PE router	Network Extended	3	339645	82	32	10
Enable IPv6 BGP Peering	Enable IPv6 BGP	2	4345	34	18	4
Enable NAT46/64 on IR	Network able to translate between IPv6 and IPv4	2	6260	44	32	5
Replace IPv4 with IPv6	IPv6 only network able to communicate to IPv4 through NAT46/NAT64	3.2	13565	98	28	11
Add HG	Building Automation in production	1	2670	36	18	2
Disable Stateless NAT64/NAT46 on IR1	IPv6 only	2	3480	31	15	5

Стратегията би била подходящ избор, ако са налични следните ограничения:

- Промените в опорната мрежа са позволени и възможни.
- Има първоначално наличен бюджет за разширения на мрежата и за подмяна на устройствата, които не поддържат IPv6.
- Няма точно фиксиран срок за въвеждането в експлоатация на новата услуга (т.е “Интелигентният дом” може да почака).
- Сравнително високи нива на риск са допустими.
- Транслацията между IPv4 и IPv6 е допустима.
- Двойният IP стек е нежелан механизъм за голяма част от възлите в мрежата (т.е. допустим е само там където има транслация на адреси).
- Изграждането на тунели е нежелано.

4.6.2 Преход към IPv6 чрез изграждане на тунели и двоен IP стек

Това е стратегия, позволяваща кратки пускови срокове за нови продукти, без поемане на излишни рискове и с минимални първоначални инвестиции. В стратегията е заложена миграция към IPv6 чрез използване на двоен IP стек на слоя за достъп, центъра за данни и зоната за достъп до Интернет. Опорната мрежа остава непроменена и поддържа само IPv4. Поради тази причина се налага използването на 6to4 или 6over4 тунели между всички останали части на мрежата и през опорната мрежа. Налагането на подобна политика позволява сравнително ранно и "евтино" въвеждане в експлоатация на услугата "Интелигентен дом".

Стъпките и състоянията на тази стратегия са представени подробно в точка 4.4.2 в Глава 4 от настоящата докторантура.

Таблица: 4-4 Бизнес ограничения на стратегията за преход от IPv4 към IPv6 чрез изграждане на тунели и двоен IP стек

Step	Target State	Risk	Cost	Time periods		
				Preparation	Lab testing	Maintenance window
Enable dual IP stack on CE, IR, DC	IPv4 + IPv6 on network periphery	2	4980	40	25	8
Enable 6to4 tunnels on CE, IR, DC	Network Periphery IPv6 linked through tunnels	1	2131	27	20	5
Enable IPv6 BGP Peering	Enable IPv6 BGP	2	4345	34	18	4
Add HG	Building Automation in production	1	2088	21	11	2
Replace P	Network IPv6 Capable	3	523731	110	31	7
Add 2PE router	Network Extended	3	339296	82	32	10
Enable dual IP stack (P, PE)	Dual IP stack plus tunnels	2	2088	24	15	6
Disable 6to4 tunnels	IPv4 + IPv6 (пълен двоен стек)	1	1656	24	12	4
Disable dual IP stack	IPv6 only	2	1613	24	12	9

Стратегията за преход към IPv6 чрез двоен IP стек и тунелиране ще бъде удачен избор в случай, че е налична комбинация от следните условия.

- Промените в опорната мрежа са силно нежелани и ако ги има трябва да са с минимално ниво на риск.

- Няма първоначално наличен бюджет за разширения на мрежата и подмяна на оборудването, което не поддържа IPv6. Такъв е планиран в даден бъдещ период.
- Има точно фиксиран и сравнително кратък срок за реализацията на новите продукти и услуги (т.е услугата "Интелигентен дом" трябва да се случи възможно най-скоро и да е успешна, за да има финансови средства за бъдещи разширения на мрежата и за подмяна на старото оборудване).
- Високите нива на риск са недопустими или ако няма как трябва да бъдат за много кратки интервали.
- Двойният IP стек е допустим механизъм.
- Механизмите за превод на адреси са несъвместими с услугите, изисквани от клиента.
- Допустимо е изграждането на тунели.

4.6.3 Преход към IPv6 чрез пълен двоен IP стек

Двоен IP стек на всяко едно мрежово устройство е сред класическите подходи за преход към IPv6. Предложената в настоящата докторантура стратегия спрямо контекста на X, предполага изнесени напред капиталови разходи за подмяна на оборудване и поетапно въвеждане на IPv6 на различните слоеве на мрежата. Миграцията към новия протокол започва от опорната мрежа, преминава през слоя за достъп, след това X се свързва към IPv6 Интернет пространството и накрая бива прехвърлен и центъра за данни. Последователността на тези стъпки не е от съществено значение. Важна в случая е стъпка 1, която гарантира, че мрежата ще бъде способна да работи с IPv6. След като мрежата е изцяло с двоен IP стек, вече може да бъде активирана услугата "Интелигентен дом". Новата услуга е базирана изцяло върху IPv6 и това е пример за стратегия, при която лесно биха се развивали нови IPv6 базирани услуги, а също и старите IPv4 такива.

Стъпките и състоянията на тази стратегия са представени подробно в точка 4.4.3 в Глава 4 от настоящата докторантура.

Таблица: 4-5 Бизнес ограничения на стратегията за преход от IPv4 към IPv6 чрез двоен IP стек

Step	Target State	Risk	Cost	Time periods		
				Preparation	Lab testing	Maintenance window
Replace P	Network IPv6 Capable	3	523731	110	31	7
Enable dual IP stack (all devices)	IPv4 + IPv6	2	8030	53	27	15
Enable IPv6 BGP Peering	Enable IPv6 BGP	1	4345	34	18	4
Add HG	Building Automation in production	1	2088	21	11	2
Add dual-stack PE router	Network extended	3	339932	83	32	10
Disable dual IP stack	IPv6 only	2	3298	28	19	13

Стратегията за преход от IPv4 към IPv6 чрез двоен IP стек би била подходящ избор, ако са налични следните условия:

- промените в опорната мрежа са позволени и възможни;
- няма първоначално наличен бюджет за разширения на мрежата и за подмяна на устройствата, които не поддържат IPv6;
- няма точно фиксиран срок за въвеждането в експлоатация на новата услуга “Интелигентен дом”;
- не са допустими високите нива на риск;
- допустим е двойният IP стек;
- изграждането на тунели е нежелан механизъм;
- преводът на адреси е нежелан механизъм.

4.6.4 Преход към IPv6 чрез превод на адреси и двоен IP стек

Преходът към IPv6 чрез прилагането на комбинация от механизми за превод на адреси и двоен IP стек е един от най-популярните методи за еволюция на IP мрежите.

