МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

УНИВЕРСИТЕТ ИМЕНИ СУЛЕЙМАНА ДЕМИРЕЛЯ

УДК (индекс универсальной десятичной классификации)

На правах рукописи

Амреев Максат Берикович

«МУЛЬТИСЕРВИСНАЯ СЕТЬ КАМПУСА СДУ»

Магистерская диссертация на соискание
академической степени магистра
по специальности 6М070400-«ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ»

АЛМАТЫ – 2012

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

УНИВЕРСИТЕТ ИМЕНИ СУЛЕЙМАНА ДЕМИРЕЛЯ

«Допущенк защите»:
Заведующий кафедрой
Вычислительная техника и
программное обеспечение
_____ к.т.н. Иванов А.И.
«___»_____ 20___г.

Заведующий отделом послевузовского образования, PhD
_____А.А.Шалбаев
«___»_____ 20___ г.

Магистерская диссертация

МУЛЬТИСЕРВИСНАЯ СЕТЬ КАМПУСА СДУ

специальность: 6М070400 «вычислительная техника и программное обеспечение»

Магистрант _____ Амреев М.Б.

Научный руководитель _____ д.т.н.,профессор
Куандыков А.А

АЛМАТЫ – 2012

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В последнее время с завидным постоянством идет речь о новинках интернет-технологий, анонсируемых тем или иным оператором связи. Речь пойдет о технологии, которая в ближайшее время может заменить Frame Relay/ATM. Это технология MPLS, которая будет интересна по соотношению цена /качество прежде всего корпоративным клиентам.

MPLS (MultiProtocol Label Switching) – это технология коммутации пакетов на основе использования меток в многопротокольных сетях. MPLS изначально предназначена для построения магистральных IP-сетей с высокими возможностями в области управления трафиком и качеством сервиса.

Metro Ethernet – это технология построения сетей агрегации на основе технологии Ethernet. Выбор Ethernet не случаен, так как эта технология давно уже является стандартом де-факто для локальных сетей.

Metro Ethernet представляет собой концепцию предоставления услуг сети Ethernet в масштабах города. Гибкость технологии Ethernet, её относительная дешевизна, а также очень большая распространенность и вероятность поддержки сетевым оборудованием различных производителей делает Metro Ethernet сети практически идеальным выбором для построения пакетной агрегационной магистрали города. Клиент в этом случае получает несколько вариантов виртуальных каналов связи с большим количеством параметров, ответственных за качество услуги, снижая при этом свои затраты на сетевое оборудование (сетевые интерфейсы типа Ethernet имеют низкую стоимость) и расходы на приобретение услуги (стоимость услуги на базе Ethernet ниже аналогичных услуг ввиду меньших затрат и расходов провайдера на поддержание и эксплуатацию оборудования сети Ethernet).

Мировая тенденция такова, что количество подключений по протоколу Frame Relay постепенно уменьшается, подключения по протоколу ATM держаться примерно на одном уровне, а число подключений к VPN, построенным на базе MPLS, стремительно растет. В России, например, данная технология очень активно внедряется такими крупными телекоммуникационными операторами, как Equant, RTComm, ТрансТелеКом.

НАЗНАЧЕНИЕ И ПРЕДМЕТНАЯ ОБЛАСТЬ

В данном проекте предпринята попытка описания принципов и концепции построения сети передачи данных Metro Ethernet г.Алматы. В работе представлены архитектура городской мультисервисной сети, принципы реализации услуг, системы управления и биллинга.

Условные обозначения и сокращения

ACP Автоматизированная Система Расчетов
AAA Authentication, Authorization, Accounting
ASN.1 Abstract Syntax Nation 1

ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
C router	Customer router
CE router	Customer Edge router
CERT	Computer Emergency Response Team
CBWFQ	Class Based WFQ
CDR	Call Detailed Records
CIC	Cisco InfoCenter
CLI	Command Line Interface
CORBA	Common Object Request Broker Architecture
CoS	Class of Service
DPT	Dynamic Packet Transport
DTMF	Dual Tone Multi Frequency
e-BGP	External BGP
EGP	Exterior Gateway Protocol
EMS	Element Management System
FE	Fast Ethernet
FIB	Forwarding Information Base
GE	Gigabit Ethernet
GK	GateKeeper
GRE	Generic Router Encapsulation
GRT	Global Routing Table
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Messaging Protocol
i-BGP	Internal BGP
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IOS	Internet working Operation System
IP	Internet Protocol
LAC	L2TP Access Concentrator

LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LLQ	Low Latency Queue
LNS	L2TP Network Server
LRQ	Location Request
LSP	Label Switched Path
M-BGP	Multi Protocol BGP
MPLS	Multi Protocol Label Switching
MS	Multi Service
MP	Merge Point
MTTRAPD	Multi-threaded SNMP Info Mediator
NHop	Next-hop router
NLRI	Network Layer Reach ability Information
NMS	Network Management Center
NNHop	Next-next-hop router
N-PE	Network facing Provider Edge
NSF	Non Stop Forwarding
MQC	Modular QoS CLI
OSPF	Open Shortest Path First
P router	Provider router
PBX	Primary Branch Exchange
PE router	Provider Edge router
PHP	Penultimate Hop Popping
PLR	Point of Local Repair
PQ	Priority Queue
QoS	Quality of Service
RD	Router Distinguisher
RIB	Routing Information Base
RR	Route Reflector
RSVP	Resource Reservation Protocol
RT	Route Target
RTP	Real Time Protocol
RTM	Robust Trap Mechanism
SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SSO	Statefull SwithOver
TE	Traffic Engineering
U-PE	User facing Provider Edge
VLAN	Virtual local Area Network
VPN	Virtual Private Network

VPDN	Virtual Private Dial-up Network
VPNSC	VPN Solution Center
VRF	VPN Routing and Forwarding Table
WFQ	Weighted Fail Queuing
WRED	Weighted Random Early Detection
XML	Extendable Markup Language

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. Для успешного ведения и выполнения бизнеса на рынке и для решения финансово-экономических задач, стоящих перед государством и крупными компаниями в условиях глобализационных процессов и роста динамики мировых процессов, важное значение приобретают электронные информационно-вычислительные ресурсы и логистика. По этой причине качественные характеристики IT-инфраструктуры частных, государственных и международных предприятий, которые являются носителями информационно-вычислительных ресурсов и виртуальных услуг, становятся стратегическим фактором нашего времени. Из-за высоких требований со стороны рынка IT-инфраструктуры все больше становятся многофункциональными, распределенными как по масштабу охвата территории, так и по принципу выполнения вычислительных процессов, способу хранения и обработки данных. Таким образом, IT-инфраструктуры становятся распределенной компьютерной системой (РКС), которая стала электронной платформой, поддерживающей сегодняшний деловой мир.

Среди РКС для предприятий или для определенного ограниченного пространства человеческой или общественной деятельности важной является создания эффективной корпоративной информационной системы (КИС).

Бизнес диктует высокие требования к функциональным возможностям КИС, которая поддерживает данный бизнес процесс.

Одним из пути достижения этой цели является построение КИС на основе конвергентной технологий.

В связи с этим тема настоящей диссертационной работы является актуальной и своевременной.

Целью магистерской работы является разработка технологической и архитектурной базы, а также математического обеспечения высокоэффективной КИС.

Научная новизна полученных результатов заключается в следующем:

1. Впервые продложена и разработана конвергентная технологий для создания КИС.
2. Разработана структура и архитектура высокоэффективной КИС на базе предложенной конвергентной технологий.
3. Разработана математическое обеспечение КИС.
4. Проведено исследование эффективности КИС.

В работе для создания конвергентной технологий взяты бакие базовые технологий как мультисервисная технология и сеть, мета-компьтинговая концепция представления оконечных систем, Active Directory для управления функционированием и безопасностью.

1. АРХИТЕКТУРА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ БАЗИРУЮЩЕЙСЯ НА КОНВЕРГЕНТНУЮ ТЕХНОЛОГИЮ

Структуру КИС, построенной на базе конвергентной технологий можно представить как на рисунке 1.1.

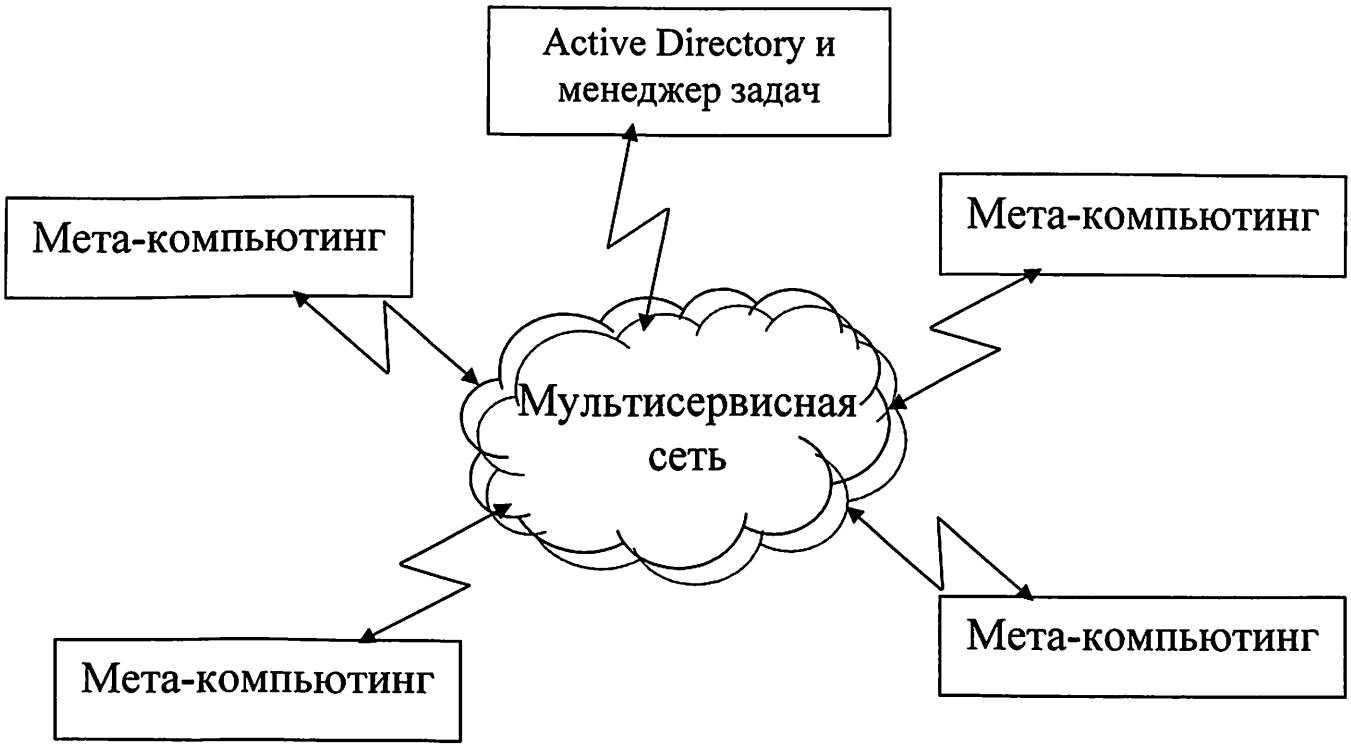


Рисунок 1.1. Структура КИС, построенной на базе конвергентной технологий

На рисунке 1.1 в качестве мета-компьютинг выступает оконечная система, которой может состоят из ЛВС или одного компьютера или какого-нибудь терминального устройства.

В работе за основу мультисервисной сети может быть принята одна из свременных технологий. В частности, следует отметить, что в последнее время с завидным постоянством идет речь о новинках интернет-технологий, анонсируемых тем или иным оператором связи. Речь пойдет о технологии, которая в ближайшее время может заменить Frame Relay/ATM. Это технология MPLS, которая будет интересна по соотношению цена /качество прежде всего корпоративным клиентам.

MPLS (MultiProtocol Label Switching) – это технология коммутации пакетов на основе использования меток в многопротокольных сетях. MPLS изначально предназначена для построения магистральных IP-сетей с высокими возможностями в области управления трафиком и качеством сервиса.

Metro Ethernet – это технология построения сетей агрегации на основе технологии Ethernet. Выбор Ethernet не случаен, так как эта технология давно уже является стандартом де-факто для локальных сетей.

Metro Ethernet представляет собой концепцию предоставления услуг сети Ethernet в масштабах города. Гибкость технологии Ethernet, её относительная дешевизна, а также очень большая распространенность и вероятность поддержки сетевым оборудованием различных производителей делает Metro Ethernet сети практически идеальным выбором для построения пакетной агрегационной

магистрали города. Клиент в этом случае получает несколько вариантов виртуальных каналов связи с большим количеством параметров, ответственных за качество услуги, снижая при этом свои затраты на сетевое оборудование (сетевые интерфейсы типа Ethernet имеют низкую стоимость) и расходы на приобретение услуги (стоимость услуги на базе Ethernet ниже аналогичных услуг ввиду меньших затрат и расходов провайдера на поддержание и эксплуатацию оборудования сети Ethernet).

Мировая тенденция такова, что количество подключений по протоколу Frame Relay постепенно уменьшается, подключения по протоколу ATM держаться примерно на одном уровне, а число подключений к VPN, построенным на базе MPLS, стремительно растет. В России, например, данная технология очень активно внедряется такими крупными телекоммуникационными операторами, как Equant, RTComm, ТрансТелеКом.

2. УСЛУГИ МУЛЬТИСЕРВИСНОЙ СЕТИ

В нашей сети могут быть реализованы следующие категории услуг:

2.1 Услуги предоставления доступа в Интернет

Предоставление доступа в Интернет является одной из основных услуг, которая подразделяется на предоставление доступа по выделенным линиям и посредством шлюза выбора услуг.

2.1.1 Услуги выделенного доступа

Выделенный доступ к сети Интернет посредством прямого подключения к одной из VPN Internet.

2.1.2 Доступ через шлюз выбора услуг

Подключение к сети Internet посредством протокола PPPoE и выбором услуги на шлюзе выбора услуг SSG.

2.2 Услуги предоставления корпоративного IP доступа

Услуги предоставления корпоративного IP доступа состоят в организации виртуальных частных сетей, логически отделенных от других подобных сетей, посредством деления на MPLS VPN. Услуги предоставления корпоративного IP доступа могут быть двух типов:

2.2.1 Услуги выделенного доступа

Базовый выделенный доступ в виртуальную сеть клиента посредством прямого включения MPLS VPN.

2.2.2 Доступ через шлюз выбора услуг

Подключение к сети Internet посредством протокола PPPoE и выбором услуги на шлюзе выбора услуг SSG.

2.3 Возможность выбора услуги на SSG

Клиент должен иметь возможность самостоятельно выбирать тип услуги посредством WEB портала. Клиент может выбрать доступ в Интернет, доступ в корпоративную сеть или другие услуги с помощью сервера выбора услуг SSG.

2.4 Услуги системы биллинга

Система биллинга должна обеспечивать следующий набор услуг:

- сбор, форматирование и архивирование статистики по оказанным услугам;
- блокирование оказания услуги абоненту при перерасходе средств;
- передачу статистической информации в существующую у оператора АСР.

3. СТРУКТУРА МУЛЬТИСЕРВИСНОЙ СЕТИ

Наша сеть будет предназначена для организации транспортной инфраструктуры в пределах г.Алматы с возможностью предоставления спектра услуг описанных в разделе 2. Естественно, должно обеспечиваться централизованное управление и тарификация, а также отказоустойчивость.

Для решения поставленной задачи предположим что сеть передачи данных Metro Ethernet г.Алматы состоит из 23 узлов территориально распределенных по городу.

3.1 Уровни сети

Наша сеть функционально и логически будет состоять из пяти основных уровней и систем, выполняющих специализированные задачи:

- Магистральный уровень;
- Уровень доступа;
- Система биллинга;
- Система безопасности;
- Система управления.

Магистральный уровень сети передачи данных Metro Ethernet будет представлять собой MPLS магистраль, объединяющую территориально распределенные городские узлы связи. Узлы соединяются оптоволоконными линиями связи 10Gigabit Ethernet. В качестве магистральных узлов можно (и нужно) использовать MPLS коммутаторы Cisco 7609 [7], обладающие высокой производительностью и функциональностью. Каждый узел доступа выступает в роли P/PE - router.

Основной задачей магистрального уровня является предоставление высокоскоростной транспортной инфраструктуры с заданным качеством обслуживания и с минимальным временем восстановления. При этом обеспечивается функционирование узлов доступа в качестве пограничных устройств MPLS PE с предоставлением услуг Виртуальных Частных Сетей MPLS VPN, а также концентрация пользовательского трафика, дифференциация услуг, обеспечение безопасности закрытых VPN.

Уровень доступа предназначен для предоставления широкого спектра услуг оконечному пользователю, используя в качестве базового физический интерфейс Fast Ethernet. Для организации узлов клиентского доступа возможно использование кольцевой топологии на базе коммутаторов Catalyst ME3750 - 24TE [7], позволяющее наиболее оптимально охватить основные потребности клиентов разных профилей.

Система биллинга городской мультисервисной сети предназначена для тарификации пользователей, выполнения функций AAA (Authentication, Authorization,

Accounting), выставления счетов клиентам и взаиморасчетов с другими поставщиками услуг.

Система безопасности городской мультисервисной сети предназначена для обеспечения безопасности сети и пользователей от неправомерных действий нарушителей, несанкционированного доступа, регистрации событий и ведения журнала о состоянии безопасности сети в целом и основных ее компонентов в отдельности.

Система управления мультисервисной сети представляет собой программно - аппаратный комплекс, предназначенный для выполнения функций мониторинга и управления оборудования.

Структура сети представлена на Рис. 3.1.

