

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ**

*На правах рукописи*

**УДК 621.396.93**

**МУХИТДИНОВ АВАЗ АДХАМОВИЧ**

**Исследование методов управление сетей следующего поколения NGN**

**5A350101 – Телекоммуникационный инжиниринг**

**Диссертация**

**на соискание академической степени магистра**

**Научный руководитель:**

**Зам.дир., АК «Узбектелеком»**

**филиал «БРМ» А.Кадиров**

**Ташкент 2015**

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА  
КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

**МАГИСТРЛИК ДИССЕРТАЦИЯСИ АННОТАЦИЯСИ**

Факультет ТТ

Кафедра ТРЭТ

Ўқув йили 2014/2015

Магистратура талабаси Мухитдтнов А.А.

Илмий раҳбар Кадиров А.А.

Мутахассислиги 5А350101 –

Телекоммуникация инжиниринги

Магистрлик диссертацияси (NGN) кейинги авлод тармоқларида бошқарув усуллари тадқиқ қилиш долзарб масаласига бағишланган. Диссертация ишида кейинги авлод тармоқлари характеристикалари ва ўзига хос хусусиятлари, тармоқларни бошқариш усуллари комплекс тадқиқотлари ўтказилади. Олинган натижаларнинг аҳамиятлилиги шундан иборатки, олинган натижалар ҳозирги кунда мавжуд тармоқларни бошқариш ва янги қуриладиган тармоқларни бошқарув усуллари ишлаб чиқиш ва тадқиқ қилиш учун ишлатилиши мумкин.

Тадқиқотлар натижалари ТРЭТ кафедрасининг семинарларида, Республика илмий-техник конференцияларида муҳокама қилинган.

Илмий раҳбар \_\_\_\_\_

Магистрант \_\_\_\_\_

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ

Факультет ТТ

Кафедра СТРВ

Учебный год 2014/2015

Магистрант Мухитдтнов А.А.

Научный руководитель Кадиров А.А.

Специальность 5А350101 –

Телекоммуникационный инжиниринг

**АННОТАЦИЯ МАГИСТРСКОЙ ДИССЕРТАЦИИ**

Магистерская диссертация посвящена актуальной задаче исследованию методов управления сетей следующего поколения (NGN) . В диссертации проводится комплексное исследование методов управления сетей следующего поколения, характеристик и особенностей сетей следующего поколения. Значимость работы заключается в том, что полученные результаты могут быть использованы в управление существующей сетей и в выборе и разработки методов управления для новых сетей связи.

Результаты исследований обсуждались на семинарах кафедры «Системы телерадиовещания», на Республиканских научно-технических конференциях.

Научный руководитель \_\_\_\_\_

Магистрант \_\_\_\_\_

MINISTRY FOR DEVELOPMENT OF INFORMATION TECHNOLOGIES  
AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

Faculty TT

Student Mukhitdinov A.A.

Department TRBS

Supervisor of studies Kadirov A.A.

Academic year 2014/2015

Speciality 5A350101 – Telecommunication  
Engineering

**SUMMARY OF MASTER DISSERTATION**

The master thesis is devoted to an actual problem of research management methods of next generation networks (NGN). The thesis conducted a comprehensive study of management of next generation networks, characteristics and features of next generation networks. The significance of the work is, that the results obtained may be used in the management of existing networks and in the selection and development of new methods for the control of communication networks.

Results of researches were discussed at seminars of Systems of TV and Radio Broadcasting chair, at Republican scientific and technical conferences.

Supervisor of studies \_\_\_\_\_

Student \_\_\_\_\_

## Оглавление

### Введение

#### **Глава I. Принципы построения сетей следующего поколения (NGN)**

1. Особенности сетей следующего поколения
2. Сети следующего поколения: услуги и архитектура
3. Сети следующего поколения, сетевые параметры и основные протоколы NGN

#### Выводы по Главе I

#### **Глава II. Управление сетями в сетях следующего поколения (NGN) и широко используемые протоколы маршрутизации в NGN**

1. Основы управления сетями, стандарт TMN.
2. Протокол SNMP для управления сетями связи
3. Протоколы маршрутизации Open Shortest Path First (OSPF), Multiprotocol Label Switching (MPLS).

#### Выводы по Главе II

#### **Глава III. Построение экспериментальной модели сети NGN, сравнения программных обеспечений и выбор наилучшего метода управления**

1. Построения экспериментальная модель NGN с маршрутизаторами Cisco 7200 на эмуляторе GNS3
2. Сравнения программного обеспечения Cacti и Mrtg, SNMPc и NetXMS.
3. Выбор метода управления централизованный или децентрализованный, Исследования нового метода.

#### Выводы по Главе III

## Введение

Телекоммуникации в настоящее время испытывают поистине революционное развитие. Это наглядно видно на примере сетей следующего поколения. Традиционные сети связи характеризуются узкой специализацией, для каждого вида связи существует отдельная сеть, которая требует собственной разработки и технического обслуживания. При этом свободные ресурсы одной сети не могут использоваться другой сетью. Сети следующего поколения это сеть которое позволяет отказаться от многочисленных наложенных вторичных сетей, обеспечить внедрение новых услуг с различным требованием к объему передаваемой информации и качеству ее передачи. Оператор сети следующего поколения сможет наиболее полно реализовать полосу пропускания для интеграции различных видов трафика и предоставления различных услуг. Пользователь же сможет удовлетворить свои потребности в получении информации любого типа при доступе из любой точки и в любое время. Потребность в создании сетей следующего поколения диктуется сформировавшимся рынком телекоммуникационных услуг.

В настоящее время большинство операторов связи пришли к необходимости создания единой мультисервисной среды для транспортировки и коммутации услуг. Мультисервисная сеть образует единую информационно-телекоммуникационную структуру, которая поддерживает все виды трафика (данные, голос, видео) и предоставляет все виды услуг (традиционные и новые, базовые и дополнительные) в любое время, в любом наборе и объеме.

У нас в стране развитию сетей следующего поколения уделяется особое внимание. В докладе Президента Республики Узбекистан на заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2012 году, И. А. Каримов упомянул что, «все большее значение приобретает ускоренная реализация мер и проектов в сфере

информационно-коммуникационных и телекоммуникационных технологий. Мы должны отдавать себе отчет, что без кардинального, я бы сказал взрывного продвижения по пути широко внедрения во все сферы экономики, в нашу повседневную жизнь современных информационно-коммуникационных систем трудно видеть перспективу. Нам необходимо в кратчайшее время не только устранить имеющее место отставание по многим видам оказания информационных услуг, но и выйти в разряд передовых стран с высоким уровнем внедрения информационно-коммуникационных технологий. Предстоит завершить строительство более 2 тысяч километров волоконно-оптических сетей широкополосного доступа по современной технологии с предоставлением услуг видеотелефонии, Интернет-телевидения, высокоскоростного интернета, просмотра каналов HDTV и других» [1]. В настоящее время Акционерная компания «Узбектелеком» уже предоставляет потребителям комплекс мультисервисных услуг передачи данных, IP-телефонии и IPTV.

Построение сетей следующего поколения и подключение потребительских услуг в настоящее время не представляет особых трудностей, но имеются определенные проблемы с управлением сетью.

#### **Актуальность темы диссертации.**

Сети следующего поколения предоставляют различные виды услуг, которые работает через один конвергентная сеть. Качество обслуживания разнородного трафика обеспечивается путем применения правильного выбора метода управления, в связи с чем, тема данной магистерской диссертации, посвященная исследования методов управления сетей следующего поколения, является весьма актуальной.

#### **Цель и задачи диссертационной работы.**

Цель диссертационной работы - разработка экспериментальной модели сети следующего поколения и разработка метода управления..

Для достижения поставленной цели в работе решались следующие задачи:

- разработка экспериментальной модели фрагмента сети следующего поколения в среде GNS3 с маршрутизаторами Cisco;
- оценка эффективности методов управления централизованный и децентрализованный.

### **Объект и предмет исследования.**

Объектом исследования является мультисервисная сеть связи с реальными маршрутизаторами. Предметом исследования является выбор метода управления.

### **Состояние изучаемого вопроса.**

На сегодняшний день исследования методов управления сетями проводились в среде имитационного моделирования Opnet Modeler, GPSS, Matlab и т.д. Данные среды имитационного моделирования основаны на законах теории вероятностей и дают приблизительные результаты. В доступной технической литературе рассмотрены только принципы работы дисциплин и даны описания, а для решения поставленных задач уделено мало внимания.

### **Научная новизна работы.**

В данной диссертационной работе для исследования методов управления сетей была разработана модель мультисервисной сети для случая реального потока трафика. Функционирование сети осуществлялось в программном среде GNS3 с маршрутизатором Cisco 7200 и программном обеспечением SNMPc для управления сетью. Данный метод является экспериментальным моделированием и дает более точные результаты по сравнению с имитационным моделированием.

### **Практическая ценность работы.**

Практическая ценность работы заключается в том, что рассматриваемый в данной работе метод исследования может быть

использован при проектировании, модернизации и оптимизации сетей передачи данных.,

### **Апробация результатов работы.**

Результаты диссертационной работы в двух частях были доложены на Республиканской научно-технической конференции «Ахборот технологиялари ва телекоммуникация муаммолари» в марте 2015 года и одна статья была доложена на газете «Xabar».

### **Структура построения диссертации.**

*Диссертация состоит из введения, трех глав, заключения и списка использованной литературы. Работа изложена на 77 страницах, иллюстрирована 61 рисунком и содержит 4 таблицы. Список использованной литературы включает 27 наименований.*

### **Содержание работы:**

**В первой главе** диссертации произведен особенности сетей следующего поколения, услуги и архитектура. Подробно описаны показатели качества мультисервисных услуг. Также, были рассмотрены требования к показателям качества обслуживания для услуг передачи данных, голоса, интерактивного и потокового видео.

**Во второй главе** приведены основы управления сетями, основные протоколы для управления сетями связи. Описаны принцип работы и структура SNMP MIB. Подробно описаны широко используемые протоколы маршрутизации OSPF и MPLS. Структура SNMP MIB

**В третьей главе** было построено экспериментальная сеть с помощью программы GNS3 и маршрутизаторами Cisco 7200. Маршрутизаторы были настроены IPv4 адресами, для маршрутизации были настроены динамическая маршрутизация OSPF, было изучена широко используемые программы для управления сетью Cacti, MRTG, SNMPc, NetXMS. Сделана сравнительная таблица преимуществ и недостатки этих программ, было выбрана централизованный метод для управления с кластерном и географически

разделенном подключением. Для теста установлена программа SNMPc.  
Схема сети было строена и настроена для управления сетью.

## **Глава I. Принципы построения сетей следующего поколения**

### **1 Особенности сетей следующего поколения**

Современный этап развития мировой цивилизации характеризуется переходом от индустриального к информационному обществу, которое предполагает новые формы социальной и экономической деятельности, базирующиеся на массовом использовании информационных и телекоммуникационных технологий. Технологической основой информационного общества является Глобальная информационная инфраструктура (ГИИ), которая должна обеспечить возможность недискриминационного доступа к информационным ресурсам каждого жителя планеты. Информационную инфраструктуру составляет совокупность баз данных, средств обработки информации, взаимодействующих сетей связи и терминалов пользователя. Доступ к информационным ресурсам в ГИИ реализуется посредством услуг связи нового типа, получивших название услуг Информационного общества или инфокоммуникационных услуг. Наблюдаемые в настоящее время высокие темпы роста объемов предоставления инфокоммуникационных услуг позволяют прогнозировать их преобладание в сетях связи в ближайшем будущем.[17] На сегодняшний день развитие инфокоммуникационных услуг осуществляется, в основном, в рамках компьютерной сети Интернет, доступ к услугам которой происходит через традиционные сети связи. В то же время в ряде случаев услуги Интернет, ввиду ограниченных возможностей ее транспортной инфраструктуры не отвечают современным требованиям, предъявляемым к услугам информационного общества. В связи с этим развитие инфокоммуникационных услуг требует решения задач эффективного управления информационными ресурсами с одновременным расширением функциональности сетей связи. В свою очередь это стимулирует процесс интеграции Интернета и сетей связи.

## Особенности инфокоммуникационных услуг

К основным технологическим особенностям, отличающим инфокоммуникационные услуги от услуг традиционных сетей связи, можно отнести следующие:

- инфокоммуникационные услуги оказываются на верхних уровнях модели OSI (в то время как услуги связи предоставляются на третьем, сетевом уровне);
- большинство инфокоммуникационных услуг предполагает наличие клиентской и серверной частей; клиентская часть реализуется в оборудовании пользователя, а серверная на специальном выделенном узле сети, называемом узлом служб;
- инфокоммуникационные услуги, как правило, предполагают передачу информации мультимедиа, которая характеризуется высокими скоростями передачи и несимметричностью входящего и исходящего информационных потоков;
- для предоставления инфокоммуникационных услуг зачастую необходимы сложные многоточечные конфигурации соединений;
- для инфокоммуникационных услуг характерно разнообразие прикладных протоколов и возможностей по управлению услугами со стороны пользователя;
- для идентификации абонентов инфокоммуникационных услуг может использоваться дополнительная адресация в рамках данной инфокоммуникационной услуги.

Большинство инфокоммуникационных услуг являются «приложениями», т.е. их функциональность распределена между оборудованием поставщика услуги и конечным оборудованием пользователя. Как следствие, функции конечного оборудования также должны быть отнесены к составу инфокоммуникационной услуги, что необходимо учитывать при их регламентации.

Бизнес-модель, определяющая участников процесса предоставления инфокоммуникационных услуг и их взаимоотношения, также отличается от модели традиционных услуг электросвязи, в которой было представлено всего лишь три основных участника: оператор, абонент и пользователь. Новая деловая модель предполагает наличие поставщика услуг, который предоставляет инфокоммуникационные услуги абонентам и пользователям. При этом сам поставщик является потребителем услуг переноса, предоставляемых оператором сети связи. На рынке могут также присутствовать дополнительные виды поставщиков услуг: поставщики информации, брокеры, и т.д. Поставщик информации предоставляет информацию поставщику услуг для распространения. Брокер предоставляет информацию о поставщиках услуг и их потенциальных абонентах, содействует пользователям в поиске поставщиков, оказывающих требуемые услуги. Ритейлер выступает как посредник между абонентом и поставщиком с целью адаптации услуги к индивидуальным требованиям абонента.

К инфокоммуникационным услугам предъявляются такие требования, как:

- мобильность услуг;
- возможность гибкого и быстрого создания новых услуг;
- гарантированное качество услуг. Большое влияние на требования к инфокоммуникационным услугам оказывает процесс конвергенции, приводящий к тому, что инфокоммуникационные услуги становятся доступными пользователям вне зависимости от способов доступа.

Уровень среды обмена информацией находится на третьей плоскости. Функции, выполняемые этим уровнем, включают процедуры установления соединений между пользователями сети и межсетевое взаимодействие.

Типичным примером оборудования, которое реализует эти функции в сети NGN, являются такие устройства как контроллер медиашлюзов MGC, сервер управления обслуживанием вызова Call Agent, привратник Gatekeeper и LDAP-сервер. Уровень доступа и транспорта располагается на четвертой плоскости. Основные функции этого уровня – перенос информации между конечными пользователями сети NGN. В качестве средств доступа в концепции сети NGN рассматриваются практически все используемые в настоящее время варианты, основанные на различных технологиях. К этому уровню относятся такие устройства, как коммутаторы, маршрутизаторы, средства обеспечения качества обслуживания QoS, шлюзы сигнализации, транспортные шлюзы (медиашлюзы), а также шлюзов для мобильной сети радиодоступа стандарта GSM/3G.[3,17] На рисунке 1.1 показано уровневая архитектура NGN.

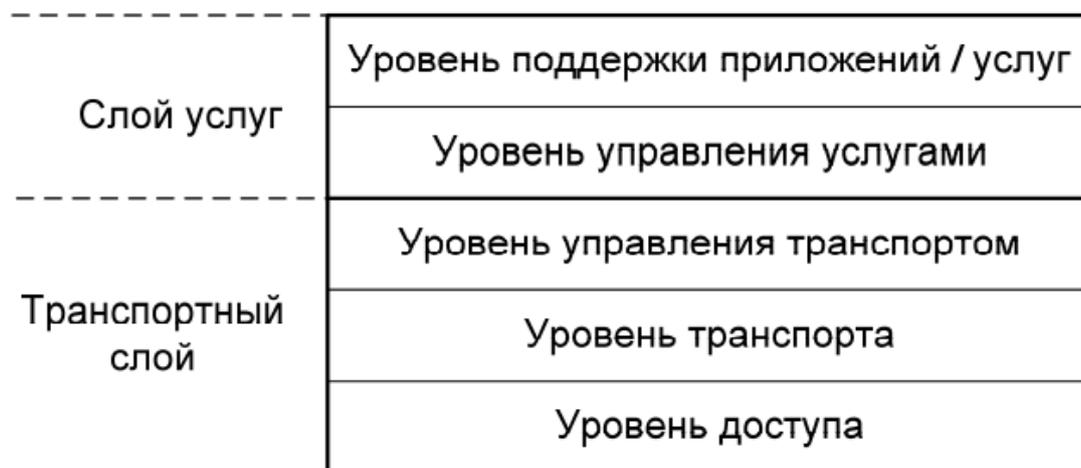


Рис.1.1. Уровневая архитектура NGN

#### Слой услуг NGN

- функции передачи услуги-ориентированных данных (service-related data);
- функции управления и эксплуатационной поддержки ресурсов услуг.

- Транспортный слой NGN:
- функции передачи данных пользователя;
- функции управления и эксплуатационной поддержки транспортных ресурсов.

Уровень доступа (абонентские линии, узлы доступа и системы передачи), Транспортный слой и технологии доступа приведен на рисунке 1.2. Функции уровня доступа:

- подключение конечных пользователей к сети;
- сбор и агрегирование трафика для передачи к
- ядру сети;
- предоставление механизмов управления качеством обслуживания, связанных непосредственно с пользовательским трафиком.