Стратегията позволява бързо въвеждане на IPv6 в слоя за достъп чрез механизъма за превод на адреси NAT-PT и ранен старт на услугата „Интелигентен дом“. Ранният старт би дал техническо предимство на X пред останалите конкуренти. Техническо предимство би могло да се превърне в пазарно такова, ако услугата е успешна. Приходите от нея биха могли да се използват за инвестиции в ново оборудване (PE_1 и PE_2) и подмяна на съществуващо (P).

Стъпките и състоянията на тази стратегия са представени подробно в точка 4.4.4 в Глава 4 от настоящата докторантура.

Таблица: 4-6 Бизнес ограничения на стратегията за преход чрез NAT и двоен IP стек

Step	Target State	Risk	Cost	Time periods		
				Preparation	Lab testing	Maintenance window
Enable dual IP stack on CE	CE IPv6 Capable	1	1313	16	10	3
Enable NAT-PT on CE	CE able to translate IPv6 to IPv4	1	1633	16	10	3
Add HG	Building automation in production	1	3600	24	16	3
Replace P	Network IPv6 Capable	3	529233	128	33	10
Add 2PE router	Network Extended	3	348783	92	35	11
Enable IPv6 BGP Peering	Enable IPv6 BGP	2	9350	62	28	11
Enable dual IP stack	IPv4 + IPv6	1	6275	38	24	6
Disable NAT-PT on CE	NAT-PT free network	2	1200	16	8	4
Enable NAT46/64 on IR_1	Network able to translate between IPv4 and IPv6	2	2767	16	12	4
Disable dual IP stack	IPv6 only network able to communicate to IPv4 through NAT46/NAT64	2	1400	12	6	6
Disable NAT64/46	IPv6 only	2	1367	10	5	2

Стратегията за преход от IPv4 към IPv6 чрез превод на адреси и двоен IP стек би била подходящ избор, ако са налични следните условия:

- Промените в опорната мрежа са силно нежелани и ако ги има трябва да са с минимално ниво на риск.
- Промените в слоя за достъп са позволени.
- Няма първоначално наличен бюджет за подмяна на оборудването, което не поддържа IPv6. Такъв е планиран за даден бъдещ период..
- Разширенията на мрежата могат да бъдат отложени за даден бъдещ период
- Новата услуга трябва да бъде въведена в експлоатация възможно най-бързо.
- Средните нива на риск са допустими
- Двойният IP стек е допустим.
- Превода на адреси е допустим.
- Недопустимо е изграждането на тунели.

4.7 Оценка на стратегиите и избор на еволюционен път

Оценката на стратегиите се извършва според алгоритъма за избор на еволюционен път, описан подробно в глава 3. За целта първоначално ще бъдат дефинирани критерии за избор, съответстващи на интересите на различни заинтересовани лица от оператора X. След това ще се направят допускания на базата, на които ще може да се остойностят различните критерии.

Намирането на еволюционния път ще започне с предварителни изчисления на всеки един от критериите за избор за всяка една от стратегиите. След това ще се провери дали дадената стратегия отговаря на техническите критерии. Ако това е така, стратегиите ще бъдат подредени спрямо това как те отговарят и на бизнес критериите за оценка. Стратегията победител ще е тази, която отговаря на техническите критерии и е най-близка до изискванията на бизнеса.

4.7.1 Критерии за оценка и формули за тяхното изчисляване

Технически критерии:

- Преходът от IPv4 към IPv6 не може да се извърши чрез използване на механизми за тунелиране.
- Допустимите механизми са двоен IP стек и превод на адреси

Бизнес критерии:

- Минималното време за прекъсване на мрежата до достигне на състояние “Building Automation In Production” .
- Ако две или повече стратегии имат едно и също време, то тогава се разглежда цената за достигане на състояние „Building automation in production”.
- Ако цените са еднакви, то се сравняват стойностите на максималния риск.
- Ако и те са еднакви, се взема под внимание крайната цена за достигане до желаното състояние (IPv6 only).
- Ако и цената на стратегиите съвпада се взема под внимание средното ниво на риска.

$$Ma\,\text{int}\,enanceTimeToState > TotalCostToState > MaxRiskToState > TotalCost > AverageRiskToState$$

Формулите за изчисление на тези параметри са представени в Глава 4, част 4.5.2.2.

4.7.2 Предварителни оценки на стратегиите за миграция от IPv4 към IPv6

На база на предварителните оценки на критериите, представени в Глава 4 част 4.5.3 за всяка една от стратегиите, може да се направи следното обобщение:

- Стратегията за пълна миграция от IPv4 към IPv6 не използва технологии за изграждане на тунели с цел предаване на трафик между IPv4 и IPv6, следователно тя е подходящ кандидат за еволюционен път.
- Стратегията с изграждане и двоен IP стек не отговаря на техническите изисквания и отпада от по-нататъшния процес по избор на еволюционен път.
- Стратегията за преход от IPv4 към IPv6 чрез пълен двоен IP стек отговаря на техническите изисквания за липса на механизми с изграждане на тунели за предаване на трафик.
- Стратегията за преход от IPv4 към IPv6 чрез механизми за превод на адреси и двоен IP стек отговаря на техническите изисквания и е потенциален кандидат за еволюционен път.

След изчислението на еволюционните бизнес критерии и оценката на техническите критерии се получава следната таблица. Стратегия номер 2 за преход чрез изграждане на

тунели и двоен IP стек не отговаря на техническите критерии. Стратегии номер 1, 3 и 4 отговарят на техническите критерии и са потенциални кандидати за еволюционен път.

Таблица: 4-7 Пресмятане критериите за избор на стратегиите за трансформация на мрежата на X от IPv4 към IPv6

Strategy	Max Risk to State Building automation In production	Average Risk to IPv6 only	Total Cost To Building Automation in Production (USD)	Total Cost (USD)	Maintenance Time To State (days)
1	3.2	3.2	890235	893715	5.0
2	***1.8***	***2.8***	***13544***	***881928***	***2.275***
3	2.8	2.8	538194	881424	3.55
4	**1.4**	**2.8**	**6546**	**906920**	**1.3**

Последната фаза на алгоритъма е оценка на бизнес критериите. Според заданието MaintenanceTimeToState трябва да има минимална стойност и е с най-висок приоритет, а след него се нарежда TotalCostToState.

Сравнението показва, следното:

MaintenanceTimeToState(4)=1.3 < MaintenanceTimeToState(3)=3.55 <MaintenanceTImeToState(1) = 5.0
TotalCostToState(4)= **6546**< TotalCostToState(3)= 538194< TotalCostToState(1) = 890235

Следователно стратегия 4 (Преход чрез превод на адреси и двоен IP стек) отговаря най-точно на критериите за избор, наложени от заинтересованите лица на X и е стратегията, избрана за еволюционен път в мрежата на оператор X.

