

«Утверждаю»

«Утверждаю»

«___» _____ 2008 г.

«___» _____ 2008 г.

Сеть широкополосного доступа

«Стрим-ТВ»

Шифр: СИТ.СТВ.ЭТП.2.9/08

Эскизно-технический проект

«Согласовано»

«Согласовано»

Москва 2008

Име. № подл.	
Подп. и дата	
Взам. инв. №	

ОГЛАВЛЕНИЕ

1.	Общие положения.....	4
2.	Общее описание технического решения	6
2.1.	Описание топологии и логики функционирования СШПД.....	6
2.1.1.	Общая схема физической и логической организации сети	6
2.1.2.	Описание топологии СШПД.....	7
2.1.3.	Описание общих принципов оказания услуг TriplePlay	10
2.2.	Описание подсистем СШПД.	10
2.2.1.	Подсистема пограничного сегмента	10
2.2.2.	Сервисная подсистема: уровень BRAS.....	13
2.2.3.	Сервисная подсистема: портал «Стрим-ТВ»	16
2.2.4.	Ядро сети	17
2.2.5.	Магистральный уровень (МУ).....	24
2.2.6.	Уровень доступа (ДУ)	28
2.2.7.	Узел телематических служб.....	31
2.2.8.	Технологическая подсистема СШПД	37
2.3.	Общие настройки оборудования СШПД.....	46
2.3.1.	Правила именования объектов в СШПД.....	48
2.3.2.	Принципы распределения VLAN	50
2.3.3.	Принципы распределения адресов.....	51
2.4.	Маршрутизация в сети «Стрим-ТВ».....	55
2.4.1.	Общие принципы организации маршрутизации	55
2.4.2.	Маршрутизация с внешними сетями	55
2.4.3.	Маршрутизация с внутренними сетями	56
2.5.	Организация многоадресных рассылок в СШПД.....	58
2.5.1.	Общие принципы организации многоадресных рассылок	58
2.5.2.	Логическая схема организации многоадресных рассылок	59
2.6.	Обеспечение качества обслуживания в сети в СШПД	60
2.6.1.	Общие принципы обеспечения качества обслуживания	60
2.7.	Описание схемы предоставления услуг	63
2.7.1.	Услуги для физических лиц.....	63
2.7.2.	Услуги для юридических лиц	68
2.8.	Организация мер СОРМ.....	77
2.8.1.	Общие принципы организации СОРМ	77
2.8.2.	Настройка оборудования для реализации СОРМ.....	77
2.8.3.	Организация канала для СОРМ.....	78
3.	Миграция существующих сетей филиалов «Стрим-ТВ» на унифицированную топологию.....	79

Взам. инв. №	
Подл. и дата	
Инв. № подл.	

3.1. Этапы миграции	79
3.2. Изменение настроек оборудования на МУ и ДУ	80
3.3. Модернизация и изменение настроек BRAS.....	80
3.4. Модернизация и изменения настроек телематических серверов.....	81
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	82
ЛИСТ ПРИМЕЧАНИЙ	83

Инв. № подл.	Подл. и дата	Взам. инв. №					СИТ.СТВ.ЭТП.2.9/08	Лист
								3
Изм	Лист	№ документа	Подпись	Дата				

1. Общие положения

- 1.1. Полное наименование: Сеть широкополосного доступа «Стрим-ТВ».
- 1.2. Сокращенное наименование: СШПД.
- 1.3. Шифр работы: КМ.СТВ.ЭТП.1.0/08.
- 1.4. Основание для разработки: Заказ № 3/08/КМ к Договору № 151/08/КМ от 26 марта 2008 между ООО «Квазар-Микро. РУ» и ЗАО «СТРИМ-ТВ».
- 1.5. Наименование предприятий Заказчика и Исполнителя:
- Заказчик: ЗАО «СТРИМ-ТВ».
 - Исполнитель: ООО «Квазар-Микро. РУ».
- 1.6. Плановые сроки начала и окончания работы: определяются Договором и Заказом к Договору между Заказчиком и Исполнителем.
- 1.7. Источник финансирования: собственные средства Заказчика.
- 1.8. Порядок финансирования: определяется Договором и Заказом к Договору между Заказчиком и Исполнителем.
- 1.9. Приемка результатов работ по выполнению Эскизно-технического проектирования Сети широкополосного доступа «Стрим-ТВ» организуется Заказчиком с привлечением представителей Исполнителя и осуществляется на предмет определения соответствия требованиям Технического задания на Эскизно-техническое проектирование. Порядок приемки определяется Техническим заданием, Договором и Заказом к договору, заключаемым между Заказчиком и Исполнителем.
- 1.10. Сведения об использованных нормативно-технических документах:
- В процессе эскизно-технического проектирования использовались следующие нормативно-технические и информационные материалы:
- ГОСТ 34.601-90 Автоматизированные системы. Стадии создания.
 - ГОСТ 34.603-92 Виды испытаний автоматизированных систем.
 - ГОСТ 34.201-89 Виды, комплектность и обозначение документов при создании автоматизированных систем.
 - ГОСТ 34.003-90 Автоматизированные системы, термины и определения.
 - РД 50-34.698-90 Методические указания. Автоматизированные системы. Требования к содержанию документов.
 - ITU-T Recommendation M.3010. Generic Network Information Model;
 - RFC 4364. BGP/MPLS IP Virtual Private Networks (VPNs).

Согласовано			

Взам. инв. №	
Подл. и дата	
Инв. № подл.	

					СИТ.СТВ.ЭТП.1.3/08			
Изм	Лист	№ документа	Подпись	Дата				
Разраб.		Михайлов			Сеть широкополосного доступа «Стрим-ТВ» Эскизно-технический проект	Стадия	Лист	Листов
						ЭТП	4	83
Н.контр.		Никифоров				СИТРОНИКС Информационные Технологии		
ГИП		Абаев						
Утвердил								

- RFC 3330. Special-Use IPv4 Addresses.
- RFC 2516. A Method for Transmitting PPP Over Ethernet (PPPoE).
- RFC 2328. OSPF Version 2.
- RFC 4271. A Border Gateway Protocol 4 (BGP-4).
- RFC 2516. A Method for Transmitting PPP Over Ethernet (PPPoE).
- Фирменные материалы компании CISCO Systems: Руководство по разработке сетей передачи данных Операторов (Designing Service Provider Networks);
- Фирменные материалы компании CISCO Systems: Руководство по разработке комплексных сетей (Internetworking Design Guide);
- Фирменные материалы компании CISCO Systems: Руководство по межсетевой операционной системе IOS (Cisco IOS Configuration Fundamentals);
- Стандарт IEEE 802.3. Спецификация параметров и требований технологии передачи "Ethernet" (Local Area Networks): Carrier Sense Multiple Access with Collision Detection (CSMA/CD) – ETHERNET;
- Стандарт IEEE 802.3u. Спецификация параметров и требований технологии передачи «Fast Ethernet» (Local and Metropolitan Area Networks-Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation, Type 100BASE-T);
- Стандарт IEEE 802.3z. Спецификация параметров и требований технологии передачи «Gigabit Ethernet» - Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation, Supplement to Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications;
- Стандарт IEEE 802.1p. Спецификация параметров и требований технологии классификации трафика и динамической широковещательной фильтрации - Standard for Local and Metropolitan Area Networks & Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering;
- Стандарт IEEE 802.1Q. Спецификация параметров и требований коммутируемой передачи виртуальных сетей (Standard for Virtual Bridged Local Area Networks).

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

2. Общее описание технического решения

Целью эскизно-технического проектирования СШПД «СТРИМ-ТВ» является создание документа, описывающего основные положения и принципы построения унифицированной сетевой инфраструктуры, функционирующей на базе централизованной технологии PPPoE, с интегрированным доступом к услугам TriplePlay.

Основными сервисами, предоставляемыми на основе проектируемой сети широкополосного доступа (СШПД) «Стрим-ТВ» являются:

- услуги доступа в Интернет физических и юридических лиц;
- услуги передачи данных для юридических лиц;
- телематические сервисы;
- услуги доступа к мультимедийному portalу Стрим-ТВ (разрабатывается по отдельному техническому заданию);
- услуги голосовой связи;
- услуги IPTV.

При эскизно-техническом проектировании принято во внимание, что СШПД должна обеспечивать:

- надежность;
- устойчивость к отказам оборудования;
- высокую скорость передачи данных абонентов сети;
- простоту локализации и устранения неисправностей в сети;
- удобство создания, удаления и блокировки учетных записей абонентов;
- возможность простого управления разрешенными скоростями доступа для абонентов;
- безопасность, как оборудования сети, так и абонентов;

унификацию моделей и конфигураций активного сетевого оборудования

2.1. Описание топологии и логики функционирования СШПД

2.1.1. Общая схема физической и логической организации сети

На логическом уровне СШПД состоит из нескольких уровней:

- Сервисный уровень (СУ), состоящий из маршрутизаторов, терминирующих абонентские сессии (BRAS), из маршрутизаторов, терминирующих L3 VPN, маршрутизаторов обеспечивающих подключение к другим операторам связи (Border Router, BR) а также из узла телематических служб и дополнительного оборудования. Оборудование сервисного уровня подключается к оборудованию Ядра сети 1GE интерфейсами.

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

6

- Уровень Ядра сети, состоящий из 2-х и более высокопроизводительных маршрутизирующих коммутаторов с 1 GE или 10 GE оптическими интерфейсами. Коммутаторы Ядра сети соединяются между собой соответственно 1 GE или 10 GE интерфейсами. К оборудованию других уровней Коммутаторы ядра подключаются 10GE или 1GE интерфейсами;
- Магистральный уровень (МУ), состоящий из высокопроизводительных коммутаторов с 10GE (или 1GE) оптическими интерфейсами. Коммутаторы МУ подключаются к оборудованию Ядра сети 10GE (или 1GE) интерфейсами и к оборудованию домовых узлов 1GE интерфейсами;
- Уровень домовых узлов (ДУ), состоящий из коммутаторов с 1GE оптическими интерфейсами и медными портами FE для подключения абонентов;

В общем случае физическая схема сети широкополосного доступа «Стрим-ТВ» представляет собой набор пересекающихся полуколец.

Физические каналы образуются волоконно-оптическими линиями связи, которые строятся в регионах по отдельным проектам силами местных строительных организаций.

2.1.2. Описание топологии СШПД

Топология Сети включает в себя 3 уровня: Ядра сети, МУ и ДУ. (Сервисный уровень в данном контексте не учитывается).

Такая топология является общей и используется в большинстве СШПД.

В некоторых случаях может быть еще один уровень - Субмагистральных узлов (СМУ), который топологически подобен уровню МУ.

Магистральные оптоволоконные кольца со скоростями передачи данных 1-10 GE, объединяют расположенные в крупных жилых массивах Магистральные Узлы связи (МУ), и сводятся на оборудовании Ядра сети.

На уровне Магистральных Узлов также производится агрегирование оптоволоконных каналов с пропускной способностью 1 Гбит/с от Домовых Узлов связи (ДУ), организуемых непосредственно в жилых и офисных зданиях.

Скорость передачи данных на линиях домовых узлов – 100 Мбит/с. Подключение абонентов к коммутаторам Домовых Узлов производится медным кабелем «витая пара».

Все устройства, отвечающие за процесс предоставления абонентам различных услуг и сервисов, выделены в отдельный Сервисный Уровень (СУ). На этом уровне расположены BRAS, пограничные маршрутизаторы (BR), серверы телематических услуг, серверы портала Стрим-ТВ.

Подключение к Интернет осуществляется через пограничные маршрутизаторы (BR), располагающиеся на Центральном Узле.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

7

Сервера телематических служб, сервера пользовательского портала и видео сервера располагаются на ЦУ, в специально выделенном для них сегменте.

На уровнях МУ и СМУ для обеспечения надежности используется кольцевая топология.

На Рисунке № 2.1.2-1 приведена общая схема топологии в СШПД «Стрим-ТВ».

Изн.	Лист	№ документа	Подпись	Дата	СИТ.СТВ.ЭТП.2.9/08	Лист
						8

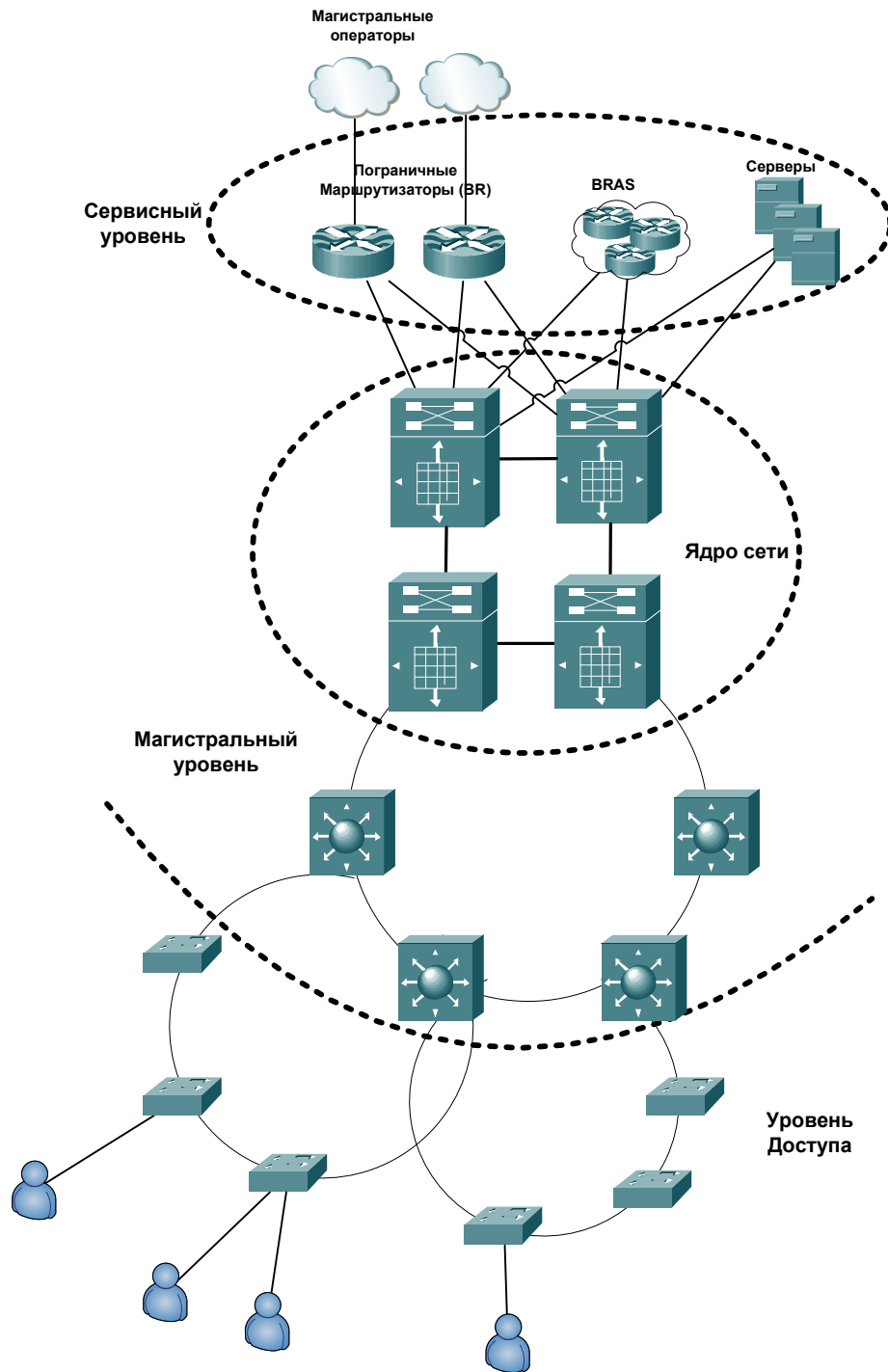


Рисунок 2.1.2.-1. Топология СШПД.

Инв. № подл.	Взам. инв. №			
	Подл. и дата			
Изм	Лист	№ документа	Подпись	Дата

2.1.3. Описание общих принципов оказания услуг TriplePlay

Услуга TriplePlay предполагает получение абонентом услуг широкополосного доступа в Интернет, телефонии (VoIP) и услуг IPTV на одном порту подключения абонента. Дизайн и технические решения по построению СШПД, описанные в настоящем Эскизно-Техническом проекте, предполагают именно такой подход.

Услуга широкополосного доступа в Интернет и к другим ресурсам СШПД предоставляется централизованно на основе технологии PPPoE.

Для получения услуги VoIP и IPTV в СШПД предусмотрена выделенная для этих услуг сеть, которая позволит абоненту подключать VoIP и IPTV терминалы к порту данных. При этом абонент будет иметь возможность одновременно получать все три услуги (или любые комбинации из трех услуг).

2.2. Описание подсистем СШПД.

2.2.1. Подсистема пограничного сегмента

2.2.1.1. Спецификация оборудования пограничного сегмента

В качестве пограничных маршрутизаторов (BR) в СШПД «Стрим-ТВ» используется Cisco 7201-NPE-G2.

Спецификация пограничных маршрутизаторов:

CISCO7201	Cisco 7201 Chassis, 1GB Memory, Dual P/S, 256MB Flash
S72PC-12231SB	Cisco 7200 NPE G2/7201 IOS Series IP PLUS
PWR-7201-AC	Cisco 7201 AC Power Supply option System
CAB-ACE	Power Cord Europe

Физическое подключение к оборудованию провайдера осуществляется через встроенный порт GE.

Если по техническим условиям Оператора связи необходимо использовать интерфейс E1, в спецификацию оборудования необходимо включить соответствующий модуль.

PA-MC-8TE1+	8 port multichannel T1/E1 8PRI port adapter
-------------	---

Как альтернативу Cisco 7201 можно предложить использовать новую линейку сервисных маршрутизаторов Cisco – ASR 100x. К преимуществам можно отнести:

- Модульная масштабируемая платформа – возможность апгрейда без замены шасси

Изн.	№ подл.	Подл. и дата	Взам. инв. №
------	---------	--------------	--------------

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

СИТ.СТВ.ЭТП.2.9/08

Лист

10

- Увеличена производительность – в 3-4 раз выше чем у 7201.

Сравнение характеристик Cisco ASR и Cisco 7201

	ASR1000	C7201
Размеры	2U, 4U,6U	1U
Производительность rps	до 20Mbps	1Mbps
Производительность Gbps	до 20	до 0,8-0,9
Модульность	да	нет
Поддержка 1GE	4 - 120	3
Поддержка 10GE	12	нет
Резервирование общих компонент	Программное, аппаратное	нет
количество абонентов BRAS (номинально)	16000	до 8000
количество абонентов ШПД с учетом QoS, ISG	16000	1000-4000
PPPoE BRAS	да	да
PPTP BRAS	нет	да
L2TP BRAS	да	да
IPoE BRAS	да	да
ISG	да (полная версия к 2009)	да
Netflow	да	да
NAT Gbps	line rate	0,1-0,2
MPLS	да	да
Personal FW	да	нет

Примерная спецификация ASR 100х:

ASR1002	
ASR1000-ESP10	

Изм. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

11

SPA-10XGE-V2	
SASR1R1-AISK9-21SR	
FLASR1-BB-RTU	
2 copy of FLASR1-BB-4K	

2.2.1.2. Подключение к операторам связи

Для обеспечения надежного подключения СШПД к сети Интернет необходимо обеспечить как минимум два подключения к независимым друг от друга (предоставляющим транспорт по физически разным линиям связи) Операторам связи. Каналы от разных Операторов связи должны быть подключены к разным пограничным маршрутизаторам.

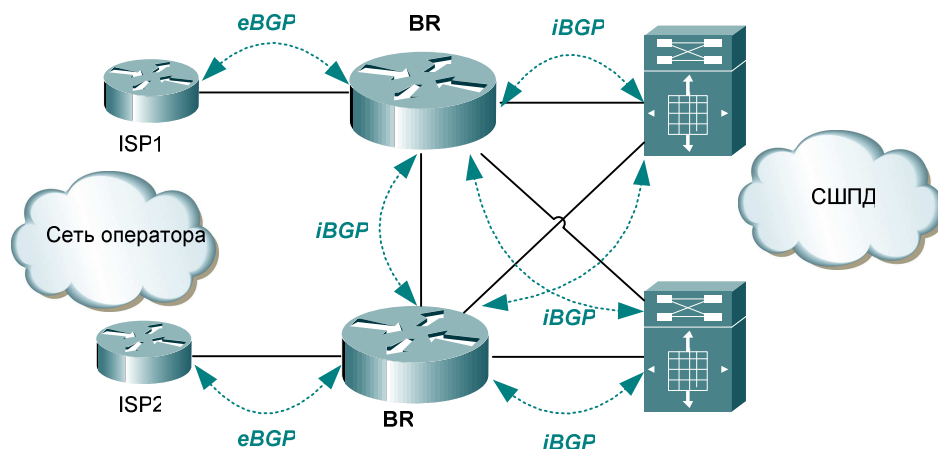
В качестве протокола маршрутизации используется протокол BGP4.

На каждом пограничном маршрутизаторе (BR) настраивается eBGP сессия с соответствующим Оператором связи. Между BR настраивается сессия iBGP. Таким образом, каждый BR несет на себе две полные маршрутные таблицы BGP - по одной от каждого Оператора связи.

