ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Сети телекоммуникаций

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)

Общие требования

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований – «UNICON.UZ» (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере информационных технологий и коммуникаций № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 21.04.2016 № 05-757

4 Настоящий стандарт разработан на основе рекомендации ITU-T Y.1314 «Virtual private network functional decomposition» (Функциональная декомпозиция виртуальной частной сети)

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, RAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Содержание

1	Область применения	1
2	Нормативная ссылка	1
3	Термины, определения и сокращения	2
4	Общие положения	6
5	Требования к функциональной архитектуре VPN	12
6	Требования к поддержке VPN топологии	28
7	Требования по качеству обслуживания в VPN	31
8	Требования к функциям для создания VPN клиент-сервер	34
9	Требования к функциям для создания VPN равноправного взаимодействия	47
10	Требования к функциям VPN по эксплуатации, управлению и обслуживанию	50
11	Требования к функциональным конвергенциям и сценариям услуг	55
12	Требования безопасности к сети VPN	56
Приложение А (рекомендуемое) Расположение точек TCP/TFP в VPN уровня клиента		57
Приложение В (рекомендуемое) Сеть VPN клиент-сервер с несколькими VPN уровня сервера		60
Приложение С (рекомендуемое) Примеры сценариев услуг в сетях VPN клиент-сервер и в сетях VPN равноправного взаимодействия		63

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATIN MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Телекоммуникациялар тармоқлари
ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАР (VPN)
Умумий талаблар

Сети телекоммуникаций
ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)
Общие требования

Telecommunications networks
Virtual Private Networks (VPN)
General requirements

Дата введения 25.04.2016

1 Область применения

Настоящий стандарт устанавливает общие требования к технологии виртуальных частных сетей (VPN), используемой на сетях телекоммуникаций общего пользования, ведомственных и выделенных сетях телекоммуникаций Узбекистана, и предназначен для поставщиков (производителей) оборудования и операторов телекоммуникаций.

Требования настоящего стандарта являются обязательными и пригодны для проведения сертификационных испытаний оборудования, использующего технологию VPN.

2 Нормативная ссылка

В настоящем стандарте использована ссылка на следующий стандарт:

O‘z DSt 2818:2014 Сети телекоммуникаций. Термины и определения

Примечание – При пользовании настоящим стандартом необходимо проверить действие ссылочных стандартов по указателю стандартов, составленному по состоянию на 1 января текущего года и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное

O‘ZSTANDART AGENTLIGI
6028 son bilan
«21» 04 2016 yilda
Davlat ro‘yxatiga olindi

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по O‘z DSt 2818, а также следующие термины с соответствующими определениями:

3.1.1 **адаптированная информация** (adapted information): Сигнал, который передается по «трактам» или «по трактам без установления соединения».

3.1.2 **взаимосвязь между клиентами и сервером VPN** (client-server relationship): Связь между сетями, создаваемая функцией «адаптации» для того, чтобы была возможна поддержка «потока» в сети уровня клиента трактом на уровне сервера.

3.1.3 **домен потока** (flow domain): Компонент топологии в сети CL, используемый для маршрутизации определенной характеристической информации.

3.1.4 **единица трафика** (traffic unit): Экземпляр характеристической информации и единица переноса.

3.1.5 **завершение потока** (flow termination): Функция обработки процесса транспортирования. Имеются два типа завершения потока, приемник и источник потока.

3.1.6 **идентификатор VPN**: Имя, используемое для идентификации конкретной сети VPN.

3.1.7 **контрольная точка** (reference point): Компонент архитектуры, который образуется при связывании входов и выходов функций обработки процесса транспортирования и транспортирующих объектов.

3.1.8 **объединение точек потока** (flow point pool): Группа одновременно существующих точек потока, которые имеют общую маршрутизацию.

3.1.9 **оконечная точка потока** (termination flow point): Опорная точка, которая представляет связывание окончания потока с потоком.

3.1.10 **подсеть** (subnetwork): Компонент топологии сети с установлением соединения (CO), используемый для маршрутизации определенной характеристической информации.

3.1.11 **подсетевое соединение** (subnetwork connection): Передача информации через подсеть и образованную путем соединения портов (выход оконечной точки источника сигнала на данном маршруте – вход оконечной точки получателя) на границах подсети.

3.1.12 **поток доменов потока** (flow domain flow): Транспортная единица, которая переносит информацию через домен потока, она образована объединением портов на границе домена потока.

3.1.13 **точка доступа** (access point): «Опорная точка», которая представляет связывание между окончанием потока и адаптирующими функциями.

3.1.14 **тракт без установления соединения** (connectionless trail): «Транспортирующий объект», ответственный за передачу информации со

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BANDAT
NAZORATINI MUVOFIQLASHTIRISHGA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

входа источника окончания потока на выход приемника окончания потока.

3.1.15 **точка потока** (flow point): Точка, в которой вход линейного потока соединяется с выходом другого линейного потока, называется точкой потока (FP). Точка, в которой выход оконечного источника маршрута без установления соединения в сети CL соединяется со входом сетевого потока, является точкой TFP источника, а точка, в которой вход оконечного приемника маршрута без установления соединения соединяется с выходом сетевого потока, является точкой TFP приемника.

3.1.16 **транспортирование** (transport): Функциональный процесс передачи информации между различными пунктами.

3.1.17 **транспортирующий объект** (transportentity): Компонент архитектуры, передающий информацию между ее входами и выходами внутри сети уровня.

3.1.18 **функция обработки процесса транспортирования** (transport processing function): Компонент архитектуры, определяемый обработкой информации, выполняемой между его входами и его выходами. Вход или выход должен быть внутри сети уровня.

3.1.19 **фрагмент домена потока** (flow domain fragment): Группирование точки потока, соединения внутри области потока должны быть ограничены только соединениями между участниками внутри каждой группы.

3.1.20 **характеристическая информация** (characteristic information): Сигнал конкретного формата, который передается в «потоках».

3.1.21 **VPN сеть уровня клиента** (VPN client layer network): Топологический компонент в сети VPN клиент-сервер, представляющий собой набор точек доступа одного типа, соединенных для передачи характеристической информации в VPN сети уровня клиента.

3.1.22 **VPN сеть уровня сервера** (VPN server layer network): Топологический компонент в сети VPN клиент-сервер, представляющий собой набор точек доступа одного типа, соединенных для передачи адаптированной информации в VPN сети уровня сервера.

3.1.23 **VPN уровня равноправного взаимодействия** (VPN peer layer network): Топологический компонент, представляющий собой набор точек доступа одного типа, соединенных для передачи характеристической информации в сети VPN равноправного взаимодействия.

3.2 В настоящем стандарте применены следующие сокращения:

BOC		- взаимосвязь открытых систем
AAA	(Authentication, Authorization and Accounting)	- аутентификация СЕ/пользователя, санкционирование доступа и расчеты
AI	Adapted Information	- адаптированная информация
AIS	(Alarm Indication Signal)	- сигнал индикации аварии
AP	(Access Point)	- точка доступа

© ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ASON	(Automatically Switched Optical Network)	- оптическая сеть с автоматической коммутацией
ATM	(Asynchronous Transfer Mode)	- асинхронный режим передачи
BFD	(Bidirectional Forwarding Detection)	- двунаправленное обнаружение передачи
BGP	(Border Gateway Protocol)	- пограничный межсетевой протокол
CAC	(Connection Admission Control)	- управление установлением соединений
CBR	(Constant BitRate)	- постоянная скорость передачи
CC	(Connectivity Check)	- проверка возможности соединения
CE	(Customer Edge)	- сторона пользователя
CI	(Characteristic Information)	- характеристическая информация
CO	(Connection-Orientated)	- с установлением соединения
CL	(Connectionless)	- без установления соединения
CL-PS	(Connectionless Packet-Switched)	- с коммутацией пакетов без установления соединения
CO-PS	Connection-Orientated Packet-Switched	- с коммутацией пакетов с установлением
CO-CS	(Connection-Orientated Circuit Switched)	- с коммутацией каналов с установлением соединения
CP	(Connection Point)	- точка соединения
CV	(Connectivity Verification)	- проверка возможности соединения
DHCP	(Dynamic Host Configuration Protocol)	- протокол динамической конфигурации сетевого узла
DLCI	(Data Link Connection Identifier)	- идентификатор канала передачи данных
EBGP	(External Border Gateway Protocol)	- расширенный пограничный межсетевой протокол
E-LMI	(External LMI)	- расширенный интерфейс локального управления
ES	(End System)	- оконечная система
FDFr	(Flow Domain Fragment)	- фрагмент домена потока
FDI	(Forward Defect Indication)	- упреждающее обнаружение ошибки
FP	Flow Point	- точка потока
FR	(Frame Relay)	- ретрансляция кадров
GRE	(Generic Routing Encapsulation)	- общее пакетирование для маршрута
IGP	(Interior Gateway Protocol)	- внутренний межсетевой протокол
IKE	(Internet Key Exchange)	-обмен ключами по сети Интернет