В глава четири е приложен подхода на автора върху контекста на оператора X. Дефинирани са начално и желано състояние на мрежата на X. Началното състояние се състои от устройства изцяло работещи с IPv4, а крайното - с устройства изцяло работещи на IPv6. Преходът между двете състояние може да се извърши на множество стъпки. За всяка една стъпка са определени технически и бизнес ограничения, действие и ефект. Стъпките са групирани в стратегии. Всяка една от стратегиите е подходяща при определени изисквания от страна на заинтересованите лица и е потенциален кандидат за еволюционен път. Авторът е предложил четири стратегии за преход от IPv4 към IPv6.

Една от тях отговаря най-добре на критериите на заинтересованите лица. Това е стратегията, по която мрежата на X ще еволюира от IPv4 към IPv6.

Глава 5: Прототип на система за трансформация на мрежата от IPv4 към IPv6

Сред основните цели на настоящата докторантура е създаването на софтуерен прототип способен да подпомогне мрежовите инженери и архитекти в процеса на трансформация на дадена мрежа от IPv4 към IPv6.

Основната цел на прототипа е да разкрива автоматично настоящето състояние на мрежата и да го променя, изпълнявайки действията от стъпките на стратегията, избрана за еволюционен път. Прототипът трябва да дава възможност на мрежовите архитекти и инженери да имат достоверна информация за топологията на мрежата на различни нива от OSI модела. Също така той трябва да предоставя информация за видовете интерфейси между устройствата и за самите устройства. Друго основно изискване към прототипа е да предоставя възможност за визуализация на разликите между две състояния на ниво топология.

Основното приложение на прототипа е в автоматизиране на прехода от IPv4 към IPv6, но той може да бъде използван в бъдеще и за редица други приложения. Примери за подобни може да са масова подмяна на оборудване, въвеждане на нови услуги, разширения, реорганизации и подмяна на параметрите на съществуващи услуги в реални мрежови инфраструктури.

5.1 Алгоритъм за разкриване на настоящето състояние на мрежата

Алгоритмът за разкриване на топологията е демонстриран на фигури 5-3 и 5-4 от Глава 5 и има за цел да открие всички IP/Ethernet устройства и връзките между тях в мрежовата инфраструктура на доставчика на услуги.

Процесът по разкриване на мрежата се изпълнява върху първоначално разкритото устройство. След това се изпълнява върху съседните устройства и след това на техните съседни устройства и така, докато не бъде разкрита цялата мрежа или докато не бъдат

изпълнени критериите за ограничение на процеса. Алгоритъмът има вграден механизъм, който предпазва от повторно изпълнение върху едно и също устройство.

Разкриването на топологията на мрежата става по следните методи:

- CDP (Cisco Discovery Protocol) е протокол за разкриване на Cisco към Cisco между съседски отношения на слой 2 от OSI модела. Методът използва данните от CDP SNMP MIB.
- LLDP (Local Link Discovery Protocol) е протокол за разкриване на междусъседски отношения в Ethernet среда, стандартизиран от IEEE.
- STP (Spanning Tree Protocol) е мрежов протокол стандартизиран от IEEE в 802.1d. Протоколът няма за цел разкриването на устройства, но тъй като създава отношения с директно свързаните съседи на ниво 2 от OSI модела, то той се използва от алгоритъма за разкриване на мрежата.
- MACtoARP (Media Access Control to Address Resolution Protocol) – методът се основава на намиране на отношението между bridge, MAC и ARP SNMP таблици.

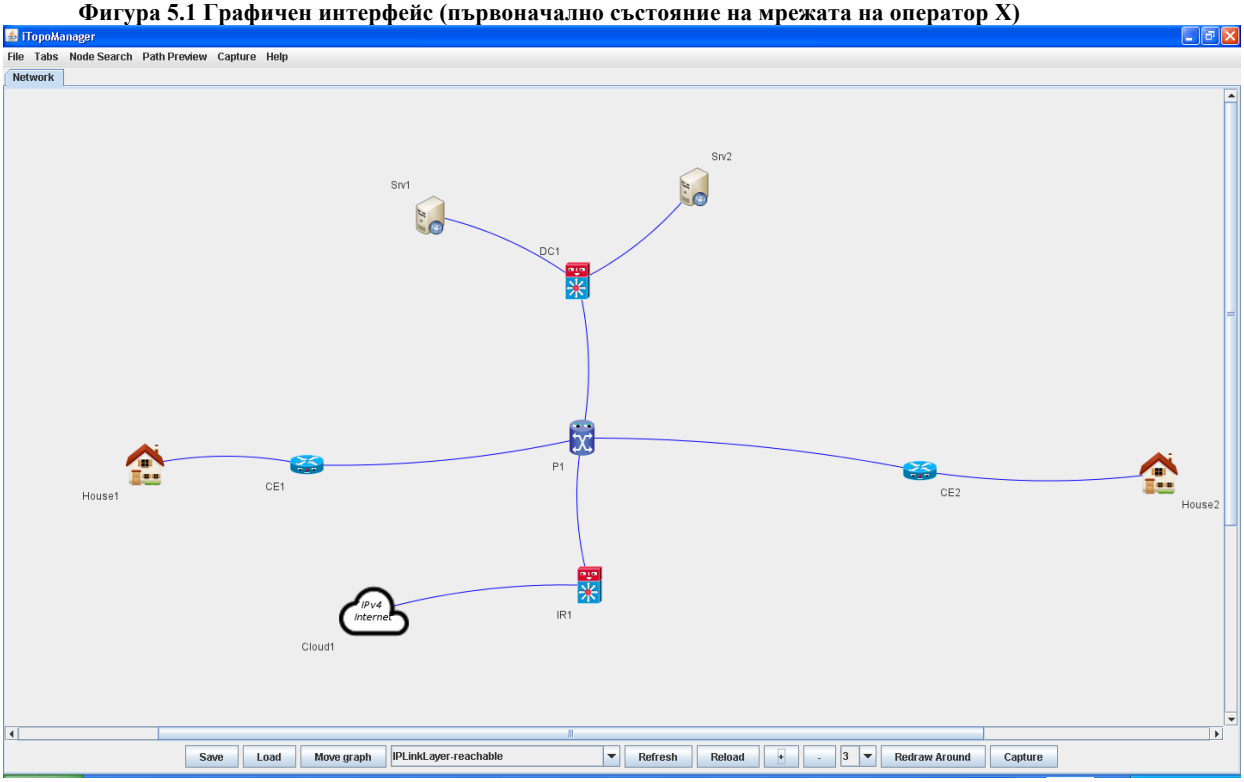
5.2 Съхранение на състоянието на мрежата

Втората основна цел на прототипа е да попълни различни модели с данните от разкритата инфраструктура. В дисертацията са създадени и подробно описани три модела - йерархичен, релационен и графовиден. Йерархичният, обектно-ориентиран модел отговаря на OSS/BSS спецификациите за SID и може да бъде съхраняван в XML структура или да бъде попълнен в релационна база данни. От него чрез XSLT трансформация се генерира графовидния модел. Той отговаря на текущото състояние на мрежата.