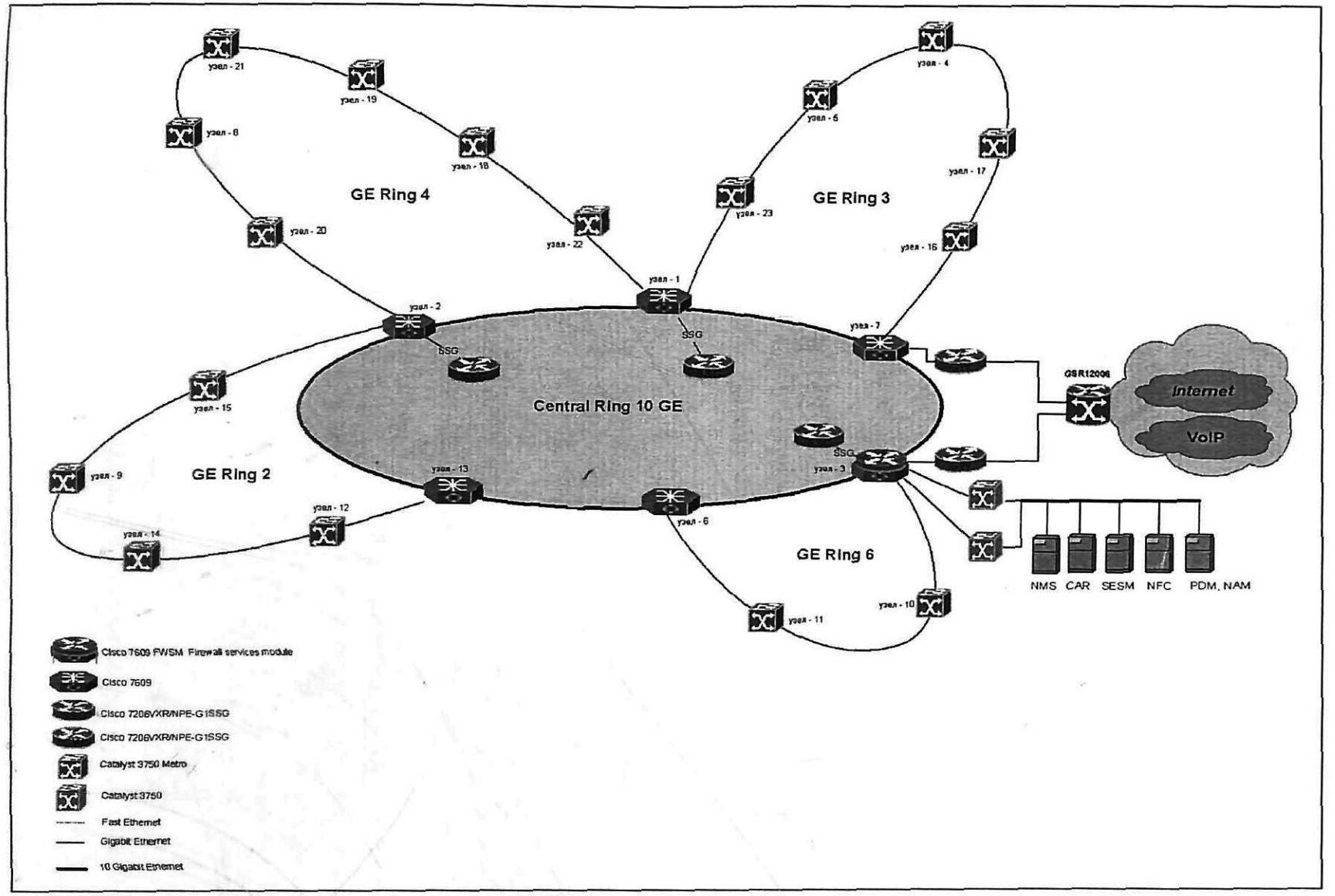


Рисунок 3.1 - Структурная схема сети передачи данных Metro Ethernet г. Алматы

3.2 СИСТЕМА АДРЕСАЦИИ

3.2.1 Блоки адресов

Естественно, для построения сети передачи данных Metro Ethernet необходимо выделить определенное количество IP адресов. По своему предназначению блоки адресов делятся на два типа:

• адреса, выделяемые для телекоммуникационного оборудования сети передачи

данных (маршрутизаторы, коммутаторы, и т.д.);

• адреса, выделяемые клиентам сети передачи данных и выделяемые для обеспечения подключения клиентов к оборудованию сети (сети типа p2p).

Адреса первого типа выделяются из числа приватных IP адресов из сети 10.0.0.0, определенных в RFC1918. Для первого типа адресации выделим два блока:

• 10.254.0.0/16

• 10.255.0.0/16

Необходимое количество адресов второго типа определяется заказчиком во время эксплуатации сети и выделяется по мере необходимости.

3.2.2 Распределение адресов

Для целей упрощения администрирования адресного пространства нашей сети блоки адресов, в соответствии с назначением, разбиваются на диапазоны:

- EOOP;
- MGMT;
- P2P;
- SERVICE.

3.2.3.1 диапазон адресов LOOP

LOOP - диапазон IP адресов, выделяемых для адресации интерфейсов Loopback0 маршрутизаторов сети.

На каждом сетевом устройстве, создается виртуальный интерфейс Loopback0, не привязанный ни к одному физическому интерфейсу. Интерфейс Loopback0 используется процессами OSPF, BGP, LDP в качестве идентификатора устройства (Router ID). Также, адрес данного интерфейса используется в качестве IP - адреса назначения для управления маршрутизатором по протоколам TELNET, SNMP и для других служебных протоколов.

Для данного диапазона выделим подсети 10.255.1.0/24, 10.255.101.0/24, 10.255.102.0/24. Распределение адресов диапазона по устройствам сети приведено в таблица 3.1

Таблица 3.1 - Распределение адресов диапазона LOOP

Подсеть/маска	Адрес	Устройство	Интерфейс
10.255.1.73/32	10.255.1.73	УЗЕЛ - 7 - 600	Loopback0
10.255.1.6/32	10.255,1.6	УЗЕЛ - 3 - 7600	Loopback0
10.255.1.62/32	10.255.1.62	УЗЕЛ - 6 - 7600	Loopback0
10.255.1.21/32	10.255.1.21	УЗЕЛ -13 - 7600	Loopback0
10.255.1.4/32	10.255.1.4	УЗЕЛ - 2 - 7600	Loopback0
10.255.1.3/32	10.255.1.3	УЗЕЛ - 1 - 7600	Loopback0
10.255.1.251/32	10.255,1.251	УЗЕЛ - 7 - GW	Loopback0
10.255.1.252/32	10.255.1.252	УЗЕЛ - 6 - GW	Loopback0
10.255.101.4/32	10.255.101.4	УЗЕЛ - 2 - SSG	Loopback0
10.255.101.3/32	10.255.101.3	УЗЕЛ - 1 - SSG	Loopback0
10.255.101.6/32	10.255.101.6	УЗЕЛ - 3 - SSG	Loopback0
10.255.102.3/32	10.255.102.3	УЗЕЛ - 1 - CON	Loopbac10
10.255.102.4/32	10.255.102.4	УЗЕЛ - 2 - CON	Loopback0
10.255.102.6/32	10.255.102.6	УЗЕЛ - 3 - CON	Loopback0
10.255.102.62/32	10.255.102.62	УЗЕЛ - 6 - CON	Loopback0
10.255.102.73/32	10.255.102.73	УЗЕЛ - 7 - CON	Loopback0
10.255.102.21/32	10.255.102.21	УЗЕЛ -13 - CON	Loopback0

3.2.3.2 Диапазон адресов MGMT

MGMT - диапазон IP адресов, выделяемых для построения указанных виртуальных сетей на объектах сети передачи данных Metro Ethernet г.Алматы.

Он включает в себя:

- 10.255.0.0/16 - для управления коммутаторами Catalyst 3750ME уровня доступа;

- 10.254.0.0/16 - для управления устройствами узлов магистрального кольца, подключенных к маршрутизаторам Cisco 7609.

Управление сетевыми устройствами Cisco Catalyst 3750ME, не поддерживающими Loopback - интерфейсы, осуществляется через VLAN - интерфейсы, выделенные для управления. Нумерация VLAN - интерфейсов осуществляется в соответствии со схемой:

VLAN 400X, где X - номер кольца доступа.

Например: в кольце 3 выделяется VLAN 4003. Таким образом происходит отделение трафика управления от трафика передачи данных на канальном уровне модели OSI, что позволяет повысить уровень защищенности сети.

Подсеть 10.255.0.0/16, для управления коммутаторами Catalyst 3750ME уровня доступа, в свою очередь, делится на подсети 10.255.xxx.0/24, где xxx - номер кольца (2, 3, 4, 6). Распределение адресов диапазона по устройствам сети приведено в таблица 3.2.

Подсеть 10.254.0.0/16, для управления устройствами узлов магистрального кольца, используется для построения локальных сетей на объектах магистрального сегмента . Данная подсеть используются для подключения устройств в пределах одного магистрального узла сети, для построения этих сетей на каждом узле при необходимости создается виртуальная сеть VLAN. Подсеть 10.254.0.0/16, в свою очередь, разбивается на подсети 10.254.xxx.0/24, где xxx номер узла (1, 2, 3, 13, 6, 7). Распределение адресов подсети 10.254.0.0/16 приведено в таблице 3.3.

Таблица 3.2 - Распределение адресов диапазона MGMT (подсеть 255)

Подсеть/маска	Адрес	Устройство	Интерфейс
10.255.2.0/24	10.255.2.4	УЗЕЛ - 2 - 7600	VLAN 4002
	10.255.2.20	УЗЕЛ - 12 - 750ME	VLAN 4002
	10.255.2.22	УЗЕЛ - 14 - 3750ME	VLAN 4002
	10.255.2.76	УЗЕЛ - 9 - 3750ME	VLAN 4002
	10.255.2.25	УЗЕЛ - 15 - 3750ME	VLAN 4002
	10.255.2.2 1	УЗЕЛ - 13 - 7600	VLAN 4002
10.255.3.0/24	10.255.3.3	УЗЕЛ - 1 - 7600	VLAN 4003
	10.255.3.38	УЗЕЛ - 23 - 3750ME	VLAN 4003
	10.255.3.52	УЗЕЛ - 5 - 3750ME	VLAN 4003
	10.255.3.51	УЗЕЛ - 4 - 3750ME	VLAN 4003
	10.255.3.3 1	УЗЕЛ - 17 - 3750ME	VLAN 4003
	10.255.3.30	УЗЕЛ - 16 - 3750ME	VLAN 4003
	10.255.3.73	УЗЕЛ - 7 - 7600	VLAN 4003
10.255.4.0/24	10.255.4.4	УЗЕЛ - 2 - 7600	VLAN 4004
	10.255.4.47	УЗЕЛ - 20 - 375OME	VLAN 4004
	10.255.4.74	УЗЕЛ - 8 - 3750ME	VLAN 4004
	10.255.4.48	УЗЕЛ - 21 - 3750ME	VLAN 4004
	10.255.4.46	УЗЕЛ - 19 - 3750ME	VLAN 4004
	10.255.4.40	УЗЕЛ - 18 - 3750ME	VLAN 4004
	10.255.4.68	УЗЕЛ - 22 - 3750ME	VLAN 4004
	10.255.4.3	УЗЕЛ - 1 - 7600	VLAN 4004
10.255.6.0/24	10.255.6.6	УЗЕЛ - 3 - 7600	VLAN 4006
	10.255.6.91	УЗЕЛ - 10 - 3750ME	VLAN 4006
	10.255.6.92	УЗЕЛ - 11 - 3750ME	VLAN 4006
	10.255.6.62	УЗЕЛ - 32 - 7600	VLAN 4006

Таблица 3.3 - Распределение адресов диапазона MGMT (подсеть 254)

Узел/диапазон IP	Подсеть	Адрес	Устройство	Интерфейс
УЗЕЛ - 3	10.254.6.0/30	10.254.6.1	УЗЕЛ - 3 - 760C	VLAN 4016

10.254.6.0/24		10.254.6.2	УЗЕЛ - 3 - 6	VLAN 4C16
	10.254.6.4/30	10.254.6.5	УЗЕЛ - 3 - 7600	Gi 8/1
		10.254.6.6	УЗЕЛ - 3 - CON	Fa 0/0
	10.254.6.8/30	10.254.6.9	УЗЕЛ - 3 - 7600	
		10.254.6.10	УЗЕЛ - 3 - NAM	
	10.254.6.16/28	10.254.6.17	УЗЕЛ - 3 - 7600	VLAN 20
		10.254.6.21	УЗЕЛ - 3 -SW1,2	VLAN 20
УЗЕЛ - 6 10.254.62.0/24	10.254.62.4/30	10.254.62.5	УЗЕЛ - 32 - 7600	Gi 8/1
		10.254.62.6	УЗЕЛ - 32 - CON	Fa 0/0
УЗЕЛ - 13 10.254.21.0/24	10.254.21.4/30	10.254.21.5	УЗЕЛ - 13 - 7600	Gi 8/1
		10.254.21.6	УЗЕЛ - 13 - CON	Fa 0/0
УЗЕЛ - 2 10.254.4.0/24	10.254.4.0/30	10.254.4.1	УЗЕЛ - 2 - 7600	VLAN 4014
		10.254.4.2	УЗЕЛ - 2 - SSG	VLAN 4014
	10.254.4.4/30	10.254.4.5	УЗЕЛ - 2 - 7600	Gi 8/1
		10.254.4.6	УЗЕЛ - 2 - CON	Fa 0/0

Продолжение таблицы 3.3.

Узел/диапазон 1P	Подсеть	Адрес	Устройство	Интерфейс
УЗЕЛ - 1 10.254.3.0/24	10.254.3.0/30	10.254.3.1	УЗЕЛ - 1 - 7600	VLAN 4013
		10.254.3.2	УЗЕЛ - 1 - SSG	VLAN 4013
	10.254.3.4/30	10.254.3.5	УЗЕЛ - 1 - 7600	Gi 8/1
		10.254.3.6	УЗЕЛ - 1 - CON	Fa 0/0
УЗЕЛ - 7 10.254.73.0/24	10.254.73.4/30	10.254.73.5	УЗЕЛ - 7 - 7600	Gi 8/1
		10.254.73.6	УЗЕЛ - 7 - CON	Fa 0/0
	10.254.73.8/30	10.254.73.9	УЗЕЛ - 7 - 7600	
		10.254.73.10	УЗЕЛ - 7 - NAM	

3.2.3.3 диапазон адресов P2P

P2P - диапазон IP адресов, выделенный для адресации связей «точка - точка» маршрутизаторов сети передачи данных.

Для данного диапазона выделена подсеть 10.255.xy.0/24, где xy образуются как:

x - равное 1, обозначает принадлежность P2P сети магистральному кольцу;

y - номер противолежащего кольца доступа (2, 3, 4, 6) ;

y - 1 для P2P - сети, соединяющей УЗЕЛ - 7 - 7600 и УЗЕЛ - 3 - 7600 и не имеющей

противолежащего кольца доступа;

у - 5 для P2P - сети, соединяющей УЗЕЛ - 13- 7600 и УЗЕЛ - 32 - 7600 и не имеющей

противолежащего кольца доступа;

60 - для P2P сети, соединяющей УЗЕЛ - 3 - 7600 с УЗЕЛ - 3 - GW;

70 - для P2P сети, соединяющей УЗЕЛ - 7 - 7600 с УЗЕЛ - 7 - GW;

Распределение адресов диапазона по устройствам сети приведено в таблице 3.4.

3.2.3.4 диапазон адресов SERVICE

Существует класс устройств, для которых необходимо выделение отдельных подсетей. К данному классу относятся сервера с различным программным обеспечением.

Функционально их можно разделить на две группы:

- сервера, обеспечивающие функционирование предоставления услуг на основе шлюза

выбора услуг SSG (Cisco Access Registrar, Cisco Subscriber Edge Services Manager);

- сервера обеспечивающие сбор статистической информации, мониторинг и обеспечение

безопасности сети (HP Open View, Cisco Netflow Collector, Cisco Works LAN Management Solution, Cisco Secure ACS).

Для данного диапазона выделены подсети 10.255.xxx.0/24, где xxx -21, 22. Распределение адресов диапазона по устройствам сети приведено в таблице 3.5.

Таблица 3.4 - Распределение адресов диапазона P2P

Подсеть	Адрес	Устройство	Интерфейс
10.255.11.0/24	10.255.11.6	УЗЕЛ - 3 - 7600	VLAN 11
	10.255.11.73	УЗЕЛ - 7 - 7600	VLAN 11
10.255.12.0/24	10.255.12.4	УЗЕЛ - 2 - 7600	VLAN 12
	10.255.12.21	УЗЕЛ - 13 - 7600	VLAN 12
10.255. 13.0/24	10.255.13.3	УЗЕЛ - 1 - 7600	VLAN 13
	10.255.13.73	УЗЕЛ - 7 - 760С	VLAN 13
10.255. 14.0/24	10.255.14.3	УЗЕЛ - 1 - 7600	VLAN 14
	10.255.14.4	УЗЕЛ - 2 - 7600	VLAN 14
10.255.15.0/24	10.255.15.21	УЗЕЛ - 13- 7600	VLAN 15
	10.255.15.62	УЗЕЛ - 32 - 7600	VLAN 15
10.255. 16.0/24	10.255.16.6	УЗЕЛ - 3 - 7600	VLAN 16
	10.255.16.	УЗЕЛ - 32 -	VLAN
	62	7600	16
10.255.60.0/30	10.255.60.1	УЗЕЛ - 3 - 7600	VLAN 60

Таблица 3.5 - Распределение адресов диапазона SERVICE

Подсеть/маска	Адрес	Устройство	Интерфейс
10.255.21.0/24	10.255.21.1	УЗЕЛ - 3 - 7600	VLAN 21
	10.255.21.21	SESM	
	10.255.21.22	SESM	(для IPMP)
	10.255.21.23	SESM	(для IPMP)
10.255.22.0/24	10.255.22.1	УЗЕЛ - 3 - 7600	VLAN 22
	10.255.22.11	HP OV	
	10.255.22.12	HP OV	(для IPMP)
	10.255.22.13	HP OV	(для IPMP)
	10.255.22.21	NFC	
	10.255.22.22	NFC	(для IPMP)
	10.255.22.23	NFC	(для IPMP)
	10.255.22.31	LMS	
	10.255.22.32	LMS	(для IPMP)
	10.255.22.33	LMS	(для IPMP)
	10.255.22.41	ACS	
	10.255.22.51	CAR	
	10.255.22.52	CAR	(для IPMP)
	10.255.22.53	CAR	(для IPMP)

3.3 Распределение VLAN

Согласно стандарту IEEE 802.1 VLAN ID могут быть назначены номера с 1 по 4094. Данный диапазон логически разделен на базовый под - диапазон (1 - 1005) и расширенный под - диапазон (1006 - 4094). Так же существуют номера VLAN зарезервированные под конкретные задачи (1002 - 1005 предназначены для организации VLAN Token Ring и FDDI). Для целей упрощения администрирования номерное пространство VLAN разбивается на отдельные диапазоны, каждый из которых имеет четкое предназначение.