E-HUKUMAT AHBOTLIGI
STANDARTLASHTIRISH, MAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

IPv4	(Internet Protocol Version 4)	- Интернет-протокол - версия 4
IPv6	(Internet Protocol Version 6)	- Интернет-протокол - версия 6
ISIS	(Intermediate System to Intermediate System)	- промежуточная система
L2TP	(Layer 2 Tunneling Protocol)	- протокол туннелирования уровня 2
LDP	(Label Distribution Protocol)	- протокол распределения меток
LMI	(Local Management Interface)	- интерфейс локального управления
LOS	(Loss Of Signal)	- потеря сигнала
LSP	(Label Switched Path)	- путь с коммутацией по меткам
MAC	(Media Access Control)	- управление доступом к среде передачи
MP2P	(Multipoint-to-Point)	- из многих пунктов - в один пункт
MPLS	(Multi-Protocol Label Switching)	- многопротокольное переключение меток
NMS	(Network Management System)	- система управления сетью
OAM	(Operations, Administration and Maintenance)	- эксплуатация, управление и обслуживание
OOB	(Out Of Band)	- внеполосный
OSPF	(Open Shortest Path First)	- открыть кратчайший путь первым
OSS	(Operational Support System)	- система оперативной поддержки
P	(Provider)	- провайдер
P2P	(Point-to-Point)	-из пункта в пункт
P2MP	(Point-to-Multipoint)	- из пункта во многие пункты
PE	(Provider Edge)	- сторона провайдера
PM	(Performance Monitoring)	- контроль качества работы
PNNI	(Private Network-to-Network Interface)	- интерфейс между частной сетью и сетью общего пользования
PW	(Pseudo Wire)	- псевдо провод
QoS	(Quality of Service)	- качество обслуживания
RADIUS	(Remote Authentication Dial In User Service)	- служба дистанционной аутентификации пользователей
RIP	(Routing Information Protocol)	- протокол маршрутизации
RPR	(Resilient Packet Ring)	- отказоустойчивая сеть передачи пакетов
RMON	(Remote MONitoring)	- дистанционный контроль
RSVP-TE	(Resource Reser Vation Protocol with Traffic Engineering (extensions))	- протокол резервирования ресурсов с управлением трафиком (расширения)
SDH	(Synchronous Digital Hierarchy)	- синхронная цифровая иерархия
SLA	(Service Level Agreement	- соглашение об уровне обслуживания

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI

SNC	(Sub Network Connection)	- подсетевое соединение
SNMP	(Simple Network Management Protocol)	- простой протокол сетевого управления
SONET	(Synchronous Optical NETwork)	- синхронная оптическая сеть
SPVC	(Switched Permanent VirtualCircuit)	- коммутируемый постоянный виртуальный канал
SSL	(Secure Socket Layer)	- протокол безопасных соединений
STP	(Spanning Tree Protocol)	- протокол связующего дерева сети
TCP	(Termination Connection Point)	- оконечная точка канала
TDM	(Time Division Multiplexing)	- мультиплексирование с разделением по времени
TFP	(Termination Flow Point)	- оконечная точка потока
UNI	(User-to-Network Interface)	- интерфейс между пользователем и сетью
VC	(Virtual Circuit/Channel)	- виртуальная линия/канал
VCCV	(Virtual Circuit Connectivity Verification)	- проверка соединения по виртуальной линии
VCI	(Virtual Channel Identifier)	- идентификатор виртуального канала
VLAN	(Virtual Local Area Network)	- виртуальная локальная сеть
VPI	(Virtual Path Identifier)	- идентификатор виртуального пути
VPN	(Virtual Private Network)	- виртуальная частная сеть
WDM	(Wavelength Division Multiplexing)	- мультиплексирование с разделением по длине волны

4 Общие положения

4.1 Сети VPN клиент-сервер

Сети VPN клиент-сервер построены по двухуровневой иерархии, в которой сеть VPN уровня сервера используется для поддержания одной или нескольких сетей VPN уровня клиента.

В таблице 1 описываются сети VPN клиент-сервер в понятиях типов VPN услуг.

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, METROLOGIYA
VA SERTIFIKATLASHTIRISH AGENTLIGI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Таблица 1 – Типы услуг в сети VPN клиент-сервер

Тип услуги	Описание
Уровень 1	Предоставляет услугу физического уровня между сайтами пользователя, принадлежащими одной VPN. Соединения строится на физических портах, оптических волнах, виртуальных соединениях SDH/SONET, частотных каналах или слотах времени
Уровень 2	Предоставляет услуги канального уровня между узлами пользователя, принадлежащими VPN. Ретрансляция пакетов данных пользователя основывается на информации, находящейся в заголовках пакетов уровня канала передачи данных (адреса DLCI, ATMVCI/VPI или MAC)
Уровень 3	Предоставляет услугу сетевого уровня межу узлами пользователя, принадлежащими VPN. Ретрансляция пакетов данных пользователя основывается на информации, находящейся в заголовках уровня 3 (адреса пунктов назначения IPv4 или IPv6)

Еще одним способом классификации сетевых технологий является деление их по режимам сетей, к которым они принадлежат. Все сетевые технологии должны быть отнесены к одному из трех типов:

- без установления соединения с коммутацией пакетов (CL-PS);
- с установлением соединения и с коммутацией пакетов (CO-PS);
- с установлением соединения и с коммутацией каналов (CO-CS).

Функциональные требования для каждого режима отличаются друг от друга, у каждого режима свои характеристики.

В таблице 2 приведены примеры технологий сетевых уровней VPN, и к какому режиму они принадлежат.

Таблица 2– Режимы работы сети и примеры

Режим работы	Примеры
(CL-PS)	IP, Ethernet, MPLS MP2P*
(CO-PS)	Ретрансляция кадров, MPLS P2P/P2MP** ATM
(CO-CS)	SDH/SONET, TDM

*Маршруты MPLS из многих пунктов в один пункт (MP2P) с коммутацией по меткам, установленные с использованием протокола распределения меток на нисходящей линии, и работающие самостоятельно, или в режиме запрошенного управления, непосредственно пересекая соседние равноправные протоколы распределения меток.

**Маршруты MPLS из пункта в пункт (P2P) или из одного пункта в несколько пунктов (P2MP) с коммутацией по меткам, установленные с использованием протокола резервирования ресурса для равноправных пользователей, или P2P маршруты MPLS с коммутацией по меткам, установленные с использованием направленного протокола распределения меток между несмежными равноправными протоколами распределения меток.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

4.2 Комбинации клиент-сервер

Существует девять возможных комбинаций клиент-сервер, основанных на трех режимах работы сети, некоторые комбинации являются более совместимыми.

В таблице 3 приведены комбинации клиент-сервер и сведения о совместимости.

Уровень сервера VPN должен поддерживать мультиплексирование/демультиплексирование для разделения плоскости данных между несколькими уровнями клиентов VPN.

Уровни сервера VPN должны также поддерживать адаптацию клиентского трафика, который определяется парой клиент/сервер и не зависит от режимов работы уровня клиента и уровня сервера сети VPN, или от используемых технологий.

Основное требование по адаптации для VPN клиентов с коммутацией каналов, обслуживаемых VPN сервером с коммутацией пакетов, является то, что функция адаптации должна обеспечивать разграничение скоростей (заполнение пустых мест) и выявление пакетов уровня клиента VPN.

Таблица 3 – Комбинации режимов работы клиент – сервер

Режим работы	CO-PSVPN уровня клиента	CL-PSVPN уровня клиента	CO-CSVPN уровня клиента
CO-PS уровня сервера VPN	- Идеален. ***Пример - Серверный уровень AP2PMPLS, поддерживающий уровень ATM клиента.***	- Стоимость обслуживания предоставления каналов VPN по запросу с небольшим временем удержания, SPVC. ***Пример - Серверный уровень ATM, поддерживающий уровень IP клиента.***	- Восстановление тактовой частоты очень сложно технически. ***Пример - Серверный уровень ATM, поддерживающий уровень TDM клиента.***
CL-PS уровня сервера VPN	- Обеспечение гарантии доставки каждого потока усложняет масштабирование; - общий подход, гарантирует доставку каждого потока, должен использовать преимущественные и классовые решения по организации приоритета очередности; - уровень клиента VPN должен быть	- Идеален, гарантии доставки для каждого потока усложняет масштабирование; - общий подход, гарантирует доставку каждого потока, должен использовать преимущественные и классовые решения по организации приоритета очередности для управления пакетным трафиком.	- Обеспечение гарантии доставки для каждого потока усложняет масштабирование; - общий подход, который гарантирует доставку каждого потока, должен использовать преимущественные и классовые решения по организации приоритета

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, RAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Окончание таблицы 3

Режим работы	CO-PSVPN уровня клиента	CL-PSVPN уровня клиента	CO-CSVPN уровня клиента
	способен к восстановлению от влияния единиц трафика, выбивающихся из общей последовательности. ***Пример - Серверный уровень IP, поддерживающий уровень ATM клиента.***	***Пример - Серверный уровень Ethernet, поддерживающий уровень IP клиента.***	очередности; - восстановление тактовой частоты технически сложно; - уровень клиента VPN должен быть способен к восстановлению от влияния единиц трафика, выбивающихся из общей последовательности. ***Пример - Серверный уровень IP, поддерживающий уровень TDM клиента.***
CO-CS уровня сервера VPN	- Нет статистического мультиплексирования между блоками; - полоса выделяется постоянно, вносимые единицы расширения приводят к ухудшению использования сети; - длительное время установления соединения для VPN, работающих по запросу, и имеющих малое время удержания. ***Пример - Серверный уровень ATM, поддерживающий уровеньTDMt клиента.***	- Нет статистического мультиплексирования между блоками; - полоса выделяется постоянно, вносимые единицы расширения приводят к ухудшению использования сети; - длительное время установления соединения для VPN, работающих по запросу, и имеющих малое время удержания. ***Пример - Серверный уровень SDH, поддерживающий уровень Ethernet клиента.***	- Идеален. ***Пример - Серверный уровень оптической сети.***

4.3 Прозрачность уровня клиента VPN

В сети VPN клиент-сервер, функциональные компоненты (маршрутизация, сигнализация, OAM, управление), принадлежащие сети VPN уровня клиента, должны быть полностью независимыми от функциональных компонентов, принадлежащих сети VPN уровня сервера.