5.3 Визуализация на топологията на мрежата

Третата цел на прототипа е да визуализира мрежовата топология чрез динамичен графичен интерфейс (Фигура 5.1).

Фигура 5.1 Графичен интерфейс (първоначално състояние на мрежата на оператор X)



5.4 Изпълнение на стъпките от стратегията

Последната цел на прототипа е моделиране и изпълнение на стъпките от стратегията, избрана за еволюционен път, и генериране на визуално изображение с разликите между предходното и настоящето състояние на мрежата след изпълнението на всяка стъпка.

Последователността от действия при изпълнението на стъпка е:

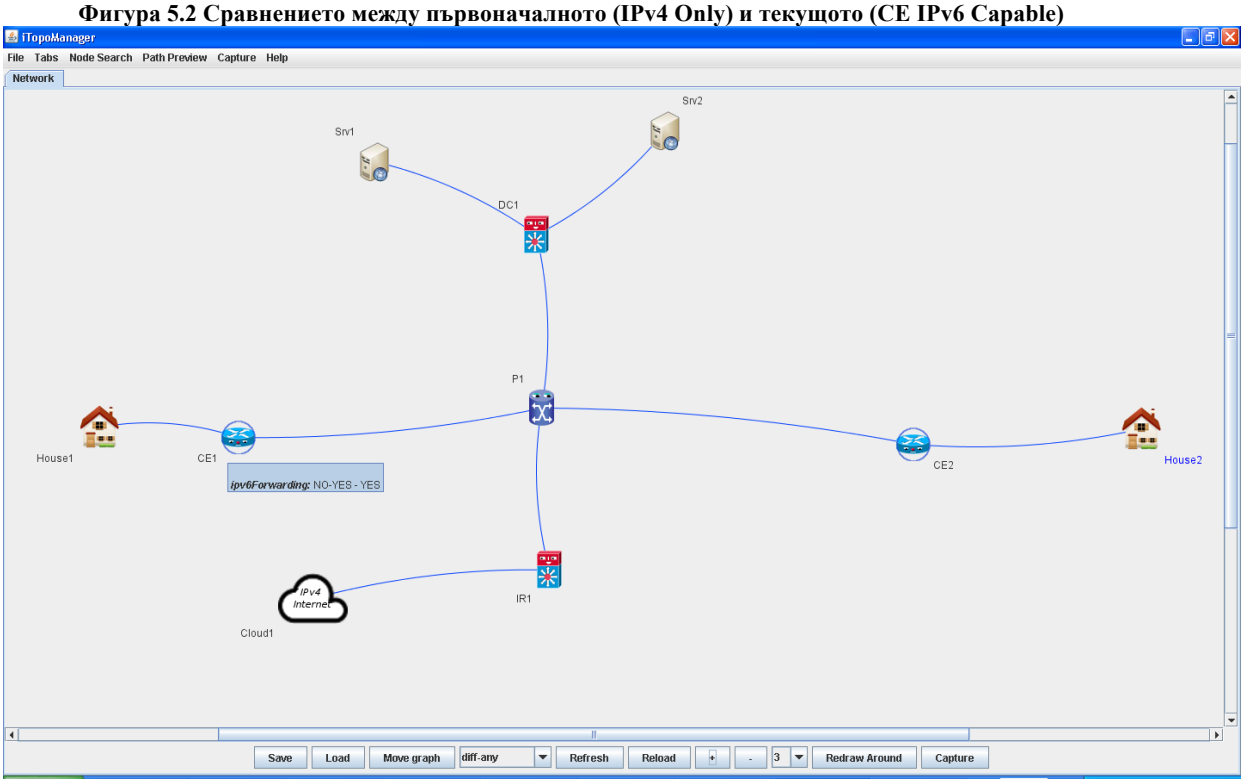
1. Подаване на входящи параметри. Параметрите може да бъдат подадени чрез въвеждане във входяща форма, да бъдат автоматично извлечени от текущия граф или от йерархичния модел.
2. Изпълнение на проверките от техническите ограничения. Ако техническите ограничения са изпълнени, се преминава към следващата стъпка. Ако не са изпълнени се прекратява изпълнението на стъпката.
3. Изпълнение на действието.
4. Разкриване на текущото състояние на мрежата.

5. Представяне на разликите между първоначалния модел на мрежата и модела на текущото състояние.
6. Проверка на ефекта от действието.

5.5 Еволюция на мрежата на X от състояние “IPv4 only” до състояние “IPv6 only”

В глава 5 част 5.8 е демонстрирано действието на прототипа и разликите между различните състояния при прилагане на стратегията „Преход към IPv6 чрез превод на адреси и двоен IP стек“ върху мрежата на X. За всеки две състояние е визуализирана разликата между топологиите на предходното и текущото състояние подобно на Фигура 5-2.

Фигура 5.2 Сравнението между първоначалното (IPv4 Only) и текущото (CE IPv6 Capable)