Технология	Среда передачи	Скорость	Максимальное расстояние
HDSL	Медная витая пара	2 Мбит/с, симметричная передача	До 5-8 км в зав. от диаметра медной жилы
ADSL	Медная витая пара	1 Мбит/с от абонента, 7 Мбит/с к абоненту, асимметричная передача	До 5-8 км в зав. от диаметра медной жилы
VDSL	Медная витая пара	10 Мбит/с, симметричная передача	До 1,5 км
PON	Волокно	10 Мбит/с для данных, 2 Мбит/с для телефонии	До 20 км
HFC	Волокно или коаксиал	40 Мбит/с нисходящий поток на группу до 100-500 абонентов	450-500 м между усилителями (без ответвлений)
Wi-Fi	Эфир	До 11/54 Мбит/с	50-100 м
WiMAX	Эфир	До 70 Мбит/с	До 3-5 км в городе, до 50 км на откр. местности
Спутниковая связь	Эфир	До 6 Мбит/с	Не ограничено
ИК-связь	Воздушные слои атмосферы	1-1250 Мбит/с	От 50 м до 3 км
HomePNA	Медная витая пара	1 Мбит/с	150 м
Ethernet / Fast Ethernet	Волокно, медная витая пара	10-100 Мбит/с	100 м (медь), до 2 км (многомодовое волокно), до 150 км (одномодовое волокно)

Рис. 1.2. Транспортный слой: технологии доступа

Коммутатор Softswitch

Коммутатор Softswitch – один из основных элементов NGN. В настоящее время ещё нет ни общепринятого перевода термина “Softswitch” ни точного перечня функций, которые выполняют соответствующие аппаратно-программные средства.[3] Некоторая неясность в перечне тех функций, которые выполняет коммутатор Softswitch, объясняется тем, что концепция NGN еще не полностью сформировалась. В процессе развития телефонии также существовали различные мнения о делении функций между коммутационными станциями и другими видами оборудования (узлами спецслужб, центрами технической эксплуатации, центрами по работе с абонентами и другими). Более того, в процессе цифровизации ТфОП функции аналого-цифрового преобразования перешли из систем передачи в абонентские комплекты коммутационных станций. Различие в принципах построения сетей с коммутацией каналов и пакетов как и одноименных технологий – не позволяет провести простую аналогию между коммутатором Softswitch и оборудованием распределения информации, которое используется в ТфОП. Это объясняется тем, что в коммутаторах Softswitch часто используется комплекс функций, которые в ТфОП распределены между коммутационными станциями, узлами Интеллектуальной сети, средствами обработки сигнальной информации, устройствами управления сетью электросвязи и другими элементами системы. С функциональной точки зрения коммутатор Softswitch можно рассматривать как аппаратно-программные средства для управления вызовами в тех телекоммуникационных сетях, которые используют технологии IP и/или АТМ [18]. Многие Операторы уже используют аппаратно-программные средства, входящие также в состав классического коммутатора Softswitch. Для таких Операторов большое практическое значение имеет распределенное (или модульное) оборудование Softswitch, которое позволяет экономично создавать и развивать IP сеть, приобретая только, отсутствующие аппаратно-программные средства.

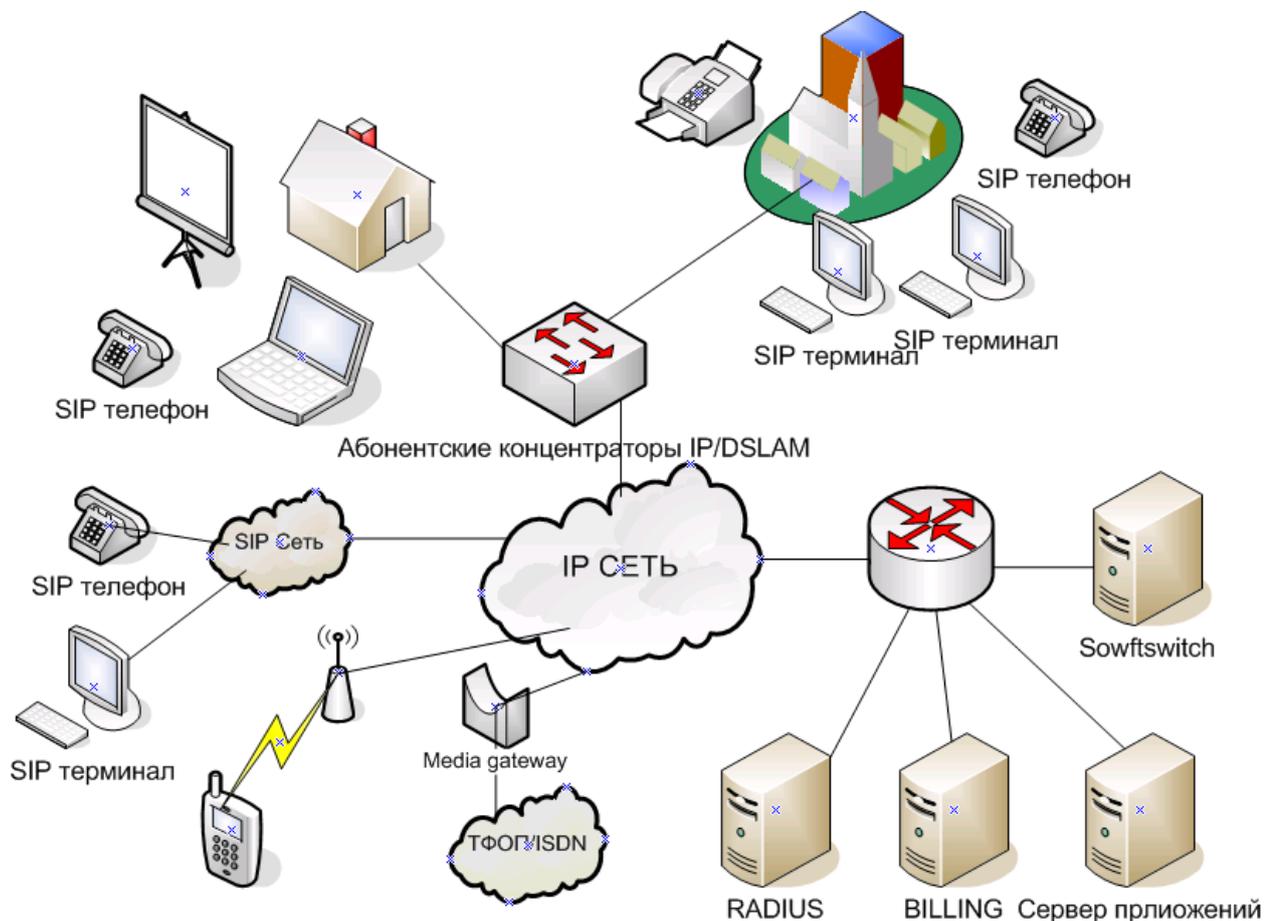


Рис.1.3. – Softswitch в составе системы электросвязи

В первую очередь коммутатор Softswitch управляет обслуживанием вызовов, то есть установлением и разрушением соединений. Точно так, как это имеет место в традиционных АТС с коммутацией каналов, если соединение установлено, то эти функции гарантируют, что оно сохранится (с установленной вероятностью) до тех пор, пока не даст отбой, вызвавший или вызванный абонент. В этом смысле коммутатор Softswitch можно рассматривать как управляющую систему. В число функций управления обслуживанием вызова входят распознавание и обработка цифр номера для определения пункта назначения; а также распознавание момента ответа,

момента, когда один из абонентов кладет трубку, и регистрация этих действий для начисления платы. Таким образом, Softswitch фактически остается все тем же привычным коммутационным узлом, только без цифрового коммутационного поля и абонентских комплектов, что позволяет легко интерпретировать его функции в различных сценариях модернизации телефонной сети общего пользования (ТФОП). Ответственность за перечисленные выше операции, выполняемые коммутатором Softswitch, возложена на входящий в его состав функциональный элемент Call Agent [3].

На рисунке 1.3. изображен коммутатор Softswitch и его взаимодействие с различными существующими и перспективными элементами сетей общего пользования по соответствующим протоколам. Другой термин, часто ассоциируемый с Softswitch, это контроллер транспортного шлюза MGC. Это название подчеркивает факт управления транспортными шлюзами и шлюзами доступа по протоколу H.248 или другому. Softswitch координирует обмен сигнальными сообщениями между сетями, то есть поддерживает функциональность шлюза сигнализации Signaling Gateway (SG). Он координирует действия, обеспечивающие соединение с логическими объектами в разных сетях, и преобразует информацию в сообщениях. Подобное преобразование необходимо, чтобы сигнальные сообщения были одинаково интерпретированы на обеих сторонах несходных сетей, обеспечивая с первого этапа модернизации работу с автоматическими телефонными станциями (АТС) [17].

Архитектура Softswitch. Исторически сложившееся разделение на классы автоматически было перенесено на Softswitch, однако на самом деле это заслуживает внимания только в случае внедрения Softswitch вместо узла с коммутацией каналов. С точки зрения передачи речи по IP-сети (Voice over IP, VoIP) это разделение будет не совсем корректным. При работе по любому сигнальному протоколу VoIP нет различий, например, между SIP-телефоном и Проxy-сервером SIP. Поэтому разделение на транзитные и местные

устройства для Softswitch важно лишь при работе в ТФОП. Эталонная архитектура сетей на базе коммутатора Softswitch, созданная консорциумом IPCC (ныне ISM Forum), состоит из четырех условных функциональных уровней:

- внизу архитектуры находится транспортный уровень (Transport Layer), отвечающий за перенос по VoIP-сети сигнальных сообщений и мультимедийной информации;
- уровень управления вызовами и сигнализации (Call Control & Signaling) управляет основными элементами VoIP-сети, особенно находящимися на транспортном уровне. На этом уровне находятся такие устройства, как контроллеры медиа-шлюзов (MGC, Call Agent, Call Controller), (Gatekeeper) и LDAP-серверы;
- уровень услуг и приложений (Service & Application) обеспечивает управление, логику и выполнение некоторого числа услуг или приложений. Уровень управления (Management) выполняет функции пользовательского обеспечения, поддержки операций и предоставления услуг, а также решает задачи биллинга и прочие задачи сетевого управления;
- уровень управления может взаимодействовать с любым из трех перечисленных уровней, используя стандартные или внутрифирменные протоколы и программные интерфейсы API. Таким образом, при фактическом соблюдении принципа функциональной декомпозиции шлюза можно наблюдать различные варианты его реализации. Первые Softswitch-решения представляли собой единый блок, то есть физической декомпозиции шлюза не было, но существовало разделение функций программных или аппаратных модулей. Иными словами, оборудование имело интегрированную архитектуру. В другом варианте физически отделялся лишь медиашлюз, а контроллер медиашлюзов и шлюз сигнализации составляли единый комплекс.

Такое решение можно считать частичной физической декомпозицией [9].

Применение технологий NGN для организации подключения конечных пользователей ТфОП. Конечными пользователями ТфОП являются:

- абоненты, использующие доступ по аналоговым абонентским линиям;
- абоненты, использующие базовый доступ ISDN;
- абоненты, использующие терминалы, предназначенные для работы в пакетных сетях (SIP и H.323-терминалы);
- УПАТС, подключаемые с использованием первичного доступа ISDN.

Абоненты, использующие аналоговый и базовый доступы, а также УПАТС могут подключаться к сети как непосредственно, так и с использованием доступа интерфейса V5. Решение задачи расширения абонентских подключений в рамках концепции NGN связано с внедрением оборудования гибкого коммутатора (если такое внедрение не было произведено ранее) и оборудования шлюзов доступа. При этом аналоговые и абоненты базового доступа подключаются к пакетной сети через оборудование резидентных шлюзов доступа. Оборудование УПАТС и существующее оборудование абонентских выносов подключается с использованием шлюзов доступа. Вновь создаваемая абонентская емкость может реализовываться на базе SIP и H.323-терминалов, что предполагает создание LAN WAN для подключения абонентов. Очевидными преимуществами решения на основе NGN являются:

- эффективное использование ресурсов первичной сети достигается за счет применения оборудования кодеков на уровне шлюзов. Использование алгоритмов компрессии речи позволяет уменьшить требуемый ресурс в 1,5 и 4 раза в зависимости от типа используемого кодека;

- расширение списка предоставляемых услуг, конвергенция услуг, упрощение процедуры ввода новой услуг. Реализация дополнительных видов обслуживания в сети ISDN требовала их поддержки со стороны всех элементов. В случае создания уровней коммутации и управления услугами мультисервисной сети, новая услуга должна поддерживаться или реализовываться на уровне Softswitch или при взаимодействии с Softswitch. Ограниченное число гибких коммутаторов позволяет достаточно легко реализовывать новые услуги;
- уменьшение эксплуатационных расходов. Смещение сетевого интеллекта в ограниченное число сетевых точек снижает расходы, связанные с обслуживанием и модернизацией оборудования. Использование IP-протоколов в пакетной сети позволяет реализовывать системы управления, мониторинга, сбора статистической информации в рамках ресурсов пакетной сети;
- возможность гибкой тарифной политики. Реализация ограниченного числа точек управления установлением соединения позволяет централизовать систему учета стоимости и обеспечить применение гибких тарифных планов в отношении абонентов всей сети из одной точки. Оборудование Softswitch осуществляет учет стоимости для всех обслуживаемых абонентов. При этом реализация новых тарифных планов осуществляется на уровне Softswitch.

Недостатками решения на основе NGN являются:

- критичность к обеспечению надежности сети. Сосредоточение функций управления в одной точке сети приведет к прерыванию связи для всех обслуживаемых соединений в случае аварии. Решение проблемы потребует разработки системы обеспечения живучести сети с более жесткими требованиями, чем в классической ТфОП;
- достаточно высокие инвестиции на начальных этапах внедрения в условиях уже развитой инфраструктуры ТфОП.



## **2 Сети следующего поколения:**

### **услуги и архитектура**

В основу концепции NGN заложена идея о создании универсальной сети, которая бы позволяла переносить любые виды информации, такие как: речь, видео, аудио, графику и т.д., а также обеспечивать возможность предоставления неограниченного спектра инфокоммуникационных услуг. Базовым принципом концепции NGN является отделение друг от друга функций переноса и коммутации, функций управления вызовом и функций управления услугами. Идеологические принципы построения сети нового поколения следующие:

- в первую очередь, подключение к сети должно быть максимально простым и удобным, без использования промежуточных систем, при этом использование традиционно применяемых протоколов и сервисов должно быть доступно в прежнем объеме;
- во-вторых, сначала строится базовая пакетная транспортная сеть на базе компьютерных технологий, обеспечивающих соответствующее качество, надежность, гибкость и масштабируемость, а потом поверх этой сети строится мощный комплекс сервисов.

В итоге все информационные потоки интегрируются в единую сеть.

Согласно рекомендации ITU-T Y.2001, «Сети следующих поколений структура и функциональные модели архитектуры», сеть последующих поколений определяется, как «сеть с коммутацией пакетов, способную предоставлять услуги электросвязи и использовать несколько широкополосных технологий транспортировки с гарантированным QoS . В этой сети возможность предоставления услуг не зависит от используемых технологий. Она обеспечивает свободный доступ пользователей к конкурирующим сетям и поставщикам услуг, поддерживает универсальную

подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям».

Сети следующего поколения представляют собой результат эволюции всей системы электросвязи. Тем не менее, основной реализацией идеи NGN служит телефонная сеть, единственная из всех существующих сетей, которая:

- обеспечивает диалоговые услуги самой большой группе абонентов;
- приносит Оператору основные доходы.

Для сети NGN характерны существенные особенности, выделяющие ее в новый класс телекоммуникационных систем. Обычно выделяют пять таких особенностей NGN:

- использование пакетных технологий передачи и коммутации для обмена всеми видами информации;
- применение систем коммутации с распределенной архитектурой, которые отличаются от функционально ориентированных телефонных станций;
- отделение функций, которые касаются поддержки услуг от коммутации и передачи;
- обеспечение возможности широкополосного доступа и мультисервисного обслуживания трафика вида “triple-play services” (речь, данные и видео);
- реализация функций эксплуатационного управления (в том числе и тех, что делегированы пользователем) за счет Web технологии.

Передача информации в форме пакетов через NGN существенно отличается от принципов, по которым создана сеть Интернет. В первую очередь, следует выделить поддержку в сети NGN заранее заданных показателей качества обслуживания (QoS – quality of service). Эти показатели

стали определяться для обеспечения качественной телефонной связи через IP сеть – услуг VoIP (Voice over IP), более известных как IP-телефония.

Уровень услуг выделяется в самостоятельный элемент архитектуры сети. Он занимает верхнюю плоскость в рассматриваемой модели. Данный уровень содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую:

- предоставление инфокоммуникационных услуг;
- управление услугами;
- создание и внедрение новых услуг;
- взаимодействие различных услуг.

В какой-то мере, выделение самостоятельного уровня услуг подобно решению, которое предложено в концепции интеллектуальной сети. К этому уровню относятся такие устройства как медиасерверы. Уровень управления располагается во второй плоскости. В модели NGN этот уровень включает совокупность функций по управлению всеми процессами в телекоммуникационной системе, а также начисление платы за услуги связи и техническую эксплуатацию. Для реализации функций, которые выполняет этот уровень, производители телекоммуникационного оборудования разработали аппаратно-программные средства, называемые Softswitch

### Базовые услуги

Под базовыми видами понимаются:

- услуги местной, междугородной, международной телефонной связи, предоставляемые с использованием (полным или частичным) фрагмента сети на основе NGN-технологий. Базовые услуги телефонии в сетях следующего поколения (ССП) могут использовать технологии компрессии речи, при этом качество

предоставления базовых услуг должно соответствовать классам «высший» и «высокий». Базовые услуги телефонии могут быть доступны пользователям, использующим терминалы сетей ТфОП, СПС и H.323, SIP-терминалы;

- услуги по передаче факсимильных сообщений между терминальным оборудованием пользователей. Услуга может предоставляться пользователям, использующим терминалы сетей ТфОП и СПС. Услуга e-fax не относится к данному классу;
- услуги по организации модемных соединений между терминальным оборудованием пользователей. Услуга может предоставляться пользователям, использующим терминалы сетей ТфОП и СПС. Услуга доступа в сети IP не относится к данному классу;
- услуга доставки информации «64 кбит/с без ограничений» и базирующиеся на ней услуги предоставления связи, определенные для технологии ISDN для установления соединений между терминальным оборудованием пользователей. Услуга может предоставляться пользователям, использующим терминалы ISDN. Курс Задачей сетевого фрагмента ССП при предоставлении базовых услуг является установление и поддержание соединения с требуемыми параметрами.

#### Дополнительные виды обслуживания (ДВО)

Предоставление базовых услуг может сопровождаться дополнительными видами обслуживания, которые расширяют возможности пользователя по получению информации о соединении, тональных уведомлений, а также позволяют изменять конфигурацию соединения. В сетевом фрагменте ССП пользователям могут быть доступны следующие дополнительные виды обслуживания:

- идентификации вызывающей линии (CLIP);
- запрет идентификации вызывающей линии (CLIR);
- предоставление идентификации подключенной линии (COLP);
- безусловная переадресация вызова (Call Forwarding No Reply);
- переадресация вызова при занятости (Call Forwarding Busy);
- безусловная переадресация вызова (Call Forwarding Unconditional);
- идентификация злонамеренного вызова (MOD);
- индикация ожидающего вызова/сообщения (Call/Message Waiting);
- завершение вызова (Call Completion);
- парковка и перехват вызовов (Call Park/Pick-up);
- удержание вызова (Call Hold);
- замкнутая группа пользователей (CUG);
- конференцсвязь с расширением (CONF);

Следует отметить, что в зависимости от используемого типа подключения и терминального оборудования, а также от возможностей Softswitch список и алгоритмы предоставления услуг могут отличаться. В настоящий момент наиболее специфицированными являются дополнительные виды обслуживания для пользователей сетей ISDN. Спецификации ряда ДВО для пользователей сетей на основе H.323 и SIP-протоколов находятся в процессе разработки в международных организациях. Также следует отметить, что фрагмент ССП для проходящих через него вызовов должен обеспечивать поддержку ДВО, инициированных в других сетях.[17]

### Услуги доступа

Услугами доступа, поддерживаемыми со стороны сетевого фрагмента ССП, являются:

- услуги доступа в сети IP по коммутируемому соединению с поддержкой процедур точки доступа и авторизации со стороны фрагмента NGN; применяются как для поддержки WWW, E-mail, FTP-приложений, так и для доступа к сетям IP-телефонии;
- услуги доступа к ресурсам ИСС с реализацией функции SSP в сетевом фрагменте NGN. Реализованный SSP на ЕСЭ РФ должен как минимум обеспечивать поддержку следующих видов услуг ИСС: а) «Бесплатный вызов»; б) «Телеголосование»; в) «Вызов с дополнительной оплатой»; г) «Вызов по предоплаченной карте».
- услуги доступа к информационно-справочным ресурсам с поддержкой точки доступа и авторизации доступа со стороны фрагмента ССП (функция Service Node при доступе к внешним ресурсам).