Сеть VPN уровня сервера должна прозрачно передавать сигналы сети VPN уровня клиента.

O`ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI

4.4 VPN равноправного взаимодействия

В сети VPN клиент-сервер, функция адаптации источника сети VPN уровня сервера адаптирует CI сети VPN уровня клиента в AI сети VPN уровня сервера, а функция адаптации приемника сети VPN уровня сервера адаптирует AI сети VPN уровня сервера в CI сети VPN уровня клиента.

Сети VPN должны создаваться с использованием сетевых технологий CL-PS, основанных на модели, в которой разграничение достижимости VPN в пределах совместно используемой области достигается за счет некоторых средств, отличных от инкапсуляции «клиент-сервер».

В уровне равноправного использования провайдер передает пакеты пользователя VPN по совместно используемой инфраструктуре на том уровне сети, на котором он получает пакеты от пользователя. Он не обозначает равноправие в плоскости управления пользователь -провайдер, пользователь и провайдер могут равноправно взаимодействовать друг с другом в плоскости управления вне зависимости от типа VPN. Такой тип VPN поддерживается только сетью CL-PS, в случаях CO-PS и CO-CS, технология, основанная на установлении соединения, усиливает разграничение достижимости, сетевые элементы могут взаимодействовать только с сетевыми элементами, которые принадлежат одному и тому же соединению P2P или P2MP.

Для поддержания сети VPN в области совместного использования, используемая технология сети должна применять одни и те же средства разграничения сетей VPN, сетевые элементы должны иметь возможность соединения только с теми сетевыми элементами, которые принадлежат той же самой сети VPN.

4.5 Сортировка пакетов/маршрутов

Одним из способов реализации разграничения сетей VPN в области совместного использования является применение фильтров пакетов вместе с устройствами PE, которые используются совместно несколькими пользователями. В такой архитектуре узлы PE используются совместно различными пользователями. Провайдер услуг выделяет пользователю часть своего адресного пространства и управляет работой фильтров пакетов в PE маршрутизаторах для того, чтобы обеспечить полную достижимость между сайтами отдельного пользователя и разграничение между различными пользователями.

Для поддержания совместимых таблиц маршрутизации и фильтров пакетов для каждого пользователя и каждого сайта, имеется альтернативное решение, основанное на фильтрации маршрутов и работающее совместно с соответствующими устройствами PE. В такой архитектуре узлы P содержат информацию обо всех маршрутах пользователя, а узлы PE содержат информацию о маршрутах только одного пользователя. Изоляция

O ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

маршрутов пользователя достигается за счет фильтрации маршрутов. Узлы PE конфигурируются с фильтрами маршрута, которые позволяют пользователям узнать только те маршруты, которые относятся к ним.

4.6 Шифрование

Шифрование пакетов гарантирует, если пользователи получают пакет из сети VPN, к которой они не принадлежат, то они не могут получить информацию, содержащуюся в этом пакете. Пользователь может зашифровать пакеты в сети VPN до подачи их в исходящий трафик, передаваемый по совместно используемой инфраструктуре и пользователь становится ответственным за управление VPN.

В сети VPN IPsec гарантирует секретность, целостность и аутентификацию источника данных, когда информация передается по совместно используемой инфраструктуре. IPsec важен для создания сетей VPN с передачей информации по сетям общего пользования или для доступа к удаленным сетям VPN.

Функционирование IPsec обеспечивается при помощи PE, CE или оконечных устройств пользователя.

Сети VPN SSL – это еще один тип VPN, в котором для изоляции отдельных VPN используется шифрование. Типовым применением сетей VPN с SSL является предоставление пользователю безопасного доступа к приложениям и файлам через Интернет. Преимущество этого подхода заключается в том, что он не требует никаких изменений конфигурации оконечных систем пользователя, и требуется поддержание только стандартизованных приложений (Web-навигаторы, почтовые клиенты).

Сети VPN с SSL являются прозрачными для сетей VPN уровня равноправного взаимодействия (шифрование выполняется на прикладном уровне) и конфигурация узлов маршрутизации/коммутации не является необходимой для поддержки сетей VPN с SSL.

4.7 Виртуальные локальные сети Ethernet

Сети VLAN должны соединяться с оконечными станциями в различных физических сегментах локальной сети, соединены с одним сегментом LAN. Оконечные пользователи и узлы/коммутаторы должны быть перенесены в различные сети VLAN путем изменения конфигурации VLAN на порту/интерфейсе, к которому подсоединена оконечная станция или узел/коммутатор.

Сети VLAN дают возможность соединять оконечные станции в различных физических сегментах локальной сети. Кадры радиовещательной передачи ограничиваются границами VLAN, поэтому оконечные станции будут получать только те кадры радиовещательной передачи, которые предназначены для той VLAN, к которой они принадлежат. Этот факт с учетом того, как работает механизм узнавания MAC-адреса, гарантирует,

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

что общаться друг с другом смогут только оконечные станции одной и той же VLAN, и, следовательно, их можно считать участниками одной сети VPN.

Разделение трафика на кадры, принадлежащие различным сетям VLAN на всей совместно используемой инфраструктуре, достигается путем введения в каждый кадр метки с идентификатором VLAN.

Идентификатор должен быть назначен каждой сети VLAN (от 1 до 4096) и должен быть уникальным в пределах одной и той же физической инфраструктуры. Он отделяет область сети VLAN провайдера от пользовательской области VLAN и позволяет пользователям применять любой идентификатор сети VLAN.

5 Требования к функциональной архитектуре VPN

5.1 Эталонная модель VPN

Эталонная модель VPN приведена на рисунке 1.

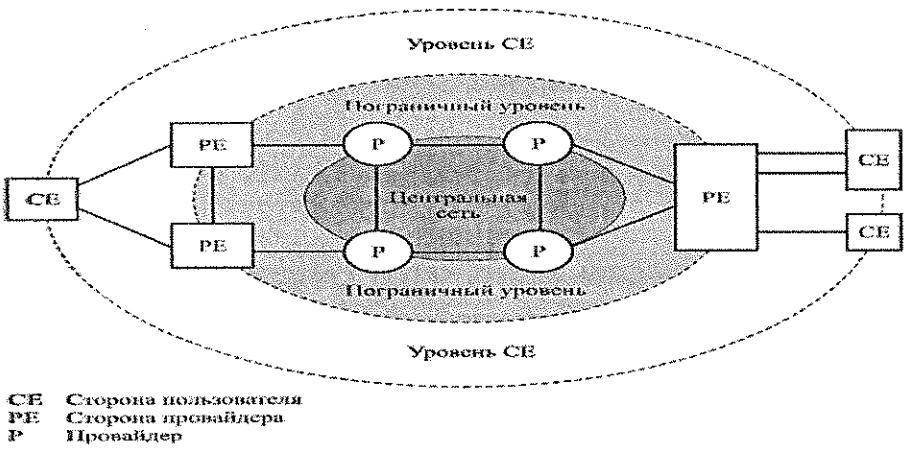


Рисунок 1 - Эталонная модель VPN

Сеть VPN должна разделить на независимые сетевые уровни, взаимодействие между которыми происходит по схеме клиент-сервер. Сетевые уровни, определенные с использованием функционального моделирования, не следует путать с уровнями из модели ВОС. Каждый уровень модели ВОС предоставляет конкретную услугу, а протокол, определенный для каждого уровня, выполняет конкретные функции, соответствующие этому уровню, например, транспортный уровень получает данные от уровня сеанса связи и передает их на сетевой уровень, предоставляя услугу сквозной доставки.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, PAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

5.2 Сети VPN с установлением соединений

Каждая сеть VPN уровня клиента и сервера должна имеет собственный набор входов и выходов для установления соединений, называемых AP. Они соединяются друг с другом с целью прозрачной передачи информации от входа до выхода данного сетевого уровня. Эффективными топологическими конструкциями связи между точками доступа для сетей CO являются соединения P2P и P2MP.Точки доступа сети VPN уровня сервера отмечают функциональную границу между сетями VPN уровня сервера и клиента. С точки зрения сети VPN уровня сервера, точка доступа сети VPN определяет направление маршрутизации, которая поддерживает маршрут передачи. С точки зрения сети VPN уровня клиента, точка доступа сети VPN уровня сервера AP представляет собой точку, в которой можно заказать пропускную способность канала.