Ниже подробно рассмотрено предназначение и распределение VLAN номеров каждого диапазона.

Распределение номеров VLAN по диапазонам приведено в таблице 3.6

Таблица 3.6 - Распределение номеров VLAN по диапазонам

VLAN IDs	Описание
1	Не используется
2 - 10	Для организации L2 доменов для пользователей PPPoE
11 - 20, 60, 70	Для организации сети управления магистралью IP/MPLS
21 - 22	Сервера системы управления, мониторинга и сбора статистики
101 - 1000	Для организации сервисных интерфейсов на SSG и серверах
1002 - 1005	Зарезервировано
2001 - 4000	Для организации пользовательских подключений в кольцах доступа
4001 - 4094	Для организации сети управления устройствами уровня доступа и SSG

4. СТРУКТУРА МАГИСТРАЛЬНОГО УРОВНЯ

4.1 Физическая топология

Физическая топология магистрального уровня представляет собой кольцо, образованное узлами УЗЕЛ - 2, УЗЕЛ - 1, УЗЕЛ - 7, УЗЕЛ - 3, УЗЕЛ - 6 и УЗЕЛ - 13, соединенными волоконно-оптическими линиями связи (ВОЛС), как показано на рис. 4.1. ВОЛС представляют собой одномодовые оптические волокна, соответствующие стандарту 0.652. Расстояния между пятью узлами не превышают 10 километров. Расстояние между узлами 6 и 13, составляет около 12 км. для прохождения указанного расстояния применяются оптические модули повышенной мощности. Для предохранения модулей от выжигания на данной линии используются аттенюаторы переменного значения.

4.2 Логическая топология

Логическая топология магистрального уровня представляет собой совокупность N-PE/P- устройств и PE- устройств, соединенных каналами связи как показано на рис. 4.2. Функции логических устройств N-PE/P, реализованы на маршрутизаторах Cisco 7609 (У-2-7600, У-1-7600, У-7-7600, У-3-7600, У-6-7600, У-13-7600). PE-устройствами являются маршрутизаторы Cisco 7206-VXR (У-7-GW, У-3-GW).

Каналы связи, соединяющие N-PE/P- устройства между собой, реализуются с использованием технологии виртуальных сетей 2-го уровня (VLAN - Virtual EAN), таким образом, что каждый канал связи представляет собой отдельный VLAN: VLAN- 11, VLAN- 12, VLAN- 13, VLAN- 14, VLAN- 15 и VLAN- 16 (рис. 4.2).

Данные VLAN реализуются на 10 Gigabit Ethernet линиях связи, соединяющих маршрутизаторы Cisco 7609.

Каналы связи, соединяющие PE-устройства с N-PE/P- устройствами, представляют собой линии связи Gigabit Ethernet.

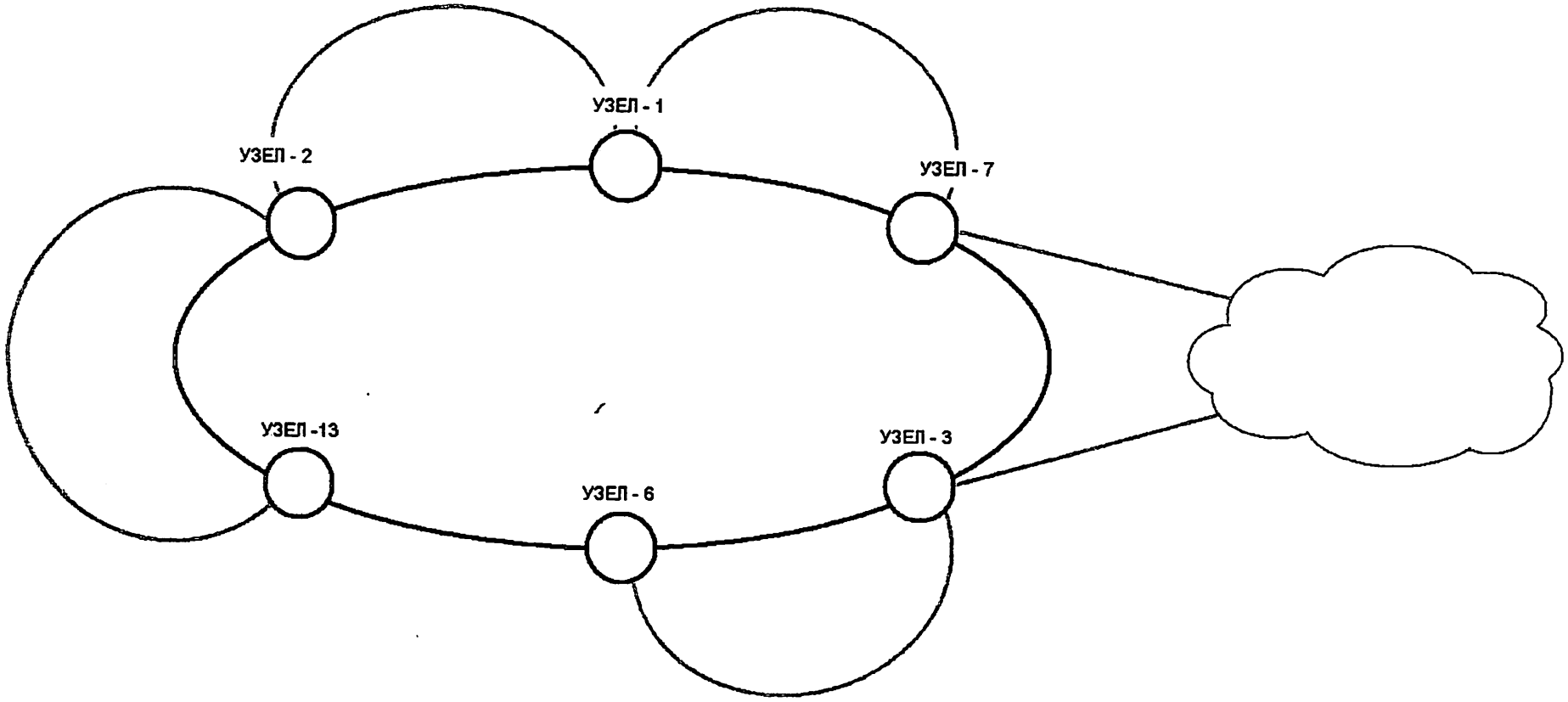


Рисунок 4.1 - Физическая топология магистрального уровня

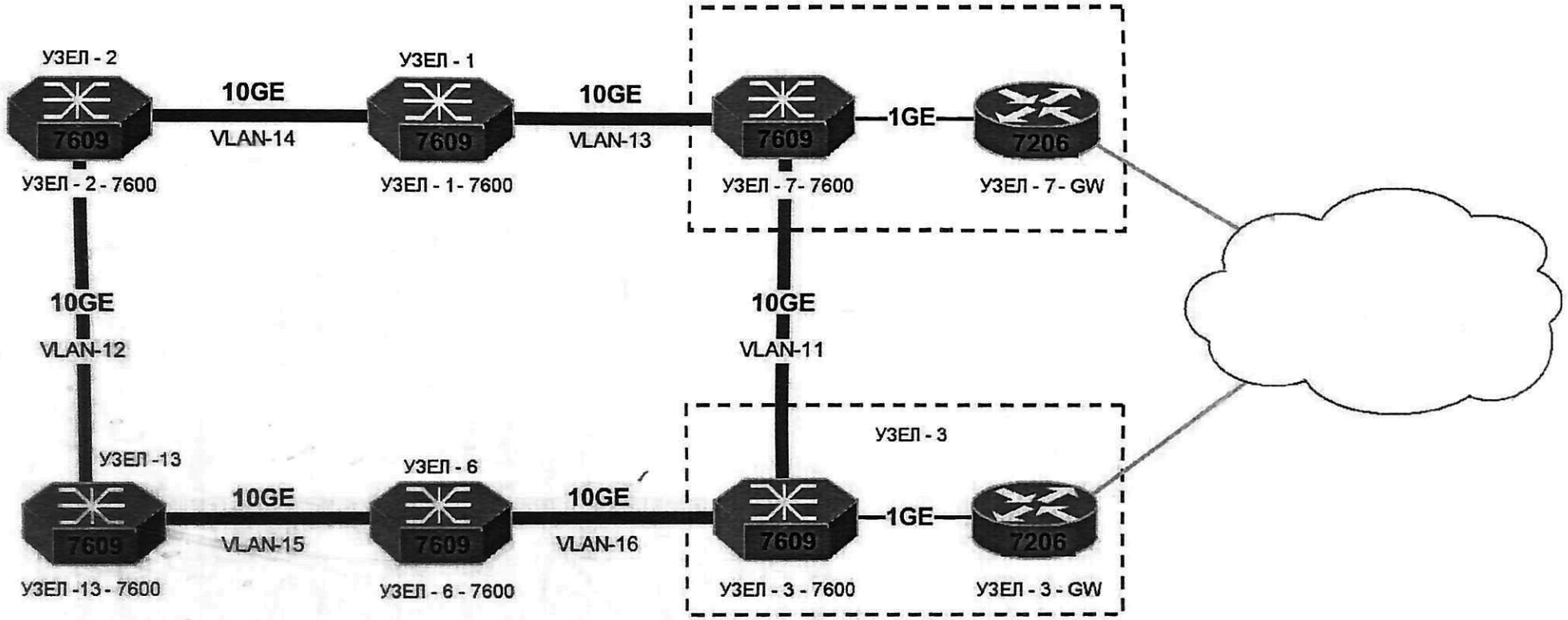


Рисунок 4.2 - Логическая топология магистрального уровня

4.3 Технология MPLS

На магистральном уровне используется технология MPLS(MultiPprotocol Label Switching). MPLS представляет собой технологию коммутации меток (Label) с установлением соединения (connection oriented).

LSR (Label Switching router) маршрутизаторы осуществляют коммутацию пакетов с использованием содержащихся в них меток. Совокупность соединенных между собой LSR-маршрутизаторов образуют MPLS-сеть. Существует два типа LSR: граничные LSR, называемые LER (Label Edge Router), и транзитные LSR или просто LSR. LER располагаются на границе MPLS-сети и соединяются как с LSR, так и с внешними устройствами, не поддерживающими MPLS-коммутацию. LSR осуществляют коммутацию только пакетов, содержащих метки.

Последовательность LSR-маршрутизаторов (от входного LER через транзитные LSR и до выходного LER), образуют LSP (Label Switching Path). В построении LSP участвуют все LSR маршрутизаторы LSR или только граничные LER маршрутизаторы В первом случае каждый LSR, включая входной LER, самостоятельно выбирает LSR для данного LSP. Во втором случае входной LER маршрутизатор принимает решение, через какие транзитные LSR-маршрутизаторы и выходной LER пройдет LSP.

В MPLS-технологии реализовано разделение функций построения LSP и функций передачи пакетов по LSP. Архитектура MPLS-устройства, реализующая разделение функций, состоит из двух компонент: компоненты выбора маршрута (Control Plane) и компоненты коммутации (Data Plane).

Компонент управления архитектуры MPLS(Control Plane) предназначен для предоставления компоненту коммутации (Data Plane) необходимой информации, используемой для коммутации пакетов.

В данном проекте на **Control Plane** реализуются функции:

- построения топологии сети с использованием топологической информации, полученной от соседних устройств (Routing Protocol);
- создание базы маршрутной информации (RIB - Routing Information Base) на основании топологии сети для:
- нахождения кратчайшего пути, в случае использования IP-маршрутизации для построения LSP;
- нахождения пути с учетом политик для построения LSP;
- построение таблицы привязки (Binding) MPLS-метки (LIB - Label Information Base):
- обмен binding-информацией с соседними MPLS-узлами для построения LSP.

Control Plane включает в себя:

- протоколы маршрутизации (Routing Protocols рис. 4.3);
- протоколы, реализующие функции внутридоменной маршрутизации IGP (Interior Gateway Protocol) OSPF, MP-BGP;

- протокол, реализующий функции междоменной маршрутизации EGP (Exterior Gateway Protocol) MP-BGP;

- протоколы распространения меток - LDP, RSVP, MP-BGP.

В данном проекте, протокол MP-BGP выполняет функции IGP-маршрутизации, EGP-маршрутизации и функции распространения меток.

4.3.1 Протоколы маршрутизации

Сеть Интернет состоит из взаимосвязанных автономных систем (AS). В свою очередь, автономная система состоит из сетей, находящихся под единым административным управлением, использующих согласованную IP-адресацию и единую политику взаимодействия с внешними AS. Соответственно, различаются задачи поиска маршрута к IP-сетям внутри AS (intra-AS Routing) и к IP-сетям, находящимся в других AS (inter-AS Routing). Intra AS маршрутизация, называемая также внутридоменной маршрутизацией, реализуется с помощью одного или нескольких протоколов маршрутизации под общим названием IGP (Interior Gateway Protocol). Соответственно, inter-AS маршрутизация, называемая также междоменной маршрутизацией, реализуется с помощью протоколов маршрутизации под общим названием EGP (Exterior Gateway Protocol).

4.3.1.1 Внутридоменная маршрутизация

Протоколы внутридоменной маршрутизации предназначены для нахождения кратчайшего, без образования замкнутых участков (петель), маршрута к IP-сетям внутри автономной системы Metro Ethernet сети.

В данном проекте IGP-маршрутизация реализует функции:

- выбора кратчайшего, беспетлевого маршрута к инфраструктурным IP-сетям;
- выбора маршрута с учетом политик;
- обмена маршрутами внутри VPN через MPLS-сеть.

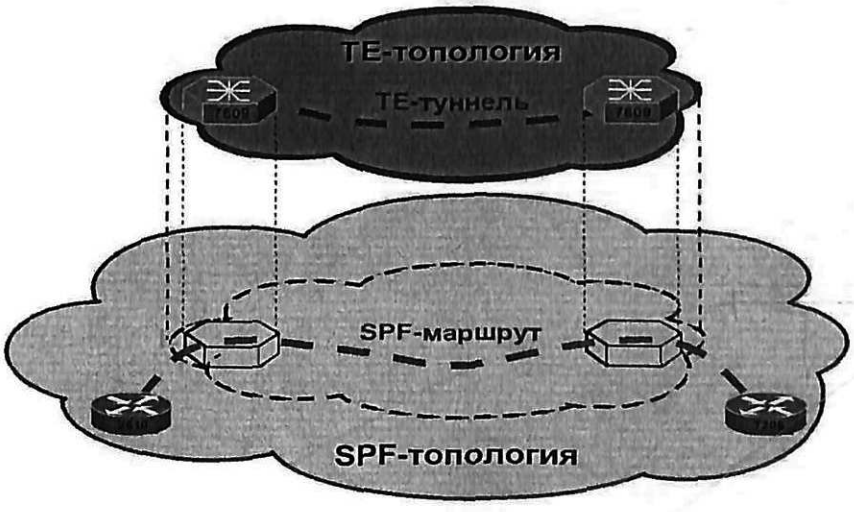
В данном проекте реализуется совместное использование протоколов OSPF и MP-BGP.

Протокол OSPF с TE-расширениями формирует две топологические базы данных:

- SPF-топологию, для построения кратчайшего пути с использованием OSPF-метрик;
- TE-топологию, для построения кратчайшего пути с учетом политик.

Маршрутизаторы Metro Ethernet сети, использующие OSPF-протокол, образуют OSPF-домен. Маршрутизаторы OSPF-домена состоят из устройств (TE-устройств), поддерживающих TE-расширения, и устройств, не поддерживающих TE-расширений (SPF-устройства). TE-устройства содержат TE-топологию и SPF-топологию, тогда как SPF-устройства содержат только SPF-топологию. Таким образом, TE-устройства участвуют и в построении TE-маршрутов (TE-туннелей) и в построении SPF-маршрутов, тогда как SPF-устройства строят только SPF-маршруты (рис. 4.3). OSPF-домен реализуется в виде одной Area0 с учетом небольшого количества используемых маршрутизаторов и сетей. Логическая схема OSPF-домена представлена на рис. 4.4.