Для стабильной работы на каждом пограничном маршрутизаторе необходимо иметь не менее 1GB оперативной памяти.

Каждый BR подключается к 2-м маршрутизаторам ядра. На каждом из них поднимается отдельная iBGP сессия. При этом в ядро может анонсироваться либо маршрут по умолчанию с выбранной метрикой, либо более специфичные префиксы. Необходимо избегать передачи в ядро полных маршрутных таблиц Интернет.

На Рисунке № 2.2.1.2.-1 приведена схема взаимодействия маршрутизаторов пограничного сегмента СШПД.



Изм	Лист	№ документа	Подпись	Дата

Рисунок 2.2.1.2.-1. Взаимодействие со Операторами связи

2.2.2. Сервисная подсистема: уровень BRAS

2.2.2.1. Спецификация оборудования BRAS

В качестве оборудования BRAS в СШПД используются маршрутизаторы Cisco 7201.

Спецификация оборудования BRAS:

CISCO7201	Cisco 7201 Chassis, 1GB Memory, Dual P/S, 256MB Flash
S72PC-12231SB	Cisco 7200 NPE G2/7201 IOS Series IP PLUS
PWR-7201-AC	Cisco 7201 AC Power Supply option System
CAB-ACE	Power Cord Europe
FR-BUS72	Cisco IOS 7200/7300/7400 Series Broadband 8000 User License

Количество BRAS для каждого узла СШПД в регионе рассчитывается исходя из числа абонентов.

При расчетах следует исходить из следующих нагрузок на BRAS:

- Число одновременно работающих абонентов – не более 1500 на один BRAS;
- Пропускная способность – не более 800 Мб/с.

Как альтернативу Cisco 7201 можно предложить использовать новую линейку сервисных маршрутизаторов Cisco – ASR 100x. К их преимуществам можно отнести:

- Модульная масштабируемая платформа – возможность апгрейда без замены шасси
- Увеличена производительность – в 4-5 раз выше чем у 7201 в режиме BRAS

Примерная спецификация ASR 100x:

ASR1002	
ASR1000-ESP10	
SPA-10XGE-V2	
SASR1R1-AISK9-21SR	
FLASR1-BB-RTU	

Име. № подл.	Подл. и дата	Взам. инв. №
--------------	--------------	--------------

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

СИТ.СТВ.ЭТП.2.9/08

Лист

13

2.2.2.2. Описание принципов функционирования BRAS

Основная функция BRAS – терминирование PPPoE (RFC 2516. A Method for Transmitting PPP Over Ethernet) туннелей абонентов СШПД.

BRAS находятся на Сервисном уровне СШПД. Физически каждый BRAS располагается на центральном узле и подключается 2-мя интерфейсами GE к оборудованию Ядра сети.

Каждый интерфейс BRAS сконфигурирован как транковый порт и принимает определенный набор (или все) VLAN с ДУ СШПД, т.е. VLAN, в которых приходит трафик абонентов. Каждый VLAN ДУ на BRAS представляет собой логический sub-interface на физическом интерфейсе.

PPPoE туннели абонентов терминируются на BRAS и представляются в виде виртуального интерфейса. IP адрес, который получает абонент - это сеть с маской /32. Маршруты на эту сеть инсталлируются в таблицу маршрутизации BRAS.

Возможен вариант, когда VLAN ДУ приходят на BRAS в виде Q-in-Q туннелей. В этом случае также используется PPPoE, но настройки услуги слегка отличаются.

Отдельный VLAN на каждом физическом интерфейсе служит для передачи деинкапсулированного трафика в сторону маршрутизаторов ядра

На BRAS конфигурируется пул IP адресов, для выдачи абонентам. Для каждого BRAS выделяется подсеть /21 из сети 172.16.0.0/12. Выделение фиксированного пула для каждого BRAS позволит агрегировать пользовательские префиксы /32, в большие блоки и в таком виде анонсировать их протоколом OSPF.

В случае отказа от NAT и перехода на прямую адресацию абонентов может быть предложен вариант получения IP адресов всеми BRAS с единого DHCP сервера. Таким образом может быть достигнута существенная экономия пространства IP адресов. Обратной стороной является усложнение конфигурации и появления единой точки отказа (кластер DHCP серверов).

Исключением являются пользователи с услугой «Статический IP адрес» – их IP не попадают под общую схему агрегации и анонсируются в виде /32 префиксов.

Для предоставления услуги L3 VPN на BRAS могут быть терминированы VLAN юридических лиц. Для каждого юридического лица строится отдельный VRF.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

Между оборудованием ядра и BRAS может настраиваться протокол MPLS, необходимый для функционирования услуги L3 VPN. Оборудование ядра выступает в роли P-устройства. Префиксы пользователей передаются по протоколу BGP.

2.2.2.3. Настройки отказоустойчивости и балансировки нагрузки BRAS

Балансировка нагрузки, т.е. распределение PPPoE сессий абонентов между BRAS происходит в полуавтоматическом режиме - в зависимости от загрузки различных сегментов сети, администратор СШПД создает несколько групп BRAS. Минимальное число BRAS в группе – два.

Установление PPPoE сессии между абонентским терминалом (АТ) и BRAS происходит после ответа первого доступного сервисного шлюза на широковещательный PPPoE запрос со стороны абонента.

При увеличении загрузки в сегменте, необходимо увеличивать в соответствующей группе число BRAS. Запросы абонентов на установление соединения при этом по-прежнему будет транслироваться на все BRAS, входящие в заданную группу, однако первым будет отвечать наименее загруженный BRAS.

На Рисунке № 2.2.2.4.-1 приведена схема балансировки нагрузки между BRAS.

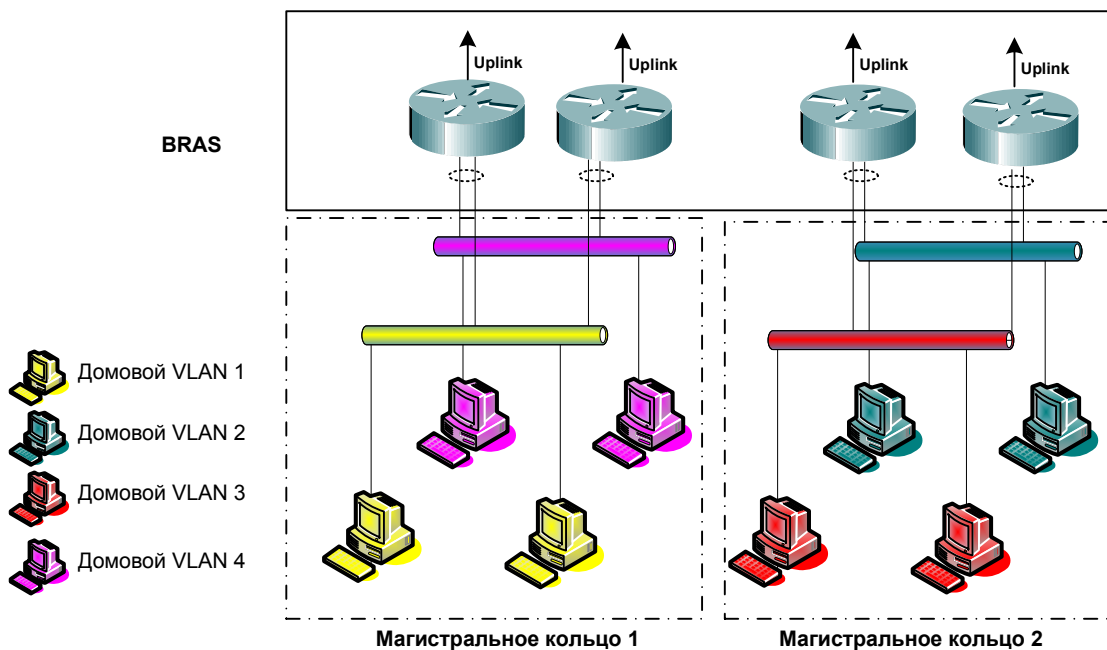


Рисунок 2.2.2.4.-1. Балансировка нагрузки группами BRAS.

Изн. № подл.	Взам. инв. №
	Подл. и дата

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

2.2.2.4. Интеграция с биллинговой системой

В данном контексте, используемая в СШПД система биллинга, выполняет функции сервера AAA. Запросы на аутентификацию/авторизацию генерируются на BRAS в момент подключения пользователей и передаются на сервер биллинга.

В случае успешной аутентификации AAA сервер присылает положительный ответ вместе с набором атрибутов, характеризующих параметры сессии абонента – IP адресом, разрешенной полосой пропускания и др.

Кроме этого, в начале, в конце, а также в течение всей сессии, BRAS передает на сервер биллинга записи, в которых содержится время работы и количество переданных байт за это время. На основании этих данных, формируются CDR (Call Detail Records), которые используются для выставления счетов абонентам.

2.2.2.5. Настройки скорости доступа Абонента к ресурсам.

Для управления скоростями доступа абонентов, RADIUS (биллинговая система) должен передавать на BRAS соответствующие атрибуты абонента. Рекомендуется использование атрибута Cisco *service-policy*.

На BRAS конфигурируются правила, которые описывают сеть абонентов и сеть портала. В профиле абонента в Биллинге создаются соответствующие атрибуты.

После успешной авторизации абонента на созданный виртуальный интерфейс накладываются политики, ограничивающие скорость к описанным объектам сети.

2.2.3. Сервисная подсистема: портал «Стрим-ТВ»

2.2.3.1. Схема подключения и организация доступа к portalу

Серверы портала «Стрим-ТВ» являются частью сервисного сегмента и располагаются на ЦУ. Основной задачей является обеспечения доступа абонентов к мультимедийному контенту.

Для надежной работы серверов предназначены следующие решения:

- Серверы портала вынесены в отдельный сетевой сегмент и доступ к ним ограничен правилами на устройствах, выполняющих функции МЭ.
- Порты серверов могут быть объединены в логические группы. Это позволяет обеспечить необходимую отказоустойчивость и/или распределять трафик между ними.

Поскольку серверы сервисного сегменты не участвуют в работе протоколов динамической маршрутизации из соображений безопасности и надежности, и при этом нуждаются в резервировании подключения к ядру сети, то для этого резервирования

Име. № подл.	Подп. и дата	Взам. ине. №

Изм	Лист	№ документа	Подпись	Дата

используется протокол HSRP, поднятый между соответствующими L3 интерфейсами на оборудовании ядра.

Скорость доступа может регулироваться:

- настройками на портах, к которым подключены серверы портала – например rate-limit, привязанный к сети абонентов или к внешним префиксам;
- настройками на абонентских портах;
- настройками скорости абонентских сессий на BRAS;

Физическое подключение серверов осуществляется через коммутатор сервисного сегмента.

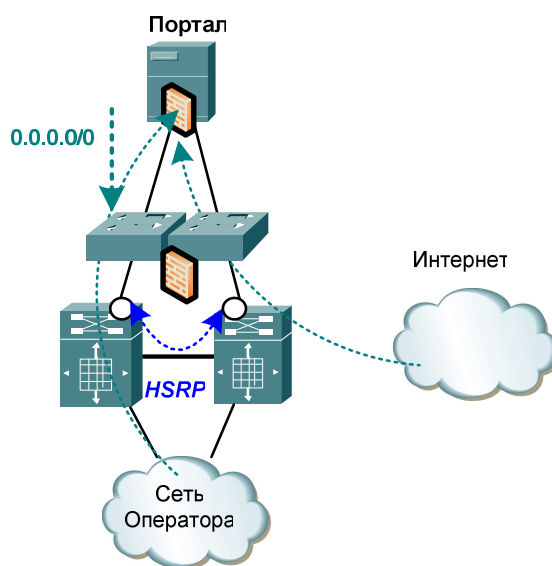


Рисунок 2.2.3.1.-1. Схема подключения портала «Стрим-ТВ».

2.2.4. Ядро сети

Ядро сети - это группа высокопроизводительных маршрутизаторов, основной задачей которых является обеспечение взаимодействия между магистральными кольцами сети «Стрим-ТВ» и сервисным сегментом.

Функции, реализуемые на уровне ядра:

- терминирование 1/10GE-соединений от нижележащих уровней;
- высокоскоростная коммутация PPPoE и multicast Ethernet-фреймов;
- балансировка нагрузки между рядом эквивалентных соединений;
- Высокоскоростная маршрутизация IP пакетов;
- Коммутация MPLS меток;

Име. № подл.	Подп. и дата	Взам. инв. №				СИТ.СТВ.ЭТП.2.9/08	Лист 17
			Изм	Лист	№ документа		

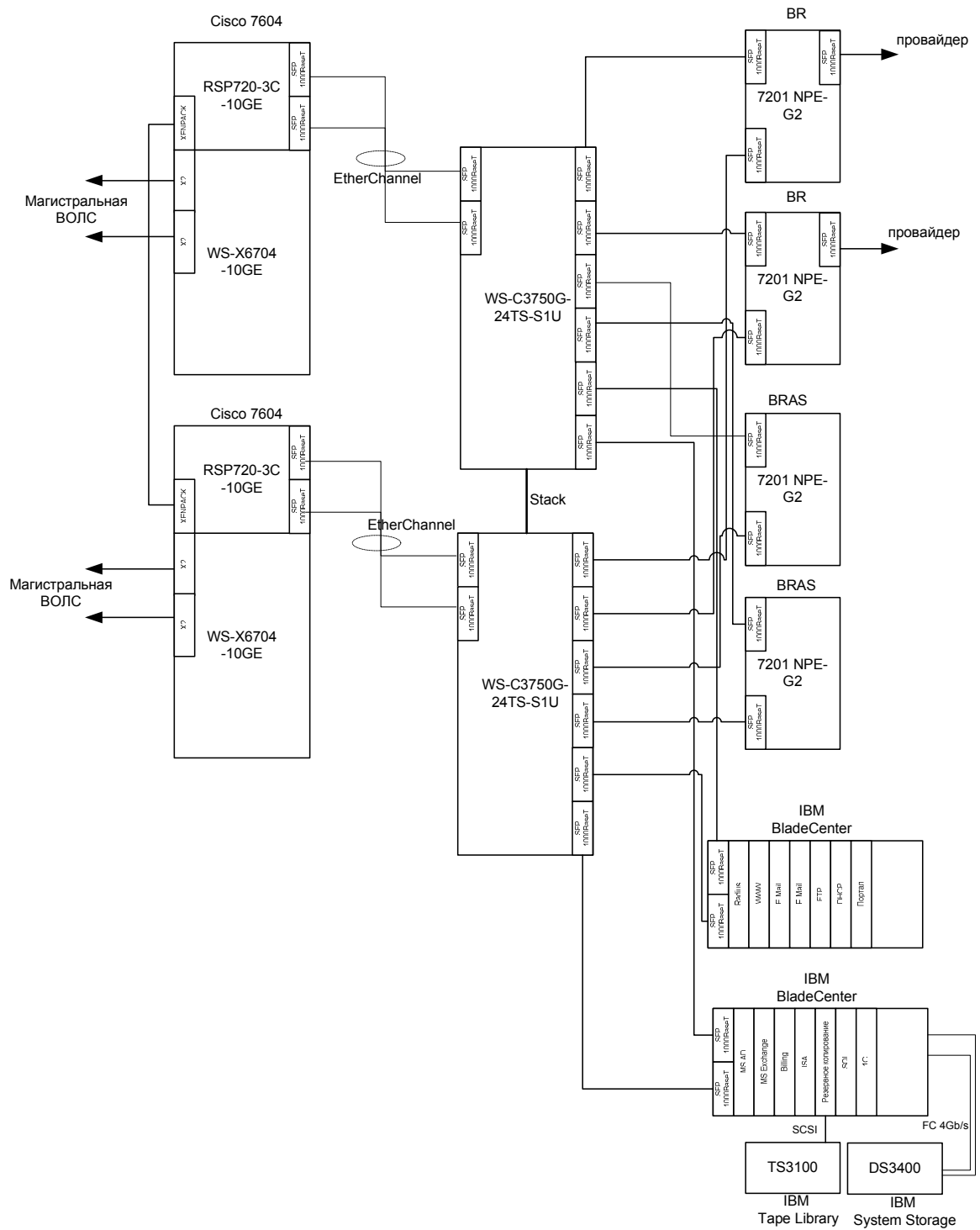


Рисунок 2.2.4-1. Схема организации ядра 10G с двумя маршрутизаторами.

Изн.	Лист	№ документа	Подпись	Дата

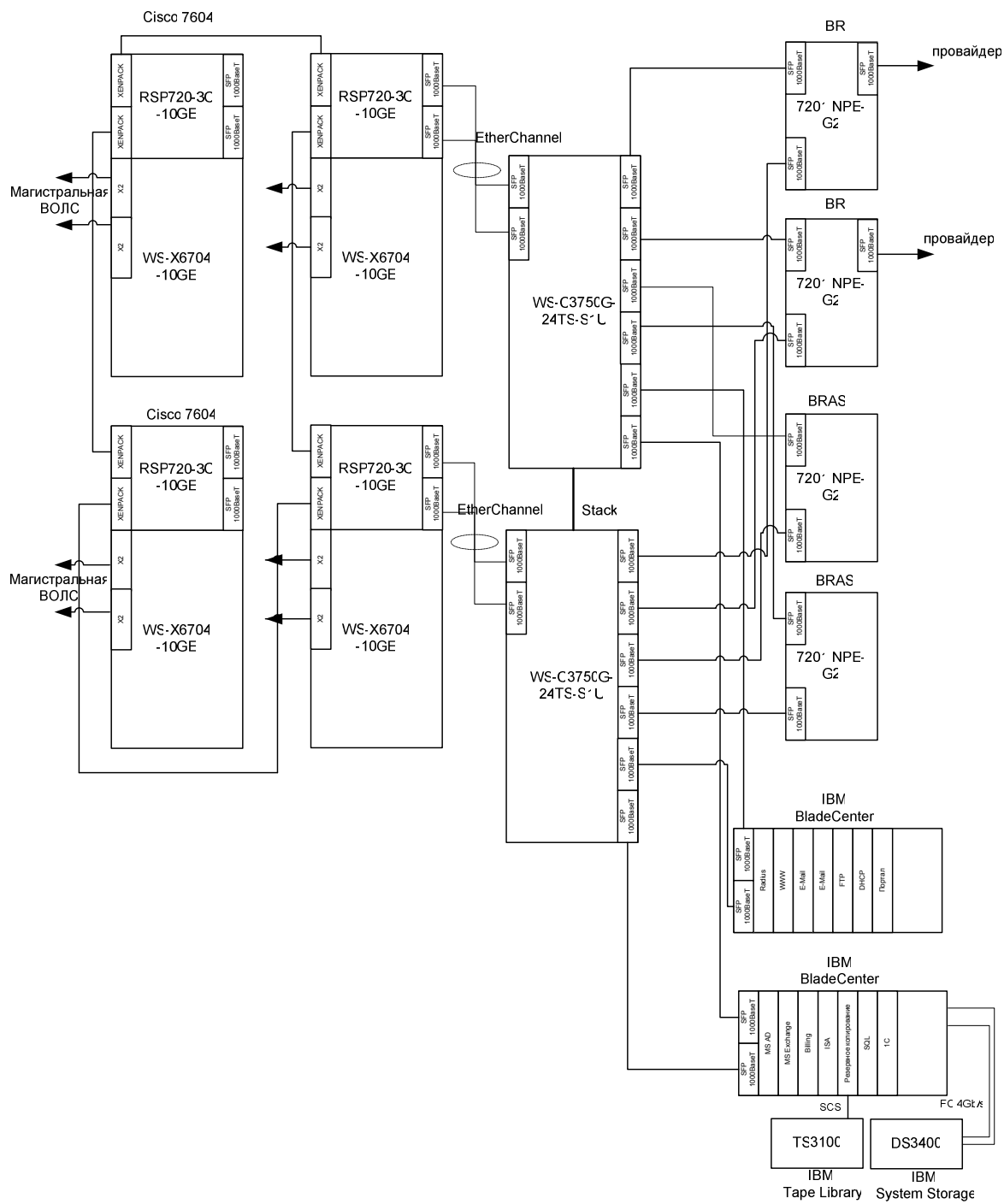


Рисунок 2.2.4-2. Схема организации ядра 10G с четырьмя маршрутизаторами.