Функциональные компоненты и контрольные точки в сети CO приведены на рисунке 2.

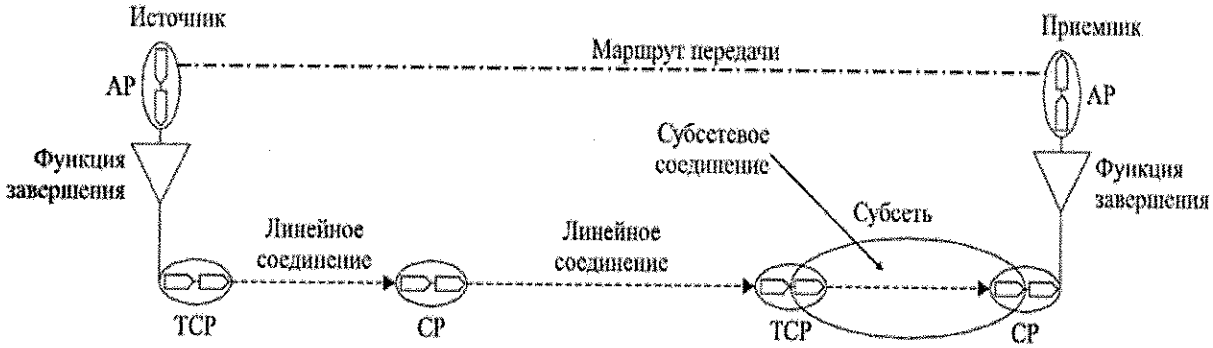


Рисунок 2 - Функциональные компоненты и контрольные точки в CO сети

Линейные соединения связывают смежные подсети, которые имеют общий набор точек. Точка, в которой вход канала соединен с выходом другого канала, является CP. Точка, в которой выход оконечного источника маршрута сети CO соединен с входом сетевого соединения является оконечной точкой канала источника, а точка, в которой вход оконечного приемника маршрута соединен с выходом сетевого соединения является оконечной точкой канала приемника. С точками CP и TCP соединены управляемые объекты и в целях управления должны сгруппироваться точки TCP и CP.

5.3 Сети VPN без установления соединений

В отличие от сетей CO, сети CL должны поддерживать различные виды топологии соединения множества пунктов с множеством пунктов MP2MP. Сети CL используют не каналы, а потоки, которые являются объ-

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

единением одного или нескольких элементов трафика с элементом общей маршрутизации. Потоки разделяются на одно направленные и двунаправленные, двунаправленные потоки состоят из двух противоположных однонаправленных потоков.

Функциональные компоненты и контрольные точки сети CL приведены на рисунке 3.

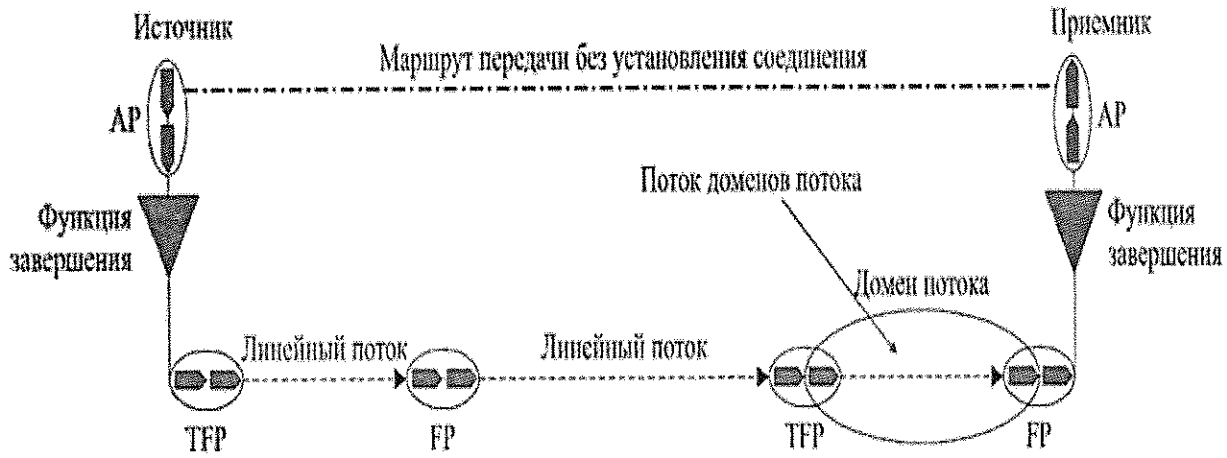


Рисунок 3 - Функциональные компоненты и контрольные точки в CL

Домен потока содержит набор точек, связанных с функцией управления в пределах одной сети CL.

Линейные потоки соединяют смежные домены потока, у которых имеется общий набор точек. Точка, в которой выход оконечного источника маршрута CL в сети соединяется с входом сетевого потока, является точкой TFP источника, а точка, в которой вход оконечного приемника маршрута без установления соединения соединяется с выходом сетевого потока, является точкой TFP приемника.

5.4 Взаимосвязи между клиентами и сервером VPN

5.4.1 Общее назначение

Сеть VPN уровня клиента, компонент топологии сети VPN клиент-сервер, который представляет собой набор точек доступа одного типа, соединенных для передачи CI сети VPN уровня клиента, поддерживаются линией связи сети VPN уровня сервера, либо маршрутом CL.

Оконечные точки канала/потока источника/приемника для сети VPN уровня клиента могут располагаться в узлах на CE, или в узлах/оконечных устройствах сети пользователя. Например, точки TCP в ATM сети VPN уровня клиента, будут размещены на узлах CE, тогда как точки TFP в Ethernet сети VPN уровня клиента будут размещены на оконечных компьютерах пользователя или серверах. Место размещения оконечных точек канала/потока источника/приемника сети VPN клиента является очень

© O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH MUAMMOLARI

важным сточки зрения пользователя, поскольку это – та точка сети пользователя, где должна выполняться адаптация сетей VPN уровня клиента и сетей вышележащего уровня. Это место очень важно с точки зрения OAM, поскольку именно здесь точки доступа канала связи или маршрута без установления соединения соединяются с каналом/потоком VPN уровня клиента.

В приложении А приведены примеры сетей VPN клиент-сервер с различными вариантами размещения точек TFP/TCP.

Сеть VPN уровня сервера содержит функции адаптации источника/приемника, которые адаптируют в сети VPN уровня клиента из адаптированной информации сети VPN уровня сервера.

Сети VPN уровня клиента и сервера должны работать в одном и том же режиме (когда уровень клиента и сервера работают без установления соединения, либо оба работают с установлением соединения), но комбинация этих двух режимов, сети CO сети VPN уровня сервера могут поддерживать CL сети VPN уровня клиента и, точно также, CL сети VPN уровня сервера могут поддерживать CO сети VPN уровня клиента.

На рисунке 4 - CL сеть VPN уровня сервера, поддерживающая CL сеть VPN уровня клиента. Нижний уровень, показанный в модели, это – сеть VPN уровня сервера, а верхний уровень это – VPN уровня клиента.

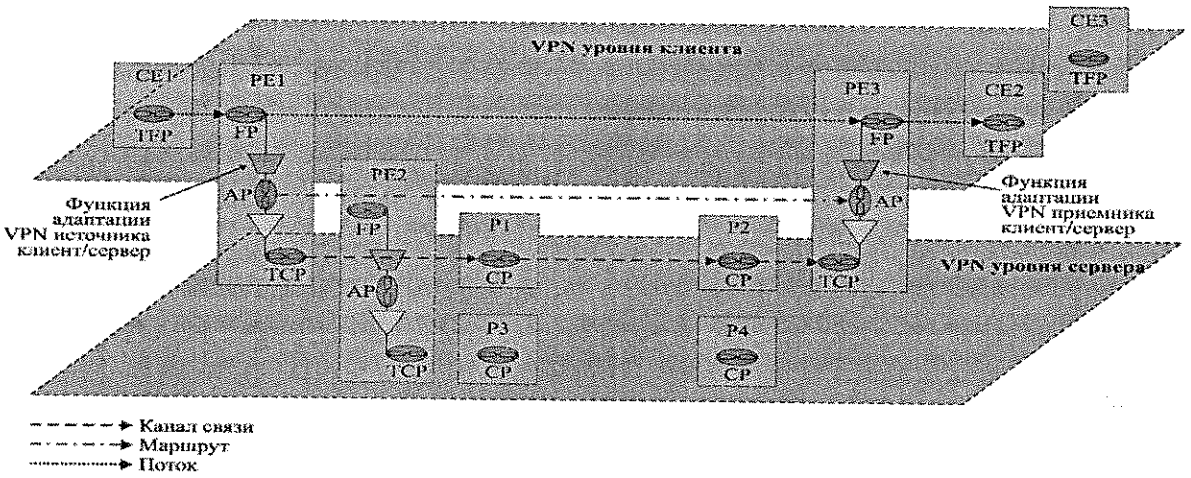


Рисунок 4 - Функциональная модель сети VPN клиент-сервер

На рисунке 4 приведено, как функциональная модель связана с диаграммой сети, изображенной на рисунке 1, какие функции и контрольные точки сети представлены, в каком сетевом элементе (в узле CE, PE или P).