#### Услуги VPN

Фрагментом ССП может поддерживаться предоставление следующих видов услуг виртуальных частных сетей:

- виртуальная частная сеть (VPN) на основе коммутируемых соединений с поддержкой адресного пространства VPN со стороны Softswitch. В этом случае задачей Softswitch является анализ номера входящего/исходящего абонента с принятием решения о возможности установления соединения в соответствии с политикой VPN. После принятия положительного решения об установлении соединения обрабатывается во фрагменте ССП как обычный вызов;
- виртуальная частная сеть на основе постоянных соединений внутри фрагмента NGN с обработкой адресной информации со стороны гибкого коммутатора. В этом случае для виртуальной частной сети изначально резервируется транспортный ресурс во фрагменте NGN. Обслуживание вызовов VPN осуществляется

гибким коммутатором в рамках выделенного для VPN транспортного ресурса;

- виртуальная частная сеть на основе постоянных соединений без обработки сигнальной информации вызова гибким коммутатором. В этом случае VPN использует фрагмент NGN только как транспортный ресурс. Обработкой сигнальной информации, относящейся к вызову, занимаются внешние к фрагменту устройства.

### Услуги мультимедиа

Мультимедийные услуги можно рассматривать с двух позиций:

- с позиции абонентов услуг связи.
- с позиции поставщика услуг (оператора связи).

С точки зрения абонентов, мультимедийная услуга связи представляет собой возможность сети обеспечить функционирование специфических мультимедийных пользовательских приложений. Фактически абоненту безразлично, на базе какой сети предоставляется мультимедийная услуга, т. е. услуга не зависит от технологической платформы сети. Мультимедийное пользовательское приложение представляет собой приложение, одновременно поддерживающее несколько «единиц» представления аудиовизуальной информации и предоставляющее абонентам общее информационное пространство в рамках одного сеанса связи. В качестве примеров мультимедийных приложений можно привести следующие: совместная работа с документами и графикой, «белая доска», дистанционное обучение, телемедицина и др. Оператор связи рассматривает мультимедийную услугу связи как перенос комбинации двух или более «единиц» представления аудиовизуальной информации (т. е. видео, звука, текста) между абонентами (группами абонентов) в рамках сетевой инфраструктуры и с учетом состава и возможностей используемого

оборудования. Таким образом, возможность предоставления той или иной мультимедийной услуги полностью зависит от технологической платформы сети. Европейский институт стандартизации в области связи (ETSI) ввел понятие «широкополосных мультимедийных услуг». Под такими услугами понимаются услуги связи, предоставление которых осуществляется на базе широкополосных сетей связи, способных обеспечить перенос информации (контента) в виде непрерывных потоков пакетов/ячеек в режиме реального времени.[17]

Классификацию мультимедийных услуг связи и предложений можно производить с различных точек зрения и с использованием различных критериев. В качестве примера классификации, отражающей точку зрения оператора сети B-ISDN, можно привести рекомендацию ITU-T I.211. Суть подхода заключается в том, что услуги связи предоставляются абонентам с помощью определенных служб B-ISDN. Согласно рекомендации, в зависимости от способов связи между терминальным оборудованием абонентов и в соответствии с возможными пользовательскими приложениями все службы делятся на интерактивные и распределительные, каждая из которых, в свою очередь, включает несколько классов служб.[3,4,17]

### Архитектура Сетей Следующего Поколения

Сети нового поколения должны предоставлять ресурсы для создания, внедрения и управления всеми видами услуг (существующих и будущих). В рамках NGN основной упор делается на возможность адаптации услуги сервис-провайдерами, многие из которых также обеспечат своим пользователям возможность приспособить свои собственные услуги. Сети нового поколения будут включать в себя обеспечивающие поддержку разработки, предоставления и управления услугами.

На рисунке 1.4 ниже показан вариант модели сети на базе концепции NGN.

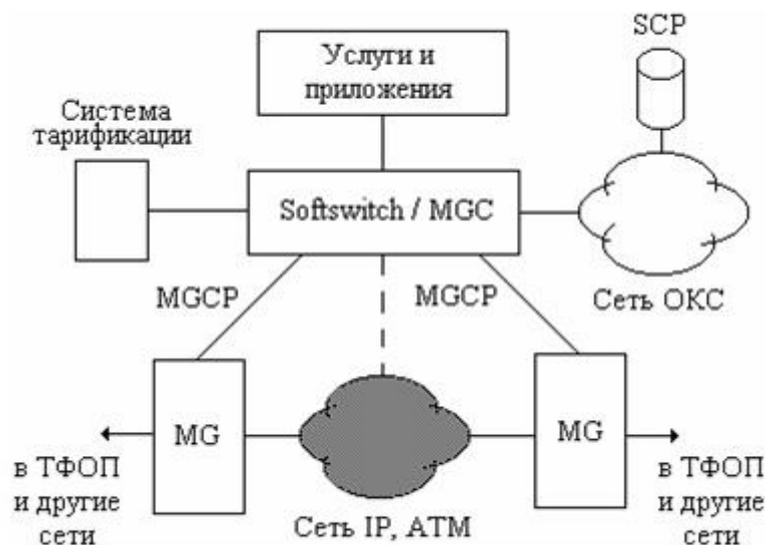


Рис.1.4. Концепция NGN

Оборудование Softswitch взаимодействует со многими компонентами в телекоммуникационной системе. В верхней части рисунка показаны такие функциональные блоки: система тарификации, платформа услуг и приложений, а также сеть общеканальной сигнализации (ОКС). Следует только отметить возможность выхода через сеть ОКС на узел управления услугами (Services Control Point – SCP), входящий в состав интеллектуальной сети, что позволяет дополнить услуги и приложения, доступные абонентам непосредственно через Softswitch, интеллектуальными услугами.

Логика обработки вызовов реализуется в контроллере шлюзов (Media Gateway Controller – MGC). Взаимодействие Softswitch с коммутационными станциями других сетей осуществляется через оборудование Media Gateway (MG). Для этих целей используется протокол MGCP (Megaco), разработка которого была выполнена в IETF (Инженерная группа по проблемам Интернет) подгруппой Megaco (Media Gateway Control). Протокол MGCP в силу того, что он был разработан в IETF, ориентирован, в основном, на IP-

технологии. В результате работы МСЭ появился проект рекомендации Н.248, который ориентирован скорее на передачу мультимедийной информации, чем передачу неструктурированного трафика данных.

Пунктирной линией на рисунке «Вариант модели сети NGN» показана связь Softswitch с пакетной сетью, которая, как правило, базируется на технологиях IP и ATM. Пакетная сеть обрабатывает основную часть трафика телекоммуникационной системы. Переход к сети с коммутацией пакетов целесообразно осуществлять путем постепенной эволюции телекоммуникационной системы.

#### Стратегии внедрения технологий NGN при развитии сети ТфОП

Основными вариантами применения пакетных технологий при модернизации существующих сетей связи являются:

- создание параллельной к существующей сети инфраструктуры NGN
- стратегия наложения;
- создание инфраструктуры NGN, поглощающей существующую

структуру ТфОП – структура замещения.

Первый вариант предполагает, что создаваемый фрагмент сети на основе NGN-технологий и существующая сеть ТфОП функционируют отдельно друг от друга, частично используя совместный ресурс первичной сети. Взаимодействие между сетями реализуется в ограниченном числе сетевых точек (шлюзов). При этом базовая услуга телефонии оказывается в обеих сетях связи или при взаимодействии сетей.

Второй вариант предполагает, что существующая ТфОП входит в состав мультисервисной сети, в основе которой лежат NGN-решения, при этом взаимодействие между любыми коммутационными узлами ТфОП осуществляется с использованием ресурсов NGN. Базовая услуга телефонии для межстанционных вызовов предоставляется при взаимодействии фрагментов существующей ТфОП и NGN или в рамках NGN.

Также рассматривается вариант с реализацией транзитного уровня существующей ТфОП в рамках NGN-сети, который можно считать переходным от варианта 1 к варианту 2.

Построение сети NGN без изменения существующей сети ТфОП. В данном варианте предполагается, что заданный фрагмент NGN создается без привязки к существующей структуре ТфОП, но привязывается к существующей структуре первичной сети. Решение об усилении существующей структуры первичной сети должно приниматься в стадии детального проектирования. При принятии решений предполагается, что создаваемый фрагмент NGN должен быть максимально доступен большинству потенциальных пользователей на территории, где предполагается его развертывание, т.е. покрытие территории является по возможности равномерным. Создание транспортного уровня NGN потребует использования существующих или создания новых ресурсов первичной сети. Выбор того или иного решения связан с состоянием существующей первичной сети. Если первичная сеть строится на основе технологий SDH и при этом первичный ресурс, достаточный для построения транспортного уровня фрагмента NGN существует или может быть получен путем использования оборудования систем передачи более высокого уровня, то возможно использование существующей первичной сети с соответствующей модернизацией в некоторых сетевых точках.

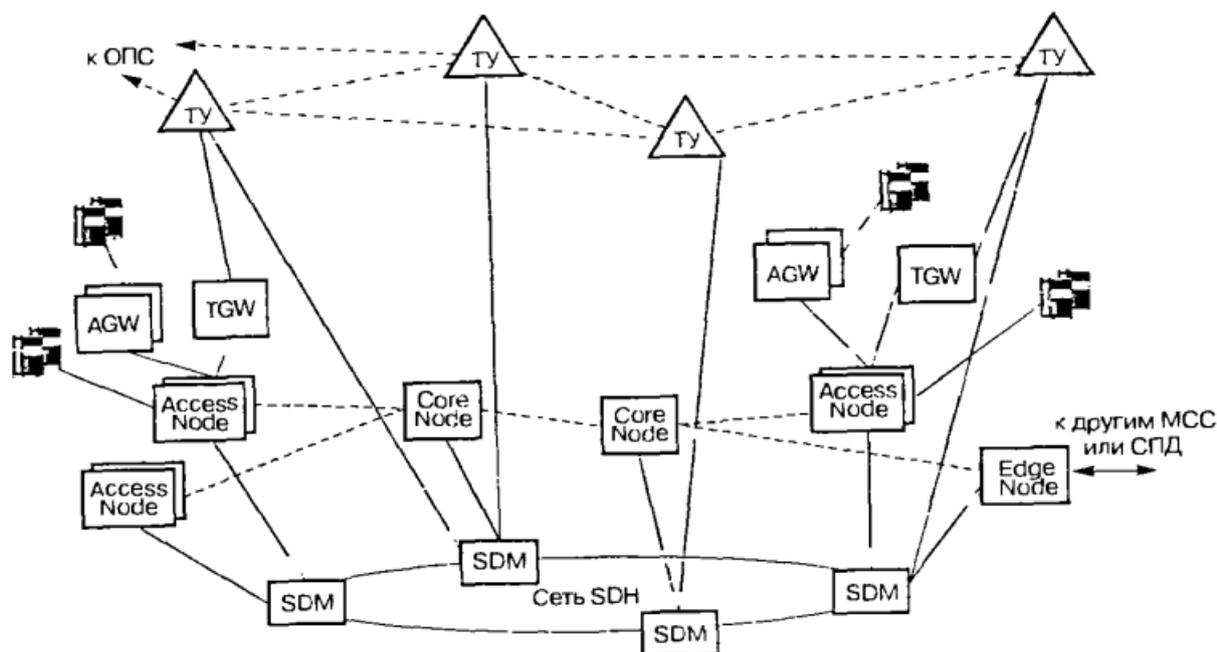


Рис.1.5. - Конфигурация транспортного уровня мультисервисной сети  
 Если первичная сеть строится на основе технологий PDH или аналоговых систем передачи, то потребуется создание параллельной структуры первичной сети.

Решение о выборе технологии для создания такой структуры должно приниматься в процессе проектирования для конкретной сети. В этом случае возможно использование технологии SDH как средства построения агрегированной первичной сети, предназначенной как для передачи информации существующего фрагмента ТфОП, так и для организации транспорта для фрагмента NGN. Альтернативным является применение технологий, базирующихся на Ethernet (например, Gigabit Ethernet), для построения транспортной основы фрагмента NGN. Но такая основа возможна только в сети NGN. Теоретически можно обеспечить туннелирование потоков E1 существующей сети ТфОП через Ethernet в первичную сеть, но эта операция потребует достаточно больших инвестиций в оборудование транспортных шлюзов.

В качестве технологии, применяемой при создании транспортного уровня, может использоваться технология IP/MPLS при использовании первичной сети на основе Ethernet, либо IP/MPLS/ATM или IP ATM при использовании первичной сети на основе SDH. В то же время, решение о выборе конкретной технологии должно приниматься в процессе формулирования технического задания на проектирование сети и зависит от ряда факторов. Реализация предоставленного варианта построения транспортного уровня потребует:

– внедрения оборудования коммутаторов магистральной транспортной сети. Число коммутаторов и сетевые точки внедрения (с привязкой к инфраструктуре существующей сети SDH) должны определяться в процессе детального проектирования;

- внедрение оборудования узлов доступа и оборудования шлюзов доступа на уровне опорных АТС, подлежащих замене, или на уровне которых планируется расширение абонентской емкости;
- расширение существующей емкости линейных сооружений (на участках где нет SDH- систем передачи – инсталляция таких систем) между оборудованием вводимых узлов доступа и мультиплексорами SDH магистральной сети;
- внедрение оборудования межсетевых шлюзов между мультисервисной сетью и сетью ТфОП.
- Внедрение оборудования граничного шлюза (шлюзов) в тех сетевых точках, которые должны использоваться для выхода на сеть передачи данных или мультисервисные сети других операторов;
- Создание структуры сети доступа (участок между пользователем и узлом доступа).

Построение мультисервисной сети с поглощением сетевой структуры существующей ТфОП.

Данный вариант предполагает, что основой транзитной сети ТфОП будет являться создаваемый фрагмент NGN. Соответственно, все опорные АТС подключаются к NGN через оборудование шлюзов. В этом случае транзитный уровень ТфОП полностью заменяется NGN, соответственно, транзитные узлы ТфОП выводятся из обслуживания трафика ТфОП. Данный вариант является завершающей стадией формирования транспортного уровня мультисервисной сети, и его реализация потребует значительных инвестиций.

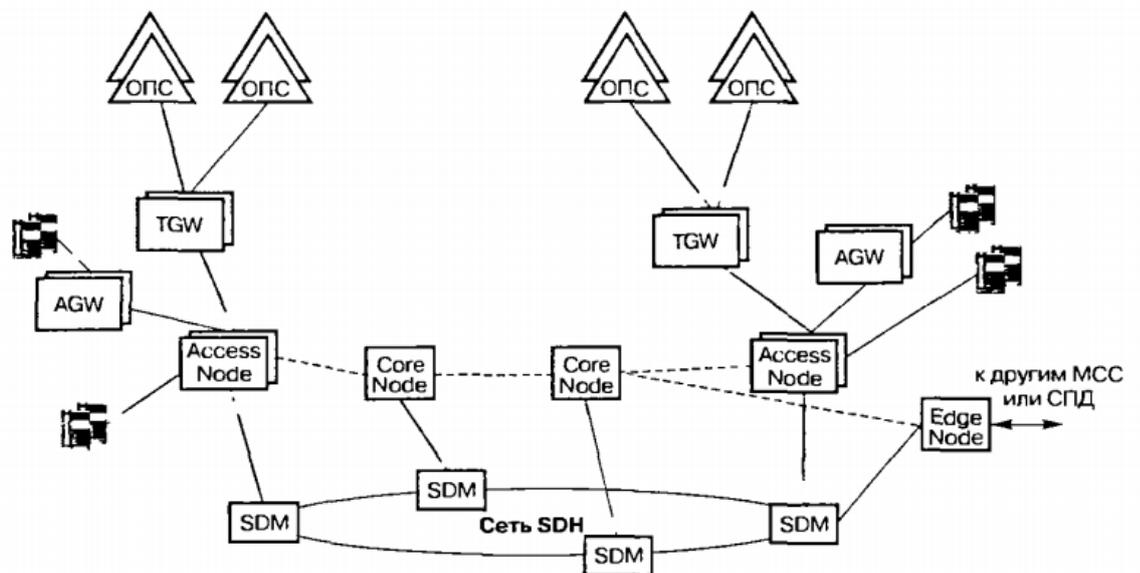


Рис.1.6. - Построение транспортного уровня мультисервисной сети,поглощающего транзитную структуру ТфОП

Комбинированный вариант. Данный вариант представляет собой стратегию частичного замещения оборудования ТфОП мультисервисной сетью связи.

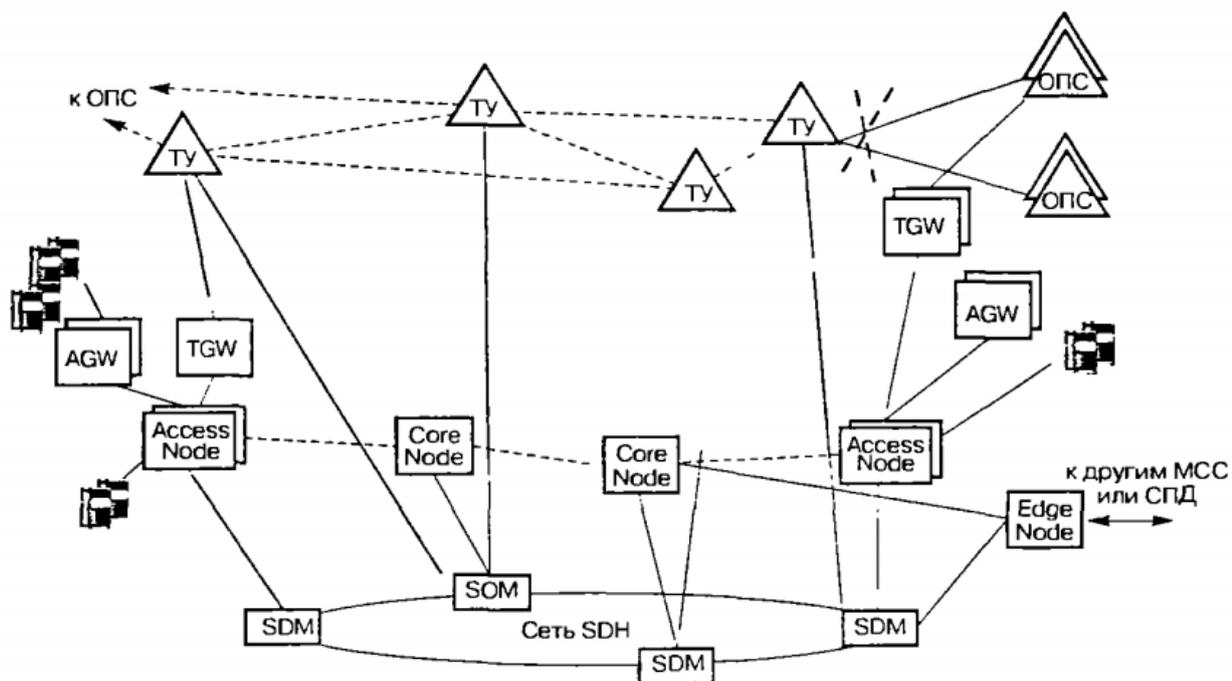


Рис.1.7. - Построение транспортного уровня мультисервисной сети.