Инд. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

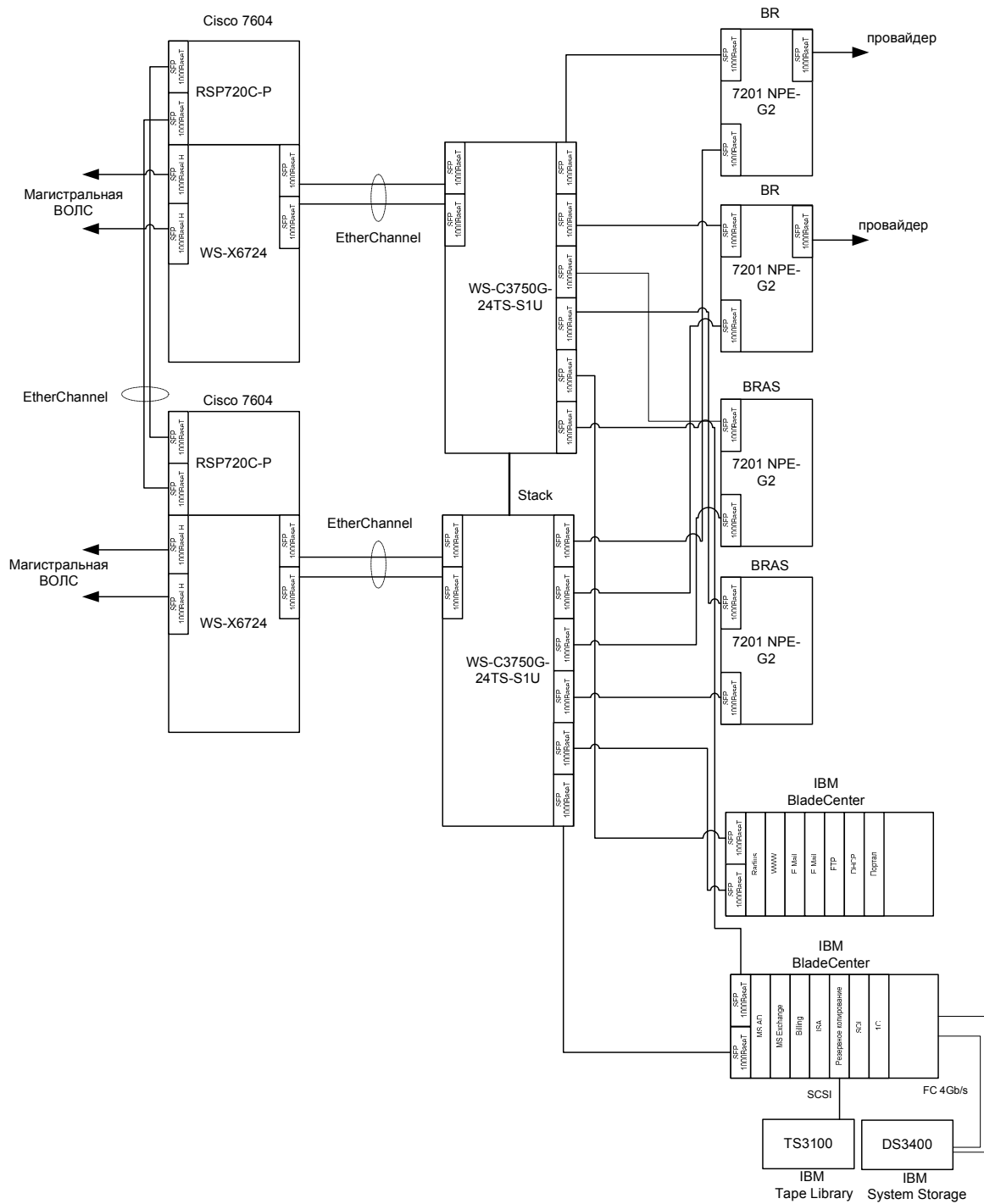


Рисунок 2.2.4-3 Схема организации ядра 1G с двумя маршрутизаторами.

2.2.4.1. Спецификация оборудования ядра сети

Оборудование уровня ядра 10G	
CISCO7604=	Cisco 7604 Chassis Spare

Изм	Лист	№ документа	Подпись	Дата

RSP720-3C-10GE=	Cisco 7600 Route Switch Processor 720Gbps fabric, PFC3C, 10GE
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E
S764AIK9-12233SRC	Cisco 7600-RSP720 IOS ADVANCED IP SERVICES SSH
WS-X6704-10GE	Cat6500 4-port 10 Gigabit Ethernet Module (req. XENPAKs)
XENPAK-10GB-LR+	10GBASE-LR XENPAK Module with DOM support
X2-10GB-LR	10GBASE-LR X2 Module

Оборудование уровня ядра 1G	
7604-RSP720C-P	Cisco 7604 Chassis,4-slot,RSP720-3C,PS
S764AIS-12233SRC	Cisco 7600-RSP720 IOS ADVANCED IP SERVICES
WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)
GLC-LH-SM	GE SFP, LC connector LX/LH transceiver

2.2.4.2. Принципы работы и настройки оборудования ядра сети.

На каждом устройстве в сети “Стрим-ТВ” присутствует набор общих настроек, облегчающих администрирование:

- Имя устройства;
- Домен;
- Описание на интерфейсах;
- Настройки syslog;
- Настройки Authentication, Authorization and Accounting (AAA);
- Настройки синхронизации времени по сети (NTP);
- Настройки SNMP;
- Базовые настройки безопасности – списки доступа, регулирующие обращение к устройству только по определенным протоколам и из определенных сегментов сети.

Маршрутизаторы ядра подключаются транковыми портами к:

- BRAS;

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

22

- Оборудованию МУ;
- Маршрутизаторам BR;
- Телематическим серверам через коммутаторы сервисного сегмента

Для предоставления услуги L3 VPN на сабинтерфейсах маршрутизаторов ядра, к которым подключаются BRAS и BR, настраивается MPLS, при этом соединения между маршрутизаторами конфигурируются как маршрутизируемые интерфейсы (*no switchport*).

VTP на маршрутизаторах Ядра сети работает в transparent режиме так как используются VLAN с номерами больше 1023.

Маршрутизаторы являются транзитными устройствами для домашних VLAN. База данных содержит все VLAN, выделенные под передачу пользовательского трафика.

На нисходящих в сторону магистральных колец интерфейсах разрешаются (*switchport trunk allowed*) только те VLAN, которые используются на этом магистральном кольце.

Поскольку серверы сервисного сегменты не участвуют в работе протоколов динамической маршрутизации из соображений безопасности и надежности, и при этом нуждаются в резервировании подключения к ядру сети, то для этого резервирования используется протокол HSRP – он конфигурируется между L3 интерфейсами, которые представляют VLAN, используемые для подключения серверов.

На каждом интерфейсе в сторону магистральных колец должен быть сконфигурирован управляющий VLAN, уникальный для каждого из колец. На L3 уровне данный VLAN представлен как сабинтерфейс с соответствующим номером. В этом VLAN передается multicast трафик и управляющий трафик. Кроме того, он используется для обмена маршрутной информацией по протоколу OSPF.

Для получения multicast трафика с серверов контента используется соответствующий VLAN, настроенный на интерфейсах, соединяющих ядро с сервисным сегментом. Для корректной работы multicast используются протоколы PIM и IGMP.

Для маршрутизации между ядром, BRAS и МУ и используется протокол OSPF. На оборудовании ядра должна быть сконфигурирована Area 0.

Для функционирования в качестве P-устройства на маршрутизаторах ядра должен быть настроен протокол BGP – для передачи префиксов сетей в L3 VPN.

Для обеспечения COPM должны быть сконфигурированы SPAN порты на каждом из маршрутизаторов, к которым подключены BRAS, BR и маршрутизаторы, терминирующие L3 VPN.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

Поскольку абоненты получают private IP адреса, на маршрутизаторах ядра (или BRAS) должен быть настроен NAT. В интересах СОРМ, для корреляции между реальным IP адресом (после NAT) и private, получаемым при авторизации, на оборудовании ядра сети настраивается NetFlow.

2.2.5. Магистральный уровень (МУ)

Магистральный уровень сформирован из высокопроизводительных коммутаторов Cisco ME 4924, задачей которых является надежная передача пользовательского трафика между ядром и остальными уровнями сети:

- Агрегация 1Gb-соединений от домашних узлов;
- Маршрутизация пользовательского трафика между сегментами сети;
- Маршрутизация multicast трафика;
- Обеспечение отказоустойчивости транспорта.

2.2.5.1. Спецификация оборудования МУ

Оборудование уровня агрегации Cisco 10G (без SFP на 1G)	
ME-BDL-01	Single switch without power supply
PWR-C49-300AC	Catalyst 4948 300-Watt AC Power Supply
S49ESK9-12237SG	Cisco CAT4900 IOS ENTERPRISE SERVICES SSH
X2-10GB-LR	10GBASE-LR X2 Module

Оборудование уровня агрегации Cisco 1G (без SFP)	
ME-BDL-01	Single switch without power supply
S49ESK9-12237SG	Cisco CAT4900 IOS ENTERPRISE SERVICES SSH
PWR-C49-300AC	Catalyst 4948 300-Watt AC Power Supply

2.2.5.2. Принципы работы и настройки оборудования МУ.

На каждом устройстве МУ в сети “Стрим-ТВ” должны быть настроены следующие параметры:

- Имя устройства;

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

- Домен;
- Описание на интерфейсах;
- Настройки syslog;
- Настройки Authentication, Authorization and Accounting (AAA);
- Настройки синхронизации времени по сети (NTP);
- Настройки SNMP;
- Базовые настройки безопасности – списки доступа, регулирующие обращение к устройству только по определенным протоколам и из определенных сегментов сети.

Коммутаторы МУ подключаются к ядру сети 10Gb/s или 1Gb/s соединениями. Топологически, они образуют полукольцо, опирающееся на маршрутизаторы ядра сети. Между собой коммутаторы соединяются 10Gb/s или 1Gb/s интерфейсами.

VTP должен быть настроен в transparent режиме, так как в СШПД используются VLAN с номерами больше 1023. Все порты в МУ являются транковыми.

На каждом магистральном кольце настраиваются:

- VLAN для передачи абонентского трафика от нижележащих сегментов сети. Номера VLAN являются уникальными для всей сети и не пересекаются с другими магистральными кольцами. VLAN для передачи абонентского трафика являются транзитными для МУ и передаются на оборудование ядра сети на L2 уровне.

Исключением является трафик от устройств STB – для корректной работы VOD трафик абонентов маршрутизируется через специально настроенные SVI на МУ. На SVI должны быть настроены ACL разрешающие передачу пакетов на ресурсы IPTV. Передача абонентского трафика через эти SVI должна быть запрещена.

Поскольку ДУ, также строятся по кольцевой топологии, на этих же SVI должен быть настроен протокол HSRP и IP адрес, являющийся default gateway для STB.

- Management VLAN и Multicast VLAN для МУ. Management VLAN и Multicast VLAN настраиваются на всех устройствах МУ данного магистрального кольца. Для маршрутизации Multicast и Management трафика МУ используются специальные SVI, которые настраиваются на всех коммутаторах МУ данного кольца.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

- Management VLAN и Multicast VLAN для ДУ.

Для управления коммутаторами ДУ на каждый коммутатор МУ выделяется VLAN, количество которых равно количеству нисходящих портов.

Для маршрутизации используются специальные SVI с соответствующими номерами. Поскольку ДУ, в свою очередь, образуют кольцо, между SVI на опорных коммутаторах поднят протокол HSRP, чей логический IP является маршрутом по умолчанию для ДУ.

Для передачи multicast на нижележащие коммутаторы на каждый коммутатор МУ выделяется VLAN, количество которых равно количеству нисходящих портов. На L3 данные VLAN представлены в виде SVI с соответствующими номерами.

Номера Management VLAN и Multicast VLAN для ДУ являются уникальными в пределах одного коммутатора МУ. Номера этих VLAN могут быть использованы на других коммутаторах МУ. Номера Management VLAN на МУ и ДУ должны быть одинаковыми

Для маршрутизации используется протокол OSPF, анонсирующий IP адреса всех L3 интерфейсов, сконфигурированных на МУ. Коммутаторы, подключенные к маршрутизаторам ядра выступают как ASBR – на них присутствует как Area 0 с ядра так и Area N с остальных коммутаторов магистрального кольца. ASBR могут агрегировать маршруты от нижележащих сегментов в сторону маршрутизаторов ядра.

Для маршрутизации multicast трафика на оборудовании ядра сети и оборудовании МУ настраивается протокол PIM.

На рисунке 2.2.5.2.-1. представлена логическая схема организации МУ.

Име. № подл.	Подп. и дата	Взам. име. №				СИТ.СТВ.ЭТП.2.9/08	Лист
Изм	Лист	№ документа	Подпись	Дата			

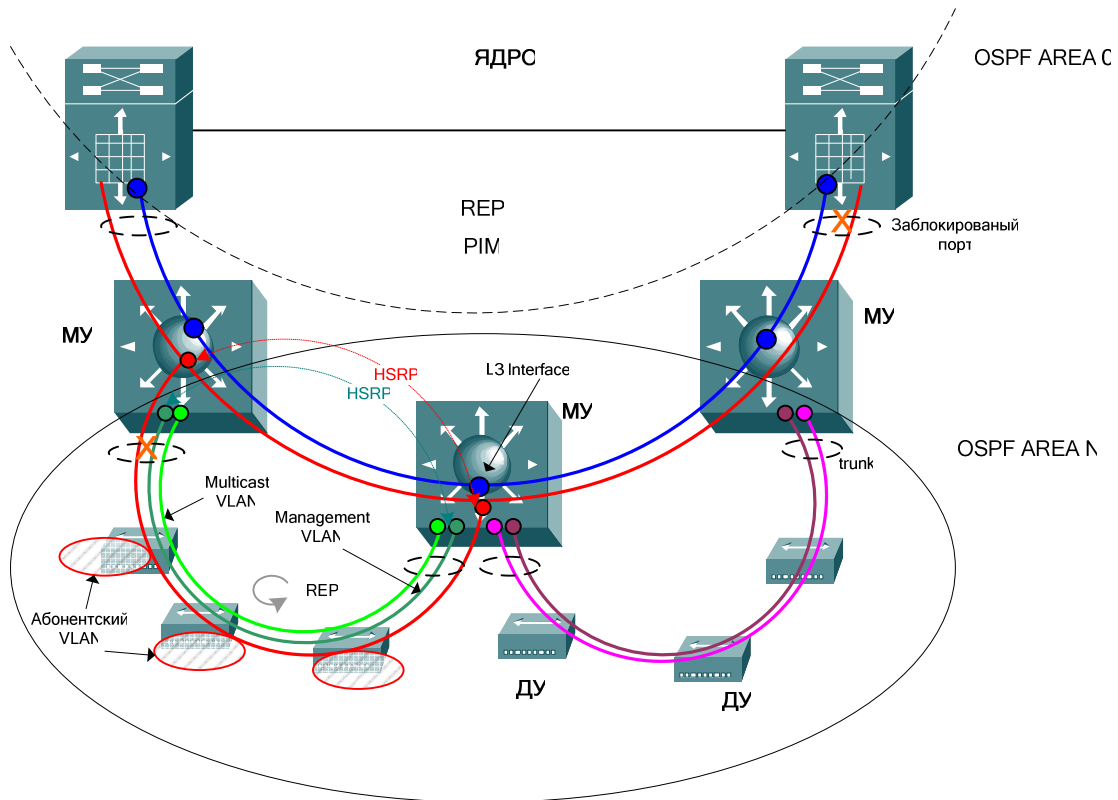


Рисунок 2.2.5.2.-1. Логическая схема магистрального уровня.

В качестве механизма резервирования и отказоустойчивости на L2 уровне используется протокол Cisco REP.

Порты, которыми соединены между собой магистральные коммутаторы представляют собой один REP сегмент – магистральный, порты, смотрящие в сторону нижележащих уровней образуют другие сегменты.

STP на нижележащих уровнях отключен. На каждом сегменте один порт является заблокированным протоколом REP, устраняя, таким образом, возможные петли. При аварии, ранее заблокированный порт переходит в активное состояние, восстанавливая связность в сегменте.

На рисунке 2.2.5.2.-2. представлена логическая схема организации отказоустойчивости.

Име. № подл.	Взам. инв. №
	Подл. и дата

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

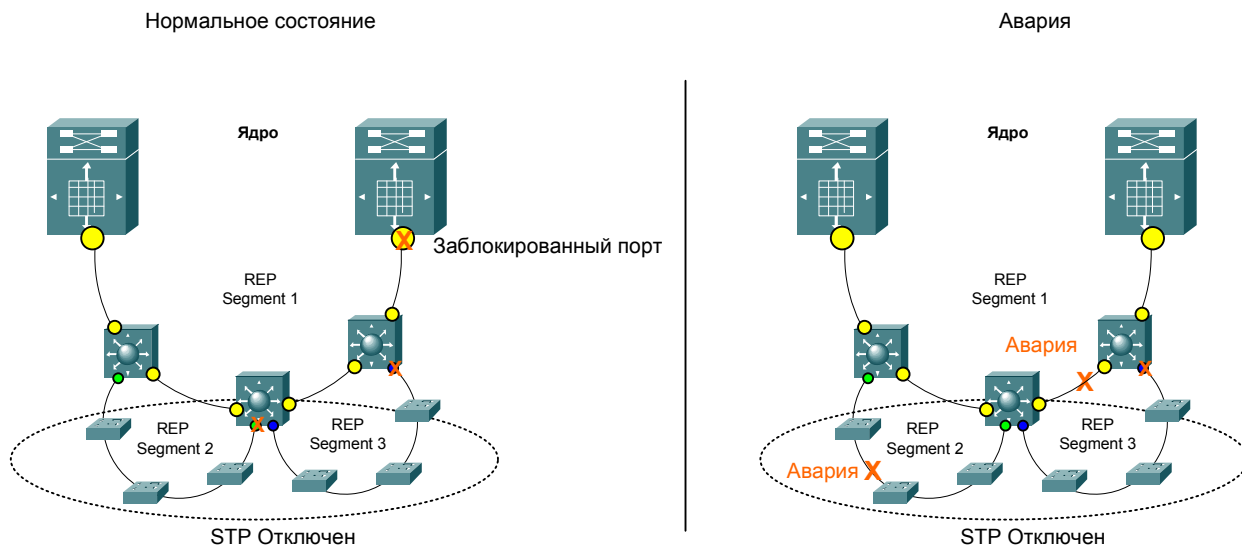


Рисунок 2.2.5.2.-2. Логическая схема организации REP.

2.2.6. Уровень доступа (ДУ)

Уровень доступа уровень в СШПД строится на коммутаторах L2, имеющих два uplink 1 GE и 24 порта для подключения абонентов. На уровне ДУ могут использоваться коммутаторы Linksys или D-Link.

2.2.6.1. Спецификация оборудования ДУ.

SPS224G4-EU	Linksys Switch 24-Port 10/100 24-port 10/100 + 4-Port Gigabit SP Switch
DES-3028	Управляемый коммутатор 2 уровня с 24 портами 10/100 Мбит/с + 2 портами 1000BASE-T + 2 комбо-портами 1000BASE-T/SFP

2.2.6.2. Принципы работы и настройки оборудования ДУ.

По уровню доступа проходит демаркационная линия, проводящая границу между абонентской базой и сетью «Стрим-ТВ». Активные устройства, составляющие аппаратную базу уровня доступа, функционируют на L2 уровне и располагаются на территориях домовладений, находясь при этом под управлением СтримТВ.

Име. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

Основной функцией этих устройств является «доставка» VLANов от ДУ к оборудованию BRAS сервисного уровня на которых реализуются услуги для абонентов.

Другими функциями, реализуемыми на устройствах ДУ являются:

- Доставка широковещательного трафика (multicast);
- Обеспечение полосы пропускания в интересах корпоративных клиентов с использованием механизмов классификации и маркировки трафика, а также политик и очередей (traffic classification, marking, policing, shaping queuing);
- Ограничение максимальной скорости абонентов, для того, чтобы избежать перегрузки ядра сети.

Поскольку оборудование ДУ формирует границу сети «Стрим-ТВ», оно должно выполнять ряд задач направленных на обеспечение безопасности сети:

- Запрет локальной коммутации на пользовательских портах: traffic segmentation (или подобные механизмы);
- списки доступа на оборудовании;
- Контроль широковещательных штормов;
- Списки доступа, пропускающие только авторизованный трафик;
- Запрет всех видов служебного трафика (CDP, STP).

Подключение коммутаторов ДУ осуществляется по кольцевой схеме. Все ДУ в одном кольце доступа принадлежат одному VLAN.

На абонентских портах домовых коммутаторов дифференцирование трафика по типу оказываемого сервиса не производится. На каждый коммутатор уровня доступа выделяется отдельная виртуальная сеть (VLAN), в которой и передается Triple Play трафик (голос, видео, данные) абонентов, подключенных к коммутатору.

На каждом устройстве ДУ должны быть настроены:

- Имя устройства;
- Домен;
- Описание на интерфейсах;
- Настройки syslog;
- Настройки Authentication, Authorization and Accounting (AAA);
- Настройки синхронизации времени по сети (NTP);
- Настройки SNMP;

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

- Базовые настройки безопасности – списки доступа, регулирующие обращение к устройству только по определенным протоколам и из определенных сегментов сети.

При первоначальной настройке на каждом коммутаторе ДУ создается 3 VLAN – VLAN для абонентов, VLAN для управления и multicast VLAN. VLAN для подключения абонентов является native

На UNI портах настраиваются ACL, в которых разрешается только описанные типы трафика:

- PPPoE (ethertype 0x8863, 0x8864);
- IP Multicast;
- DHCP;
- IP unicast с определенных блоков адресов на оборудование IPTV.
- Все остальные типы трафика запрещены.

STP протокол должен быть отключен на всех ДУ.