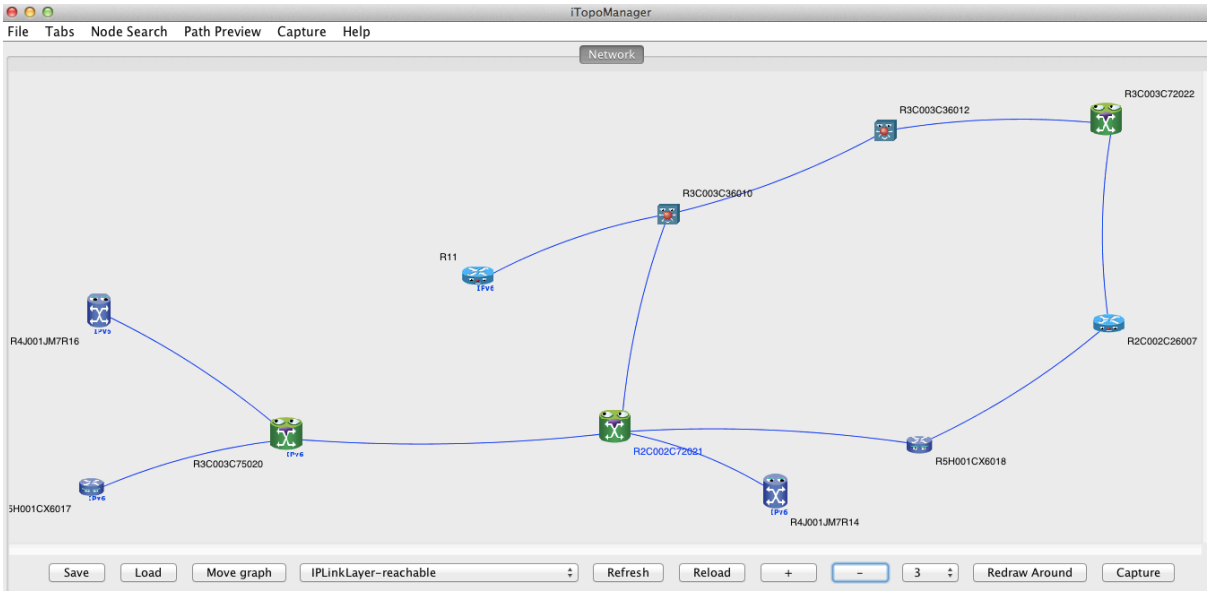
Глава 6: Разработени програмни системи

6.1 Прототип на система за трансформация на мрежи

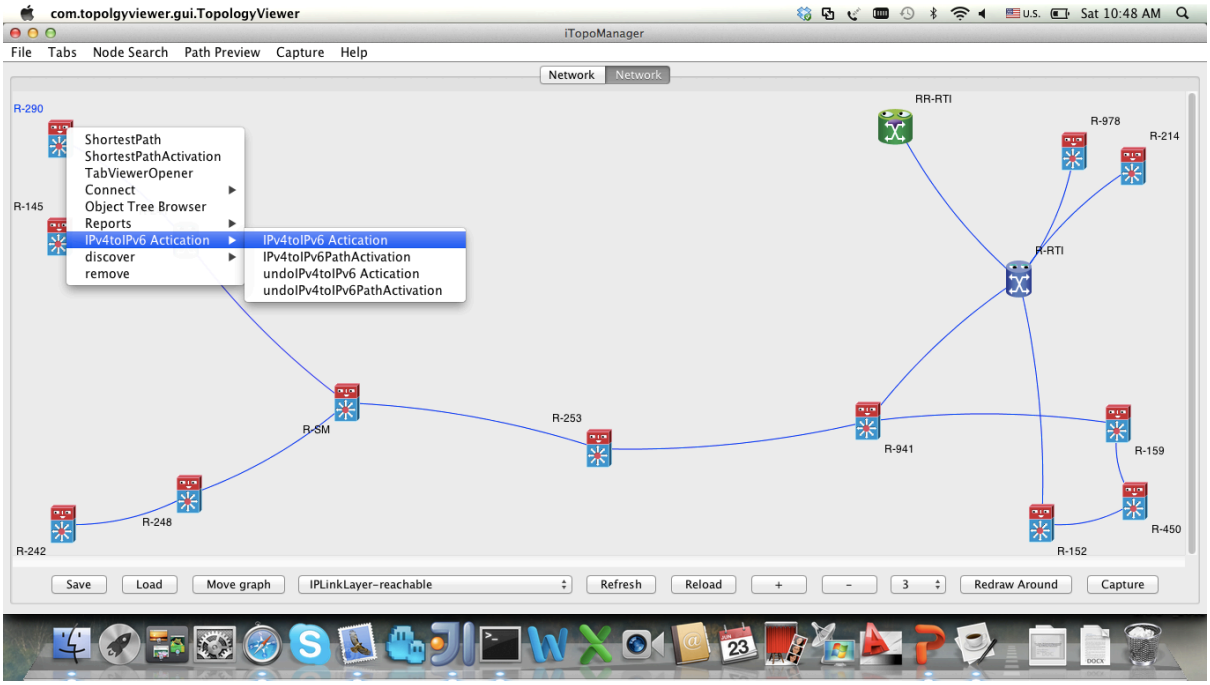
През последната половин година, разработения от автора прототип бе разпространен и приложен в мрежовите инфраструктури на множество оператори и бизнес организации.

Изгледи от различни реални мрежови топологии са демонстрирани на фигури Фигура 6.1 - Фигура 6.6. С цел гарантиране сигурността на отделните организации, имената и адресите от реалните устройства са подменени с други – автоматично генерирани такива.

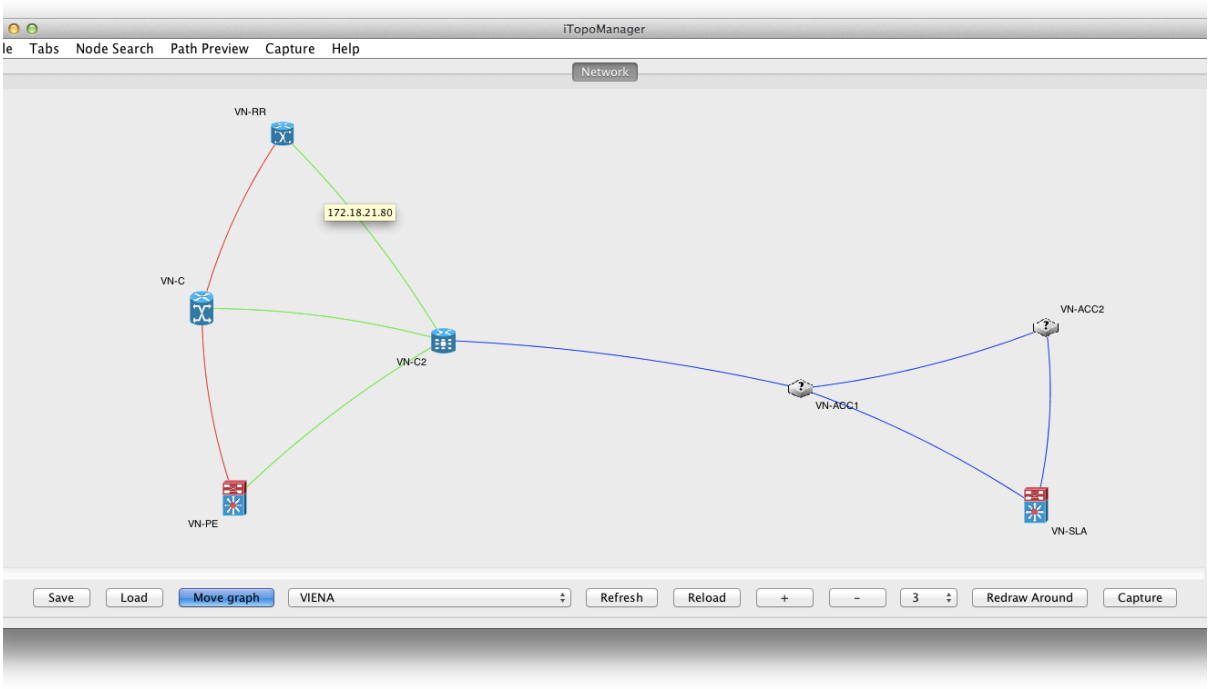
Фигура 6.1 Мрежа с оборудване на Cisco, Huawei, Juniper – филтър по IP свързаност