#### Комбинированный вариант

В этом случае часть ОПС подключается к оборудованию мультисервисной сети через оборудование транкинговых шлюзов (TGW), а остальные ОПС сохраняются в структуре ТфОП. Введение новой абонентской емкости в замещаемом фрагменте сети и замена выводимых из эксплуатации АТС осуществляется в рамках развития местной сети связи. Данный вариант является способом постепенного развития варианта 1 до варианта 2 и не может рассматриваться как альтернативным [19]. Дополнительно к варианту 1 реализация потребует:

- внедрения на уровне всех опорных станций (ОПС) оборудования шлюзов;
- замены линейных сооружений и систем передачи, не ориентированных на поддержку SDH, на участках между ОПС и узлами доступа и магистральной сетью SDH. В то же время усиление магистральной сети SDH не потребуется;

- внедрение более мощных, по сравнению с первым вариантом, узлов ядра сети;
- внедрение оборудования шлюзов для подключения сетей альтернативных операторов (исключение составляет подключение на уровне опорных АТС);
- использование большего числа гибких коммутаторов или гибких коммутаторов с большей производительностью.

Функциональная модель сетей NGN, в общем случае, может быть представлена тремя уровнями:

- транспортный уровень;
- уровень управления коммутацией и передачей информации;
- уровень управления услугами.

Задачей транспортного уровня является коммутация и прозрачная передача информации пользователя. Задачей уровня управления коммутацией и передачей является обработка информации сигнализации, маршрутизация вызовов и управление потокам. Уровень управления услугами содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую следующие потребности:

- предоставление инфокоммуникационных услуг;
- управление услугами;
- создание и внедрение новых услуг;
- взаимодействие различных услуг.

Уровень управления услугами позволяет реализовать специфику услуг, и применять одну и ту же программу логики услуги вне зависимости от типа транспортной сети (IP, ATM, FR и т.п.) и способа доступа. Наличие этого

уровня позволяет также вводить на сети любые новые услуги без вмешательства в функционирование других уровней. Данный уровень может включать множество независимых подсистем ("сетей услуг"), базирующихся на различных технологиях, имеющих своих абонентов и использующих свои, внутренние системы адресации.

Архитектура сетей NGN будет состоять из IP-ядра и нескольких сетей доступа, использующих разные технологии. Основу сети NGN составляет универсальная транспортная сеть, реализующая функции транспортного уровня и уровня управления коммутацией и передачей. Назначением транспортной сети является предоставление услуг переноса.

В состав транспортной сети NGN могут входить следующие компоненты:

- транзитные узлы, выполняющие функции переноса и коммутации;
- оконечные (граничные) узлы, обеспечивающие доступ абонентов к мультисервисной сети;
- контроллеры сигнализации, выполняющие функции обработки информации сигнализации, управления вызовами и соединениями;
- шлюзы, позволяющие осуществить подключение традиционных сетей связи (ТФОП, СПД, СПС).

Контроллеры сигнализации могут быть вынесены в отдельные устройства, предназначенные для обслуживания нескольких узлов коммутации. Использование общих контроллеров позволяет рассматривать их как единую систему коммутации, распределенную по сети. Такое решение не только упрощает алгоритмы установления соединений, но и является наиболее экономичным для операторов и поставщиков услуг, так как позволяет заменить дорогостоящие системы коммутации большой емкости небольшими, гибкими и доступными по стоимости даже мелким поставщикам услуг.

Реализация инфокоммуникационных услуг осуществляется на базе узлов служб (Services Node – SN) и/или узлов управления услугами (SCP). SN является оборудованием поставщиков услуг и может рассматриваться в качестве сервера приложений для инфокоммуникационных услуг, клиентская часть которых реализуется конечным оборудованием пользователя. SCP является элементом распределенной интеллектуальной платформы и выполняет функции управления логикой и атрибутами услуг. Совокупность нескольких узлов служб и/или узлов управления услугами, задействованных для предоставления одной и той же услуги, образуют платформу управления услугами. В состав платформы также могут входить узлы административного управления услугами и серверы различных приложений.

Оконечные/оконечно-транзитные узлы транспортной сети могут выполнять функции узлов служб, т.е. состав функций граничных узлов может быть расширен за счет добавления функций предоставления услуг. Для построения таких узлов может использоваться технология гибкой коммутации (Softswitch). Если представить топологию сети NGN в виде набора плоскостей, то внизу окажется плоскость абонентского доступа (базирующаяся, например, на трех средах передачи: металлическом кабеле, оптоволокне и радиоканалах), далее идет плоскость коммутации (коммутации каналов и/или коммутации пакетов). В указанной плоскости находится и структура мультисервисных узлов доступа. Над ними располагаются программные коммутаторы SoftSwitch, составляющие плоскость программного управления, выше которой находится плоскость интеллектуальных услуг и эксплуатационного управления услугами.

Инфокоммуникационные услуги предполагают взаимодействие поставщиков услуг и операторов связи, которое может обеспечиваться на основе функциональной модели распределенных (региональных) баз данных, реализуемых в соответствии с рекомендацией МСЭ-Т X.500, доступ к

которым организуется с использованием протокола LDAP (Lightweight Directory Access Protocol).

Основными услугами сети доступа должно являться обеспечение подключения следующих типов абонентов:

- абоненты аналогового доступа ТФОП;
- абоненты доступа ЦСИС;
- абоненты доступа xDSL;
- абоненты выделенных каналов связи Nx64 кбит/с и 2 Мбит/с;
- абоненты, использующие для доступа оптические кабельные технологии (PON);
- абоненты, использующие для доступа структурированные кабельные системы (HFC);
- абоненты, использующие системы беспроводного доступа и радиодоступа (Wi-Fi).

В каждой из перечисленных выше типов услуг возможна дальнейшая дифференциация в зависимости от используемой скорости передачи и/или технологии доступа.

Концепция NGN во многом опирается на технические решения, уже разработанные международными организациями стандартизации. Так, взаимодействие серверов в процессе предоставления услуг предполагается осуществлять на базе протоколов, специфицированных IETF (MEGACO), ETSI (TIPHON), Форумом 3GPP2 и т.д. Для управления услугами будут использованы протоколы H.323, SIP и подходы, применяемые в интеллектуальных сетях связи. В качестве технологической основы построения транспортного уровня мультисервисных сетей рассматриваются ATM и IP с возможным применением в будущем оптической коммутации (PON).

Работа по проблемам архитектуры и протоколов для NGN должна концентрироваться на следующих аспектах:

- рассмотрение использования техники эталонного моделирования,
- определение, как могут быть поддержаны на гетерогенных сетях службы из конца в конец, управление вызовом и мобильность пользователя,
- определение функций взаимодействия для поддержания действующих терминалов, не способных работать на NGN,
- определение функциональности терминалов, способных работать на NGN, через механизм обновления программного обеспечения, резервирования и эволюции терминалов, согласование версии и управление.

### 3 Сети последующих поколений, сетевые параметры и основные протоколы NGN

Современная тенденция конвергенции сетей различных типов привела к необходимости переноса сетью всех видов трафика, а не только традиционного для компьютерных сетей трафика приложений доступа к файлам и электронной почты.

Характеристики QoS особенно важны в случае, когда сеть передает одновременно трафик разного типа, например, трафик web-приложений и голосовой. Это связано с тем, что различные типы трафика предъявляют разные требования к характеристикам QoS. Добиться синхронного соблюдения характеристик QoS для всех видов трафика очень сложно, поэтому обычно используют следующий подход: классифицируют существующие в сети трафики, относя каждый из них к одному из распространенных типовых видов, а затем добиваются одновременного выполнения определенного подмножества из набора требований QoS.

#### Требования к качеству обслуживания для голоса

Определяя требования QoS для VoIP трафика рекомендуется придерживаться следующих правил [5,14]:

- потери пакетов предоставления VoIP сервиса высокого качества не должны превышать 0.25 процентов;
- односторонняя задержка (One-Way Delay) не должна превышать 150 мс, в соответствии с рекомендацией (ITU) G.114;
- в хорошо спроектированных сетях значение общей задержки (End-to-End Delay) должно быть менее 100 мс, хотя задержка до 400 мс считается приемлемым;
- колебания задержки (джиттер) должны быть менее 10 мс. Максимальный джиттер должен быть менее чем бюджет по задержке в сети минус минимальная сетевая задержка. Это типовое значение колебания

задержки для VoIP обусловлено бюджетом по задержке, так называемым mouth-to-ear, в 100 мс. (Это достаточно консервативный бюджет по сравнению с G.114, в котором рекомендуется джиттер менее 150 мс). Из этого значения вычитается время распространения по магистрали (30 мс) и задержку кодека (35 мс), что дает бюджет для джиттер в 35 мс. Эти 35 мс разбиваются на 30 мс на доступе (15 мс вход/выход) и 5 мс на магистрали. То есть в худшем варианте, для адаптивных джиттер-буферов, колебания задержки должны быть менее 10 мс;

- для каждого разговора (в зависимости от частоты квантирования, кодека и заголовка второго уровня) требуется 21-106 kbps гарантированной приоритетной полосы пропускания;

- для трафика сигнализации требуется 150 bps (плюс заголовков второго уровня) гарантированной полосы пропускания.

На качество голосовой связи напрямую влияют все три фактора качества QoS: потери пакетов, задержка и вариации задержки:

- потери пакетов вызывают кратковременные пробелы в разговоре. Предположив случайное распределение сбросов пакетов в одном речевом потоке, сброс 1-го процента в голосовом потоке привела бы в среднем к потере, которую нельзя было бы восстановить каждые 3 минуты. Аналогично, уровень сброса 0,25 процента привел бы в среднем к потере, которую нельзя было бы восстановить каждые 53 минуты;

- задержка более 200 мс может вызвать деградацию качества голосовой связи. Если общая задержка в канале становится слишком большой, разговор по телефону начинает напоминать переговоры по спутниковому каналу связи или по симплексному радиоканалу. В стандарте Международного Союза Электросвязи для технологии VoIP (G.114) говорится, что задержка величиной в 150 мс в одном направлении является приемлемой для качество голосовой связи. Было продемонстрировано, что разница в качестве голоса между сетями с задержкой в 150 мс и 200 мс является незначительной и практически незаметной для пользователя.

## Требования к качеству обслуживания для видео

Существует два основных типа видео приложений: Интерактивное видео (например, видео конференции) и потоковое видео (например, IPTV, которое может использовать как одно, так и многоадресную рассылку).

### Требования для интерактивного видео

При настройке интерактивного видео (видео конференций) рекомендуется следующее [5,14]:

- интерактивный видео трафик, в соответствии с “Базовыми основами QoS”, должен быть промаркирован AF41;
- потери должны быть не более одного процента;
- однонаправленная задержка должна быть не более 150 мс;
- колебания задержки должны быть не более 30 мс;
- минимально гарантированная полоса пропускания (LLQ) должна быть равна размеру сессии видео конференции плюс 20 процентов. (Например, сессия видео конференции в 384 kbps требует настройки 460 kbps полосы трафика гарантированного приоритета.) Так как видео конференция включает аудио кодек G.711 для речи, то у нее и соответствующие голосовому трафику требования к потерям, задержке и колебаниям задержки. Однако трафик видео конференции радикально отличается от трафика голоса. Например, трафик видео конференций использует переменные размеры пакетов и переменные скорости передачи пакетов.

### Требования для потокового видео

При настройке потокового видео рекомендуется следующее [5,14]:

- потери должны быть менее 2 процентов;

- задержка должна быть менее 4-5 секунд (в зависимости от возможностей буферизации видео приложений);
- система IPTV максимально может допускать 50 мс величину отклонений (джиттера);
- потоковое видео обычно однонаправленное и, поэтому, в удаленных филиалах маршрутизаторы можно не настраивать на поддержку потокового видео в направлении от филиала к центру.

Приложения потокового видео менее требовательны к QoS, так как они менее чувствительны к задержкам (может пройти несколько секунд перед началом видео картинки) и нечувствительны к колебаниям задержки (благодаря буферизации на уровне приложений). Однако, потоковое видео может содержать важную информацию, такую как электронное обучение или трансляцию корпоративных совещаний и, следовательно, требовать гарантий QoS. Не важное видео содержание (такое как фильмы, музыкальные видео клипы и так далее) может рассматриваться как Интернет сервис (сервис хуже чем “Best Effort”), что означает, что эти потоки работают пока есть полоса пропускания, но будут вытесняться в случае возникновения перегрузок в сети.

#### Требования к качеству обслуживания для трафика данных

Трафики данных можно разделить на четыре основных классов трафика, такие как [14]:

- локально-определенный/критический (для критически важных приложений) - транзакционные и интерактивные приложения с высоким бизнес-приоритетом;
- транзакционный/интерактивный - приложения клиент-сервис, приложения по передаче сообщений;

- объемные приложения - передача больших файлов, синхронизация и репликация баз данных, электронная почта (e-mail), распространение видео содержания;
- по возможности - класс по умолчанию для всего не назначенного трафика, конфигурируется как минимум 25 процентов полосы для этого класса;
- опционный класс - Интернет/scavenger (игровой трафик, развлечения и т.д.). Дополнительный опционный класс включает в себя маршрутизацию и сетевое управление.

### Протоколы в NGN

Сети NGN можно рассматривать в качестве сетевых решений, объединяющих фрагменты различных существующих сетей (Интернет и СТОП) с применением свойственных этим сетям технологий. Соответственно, в NGN применяются как протоколы Интернет (например, IP, TCP, UDP, FTP, HTTP, SMTP и другие протоколы стека TCP/IP), так и протоколы СТОП (например, ОКС7, EDSS1, протоколы интерфейса V5). Кроме того, некоторые протоколы NGN являются перспективными, прямо или косвенно затрагивая принципы взаимодействия сетей Интернет и СТОП в рамках создания мультисервисной сети. Протоколы NGN с некоторой долей условности можно классифицировать следующим образом.[17]

Базовые протоколы стека TCP/IP. Протоколы Интернет можно использовать для передачи сообщений через любой набор объединенных между собой сетей. Они в равной мере пригодны для связи как в локальных, так и в глобальных сетях. Комплект протоколов Интернет включает в себя не только спецификации низших уровней (например, TCP и IP), но также спецификации для таких общих применений, как почта (SMTP), приложения гипертекстовых терминалов (HTTP) и передача файлов (FTP).

Маршрутизация по протоколу IP (Internet Protocol) определяет формат, адресацию и характер перемещения дейтаграмм IP через объединенные сети (по одной пересылке за раз). В начале следования дейтаграмм весь их маршрут не известен. Вместо этого на каждом промежуточном узле вычисляется следующий пункт назначения путем сопоставления адреса пункта назначения, содержащегося в дейтаграмме, с записью данных в маршрутной таблице текущего узла. Участие каждого узла в процессе маршрутизации заключается в продвижении пакетов, базирующемся лишь на внутренней информации, вне зависимости от того, насколько успешным будет процесс, и того, достигнет или нет пакет конечного пункта назначения. Другими словами, IP не обеспечивает отправку на узел-источник сообщений о неисправностях, когда имеют место аномалии маршрутизации. Выполнение этой задачи предоставлено другому протоколу Интернет, а именно протоколу управляющих сообщений Интернет (Internet Control Message Protocol - ICMP).

Сигнальные протоколы SIP H.323. В настоящее время для установления мультимедийных вызовов через сети IP создано несколько протоколов, например SIP (Session Initiation Protocol) [RFC 2543] и H.323. Появление данных стандартов открывает широкие возможности децентрализации обеспечения услуг телефонии, причем услуги могут управляться со стороны пользователя. Протокол инициирования сеансов связи (SIP) предназначен для организации, модификации и завершения мультимедийных сеансов или вызовов. Мультимедийные сеансы включают в себя мультимедийные конференции, Интернет-телефонию и другие аналогичные приложения. SIP является одним из ключевых протоколов, используемых для реализации передачи речи по сетям IP (Voice over IP - VoIP). Таким образом, SIP есть упрощенный протокол сигнализации, имеющий широкое применение в Интернет-телефонии.

Если для управления ресурсами среды передачи MG между MGC и шлюзами среды передачи (то есть транспортными или медиа-шлюзами) используется протокол H.248/MEGACO (MGCP), то SIP или H.323 могут применяться для установления речевого соединения на участке между MGC и клиентом VoIP. Хотя и H.323, и SIP могут использоваться для осуществления такой сигнализации, необходимо отметить, что ни один, ни другой из них не разрабатывался в расчете на поддержку услуг этого типа. Следовательно, можно ожидать, что для поддержки связи между MGC в целях предоставления услуг VoIP тот и/или другой будут соответственно оптимизированы.

Несмотря на то, что SIP в типовом варианте применяется поверх протоколов UDP или TCP, без внесения каких-либо технических изменений он может использовать возможности протоколов IPX, Frame Relay, AAL5/ATM или X.25 [6]. SIGTRAN. Стек протоколов SIGTRAN служит для передачи сигнализации TDM через IP-сеть. Транспортным протоколом в этом стеке является SCTP, он обеспечивает надежную передачу сигнальных сообщений между двумя точками, которые коммуницируют по IP-протоколу. В стеке протоколов TCP/IP находится на месте протоколов TCP или UDP. По сравнению с выше упомянутыми, SCTP (Stream Control Transmission Protocol) имеет дополнительные функции, которые необходимы для надежной передачи сигнальных сообщений.

Над протоколом SCTP находятся уровни адаптации сигнализации (Signaling User Adaptation Layers) (M3UA – MTP3 User Adaptation Layer, M2UA – MTP2 User Adaptation Layer и т.д.), которые обеспечивают адаптацию работы протокола SCTP сигнализации TDM (ISUP, MTP3 - Message Transfer Part level2, V5.2, DSS1 и т.д.)

Уровень адаптации пользователей M3UA поддерживает передачу любой пользовательской сигнализации MTP3, например, сообщения ISUP или SCCP (Signaling Connection Control Part) через IP-сеть. При этом

используются услуги протокола передачи с управлением потока (SCTP). Для передачи сообщений ОКС7 через IP-сеть пункты сигнализации ОКС7 переводятся в IP-адреса. Сигнализация используется для коммуникации между шлюзом сигнализации SG и программным коммутатором CS.

Уровень адаптации пользователя ISDN обеспечивает функциональность передачи цифровой абонентской сигнализации номер 1 (DSS1) из сети TDM через SG в IP-сеть. Сигнализация используется для установления коммуникации между шлюзом сигнализации (SG) и программным коммутатором CS для:

- передачи примитивов интерфейса Q.921/Q.931;
- передачи информации между модулями управления уровнями в SG и CS;
- управления активными соединениями между SG и CS;
- активации и деактивации физического уровня абонентских соединений ISDN.