Обмен трафиком на втором (L2) уровне между абонентами сети «Стрим-ТВ» запрещен. Это связано с необходимостью учитывать и тарифицировать локальный трафик в сети. Такая изоляция достигается за счет использования виртуальных сетей (VLAN), механизма traffic segmentation, поддерживаемого коммутаторами второго уровня D-Link и LinkSys и использования PPPoE туннелей, доставляющих пользовательский трафик к BRAS.

Поскольку коммутаторы ДУ подключены по кольцевой схеме, traffic segmentation не работает между пользователями, подключенными к разным коммутаторам. Чтобы решить эту проблему, на пользовательских портах должны быть настроены списки доступа (ACL), запрещающие такой обмен.

Все виртуальные сети (VLAN), по которым передается абонентский трафик, терминируются на сервисном уровне, на логических sub-интерфейсах BRAS.

Для управления на всех ДУ сконфигурирован Management VLAN. IP адрес для управления должен находиться в этом VLAN. Маршрут по умолчанию должен указывать на HSRP IP адрес на опорных МУ.

На коммутаторах должен быть настроен Multicast VLAN, по которому осуществляется передача многоадресного трафика.

На коммутаторах уровня доступа должна быть включена функция IGMP Snooping.

На рисунке 2.2.6.2.-1 представлена общая логическая схема организации ДУ.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

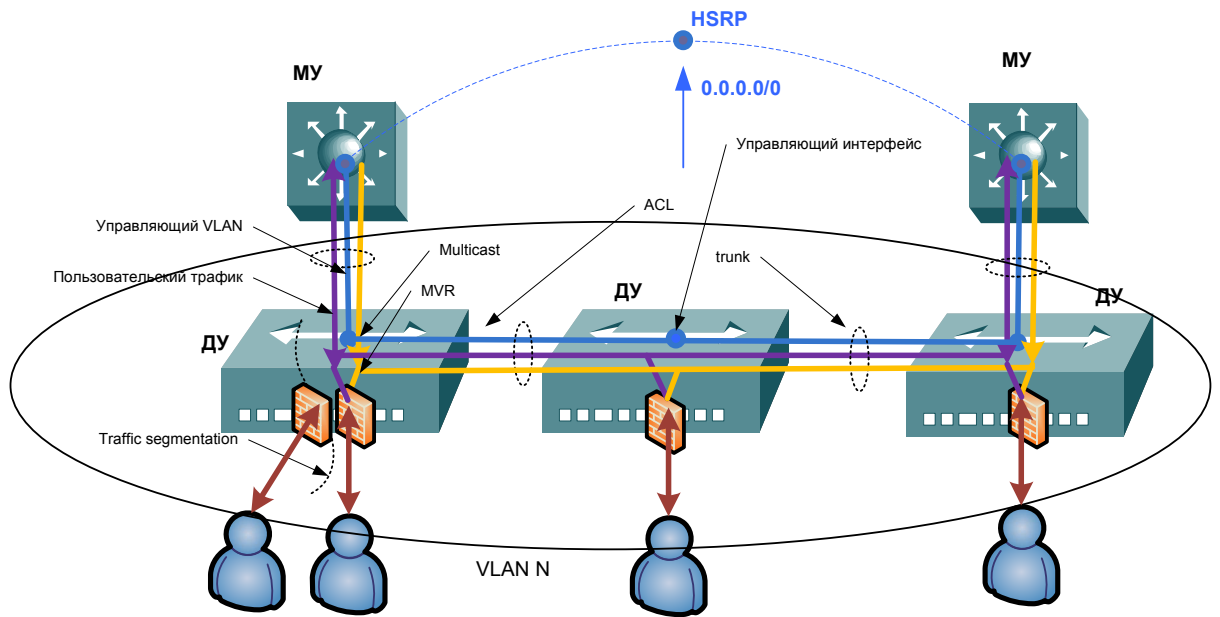


Рисунок 2.2.6.2.-1. Логическая схема уровня доступа.

2.2.7. Узел телематических служб

Узел телематических служб обеспечивает поддержку сервисов, необходимых для реализации услуг доступа в Интернет (например, службы разрешения имен), а также дополнительных служб, таких как электронная почта, web-хостинг, и услуги голосовой связи.

Для наиболее полного использования аппаратных ресурсов при построении узла телематических служб используется программная виртуализация.

Применение виртуализации ресурсов позволяет свести к минимуму простой и время восстановления сервисов в случае аварий, взлома или модернизации оборудования. Гибкость управления такими системами, позволяет в случае загруженности физического сервера перенести настроенную виртуальную машину (сервис) на менее загруженное оборудование, тем самым, оптимизировав использование имеющихся ресурсов.

В качестве платформы виртуализации используется гипервизор XEN, входящий в состав используемой при построении узла телематических служб операционной системы CentOS 5.2. XEN с минимальными потерями производительности обеспечивает создание и поддержку большого количества виртуальных машин на одном физическом сервере.

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

При распределении сервисов по физическим серверам использовалось два основных критерия:

- Сервис, требующий дублирования, распределяется по различным физическим серверам;
- Максимальный объем памяти, доступный гостевым OS, равен объему оперативной памяти, установленной в сервер, минус 512Мб для нулевого домена;

В типовом случае распределение сервисов между физическими серверами и виртуальными машинами («доменам» в терминологии XEN) необходимо производить согласно Таблицам № 2.2.8.-1 – 3.

Таблица 2.2.8.-1. Сервер телематических служб №1 (NS).

(IBM VCHS21 – 2 x Xeon 2.50G / 2G RAM / 2 x 146GB SAS HDD)

Сервис	Виртуальная машина	Выделяемый объем памяти, Гб
Основной сервис разрешения имен (DNS Primary)	Domain 1	1
<i>Основная служба точного времени (NTP Primary)*</i>		

Таблица 2.2.8.-2. Сервер телематических служб №2 (MAIL).

(IBM VCHS21 – 2 x Xeon 2.50G / 10G RAM / 2 x 146GB SAS HDD)

Сервис	Виртуальная машина	Выделяемый объем памяти, Гб
Почтовая система	Domain 1	4
Web-сервисы «Стрим-ТВ»	Domain 2	1
Дополнительный сервис разрешения имен (DNS Secondary)	Domain 3	1
<i>Дополнительная служба точного времени (NTP Secondary)*</i>		
<i>Дополнительный технологический сервис DHCP*</i>	Domain 4	1

* – На серверах телематических служб также выполняются дополнительные технологические сервисы динамического распределения адресного пространства (DHCP), а также основная и дополнительная служба точного времени (NTP) более подробно описанные в Разделе 2.2.9. Технологической Подсистемы.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

СИТ.СТВ.ЭТП.2.9/08

Таблица 2.2.8.-3. Сервер телематических служб №3 (HOSTING).

(IBM BCHS21 – 2 x Xeon 2.50G / 6G RAM / 2 x 146GB SAS HDD)

Сервис	Виртуальная машина	Выделяемый объем памяти, Гб
Сервис клиентского web-хостинга	–	6

2.2.7.1. Сервис разрешения имен (DNS)

2.2.7.1.1. Спецификация аппаратной платформы

Основной сервис разрешения имен (DNS Primary)

- BCHS21 2,50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2.).

Дополнительный сервис разрешения имен (DNS Secondary)

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 8GB (2x4GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2.).

Рекомендуемы параметры для сервисов DNS Primary и DNS Secondary:

- CPU 2,5 Hz;
- RAM 512 Mb;
- HDD 1 Gb.

2.2.7.1.2. Спецификация программного обеспечения

Сервис DNS реализуется на базе OpenSource пакета BIND, развертываемого на двух серверах в виртуальных доменах XEN под управлением CentOS 5.2.

Для оптимального использования ресурсов, сервис разрешения имен (DNS) совмещается с сервисом точного времени (NTP). Совмещаются DNS Primary и NTP Primary, а также DNS Secondary и NTP Secondary и соответственно Secondary DNS и Secondary NTP в рамках двух серверов.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

					СИТ.СТВ.ЭТП.2.9/08	Лист
						33
Изм	Лист	№ документа	Подпись	Дата		

2.2.7.1.3. Резервирование и распределение нагрузки

Для резервирования и распределения нагрузки должна использоваться конфигурация MASTER\SLAVE, которая позволяет автоматически реплицировать изменения зон с Primary на Secondary DNS сервер.

2.2.7.2. Система электронной почты

2.2.7.2.1. Спецификация аппаратной платформы

Аппаратная платформа почтового сервера

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 8GB (2x4GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2.).

Рекомендуемы параметры для работы сервиса электронной почты

- CPU 2,5 Hz;
- RAM 4 Gb;
- HDD 100 Gb.

2.2.7.2.2. Спецификация программного обеспечения

Почтовый сервис реализуется на базе OpenSource пакетов Postfix, Courier-IMAP, MySQL, SASL, SpamAssasin и ClamAV, развертываемых на одном сервере в виртуальном домене XEN под управлением CentOS 5.2.

2.2.7.2.3. Описание компонентов системы и их взаимодействия

В данной реализации Postfix используется в качестве модульного MTA, обеспечивающего поддержку протокола SMTP, расширений SSL\TLS и квотирования объема почтовых ящиков.

Аутентификация SMTP обеспечивается пакетом SASL.

Поддержка протоколов IMAP\POP3 и их SSL\TLS расширений обеспечивается пакетом MDA Courier-IMAP.

Фильтрация на вирусное и спам содержимое выполняется продуктами SpamAssasin и ClamAV.

Учётные записи пользователей, квоты и другая сопутствующая информация должны хранятся в общей базе MySQL, почтовой системы.

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

34

Администрирование почтовой системы может производиться как через web-интерфейс пакета PostfixAdmin, так и через интеграцию с биллинговой системой.

В качестве сервиса web-почты используется пакет RoundCube.

2.2.7.3. Службы web-хостинга

2.2.7.3.1. Спецификация аппаратной платформы

Аппаратная платформа web-служб «Стрим-ТВ»

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 8GB (2x4GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Аппаратная платформа клиентского web-хостинга

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 4GB (2x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS.

Рекомендуемы параметры для функционирования web-служб «Стрим-ТВ»

- CPU 2,5 Hz;
- RAM 1 Gb;
- HDD 10 Gb.

Рекомендуемы параметры для работы площадки клиентского web-хостинга

- CPU 2,5 Hz;
- RAM 6 Gb;
- HDD 100 Gb.

2.2.7.3.2. Спецификация ПО

Сервис web-хостинга реализуется на базе OpenSource продуктов Apache, PHP, MySQL и ProFTP, работающих под управлением CentOS 5.2.. Хостинг сайтов «Стрим-ТВ» организуется в рамках виртуального домена XEN поверх CentOS 5.2. Хостинговая площадка для клиентов «Стрим-ТВ» организована на отдельном физическом сервере с CentOS 5.2..

Изн. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

2.2.7.3.3. Описание принципов организации сервиса web-хостинга

Основным программным пакетом, обеспечивающим работу сервиса web-хостинга, является модульный web-сервер Apache.

Набор пакетов PHP используется для поддержки выполнения сценариев PHP, а сервер баз данных MySQL - для хранения баз данных размещаемых сайтов.

Для поддержки удаленной загрузки и модификации контента используется сервер ProFTP.

2.2.7.3.4. Описание технологии виртуализации ресурсов

В случае необходимости, на площадке клиентского web-хостинга может быть реализована услуга виртуального хостинга (VPS).

VPS реализуется на базе гипервизора XEN, обеспечивающего создание и поддержку большого количества виртуальных машин на одном физическом сервере с минимальными потерями производительности.

Объем устанавливаемой в сервер оперативной памяти прямо пропорционален рассчитываемому количеству обслуживаемых доменов XEN.

2.2.7.4. Службы голосовой связи

2.2.7.4.1. Спецификация программно-аппаратной платформы

Голосовые сервисы реализуются на базе OpenSource PBX Asterisk, поддерживающей все распространённые VoIP протоколы.

Использование Asterisk обеспечивает взаимодействие с клиентским оборудованием (голосовые абонентские терминалы и аналоговые шлюзы).

Открытая архитектура Asterisk, позволяет использовать внешние модули, описывающие логику обработки вызовов.

Взаимодействие со сторонними операторами связи осуществляется через голосовой шлюз Cisco.

Спецификация программно-аппаратной платформы голосовых сервисов:

Программно-аппаратная платформа PBX Asterisk

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- IBM 146GB SAS 10K 2,5" SFF NHS;
- допускается виртуализация XEN с рекомендованными требованиями

Име. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

CPU 2,5 Hz/ RAM 1 Gb/ HDD 10 Gb;

- Asterisk-1.4.19.1.tar.gz;
- Asterisk-addons-1.4.6.tar.gz.

Программно аппаратная платформа голосового шлюза

- [CISCO2811-V/K9] 2811 Voice Bundle,PVDM2-16,SP Serv,64F/256D;
- [VWIC-2MFT-E1] 2-Port RJ-48 Multiflex Trunk - E1;
- [PVDM2-16] 16-Channel Packet Voice/Fax DSP Module.

2.2.7.4.2. Принципы организации голосовой связи

Абонентские терминалы регистрируются по протоколу SIP на PBX Asterisk. SIP аккаунты хранятся в конфигурационном файле Asterisk.

Для снижения нагрузки на сервер Asterisk обрабатывает только сигнальный трафик. RTP-сессии устанавливаются непосредственно между абонентскими терминалами и шлюзами, а проксирование RTP-трафика промежуточными устройствами не требуется.

Местные и междугородные/международные вызовы в телефонную сеть общего пользования осуществляются через устанавливаемый для этой цели голосовой шлюз, имеющий присоединение к федеральному оператору телефонной связи.

2.2.7.4.3. Протоколы и типы абонентских терминалов

В рамках сети филиала «Стрим-ТВ» при организации внутренней голосовой связи используется протокол SIP и один голосовой кодек G711.

В качестве абонентских терминалов SIP могут использоваться IP-телефоны, АТА адаптеры и многопортовые голосовые шлюзы.

2.2.8. Технологическая подсистема СШПД

Технологическая подсистема СШПД обеспечивает поддержку служебных сервисов, необходимых для нормального функционирования сетевой инфраструктуры (например, системы мониторинга), а также дополнительных служб, повышающих надежность и безопасность сетевых и серверных ресурсов.

Аналогично узлу телематических служб, в качестве платформы виртуализации используется гипервизор XEN, входящий в состав используемой при построении узла телематических служб операционной системы CentOS 5.2..

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

В типовом случае распределение технологических сервисов между физическими серверами и виртуальными машинами («доменам» в терминологии XEN) необходимо производить согласно Таблицам № 2.2.9.-1 – 2.

Таблица 2.2.9.-1. Сервер технологических служб №1 (MANAGEMENT).

(IBM VCHS21 – 2 x Xeon 2.50G / 6G RAM / 2 x 146GB SAS HDD)

Сервис	Виртуальная машина	Выделяемый объем памяти, Гб
Система сбора предварительной статистики	Domain 1	2
Система сетевого мониторинга		
Основной технологический сервис DHCP	Domain 2	1
Технологический сервис AAA	Domain 3	0,5
Служба удаленного доступа для администраторов	Domain 4	0,5

Таблица 2.2.9.-2. Сервер технологических служб №2 (BACKUP).

(IBM VCHS21 – 2 x Xeon 2.50G / 2G RAM / 2 x 146GB SAS HDD)

Сервис	Виртуальная машина	Выделяемый объем памяти, Гб
Система резервного копирования	–	2

Дополнительный технологический сервис динамического распределения адресного пространства (DHCP) разворачивается на сервере телематических служб №2 (MAIL) в отдельной виртуальной машине №4 со следующими параметрами: CPU 2,5 Hz/ RAM 1 Gb/ HDD 1 Gb;).

2.2.8.1. Подсистема межсетевого экранирования (МЭ)

В СШПД не используется специально выделенное оборудование для реализации функций межсетевого экранирования. Данный функционал возложен на Cisco IOS. Пакетные фильтры конфигурируются на пограничных маршрутизаторах и на оборудовании ядра, где терминируются соединения к сегменту DMZ.

Изн. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

38

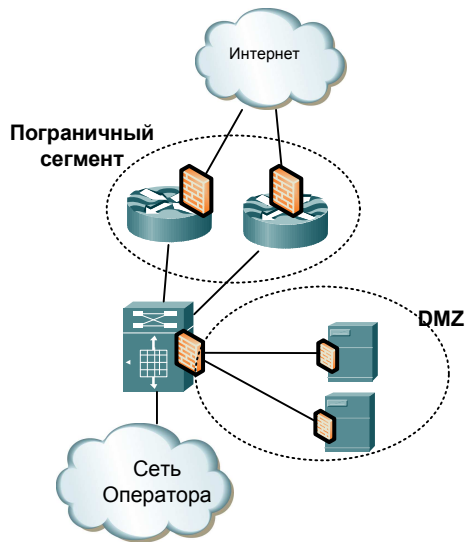


Рисунок 2.2.9.1.- 1. Подсистема межсетевое экранирования.

2.2.8.2. Система динамического распределения адресов (DHCP)

2.2.8.2.1. Спецификация аппаратной платформы сервера DHCP

Аппаратная платформа основного сервера DHCP

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 4GB (2x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Аппаратная платформа дополнительного сервера DHCP

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 8GB (4x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Рекомендуемы параметры для основного и дополнительного сервиса DHCP

- CPU 2,5 Hz;
- RAM 1 Gb;
- HDD 1 Gb.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

2.2.8.2.2. Спецификация программного обеспечения сервиса DHCP

Основной задачей сервиса DHCP является динамическое выделение IP-адресов абонентских терминалам SetTopBox (STB), выполняемое на этапе их начальной настройки.

Реализация сервиса DHCP осуществляется с использованием OpenSource продукта ISC DHCP, развертываемого на двух независимых CentOS 5.2. серверах в виртуальных доменах XEN. Резервирование сервиса DHCP реализуется в соответствии с RFC 2131.

2.2.8.3. Технологический AAA-сервер для доступа к оборудованию

Для удобства управления доступом к активному сетевому оборудованию центрального узла используется сервер RADIUS, позволяющий централизованно хранить учётные записи администраторов, разграничивать их права и производить аккаунтинг сессий. Такой подход к организации доступа к активному сетевому оборудованию повышает безопасность сети, и упрощает управление доступом.

2.2.8.3.1. Спецификация аппаратной платформы сервера AAA

Аппаратная платформа сервера AAA

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 4GB (2x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Рекомендуемы параметры для основного и дополнительного сервиса DHCP

- CPU 2,5 Hz;
- RAM 0,5 Gb;
- HDD 1 Gb.

2.2.8.3.2. Спецификация ПО

Сервис AAA (Authentication, Authorization, Accounting) реализован на базе OpenSource пакета FreeRadius работающего в отдельной виртуальной машине XEN под управлением CentOS 5.2..

2.2.8.3.3. Требования к активному сетевому оборудованию

Для реализации функционала AAA при доступе администраторов «Стрим-ТВ» к активному сетевому оборудованию маршрутизаторы и коммутаторы ядра и сервисного

Име. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

уровня, а также коммутаторы магистрального и субмагистрального уровней должны поддерживать авторизацию по протоколу RADIUS.

2.2.8.4. Служба точного времени (NTP)

2.2.8.4.1. Спецификация программно-аппаратной платформы NTP сервера

Сервис NTP реализуется на базе одноимённого OpenSource пакета NTP, запущенного на серверах узла телематических служб №1 и №2 в рамках независимых друг от друга виртуальных машинах XEN. Совместно с сервисом NTP в этих виртуальных машинах в отдельном chroot-окружении запущены основной и дополнительный сервисы разрешения имен (DNS).

Аппаратная конфигурация сервера телематических служб №1:

- BCHS21 2,50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Аппаратная конфигурация сервера телематических служб №2:

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 8GB (2x4GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Рекомендуемы параметры для основного и дополнительного сервисов NTP:

- CPU 2,5 Hz;
- RAM 512 Mb;
- HDD 1 Gb.

2.2.8.4.2. Синхронизация сетевых служб и сервисов (NTP-сервис)

Серверы NTP синхронизируют локальные часы операционной системы сервера и NTP-клиентов, опираясь на информацию, о времени получаемую от нескольких (не менее 3-х) публичных серверов первого или второго уровня, использующих GPS и эталоны времени на базе атомных часов.

Резервирование обеспечивается двумя серверами NTP.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

2.2.8.5. Система резервного копирования (СРК)

2.2.8.5.1. Спецификация аппаратной платформы СРК

Аппаратная платформа сервера СРК

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- IBM 146GB SAS 10K 2;5" SFF NHS.

2.2.8.5.2. Спецификация ПО СРК

Для резервного копирования настроек сервисов, функционирующих в рамках узла телематических служб, а также уникальных конфигураций активного сетевого оборудования, используются OpenSource продукты ProFTP, SCP(Secure Copy via OpenSSH), XDelta, и набора shell скриптов, функционирующих в среде CentOS 5.2..

Резервное копирование из доверенных сегментов выполняется поверх протокола FTP. Для безопасного копирования из недоверенных участков сети используется протокол SCP.

2.2.8.5.3. Процедура резервного копирования

Резервное копирование сервиса web-хостинга

- генерация и компрессия дампа баз данных сервера MySQL;
- архивирование и компрессия web-директорий;
- архивирование и компрессия конфигурационных файлов сервера Apache;
- генерация дельты архива и MD5 хеша оригинальных web-директорий;
- выгрузка архивов и дельт на сервер резервного копирования по протоколу FTP или SCP.