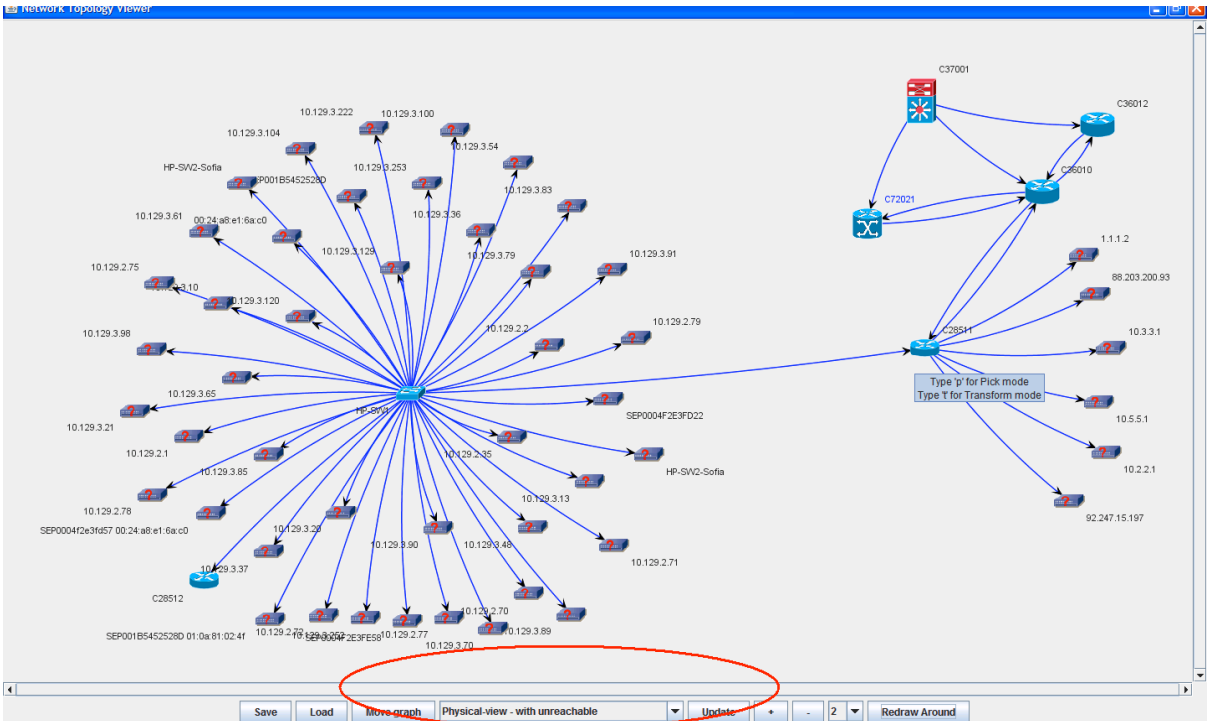
Фигура 6.2 Мрежа съставена от CISCO 76xx, RR-RTI и R-RTI са BGP route-reflectors и са на друг производител на техника (Riverstone)



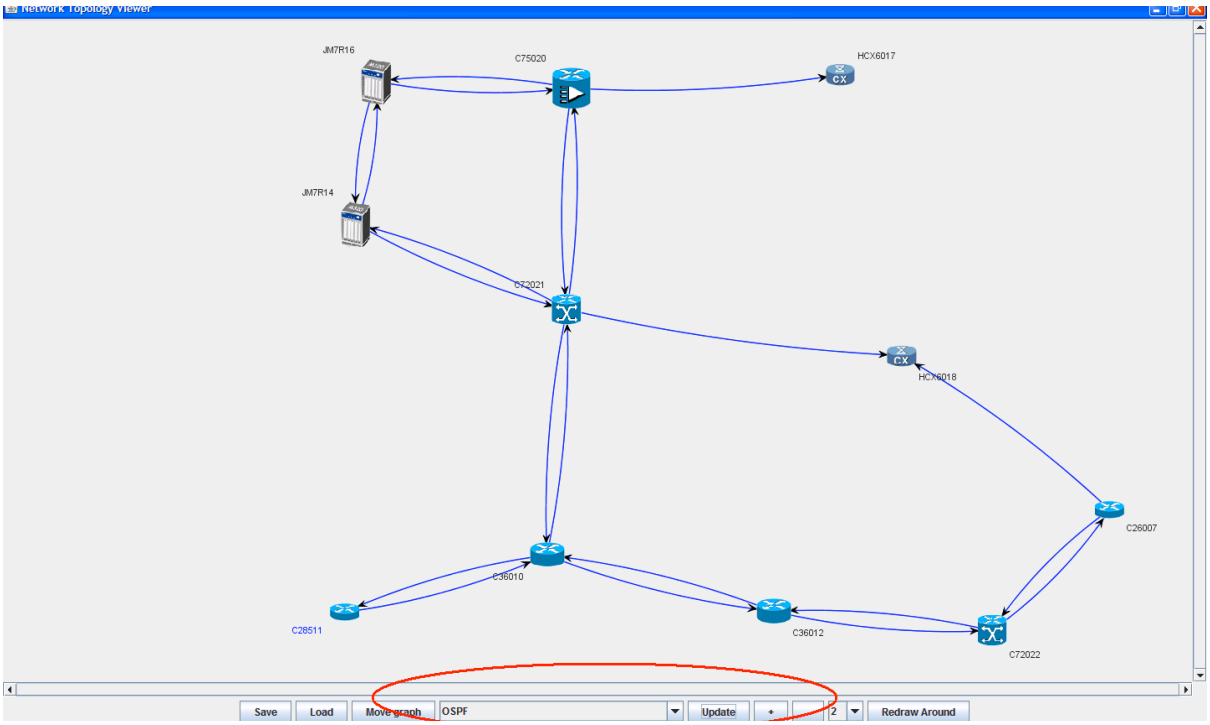
Фигура 6.3 Филтриране по местоположение (показани са устройствата във Виена)