IUA поддерживает основной и первичный доступ, а также соединения точка-точка и точка-многоточка. Сигналы ISDN поступают в SG, откуда IUA передает сигнальную информацию уровня Q.921 (обычно Q.931) пользователю Q.921 в программном коммутаторе. Функция шлюза, следовательно, выполняется на втором уровне. В SG на абонентском доступе терминируются протоколы физического (I.430 и/или I.431) и канального уровней (Q.921), в то время как протоколы сетевого уровня Q.931 или QSIG терминируются в программном коммутаторе. SG выполняет функции сетевого взаимодействия, которые обеспечивают взаимодействие протоколов абонентского доступа с транспортными функциями IP-сети. IUA использует услуги протокола передачи с управлением потока (SCTP) для надежной и своевременной передачи абонентской сигнализации через IP-сеть

Протокол SIP-T. Протокол инициирования сеансов для телефонии SIP-T (SIP for telephones) базируется на протоколе SIP и обеспечивает его использование для передачи телефонных сигналов между сетью TDM, которая использует сигнализацию SSN7, и IP-сетью. SIP-T обеспечивает прозрачную передачу сигнализации TDM через IP-сеть. Сообщения SIP-T являются сообщениями SIP, которые содержат сигнальную информацию (например: сообщения ISUP в случае ОКС7) и другую информацию, необходимую для установления каналов.

Для передачи телефонных сигналов сигнализации ТфОП используются два отдельных механизма, которые используются одновременно: туннелирование (инкапсуляция) и преобразование (трансляция). Двоично-закодированные сигналы ISUP добавляются к телу сообщения SIP и таким образом инкапсулируются. Туннелирование обеспечивает прозрачную передачу сигналов сигнализации ISUP. Преобразование включает преобразование протоколов сигнализации SIP и ISUP в обоих направлениях. Происходит как преобразование самих сигналов, так и преобразование параметров ISUP в поля SIP и обратно. Сообщения ISUP передаются в теле сообщения SIP. Заголовок

SIP содержит переведенную информацию маршрутизации ISUP. SIP-T также определяет применение метода SIP INFO для надежной сигнализации in-call ISUP в IP-сетях.

Сигнализация SIP-T используется для соединения между программными коммутаторами CS - CS и CS - iCS. Медиапоток SIP-T передается с помощью протокола RTP через UDP [13]. Протокол управления шлюзом MGCP. Протокол управления медиа-шлюзом (MGCP) служит для контроля работы между медиашлюзом (MG) и программным коммутатором (CS). Программные коммутаторы используют протокол MGCP для сообщения медиашлюзам, какие медиапотoki TDM и IP он должен соединять между собой. Определяет способ коммуникации между MG и CS, при чем

весь интеллект выполнения вызовов заложен в CS, MG только выполняет команды и оповещает CS о событиях, происшедших на конечных точках, которые он объединяет. То есть обеспечивает, чтобы программный коммутатор управлял неинтеллектуальным медиашлюзом. MGCP предназначен для сетей с централизованной архитектурой. Обеспечивает увеличение количества портов и функциональности сетевых серверов, чтобы не было необходимости замены терминального оборудования. Для различных сигнализаций используются различные пакеты, которые определяют общую функциональность сигнализации ТфОП (пакеты Line и DTMF - Dual Tone Multifrequency), соединение абонентских линий и выполнения услуг, например, удержание вызова и передача соединения.

### **Выводы по Главе I**

Из изложенного в первой главе, следует что:

- 1- Сети следующего поколения представляют собой результат эволюции всей системы электросвязи. Тем не менее, основной реализацией идеи NGN служит телефонная сеть, единственная из всех существующих сетей, которая:
  - обеспечивает диалоговые услуги самой большой группе абонентов;
  - приносит Оператору основные доходы.
2. для качественного предоставления мультисервисной услуг сети следующего поколения , таких, как передача данных, голоса и видео, нужно придерживаться определенных значений некоторых показателей.
3. по показателям качества мультисервисных услуг можно проанализировать насколько эффективно работает та или иная дисциплина.



## Глава II. Управление сетями в сетях следующего поколения (NGN) и широко используемые протоколы маршрутизации в NGN

### 1. Основы управления сетями, стандарт TMN.

Управление сетями связи — это совокупность организационно-технических мероприятий, направленных на обеспечение функционирования сети связи, в том числе регулирование трафика. В настоящее время управление сетями связи сводится к процессам наблюдения и контроля состояния узлов, линий и взаимодействий узлов, а также управление работой приложений.[7]

Существует ряд аспектов построения системы управления сетями специальной связи. Основные из них — это:

- архитектура системы управления;
- структура системы управления;
- уровни управления;
- области управления;
- методы и используемые протоколы.[7]

Далее рассмотрим аспекты более детально.

#### Архитектура системы управления

Большинство архитектур управления сети используют одну и ту же базовую структуру и набор взаимоотношений. Конечные станции (*managed devices* - управляемые устройства), такие как компьютерные системы и другие сетевые устройства, прогоняют программные средства, позволяющие им посылать сигналы тревоги, когда они распознают проблемы. Проблемы распознаются, когда превышен один или более порогов, заданных пользователем. *Management entities* (управляющие объекты)

запрограммированы таким образом, что после получения этих сигналов тревоги они реагируют выполнением одного, нескольких или группы действий, включающих:

- Уведомление оператора
- Регистрацию события
- Отключение системы
- Автоматические попытки исправления системы

Управляющие объекты могут также опросить конечные станции, чтобы проверить некоторые переменные. Опрос может быть автоматическим или его может инициировать пользователь. На эти запросы в управляемых устройствах отвечают "агенты". Агенты - это программные модули, которые накапливают информацию об управляемом устройстве, в котором они расположены, хранят эту информацию в "базе данных управления" и предоставляют ее (проактивно или реактивно) в управляющие объекты, находящиеся в пределах "систем управления сети" (NMSs), через протокол управления сети. В число известных протоколов управления сети входят "the Simple Network Management Protocol (SNMP)" (простой протокол сетевого управления) и "Common Management Information Protocol (CMIP)" (Протокол Информации Общего Управления). "Management proxies" (Уполномоченные управления) - это объекты, которые обеспечивают информацию управления от имени других объектов. Типичная архитектура управления сети показана на рис. 2-1.[9]

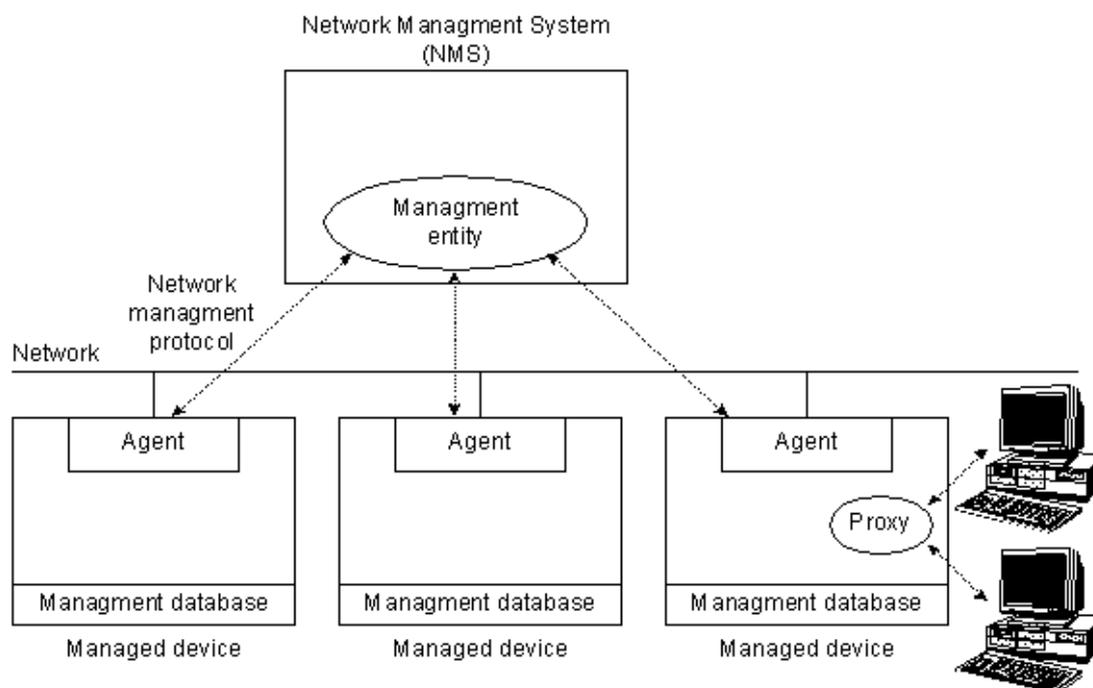


Рис 2.1 - Архитектура управления сети

### Структура системы управления

Существует два принципиальных подхода к организации управления сложными сетями:

- централизованное управление;
- децентрализованное управление.

Централизованное управление осуществляется из единого центра управления сетью, в который стекается вся информация управления от всех управляемых объектов. Достоинствами централизованного управления являются:

- концентрация всей информации о состоянии сети в одном узле управления;
- целостная картина построения сети;
- относительная простота управления правами администраторов сети;

- минимальная длина цикла управления;
- непротиворечивость принимаемых решений.

В то же время при значительном масштабе сети централизованное управление теряет ряд преимуществ. К недостаткам такого подхода следует отнести:

- уязвимость системы управления;
- значительный объём обрабатываемой информации требует высокопроизводительных серверов;
- значительная часть пропускной способности каналов сети используется для передачи служебной информации центру управления.

Децентрализованное управление сетью характеризуется отсутствием единого центра управления сетью. Его функции перераспределяются между множеством систем управления сетью. Достоинствами такого подхода являются:

- живучесть системы управления;
- отсутствует необходимость в высокопроизводительных серверах;
- меньшие по сравнению с централизованным подходом объёмы обрабатываемой информации и трафик служебной информации.

К недостаткам данного подхода следует отнести:

- сложность разграничения «зон ответственности»;
- сложность управления правами администраторов сети;
- отсутствие целостной картины построения сети;
- противоречивость принимаемых решений.[7]

### Уровни управления

В многоуровневой архитектуре TMN выделены пять уровней управления:

- бизнесом;
- услугами;
- сетью;
- элементами сети;
- уровень элементов сети.

### Области управления

Согласно стандартам ISO, существует пять областей управления:

- ошибками;
- конфигурацией;
- доступом;
- производительностью;
- безопасностью.[7]

### Протоколы управления

В своей работе системы управления опираются на стандартизованные протоколы управления, такие как:

- SNMP — один из первых и наиболее простой протокол управления, в настоящий момент актуальной является третья версия протокола, поддерживается в очень большом количестве устройств;
- CMIP — протокол управления, рекомендованный ISO в качестве базового, не получил широкого распространения вследствие своей сложности;
- TMN — концепция сетевого управления, включающая в себя множество протоколов управления и вводящая понятие уровней управления;
- LNMP — протокол управления для ЛВС;
- ANMP — протокол управления для сетей специального назначения.[7,9]

## Сеть управления телекоммуникациями (TMN Telecommunications Management Network )

Сеть управления телекоммуникациями (TMN) определяется системой стандартов на эту сеть. Термин "управление сетью" в начале 1980-х годов означал поддержание правильного функционирования и техническое обслуживание телекоммуникационных сетей.[8,9]

Широко распространённые в настоящее время системы сетевого управления, работающие на базе протокола SNMP являются сильно упрощёнными с «точки зрения» TMN.[10]

Поддержание правильного функционирования — это обеспечение выполнения основных задач, поставленных перед сетью, в нормальных условиях и в ситуациях, когда меняются характеристики сети, — например, когда увеличивается поступающая пользовательская нагрузка (трафик). Техническое обслуживание подразумевает работу по восстановлению работоспособности или характеристик сети, когда нарушается работа элементов, входящих в саму сеть (отказы оборудования или программы). При этом применяется комплекс мер, включающий оперативную диагностику для выявления места повреждения и проведение работ по устранению неисправностей.[8]

В соответствии с концепцией TMN процесс управления сетью включает в себя следующие функции управления:

- управление процессом устранения отказов (Fault Management, FM);
- управление конфигурацией сети (Configuration Management, CM);
- управление расчётами с пользователями и поставщиками услуг (Accounting Management, AM);
- контроль производительности сети (Performance Management, PM);

- обеспечение безопасности работы сети (Security Management, SM).[10]

Однако существенное развитие этих функций в последние годы привело к расширению области использования термина "управление сетью".

Основные положения системы TMN разрабатывались многими организациями, но главные правила и основные положения, используемые в сетях, являются рекомендациями следующих организаций: Международная организация стандартов (ISO — International Standards Organization, ИСО), Сектор стандартизации электросвязи Международного союза электросвязи (ITU — International Telecommunications Union — Telecommunication Standardization), Американский национальный институт стандартов (ANSI — American National Standards Institute), ETSI (European Telecommunication Standards Institute — Европейский институт стандартов электросвязи).[8]

### Основные принципы TMN

Концепция TMN охватывает сетевые элементы (NE) — компьютеры, базы данных, терминалы, сети связи и системы по поддержанию функционирования (OSS). Она связывает их в структуру, архитектуру, организация которой обеспечивает взаимосвязь различных типов сетевых элементов и систем поддержки функционирования сети. TMN также описывает стандартизированные интерфейсы и протоколы, используемые для обмена информацией между ними, а также функциональные возможности, необходимые для управления сетью.

Объектами управления в модели TMN служат:

Сетевой элемент — NE (Network Element) и Система поддержки функционирования — OSS (Operations Support Systems). Сетевой элемент —

аппаратурная единица оборудования сети, управляемая в TMN. Это могут быть и простые, и очень сложные, и "интеллектуально продвинутые" сетевые элементы, как, например, станции с программным управлением, с собственной системой поддержки функционирования и технического обслуживания. Они обеспечивают непрерывное наблюдение за своей работой, инициируют аппаратную и программную автоматические обработки сигнала аварии и содержат избыточное оборудование, например, в форме дублирования важных функциональных частей. Когда возникает отказ, автоматически включается диагностика, которая может определить характер ошибки, заблокировать дефектный модуль и связанное с ним оборудование.

Как противоположность сетевому элементу "станция" мы можем привести другой NE — "регенератор", который является наименьшей единицей в сети цифровой передачи сигналов. Число регенераторов на сети огромно, но они не содержат большого числа элементов и подсистем обслуживания. Эти простые модули могут вызвать серьезную аварию в случае ошибки.

Эти два примера сетевых элементов представляют два полюса — наиболее управляемые объекты (телефонная станция) и наименее управляемые (регенератор). Диапазон между ними включает много других типов сетевых элементов.

Второй тип объектов управления TMN — OSS (системы поддержки функционирования).

Этот термин определяет процедуры (не только автоматизированные, но и, возможно, выполняемые вручную), которые направлены на поддержание функционирования сети. Это могут быть системы:

- обмена с имеющимся оборудованием управления NE;
- установления порядка обработки аварийных сообщений;

- инициирования процедур в NE;
- диспетчерования и ведения очередей на обработку;
- введения финансовых расчетов и других процедур.

Сетевые элементы (NE) и системы поддержки функционирования связываются между собой с помощью Q-интерфейса, который определен в виде двух частей:

- информационной модели и
- протоколов связи.[8]

## 2. Протокол SNMP для управления сетями связи

**SNMP** Simple Network Management Protocol — простой протокол сетевого управления — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определен Инженерным советом интернета (IETF) как компонент TCP/IP. [12,13]

Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB (Management Information Base). Простота SNMP во многом определяется простотой MIB SNMP, особенно их первых версий MIB I и MIB II. Кроме того, сам протокол SNMP также весьма несложен. Существуют стандарты,

определяющие структуру MIB, в том числе набор типов ее объектов, их имена и допустимые операции над этими объектами .

Древовидная структура MIB содержит обязательные (стандартные) поддеревья, а также в ней могут находиться частные (private) поддеревья, позволяющие изготовителю интеллектуальных устройств управлять какими-либо специфическими функциями устройства на основе специфических объектов MIB.

Агент в протоколе SNMP - это обрабатывающий элемент, который обеспечивает менеджерам, размещенным на управляющих станциях сети, доступ к значениям переменных MIB и тем самым дает им возможность реализовывать функции по управлению и наблюдению за устройством.

Основные операции по управлению вынесены в менеджер, а агент SNMP выполняет чаще всего пассивную роль, передавая в менеджер по его запросу значения накопленных статистических переменных. При этом устройство работает с минимальными издержками на поддержание управляющего протокола. Оно использует почти всю свою вычислительную мощность для выполнения своих основных функций маршрутизатора, моста или концентратора, а агент занимается сбором статистики и значений переменных состояния устройства и передачей их менеджеру системы управления.[13]

### Примитивы протокола SNMP

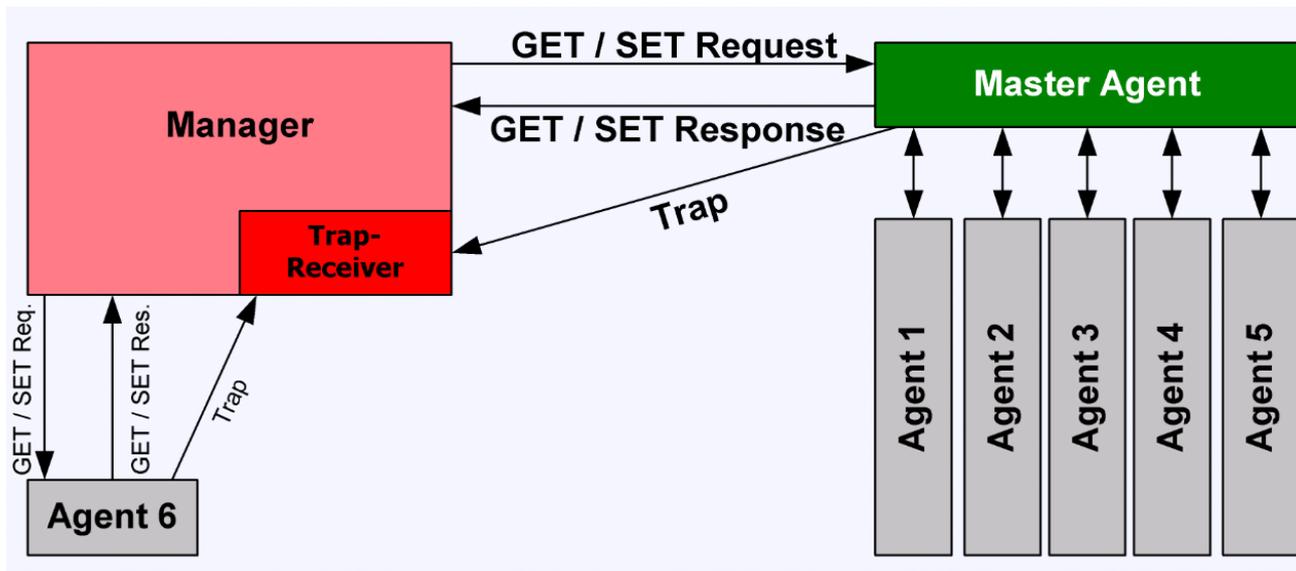


Рис.2.2 – Принцип работы SNMP

SNMP - это протокол типа «запрос-ответ», то есть на каждый запрос, поступивший от менеджера, агент должен передать ответ. Особенностью протокола является его чрезвычайная простота - он включает в себя всего несколько команд.