Резервное копирование сервиса электронной почты

- генерация и компрессия дампа баз данных сервера MySQL;
- архивирование и компрессия mail-директорий почтовой системы;
- архивирование и компрессия конфигурационных файлов Postfix и Courier-IMAP;
- генерация дельты архива и MD5 хеша оригинальных mail-директорий;
- выгрузка архивов и дельт на сервер резервного копирования по протоколу FTP или SCP.

Резервное копирование конфигураций ключевого активного сетевого оборудования

- SNMP запрос на активное оборудование (выполняется сервером СРК);

Име. № подл.	Подп. и дата	Взам. инв. №					СИТ.СТВ.ЭТП.2.9/08	Лист	
									42
			Изм	Лист	№ документа	Подпись			

- выгрузка конфигураций по протоколу FTP (выполняется активным сетевым устройством);
- компрессия файла конфигурации (выполняется сервером СРК).

2.2.8.6. Система сетевого мониторинга

2.2.8.6.1. Спецификация аппаратной платформы

Аппаратная конфигурация системы сетевого мониторинга:

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 4GB (2x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Рекомендуемы параметры для работы системы сетевого мониторинга:

- CPU 2,5 Hz;
- RAM 1 Gb;
- HDD 20 Gb.

2.2.8.6.2. Спецификация программного обеспечения

В основе системы мониторинга сетевой инфраструктуры используется OpenSource продукт Nagios с набором плагинов, работающий на виртуальной машине XEN совместно с системой сбора предварительной статистики. Функционирование виртуальной машины XEN обеспечивается встроенными средствами CentOS 5.2..

2.2.8.6.3. Описание технологий и протоколов, используемых для сетевого мониторинга

Система мониторинга Nagios, используя подключенные к ней модули (плагины), опрашивает устройства по протоколам SNMP и ICMP.

Телематические службы (почтовый сервер, сервисы web-хостинга, DNS-сервер и т.п.), опрашиваются с использованием соответствующих модулей (SMTP, POP3, HTTP, DNS и т.д.).

По результатам опроса Nagios строит таблицы состояний и графики доступности сервисов, а при возникновении инцидентов генерирует соответствующие сообщения администраторам.

Для визуализации карты сети используется Nagios-плагин Weathermap.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

2.2.8.7. Система сбора предварительной статистики

2.2.8.7.1. Спецификация аппаратной платформы

Аппаратная конфигурация системы сбора предварительной статистики:

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 4GB (2x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Рекомендуемые параметры для работы системы сбора предварительной статистики:

- CPU 2,5 Hz;
- RAM 1 Gb;
- HDD 80 Gb.

2.2.8.7.2. Спецификация программного обеспечения

Система сбора предварительной статистики представляет собой OpenSource решение на основе программных продуктов Cacti, RRDTool и Ntop, работающих на виртуальной машине XEN совместно с системой сетевого мониторинга. Функционирование виртуальной машины XEN обеспечивается встроенными средствами CentOS 5.2..

2.2.8.7.3. Принципы организации сбора и учета статистики

Cacti предоставляет собой web-интерфейс к утилите RRDTool, предназначенной для работы с Round Robin Database, используемыми для хранения информации об изменении одной или нескольких величин во времени.

Интерфейс отображения статистики, собранной с сетевых устройств, представляется в виде иерархического дерева.

Хранилище создается на основе шаблона данных (Data Template), задающего соответствие входных величин (полученных из SNMP и Netflow/SFlow-источников) полям в базе данных, а также устанавливает дополнительные параметры, используемые при хранении этих величин.

2.2.8.7.4. Перечень систем, с которых должен осуществляться сбор предварительной статистики

Сбор статистических данных об общем состоянии системы (загрузка CPU, памяти, рабочая температура и т.п.) необходимо выполнять со всего активного сетевого

Изм	Лист	№ документа	Подпись	Дата

Изм. инв. №

Подл. и дата

Изм. № подл.

оборудования ядра, магистрального, субмагистрального и сервисного уровней, а также со всех серверов узла телематических служб и технологической подсистемы.

Информацию о загрузке сетевых интерфейсов необходимо собирать магистральных коммутаторов (все интерфейсы), коммутаторов ядра (все интерфейсы), пограничных маршрутизаторов (uplinks), а также с серверов узла телематических служб и технологической подсистемы.

Статистическая информация о профилях трафика («срезах трафика»), проходящего по сети, снимается по протоколу Netflow v5 на коммутаторах ядра с SVI, через которые маршрутизаторы BRAS передают деинкапсулированный трафик PPPoE-абонентов.

2.2.8.7.5. Хранение и отображение собранных результатов

Хранение данных предварительной статистики, полученных по протоколам SNMP и Netflow система Cacti сохраняет в поддерживаемых RRDTOol базах RRD.

Время хранения собранных данных по умолчанию задается равным двум месяцам и в зависимости от интенсивности внутрисетевого трафика может быть изменено администратором в большую или меньшую сторону.

2.2.8.8. Служба удаленного доступа для администраторов

2.2.8.8.1. Спецификация аппаратной платформы службы удаленного доступа администраторов

Аппаратная платформа службы удаленного доступа администраторов:

- BCHS21 2;50G 12MB 2G 0HDD;
- QC Intel Xeon Procesor E5420;
- 4GB (2x2GB) PC2-5300;
- IBM 146GB SAS 10K 2;5" SFF NHS;
- виртуальный домен XEN (CentOS 5.2).

Рекомендуемы параметры для работы службы удаленного доступа:

- CPU 2,5 Hz;
- RAM 512 Mb;
- HDD 1 Gb.

2.2.8.8.2. Спецификация программного обеспечения

Для реализации удалённого доступа к оборудованию из недоверенных сетей, часто используемого администраторами, применяются Microsoft MPPE\MPPC-совместимые

Име. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

VPN-тоннели, терминируемые OpenSource решениями PopTop и PPPd. Данные программные продукты запускаются в рамках отдельной виртуальной машины XEN, работающей под управлением CentOS 5.2..

2.2.8.8.3. Описание принципов организации удаленного управления оборудованием

Для доступа к управлению оборудованием из недоверенных сетей, администраторы «Стрим-ТВ» устанавливают Microsoft MPPE\MPPC совместимое VPN соединение с сервером удалённого доступа и после аутентификации попадают в доверенный сегмент, из которого разрешено администрирование серверного, и активного сетевого оборудования. Для контроля подключений VPN-сервером производится аккаунтинг сессий.

2.3. Общие настройки оборудования СШПД.

Ниже приводятся общие настройки для оборудования СШПД. Синтаксис команд приведен для оборудования Cisco Systems. У оборудования LinkSys синтаксис команд схожий. При расхождениях в синтаксисе необходимо обратиться к User Guide LinkSys.

Настройки временной зоны:

```
clock timezone MSK 3
clock summer-time MSD recurring last Sun Mar 2:00 last Sun Oct 3:00
```

Включение механизма Path MTU Discovery (PMTUD):

```
ip tcp path-mtu-discovery
```

Эта команда включает механизм Path MTU Discovery (PMTUD) для локальных tcp соединений. Сервис PMTUD влияет только на трафик, который либо создан самим устройством, либо предназначен для этого устройства.

Обычной практикой в больших сетях является использование стартовых баннеров.

Пример стартового баннера:

```
banner login *
Authorized access only. This system is the property of STREAM-TV
Disconnect IMMEDIATELY if you are not an authorized user!
Users (authorized or unauthorized) have no explicit or implicit expectation of
privacy. Any or all uses of this system may be subject to one or more of the
following actions: interception, monitoring, recording, auditing, inspection and
```

Име. № подл.	Подл. и дата	Взам. инв. №
Изм	Лист	№ документа
		Подпись
		Дата

disclosing to security personnel. Disconnect IMMEDIATELY if you do not agree to this conditions.

Contact +7(495) xxx-xxx , noc@stream-tv.ru for help

banner motd *

-==Hostname \$(hostname).\$(domain)==-

Команда no transport preferred:

line vty 0 15

no transport preferred

Эта команда позволяет избежать ожидания при введении команды с синтаксической ошибкой (работает только на оборудовании Cisco).

Каждое устройство конфигурируется для отправки служебных/системных сообщений на сервер Syslog.

Настройка Syslog:

logging 10.0.3.10 severity critical

Рекомендуется установить значение таймаута для административных соединений в диапазоне 20-30 минут. Для удобства работы так же рекомендуется использовать команду logging synchronous:

Настройки timeout для административных соединений:

line con 0

exec-timeout 30 0

logging synchronous

line aux 0

no exec

line vty 0 15

exec-timeout 30 0

logging synchronous

Ине. № подл.	Подл. и дата	Взам. ине. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

47

Настройки TCP keepalive:

```
service tcp-keepalives-in
service tcp-keepalives-out
```

Установка параметра TCP keepalive для входящих/исходящих соединений будет гарантировать, что любое соединение, удерживаемое удаленным/локальным устройством вследствие «зависания» устройства, не будет блокировать доступные VTY порты для администрирования устройства.

Комментарии к интерфейсам должны в обязательном порядке присутствовать на всех устройствах и их формат должен быть стандартизован.

Пример комментария к интерфейсу:

```
Interface GigabitEthernet 0/1
Description ----- STTK
```

Из соображений безопасности доступ к устройствам должен осуществляться только из доверенных сегментов сети.

Настройки VTY access-list:

```
access-list 1 permit 10.0.3.0 0.0.0.255
line vty 0 15
access-class 1 in
```

Для корректной работы оборудования Cisco с SFP сторонних производителей необходимо использовать этот сервис «unsupported-transceiver».

Пример настройки оборудования Cisco для использования неоригинальных SFP:

```
no errdisable detect cause gbic-invalid
service unsupported-transceiver
errdisable recovery cause gbic-invalid
```

2.3.1. Правила именования объектов в СШПД.

Все устройства в СШПД «Стрим-ТВ» именуются в соответствии со следующей схемой:

- оборудование ДУ: I3-<номер устройства вышестоящего МУ>-<тип устройства><номер устройства>. домен;

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

- оборудование СМУ: 12-<номер устройства вышестоящего МУ>-<тип устройства><номер устройства>. домен;
- Оборудование МУ: 11-<тип устройства><номер устройства>.домен;
- Оборудование Ядра Сети: 10-<тип устройства><номер устройства>.домен;
- оборудование сервисного уровня: <тип устройства><номер устройства>.домен,

где

- тип устройства – коммутатор (sw) или маршрутизатор (r)
- номер устройства – порядковый номер устройства, состоящий из нескольких цифр и отсчитываемый от «01»;
- имя домена состоит из идентификатора города и суффикса «stream-tv.ru».

Далее приведен список имен доменов для именования активного сетевого оборудования в филиалах «Стрим-ТВ»:

Город	Имя домена
Ижевск	izhevsk.stream-tv.ru
Краснодар	ksnd.stream-tv.ru
Астрахань	astr.stream-tv.ru
Вологда	vologda.stream-tv.ru
Воронеж	vrn.stream-tv.ru
Иваново	ivanovo.stream-tv.ru
Калуга	kaluga.stream-tv.ru
Кемерово	kemerovo.stream-tv.ru
Курск	kursk.stream-tv.ru
Москва	msk.stream-tv.ru
Нижний Новгород	nnov.stream-tv.ru
Новгород	nov.stream-tv.ru
Омск	omsk.stream-tv.ru
Орел	oryol.stream-tv.ru
Пермь	perm.stream-tv.ru
Ростов	rnd.stream-tv.ru
Саратов	saratov.stream-tv.ru
Екатеринбург	ekt.stream-tv.ru
Смоленск	smolensk.stream-tv.ru
Тамбов	tambov.stream-tv.ru

Име. № подл.	Подп. и дата	Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

СИТ.СТВ.ЭТП.2.9/08

Лист

49

Тверь	tver.stream-tv.ru
Ульяновск	uln.stream-tv.ru
Норильск	norilsk.stream-tv.ru
Н.Тагил	tagil.stream-tv.ru
Дзержинск	dzg.stream-tv.ru
Северодвинск	svd.stream-tv.ru
Таганрог	taganrog.stream-tv.ru

Пример:

10-sw0.ivanovo.stream-tv.ru – коммутатор ядра, расположенного в г. Иваново.

2.3.2. Принципы распределения VLAN

Пул VLAN являются ограниченным ресурсом, поэтому его распределение требует тщательного планирования.

На каждое кольцо ДУ выделяется свой VLAN для абонентов. Для этого используются VLAN с номерами от 1024 до 3024. Пользователи на всех ДУ подключаются в Native VLAN для данного ДУ (по умолчанию первый). На портах МУ, куда подключается данное кольцо ДУ, VLAN с соответствующим номером тоже настраивается как native. Таким образом упрощается настройка коммутаторов на ДУ.

VLAN с номерами от 4024 до 4096 используются передачи управляющего трафика к коммутаторам ДУ. Диапазон с 3000 до 4000 зарезервирован под будущее расширение сети.

VLAN в первой тысяче используются для подключения корпоративных пользователей и адресации устройств ядра сети. Такой выбор обусловлен тем, что протокол VTP, служащий для распространения базы VLAN среди устройств CISCO, поддерживает VLAN с 1 по 1023.

Несмотря на то, что в настоящее время эта функциональности не используется, она может потребоваться в будущем.

Описание	VLAN
Резервные VLAN	1-4
Серверы телематических служб и портала	5-10

Изм.	Лист	№ документа	Подпись	Дата

VLAN для multicast	4048-4071
Управляющие VLAN на ДУ	4072-4096
VLAN для подключения физических лиц	1024-3024
VLAN для подключения юридических лиц	100-1000
Резервные VLAN	1007-1023, 3025-4047
Зарезервированные VLAN Cisco	1001-1006
Подключение BRAS, BR	11-99

Таблица 2.3.2.-1. Распределение VLAN.

Управляющий VLAN для ДУ выбираются следующим образом: используются VLAN из диапазона 4072 – 4096, каждому порту МУ соответствует свой VLAN, например, 4072 – порт 1, 4073 – порт 2 и т.д. Все нижележащие ДУ, подключенные к этому порту сконфигурированы так, что соответствующий VLAN является управляющим для них. Т.е. вся ветка коммутаторов, подключенных к одному порту МУ, находится в одном L2 пространстве. Интерфейс SVI, соответствующий данному VLAN, настраивается на МУ.

Выбранный диапазон VLAN не является уникальным для всей сети и повторно используется на каждом МУ. По такому же принципу выделяются VLANы для передачи multicast трафика, для этого используется 4048 – 4071. Такой подход позволяет обойтись небольшим количеством VLAN для управления всеми коммутаторами.

2.3.3. Принципы распределения адресов

2.3.3.1. Адресация активных сетевых устройств

Схема распределения IP-адресов в большой сети должна удовлетворять следующим основным требованиям:

- **Масштабируемость.** Возможность выделения достаточного количества адресных подпространств из единого плана IP-адресации.
- **Согласованность.** Адресные подпространства всех уровней не должны пересекаться. Это позволяет упростить логическую топологию всей IP-сети и обеспечить однозначную идентификацию единиц сетевого взаимодействия.
- **Агрегируемость.** Для всей совокупности подсетей должна существовать маска, точно покрывающая указанную совокупность. Это позволяет значительно

Име. № подл.	
Подп. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

упростить схему и объем таблиц маршрутизации, а также схему и количество записей в таблицах контроля доступа межсетевых экранов.

- **Информативность.** Сетевой администратор по виду IP-адреса должен иметь возможность определения класса оборудования, которому он принадлежит (например: активное сетевое оборудование уровня доступа, субмагистральный коммутатор, сервисный шлюз и т.д.).

Для адресации активных сетевых устройств «Стрим-ТВ» используется блок IP-адресов класса А – 10.0.0.0/8, определенный документом IETF RFC 1918 для применения в частных IP-сетях. Второй октет блока 10.0.0.0/8 должен быть зарезервирован под регион.

На каждый регион (город) выделяется четыре сети с маской /16.

Таким образом, для города N это будут 10.n.0.0/16, 10.n+1.0.0/16, 10.n+2.0.0/16, 10.n+3.0.0/16. Агрегированный префикс этих сетей - 10.n.0.0/14.

В Таблице № 2.3.3.1.-1 приведена схема распределения адресного пространства по регионам.

Регион	Адрес
Москва	10.0.0.0/14
Балаково	10.4.0.0/14
В. Новгород	10.8.0.0/14
Воронеж	10.12.0.0/14
Кемерово	10.16.0.0/14
Новокузнецк	10.20.0.0/14
Астрахань	10.24.0.0/14
Вологда	10.28.0.0/14
Дзержинск	10.32.0.0/14
Екатеринбург	10.36.0.0/14
Иваново	10.40.0.0/14
Ижевск	10.44.0.0/14
Калуга	10.48.0.0/14
Краснодар	10.52.0.0/14
Курск	10.56.0.0/14
Н.Новгород	10.60.0.0/14
Н.Тагил	10.64.0.0/14

Име. № подл.	Подп. и дата	Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

СИТ.СТВ.ЭТП.2.9/08

Норильск	10.68.0.0/14
Пермь	10.72.0.0/14
Омск	10.76.0.0/14
Ростов-на-Дону	10.80.0.0/14
Саратов	10.84.0.0/14
Северодвинск	10.88.0.0/14
Смоленск	10.92.0.0/14
Таганрог	10.96.0.0/14
Тамбов	10.100.0.0/14
Тверь	10.104.0.0/14
Ульяновск	10.108.0.0/14
Орел	10.112.0.0/14

Таблица 2.3.3.1.-1. Распределение адресного пространства.

Для специальных абонентских терминалов (STB, IP телефоны и проч.) выделяются адреса из сети 10.n.0.0/15. Общее количество адресов, подпадающих под этот префикс, составляет 131072.

На каждый кольцо домовых коммутаторов выделяется сеть с маской /23. Это дает 510 адреса для устройств абонентов на каждый кольцо ДУ и представляется достаточным для использования с учетом внедрения IPTV и установкой STB.

Маршрутом по умолчанию будет являться первый адрес в каждой сети. Такой подход позволит адресовать клиентов, подключенных к 256 кольцам ДУ.

Сеть 10.n+2.0.0/16 зарезервирована или используется для абонентов, которые по каким-то причинам не укладываются в стандартную схему адресации (Например, для подключения юридических лиц, не нуждающихся в прямых IP адресах).

Сеть 10.n+3.0.0/16 используется для адресации сетевых устройств провайдера.

Сеть 10.n+3.0.0/24 используется для служебных адресов (Loopback и проч.)

Сеть 10.n+3.4.0/22 используется для адресации point-to-point интерфейсов BRAS и BR, при подключении к оборудованию Ядра Сети.

Для серверов телематических служб используются либо реальные IP либо сеть 10.n+3.16.0/22.

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

53

Сеть 10.n+3.64.0/18 выделяется для адресации интерфейсов магистральных коммутаторов. Из этой сети выделяются подсети /24 на каждый магистральный сегмент.

Сеть 10.n+3.100.0/24 выделяется для устройств и компьютеров, которым будет разрешено управлять сетевыми устройствами. Доступ к устройствам будет осуществляться только из этой сети.

Для адресации интерфейсов магистральных коммутаторов, служащих для передачи multicast трафика, используется сеть 10.n+3.128.0/17 - по /26 на коммутатор. Адреса имеют маску /32 и анонсируются по протоколу OSPF

Для динамической адресации PPPoE туннелей на BRAS используются адреса из сети 172.16.0.0/12. Выбор блока, отличного от 10.0.0.0/8, удобен с точки зрения эксплуатации, поскольку позволяет легко визуально отделять адресацию абонентов и сетевых устройств.

Блок адресов 172.16.0.0/12 делится на подсети /21 на каждый BRAS.

Иллюстрация распределения адресного пространства приведена на Рисунке 2.3.3.1.-1.

Рисунок 2.3.3.1.-1. Распределение адресного пространства.

В Таблице № 2.3.3.1.-2 приведены сводные данные, отображающие принципы распределения адресного пространства в СШПД «Стрим-ТВ».

Динамические адреса абонентов (PPPoE)		172.16.0.0/12	/21 на каждый BRAS
Адресация абонентских устройств (IP телефонов, STB) на ДУ		10.n.0.0/15	/23 на каждый кольцо ДУ
Резервные адреса и адреса для юридических лиц.		10.n+2.0.0/16	
Адреса оборудования СШПД	Агрегированный префикс	10.n+3.0.0/16	
	Служебные адреса (Loopback и проч.)	10.n+3.0.0/24	
	Подключения BR и BRAS к Ядру сети	10.n+3.4.0/22	
	Адреса серверов телематических служб.	10.n+3.16.0/22 Либо реальные IP	

Име. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

	Адресация интерфейсов коммутаторов МУ	10.n+3.64.0/18	/24 на каждый магистральный сегмент.
	Адреса для управления сетью	10.n+3.100.0/24	
Адреса для multicast трафика		10.n+3.128.0/17	

Таблица 2.3.3.1.-2. Принципы распределения адресного пространства.