Рисунок 4.3 - TE- и SPF-топологии OSPF домена



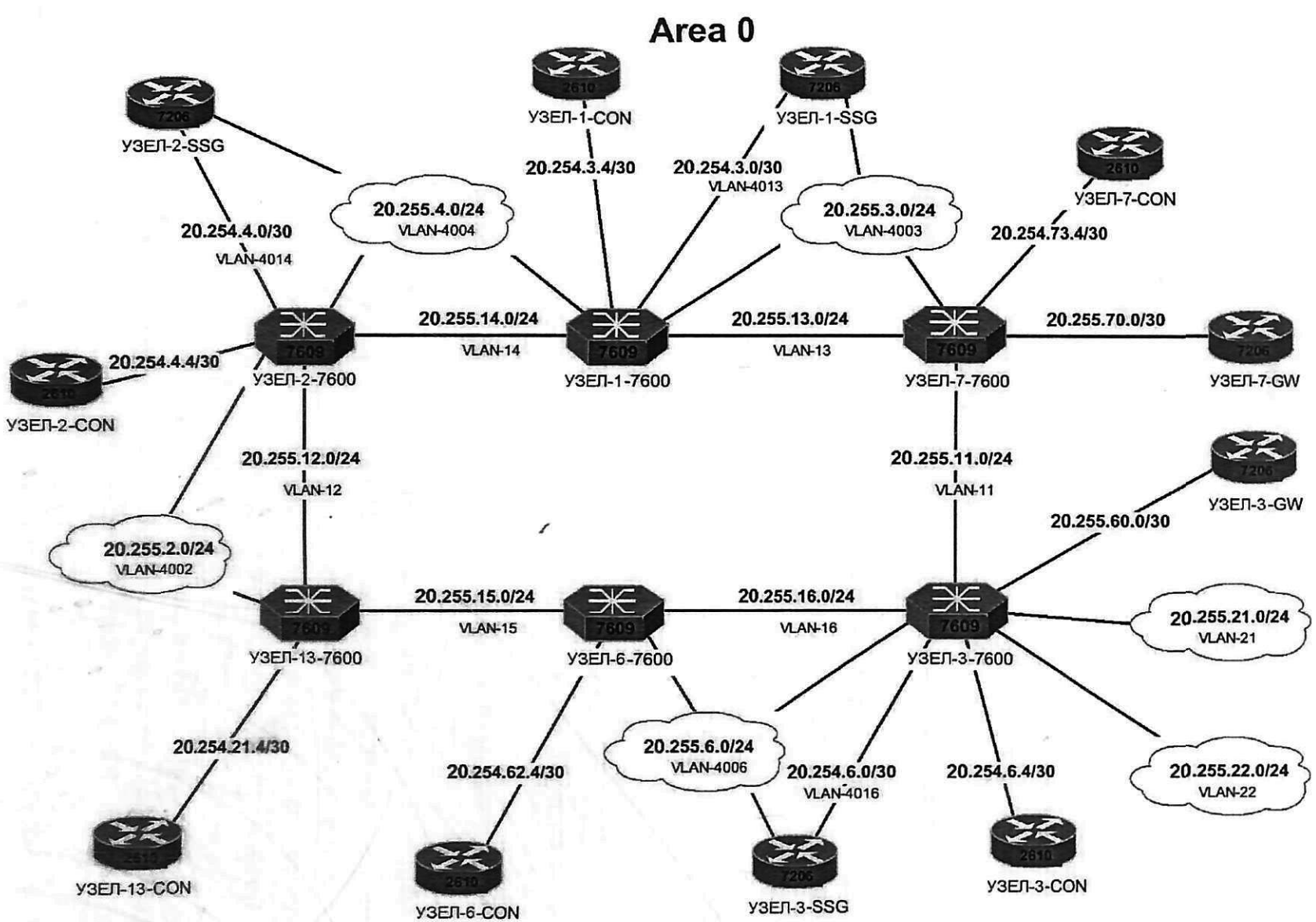


Рисунок 4.4 - Логическая схема OSPF-домена

В качестве Router ID для SPF-топологии и для TE-топологии используется IP-адрес Loopback0-интерфейса маршрутизаторов (таблица 3.2). Router ID для SPF-топологии и TE-топологии задается следующими командами соответственно:

(config-router)# **router-id A.B.C.D**

(config-router)# **mpls traffic-eng router-id Loopback0**

Для того чтобы исключить включение клиентских маршрутизаторов в OSPF-домен:

- изначально все интерфейсы переводятся в пассивное состояние, а именно, на всех

интерфейсах запрещается обмен OSPF-сообщениями с использованием команды

(config-router)# **passive interface default**;

- интерфейсы, подключенные к IP-подсетям, показанным на рис. 4.5, за исключением интерфейсов узла-3-7600, подключенных к сетям центра управления 10.255.21.0/24 и 10.255.22.0/24, переводятся в активное состояние явным образом с использованием команды (config-router)# **no passive interface** *название_интер фейса;*

- каждый активный интерфейс назначается в Area 0 отдельно с использованием маски минимальной длины 0 (0.0.0.0), позволяющей идентифицировать только один IP-адрес

(config-router)# **network A.B.C.D 0.0.0.0 area 0**;

- для аутентификации OSPF-маршрутизаторов Metro Ethernet сети используется MD5 хэш-функция с помощью команд: (config-router)# **area 0 authentication message-digest**;

(config-router)# **ip ospf message-digest-key 1 md5 ME-CISCO**.

Для уменьшения времени восстановления Metro Ethernet сети выполняется следующее:

- осуществляется уменьшение топологических базы данных путём настройки режима

point-to-point на интерфейсах VLAN и Gigabit Ethernet, соединяющих соседние маршрутизаторы между собой (каналы связи между маршрутизаторами на рис. 4.5) при помощи команды (config-router)# **ip ospf network point-to-point;**

- используется инкрементальный алгоритм вычисления кратчайшего маршрута, пересчитывающий только маршруты, ставшие недействительными в результате изменения топологии - команда (config-router)# **ispf;**

- уменьшение времени обнаружения изменения топологии: на 10Gigabit Ethernet-интерфейсах и Gigabit Ethernet-интерфейсах, соединяющих

УЗЕЛ-7-7600 с УЗЕЛ-7-GW и УЗЕЛ-3-7600 с УЗЕЛ-3- GW, до одной секунды при помощи команды

(config-router)# **ip ospf dead-interval minimal hello-multiplier 4;**

задающей интервал hello-interval, равный 250 миллисекунд и dead-interval равный 1 секунде;
на остальных интерфейсах до 4-х секунд с использованием команды

(config-router)# **ip ospf hello-inteval 1**

(dead-interval равный четырем hello-interval - значение по умолчанию).

По умолчанию, метрика каждого интерфейса (cost) вычисляется как отношение эталонного значения полосы пропускания, равного 100 Мбит/сек, к полосе пропускания интерфейса с округлением до большего целого значения, что приводит к равенству метрик (cost = 1) интерфейсов 10Gigabit Ethernet (10000 Мбит/сек) и Gigabit Ethernet (1000 Мбит/сек) и некорректному построению SPF-маршрута.

Для получения корректных метрик на интерфейсах с разной полосой пропускания, эталонное значение полосы пропускания задается равной полосе пропускания 10Gigabit Ethernet-интерфейса при помощи команды

(config-router)# **auto-cost reference-bandwidth 10000**

На ТЕ-устройствах (Cisco 7609, рис. 4.4) конфигурирование Area0 для поддержки ТЕ осуществляется командой

(config-router)# **mpls traffic-eng area 0.**

Пример настройки OSPF на маршрутизаторе УЗЕЛ-3-7600 для интерфейса Gigabit Ethernet 7/1 приведен на рис. 4.5.

```
hostname УЗЕЛ-3-7600
...
interface Loopback0
 ip address 20.255.1.6 255.255.255.255
...
interface GigabitEthernet7/1
 description <<<<<<<<<<To-УЗЕЛ-3-GW>>>>>>>>>>>>>>
 ip address 20.255.60.1 255.255.255.252
 ip ospf message-digest-key 1 md5 ME-CISCO
 ip ospf dead-interval minimal hello-multiplier 4
...
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 router-id 20.255.1.6
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 redistribute connected subnets route-map CONN_NETS
 ip ospf network point-to-point
 passive-interface default
 no passive-interface GigabitEthernet7/1
 network 20.255.60.1 0.0.0.0 area 0
 ...
access-list 10 permit 20.255.21.0
access-list 10 permit 20.255.22.0
access-list 10 remark ---------NOC_subnetsnets----------
...
route-map CONN_NETS permit 10
 match ip address 10
```

Рисунок 4.5 - Пример настройки OSPF на маршрутизаторе УЗЕЛ-3-7600 для интерфейса Gigabit Ethernet 7/1

4.3.1.2 Внутридоменная маршрутизация

В качестве протокола междоменной маршрутизации используется протокол MP-BGP (MultiProtocol Border Gateway Protocol). Обмен маршрутной информацией с другими AS осуществляется через MP-eBGP сессии. AS Metro Ethernet сети г.Алматы (Рис. 4.6) связана с AS провайдера и с АЫ VPN-клиентов, в случае использования ими протокола BGP при подключении к MPLS-сети.

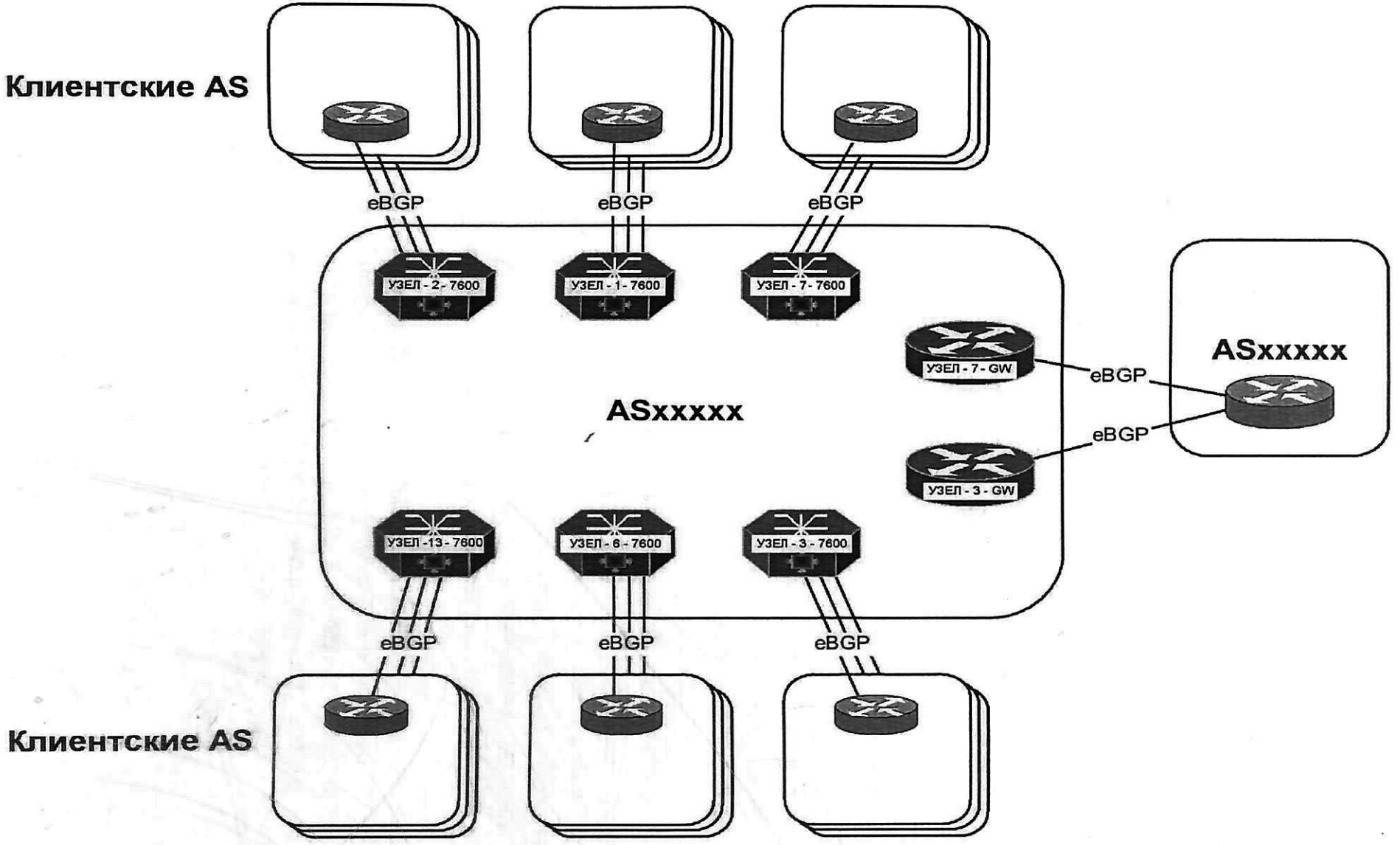


Рисунок 4.6 - Связь с внешними автономными системами

5. СТРУКТУРА УРОВНЯ ДОСТУПА

5.1 Физическая топология

Уровень доступа состоит из коммутаторов Cisco Catalyst 3750 Metro серии, которые цепочкой соединяются между собой и двумя устройствами Cisco7906 магистрального кольца. Таким образом, образуется кольцевая топология, позволяющая обеспечить резервирование уровня доступа. К уровню доступа относится маршрутизаторы Cisco7206VXR [7], подключаемые к Cisco7906, и сервера аутентификации и авторизации пользователей – Cisco Access Registrar (CAR) и сервера выбора услуг – Cisco Subscriber Edge Services Manager (SESM), которые устанавливаются в центре управления системы. Функциональная схема уровня доступа представлена на рис. 5.1.

Основными функциями уровня доступа являются:

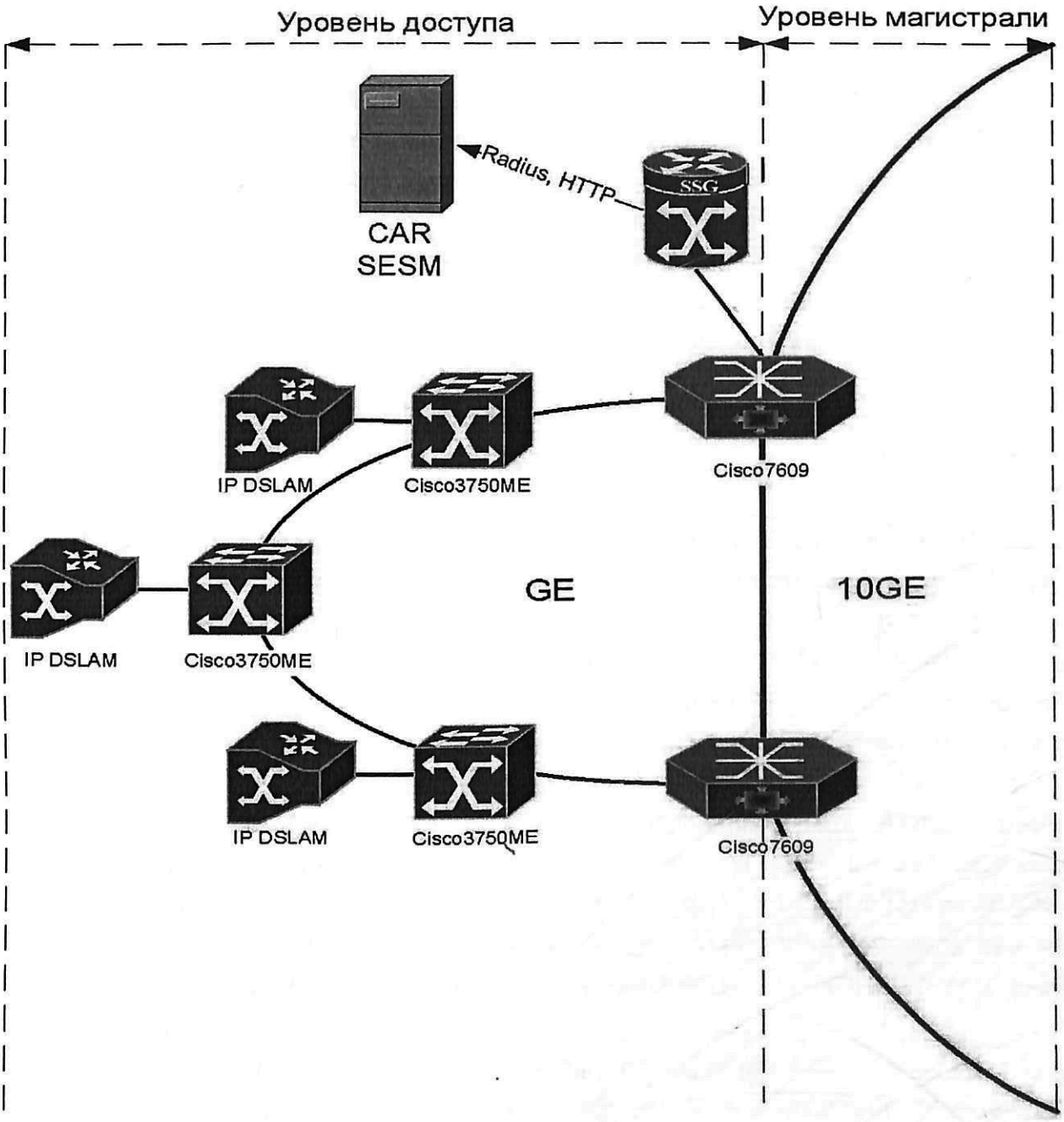
- организация Ethernet доступа к MPLS магистрали;
- терминация PPPoE трафика клиентов;
- предоставление возможности выбора услуг SSG;
- выполнение трансляции IP адресов – NAT.

Catalyst 3750 Metro Ethernet - Ethernet коммутатор, который обеспечивает доступ второго уровня к узлам магистрального уровня и маршрутизатору Cisco7206. Коммутатор используется как для подключения конечных пользователей, так и для подключения IP DSLAM-ов (для организации xDSL доступа).

Маршрутизатор Cisco 7206 обеспечивает подключение PPPoE клиентов с использованием технологии доступа xDSL (Подробнее данный способ подключения описан в следующей главе). Программное обеспечение Service Selection Gateway (SSG) предоставляет пользователю возможность выбора сервиса (услуги операторов) и подключение пользователя к выбранному сервису. Функции аутентификации, авторизации, сбора статистики, осуществляются SSG совместно с SESM и CAR.

Cisco Subscriber Edge Services Manager (SESM) - сервер выбора услуг (сервисов), который представляет собой специализированный WWW сервер, работающий на платформе Sun SPARC Solaris, и взаимодействующий с SSG и CAR. SESM предоставляет абоненту сети WWW интерфейс для выбора сервисов при подключении к сети передачи данных.

Cisco Access Registrar (CAR) – RADIUS-сервер непосредственно обеспечивает аутентификацию, авторизацию и аккаунтинг пользователей. CAR представляет собой программный продукт CISCO Systems, работающий на платформе Sun



SPARC.

Рисунок 5.1 - Функциональная схема уровня доступа

5.1.1 xDSL-доступ

5.1.1.1 RFC 1483

Данный способ подключения клиентского оборудования к сети основывается на рекомендации RFC 1483. Согласно пункту 4.1 RFC 1483, сначала IP пакет

инкапсулируется в LLC/SNAP (Logical Link Control / SubNetwork Attachment Point) фрейм путем добавления к IP пакету восьми байт. Затем в соответствии с форматом AAL5 ATM форума, полученный фрейм сегментируется в ATM ячейки (ce11s) и передаётся по ADSL/ATM соединению от клиентского оборудования до IP DSLA-ма. IP DSLAM производит сборку IP пакета из AAL5 ATM ячеек, добавляет заголовок 802.1 и коммутирует до маршрутизатора магистрального уровня Cisco7609. Стек протоколов данного типа подключения показан на рис. 5.2.

Рисунок 5.2 - Стек протоколов при подключении по рекомендации RFC 1483

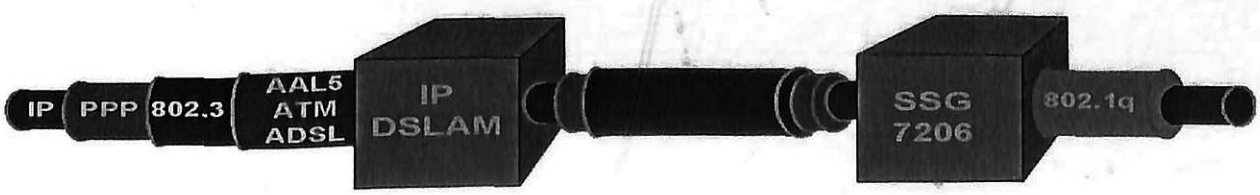
Этот способ подключения применяться в основном для корпоративных пользователей и может рассматриваться как аналог или замена выделенной линии при использовании технологии ADSL. Особенностями данного способа подключения является необходимость в использовании постоянного IP адреса, а также терминирование VLAN на Cisco7609 в определенный заранее IP VPN VRF для пользователя см. рис. 5.4.