Узлы CE и P относятся к сетям VPN уровней клиента и сервера соответственно, тогда как узлы PE относятся к обоим уровням.

Точки TFP в сети VPN уровня клиента определяют, где поток P2P сети VPN начинается (источник сети) и заканчивается (приемник сети), точки FP определяют, через какие узлы PE проходит поток P2P. Точки TFP в сети VPN уровня сервера определяют источник и приемник соединения

© O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
Joriy etish boshqarmasi

VPN уровня сервера, а точки FP определяют, через какие узлы P проходит поток. AP в сети VPN уровня сервера определяют источник/приемник маршрута передачи в VPN уровня сервера.

5.4.2 Сеть VPN уровня клиента с установлением соединения, поддерживаемая сетью VPN уровня сервера с установлением соединения

На рисунке 5 приведен пример CO сети VPN уровня клиента, которая поддерживается CO сетью VPN уровня сервера.

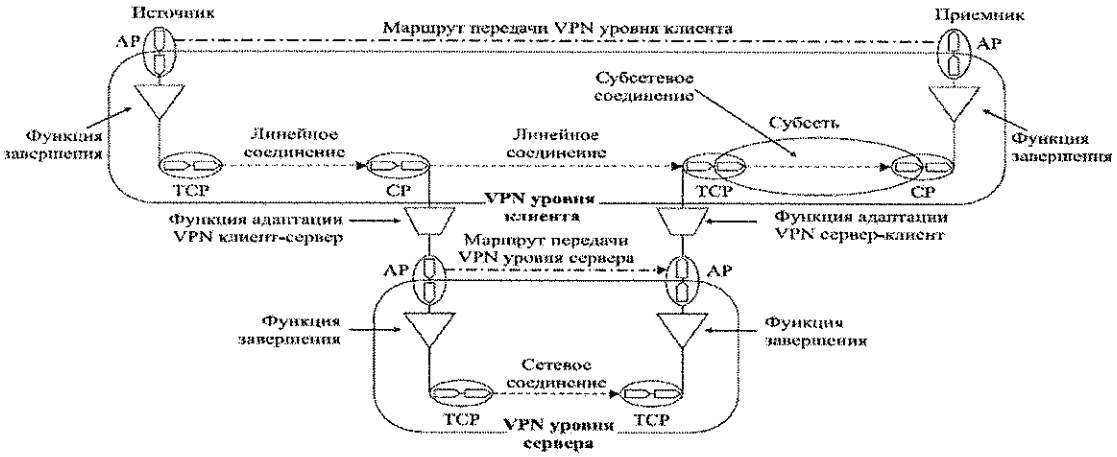


Рисунок 5 - CO сеть VPN уровня сервера с CO сетью VPN клиента

В этом рисунке CO соединение сети VPN уровня клиента поддерживается CO маршрутом передачи в сети VPN уровня сервера. Функция адаптации источника CO сети VPN уровня сервера адаптирует CI CO сети VPN уровня клиента, преобразуя ее в AI в CO сети VPN уровня сервера. Функция адаптации получателя CO сети VPN уровня сервера адаптирует AI CO сети VPN уровня сервера, преобразуя ее в характеристическую информацию CO сети VPN уровня клиента.

5.4.3 Сеть VPN уровня клиента без установления соединения, поддерживаемая сетью VPN уровня сервера без установления соединения

На рисунке 6 приведен пример CL сети VPN уровня клиента, которая поддерживается CL сетью VPN уровня сервера.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, PAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI

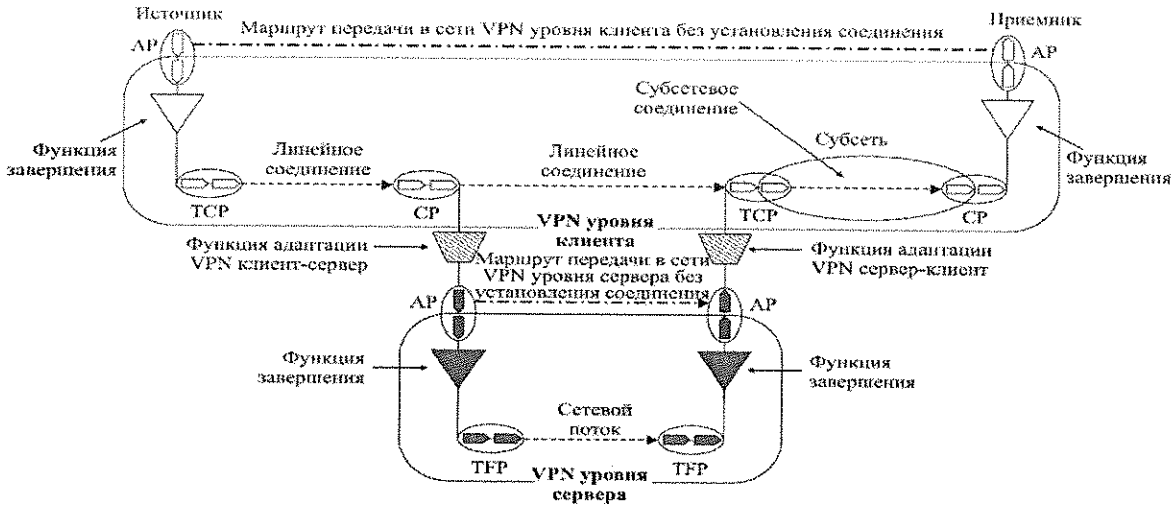


Рисунок 6 - CL сеть VPN уровня сервера с CL сетью VPN клиента

В этом примере CL поток сети VPN уровня клиента поддерживается маршрутом CL сети VPN уровня сервера. Функция адаптации источника CL сети VPN уровня сервера адаптирует CI CL сети VPN уровня, преобразуя ее в AI в CL сети VPN уровня сервера. Функция адаптации получателя CL сети VPN уровня сервера адаптирует AI CL сети VPN уровня сервера, преобразуя ее характеристическую информацию CL сети VPN уровня клиента.

5.4.4 Сеть VPN уровня клиента с установлением соединения, поддерживаемая сетью VPN уровня сервера без установления соединения

На рисунке 7 приведен пример CO сети VPN уровня клиента, которая поддерживается CL сетью VPN уровня сервера.

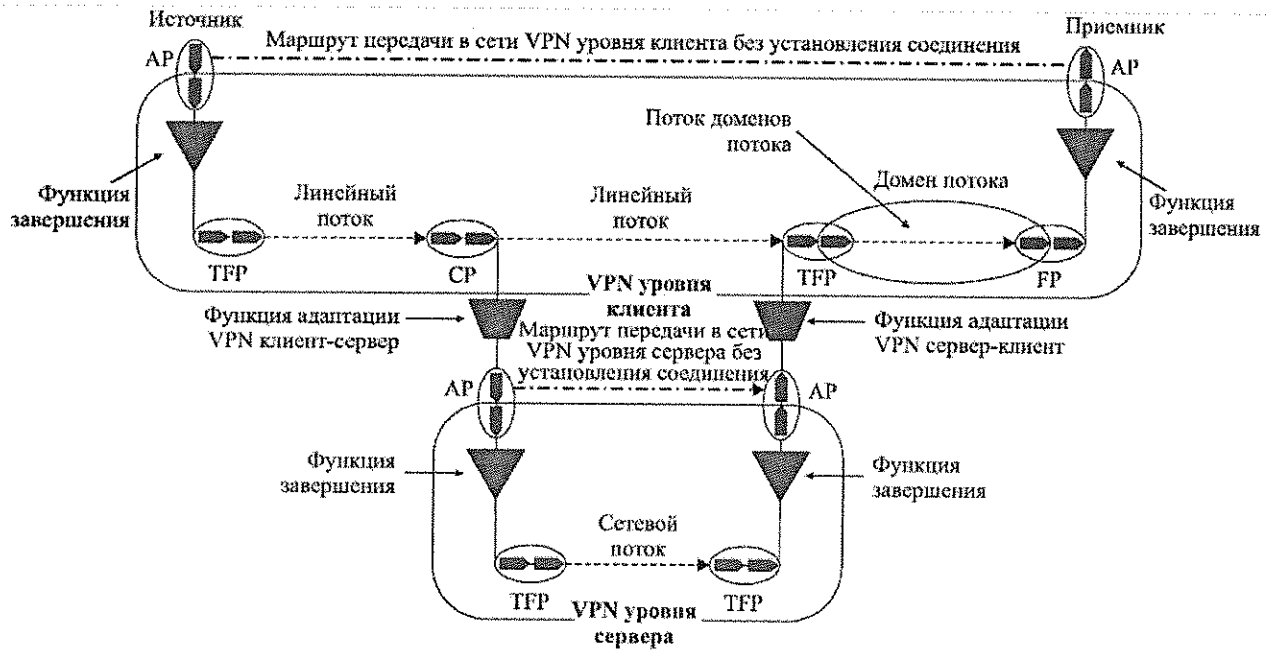


Рисунок 7 - CL сеть VPN уровня сервера с CO клиентом

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

В этом примере CO соединение сети VPN уровня клиента поддерживается маршрутом CL сети VPN уровня сервера. Функция адаптации источника CL сети VPN уровня сервера адаптирует CI CO сети VPN уровня, преобразуя ее в AI CL сети VPN уровня сервера. Функция адаптации получателя CL сети VPN уровня сервера адаптирует AI CL сети VPN уровня сервера, преобразуя ее в CI CO сети VPN уровня клиента.