2.4. Маршрутизация в сети «Стрим-ТВ»

2.4.1. Общие принципы организации маршрутизации

Для управления маршрутной информацией внутри сети филиала «Стрим-ТВ» в качестве основного IGP-протокола используется протокол OSPF.

OSPF используется для передачи данных о маршрутах на управляющие интерфейсы активного сетевого оборудования и точки терминирования multicast-VLAN, а также о хост-роутах PPPoE-абонентов и о маршрутах на подсети сервисного уровня.

Для маршрутизации с внешними по отношению к филиалу сетями используется eBGP. При организации отказоустойчивости в пограничном сегменте, а также для выбора оптимального пути к внешним ресурсам используется iBGP.

Для организации услуги IP-VPN (L3-VPN) для корпоративных клиентов (юридических лиц) в ядре сети совместно с технологией MPLS используется протокол BGP .

2.4.2. Маршрутизация с внешними сетями

2.4.2.1. Распределение номеров автономных систем (AS)

На начальном этапе модернизации сетей филиалов «Стрим-ТВ» при маршрутизации с внешними сетями могут использоваться существующие автономные системы, полученные через собственные учетные записи RIPE NCC, или выделенные другими LIR.

В процессе модернизации, для оптимизации административных и финансовых затрат, возможно прекратить членство в RIPE для всех филиалов «Стрим-ТВ», сохранив контракт с RIPE только центральным офисом СтримТВ.

В этом случае IPV4-префиксы, полученные ранее филиалами «Стрим-ТВ» - членами RIPE, должны быть перерегистрированы на LIR головного офиса «Стрим-ТВ». При этом полученные блоки адресов могут использоваться филиалами.

Име. № подл.	Подл. и дата	Взам. ине. №

Изм	Лист	№ документа	Подпись	Дата

Избыточное адресное пространство может быть перераспределено между филиалами «Стрим-ТВ» по мере необходимости.

В дальнейшем, возможно использовать единую автономную систему для всех регионов, зарегистрированную головным офисом «Стрим-ТВ».

2.4.2.2. Правила взаимодействия между автономными системами

В общем случае, взаимодействие между филиалами «Стрим-ТВ» осуществляется через сети Операторов связи. Для этого между пограничным маршрутизатором «Стрим-ТВ» и маршрутизатором Оператора должна быть установлена eBGP-сессия.

При использовании одного и того же номера автономной системы во всех филиалах «Стрим-ТВ» возникает техническая проблема, возникающая при получении одним филиалом eBGP-апдейта из другого филиала.

Проблема возникает из-за того, что протокол eBGP в качестве одного из основных транзитивных атрибутов использует строку AS-PATH, в которую включаются номера всех автономных систем, через которые прошел апдейт. Получив апдейт со своим же номером автономной системы в строке AS-PATH eBGP-маршрутизатор отклоняет такое обновление, а связанность между филиалами «Стрим-ТВ» при этом не устанавливается.

Для разрешения описанной проблемы при настройке пограничных маршрутизаторов «Стрим-ТВ», использующих один и тот же номер автономной системы, при настройке пиринга со сторонним Оператором связи используется команда *neighbor x.x.x.x allowas-in*, позволяющая принимать eBGP-обновления со своим номером AS в строке AS-PATH.

2.4.3. Маршрутизация с внутренними сетями

2.4.3.1. Принципы организации IGP маршрутизации

Основным протоколом маршрутизации в СШПД является OSPF. OSPF должен быть настроен на оборудовании ядра сети, BRAS и магистральных коммутаторах.

Домен OSPF должен быть разбит на зоны (*area*). Area 0 настраивается для магистральных соединений всех сетевых устройств.

Downlinks должны быть настроены как area N, где N соответствует магистральному сегменту. Магистральные коммутаторы, примыкающие к ядру, являются ASBR. Пользовательские префиксы инжектируются в соответствующую зону, и на границе с area 0 агрегируются в префикс с меньшей маской.

Таким образом, специфичная маршрутная информация остается локализованной.

Име. № подл.	Подл. и дата	Взам. инв. №
--------------	--------------	--------------

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

Пользовательские PPPoE туннели, терминирующиеся на BRAS, представляются в виде виртуального интерфейса. IP адреса, выдаваемые пользователям, инсталлируются в таблицу маршрутизации с маской /32. Благодаря тому, что на каждый BRAS выделен соответствующий блок IP адресов, пользовательские префиксы агрегируются в большие блоки и в таком виде анонсируются протоколом OSPF. Исключением являются пользователи с услугой “Статический IP адрес” – их IP не попадают под общую схему агрегации и анонсируются в виде /32 префиксов.

На каждом BR поднят OSPF процесс и каждый BR анонсирует маршрут по умолчанию в ядро сети. Если существуют явные предпочтения в сторону одного из аплинков, то OSPF маршрут 0.0.0.0/0 с этого BR надо анонсировать с меньшей метрикой.

На коммутаторах ДУ не используется динамическая маршрутизация. На оборудовании ДУ должен быть сконфигурирован маршрут по умолчанию, указывающий на соответствующий коммутатор магистрального уровня. Если ДУ образуют кольцо, то в качестве маршрута по умолчанию используется HSRP интерфейс между опорными МУ.

В СШПД должен быть настроен iBGP. Через iBGP BR должны анонсировать маршруты в ядро (как маршрут по умолчанию так и более специфичные префиксы, если возникнет такая потребность). iBGP также используется между BRAS, на которых терминируются L3 VPN абонентов, и оборудованием ядра сети.

Для multicast используются протоколы IGMP и PIM. PIM должен быть настроен на оборудовании ядра сети и на оборудовании МУ.

На Рисунке № 2.4.3.1.-1 приведена общая схема организации маршрутизации IGP.

Име. № подл.	Подл. и дата	Взам. име. №						СИТ.СТВ.ЭТП.2.9/08	Лист
									57
			Изм	Лист	№ документа	Подпись	Дата		

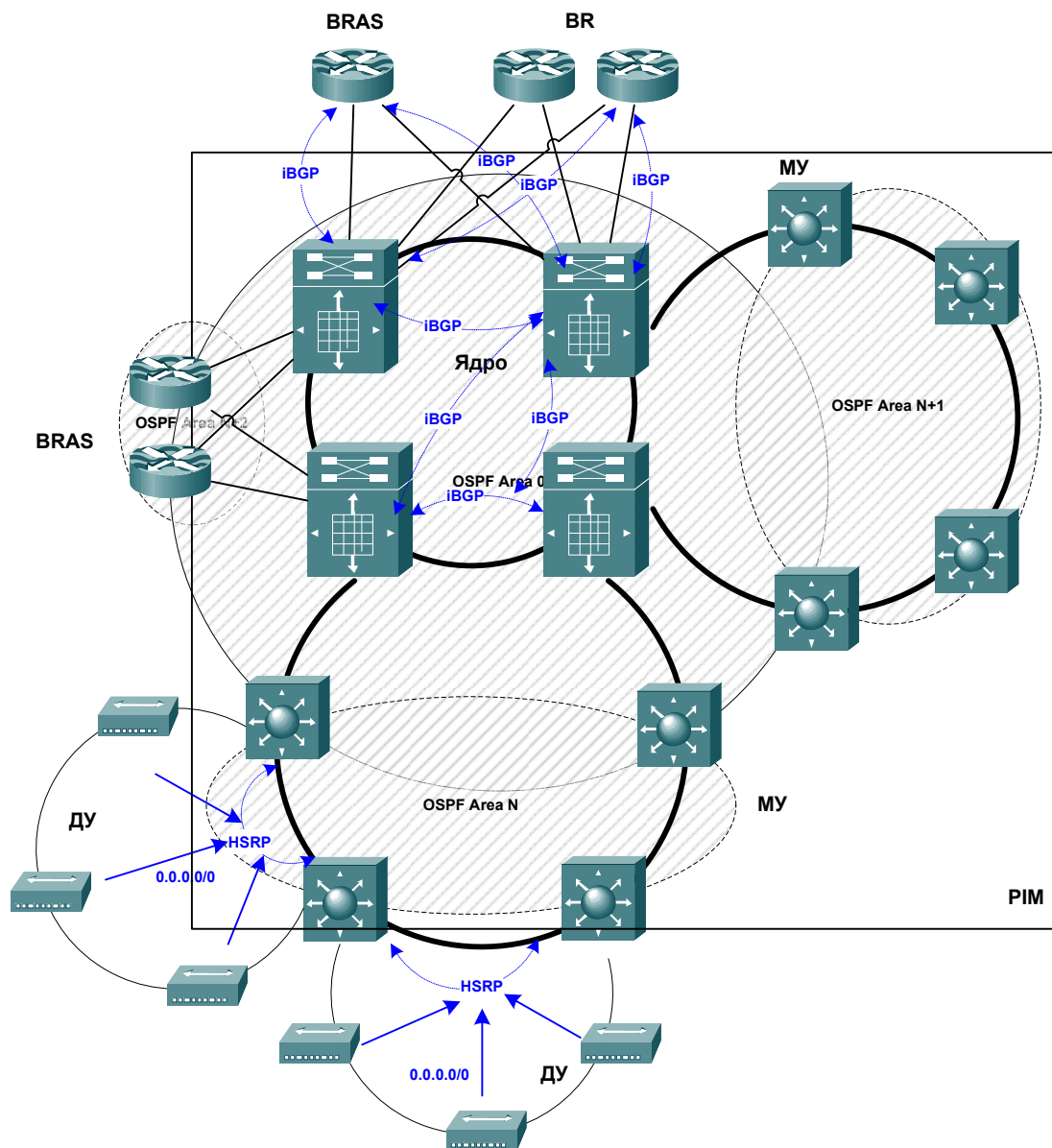


Рисунок 2.4.3.1.-1. Общая схема организации маршрутизации IGP.

2.5. Организация многоадресных рассылок в СШПД

2.5.1. Общие принципы организации многоадресных рассылок

Многоадресная рассылка данных применяется для организации телевидения с использованием сетевой инфраструктуры «Стрим-ТВ».

При осуществлении такой рассылки задействованы механизмы группового управления и многоадресной маршрутизации. Работу механизма группового управления обеспечивает протокол IGMP, участвующий в создании и сопровождении списков рассылки, а многоадресная маршрутизация работает благодаря протоколу PIM, выбирающему маршруты для передачи пакетов.

Изн. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

2.5.2. Логическая схема организации многоадресных рассылок

Для обеспечения многоадресной рассылки на каждый сегмент ДУ выделяется отдельная виртуальная сеть (multicast VLAN), терминируемая на магистральных опорных коммутаторах.

На магистральные коммутаторы и маршрутизаторы ядра сети «Стрим-ТВ» возлагается задача маршрутизации multicast-трафика с помощью PIM от источника многоадресной рассылки (Multicasting-сервера) до входов в multicast VLAN.

На коммутаторах ДУ должна быть настроена функция IGMP Snooping.

Поскольку трафик абонента инкапсулируется в PPPoE, и на абонентском порту нет разделения услуг по VLAN, это может создать проблему получения multicast трафика для устройств STB.

Для решения этой проблемы применяется следующий подход – VLAN ДУ терминируются не только на BRAS но и на магистральных узлах. STB при включении отправляет DHCP запрос на получение IP адреса, коммутатор МУ перенаправляет этот запрос на DHCP сервер. На DHCP сервере производится проверка MAC. DHCP сервер должен отвечать только на запросы с source MAC STB.

При этом, на магистральных коммутаторах сконфигурированы ACL, запрещающие любой трафик кроме multicast и unicast между STB и сервером IPTV.

В случае если абонент получает услугу IPTV непосредственно на компьютере (без использования STB) то существуют два варианта:

- Схема, аналогичная работе STB;
- Получение видео трафика как unicast через BRAS.

Протокол PIM в СШПД должен быть настроен в Sparse-Dense mode.

На Рисунке № 2.5.2.-1 показана схема организации многоадресных рассылок в СШПД.

Име. № подл.	Подл. и дата	Взам. инв. №					
Изм	Лист	№ документа	Подпись	Дата	СИТ.СТВ.ЭТП.2.9/08		Лист
							59

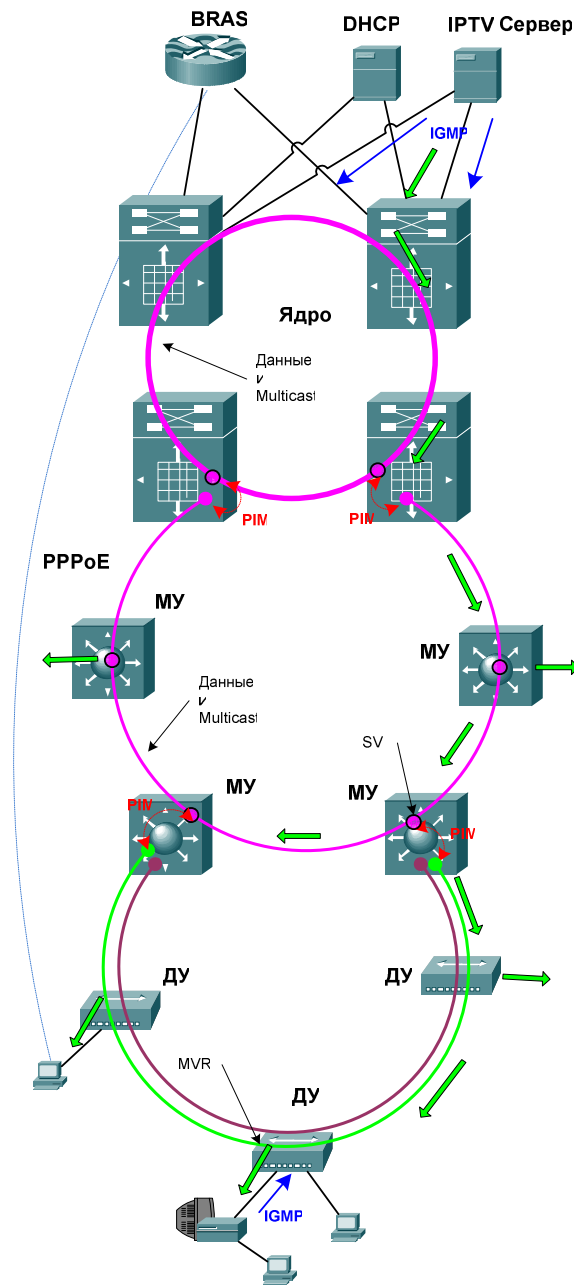


Рисунок 2.5.2.-1. Организация многоадресных рассылок в СШПД «Стрим-ТВ».

2.6. Обеспечение качества обслуживания в сети в СШПД

2.6.1. Общие принципы обеспечения качества обслуживания

Гарантирование качества обслуживания (QoS – Quality of Service) – функциональная способность сети обеспечивать лучшие характеристики при передаче определенного типа трафика по отношению к другому трафику.

Задачей QoS является предоставление определенным типам трафика приоритета при его транспортировке по сети, а также выделение необходимой полосы пропускания для

Име. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

передачи данного вида трафика, что в свою очередь обеспечивает предсказуемую величину задержки и ее вариации (jitter).

Для достижения требуемых характеристик сетевой инфраструктуры предлагается использовать архитектуру Diff-Serv. Одним из основных понятий данной архитектуры является понятие «сервис», описывающее ключевые характеристики передачи пакета в одном направлении. Данные характеристики в зависимости от контекста могут включать в себя абсолютные показатели, такие как задержка, вариация задержки и вероятность доставки, а также относительные показатели, например приоритетность предоставления ресурсов сети.

Архитектура дифференцированного сервиса состоит из:

- подмножества режимов (способов) передачи пакетов (per-hop traffic forwarding behaviors);
- функций классификации пакетов;
- функций, регулирующих потоки трафика.

Архитектура Diff-Serv позволяет строить масштабируемые решения, организовывая классификацию на границе сети для агрегирования (группировки) трафика в классы и использовать различные режимы передачи пакетов для различных классов трафика внутри сети.

Внутри СШПД принадлежность пакета тому или иному классу определяются по значению поля DSCP (DiffServ Code Point). Использование классов (групп) трафика позволяет отказаться от отслеживания потоков приложений или конкретных сессий внутри сети. Режим передачи пакетов определяет необходимое количество ресурсов соединений сети при передаче трафика того или иного класса, а так же внутренние ресурсы сетевых устройств (буферы, очереди и т.п.).

Основные правила реализации дифференцированного сервиса описываются следующим образом:

- единый сервис предоставляется всему классу трафика;
- функция классификации определяет, к какому классу принадлежит пакет и, соответственно, какой режим должны использовать маршрутизаторы при его передаче;
- поле DSCP используется для определения принадлежности конкретного пакета тому или иному классу трафика (оно может быть определено на границе с использованием функции классификации);
- всякий маршрутизатор внутри сети использует один и тот же режим передачи пакетов для класса.

Ине. № подл.	Подл. и дата	Взам. ине. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Архитектура базируется на простой модели, в которой трафик профилируется на границе сети (домена дифференцированного сервиса – далее ДС-домен) в некоторый класс. На входе в ДС-домен проверяется, отвечает ли пакет тому профилю, которому он принадлежит. Если да, то пакету присваивается значение поля DSCP, закрепленное за его классом. Каждый класс идентифицируется уникальным значением поля DSCP.

Внутри ДС-домена каждому значению поля DSCP ставится в соответствие определенный режим передачи пакета. Все пакеты передаются в режиме, соответствующем значению поля DSCP внутри этого пакета. Таким образом, домен ДС это множество сетевых устройств, работающих в соответствии с единой политикой и обладающие единым набором режимов передачи пакета. На границе ДС-домена располагаются сетевые устройства с четко прописанными правилами классификации, снабжающие всякий пакет, входящий в домен ДС, соответствующей «раскраской», отвечающей политике домена ДС. Коммутаторы внутри ДС-домена выбирают подходящий режим пересылки пакета на основе значения поля DSCP.

Для обеспечения качества обслуживания трафика «из конца в конец» необходимо, чтобы все домены использовали согласованные правила профилирования трафика. Профили трафика формируются в соглашении о профилях трафика, которое содержит:

- правила классификации пакета;
- параметры и механизм передачи пакета для каждого класса.

В СШПД можно выделить несколько отдельных классов трафика:

Данные физических лиц	обыкновенный
Данные юридических лиц	обыкновенный
Трафик VOIP - приоритетный	приоритетный
Видео-трафик (multicast и VOD)	приоритетный
Данные с корпоративного портала	обыкновенный

Классы обслуживания и механизмы передачи трафика

Класс трафика	Поле DSCP (dec)	Поле IP precedence	Механизм передачи	Реализация
приоритетный	40	5	приоритетный	LLQ
обыкновенный	8	1	обыкновенный	WFQ (очередь по умолчанию)

На Рисунке № 2.6.1.-1 показаны точки классификации пакетов.

Изн. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

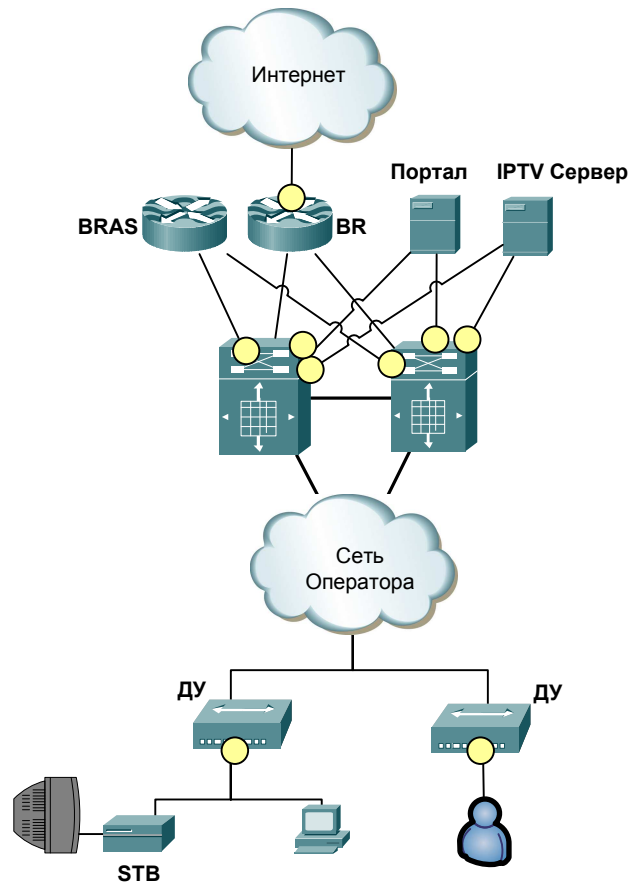


Рисунок 2.6.1.-1. Классификация пакетов в сети «Стрим-ТВ».

2.7. Описание схемы предоставления услуг

2.7.1. Услуги для физических лиц

2.7.1.1. Услуги «подключение к Интернет», «подключение к локальной сети» и «подключение к порталу «Стрим-ТВ».

Все три услуги для абонентов сети выглядит следующим образом.

Абонент, подключается к порту коммутатора ДУ СШПД СтримТВ. Интерфейс подключения – Ethernet.

Для абонента нет необходимости настраивать IP адрес на Ethernet интерфейсе своего компьютера. Строго говоря, настройки Ethernet интерфейса на компьютере абонента могут быть любыми (с IP адресом, с получением IP адреса автоматически), – на получение услуг это не влияет.