5.1.1.2 PPPoE

Подключение пользователей по технологии PPP over Ethernet (PPPoE) является одним из основных методов подключения домашних пользователей к СПД. Данный метод подключения для своей работы требует наличия программного продукта на персональном компьютере клиента - PPPoE клиент. Метод основывается на рекомендации RFC2516 и состоит в том, что IP пакеты инкапсулируются в PPP фреймы, PPP инкапсулируются в Ethernet фреймы, Ethernet фреймы согласно рекомендации RFC1483 инкапсулируются в формат ATM AAL5, а затем сегментируются в ATM ячейки, которые передаются по ADLS линии от пользовательского оборудования через DSLAM к устройству агрегирования - Cisco7206VXR. Cisco7206VXR собирает PPP фреймы, затем извлекает IP пакет и маршрутизирует их. При этом пользовательское ADSL оборудование выполняет роль обыкновенного Ethernet -bridge, осуществляющего передачу Ethernet фреймов по ADSL линии.

Наличие протокола PPP (RFC1331) предусматривает использование в данном способе подключения сервера аутентификации и авторизации пользователя - CiscoAccess Registrar (CAR) и SSO/SESM. Стек протоколов для данного типа подключения показаны на рис. 5.3.

Рисунок 5.3 - Стек протоколов при подключении по протоколу PPPoE



Преимущество данного метода по сравнению с предыдущим состоит в том что, используя обычный Ethernet коммутатор, по одной ADSL линии можно подключать сразу несколько пользователей клиентов к сети, а аутентификацию, авторизацию и учёт использованных ресурсов можно вести для каждого пользователя в отдельности.

Использование данного метода позволяет значительно упростить управление и настройку пользовательского оборудования, так как любой применяемый ADSL модем должен быть настроен только для выполнения функций Ethernet-bridge, все остальные настройки выполняются на персональном компьютере клиента. Данный способ не требует постоянного IP адреса для подключения пользовательского оборудования, который будет назначаться в момент установления PPP соединения. В отличие от предыдущего способа.

5.2 Шлюз выбора информационных услуг

Шлюз выбора услуг SESM/SSG - комплекс программно-аппаратных средств, который позволяет ADSL пользователям, использующих в качестве доступа протокол PPPoE, возможность выбирать услуги: доступ в сеть Интернет, корпоративная сеть и другие сервисы через WWW браузер. Смена услуги или провайдера не требует переустановления соединения и процессов авторизации, аутентификации пользователя. Указанный комплекс реализуется на следующем оборудовании и программном обеспечении: Service Selection Gateway (SSG), Cisco Subscriber Edge Service Manager (SESM) и Cisco Access Registrar (CAR) см. рис. 5.4-5.7.

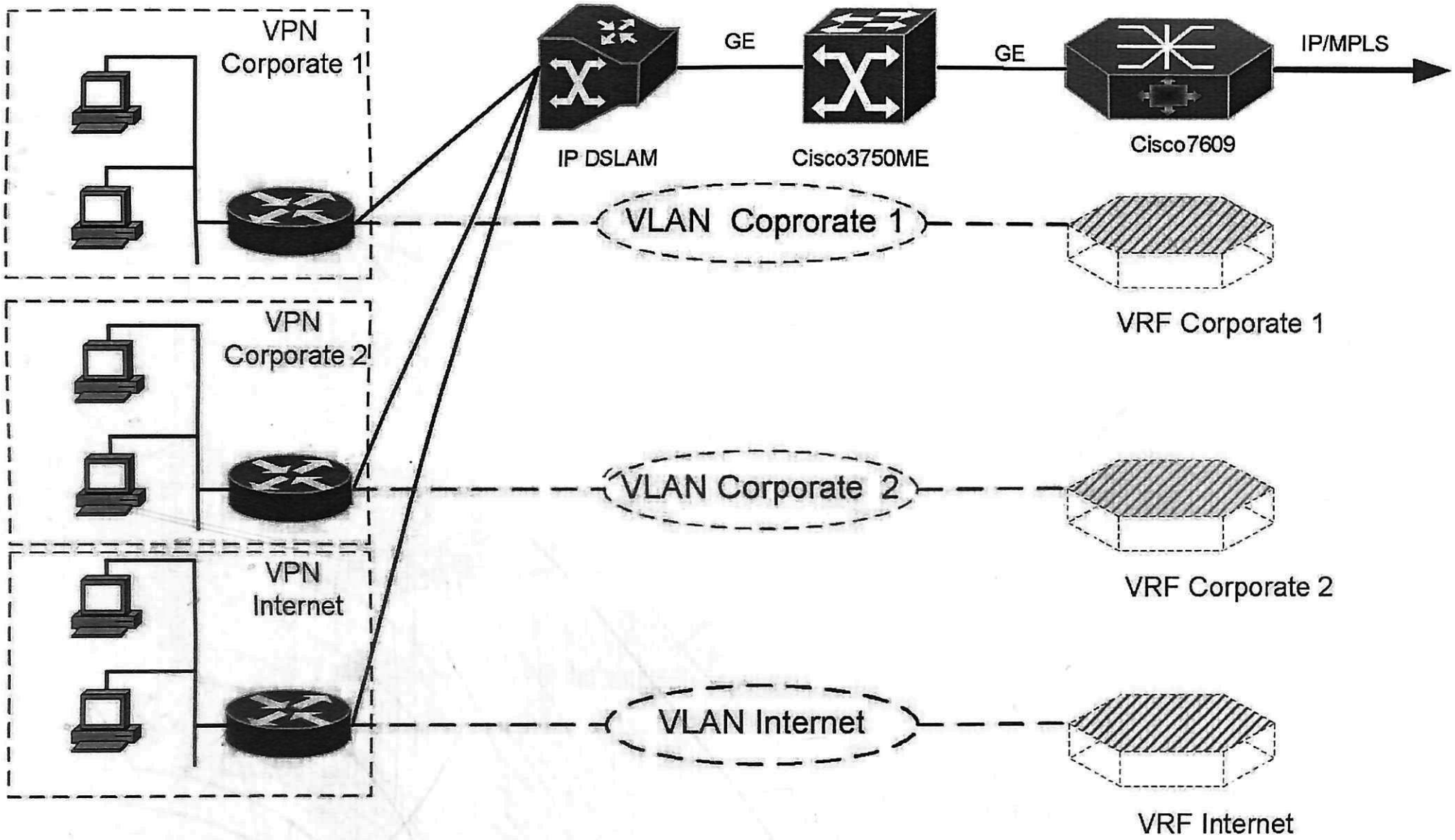


Рисунок 5.4 - Логическая схема подключения по рекомендации RFC 1483

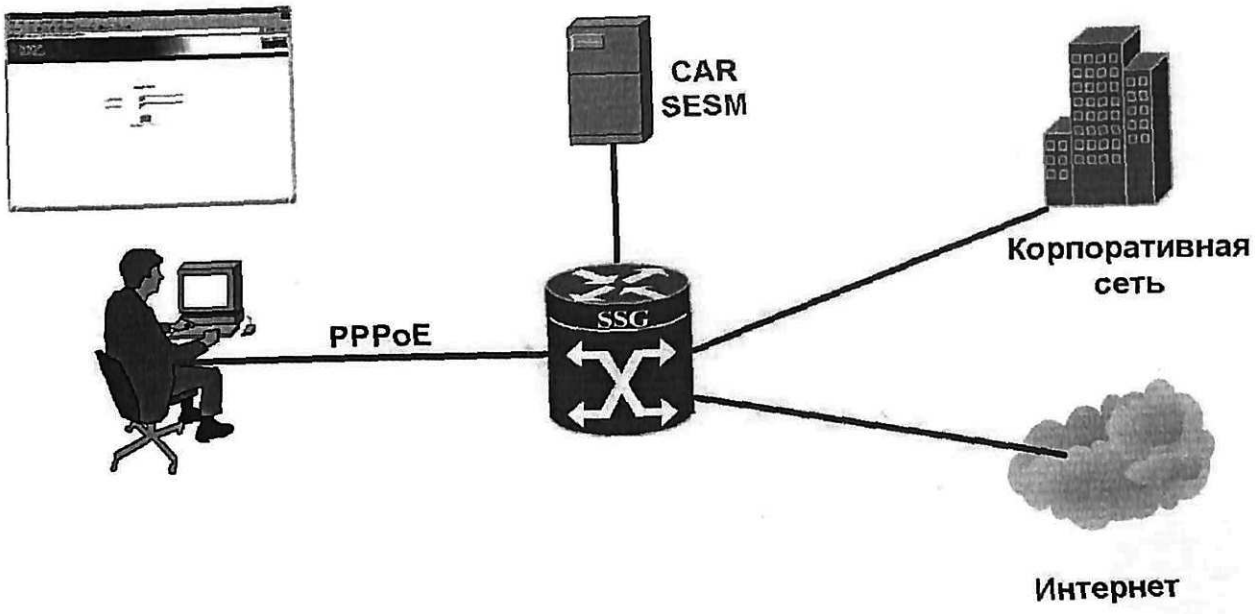


Рисунок 5.5 - Комплекс SSG/SESM

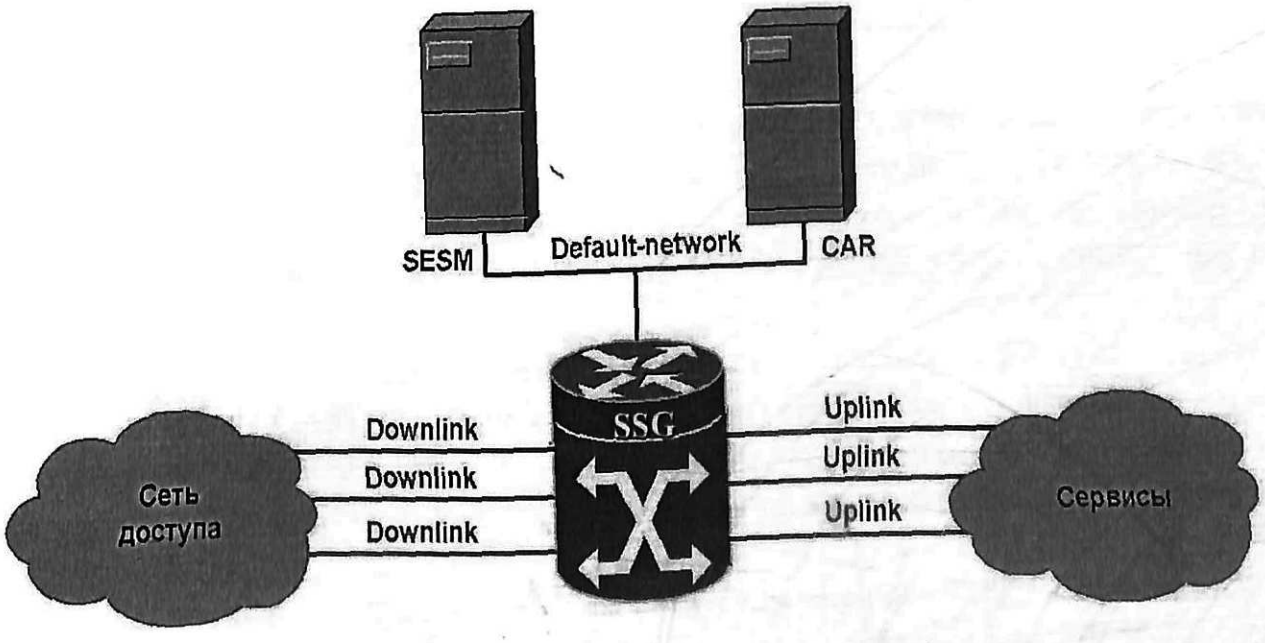


Рисунок 5.6 - Топология включения SESM/SSG

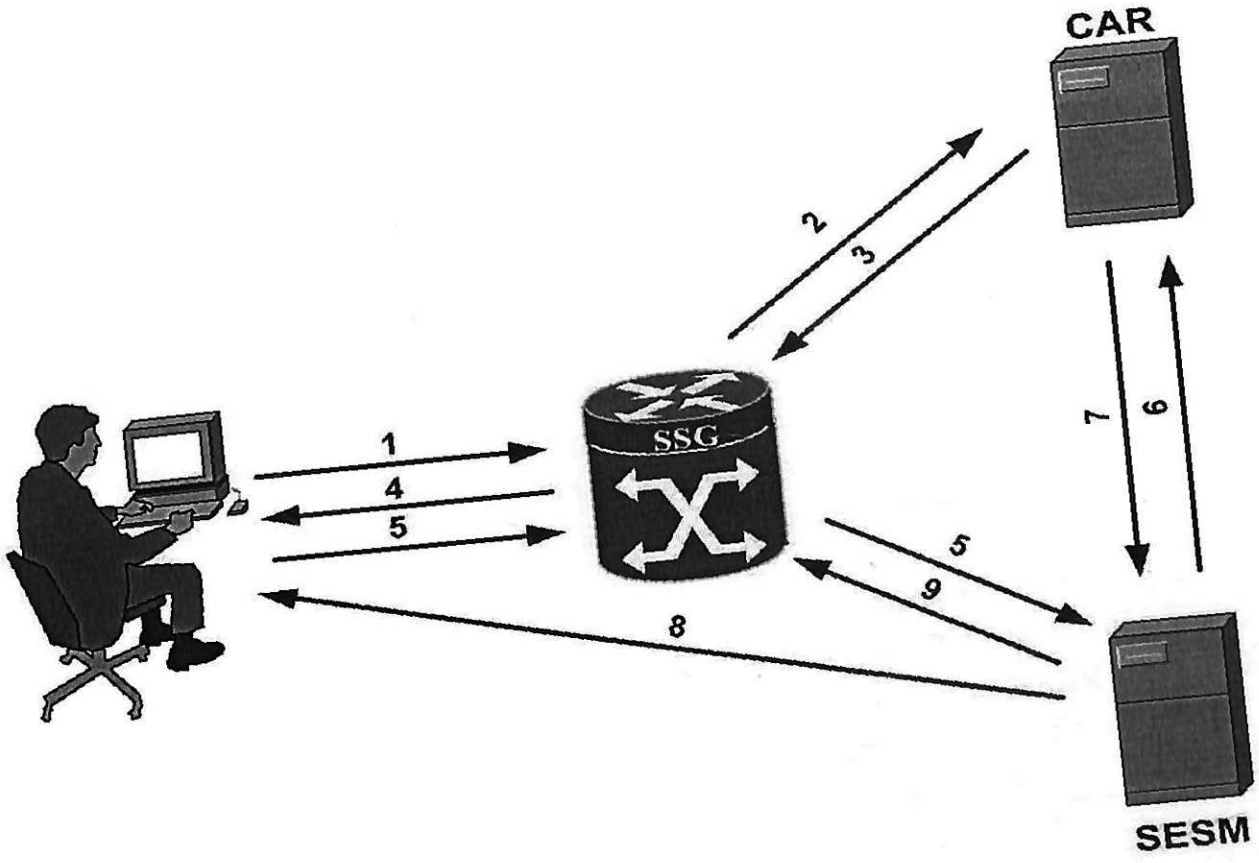


Рисунок 5.7 - Схема работы SESM/SSG

После установления PPP соединения, пользователю необходимо активировать необходимые сервисы на WEB портале SESM. Пользователь, по средствам WEB браузера, вводит специально определенный URL для сервера SESM. Так как сервер DNS находится в сети Internet, WEB браузер не имеет возможности определить IP адрес SESM.

Для решения данной задачи используется специальный тип сервиса называемый OPEN GARDEN. Данный сервис доступен для всех пользователей и не требует какой либо активации. В этот сервис включен сегмент сети, в котором располагается сервер DNS. Профиль для этого сервиса хранится непосредственно на SSG.

Как упоминалось ранее, пользователь может активировать одну или несколько услуг (сервисов) из числа доступных для данного пользователя. В SSG/SESM определены три основных типа услуг.

Pass-Through - направление движения трафика происходит с использованием стандартной таблицы маршрутизации. Этот тип сервиса применяется для стандартного использования доступа к Internet и других сервисов не требующих дополнительной аутентификации и установления L2TP туннелей.

Tunnel - SSG является LAC и инициирует соединение по Layer 2 Tunneling Protocol (L2TP) к удаленному L2TP серверу (LNS). Между IP адресом пользователя и адресом, назначенным LNS автоматически, включается NAT.

Proxy - соединение с услугой такого типа требует дополнительной аутентификации на удаленном AAA сервере. Если в процессе авторизации пользователю выделяется IP адрес, то между IP адресом пользователя и адресом, выделенным AAA сервером, автоматически включается NAT.

В SSG/SESM определены два основных режима доступа к услугам.

Concurrent mode -позволяет пользователям использовать одни услуги, не разрывая соединения с другими. Такой режим наиболее подходит для сервисов не требующих дополнительной аутентификации и установления L2TP туннелей такой как доступ в сеть Интернет.

Sequential mode -доступ требует, чтобы пользователь отключился от всех услуг, перед соединением с этой услугой. данный режим идеален для услуг, для которых важна безопасность, т.е. таких как доступ к корпоративным сетям, или для исключения возможности перекрывающегося адресного пространства.

Помимо информации о типе и режиме услуги, в описании сервиса необходимо указать сети, которые будут доступны после выбора сервиса. Так же, значение DNS доменов и IP адреса DNS серверов, которые будут использоваться, когда пользователь выберет данный сервис.

Для описания пользователей и сервисов используются стандартные атрибуты, определяемые RADIUS протоколом. Взаимодействие с SSG/SESM требует введения дополнительных атрибутов: **Cisco-SSG-Account-Info, Cisco- SSG- Service-Info, Cisco-Avpair и Cisco-SSG-Control-Info**. Эти атрибуты определены компании Cisco и имеют следующие идентификаторы (ID) в RADIUS протоколе:

Attribut ID	Vendor ID	Sub. Attribut ID	Название	Тип
26	9	250	Cisco-SSG-Account-Info	Строка
26	9	251	Cisco-SSG-Service-Info	Строка
26	9	1	Cisco-Avpair	Строка
26	9	253	Cisco-SSG-Control-Info	Строка

5.2.1 Конфигурация SSG

Настройка 6 включает в себя следующие основные этапы:

- Запуск SSG процесса и настройка основных параметров;
- Настройка взаимодействия с SEMS;
- Настройка взаимодействия с CAR.