5.4.5 Сеть VPN уровня клиента без установления соединения, поддерживаемая сетью VPN уровня сервера с установлением соединения

На рисунке 8 приведен пример CL сети VPN уровня клиента, которая поддерживается CO сетью VPN уровня сервера.

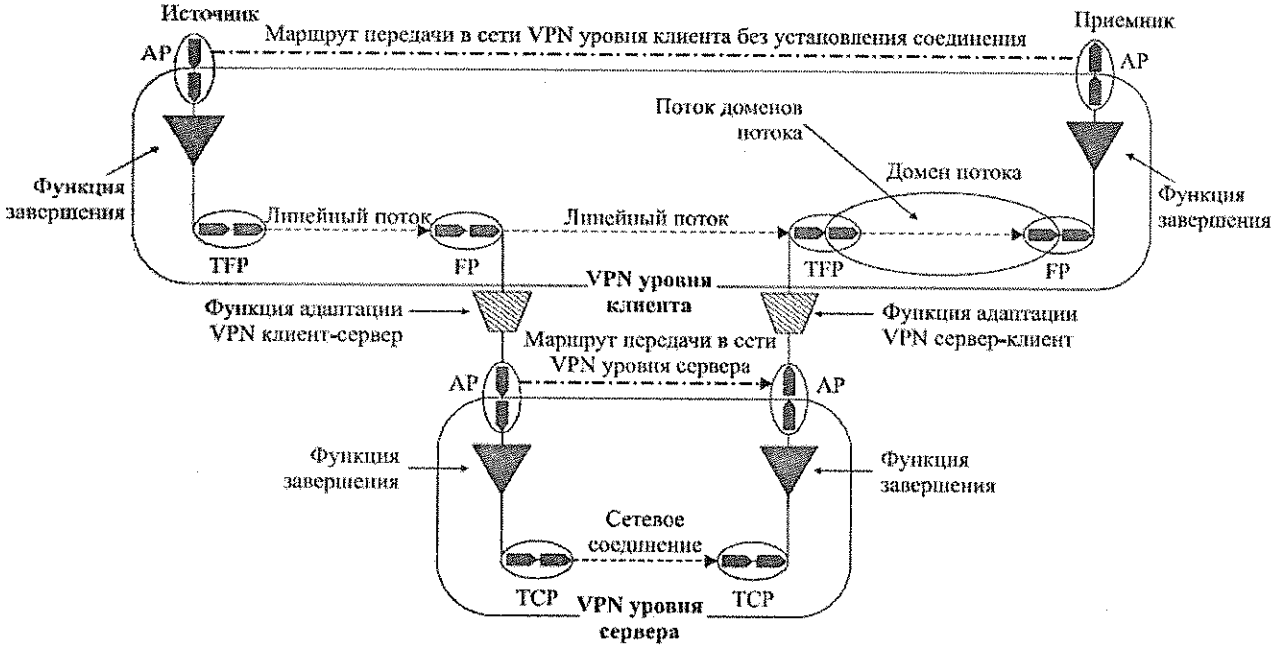


Рисунок 8 - CO VPN уровня сервера с CL клиентом

В этом примере CL поток сети VPN уровня клиента поддерживается CO маршрутом передачи сети VPN уровня сервера. Функция адаптации источника CO сети VPN уровня сервера адаптирует CI CL сети VPN уровня клиента, преобразуя ее в AI в CO сети VPN уровня сервера. Функция адаптации получателя CO сети VPN уровня сервера адаптирует AI CO сети VPN уровня сервера, преобразуя ее в CI CL сети VPN уровня клиента.

5.5 Несколько сетей уровня VPN клиента

В рассмотренных ранее примерах, для полного сквозного соединения по сети провайдера использовалась одна единственная сеть VPN уровня сервера, поддерживающая сети VPN уровня клиента. Однако, это не всегда так; например, провайдер может не иметь возможности выполнить сквоз-

E-STANDART ASENTLIGA
STANDARTLASHTIRISH, MAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ное соединение, если он использует одну единственную сеть VPN уровня сервера из-за отсутствия сетевого покрытия, или если сети VPN уровня клиента требуется передать информацию по сетям нескольких провайдеров. В таких условиях требуется несколько сетей VPN уровня сервера.

В зависимости от конкретных сетевых технологий и возможностей взаимодействия оборудования провайдера, отдельные сети VPN уровня сервера могут взаимодействовать на равноправной основе, или взаимодействовать с VPN клиентом на основе клиент-сервер.

В этом случае две различные сети VPN уровня клиента должна взаимодействовать на равных основаниях. Взаимодействующие в VPN на уровне клиента обе технологии должны быть технологиями Уровня 2, но они считаются разными сетевыми уровнями, поскольку в них находятся различные точки доступа, которые также являются точками разного типа.

Функция взаимодействия должна выполняться либо до функции адаптации источника сети VPN уровня сервера, или после функции адаптации приемника сети VPN уровня сервера. На рисунке 9 показана физическая топология сети VPN клиент-сервер, в которой на каждой стороне сети VPN используются различные сети VPN уровня клиента.

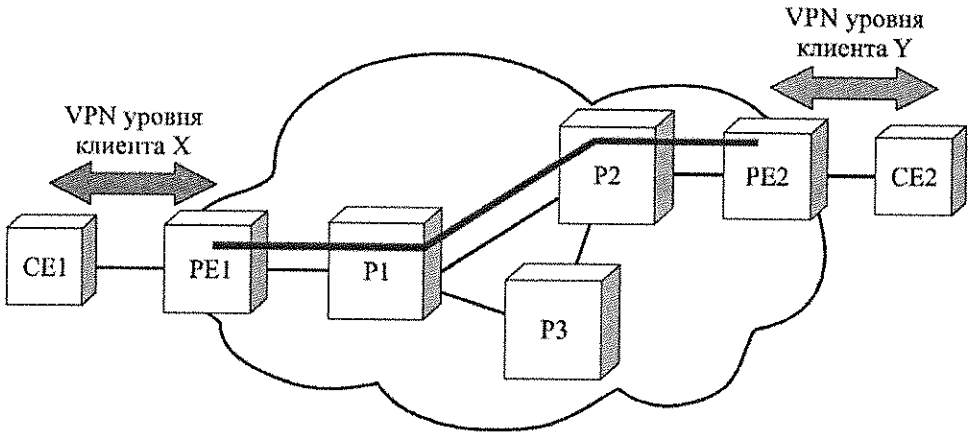


Рисунок 9-Физическая топология сети VPN клиент-сервер уровня равноправного взаимодействия

На рисунке 10 представлена общая функциональная модель равноправного взаимодействия сети VPN уровня клиента, основанная на физической топологии, показанной на рисунке 8, где функция взаимодействия выполняется до функции адаптации источника сети VPN уровня сервера.

© ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

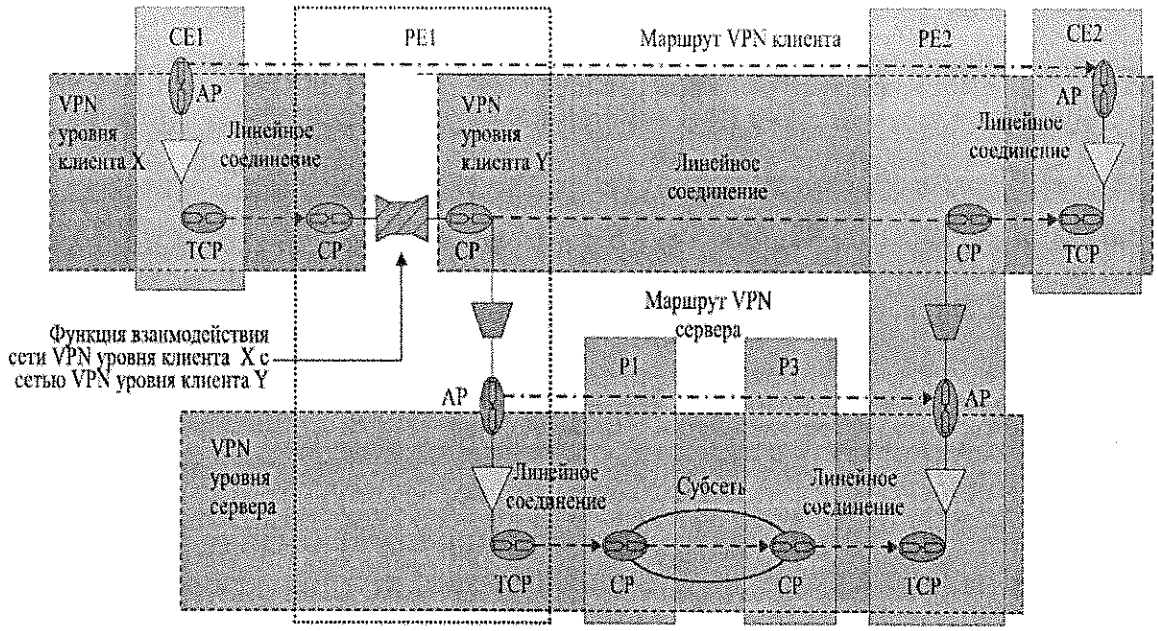


Рисунок 10 - VPN уровня равноправное взаимодействие клиента (адаптация до источника сервера VPN)