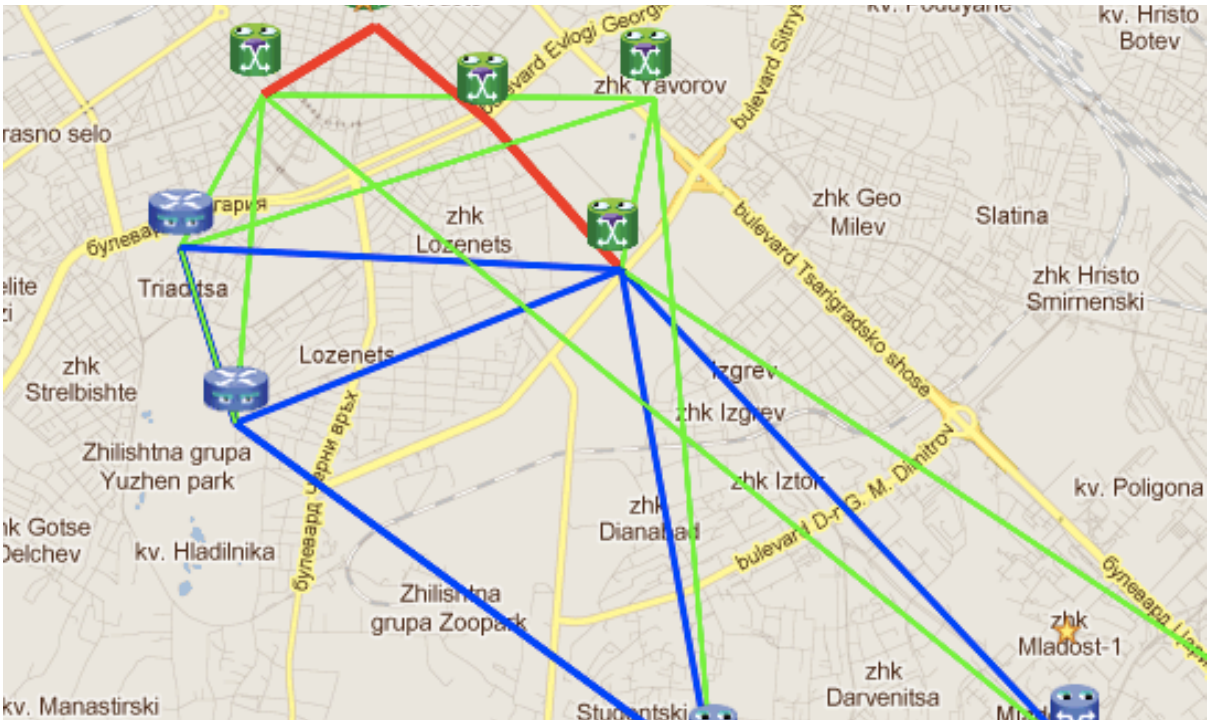
Фигура 6.4 В топологията са включени мрежовите и разкритите крайни устройства (компютри или модеми)



Фигура 6.5 Филтрация по маршрутизиращ протокол - OSPF



Фигура 6.6 Демонстрация на топология върху топографска карта (Google Maps)



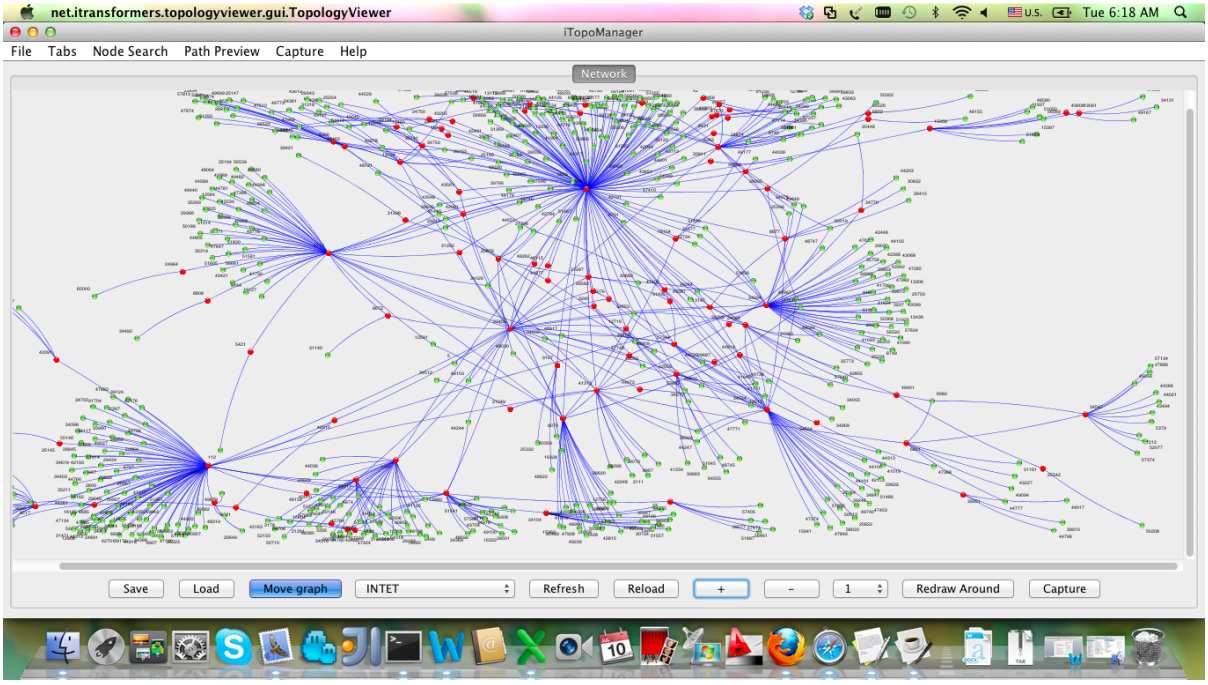
6.2 InternetMap

InternetMap е софтуер, базиран на основния прототип, целящ да създаде карта на свързаността между различните BGP автономни системи на различните доставчици в Интернет. Целта на създаването му бе да покаже че създаденият от Автора механизъм за разкриване на мрежови инфраструктури може да се използва без съществени промени и за генериране на други модели и съответно за изчертаването им.