К основным настройкам SSG (на примере УЗЕЛ-1-SSG) относится следующие команды:

Команда **ssg enable** запускает процесс SSG. После установления PPP

```
ssg enable
ssg default-network 20.255.21.21 255.255.255.255
ssg service-password servalme
ssg port-map enable
ssg port-map destination range 80 to 80 ip 20.255.21.21
ssg port-map source ip Loopback0
ssg bind service Corporate_VPN 20.254.3.1
ssg bind service Internet x.x.x.x
ssg bind direction uplink GigabitEthernet 0/1.4003
ssg bind direction uplink GigabitEthernet 0/2.101
ssg bind direction downlink Virtual-Template1
ssg open-garden OG_DNS
ssg service-search-order local remote
```

соединения, пользователь получает доступ только к сегменту сети, в котором расположен SESM. Данный сегмент описывается командой **default-network**. Для обеспечения функциональности Port-Bundle Host Key необходимо запусти процесс командой **ssg port-map enable**, определить диапазон TCP портов и IP адрес SESM командой **ssg port-map destination** и определить адрес SSG на который будет меняться IP адрес пользователя - **ssg port-map source ip**.

Все интерфейсы, по которым возможен заход пользователей, должны быть описаны Downlink - **ssg bind direction downlink.** Интерфейсы, приписанные к 6 сервисам должны быть описаны как Uplink - **ssg bind direction uplink**. Для каждого сервиса необходимо определить адрес следующего маршрутизатора, через который будет доступен данный сервис – **ssg bind service**. Команда **ssg open garden** определяет, что сервис OG_DNS является сервисом типа OPEN GARDEN. Для SSG необходимо определить последовательность в которой будет осуществляться поиск профилей для сервисов, так как профиль для OG_DNS хранится локально, начальный поиск необходимо осуществлять непосредственно на SSG.

Для взаимодействия SSG с SESM необходимо настроить номера TCP портов и ключ для приема RADIUS запросов.

Описание профиля для Open Garden сервиса доступа к ЕЯ осуществляется следующими командами:

Где **X.X.X.X** - IP адрес DNS сервера.

Конфигурация для аутентификации и авторизации пользователей с использованием CAR осуществляется следующими командами.

```
aaa new-model
aaa authentication ppp PPPoE_USERS group radius
aaa authorization network PPPoE_USERS group radius
aaa accounting network PPPoE_USERS start-stop group radius
radius-server host 20.255.22.51 auth-port 1645 acct-port 1646
radius-server key radiusALME
radius-server vsa send accounting
radius-server vsa send authentication
```

aaa new-model - использовать AAA модель при аутентификации и авторизации пользователей.

aaa authentication ppp PPPoE_USERS group radius - выполнять аутентификацию PPP пользователей на CAR

aaa authorization network PPPoE_USERS group radius - CAP разрешено определять сетевые ресурсы PPP соединений.

aaa accounting network PPPoE_USERS start-stop group radius - посылать уведомления об открытии и закрытии соединений на CAR.

radius-server host 10.255.22.51 auth-port 1645 acct-port 1646 IP адрес и порты аутентификации и чета CAR.

radius-server key radiusALME - ключ для доступа к CAR серверу.

radius-server vsa send accounting - разрешить посылать специальные атрибуты Cisco для учета трафика.

radius-server vsa send authentication - разрешить посылать специальные атрибуты Cisco для аутентификации пользователей.

5.2.2 Конфигурация CAR

На начальном этапе для PPPoE пользователей будет доступно две услуги. Это доступ в сеть Интернет и доступ в корпоративную сеть по средствам установления L2TP туннеля до сервера доступа некой организации.

С начало необходимо завести пользователя на CAR с указанием доступных для него сервисов. Ниже приведен пример пользователя 111 для которого доступно два сервиса.

```
[ 111 ]
   Name = 111                                  Имя пользователя
   Description =
   Password = <encrypted>
   Enabled = TRUE
   Group~ =
   BaseProfile~ = ssg-user                     Имя профиля пользователя
   AuthenticationScript~ =
   AuthorizationScript~ =
   UserDefined1 =
   AllowNullPassword = FALSE
   Attributes/
   CheckItems

Name = ssg-user                                Имя профиля пользователя
   Description =
   Attributes/
   Cisco-SSG-Account-Info = NInternet          Доступный сервис
   Cisco-SSG-Account-Info = NCorporate_VPN     Доступный сервис
   Framed-Protocol = PPP                       Данный профиль для PPP
   Service-Type = Framed                       пользователя
```

Ниже приведен пример описания сервиса, при выборе которого пользователь получает доступ в сеть Интернет.

[Internet]	
Name = Internet	*Имя сервиса*
Description =	
Password = <encrypted>	
Enabled = TRUE	
Group~ =	
BaseProfile~ = Internet-profile	*Имя профиля сервиса*
AuthenticationScript~ =	
AuthorizationScript~ =	
UserDefined1 =	
AllowNullPassword = FALSE	
Attributes/	
CheckItems/	
Name = Internet	*Имя профиля сервиса*
Description =	
Attributes/	
Cisco-SSG-Service-Info = IInternet	*Имя сервиса*
Cisco-SSG-Service-Info = MC	*Сервис может быть выбран одновременно с другим*
Cisco-SSG-Service-Info = TP	*Сервис не требует дополнительной аутентификации*
Cisco-SSG-Service-Info = R0.0.0.0;0.0.0.0	*Сети которые будут доступны после выбора данного сервиса*
Service-Type = Outbound	*Указывает на то. что данный*

Следующий пример описывает сервис после выбора которого устанавливается L2TP туннель до удаленного сервера.

```
[ Corporate_VPN ]                                          Имя сервиса
  Name = Corporate_VPN
  Description =
  Password = <encrypted>
  Enabled = TRUE
  Group~ =
  BaseProfile~ = Corporate_VPN-profile                     Имя профиля сервиса
  AuthenticationScript~ =
  AuthorizationScript~ =
  UserDefined1 =
  AllowNullPassword = FALSE
  Attributes/
  CheckItems/

  Name = VPDN                                              Имя профиля сервиса
  Description =
  Attributes/
  Cisco-AVpair = vpdn:tunnel-id=VPDN                       Идентификатор туннеля
  Cisco-AVpair = vpdn:tunnel-type=l2tp                     Тип туннеля
  Cisco-AVpair = vpdn:ip-addresses=X.X.X.X                 IP адрес  удаленного
                                                           сервера доступа
  Cisco-AVpair = vpdn:l2tp-tunnel-password=Cisco           Пароль для установки туннеля
  Cisco-SSG-Service-Info = IVPDN                           Имя сервиса
  Cisco-SSG-Service-Info = R0.0.0.0;0.0.0.0                Сети которые  будут
                                                           доступны после выбора
                                                           данного сервиса
  Cisco-SSG-Service-Info = TT                              Тип сервиса- туннель

  Cisco-SSG-Service-Info = MS                              Сервис не может быть
                                                           выбран одновременно с другим
```

5.2.3 Конфигурация SESM

Конфигурация web портала SESM расположена в xml файле nwsp.xml. К основным настройкам относится следующие части данного файла: параметры взаимодействия SESM с SSG, настройка функциональности Port-Bundle Host Key, параметры взаимодействия SESM с CAR.

Для настройки взаимодействия с SSG необходимо настроить:

- номер порта для обмена RADIUS пакетами с SSG. Данный параметр должен совпадать с

установленным на SSG;

- максимальное время ожидания ответа;
- количество повторных запросов;
- ключ для доступа к SSG. Данный параметр должен совпадать с установленным на SSG.

```
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1645</Arg></Call>
<Call name="setGlobalAttribute"><Arg>TIMEOUTSECS</Arg><Arg>10</Arg></Call>
<Call name="setGlobalAttribute"><Arg>RETRIES</Arg><Arg>3</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>THROTTLE</Arg><Arg>20</Arg></Call>
```

Для настройки функциональности Port-Bundle Host Key необходимо указать параметр BUNDLE_LENGHT. Значение параметра должно совпадать с

```
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
```

установленным на SSG.

Для аутентификации пользователей и на web портале и получения профилей сервисов на CAR необходимо настроить RADIUS клиента на Необходимо настроить следующие параметры:

- IP адрес CAR;
- номер порта;
- ключ для доступа к CAR;
- пароль, используемый для запроса информации о сервисе.

Так как RADIUS сервер не резервируется, значения параметров для первичного и вторичного сервера устанавливаются одинаковые.

```
<Configure jmxname="com.cisco.sesm:name=AAA,connection=ServiceProfile">
  <Set name="throttle" type="int">256</Set>
  <Set name="timeOut" type="int">4000</Set>
  <Set name="maxRetries" type="int">3</Set>
  <Set name="primaryIP">20.0.28.200</Set>
  <Set name="primaryPort" type="int">1645</Set>
  <Set name="secret">cisco</Set>
  <Set name="secondaryIP">20.0.28.200</Set>
  <Set name="secondaryPort" type="int">1645</Set>
  <Set name="servicePassword">ssg</Set>
  <Set name="serviceGroupPassword">ssg</Set>
</Configure>
```

6. ПОСТРОЕНИЕ СИСТЕМЫ БИЛЛИНГА

6.1 Сбор статистической информации с использованием RADIUS CDR

Для пользователей, которые используют комплекс программно-аппаратных средств SESM/SSG для выбора услуг, учет потребления ресурсов осуществляется на основе протокола RADIUS в соответствии с (RFC2866). В технологии SSG сам учет производиться шлюзом, и периодически результаты (счетчики трафика), в виде RADIUS сообщения Account-Request, сбрасываются им в radius сервер CAR.

Сообщение Account-Request различаются по трем типам:

- Account start;
- Account stop;
- Interim-update.

Когда пользователь установил соединение, SSG посылает "Account start" сообщение CAR серверу. После закрытия соединения SSG посылает сообщение "Account stop". В промежутке времени, когда сессия остается активной, SSG посылает периодические сообщения "Interim-update" с текущей статистикой потребляемых ресурсов. Интервал посылки сообщений является глобальной настройкой SSG:

ssg accounting interval 60

В SSG передаются следующие метрики потребления:

- Acct-Session-Time (Atribute 46.) Передает кол-во времени в течение которого абоненту
  предоставлялся доступ к данному сервису.
- Acct-Input-Octets (Atribute 42.) Число переданных абонентом октетов данных в сторону
  сервиса.
- Acct-Output-Octets (Atribute 43.) Число принятых абонентом октетов данных от сервиса.
- Acct-Input-Packets (Atribute 47.) Число переданных абонентом пакетов данных в сторону
  сервиса.
- Acct-Output-Packets (Atribute 48.) Число принятых абонентом пакетов данных от сервиса.

Cisco CAR сервер записывает сообщения со статистикой в accounting.log файлы в директорию **/opt/CISCOar/log** сервера. Имя файла (например: accounting - 20050322-1) состоит из трех основных частей:

- префикс файла;
- дата создания файла;
- номер файла за период времени (rollover).

Все параметры хранения статистической информации описываются в соответствующем сервисе CAR сервера:

```
[ ///localhost/radius/Services/Accounting ]
  Name = Accounting
  Description =
  Type = file
  IncomingScript~ =
  OutgoingScript~ =
  OutagePolicy~ = RejectAll
  OutageScript~ =
  FilenamePrefix = accounting
  MaxFileSize = "10 Megabytes"
  MaxFileAge = "1 Day"
  RolloverSchedule =
  UseLocalTimeZone = FALSE
```

Для определения того, как часто будет создаваться новый файл для хранения статистики, необходимо определить следующие параметры:

- **MaxFileSize** -максимальный размер файла в килобайтах (КВ), мегабайтах (МВ) или

гигабайтах (ОВ);

- **MaxFileAge** - максимальный время записи в файл в минутах, часах, днях или неделях;

- **RolloverSchedule** -указывает точное время, включающие день месяца или день недели, часы и минуты, когда необходимо создать новый файл.

Значение данных параметров определяются в процессе интеграции с системой биллинга, поэтому в данном проекте эти параметры имеют значения по умолчанию.

6.2 Сбор статистической информации с использованием NetFlow

6.2.1 Общие положения

NetFlow сервис представляет собой функционал, который осуществляет захват статистической информации о трафике, экспортируемой маршрутизаторами и коммутаторами в процессе осуществления ими коммутации IP пакетов, данные NetFlow представляют собой поток трафика, который состоит из однонаправленной последовательности пакетов между определенным источником и получателем пакетов, использующих один и тот же протокол и информацию транспортного уровня. Полученная статистическая информация может быть использована в различных целях: анализ и планирование сети, управление сетью, тарификация.

Ввиду однонаправленности, потоки от клиента к серверу отличны от потоков от сервера к клиенту. Потоки между одной и той же парой источник - получатель также различаются по используемым протоколам.

Маршрутизаторы и коммутаторы идентифицируют потоки, основываясь на следующих полях IP пакетов:

- IP адрес источника;

- IP адрес получателя;
- номер порта источника;
- номер порта получателя;
- протокол;
- тип сервиса (ToS);
- входной интерфейс.

Экспорт данных NetFlow позволяет использовать собранную по трафику статистику в целях планирования сети, тарификации и т.д. Экспортирующее устройство обеспечивает кэширование потоков для обеспечения захвата статистики трафика, основываясь на потоках. Статистика для каждого активного потока собирается в кэше и обновляется каждый раз, как появляется пакет, коммутируемый в рамках данного потока.

Периодически, суммарная статистическая информация для закрытых потоков экспортируется устройством посредством протокола UDP на коллектор NetFlow для обработки.

Поток считается закрытым в следующих случаях:

- протокол транспортного уровня просигнализировал о закрытии соединения (TCP FIN) и по прошествии небольиюго интервала, необходимого для получения подтверждения на команду FIN;
- интервал отсутствия трафика превысил 15 минут.

Для потоков, которые остаются постоянно активными, каждые 30 минут производится закрытие записи в кэше для обеспечения передачи периодических отчетов по активным потокам.

Данные NetFlow экспортируются на определенные узлы, где запущены приложения NetFlow Collector.

6.2.2 Настройка NetFlow Collection Engine

NetFlow Collection Engine (NFC) представляет собой программный продукт, устанавливаемый на платформу Sun Solaris 8. Для запуска NFC необходимо зайти на сервер (10.255.22.21) по определенному при установке имени и паролю и ввести следующую команду:

```
# /opt/CSCOnfc/bin/nfcollector start all
```

Для остановки работы ТЧЕС производятся следующие действия.

```
# /opt/CSCOnfc/bin/nfcollector shutdown
```

В экстренных случаях возможна немедленная остановка ТЧЕС.

```
# /opt/CSCOnfc/bin/nfcollector clean
```

В тоже время возможна остановка различных сервисов без остановки самого ТЧЕС (например, для приостановки сбора статистической информации) необходимо выполнить следующую команду:

 # /opt/CSCOnfc/bin/nfcollector stop collection

Перечень конфигурационных файлов NetFlow представлен в таблице 6.1.

Настройку NFC можно проводить посредством графического пользовательского WEB -интерфейса. Для запуска **CNS NetFlow Collection Engine User Interface** необходимо выполнить следующую команду:

 # /opt/CSCOnfc/bin/nfcollector start web

Таблица 6.1 - Расположение конфигурационных файлов CNS NetFlow

Файл	Расположение	Описание
nfc-config.xml	/opt/CSCOnfc/config	Конфигурационный файл коллектора для специализированных пользовательских настроек
nfc-config-predefined.xml	/opt/CSCOnfc/config	Конфигурационный файл коллектора предустановленных настроек. Данный файл не подлежит изменению
nfcbgp.xml	/opt/CSCOnfc/config	Конфигурационный файл BGP peer
nfcre.xml	/opt/CSCOnfc/config	Конфигурационный файл генератора отчетов
nfcpw.xml	/opt/CSCOnfc/config	Конфигурационный файл диспетчера процессов
nfcifname.xml	/opt/CSCOnfc/config	Конфигурационный файл назначения SNMP имен интерфейсов
dnslookup.conf	/opt/CSCOnfc/config	Конфигурационный файл назначения DNS
nfc-log4j.properties	/opt/CSCOnfc/config	Файл, содержащий свойства документирования событий, происходящих на коллекторе
nfcweb-log4j.properties	/opt/CSCOnfc/config	Файл, содержащий свойства документирования событий, графического пользовательского web-интерфейса
nfcpw-log4j.properties	/opt/CSCOnfc/config	Файл, содержащий свойства документирования событий, диспетчера процессов
nfcre-log4j.properties	/opt/CSCOnfc/config	Файл, содержащий свойства документирования событий, генератора отчетов
nfcxml-log4j.properties	/opt/CSCOnfc/config	Файл, содержащий свойства документирования событий, CNS/XML интерфейса
nfcbgp-log4j.properties	/opt/CSCOnfc/config	Файл, содержащий свойства документирования событий, BGP peer.
server.xml	/opt/CSCOnfc/tomcat/conf	Конфигурационный файл WEB-сервера
web.xml	/opt/CSCOnfc/tomcat/webapps/nfc/WEB-INF	Конфигурационный файл web-приложения для графического пользовательского web-интерфейса

Collection Engine

6.2.2.1 Использование CNS NetFlow Collection Engine User Interface (NFC UI)

В адресной строке необходимо ввести: ***http://20.255.22.21:8080/nfc***

В качестве стартового окна должна появиться следующая картинка. см. рис. 6.1.