Име. № подл.	Подл. и дата	Взам. инв. №					Лист
Изм	Лист	№ документа	Подпись	Дата	СИТ.СТВ.ЭТП.2.9/08		63

Абоненту необходимо настроить только логический интерфейс PPPoE, в терминологии MS Windows – Miniport WAN (PPPoE).

Настройки могут быть выполнены абонентом самостоятельно, используя Мастер новых подключений MS Windows.

Для получения услуг абонент должен «подключить» логическое соединение и ввести свои login и password в соответствующие поля.

Скорость доступа абонента ко всем услугам может быть разной, и определяется тарифом абонента.

Для передачи PPPoE трафика используется абонентский VLAN, общий для всего кольца ДУ. Поскольку сеть СШПД состоит из колец, то для устранения петель один из возможных путей распространения трафика должен быть заблокирован. Для это служит Cisco REP, разрывающий кольцо на ДУ. На магистральном уровне REP не используется, так как замыкание двух VLAN через BRAS не создает петли.

После транспортировки через ядро СШПД пользовательские VLAN должны быть терминированы на BRAS. BRAS должен быть присоединен к ядру сети 2 физическими интерфейсами. Каждый интерфейс BRAS должен быть сконфигурирован как транковый порт и принимать определенный набор (или все) VLAN с ДУ СШПД, т.е. VLAN, в которых приходит трафик абонентов. Каждый VLAN ДУ на BRAS представляет собой логический sub-interface на физическом интерфейсе.

Отдельный VLAN на каждом физическом интерфейсе служит для передачи деинкапсулированного трафика в сторону маршрутизаторов ядра.

На BRAS конфигурируется local pool IP адресов, для выдачи абонентам. Для local pool для каждого BRAS выделяется подсеть /21 из сети 172.16.0.0/12. Выделение фиксированного local pool для каждого BRAS позволит агрегировать пользовательские префиксы /32, в большие блоки и в таком виде анонсировать их протоколом OSPF.

Балансирование, т.е. распределение PPPoE сессий абонентов по разным BRAS происходит в полуавтоматическом режиме.

В зависимости от загрузки различных сегментов сети, администратор СШПД создает несколько групп BRAS. Минимальное число BRAS в группе – два.

Установление PPPoE сессии между абонентским терминалом (АТ) и BRAS происходит после ответа первого доступного сервисного шлюза на широковещательный PPPoE запрос со стороны абонента.

AAA запросы генерируются на BRAS в момент подключения пользователей и отсылаются на сервер биллинга.

Име. № подл.	Подп. и дата	Взам. име. №
--------------	--------------	--------------

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

В случае успешной авторизации AAA сервер присылает положительный ответ вместе с набором атрибутов, характеризующих параметры сессии абонента – IP адресом, разрешенной полосой пропускания и др.

Кроме этого, в начале, в конце а также в течении всей сессии, BRAS преаает на сервер биллинга записи, в которых содержится время работы и количество переданных байт за это время. На основании этих данных, формируются CDR, которые используются для биллинга абонентов.

При успешной авторизации и установлении PPPoE туннеля каждый абонент получает динамический «частный» (private) IP адрес.

В соответствие с требованиями СОРМ, оператор должен иметь возможность предоставить точное соответствие между «частным» IP абонента в СШПД и публичным IP в сети Интернет в любой момент времени.

Для предоставления этой информации уполномоченным органам оператор должен выполнить корреляцию между CDR, получаемых в момент авторизации с BRAS и данными Netflow с оборудования Ядра сети.

Для выхода в Интернет «частный» IP адрес транслируется в «публичный». Настройки трансляции адресов производятся на маршрутизаторах ядра сети либо на BRAS. Выбор места трансляции осуществляется по усмотрению конкретного региона и согласованию с центром сети. Кроме того, для трансляции в некоторых случаях допускается использовать выделенный сервер. На рисунке 2.7.1.1-1 приведен вариант, где трансляция производится в ядре.

Во время трансляции на маршрутизаторах, осуществляющих эту процедуру, создается и поддерживается таблица соответствия между оригинальными IP адресами и измененными.

Это накладывает следующее ограничение – не допускается асимметричная маршрутизация – пакет должен уходит из BRAS и возвращаться одним и тем же маршрутом. Для обеспечения симметричной маршрутизации необходимо сделать один маршрут более предпочтительным чем альтернативный, например, манипулируя метриками OSPF маршрутов. В этом случае весь трафик с одного BRAS будет идти через одни маршрутизатор ядра, в то время как второй будет оставаться в резерве.

На рисунке 2.7.1.1-1 Представлена общая логическая схема предоставления услуг физическим лицам.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

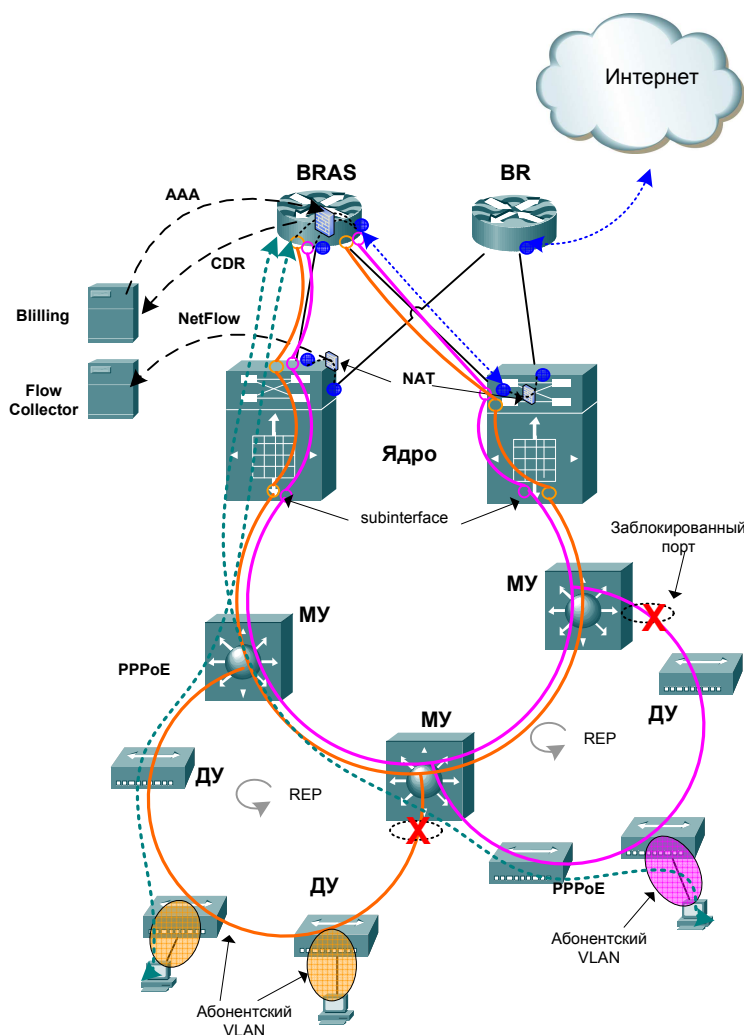


Рисунок 2.7.1.1-1. Общая логическая схема представления услуг физическим лицам.

В крупных городах в ядре сети может быть более двух маршрутизаторов.

В этом случае меняется логика транспортировки абонентских VLAN до BRAS.

В случае с 4 и более маршрутизаторов ядра сети, BRAS должны быть подключены к одной паре маршрутизаторов, а абонентские VLAN птерминируются а другой паре маршрутизаторов. До BRAS абонентские VLAN доставляются с помощью MPLS туннелей (*xconnect*).

На рисунке 2.7.1.1-2 представлена общая логическая схема предоставления услуг физическим лицам для случая с 4 маршрутизаторами ядра сети.

Ине. № подл.	Подл. и дата	Взам. ине. №

Изм	Лист	№ документа	Подпись	Дата

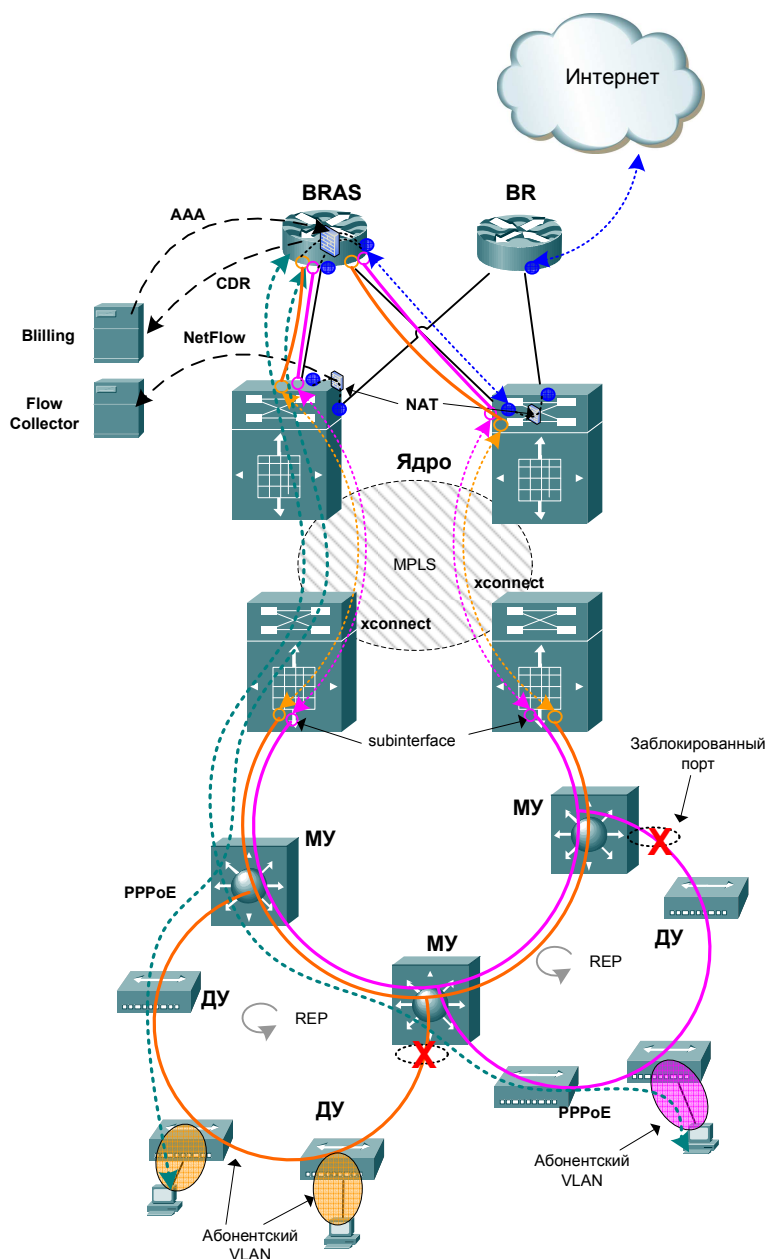


Рисунок 2.7.1.1-2 Общая логическая схема предоставления услуг физическим лицам для случая с 4 маршрутизаторами ядра сети.

2.7.1.2. Услуга «IP-телефония» и группа услуг IP TV.

Услуги VoIP и группы услуг IP TV абонент получает в том же порту коммутатора ДУ СШПД СтримТВ.

Предполагается, что для получения этих услуг абоненту будет устанавливаться специализированное устройство – SetTopBox (STB) для получения услуг IPTV и голосовой шлюз или IP телефон для получения услуг VoIP.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

В случае, если абоненту необходимо получение нескольких услуг (ШПД, VoIP и IP TV) одновременно, ему будет необходимо поставить коммутатор, который будет подключаться к оборудованию ДУ СШПД. Такой коммутатор является оборудованием клиента (CPE) и не входит в зону ответственности СтримТВ.

Настройки STB и голосового шлюза осуществляются службой эксплуатации СтримТВ при подключении абонента.

Возможно получение услуг непосредственно на компьютере абонента. В этом случае абоненту необходимо настроить сетевой интерфейс на своем компьютере для получения IP адреса автоматически и выполнить настройки приложений по инструкции, которая должна быть предоставлена эксплуатационной службой СтримТВ при заключении контракта.

2.7.2. Услуги для юридических лиц

Юридическим лицам могут быть оказаны следующие услуги:

- Услуга подключения к интернет;
- Услуга VPN L2;
- Услуга VPDN;
- Услуга VPN L3.

2.7.2.1. Услуга «подключение к Интернет»

Услуга подключения к Интернет для юридических лиц может быть предоставлена несколькими способами.

- Настройка PPPoE как в случае с подключениями физических лиц. Т.е. на одном из компьютеров клиента – юридического лица, настраивается PPPoE соединение, и этот компьютер при этом является шлюзом для других компьютеров локальной сети клиента.
- Настройка на существующем у клиента маршрутизаторе PPPoE соединения. При этом оборудование клиента (CPE) не входит в зону ответственности СтримТВ.
- Создание выделенного канала в интернет.
- Организация доступа по технологии, аналогичной L3 VPN.

2.7.2.2. Услуга передачи данных VPN L2

В простейшем случае услуга VPN L2 предоставляет симметричную в обоих направлениях полосу пропускания, без использования в ее рамках параметров качества обслуживания. Примером применения VPN L2 является соединение двух и более офисов по выделенному каналу.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

Для предоставления этой услуги на портах ДУ, к которым подключены точки абонента, должен быть настроен транспортный VLAN из выделенного диапазона. Этот же транспортный VLAN должен быть сконфигурирован на всех транзитных коммутаторах, на пути между точками подключения.

Чтобы избежать необходимости передавать BPDU STP через оборудования ядра и в тоже время оставить возможность резервировать данную услугу, в случае двух маршрутизаторов в ядре, применяется следующий подход: точки подключения абонента помещаются в один VLAN только в пределах одного магистрального кольца, в других сегментах используются другие VLAN. Трафик между VLAN благодаря тому, что порты, принадлежащие разным VLAN, соединены патч-кордом на коммутаторе, находящемся в центральной точке присутствия абонента. За блокировку избыточных маршрутов в магистральном сегменте отвечает REP.

На Рисунке № 2.7.2.2.-1 приведена схема организации услуги передачи данных point-to-point и point-to-multipoint в случае 2-х маршрутизаторов.

Име. № подл.					СИТ.СТВ.ЭТП.2.9/08	Лист
						69
Подл. и дата						
Взам. име. №						
Изм	Лист	№ документа	Подпись	Дата		

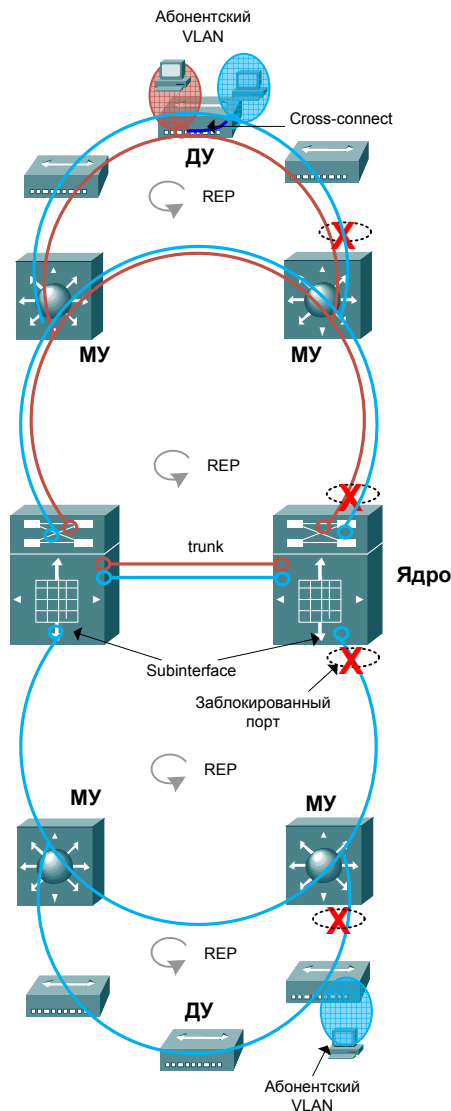


Рисунок 2.7.2.2.-1. схема организации услуг point-to-point и point-to-multipoint случае 2-х маршрутизаторов.

Использование вышеописанной схемы имеет существенные недостатки:

- проблемы с масштабированием, управляемостью и устойчивостью.
- Недостаток VLAN ID
- Большие MAC-таблицы в ядре
- Трудности с поддержкой данных топологий.

В связи с этим, эту схему допускается использовать только в небольших сайтах с маленьким количеством потребителей услуги.

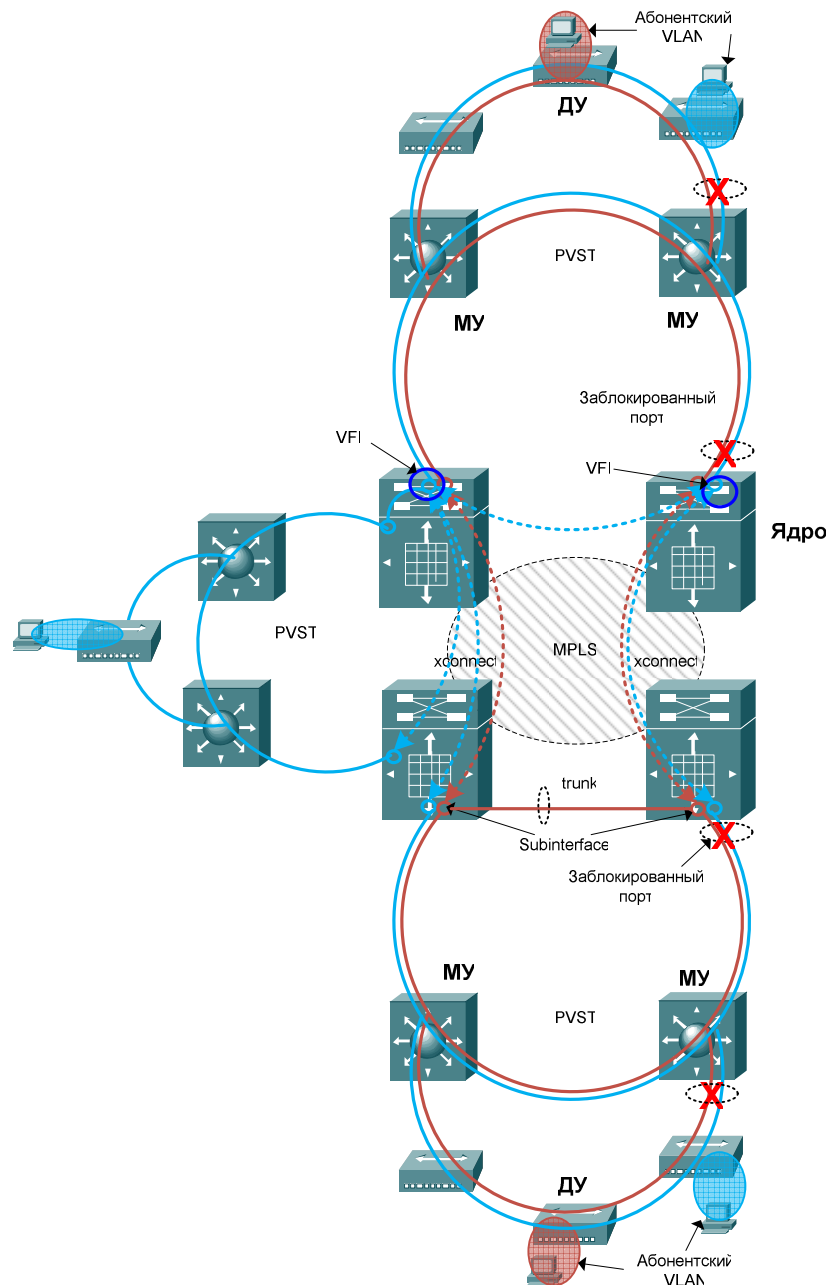
В СШПД для избежания проблем, описанных выше, может быть использована технология VPLS, где через MPLS сеть проходит по одному туннелю, соединяющему

Изм.	Лист	№ документа	Подпись	Дата
------	------	-------------	---------	------

сконфигурированные VFI на каждом маршрутизаторе ядра сети. При этом все VFI должны быть полносвязанными.

Для реализации технологии VPLS в оборудовании ядра сети необходимо использовать дополнительное оборудование -- карту 7600 ES20 Line Card.

На Рисунке 2.7.2.2.-3 представлен вариант этой схемы, когда используется только две карты ES20, в этом случае полносвязанность формируется между VFI и сабинтерфейсами (или SVI).



Инв. № подл.	Подл. и дата				Взам. инв. №			
	Изм	Лист	№ документа	Подпись	Дата			

Рисунок 2.7.2.2.-3. общая логическая схема предоставления услуг с использованием технологии VPLS для случаев числом маршрутизаторов ядра сети больше 2-х.

2.7.2.3. Организация виртуальной сети для заказчика, не имеющего непосредственного подключения к сети «Стрим-ТВ» (VPDN)

Для организации виртуальной сети с участием одного или нескольких сегментов сети заказчика, не имеющих непосредственного подключения к сети «Стрим-ТВ» используется технология VPDN.