- Команда Get-request используется менеджером для получения от агента значения какого-либо объекта по его имени.
- Команда GetNext-request используется менеджером для извлечения значения следующего объекта (без указания его имени) при последовательном просмотре таблицы объектов.
- С помощью команды Get-response агент SNMP передает менеджеру ответ на команды Get-request или GetNext-request.
- Команда Set используется менеджером для изменения значения какого-либо объекта. С помощью команды Set происходит собственно управление устройством. Агент должен понимать смысл значений объекта, который используется для управления устройством, и на основании этих значений выполнять реальное управляющее воздействие - отключить порт, приписать порт определенной VLAN и т. п. Команда Set пригодна также для установки условия, при

выполнении которого агент SNMP должен послать менеджеру соответствующее сообщение. Может быть определена реакция на такие события, как инициализация агента, рестарт агента, обрыв связи, восстановление связи, неверная аутентификация и потеря ближайшего маршрутизатора. Если происходит любое из этих событий, то агент инициализирует прерывание.

- Команда Trap используется агентом для сообщения менеджеру о возникновении особой ситуации.
- Версия SNMP v.2 добавляет к этому набору команду GetBulk, которая позволяет менеджеру получить несколько значений переменных за один запрос.

### Структура SNMP MIB

На сегодня существует несколько стандартов на базы данных управляющей информации для протокола SNMP. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Кроме этого существуют стандарты для специальных устройств MIB конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

Версия MIB-I (RFC 1156) определяет 114 объектов, которые подразделяются на 8 групп.

- System - общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы).

- Interfaces - параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета).
- Address Translation Table - описание соответствия между сетевыми и физическими адресами (например, по протоколу ARP).
- Internet Protocol - данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика о IP-пакетах).
- ICMP - данные, относящиеся к протоколу обмена управляющими сообщениями ICMP.
- TCP - данные, относящиеся к протоколу TCP (например, о TCP-соединениях)
- UDP - данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UDP-дейтаграмм).
- EGP - данные, относящиеся к протоколу обмена маршрутной информацией Exterior Gateway Protocol, используемому в Internet (число принятых с ошибками и без ошибок сообщений).[13]

### **3. Протоколы маршрутизации Open Shortest Path First OSPF, Multiprotocol Label Switching MPLS.**

#### **Open Shortest Path First OSPF**

OSPF обеспечивает маршрутизацию пакетов IP исключительно на основе IP-адресов получателей, определенных из заголовка пакетов IP. Пакеты IP маршрутизируются без их изменения инкапсуляция в какие-то иные пакеты. OSPF является динамическим протоколом маршрутизации, обеспечивающим быстрое обнаружение топологических изменений в AS (например, сбои маршрутизаторов или каналов) и расчет новых беспетлевых (loop-free) маршрутов. Период схождения (convergence) – расчет нового маршрута – достаточно короток и уровень служебного трафика невелик. В протоколах на основе состояния каналов (link-state) каждый маршрутизатор

поддерживает базу данных с описанием топологии AS. Эти базы называют базами данных о состоянии каналов 1 (link-state database). Базы данных всех маршрутизаторов идентичны. Каждый элемент базы данных представляет собой локальное состояние отдельного маршрутизатора (например, поддерживаемые интерфейсы или доступные соседи). Маршрутизаторы распространяют информацию о своем локальном состоянии путем лавинной маршрутизации (flooding).

Все маршрутизаторы работают в параллель, используя одинаковый алгоритм. На основе базы каналов каждый маршрутизатор строит дерево кратчайших путей, корнем которого является сам маршрутизатор. Это дерево содержит маршруты ко всем адресатам внутри AS. Маршрутная информация внешнего происхождения представляется как листья дерева. При наличии нескольких путей равной стоимости к одному адресату, трафик поровну распределяется между всеми маршрутами. Стоимость маршрута описывается безразмерной метрикой, представляемой в виде одного числа. OSPF позволяет группировать сети – такие группы называют областями (area). Топология области невидима для остальной части AS. Такое сокрытие (избыточной) информации позволяет существенно снизить уровень служебного трафика. Кроме того, маршрутизация внутри области определяется исключительно внутренней топологией этой области, что обеспечивает защиту областей от использования некорректной маршрутной информации. Понятие области является обобщением подсетей IP. OSPF обеспечивает возможность гибкой настройки подсетей IP. Каждый маршрут в OSPF распространяется с указанием адресата и маски подсети. Две разных подсети одной сети IP могут иметь различные размеры (т. е., разные маски) – для обозначения этого обычно используется термин variable length subnetting (переменный размер подсетей). Пакеты маршрутизируются по пути с наилучшим (т. е., самым длинным или более конкретным) соответствием. Маршруты к хостам рассматриваются как пути в подсети с маской из одних единиц (all ones или 0xffffffff 2 ). Весь обмен информацией OSPF

осуществляется с использованием аутентификации. Это означает, что в маршрутизации внутри AS могут участвовать только уполномоченные маршрутизаторы. Могут использоваться различные схемы аутентификации; в частности, допустимо применение различных схем для каждой подсети IP. Внешние маршрутные данные (т. е., маршруты, полученные от протоколов внешних шлюзов EGP - например, BGP - [Ref23]) анонсируются через AS. Такие данные сохраняются отдельно от данных OSPF о состоянии каналов. Каждый внешний маршрут может также быть помечен (tagged) анонсирующим его маршрутизатором – это дает возможность передачи дополнительной информации между маршрутизаторами на границе AS.[16]

### Характеристики OSPF

OSPF—это протокол маршрутизации с учетом состояния каналов, который предусматривает, что все маршрутизаторы в домене маршрутизации обмениваются информацией и благодаря этому имеют сведения о топологии всей сети. Поскольку каждый маршрутизатор имеет информацию о топологии всей сети, применение алгоритма SPF позволяет обеспечить исключительно быстрый переход сети в установившееся состояние. Протокол OSPF обладает также следующими важными характеристиками:

- предоставляет маршрутную информацию для той части набора протоколов TCP/IP, которая относится к протоколу IP, поэтому, наряду с RIP, наиболее часто используется в качестве маршрутизирующего протокола;
- предусматривает передачу от одного маршрутизатора к другому только данных об обновлениях в таблицах, а не всех таблиц;
- в конечном итоге является более экономичным маршрутизирующим протоколом по сравнению с RIP, поскольку требует передачи меньшего объема сетевого трафика.[14]

## Протокол маршрутизации Multiprotocol Label Switching MPLS

MPLS (англ. MultiProtocol Label Switching — многопротокольная коммутация по меткам) — механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток. MPLS является масштабируемым и независимым от каких-либо протоколов (PPTP, L2TP, PPPoE и т.д.) механизмом передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счет этого возможно создание сквозного виртуального канала, независимого от среды передачи и использующего любой протокол передачи данных.

MPLS VPN сеть делится на две области: IP сети клиентов и магистраль провайдера. Классическая конструкция MPLS L3VPN состоит из следующих компонентов: граничные маршрутизаторы провайдера LER, обращенные к клиентскому оборудованию CE, соединены между собой LSR маршрутизаторами в MPLS домене.

Маршрутизаторы, расположенные на входе или выходе MPLS-сети называются LER (англ. Label Edge Router — граничный маршрутизатор меток). LER на входе в MPLS-сеть добавляют метку MPLS к пакету данных, а LER на выходе из MPLS-сети удаляет метку MPLS из пакета данных.

Маршрутизаторы, выполняющие маршрутизацию пакетов данных, основываясь только на значении метки, называются LSR (англ. Label Switching Router — коммутирующий метки маршрутизатор).

LDP (англ. Label Distribution Protocol) – протокол, который используется LSR-маршрутизаторами для обмена информацией о метках. Предоставляет возможность маршрутизаторам обнаруживать друг друга и устанавливать взаимодействие.

LSP (англ. Label Switch Path) – последовательность LSR, которые коммутируют помеченный пакет через сеть MPLS. Фактически, это маршрут следования пакетов через сеть MPLS.

MPLS L3VPN инфраструктура предполагает обеспечение изоляции распределенных клиентских IP сетей в рамках VPN. То есть обеспечивается только обмен пакетами между IP сетями одной VPN.

Каждая VPN логически связана с одним или более комплексов маршрутизации и пересылки (VRF). VRF определяет членство в VPN подсети за узлом CE, подключенного к PE. Интерфейсы PE маршрутизаторов, обращенные к CE, логически связаны с индивидуальными VRF.[24]

#### Принцип коммутации

В основе MPLS лежит принцип обмена меток. Любой передаваемый пакет ассоциируется с тем или иным классом сетевого уровня (Forwarding Equivalence Class, FEC), каждый из которых идентифицируется определенной меткой. Значение метки уникально лишь для участка пути между соседними узлами сети MPLS, которые называются также маршрутизаторами, коммутирующими по меткам (Label Switching Router, LSR). Метка передается в составе любого пакета, причем способ ее привязки к пакету зависит от используемой технологии канального уровня.

Маршрутизатор LSR получает топологическую информацию о сети, участвуя в работе алгоритма маршрутизации— OSPF, BGP, IS-IS. Затем он начинает взаимодействовать с соседними маршрутизаторами, распределяя метки, которые в дальнейшем будут применяться для коммутации. Обмен метками может производиться с помощью как специального протокола распределения меток (Label Distribution Protocol, LDP), так и модифицированных версий других протоколов сигнализации в сети (например, незначительно видоизмененных протоколов маршрутизации, резервирования ресурсов RSVP и др.).

Распределение меток между LSR приводит к установлению внутри домена MPLS путей с коммутацией по меткам (Label Switching Path, LSP).

Каждый маршрутизатор LSR содержит таблицу, которая ставит в соответствие паре «входной интерфейс, входная метка» тройку «префикс адреса получателя, выходной интерфейс, выходная метка». Получая пакет, LSR по номеру интерфейса, на который пришел пакет, и по значению привязанной к пакету метки определяет для него выходной интерфейс. (Значение префикса применяется лишь для построения таблицы и в самом процессе коммутации не используется.) Старое значение метки заменяется новым, содержащимся в поле «выходная метка» таблицы, и пакет отправляется к следующему устройству на пути LSP. Вся операция требует лишь одноразовой идентификации значений полей в одной строке таблицы. Это занимает гораздо меньше времени, чем сравнение IP-адреса отправителя с наиболее длинным адресным префиксом в таблице маршрутизации, которое используется при традиционной маршрутизации.[23]

#### Преимущества технологии MPLS

- Отделение выбора маршрута от анализа IP-адреса (дает возможность предоставлять широкий спектр дополнительных сервисов при сохранении масштабируемости сети)
- Ускоренная коммутация (сокращает время поиска в таблицах)
- Гибкая поддержка QoS, интегрированных сервисов и виртуальных частных сетей
- Эффективное использование явного маршрута
- Сохранение инвестиций в установленное ATM-оборудование
- Разделение функциональности между ядром и граничной областью сети [22,23]

### **Выводы по Главе II**

Из изложенного во второй главе, следует что:

- 1- Существует два принципиальных подхода к организации управления сложными сетями:

- централизованное управление;
- децентрализованное управление.

2- Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB

3- Широко используемым Протокол маршрутизации является OSPF и MPLS .

## Глава III. Построение экспериментальной модели сети NGN, сравнения программных обеспечений и наилучшего метода управления

### 1. Построение экспериментальной модели NGN с маршрутизаторами Cisco 7200 на эмуляторе GNS3

Магистральная топология экспериментальной сети NGN

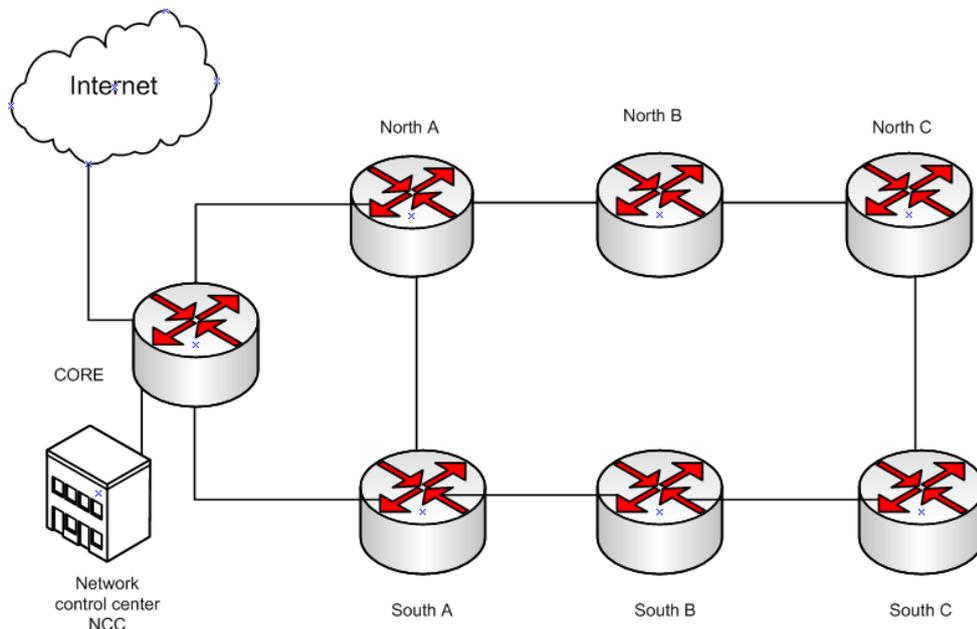


Рис.3.1 - Магистральная топология

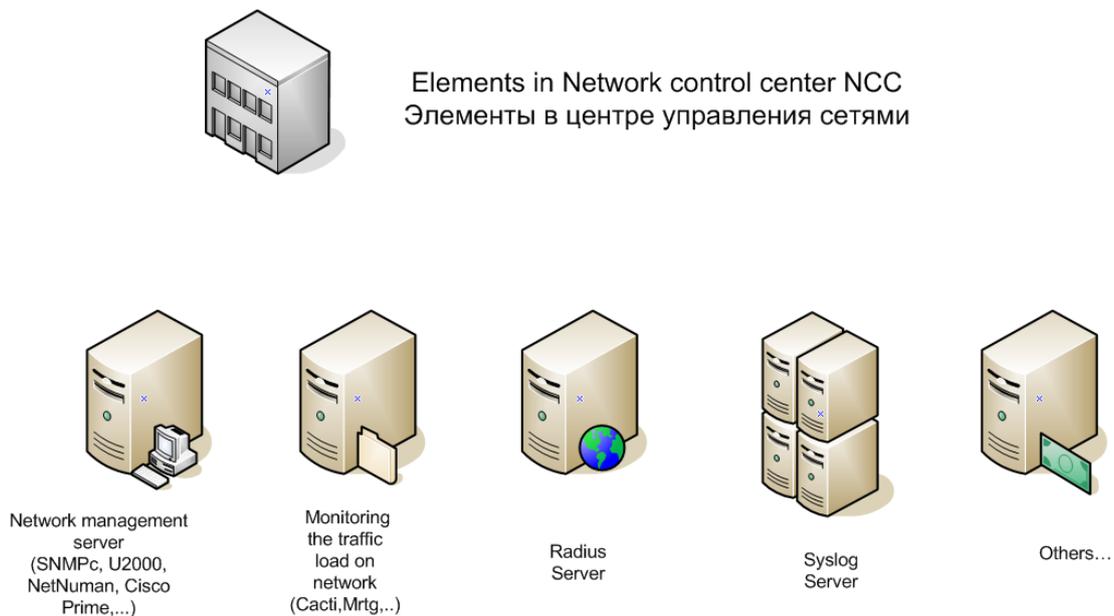


Рис.3.2 – Элменты в центре управления сетями

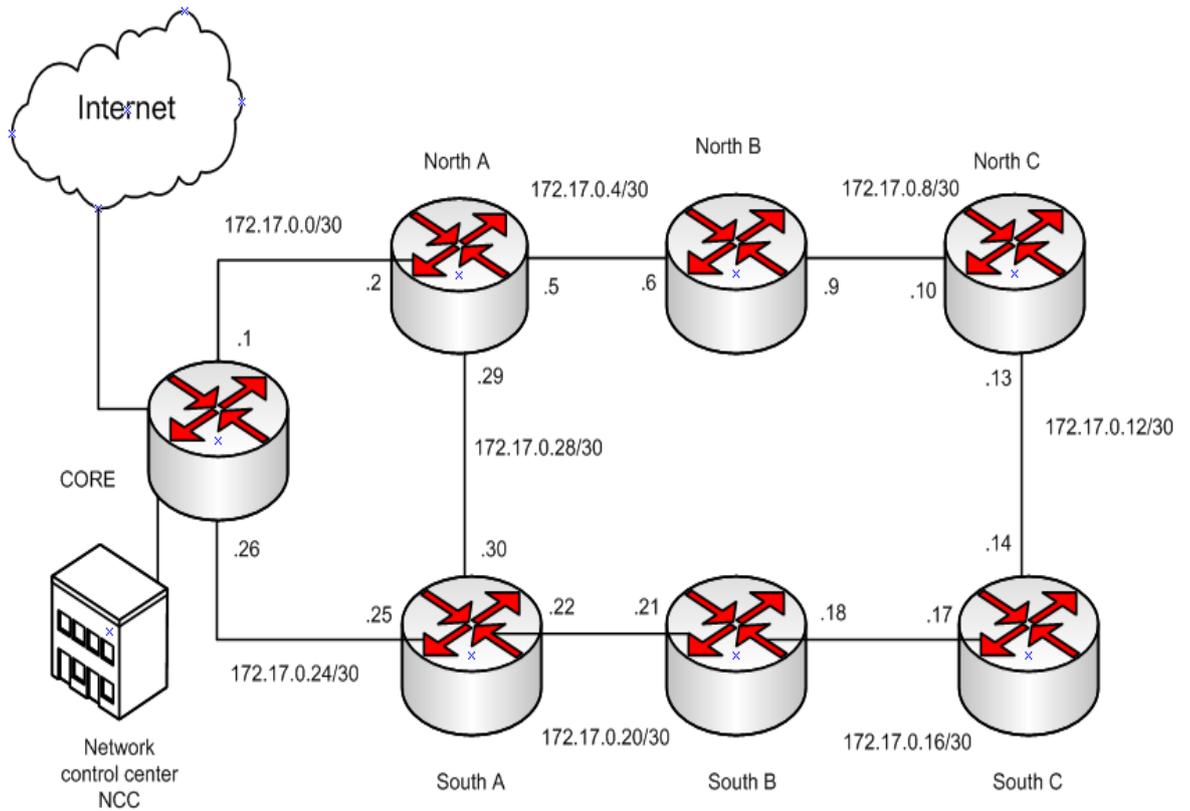


Рис.3.3 – План IP адресации

Настроим каждый маршрутизатор соответствующем IP адресом и настроим протокол динамической маршрутизации OSPF.