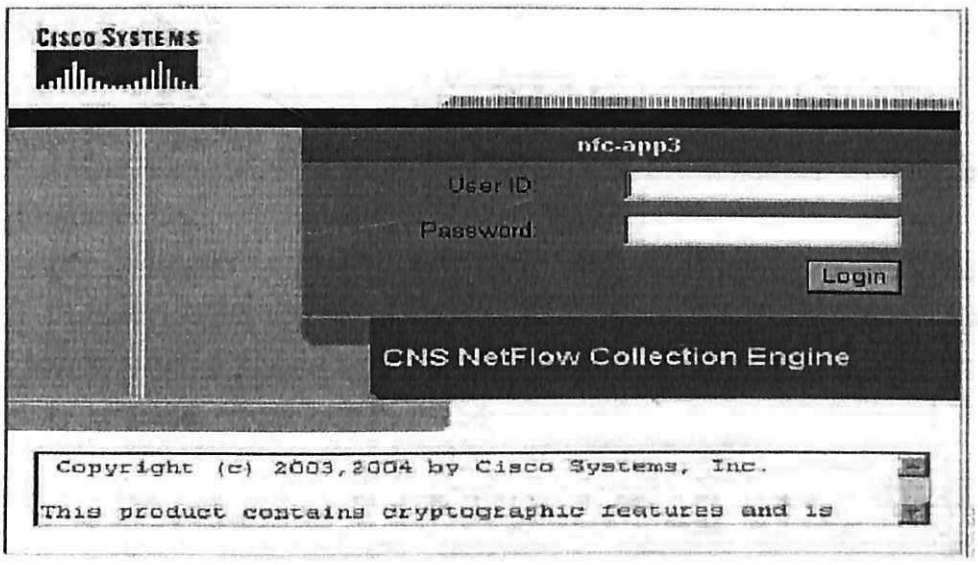


Рисунок 6.1 - Экран Login

С целью обеспечения безопасности, пользователь должен аутентифицироваться в системе, используя корректные имя и пароль. По умолчанию используется следующая пара **nfcuser/nfcuser**.

При успешной авторизации открывается доступ к главному экрану пользовательского интерфейса. Внешний вид данного экрана представлен на рис. 6.2.

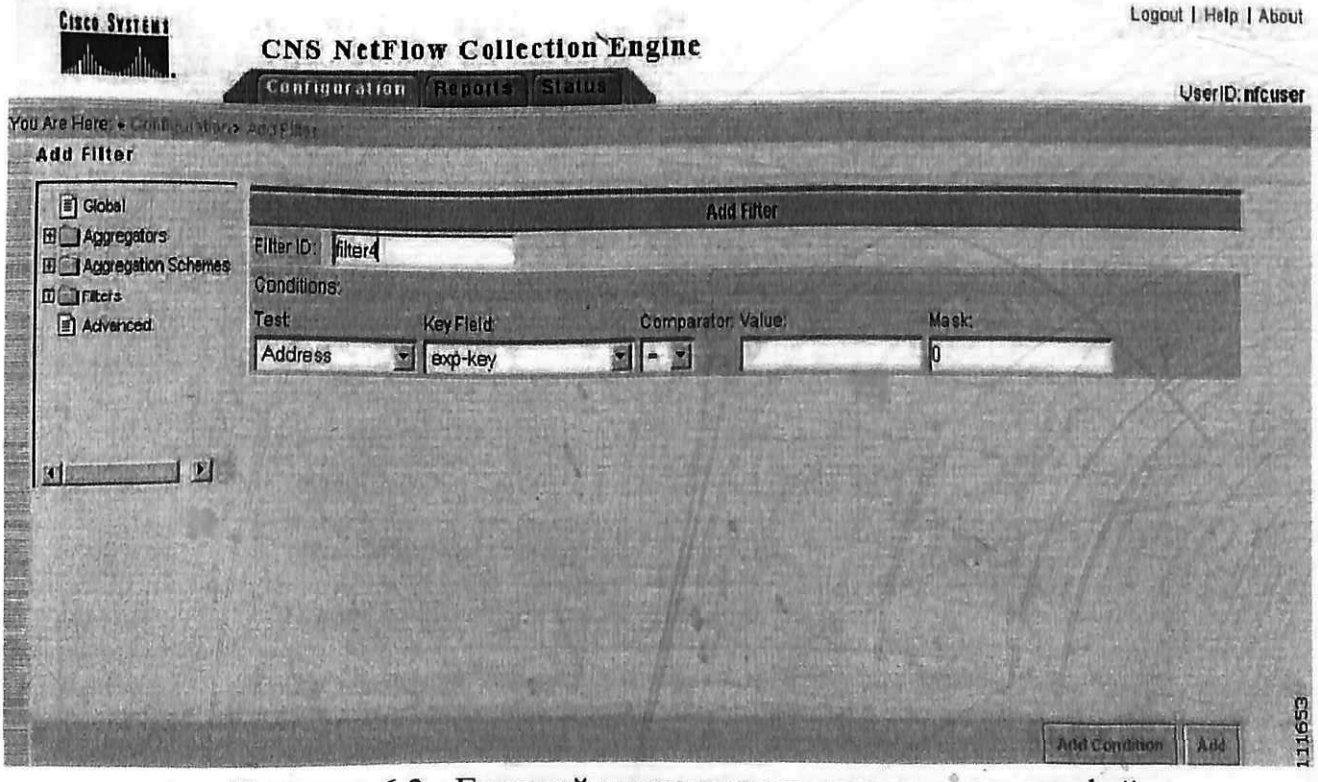


Рисунок 6.2 - Главный экран пользовательского интерфейса

Функционал разделен на три больших раздела, названия которых можно видеть на панели управления: **Configuration, Reports, Status**.

Раздел **Configuration** предназначен для настройки NFC. Здесь задаются общие настройки NFC конфигурируются шаблоны схем агрегации статистической информации, на основе которых создаются конкретные агрегационные конфигурации, создаются и применяются различные фильтры.

Раздел **Reports** позволяет управлять процессом генерации и представления различных типов отчетов.

Раздел **Status** отвечает за предоставление информации о работоспособности системы сбора статистической информации, текущую статистику по собираемым потокам, а так же позволяет просматривать различные log - файлы.

6.2.2.2 Использование NFC для системы тарификации

После запуска NFC начинает сбор данных, основываясь на выбранной схеме агрегации, и сохраняет полученные данные в файлы. По умолчанию NFC использует следующий путь для сохранения указанных файлов: **/opt/CISCOnfs/Data.** Формат файла данных состоит из заголовка, содержащего информацию о записях и одной или более записи данных в соответствии с указанной агрегационной схемой. Пример заголовка представлен ниже.

SOURCE source | FORMAT format | AGGREGATION aggregation | PERIOD period

STATTIME time | ENDTime time | FLOWG flowg | MISSED missed | RECORDS records

AGGREGATION_DEFINITION key [| key …] | value [| value …]

Описание соответствующих полей представлено в таблице 6.2.

Таблица 6.2 - Описание полей заголовка файла данных

Ключ	Описание
SOURCE	Указывает на источник статистической информации. В качестве идентификатора может выступать IP адрес источника.
FORMAT	Указывает на версию формата файла данных. В данном случае этот параметр равен 2
AGGREGATION	Название схемы агрегации
PERIOD	Период времени в минутах, в течение которого производился сбор данных.
STARTTIME	Время старта сбора информации в секундах UTC
ENDTIME	Время окончания сбора информации в секундах UTC
FLOWS	Общее количество NDE записей, которые были агрегированы в данном файле.
MISSED	Количество записей потоков, которые NFC должен был получить, но не получил.
RECORDS	Счетчик агрегационных записей присутствующих в файле данных.

6.2.3 Настройка маршрутизаторов

Для настройки маршрутизаторов магистрали на экспорт статистической информации необходимо произвести следующие действия:
- настроить адрес получателя статистической информации (адрес NetFlow Collector);
- определить интерфейсы, на которых будет осуществляться сбор статистики.

6.2.3.1 Настройка Gateway (Cisco 7206VXR)

На маршрутизаторах УЗЕЛ-3-GW и УЗЕЛ-7-GW, выполняющих роль шлюзов между сетью нашего предприятия и городской сетью г.Алматы, необходимо настроить адрес получателя статистической информации (адрес NetFlow коллектора):

```
ip flow-export source Loopback0
ip flow-export 20.255.22.21 xxxx version 5
```

Затем на интерфейсах PE устройства с которых мы хотим собирать статистическую информацию необходимо активизировать данную функцию

```
ip route-cache flow
```

командой:

Таким образом, пограничные шлюзы будут собирать статистику по всему IP трафику, приходящему на PE устройство со стороны магистрального сегмента сети в сторону городской сети и VRF, в частности.

6.2.3.2 Настройка магистральных маршрутизаторов (Cisco 7609)

На маршрутизаторах УЗЕЛ-7-7600, УЗЕЛ-1-7600, УЗЕЛ-2-7600, УЗЕЛ-13-7600, УЗЕЛ-6-7600 и УЗЕЛ-3-7600 необходимо провести манипуляции схожие с конфигурированием пограничных шлюзов. Но следует отметить, что в маршрутизаторах серии Cisco 7609 присутствует два источника статистической информации: PFC и MSFC.
Настройка каждого из компонентов отличается, для настройки NDE на MSFC необходимо задать адрес получателя статистической информации.

```
ip flow-export source Loopback0
ip flow-export 20.255.22.21 xxxx version 5
```

Затем на интерфейсах PE устройства с которых мы хотим собирать статистическую информацию необходимо активизировать данную функцию

```
ip route-cache flow
```

командой:

При использовании в качестве источника статистической информации PEC необходимо активизировать данную функцию на PEC.


```
mls nde sender version 5
```

7. ПОСТРОЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Целью создания системы безопасности Сети передачи данных Metro Ethernet г.Алматы является реализация политики сетевой безопасности, принятой в отношении компонентов и узлов сети, а также процедур управления, аутенфикации и авторизации, учета, и межсетевого взаимодействия.

7.1 Политика безопасности

Политика безопасности определяет правила доступа к объектам сети, целью которых является защита от несанкционированного доступа к данным и управлению, нарушению работоспособности сети и отдельных ее компонентов. Также в политике безопасности должны быть определены методы контроля состояния компонентов сети на соответствие определенному уровню безопасности, определены обязанности и ответственность персонала по отношению к соблюдению политики безопасности, сформулированы требования к регистрации фактов нарушения безопасности, правила реагирования на факты нарушения.

Опираясь на требования политики безопасности, осуществляется проектирование сети, настройка сетевых устройств и сервисов, установка специализированных устройств и программного обеспечения. Методы и принципы реализации политики безопасности можно разбить на следующие разделы:

- общие правила и средства защиты;
- защита сетевых устройств и сервисов;
- защита протоколов сетевого взаимодействия;
- анализ и фильтрация сетевого трафика;
- ограничение пропускной способности;
- системы обнаружения вторжений;
- доступ и управление устройствами сети;
- регистрация событий безопасности;
- аудит безопасности.

В основе построения сети передачи данных Metro Ethernet используется принцип организации виртуальных частных сетей MPLS VPN данная технология позволяет достичь высокого уровня безопасности, изолируя трафик между компонентами и клиентами сети внутри отдельных виртуальных сетей.

7.2 Общие правила и средства защиты

7.2.1 Синхронизация времени, NTP

Для упорядочивания событий, происходящих на сети, каждое событие, отчет о котором направляется на управляющую станцию, содержит время события, для того

чтобы все устройства сети работали в едином масштабе времени, необходимо наличие временной синхронизации. Синхронизация по времени реализуется с помощью протокола NTP, который конфигурируется и запускается на каждом устройстве сети. Все устройства синхронизируются от двух первичных источников NTP ТЧТР уровня stratum 3, располагающихся на станциях сети управления.

7.2.2 Регистрация системных сообщений, Syslogo

Использование журналов системных событий (Syslog) для отслеживания изменения состояний интерфейсов, изменения состояния конфигураций, температурных режимов и режимов электропитания является общей практикой отслеживания и управления состоянием сети. Каждое устройство конфигурируется для отправки служебных/системных сообщений на выделенные станции управления.

В сети предлагается использовать для хранения журналов станции системы управления.

Все сообщения направляются на эти станции, где конфигурируется и запускается процесс Syslog для сохранения и последующей обработки всех системных сообщений.

7.2.3 Установка времени системных сообщений

Для того чтобы все системные сообщения сопровождались установленным временем происхождения события, необходима конфигурация:

При данной конфигурации формат системных сообщений будет следующим:

service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
JUN 14 10:19:18.555 MET-DST: %SYS-5-CONFIG_I: Configured by console by vty0 (10.255.1.11)

По умолчанию Syslog сообщения содержат IP адрес интерфейса, который используется для выхода из устройства. для того, чтобы все Syslog сообщения содержали IP адрес сети, используемой для управления устройствами сети, необходимо использовать конфигурацию:

7.2.4 Настройка IP-стека устройств

logging source-interface loopback0

Каждое устройство Cisco содержит набор функций по умолчанию, которые могут создавать проблемы с безопасностью сети/, К этим функциям относятся **ip redirects**, **directed broadcast**, **proxy arp**. Для обеспечения устойчивой работы сети

no ip redirects
no ip directed-broadcast
no ip proxy-arp
no ip source-route

эти функции необходимо отключать. для этого необходимо произвести конфигурацию:

no ip redirects - блокирует пакеты ICMP redirects.

no ip directed-broadcast - блокирует распространение directed broadcast пакетов, которые могут использоваться при так называемых SMURF атаках.

no ip proxy-arp - блокирует ответы на ARP запросы, адреса которых известны устройству, что упрощает работу с подключенными сетями и защищает от потенциальных проблем с безопасностью сети.

no ip source-route - заставляет устройства удалять ip пакеты, в которых включена опция source routing. Наличие данной опции может позволить пользователю направлять пакеты в обход средств защиты межсетевых экранов.

7.3 Защита сетевых устройств и сервисов

7.3.1 Сервисы и протоколы общего назначения

Каждое устройство Cisco по умолчанию поддерживает набор информационных сервисов, а также сервисов, используемых для тестирования соединений. Наличие данных сервисов, может создать потенциальные проблемы с безопасностью устройства и сети в целом. В связи с этим, на всех устройствах данные сервисы

no ip finger
no ip ident
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no ip http server
no ip rcmd rcp-enable
no ip rcmd rsh-enable

выключаются:

no ip finger - блокирует службу йп8ег, позволяющую получать информацию о тех, кто подключен к устройству. Поскольку мониторинг устройств осуществляется персоналом сети, наличие службы finger не является необходимым для проверки подключенных пользователей.

no ip ident - отключает поддержку сервиса идентификации ident. Этот сервис разрешает использование незащищенного протокола, описанного в RFC1413, для получения информации о клиенте, инициировавшего TCP соединение. Данный должен быть отключен во всех устройствах сети.

no service-pad - отключает **x25 pad** вход. Нет необходимости в данном сервисе.

no small service - блокирует сервисы контроля типа chargen, echo, drop. Наличие данных сервисов потенциально может образовать брешь в безопасности

системы.

no boottp server - данный сервис, как правило, работает на локальных сетях и не используется в WAN.

no ip http server - сервис удаленного управления устройством с использованием встроенного HTTP сервера. Как правило используется для управления одиночными устройствами в простой конфигурации.

no ip rcmd rcp-enable, no ip rcmd rsh-enable - выключает сервисы RCP и RSH, как имеющие опасно низкий уровень защищенности механизмов аутентификации.

7.3.2 Протокол CDP

Cisco Discovery Protocol (CDP) используется для выполнения некоторых функций управления устройствами Cisco. В основном, он позволяет распознавать непосредственно подключенное Cisco устройство, а также определять его тип switch, маршрутизатор, версию программного обеспечения. Эта информация может быть полезна для поиска и устранения неисправностей. Информация доступная по протоколу CDP сама по себе не нарушает безопасность системы, но может быть использована «хакерами» для проникновения в сеть или блокировки ее работоспособности. CDP должен быть глобально блокирован.

```
no cdp run

interface X
 no cdp enable
```

7.4 Обеспечение безопасного доступа к устройствам

7.4.1 Криптование паролей

В конфигурации каждого устройства присутствуют два пароля: enable secret и enable password. Пароль типа enable secret обеспечивает зашифрованное сохранение пароля в виде MD5 hash функции. Однако данный пароль не может быть использован в некоторых случаях, когда устройство находится в boot режиме. Для сохранения безопасности работы в этом случае необходимо наличие пароля enable password. Для сохранения данного пароля в зашифрованном режиме необходимо наличие команды **service password encryption**.

Поскольку уровень шифрования enable password значительно слабее чем MD5 в enable secret, следует использовать разные пароли для enable password и enable secret.

```
service password-encryption
enable secret cisco
enable password cisco1
```

7.4.2 Настройка терминальных сессий

Для того, чтобы производить автоматическое отключение административного соединения в случае, если администратор забыл отключиться или отошел от станции или терминала, устанавливаются таймауты. В случае не активности соединения пользователя более 5 минут, соединение будет разорвано. Установление параметра TCP keepalive для входящих соединений будет гарантировать, что любое соединение удерживаемое удаленным устройством вследствие «зависания» устройства не будет блокировать доступные vty порты для администрирования устройства. Настройка терминальных сессий:

```
service password-encryption
enable secret cisco
enable password cisco1
```

7.4.3 Система AAA (Cisco Secure ACS)

7.4.3.1 Общие положения

Система AAA (authentication, authorization, accounting) является одной из важнейших составляющих системы информационной безопасности. Она состоит из трех частей:

- аутентификация (authentication) -идентификация объекта;
- авторизация (authorization) -определение различных параметров, присвоенных объекту

(например, список доступных пользователю сетевых ресурсов или конфигурационных

команд);

- учет доступа к сетевым ресурсам (accounting).

В сети можно выделить два основных компонента, принимающих участие в построении системы AAA:

- клиентское приложение, поддерживающее один из протоколов системы AAA

(ПО коммутаторов и маршрутизаторов, и т.п.);

- Сервер AAA (Cisco Secure ACS).

7.4.3.2 Сервер Cisco Secure ACS

Главным компонентом системы AAA в сети является сервер Cisco Secure ACS. Сервер работает под управлением операционной системы Windows 2000 Server. Сервер CS, расположенный в серверной комнате, подключенный к коммутатору центрального узла и имеющий адрес из серверной сети (10.255.22.41), является сервером системы AAA. В обычном режиме все клиенты обращаются к данному серверу.

7.4.3.3 Администрирование серверов Cisco Secure ACS

Администрирование серверов производится через интуитивно понятный WEB-нтерфейс. На рабочей станции администратора должен быть установлен один из следующих браузеров (только английская версия!):

- Microsoft Internet Explorer 6.0 (с установленным SP1) для Microsoft Windows;
- Netscape Communicator 7.0 для Microsoft Windows.