В этом случае PPPoE сессия клиента после авторизации, не терминируется на BRAS, а инкапсулируется в L2TP туннель и передается дальше, в корпоративную сеть клиента, где терминируется на L2TP Network Server (LNS) клиента.

Поскольку L2TP работает поверх IP, LNS может находиться в произвольном месте.

Вся необходимая информация для такого подключения, хранится в учетной записи абонента и становится доступной BRAS через протокол RADIUS в момент успешной авторизации. Никаких дополнительных настроек BRAS не требуется, – достаточно прописать необходимые данные в учетной записи клиента.

Схема организации услуги виртуальной сети для заказчика, не имеющего непосредственного подключения к сети «Стрим-ТВ» (VPDN), приведена на Рисунке № 2.7.2.3.-1.

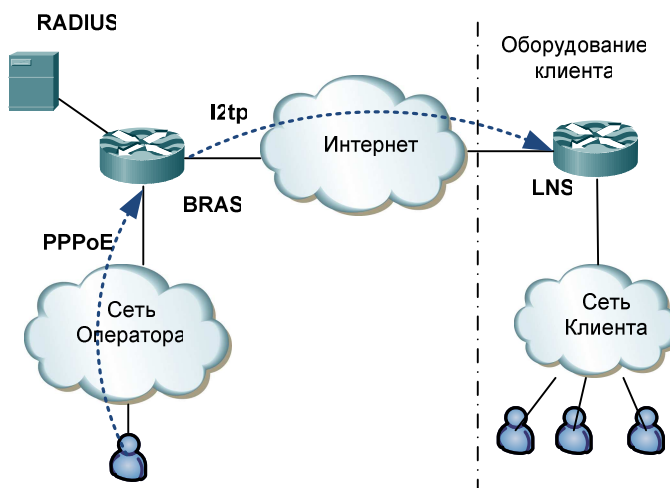


Рисунок 2.7.2.3.-1. Схема организации услуги VPDN.

2.7.2.4. Услуга L3 VPN.

Име. № подл.	
Подл. и дата	
Взам. инв. №	

Изм	Лист	№ документа	Подпись	Дата

Услуга MPLS IP VPN (MPLS Layer 3 VPN, L3VPN) предназначена для передачи IP пакетов абонента по СШПД. IP VPN позволяет организовать L3 соединение между граничными маршрутизаторами сети абонента через сеть IP MPLS СШПД. Подключение, организованное на базе услуги IP VPN, с точки зрения сетевой инфраструктуры сети абонента выглядит как обычное маршрутизируемое соединение двух и более единиц активного сетевого оборудования.

Основное преимущество технологии L3 VPN заключается в отсутствии необходимости в транспортировке дополнительных заголовков протоколов L2 и создания end-to-end VLAN в СШПД.

В случае предоставления услуги L3 VPN VLAN абонента терминируются на BRAS. На каждую точку подключения выделяется отдельный VLAN.

До BRAS VLAN абонентов доставляются аналогично тому, как это делается в случае услуг для физических лиц.

BRAS, используемые для терминирования VLAN абонентов, могут быть как отдельные так и совмещенные с теми, что обслуживают обычные подключения. И в том и в другом случае принцип настроек одинаков:

VLAN от точек подключения терминируются на сабинтерфейсах BRAS. При этом получившиеся L3 интерфейсы помещаются в VRF, созданный для этого абонента. Принцип создания VRF должен быть унифицирован – именем является латинизированное название организации-клиента, RD составляется в виде AS:NN, где AS – Номер автономной системы, NN – порядковый номер, увеличивающийся с каждым новым абонентом.

Если есть необходимость в резервировании, то можно использовать 2 BRAS и терминировать VLAN на каждом из них. Тогда внутри VRF между разными BRAS настраивается протокол HSRP, при этом необходимо, чтобы маршрутизатор, выбранный активным в HSRP группе, также был более предпочтительным с точки зрения BGP. Так как на одном маршрутизаторе может быть не более 256 HSRP групп, то использование общего пула BRAS для всех видов услуг представляется наиболее предпочтительным.

Опционально, внутри абонентского VRF может быть сконфигурирован протокол маршрутизации (OSPF, RIP) для передачи маршрутной информации между маршрутизаторами абонентов. Маршрутные префиксы при этом остаются изолированными внутри адресного пространства абонента. Таким образом, с точки зрения заказчика, все его пограничные маршрутизаторы подключаются к виртуальному маршрутизатору сети СШПД.

На рисунке 2.7.2.4-1 представлена общая логическая схема оказания услуги L3 VPN.

Име. № подл.	Подп. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

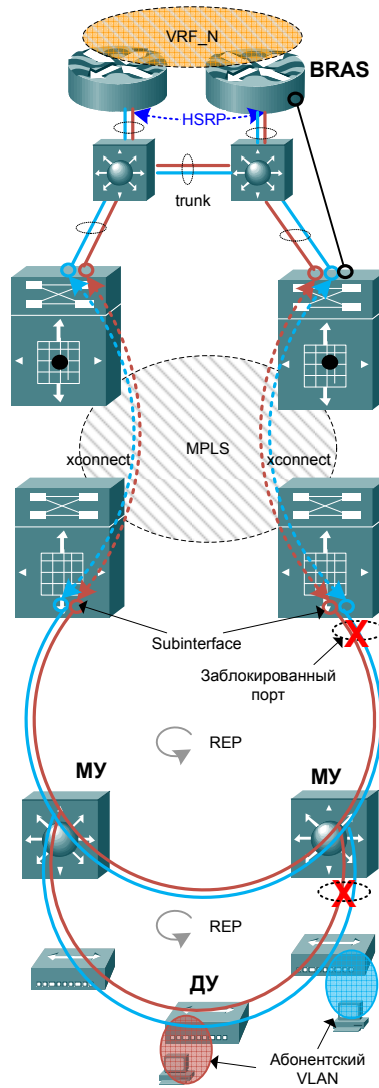


Рисунок 2.7.2.4-1 Общая логическая схема оказания услуги L3 VPN.

Для передачи трафика L3 VPN между разными регионами СтримТВ используется Inter-AS MPLS option B. Трафик всех VPN передается между регионами в одном логическом интерфейсе. При этом для разграничения VPN, как и в intra-AS случае, используется MPLS метка, т.е. трафик между сетями передается MPLS-инкапсулированным.

Для передачи информации о метках используется расширения протокола BGP. ASBR получает VPN-префикс, инжектированный PE, меняет next-hop для этого префикса его метку и анонсирует по eBGP в другую AS. ASBR в соседней AS, получив VPN префикс, анонсирует его в собственную AS. В результате между границами AS формируется LSP для передачи VPN трафика. После этого алгоритм передачи VPN трафика ASBR фактически аналогичен алгоритму P-маршрутизатора. ASBR меняет метки, просигнализированные протоколом BGP.

Име. № подл.	
Подл. и дата	
Взам. име. №	

Изм	Лист	№ документа	Подпись	Дата

В СШДП “Стрим-ТВ” функции PE выполняют выделенные под эту задачу маршрутизаторы. В случае небольшой нагрузки для этой цели можно использовать существующие BRAS. Маршрутизаторы ядра являются P устройствами. Один их сабинтерфесов между BRAS и ядром сконфигурирован как способный переносить MPLS метки. На нем же поднят iBGP процесс между BRAS и опорным маршрутизатором ядра. iBGP служит для транспортирования сигнальной информации о каждом из VPN.

На рисунке 2.7.2.4-2 представлена общая логическая схема оказания услуги L3 VPN между разными регионами СтримТВ.

Име. № подл.	Подп. и дата	Взам. име. №					
			СИТ.СТВ.ЭТП.2.9/08				Лист
							75
Изм	Лист	№ документа	Подпись	Дата			

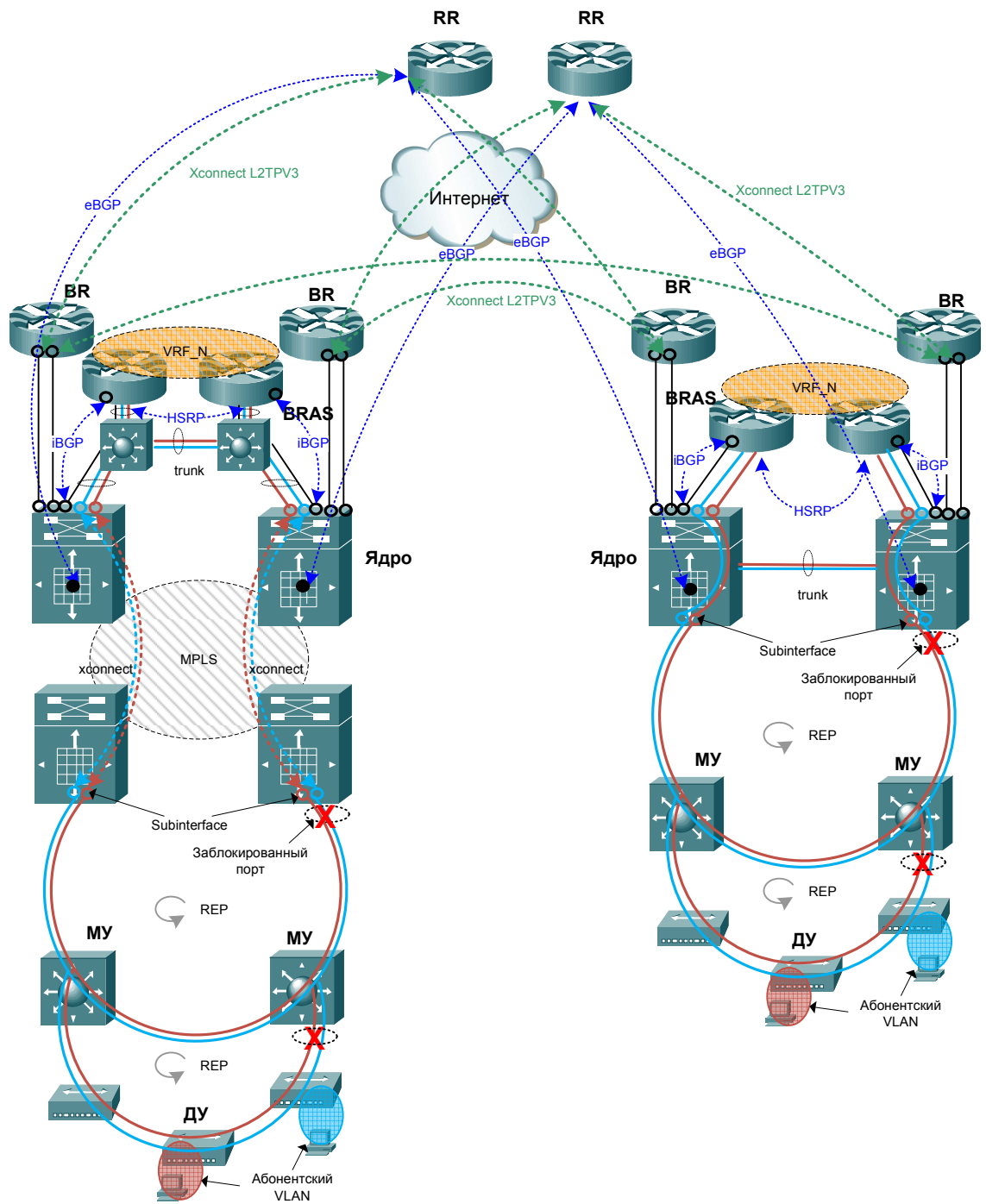


Рисунок 2.7.4.2.-2. общая логическая схема оказания услуги L3 VPN между разными регионами СтримТВ.

Поскольку основным типом подключений будет арендованный у магистрального оператора канал в Интернет, то для передачи MPLS трафика нужно использовать туннели. В данном решении используются L2TPv3 туннели, начинающиеся и терминирующиеся на входящих со стороны ядра интерфейсах пограничных

Изн. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

маршрутизаторах. Эти туннели должны образовать полносвязанный граф, узлами которого являются регионы, предоставляющие услугу L3 VPN.

BGP, в отличие от туннелей, настраивается только между маршрутизаторами ядра в регионе и между маршрутизаторами ядра в одном из центров СШПД, которые в данном случае выступают как отражатели маршрутов (RR - route reflectors).

2.8. Организация мер СОРМ

2.8.1. Общие принципы организации СОРМ

Внедрение СОРМ производится на основании Технических Условий, выдаваемых уполномоченными органами (региональными УФСБ), которые регламентируют месторасположение оборудования СОРМ, требования к помещению, каналу связи и прочее.

Для организации СОРМ в Сети необходимо организовать SPAN сессию со всех маршрутизаторов ядра сети.

На Рисунке № 2.8.1.-1 представлена схема организации СОРМ.

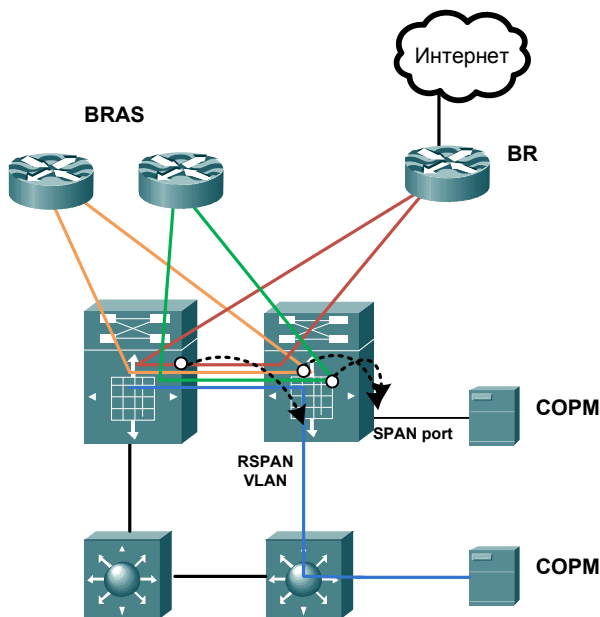


Рисунок 2.8.1.-1. Схема организации СОРМ.

2.8.2. Настройка оборудования для реализации СОРМ

Возможны два варианта настройки оборудования для реализации СОРМ:

Изн. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

Вариант №1: В качестве источника трафика для COPM конфигурируются VLAN, через которые BRAS подключаются к ядру Сети.

В этом случае в порт для COPM будет попадать весь трафик абонентов туннелированный в PPPoE. В случае, если необходимо (по ТУ уполномоченных органов) отдавать в порт COPM детуннелированный (без PPPoE) трафик, между оборудованием COPM и портом маршрутизатора ядра сети необходимо установить дополнительный шлюз (Cisco 7201) с включенной функцией lawful intercept. Пропускная способность указанного шлюза с включенной функцией lawful intercept составляет 500 Мбит/с.

Настройки оборудования ядра Сети:

```
monitor session 1 source vlan 11-20
monitor session 1 destination port GigabitEthernet 1/24 ....!### Порт COPM ###
```

Вариант №2: В качестве источника трафика для COPM конфигурируются VLAN, через которые маршрутизаторы пограничного сегмента (BR) подключаются к интернет.

В этом случае в порт COPM будет попадать только трафик абонентов в интернет.

Настройки оборудования ядра Сети:

```
monitor session 1 source vlan 60-70
monitor session 1 destination port GigabitEthernet 1/24 ....!### Порт COPM ###
```

2.8.3. Организация канала для COPM

Канал для COPM организуется на основании Технических Условий, выдаваемых уполномоченными органами (региональными УФСБ). В зависимости от ТУ, для организации канала связи необходимо предусмотреть дополнительное оборудование (маршрутизатор), который будет подключен к Сети.

Ине. № подл.	
Подл. и дата	
Взам. ине. №	

3. Миграция существующих сетей филиалов «Стрим-ТВ» на унифицированную топологию

Миграция сетей филиалов «Стрим-ТВ» на унифицированное техническое решение, описанное настоящим Проектом, производится для их типизации и повышения управляемости, снижения административных издержек, а также для подготовки филиальной инфраструктуры «Стрим-ТВ» к оказанию единого набора услуг.

Решение о необходимости модернизации и реструктурирования тех или иных компонентов филиальной инфраструктуры, порядке, этапах и нюансах модернизации для каждого филиала «Стрим-ТВ» принимается индивидуально на основе данных, полученных в результате технологического обследования.

В общем случае, миграции подлежат сети с децентрализованной топологией, допускающие возможность неавторизованного использования ресурсов сети «Стрим-ТВ», а также неконтрольный обмен трафиком между абонентами. Также в ходе миграции необходимо разворачивать отсутствующие телематические и технологические службы и модернизировать существующие, не удовлетворяющие настоящему техническому решению, сервисы.

3.1. Этапы миграции

На начальном этапе миграции проводится технологическое обследование, и на его основе осуществляется планирование дальнейших работ. В первую очередь оценивается объем выполняемых в рамках миграции работ, формируется команда, которая будет участвовать в миграции и создается поэтапный план перехода на новую телекоммуникационную инфраструктуру.

В случае сохранения элементов сетевой инфраструктуры филиала «Стрим-ТВ» на следующем этапе производится модернизация (оптимизация) ядра сети, пограничного сегмента, сегментов телематических и технологических служб, а также подготовка к миграции сетевой инфраструктуры всех уровней.

На следующем этапе на новой программно-аппаратной платформе выполняется развертывание необходимых телематических и технологических сервисов, работающих в тестовом режиме.

Затем производится адаптация конфигураций телематических и технологических сервисов и их последующий перенос на развернутые ранее платформы. По окончании настройки выполняется отладка настроенных служб и сервисов.

Име. № подл.	Подл. и дата	Взам. ине. №
--------------	--------------	--------------

Изм	Лист	№ документа	Подпись	Дата
-----	------	-------------	---------	------

Миграция на унифицированное техническое решение также включает в себя установку, настройку и интеграцию в сформированную сетевую инфраструктуру сервисного уровня маршрутизаторов BRAS в полном соответствии с настоящим Проектом.

По окончании предварительных настроечных работ в сети филиала «Стрим-ТВ» создается тестовый сегмент, моделирующий текущую штатную схему подключения абонента. На примере такого сегмента отлаживается механизм информирования абонентов о смене схемы предоставления услуг, технология смены схемы услуги, а также проверяется доступность и корректная работа всех телематических и технологических служб и сервисов.

На финальном этапе осуществляется информирование абонентов о смене схемы предоставления услуг и поэтапное, сегмент за сегментом, переключение пользователей на обновленную сетевую и сервисную инфраструктуру.

3.2. Изменение настроек оборудования на МУ и ДУ

В зависимости от текущей схемы подключения абонентов выбирается стратегия внесения изменений в конфигурацию оборудования МУ и ДУ.

В общем случае, при переводе абонента на новую схему предоставления услуг от BRAS к ДУ прокладываются два новых VLAN (для unicast-сервисов и для multicast-сервисов). В соответствии с настоящим Проектом выполняется маршрутизация этих VLAN, производится конфигурирование коммутаторов ядра сети, МУ и ДУ в части общих настроек, настроек данных VLAN и настроек портов, через которые выполняется транзит абонентского трафика. На финальной стадии выполняется настройка абонентского порта и настройка на нем проложенных на предыдущих шагах VLAN.

По окончании настроек активного сетевого оборудования МУ и ДУ производится перенастройка персонального компьютера абонента в соответствии с новой схемой предоставления услуг. В частности, существующие настройки сетевого интерфейса приводятся в исходное состояние по умолчанию, выполняется настройка PPPoE соединения, а также проверяются настройки браузера и почтового клиента.

3.3. Модернизация и изменение настроек BRAS

В общем случае, при выполнении миграции сетей филиалов «Стрим-ТВ» на унифицированное техническое решение, выполняется установка новых BRAS и настройка их в соответствии с настоящим Проектом.

При наличии в сети филиала NAS (Network Access Server), VPN-серверов или BRAS, перевод абонентов с них производится в рабочем порядке, абонент за абонентом. Сначала в соответствии с п.п. 3.3. настоящего Проекта выполняется настройка

Име. № подл.	
Подп. и дата	
Взам. ине. №	

Изм	Лист	№ документа	Подпись	Дата

активного сетевого оборудования ядра сети, МУ и ДУ, затем выполняется терминирование unicast-VLAN на BRAS, а на завершающей стадии выполняется перенастройка или создание нового соединения на персональном компьютере абонента.

3.4. Модернизация и изменения настроек телематических серверов

При выполнении миграции на обновленные телематические и технологические сервисы в первую очередь выполняется перенос наиболее критичных сервисов DNS и электронной почты.

По окончании отладки сервисов разрешения имен и почтового сервиса существующие серверы выключаются, а на новых серверах производится изменение тестовых IP-адресов на IP-адреса, используемые продуктивными системами. Перенос данных с почтового сервера осуществляется на этапе настройки/отладки и производится только в случае использования системы хранения MAILDIR.

Аналогичным образом в рабочем порядке производится перенос остальных телематических и технологических сервисов.

Ине. № подл.	Подл. и дата	Взам. ине. №						СИТ.СТВ.ЭТП.2.9/08	Лист
									81
			Изм	Лист	№ документа	Подпись	Дата		

ЛИСТ ПРИМЕЧАНИЙ

Изн. № подл.	Подл. и дата	Взам. инв. №

Изм	Лист	№ документа	Подпись	Дата

СИТ.СТВ.ЭТП.2.9/08

Лист

83