Две гетерогенных сети VPN уровня клиента в этой модели – это сеть VPN уровня клиента X и сеть VPN уровня клиента Y. Функцию взаимодействия выполняет PE. Функция взаимодействия преобразует CI сети VPN уровня клиента X в CI сети VPN уровня клиента Y. Функция адаптации источника сети VPN уровня сервера преобразует CI сети VPN уровня клиента Y в AI сети VPN уровня сервера, затем AI сети VPN уровня сервера передается по маршруту VPN уровня сервера. На приемном конце сети VPN уровня сервера функция адаптации преобразует AI сети VPN уровня сервера в CI сети VPN уровня клиента Y.

Например, уровень клиента X является сетью технологии FR, а сеть VPN уровня клиента Y является сетью технологии ATM, то источник PE будет преобразовывать трафик FR в трафик ATM и трафик сети VPN уровня клиента будет передаваться по сети VPN уровня сервера как трафик ATM.

На рисунке 11 представлена общая функциональная модель равноправного взаимодействия сети VPN уровня клиента, где функция взаимодействия выполняется после функция адаптации приемника сети VPN уровня сервера.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

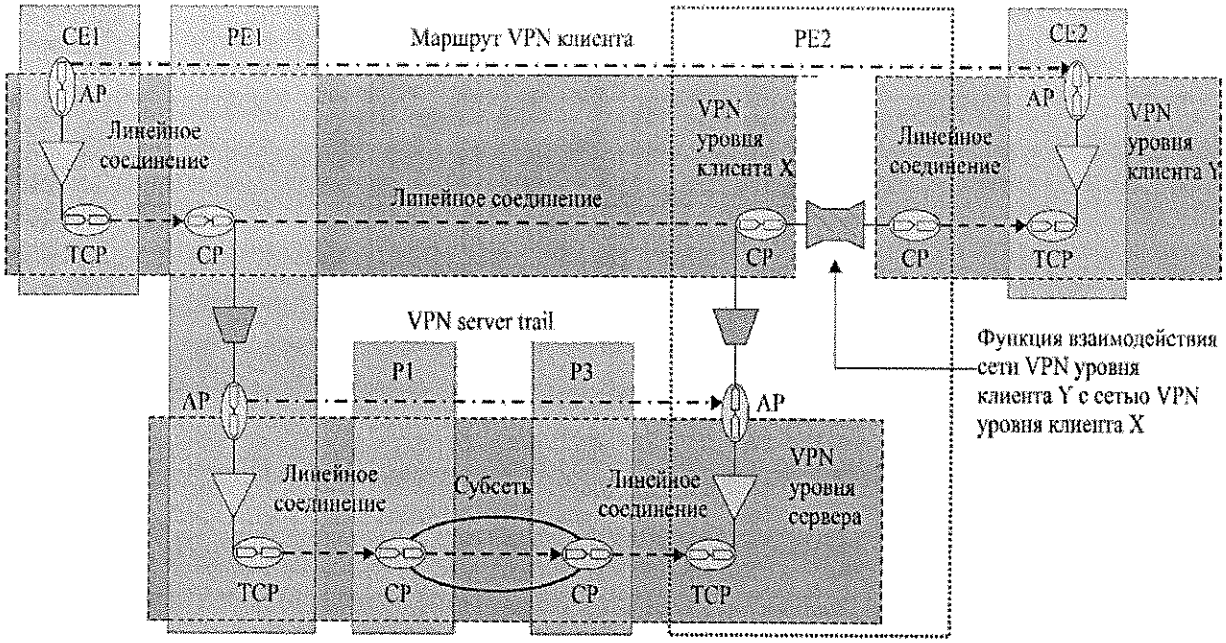


Рисунок 11 - VPN уровня равноправное взаимодействие клиента (адаптация после приемника сервера VPN)

Функция адаптации источника сети VPN уровня сервера преобразует CI сети VPN уровня клиента X в AI сети VPN уровня сервера, и AI сети VPN уровня сервера передается по маршруту VPN уровня сервера. На приемном конце сети VPN уровня сервера функция адаптации преобразует AI сети VPN уровня сервера в CI сети VPN уровня клиента X.

Функция взаимодействия преобразует CI сети VPN уровня клиента X в CI сети VPN уровня клиента Y. Если VPN уровня клиента X является сетью технологии FR, а сеть VPN уровня клиента Y является сетью технологии ATM, то трафик сети VPN уровня клиента будет передаваться сети VPN уровня сервера как трафик FR, и преобразовываться в трафик ATM на PE приемнике.

5.6 Несколько сетей VPN уровня сервера

В рассмотренных ранее примерах, для полного сквозного соединения по сети провайдера использовалась одна-единственная сеть VPN уровня сервера, поддерживающая сети VPN уровня клиента. Однако, это не всегда так; например, провайдер может не иметь возможности выполнить сквозное соединение, если он использует одну-единственную сеть VPN уровня сервера из-за отсутствия сетевого покрытия, или если сети VPN уровня клиента требуется передать информацию по сетям нескольких провайдеров. В таких условиях требуется несколько сетей VPN уровня сервера.

В зависимости от конкретных сетевых технологий и возможностей взаимодействия оборудования провайдера, отдельные сети VPN уровня

© ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

сервера могут взаимодействовать на равноправной основе, или взаимодействовать с VPN клиентом на основе клиент-сервер.

Вполне возможно применение нескольких сетей VPN уровня сервера. Имеется несколько факторов, которые следует учитывать при принятии решения об использовании нескольких MPLS сетей VPN уровня сервера. Факторы, требующие рассмотрения, зависят от требуемого типа взаимодействия и применяемых сетевых технологий в сети VPN уровня сервера.

В приложении В приведены примеры равноправного взаимодействия и взаимодействия клиент-сервер для нескольких уровней сервера.

Применение нескольких уровней сервера, расположенных ниже сети VPN уровня сервера, не следует путать с применением нескольких сетей VPN уровня сервера.

Например, как показано на рисунке 12, провайдер услуг может использовать одну MPLS сеть VPN уровня сервера для сквозного соединения, но при этом на одном из участков сети использовать сеть MPLS уровня сервера ниже сети VPN уровня сервера, и использовать сеть IP уровня сервера на другом участке сети.

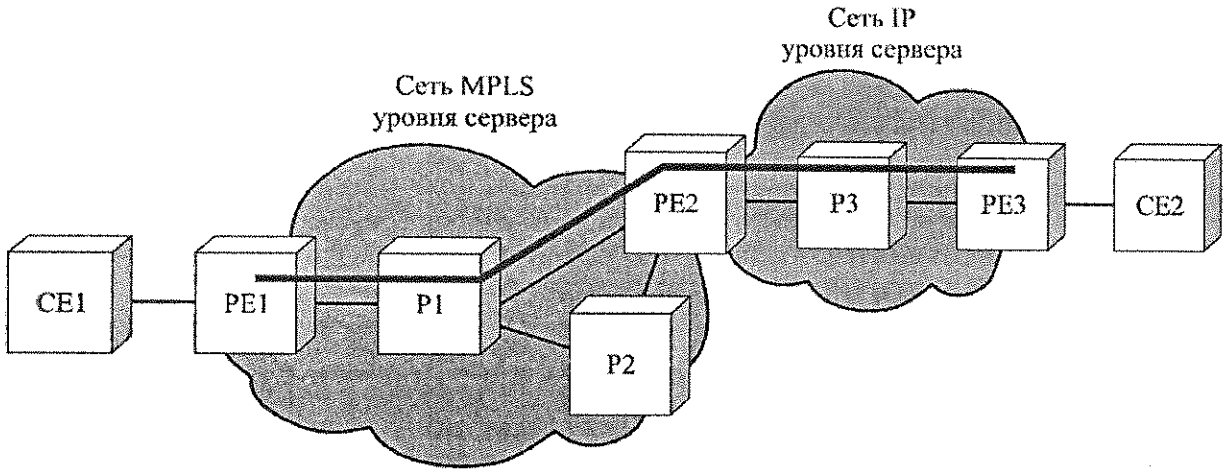


Рисунок 12 - Сеть VPN клиент-сервер с сетями MPLS и IP уровнями сервера

Все маршрутизаторы PE и P должны поддерживать MPLS в сети MPLS уровня сервера, однако, только маршрутизаторы PE в IP сети уровня сервера должны поддерживать MPLS, маршрутизаторы P не должны поддерживать MPLS. Функциональная модель сети VPN уровня сервера, поддерживаемая несколькими уровнями сервера описывается на рисунке 13.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, RAVLAT
MAZMUNINI MUVOFIQLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI
Joriy etish boshqarmasi