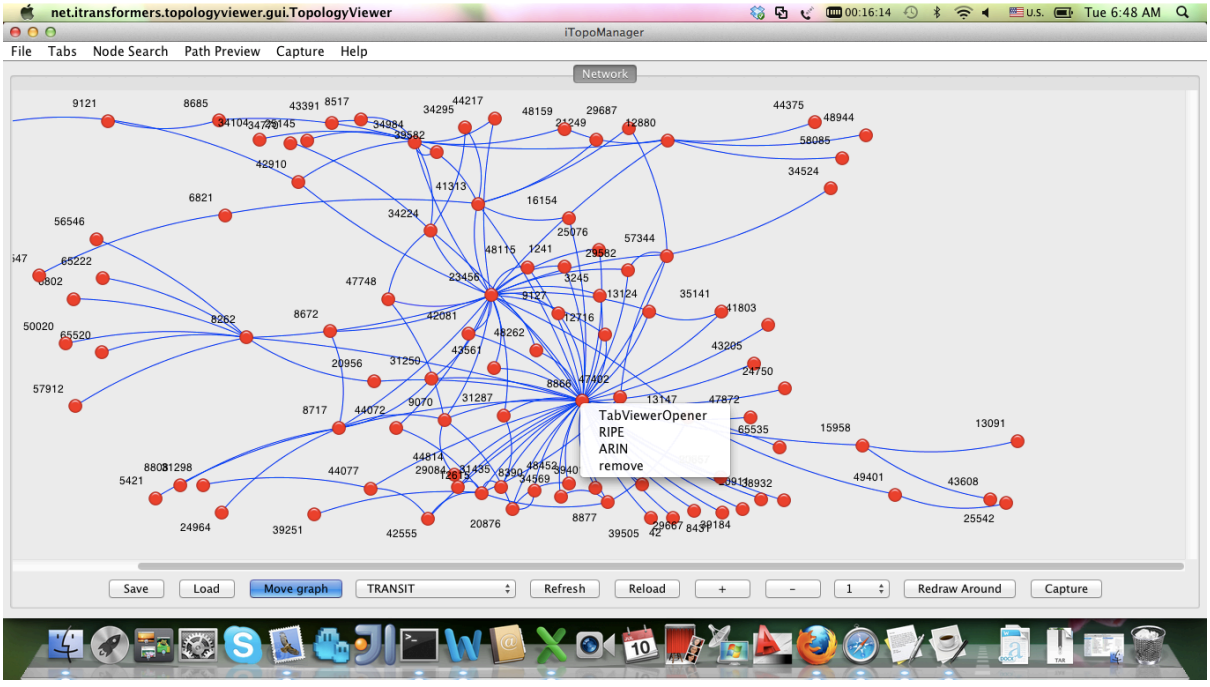
На Фигура 6.7 е демонстрирана карта на Българското Интернет пространство. Червените точки представляват номерата на транзитните автономни системи, а зелените на крайните.

На Фигура 6.8 е демонстрирана същата карта, но е приложен филтър и са оставени единствено транзитните автономни системи. На фигурата е показано и RightClick меню, което има 4 метода. Методите RIPE & ARIN предоставят възможност на потребителя да получи информация за дадената автономна система, за организацията която стои зад нея, за административно отговорните лица и за разпространените от нея IP маршрути в глобалната Интернет таблица.

Фигура 6.7 InternetMap (Bulgarian BG peering)



Фигура 6.8 InternetMap (Bulgarian BG peering – транзитни автономни системи)



Заключение и резюме на получените резултати

В разработения дисертационен труд е отразена литературна справка от български и английски автори и разработки. Резултатите от проучванията показват огромно разнообразие от мрежови технологии и механизми за преход от IPv4 към IPv6. Въпреки това многообразие, преходът не е масова практика, особено при големите доставчици на мрежова свързаност.

Част от проблема с прехода е и наличието на голямо количество софтуер за управление на бизнеса и мрежата, който също трябва да бъде адаптиран към новия протокол.

Проведеният анализ ясно показва необходимостта от разработка на нов подход към прехода от IPv4 към IPv6. Подходът трябва да бъде независим от различните мрежови технологии и да работи еднакво добре с всеки един от механизмите за преход.

В резултат от извършените изследвания и работата по дисертационния труд са получени следните основни резултати от научно-приложен и изцяло приложен характер:

1. Обстойно са изследвани съществуващите мрежови технологии под и над IP слоя, архитектурата на мрежата на съвременен доставчик на услуги, IPv4/v6 протокол, процеса на раздаване на адреси при IPv4 и съответно при IPv6, и механизмите за преход от IPv4 към IPv6.
2. Анализирана е архитектурата на съществуващите системи за управление на мрежата и бизнеса, като са изследвани NGOSS, SID модела, MTOSI, OSS/J. Идентифицирани са възможности за интеграция на системата за еволюция на мрежата със съществуващия OSS/BSS.
3. Предложен е подход за решение на проблема с прехода от IPv4 към IPv6. Подходът разглежда процеса на миграция като преход от едно текущо към друго желано състояние на мрежата.
4. Предложено е прехода да се извърши чрез изпълнение на множество еволюционни стъпки. Всяка една стъпка се състои от технически и бизнес ограничения, действие и ефект върху мрежата. Стъпките може да бъдат групирани в стратегии. Всяка една стратегия може да бъде оценена по дадени технически и бизнес еволюционни

критерии. Предложен е алгоритъм за избор на еволюционния път – стратегията, която отговаря най-добре на зададените еволюционни критерии.

5. Разработени са модели на състоянието на мрежата. Основният моделът е графовиден в graphml формат. Устройствата са представени като възли а връзките като ребра. Всеки един възел и всяка една връзка се характеризира с определени свойства. На базата на елементите и техните свойства мрежата се извършва топологична филтрация и визуализация на топологията на различни нива от OSI модела. Метаданните от моделите се използват като входящи параметри на еволюционните стъпки.
6. Подходът е експериментално приложен върху контекста на оператор X. Условията, в които е поставен операторът X са определени на базата на анализ на ситуацията, в която се намират повечето от съвременните телеком оператори. Дефинирани са първоначално и желано състояние на мрежата. Разработени са множество еволюционни стъпки, съответстващи на различните механизми за преход от IPv4 към IPv6.
7. Предложени са четири стратегии за преход от IPv4 към IPv6. Дефинирани са критерии за избор спрямо контекста на оператор X. Избрана е стратегия, по която да еволюира мрежата на базата на алгоритъма за еволюционния път.
8. Разработен е прототип на системата за еволюция на мрежата. Прототипът е способен да разкрие текущото състояние на мрежата, да попълни модела на състоянието, да се интегрира с останалите OSS/BSS приложения чрез попълване на актуални данни за мрежата в техните SID модели, да визуализира разликите между две състояния на мрежата и да изпълни стъпките от стратегията.
9. Прототипът има приложно и педагогическо значение и е успешно интегриран в множество телекомуникационни оператори и в курсовете по IP телекомуникационни мрежи и MPLS опорни мрежи от програма Телекомуникации (електронни комуникации) на магистърски факултет на Нов Български Университет.