### Настройка маршрутизатора **CORE [R1]**

```

R1_CORE_CORE#
hostname R1_CORE_CORE
!
!
no ip domain lookup
!
interface Loopback0
ip address 172.17.254.1 255.255.255.255
!
interface FastEthernet0/0
description ## LINK TO R2 0/0 ##

```

```

ip address 172.17.0.1 255.255.255.252
duplex half
!
interface Ethernet1/0
description ## LINK TO R7 1/0 ##
ip address 172.17.0.26 255.255.255.252
duplex half
!
router ospf 1
router-id 172.17.254.1
log-adjacency-changes
redistribute connected subnets
redistribute static subnets
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface Ethernet1/0
network 172.17.0.0 0.0.0.3 area 0
network 172.17.0.24 0.0.0.3 area 0
!
end

```

R1\_CORE\_CORE#

### Настройка маршрутизатора **North A [R2]**

```

R2_North_A#
!
hostname R2_North_A
!
!
interface Loopback0
ip address 172.17.254.2 255.255.255.255
!
interface FastEthernet0/0
description ## LINK TO R1 0/0 ##
ip address 172.17.0.2 255.255.255.252
duplex half
!
interface Ethernet1/0
description ## LINK TO R3 1/1 ##
ip address 172.17.0.5 255.255.255.252
duplex half

```

```
!  
interface Ethernet1/1  
description ## LINK TO R7 1/2 ##  
ip address 172.17.0.29 255.255.255.252  
duplex half  
!  
!  
router ospf 1  
router-id 172.17.254.2  
log-adjacency-changes  
redistribute connected subnets  
redistribute static subnets  
passive-interface default  
no passive-interface FastEthernet0/0  
no passive-interface Ethernet1/0  
no passive-interface Ethernet1/1  
network 172.17.0.0 0.0.0.3 area 0  
network 172.17.0.4 0.0.0.3 area 0  
network 172.17.0.28 0.0.0.3 area 0  
!  
end
```

R2\_North\_A#

### Настройка маршрутизатора **North B [R3]**

R3\_North\_B#

```
!  
hostname R3_North_B  
!  
interface Loopback0  
ip address 172.17.254.3 255.255.255.255  
!  
interface Ethernet1/0  
description ## LINK TO R4 1/0 ##  
ip address 172.17.0.9 255.255.255.252  
duplex half  
!  
interface Ethernet1/1  
description ## LINK TO R2 1/0 ##  
ip address 172.17.0.6 255.255.255.252  
duplex half
```

```
!  
!  
router ospf 1  
  log-adjacency-changes  
  redistribute connected subnets  
  redistribute static subnets  
  passive-interface default  
  no passive-interface Ethernet1/0  
  no passive-interface Ethernet1/1  
  network 172.17.0.4 0.0.0.3 area 0  
  network 172.17.0.8 0.0.0.3 area 0  
!  
end
```

R3\_North\_B#

### Настройка маршрутизатора **North C [R4]**

R4\_North\_C#

```
!  
hostname R4_North_C  
!  
interface Loopback0  
  ip address 172.17.254.4 255.255.255.255  
!  
interface FastEthernet0/0  
  no ip address  
  shutdown  
  duplex half  
!  
interface Ethernet1/0  
  description ## LINK TO R3 1/0 ##  
  ip address 172.17.0.10 255.255.255.252  
  duplex half  
!  
interface Ethernet1/3  
  description ## LINK TO R5 1/3 ##  
  ip address 172.17.0.13 255.255.255.252  
  duplex half  
!  
!  
router ospf 1
```

```
log-adjacency-changes
redistribute connected subnets
redistribute static subnets
passive-interface default
no passive-interface Ethernet1/0
no passive-interface Ethernet1/3
network 172.17.0.8 0.0.0.3 area 0
network 172.17.0.12 0.0.0.3 area 0
!
end
```

R4\_North\_C#

### Настройка маршрутизатора **South C [R5]**

R5\_South\_C#

```
!
hostname R5_South_C
!
!
interface Loopback0
ip address 172.17.254.5 255.255.255.255
!
!
interface Ethernet1/2
description ## LINK TO R6 1/2 ##
ip address 172.17.0.17 255.255.255.252
duplex half
!
interface Ethernet1/3
description ## LINK TO R3 1/3 ##
ip address 172.17.0.14 255.255.255.252
duplex half
!
!
router ospf 1
log-adjacency-changes
redistribute connected subnets
redistribute static subnets
passive-interface default
no passive-interface Ethernet1/2
no passive-interface Ethernet1/3
```

```
network 172.17.0.12 0.0.0.3 area 0
network 172.17.0.16 0.0.0.3 area 0
!
!
end
```

R5\_South\_C#

### Настройка маршрутизатора **South B [R6]**

R6\_South\_B#

```
!
hostname R6_South_B
!
interface Loopback0
ip address 172.17.254.6 255.255.255.255
!
!
interface Ethernet1/0
description ## LINK TO R7 1/1 ##
ip address 172.17.0.21 255.255.255.252
duplex half
!
!
interface Ethernet1/2
description ## LINK TO R5 1/2 ##
ip address 172.17.0.18 255.255.255.252
duplex half
!
router ospf 1
log-adjacency-changes
redistribute connected subnets
redistribute static subnets
passive-interface default
no passive-interface Ethernet1/0
no passive-interface Ethernet1/2
network 172.17.0.16 0.0.0.3 area 0
network 172.17.0.20 0.0.0.3 area 0
!
!
end
```

R6\_South\_B#

### Настройка маршрутизатора **South A [R7]**

R7\_South\_A#

```
!  
hostname R7_South_A  
!  
!  
interface Loopback0  
ip address 172.17.254.7 255.255.255.255  
!  
interface Ethernet1/0  
description ## LINK TO R1 1/0 ##  
ip address 172.17.0.25 255.255.255.252  
duplex half  
!  
interface Ethernet1/1  
description ## LINK TO R6 1/0 ##  
ip address 172.17.0.22 255.255.255.252  
duplex half  
!  
interface Ethernet1/2  
description ## LINK TO R2 1/1 ##  
ip address 172.17.0.30 255.255.255.252  
duplex half  
!  
!  
router ospf 1  
router-id 172.17.254.7  
log-adjacency-changes  
redistribute connected subnets  
redistribute static subnets  
passive-interface default  
no passive-interface Ethernet1/0  
no passive-interface Ethernet1/1  
no passive-interface Ethernet1/2  
network 172.17.0.20 0.0.0.3 area 0  
network 172.17.0.24 0.0.0.3 area 0  
network 172.17.0.28 0.0.0.3 area 0  
!  
!
```

end

R7\_South\_A#

Проверим связь между маршрутизаторами с помощью команды Ping

```
R1_CORE_CORE#tcls
R1_CORE_CORE#tclsh
R1_CORE_CORE(tcl)#foreach address {
+>172.17.254.1
+>172.17.254.2
+>172.17.254.3
+>172.17.254.4
+>172.17.254.5
+>172.17.254.6
+>172.17.254.7
+>} { ping $address rep 15 si 1500
+>}
```

Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.1, timeout is 2 seconds:

!!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 1/3/8 ms

Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.2, timeout is 2 seconds:

!!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 16/81/148 ms

Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.3, timeout is 2 seconds:

!!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 16/89/144 ms

Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.4, timeout is 2 seconds:

!!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 96/120/156

ms

Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.5, timeout is 2 seconds:

!!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 76/114/148

ms

Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.6, timeout is 2 seconds:

!!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 56/93/148 ms  
Type escape sequence to abort.

Sending 15, 1500-byte ICMP Echos to 172.17.254.7, timeout is 2 seconds:  
!!!!!!!!!!!!!!

Success rate is 100 percent (15/15), round-trip min/avg/max = 44/68/112 ms  
R1\_CORE\_CORE(tcl)#

### Проверим таблицу маршрутизации

R1\_CORE\_CORE#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

```

    172.17.0.0/16 is variably subnetted, 19 subnets, 2 masks
C    172.17.0.0/30 is directly connected, FastEthernet0/0
L    172.17.0.1/32 is directly connected, FastEthernet0/0
O    172.17.0.4/30 [110/11] via 172.17.0.2, 02:13:02, FastEthernet0/0
O    172.17.0.8/30 [110/21] via 172.17.0.2, 02:13:02, FastEthernet0/0
O    172.17.0.12/30 [110/31] via 172.17.0.2, 02:13:02, FastEthernet0/0
O    172.17.0.16/30 [110/30] via 172.17.0.25, 02:12:51, Ethernet1/0
O    172.17.0.20/30 [110/20] via 172.17.0.25, 02:12:51, Ethernet1/0
C    172.17.0.24/30 is directly connected, Ethernet1/0
L    172.17.0.26/32 is directly connected, Ethernet1/0
O    172.17.0.28/30 [110/11] via 172.17.0.2, 02:13:02, FastEthernet0/0
C    172.17.0.32/30 is directly connected, Ethernet1/7
L    172.17.0.33/32 is directly connected, Ethernet1/7
C    172.17.254.1/32 is directly connected, Loopback0
O E2  172.17.254.2/32 [110/20] via 172.17.0.2, 02:13:03, FastEthernet0/0
O E2  172.17.254.3/32 [110/20] via 172.17.0.2, 02:13:03, FastEthernet0/0
O E2  172.17.254.4/32 [110/20] via 172.17.0.2, 02:13:03, FastEthernet0/0
O E2  172.17.254.5/32 [110/20] via 172.17.0.25, 02:12:52, Ethernet1/0
O E2  172.17.254.6/32 [110/20] via 172.17.0.25, 02:12:52, Ethernet1/0
O E2  172.17.254.7/32 [110/20] via 172.17.0.25, 02:12:52, Ethernet1/0
R1_CORE_CORE#
```

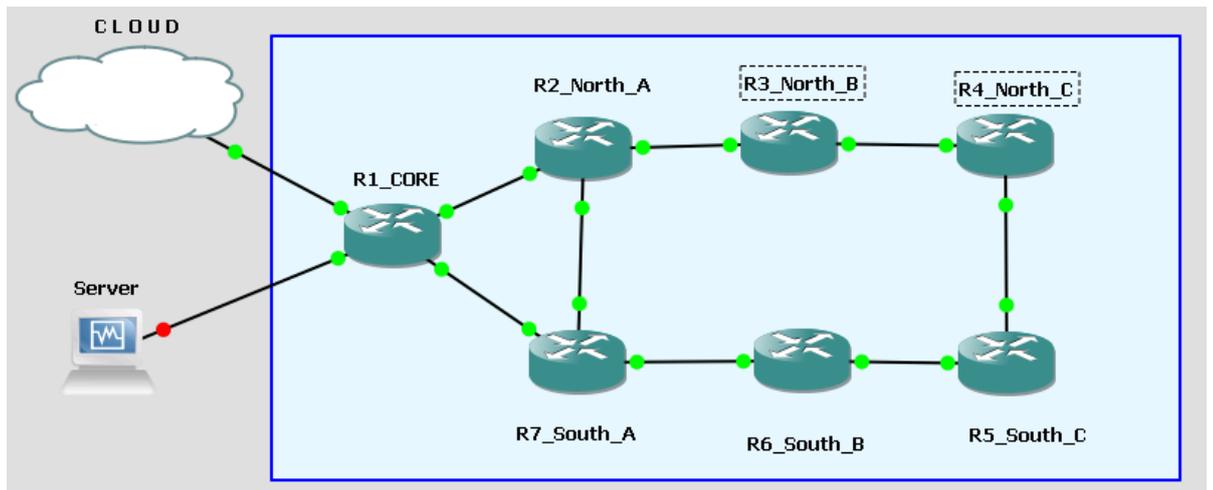


Рис.3.4 - Топология сети в GNS3

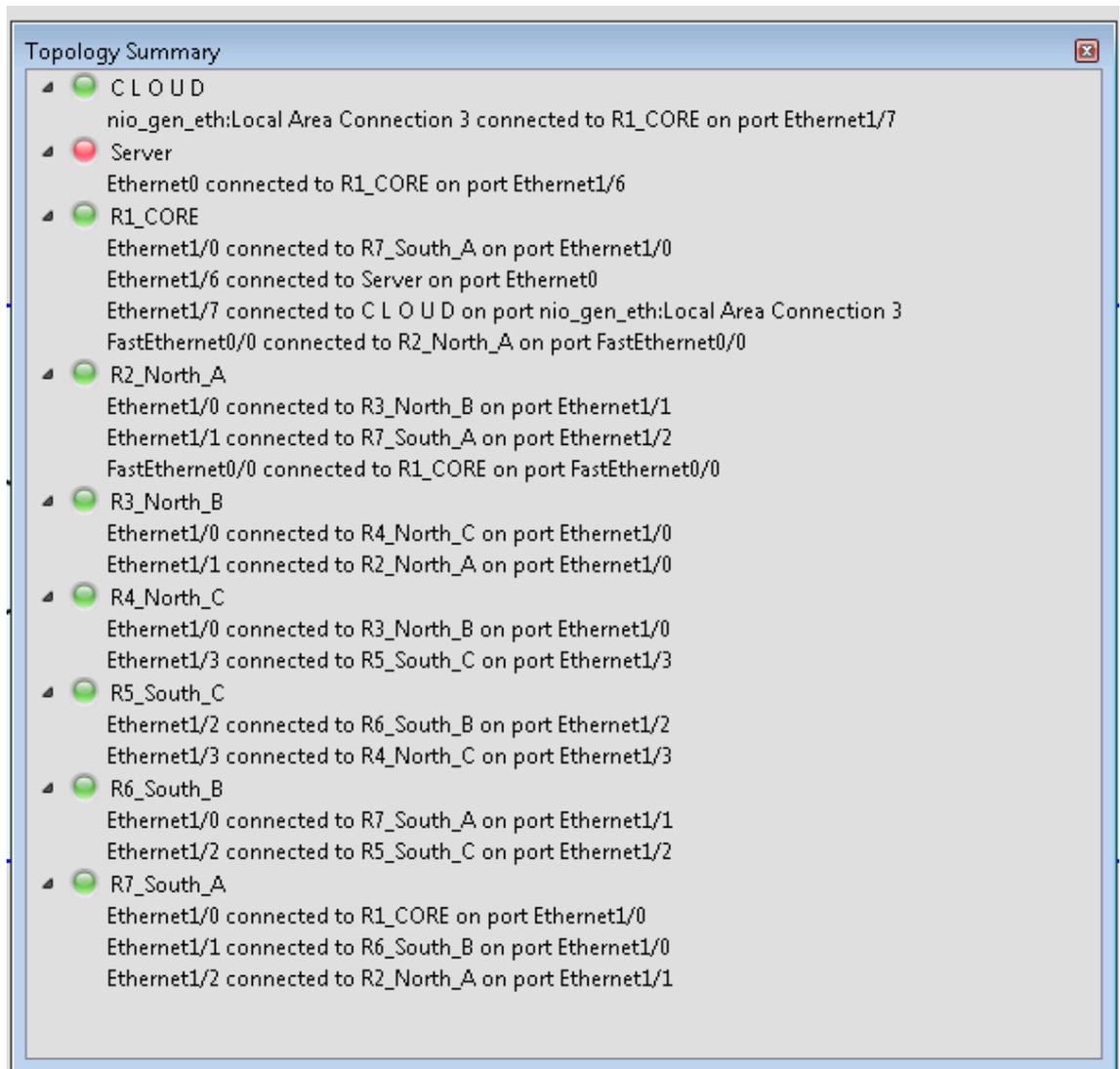


Рис.3.5 - Физическое подключения между маршрутизаторами  
**2. Сравнения программного обеспечения Cacti и Mrtg, SNMPc и NetXMS.**

В данном разделе мы рассмотрим несколько видов широко используемые программы для управления сетями. С начало рассмотрим программы Cacti и MRTG для рисования загрузенность интерфейса, процессора, оперативной памяти и другие видов графики которые нужны для управления сетями. Следующие программы SNMPc и NetXMS используется для проверки доступности оборудования, для контроля статуса интерфейсов, для сбора журнал события ов от оборудование и другие.

### Программа Cacti

Cacti это комплексное решение для сетевого графического анализа.. Cacti обеспечивает быструю регистрацию, расширенный график шаблонов, несколько методов сбора данных. Все это, завернутый в интуитивный, простой в использовании интерфейс. Cacti это полный интерфейс для RRDTool, он хранит все необходимую информацию для создания графиков и заполняет их с необходимыми данными. В качестве базы данных использует MySQL. [15]

### MRTG Multi Router Traffic Grapher

MRTG является свободным программным обеспечением под лицензией GPL. Это инструмент для организации сервиса мониторинга и измерения данных с течением времени. Данные от различных источников собираются и затем отображаются в виде графиков. Утилита первоначально была разработана Тобиасом Отикером и Дейвом Рэндом для мониторинга трафика, но впоследствии превратилась в удобный инструмент для создания графиков и сбора статистических данных для различных задач и процессов.

### Области применения

- загрузенность канала (входящий, исходящий, максимальный, средний трафик);

- использование процессора, оперативной памяти, жёсткого диска;
- наблюдение за температурными показателями аппаратных ресурсов;
- погодные данные и т.д.[16]

## SNMPc 9

Система мониторинга для масштабируемой многопользовательской сети

AGNEKO SNMPc 9 Enterprise - это надежная, простая в использовании система управления сетью в режиме реального времени с расширенными возможностями. AGNEKO SNMPc 9 Enterprise включает:

- неограниченное количество удаленных консолей
- 10 удаленных опросчиков
- неограниченное количество консолей Java
- модуль SNMPc OnLine

Ключевые характеристики продукта:

- Мониторинг SNMP устройств, серверов, приложений, сетевых соединений
- Поддержка интернет протокола версии 6 (IPv6)
- Поддержка SNMP v1, v2c и защищенного SNMP v3
- Масштабируемая распределенная архитектура
- Уведомления о событиях по Email/Пейджеру
- Основной/резервный серверы с автоматическим переключением
- Ведение журнала событий Syslog
- Автоматическое обнаружение сети
- Программирование / Интерфейсы скриптов

## NetXMS

NetXMS является система корпоративного уровня с открытым исходным кодом для управления сетью и мониторинга. Это обеспечивает комплексное управление событиями, мониторинг производительности,

предупреждая, отчетности и графиков для всех слоев ИТ-инфраструктуры - от сетевых устройств бизнес-приложений слоя.

Система имеет трехуровневую архитектуру: информация собирается путем мониторинга агентов (или наших агентов высокой производительности или SNMP агентов) и поставляется с сервером мониторинга для обработки и хранения. Администратор сети может получить доступ к собранные данные, используя богатый клиентское приложение или веб-интерфейс. После были разработаны с гибкостью и масштабируемостью в виду, NetXMS предлагает широкий спектр поддерживаемых платформ, операционных систем и СУБД, обеспечивая тем самым полную интеграцию с любой инфраструктуры.