При этом браузер должен быть настроен следующим образом:

- активирована опция Java;
- активирована опция Java Script;
- отключено использование прокси.

Доступ к интерфейсу управления осуществляется по следующему адресу: 10.255.22.41:2002

Для разграничения полномочий и возможности мониторинга процессов AAA на сервере создано два пользователя с разным уровнем привилегий:

- administrator -имеет, как следует из названия, администраторские полномочия;
- readonly -имеет доступ только к разделу "Reports & Activity" интерфейса управления, и может собирать информацию о сетевой активности, связанной с системой AAA.

7.4.3.4 Взаимодействие клиентов с сервером

Каждый AAA клиент, обращающийся к AAA серверу, должен быть на этом сервере описан. Обращения от клиентов, не настроенных на сервере, не обрабатываются.

Настройка клиента производится в разделе "Network Configuration" управляющего web-интерфейса сервера. для каждого AAA-клиента при настройке должны быть указаны следующие параметры:

- имя клиента;
- ip адрес;
- принадлежность к группе устройств;
- протокол взаимодействия клиента с сервером. В проектируемой сети используется протокол TACACS+.

7.4.3.5 Аутентификация (authentication)

Говоря о контроле доступа, безопасности административного доступа к оборудованию следует уделить, пожалуй, едва ли не самое пристальное внимание. За счет практически неограниченных полномочий администраторов, уязвимости в системе административного доступа могут привести к разрушительным последствиям и свести к нулю эффективность других элементов системы информационной безопасности.

В данном разделе мы рассмотрим механизм аутентификации при административном доступе к устройствам.

Для аутентификации административного доступа к активному сетевому оборудованию применяется протокол TACACS+. Все запросы на подключение к устройствам по сети (telnet и ssh) обрабатываются через ACS. Для удобства администрирования настраивается обращение к ACS с адреса виртуального интерфейса Loopback0 (там, где это возможно -например, на маршрутизаторах). для доступа в привилегированный режим используется также аутентификация через ACS.

Для сохранения возможности успешной аутентификации даже при недоступности сервера, в качестве резервного метода настраивается локальная аутентификация (с именем пользователя **admin**). Ниже приводятся фрагменты

```
aaa new-model
!
aaa authentication login Admin group tacacs+ local
aaa authentication enable default group tacacs+ enable
!
username admin privilege 15 password 7 094F471A1C1C1114
!
ip tacacs source-interface Loopback0
!
tacacs-server host 20.255.22.41 key <...>
!
line vty 0 15
login authentication Admin
```

конфигурации для Cisco IOS.

Поскольку консольные порты активного сетевого оборудования используются, как правило, в случае сбоев или для целей отладки и при этом физически защищены от несанкционированного доступа (физический доступ к оборудованию ограничен), то для консольных портов не настраивалась аутентификация через ACS, а используется только локальная аутентификация:

```
aaa authentication login Console local
!
line con 0
 login authentication Console
```

Для взаимодействия системы управления с активным сетевым оборудованием (в частности, конфигурирования устройств) система управления должна иметь возможность административного доступа к упомянутым устройствам. для этого в локальной базе пользователей ACS был создан пользователь cwuser (принадлежащий к группе администраторов).

7.4.3.6 Авторизация (authorization)

В дополнение к аутентификации, для административного доступа к активному сетевому оборудованию по протоколам telnet и ssh была настроена также и авторизация.

Авторизация, которая для своей работы требует успешной аутентификации, позволяет контролировать полномочия аутентифицированного пользователя. Всего настроено два типа авторизации:

- exec - контроль полномочий, связанных с shell-сессиями пользователя (уровень привилегий и т.п.);
- command - ограничения, накладываемые на возможности исполнения различных команд.

В качестве протокола взаимодействия с ACS используется TACACS+. Кроме того, на случай недоступности сервера авторизации предусмотрена локальная авторизация.

```
aaa authorization config-commands
aaa authorization exec Admin group tacacs+ local if-authenticated
aaa authorization commands 15 vtycommands local group tacacs+
!
line vty 0 15
 authorization exec Admin
 authorization commands 15 vtycommands
```

Ниже приведены фрагменты конфигурационных файлов, описывающие настройку авторизации на активном сетевом оборудовании для случая Cisco IOS:

При консольном доступе авторизации не применяется (по тем же причинам, по которым было решено не использовать ACS для аутентификации консольного доступа).

Настройка авторизации на ACS состоит из следующих основных компонентов:

- создание групп пользователей;
- создание групп сетевых устройств;
- создание наборов команд;
- настройка того, какие группы пользователей могут исполнять какие группы команд на каких устройствах.

Устройства, административный доступ к которым авторизуется на ACS, были объединены в одну группу (Network Device Group(NDS)). Для авторизации административного доступа к устройствам было создано две группы:

ADMIN (администраторы, имеющие максимальные полномочия на всех группах устройств -могут выполнять набор команд ЕПIIACCCSS на всех группах устройств);

- HELPDESK (сотрудники технической поддержки, не имеющие возможность изменять конфигурации устройств, а только производить анализ конфигурации и собирать необходимую информацию - могут выполнять набор команд readonly на всех группах
устройств).

7.4.3.7 Учет доступа к сетевым устройствам (accounting)

Последний элемент подсистемы **aaa - accounting**, учет доступа к сетевым устройствам. Существуют четыре категории учета доступа:

- **system** - фиксация системных событий, не связанных с пользователями (например, перезагрузка оборудования);
- **connection** - учет исходящих соединений с данного оборудования (например, telnet);
- **exec** - учет событий, связанных с shell-сессиями пользователей (например, автоматическое выполнение команд);
- **command** - учет всех команд, выполненных пользователем.

В качестве протокола, применяемого для учета доступа, был выбран TACACS+, поскольку он (в отличие от RADIUS) позволяет вести учет команд, выполненных пользователем.

Ниже приводятся фрагменты конфигурации, описывающие настройку учета доступа к сетевым устройствам для случаев Cisco IOS:

```
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
```

При аутентификации и авторизации пользователей сервер ACS делает соответствующие записи в журнале событий. Просмотр этих записей возможен в разделе
Reports & Activity -> TACACS Administration и TACACS Accounting.

7.4.4 Идентификация и авторизация при удаленном доступе

Для обеспечения большей степени защиты сетевых устройств, задачи по аутентификации и авторизации администраторов сети должны быть полностью изолированы. для этого аутентификация и авторизация администраторов сети производится с помощью TACACS сервера (Cisco Secure ACS). Использование TACACS сервера для аутентификации и авторизации администраторов сети при удалённом доступе к сетевым устройствам IP-Системы

позволяет:

- иметь единую централизованную базу данных администраторов сети;
- вести полный отчет о доступе к сетевым устройствам с указанием имени администратора, времени доступа и полной информации о выполненных командах;
- разграничивать доступ к сетевым устройствам между администраторами сети на уровне отдельных команд IOS.

Протокол аутентификации TACACS является индустриальным стандартом и базируется на спецификации RFC1492. Компания Cisco Systems адаптировала и расширила спецификацию данного протокола. В настоящее время во всех устройствах Cisco Systems поддерживается расширенная версия данного протокола TACACS+ (далее по тексту TACACS следует понимать как ссылку на протокол TACACS+).

для обеспечения аутентификации и авторизации администраторов сети при удалённом доступе к сетевым устройствам с использованием сервера авторизации TACAC необходимо выполнить настройки приведенные ниже.

```
aaa new-model
!
!
aaa authentication login Admin group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication login Console local
aaa authorization config-commands
aaa authorization exec Admin group tacacs+ local
aaa authorization commands 15 vtycommands local group tacacs+
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
username admin privilege 15 password 7 094F471A1C1C1114
!
ip tacacs source-interface Loopback0
!
tacacs-server host 20.255.22.41key <...>
!
line con 0
 login authentication Console
!
line vty 0 4
 login authentication Admin
 authorization exec Admin
 authorization commands 15 vtvcommands
```

7.5 Безопасность VPN

В данном проекте реализуются следующие функции безопасности VPN-сервисов:

- обеспечение конфиденциальности (закрытости) VPN-трафика для клиентов других VPN-сервисов;
- обеспечение целостности данных VPN-трафика;
- обеспечение доступности VPN-сервисов.

Используемая в данном проекте технология MPLS VPN сочетает в себе преимущества **Peer-to-peer** - модели и **overlay** – модели. Peer-to-peer - модель, в контексте MPLS VPN, используется на уровне Control Plane для обмена маршрутной информацией между VPN-клиентами через MPLS-сеть. Overlay - подход используется на уровне Data Plane. На уровнях Control Plane и Data Plane реализуются собственные средства обеспечения безопасности VPN-сервисов.

7.5.1 Безопасность на уровне Control Plane

На уровне Control Plane выполняются внутренние служебные функции и функции взаимодействия с клиентскими сетями. Внутренние служебные функции используются для реализации VPN-сервисов, а именно для распространения клиентских маршрутов через MPLS-сеть, построения LSP, реализации механизма FRR и построения маршрутов для управления активным сетевых оборудованием Metro Ethernet сети.

Функции взаимодействия с клиентскими сетями используются для предоставления CE-маршрутизаторам доступа в VPN сервисам. Взаимодействие CE-маршрутизаторов с внутренними служебными функциями исключается.

Безопасность VPN сервисов на уровне Control Plane достигается за счет:

- использования VPN IPv4 адресации;
- контролируемого импорта/экспорта VPN IPv4 маршрутов в/из VRF VPN-клиентов на PE-маршрутизаторах;
- аутентификации CE-маршрутизаторов, участвующих в EBGP-сессиях с PE-маршрутизаторами;
- контроль интенсивности маршрутных BGP-объявлений;
- контроль стабильности объявляемых CE маршрутов;
- использования статической маршрутизации между CE- и PE-маршрутизаторами.

Конфиденциальность, т.е. невозможность клиентом одной VPN несанкционированного чтения (перехвата) информации из другой VPN обеспечивается запретом использования extended community атрибутов в BGP сессии между CE и PE. Extended community атрибуты используются в P-сети для контроля взаимодействия между VRF на различных PE. Использование клиентом extended community атрибутов на CE приведет к экспорту маршрутов в VRF чужих VPN и соответственно к перенаправлению на CE, трафика из другой VPN. Запрет использования extended community атрибутов в BGP-сессии между CE и PE реализуется с помощью удаления из BGP-объявлений, поступающих от CE, extended community атрибутов, содержащих в поле AS номер автономной системы *(65327)*, используемый сетью Metro Ethernet г.Алматы.

Изоляция трафика одной VPN от других VPN достигается контролируемым импортом/экспортом клиентских VPN IPv4 маршрутов в/из соответствующие VRF на PE-маршрутизаторах в явном виде, т.е. таблица маршрутизации клиентского VRF содержит только те маршруты, для которых настроена соответствующая политика импорта/экспорта. Таким образом, импорт маршрутов через MPLSS-сеть в таблицу маршрутизации VRF полностью контролируется оператором и исключается влияние клиентов на политику импорта/экспорта в MPLS сети.

Доступность VPN-сервисов, а именно устойчивость к непредусмотренной или несанкционированной активности клиентов, обеспечивается за счет изоляции внутренних служебных функций от функций взаимодействия с клиентскими сетями,

а также за счет контроля взаимодействия клиентских сетей с VPN сервисами. Изоляция достигается использованием независимых баз коммутации и маршрутизации (VRF). Для передачи служебного и управляющего трафика P-сети используются глобальные таблицы N-PE/PE маршрутизаторов, которые изолированы от клиентских VRF. Клиентские сети при получении доступа к VPN сервисам взаимодействуют только со своими VRF и не имеют доступа к глобальной таблице маршрутизации, в результате чего обеспечивается невидимость внутренних служебных функций для VPN-клиентов.

Доступ клиентских сетей к VPN-сервисам осуществляется двумя способами: с помощью статической маршрутизации и с помощью протокола BGP. Наибольший уровень безопасности достигается с использованием статической маршрутизации. В этом случае P-сеть полностью скрыта от клиентских сетей. CE-маршрутизаторы не содержат никакой информации о P-сети, за исключением IP-адреса N-PE-маршрутизатора, который используется в статических маршрутах на CE-маршрутизаторе в качестве IP next-hop адреса. Контроль взаимодействия клиентских сетей с VPN-сервисами, в случае использования между CE и TE-PE протокола BGP, осуществляется с помощью аутентификации CE-маршрутизаторов, а также контроля стабильности CE-маршрутов и интенсивности их объявлений.

С помощью аутентификации исключается подключение несанкционированных CE-маршрутизаторов, а также устраняется возможность деструктивного влияния злоумышленников на установленные легальные EBGP-сессии.

Контроль стабильности CE-маршрутов позволяет ограничить количество маршрутных BGP-объявлений, вызванных нестабильностью клиентских маршрутов, что повышает общую стабильность P-сети и доступность VPN сервисов.

Неконтролируемая генерация CE-маршрутизаторами BGP-объявлений может привести к переполнению памяти N-PE-маршрутизаторов и повлиять их устойчивость. для повышения устойчивости P-сети и доступности VPN сервисов, а также для улучшения масштабируемости при увеличении числа VPN клиентов и роста их сетей используется ограничение количества BGP-маршрутов, которое CE-маршрутизатор может объявлять через MPLS-сеть.

7.5.2 Безопасность на уровне Data Plane

Безопасность VPN сервисов на уровне Data Plane достигается за счет:

- использования LSP для передачи VPN трафика;
- использование метки-идентификатора клиентского маршрута;
- использования MPLSS-пакетов только в P-сети.

Конфиденциальность и целостность VPN-трафика обеспечивается использованием LSP, а также реализацией MPLS-функций только в P-сети. N-PE-маршрутизаторы принимают от CE-маршрутизаторов только unlabeled-пакеты, т.е. между CE и N-PE не допускается использование пакетов, содержащих MPLS-метки. Отсутствие MPLS-меток в пакетах на входе в MPLS-сеть исключает возможность несанкционированного проникновения клиентских пакетов в LSP других VPN.

Использование предустановленных LSP между N-PE/PE через MPLS -сеть совместно с VPN-меткой, идентифицирующей клиентский маршрут и VRF, обеспечивает изоляцию трафика различных VPN и исключает возможность проникновения трафика из одной VPN в другую. Доступность VPN-сервисов обеспечивается использованием отдельных таблиц коммутации для VPN и для реализации внутренних служебных функция P-сети. Изоляция таблицы коммутации VRF от глобальной таблицы коммутации не позволяет клиентскому трафику влиять на внутренние служебные функции, что позволяет обеспечить доступность VPN-сервисов.

ЗАКЛЮЧЕНИЕ

В последние годы Ethernet достиг абсолютного доминирования в локальных и кампусных сетях. Другие технологии при построении новых сетей рассматриваются только в том случае, если необходимо расширять существующую сеть, но и тогда чаще всего принимается решение перейти на Ethernet. Несколько иная ситуация с городскими сетями, где Ethernet еще не обеспечил себе полного превосходства, но тенденции последнего времени говорят о том, что и здесь другие технологии могут быть вытеснены с рынка.

Использование технологии Ethernet для построения городских сетей широкополосного доступа действительно очень актуально, как для зарубежных, так и казахстанских операторов связи и провайдеров услуг. Успех Ethernet обусловлен прежде всего следующими причинами: высокая скорость, легкость масштабирования технологии и ее простота для массового использования. Легкость масштабирования была заложена еще при разработке технологии, что обеспечило ей конкурентные преимущества перед технологиями с кольцевыми топологиями.

Опыт эксплуатации сетей Metro Ethernet показывает, что они не только сочетают все преимущества оптоволоконных каналов связи и технологии Ethernet, но и отвечают требованиям к мультисервисным сетям

Кроме того, модель с сетевой инфраструктурой на основе Metro Ethernet позволяет организовывать виртуальные частные сети.

Возможности конвергенции с традиционными сетями и интеграции услуг данных, голоса, видео в рамках единой интеллектуальной сетевой инфраструктуры также подтверждают широкие перспективы сетей Metro Ethernet.

СПИСОК ЛИТЕРАТУРЫ

1. Н. И. Баклашов, Н. Ж. Китаева, Б. Д. Терехов. Охрана труда на предприятиях связи и охрана окружающей среды: Учебник для вузов - М.: Радио и связь, 1989. - 288 с.;

2. Долин П.А. - Основы техники безопасности в электроустановках: Учеб. пособие для вузов. - 2-е изд.; перераб. и доп. - М.: Энергоатомиздат, 1984. - 448 с.;

3. Производственное освещение. Методические указания к выполнению раздела "Охрана труда" в дипломном проекте, (для студентов энергетических специальностей всех форм обучения) - Алма-ата, изд. РУМК, с.40. Составители: Кошулько Л.П., Суляева Н.Г., Генбач А.А. ;

4. Защита персонала от поражения электрическим током (часть 1). Методические указания к дипломному проекту - Алматы: АЭИ, 1996 - 26 с. Составители: Санатова Т.С., Кошулько Л.П.;

5. Вентиляция производственных помещений. Часть1. Меодические указания к выполнению раздела «Охрана труда и окружающей среды» в дипломном проекте. - Алма-ата: КазПТИ, 1986. – 42с.

6. Голубицкая Е.А., Жигульская Г.М. - Экономика связи: Учебник для вузов.- М.: Радио и связь, 2000.- 392с.;

7. Срапионов О.С., Горелкин М.А. и др. - Экономика связи: Учебник для вузов.- М.: Радио и связь, 1992.- 320с.;

8. Сайт компании Cisco. www.cisco.com;

9. Дипломное проектирование. Методические указания. Кафедра экономики и менеджмента в связи. Составитель:С.А. Алибаева. – Алматы: АИЭС, - 2001. – 17с.;

10. Internet.

АҢДАТПА

Бұл дипломдық жобада Алматы қаласының «Metro Ethernet» деректерді тарату желісінің әзірлемесі ұсынылған.

Бұл жұмыста қалалық мультисервистік желісінің архитектурасы, іске асыру қызметінің принциптері, басқару жүйесі және биллинг көрсетілген.

АННОТАЦИЯ

В данном дипломном проекте приводится разработка сети передачи данных «Metro Ethernet» г.Алматы.

В работе представлены архитектура городской мультисервисной сети, принципы реализации услуг, системы управления и биллинга.

ABSTRACT

In this graduation project development of data networks «Metro Ethernet» Almaty. The paper presents the architecture of the city multi-service network, the principles of implementation services, system management and billing.