Важные функции:

Единая платформа для управления и мониторинга всей ИТ-инфраструктуры

Предназначен для максимальной производительности и масштабируемости

- Распределенный мониторинг сети
- Автоматическое обнаружение сети
- Гибкий и простой в использовании обработки событий
- Инструменты анализа воздействия на бизнес
- Быстрое развертывание с минимальными усилиями конфигурации
- Легкий и простой интеграции со смежными продуктами
- Встроенная поддержка многих популярных платформ и операционных систем

Сравнительная таблица

	Cacti	Mrtg	NetXMS	SNMPc
Логическое	Да	Нет	Да	Да

группирование				
Автоматический обнаружение	Через плагин	Нет	Да	Да
SNMP	Да	Да	Да	Да
Syslog	Через плагин	Нет	Да	Да
Traffic Analysis	Через плагин	Нет	Нет	Нет
Внешние скрипты	Да	Да	Да	Да
Плагины`	Да	Да	Да	Да
Распределённый мониторинг	Нет	Нет	Да	Да
События	Нет	Нет	Да	Да
Карты	Плагин Weather map	Нет	Да	Да
Лицензия	GNU GPL	GNU GPL	GNU GPL	Коммерческий
Метод хранения данных	RRDtool,MySQL	Mysql	Mysql	Mysql
Диаграммы	Да	Нет	Да	Нет

Из таблица видно преимущества Cacti, NetXMS больше чем Mrtg и SNMPc. Один из примушеств NetXMS можно считать что оно бесплатный (GNU GPL) а SNMPc платный (коммерческий).

### **3. Выбор метода управления централизованный или децентрализованный, Исследования нового метода.**

Как мы уже рассмотрели во втором главе существует два принципиальных подхода к организации управления сложными сетями:

- централизованное управление;
- децентрализованное управление.

На каждом методе есть свои достоинства и недостатки, например децентрализованное управление не требует высокопроизводительные сервера но на данном методе надо будет построить сразу несколько центра управления. Централизованное управления представляет цельную картину сети и концентрацию всей информации о состоянии сети в одном узле управления. Одно из недостатков данного метода является нахождения всех серверов управления в одном месте. При аварийных ситуациях мы потеряем связь со всеми серверами управления.

Центры управления сетями состоит из несколько серверов как показано на рисунке 3.2. На сегодняшний день многие сервера используется как кластер, кластер это группа серверов, объединённых логически, способных обрабатывать идентичные запросы и использующихся как единый ресурс. Если разделить сервера установленные в центры управления сетями географически и соединить их как кластер через IP/MPLS сеть, получается централизованное метод управления с географическим резервированием. Внедряем этот метод в наш экспериментальной сеть. Как показано на рисунке 3.4 сервер с названием «Server» уже подключен на маршрутизатор CORE R1, подключем другой сервер на маршрутизатор North C и настроим между ними L2 MPLS/VPN тунел для кластеризация. Для этого сначала на всех маршрутизаторах включаем MPLS с помощью команд: « mpls ip » после настройке появляется лог сообщения о нахождения MPLS соседе на каждом маршрутизаторе, далее приведём лог с маршрутизатора CORE R1:

```
*May 31 12:15:08.867: %LDP-5-NBRCHG: LDP Neighbor 172.17.254.7:0 (1) is
UP
*May 31 12:15:09.679: %LDP-5-NBRCHG: LDP Neighbor 172.17.254.2:0 (2) is
UP
```

Настроим L2 тунел между маршрутизаторами для этого выполним следующие набор команд на CORE R1:

```
R1_CORE_CORE#conf t
R1_CORE_CORE(config)#interface ethernet 1/6
R1_CORE_CORE(config-if)#no shutdown
R1_CORE_CORE(config-if)# description LINK->>SERVER
R1_CORE_CORE(config-if)#xconnect 172.17.254.4 30 encapsulation mpls
R1_CORE_CORE(config-if-xconn)#end
R1_CORE_CORE#
```

И на маршрутизаторе North C R4:

```
R4_North_C#conf t
R4_North_C(config)#interface ethernet 1/6
R4_North_C(config-if)#description LINK->>SERVER
R4_North_C(config-if)#no shutdown
R4_North_C(config-if)#xconnect 172.17.254.1 30 encapsulation mpls
R4_North_C(config-if-xconn)# end
R4_North_C#
```

После настройке раверим состояние тунела для этого вводим:

```
R4_North_C#show mpls l2transport vc 30
```

Local intf	Local circuit	Dest address	VC ID	Status
Et1/6	Ethernet	172.17.254.1	30	UP

```
R4_North_C#
```

```
R1_CORE_CORE#show mpls l2transport vc 30
```

Local intf	Local circuit	Dest address	VC ID	Status
Et1/6	Ethernet	172.17.254.4	30	UP

```
R1_CORE_CORE#
```

Состояния канала в статусе «UP» теперь можно использовать это тунел.

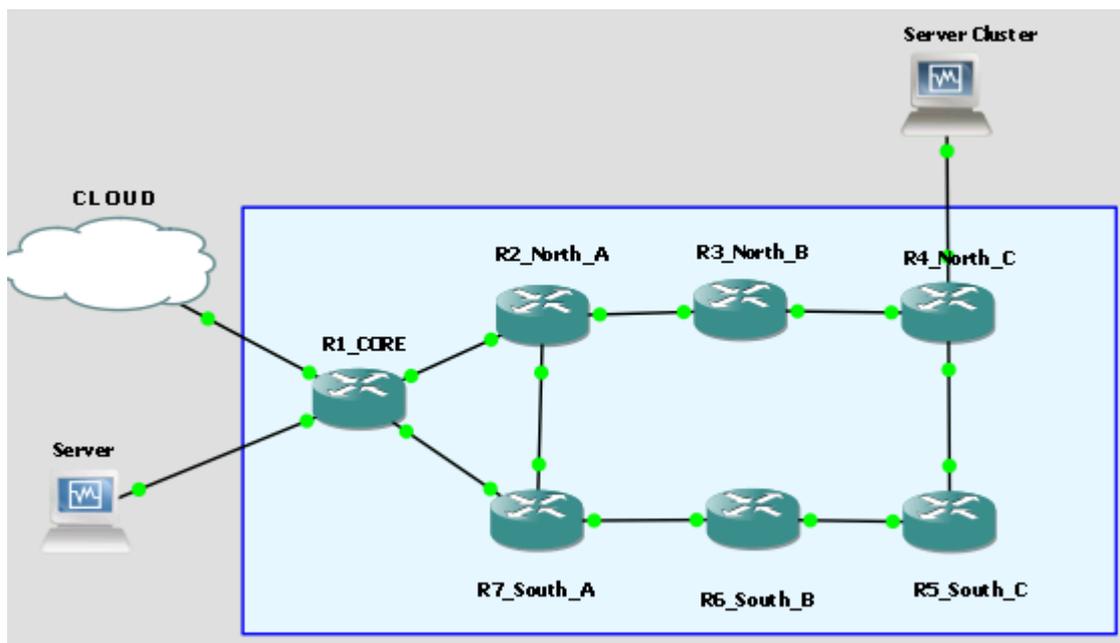


Рис 3.6 – Сервер управления «Server» и «Server Cluster» соединены между собой как кластер и резервирует друг друга.

Установим SNMPc на этом сервере и добавим маршрутизаторов магистральной сети для управления. Для добавление маршрутизаторов необходимо будет настроить SNMP конфигурацию, добавим следующий настройки на все маршрутизаторы:

```
snmp-server community magistr RO
```

```
snmp-server community magistr RW
```

Слово «magistr» необходимо указать в настройке SNMPc сервера.

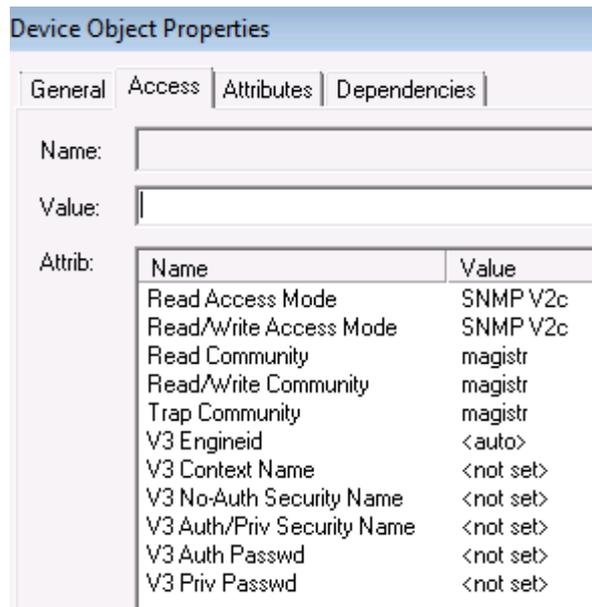


Рис.3.7 – Установим слово «magistr» пункте Community

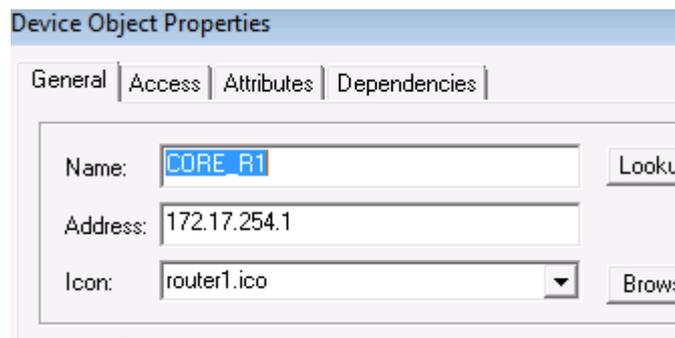
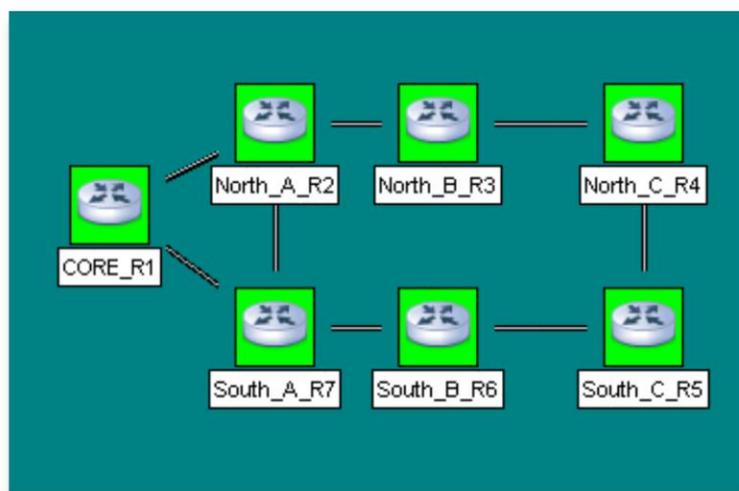


Рис.3.8 – Добавим маршрутизатор CORE R1

Таким способом добавляем и остальные маршрутизаторы и строится схема



сети

Рис.3.9 - Схема сети в SNMPc

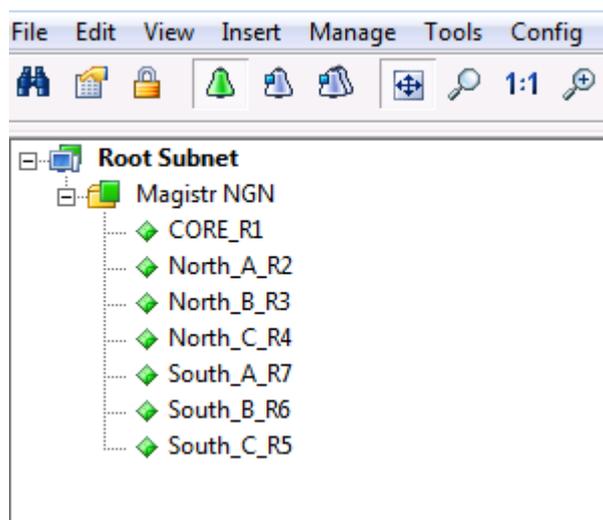


Рис.3.9 – Список элементов в SNMPc

Index	Descr	Name	Alias
1	FastEthernet0/0	Fa0/0	## LINK TO R2 0/0 ##
2	Ethernet1/0	Et1/0	## LINK TO R7 1/0 ##
3	Ethernet1/1	Et1/1	
4	Ethernet1/2	Et1/2	
5	Ethernet1/3	Et1/3	
6	Ethernet1/4	Et1/4	
7	Ethernet1/5	Et1/5	
8	Ethernet1/6	Et1/6	LINK->>SERVER
9	Ethernet1/7	Et1/7	LINK->>CLOUD
10	VoIP-Null0	Vo0	
11	Null0	Nu0	
12	Loopback0	Lo0	
13	FastEthernet0/0-mpls layer	FastEthernet0/0	
14			

Рис.3.10 – Список интерфейсов маршрутизатора CORE R1

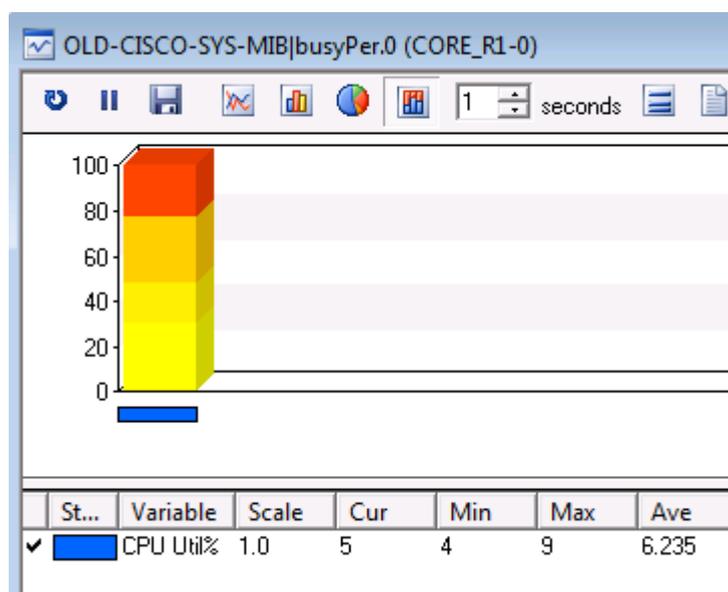


Рис.3.11 – Загруженность процессора маршрутизатора CORE R1

### Выводы по Главе III

В данной главе в первом разделе было построено экспериментальная сеть с помощью программы GNS3 и маршрутизаторами Cisco 7200. Маршрутизаторы были настроены IPv4 адресами, для маршрутизации были настроены динамическая маршрутизация OSPF. Во втором разделе было изучено широко используемые программы для управления сетью Cacti, MRTG, SNMPc, NetXMS. Сделана сравнительная таблица преимуществ и недостатков этих программ. Из таблицы видны преимущества Cacti, NetXMS больше чем Mrtg и SNMPc. Одним из преимуществ NetXMS можно считать то, что оно бесплатное (GNU GPL) а SNMPc платный (коммерческий). В третьем разделе была выбрана централизованный метод для управления с кластерным и географически разделенным подключением. Для теста установлена программа SNMPc. Схема сети была построена и настроена для управления сетью.

## Заключение

Основные выводы по проведенным исследованиям заключаются в следующем:

1. Дисциплина FIFO при высоких загрузках на сетевой интерфейс не в состоянии обеспечить необходимое качество для услуг мультисервисных сетей. Причиной является переполнение буфера более интенсивным видом трафика (видео). В результате, отбрасывается менее интенсивный трафик голоса и данных.
2. Дисциплина PQ эффективно работает только при передаче голоса (высокий приоритет) и видео (средний приоритет). При передаче трафика данных (низкий приоритет) полоса пропускания используется не эффективно.
3. Дисциплина RED удерживала задержку на установленном уровне. Но показатели других параметров превысили приемлемое значение. Данная дисциплина не эффективна при высоких загрузках.
4. Дисциплина SFQ эффективно использует полосу пропускания только при передаче не интенсивного вида трафика (голос и данные). Для интенсивного трафика (видео) полосу пропускания используется не эффективно.
5. Дисциплину приоритетного обслуживания (PQ) необходимо использовать при высоких загрузках сети.

Результаты диссертации рекомендуется использовать в мультисервисных сетях связи для обеспечения работоспособности услуг передачи данных, голоса и видео при высоких загрузках сети.

## **Список использованной литературы**

### **I. Доклады президента Республики Узбекистан И. А. Каримова**

1. Доклад Президента Республики Узбекистан Ислама Каримова на заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2012 году и важнейшим приоритетным направлениям экономической программы на 2013 год 18.01.2013.

### **II. Список основной литературы**

2. Шринивас Вегешна. Качество обслуживания в сетях IP. : Пер. с англ. – М.: «Вильямс», 2003. – 368 с.
3. Битнер В.И. «СЕТИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ» магистерская программа —Телекоммуникационная информатика» по направлению 210400.68 Телекоммуникации.
4. Кучерявый, А.Е., Сети связи следующего поколения / А.Е Кучерявый, А.Л. Цуприков. - М.: ФГУП ЦНИИС, 2006. - 278 с.
5. Кустов А. Мультисервисная сеть: качество обслуживания и мультикаст. // Системный администратор, №4, апрель 2008. – с: 72-77.
6. Назаров, А.Н. Модели и методы расчёта структурно-сетевых параметров АТМ сетей / А.Н. Назаров. - М.: Горячая линия-Телеком, 2002. -256 с.

### **III. Список интернет источников**

7. [http://ru.wikipedia.org/wiki/Управление\\_сетями\\_связи](http://ru.wikipedia.org/wiki/Управление_сетями_связи) - Управление сетями связи.

8. <http://www.intuit.ru/studies/courses/1155/269/lecture/6839?page=3>  
Техобслуживание, эксплуатация и администрирование станций, сеть управления телекоммуникациями (TMN)
9. <http://citforum.ru/nets/ito/4.shtml#4.3.1> \_ Основы управления сетями
10. <https://ru.wikipedia.org/wiki/TMN> \_\_\_\_\_ Telecommunication Management Network, Система управления сетями операторов электросвязи
11. <http://www.itu.com> INTERNATIONAL TELECOMMUNICATION UNION Recommendation X.700 (09/92)
12. <https://ru.wikipedia.org/wiki/SNMP> - Simple Network Management Protocol — простой протокол сетевого управления
13. <http://total100.narod.ru/olifer/head7.htm> \_\_ Средства анализа и управления сетями
14. [http://www.opennet.ru/docs/RUS/qos\\_oper/](http://www.opennet.ru/docs/RUS/qos_oper/) - Качество обслуживания в операторских сетях.
15. [http://www.cacti.net/what\\_is\\_cacti.php](http://www.cacti.net/what_is_cacti.php) What is Cacti?
16. <https://ru.wikipedia.org/wiki/MRTG> Multi Router Traffic Grapher

#### **IV. Список дополнительной литературы**

17. ТУИТ, Кафедра Устройства и систем радиосвязи. Конспект лекций по курсу «Техническая Эксплуатация мобильных систем связи» Составитель Д.Давронбеков.
18. Семёнов, Ю.В. Проектирование сетей связи следующего поколения / Ю.В. Семёнов. - М.: ОАО Гипросвязь, 2005. - 240 с.
19. Перспективные телекоммуникационные технологии. Потенциальные возможности / Под ред. Л.Д. Реймана и Л.Е. Варакина. - М.: МАС, 2001. - 256 с.
20. Структура и реализация сетей на основе протокола OSPF. Томас М. Москва, Киев 2004.
21. Протокол OSPF версии 2, Request for Comments (RFC) 2328. J. Moy

22. MPLS в разнородных сетях СЕССИЯ RST-3104. Михаил Захватов,  
Consulting System Engineer, CCIE
23. Примеры технологий коммутации по меткам. Бигаров Руслан D-LINK  
(Pre-sale manager)