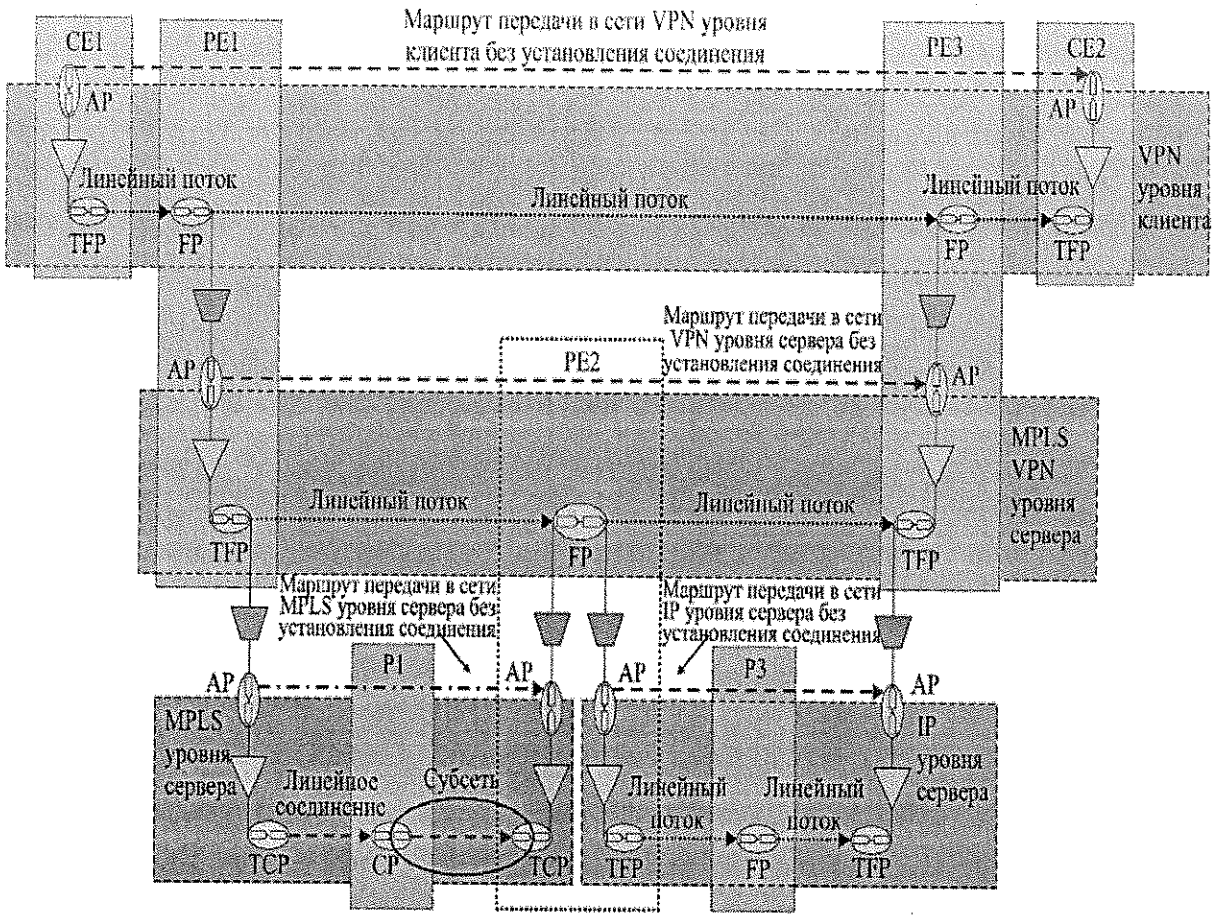


Рисунок 13 - Сеть VPN уровня сервера, поддерживаемая несколькими уровнями сервера

В этом примере функция адаптации источника сети MPLS уровня сервера преобразует CI MPLS сети VPN уровня сервера AI в сети MPLS уровня сервера, а функция адаптации приемника сети MPLS уровня сервера преобразует AI сети MPLS уровня сервера, в CI MPLS сети VPN уровня сервера. Функция адаптации источника сети IP уровня сервера преобразует CI MPLS сети VPN уровня сервера в AI сети IP уровня сервера, а функция адаптации приемника сети IP уровня сервера преобразует AI сети IP уровня сервера, в CI MPLS сети VPN уровня сервера.

5.7 Моделирование сети VPN с применением деления на части

Функциональные модели разработаны с применением многоуровневого подхода, разделив сеть на множество независимых сетей различных уровней, можно смоделировать взаимодействие клиент-сервер между сетями смежных уровней, завершения и взаимодействия.

Альтернативный способ моделирования – деление сети на части, он применяется для определения структуры сети в пределах сети одного уровня и административных/маршрутных границ между доменами сети, например, сетями, принадлежащими различным операторам. Деление поз-

© O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

воляет разделить подсеть одного уровня на несколько содержащихся в ней подсетей и каналы связи между ними. Такое деление должно продолжаться до тех пор, пока не будет достигнут предел рекурсии, то есть, пока отдельные подсети не будут состоять из одного сетевого элемента. Деление на части приведено на рисунке 14.

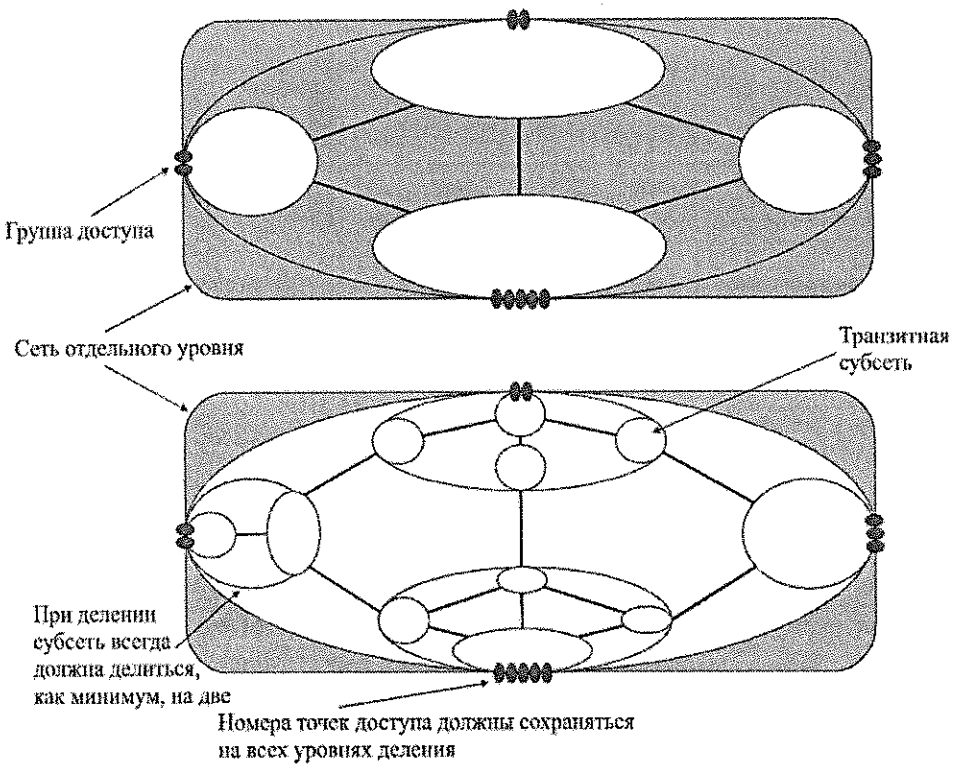


Рисунок 14 -Деление подсетей в пределах одного уровня сети

В ходе деления сети на части, число точек потока/соединения в наибольшей подсети остается неизменным, при этом выявляются точки соединения, являющиеся внутренними на следующем уровне деления. Соединение подсети представляет собой гибкое звено между входами и выходами соединения (точками доступа источника/приемника или точками потока/соединения). Это позволяет любой вход соединить с любым выходом.

Эта модель достаточна для сетей общего пользования, где все ресурсы можно считать доступными для использования. Она непригодна для виртуальных частных сетей. Причина, возможность установления соединения между входами и выходами в подсети/домене потока ограничена только теми входами и выходами, которые принадлежат одной сети VPN.

Для моделирования сети VPN с применением подхода на основе деления, используются конструктивные единицы. Единицы FDFr/SNC разбиваются на фрагменты при помощи выделения в различные группы их входов и выходов. Возможность установления соединения ограничена, оно должно быть установлено только между членами одной группы. Такая

группа может быть сетью VLAN на мосту Ethernet или сетью VPN в подсети или домене потока. Надо учитывать, что фрагмент не содержит точек потока; они связаны с доменом потока. Единица FDFr/SNC носит метку, определенную в зависимости от соединенного с ней сетевого уровня и номера фрагмента, или в зависимости от группирования точек потока в определенный фрагмент, например, идентификатор сети VLAN.

Пример сети, в которой используются сети VLAN для обеспечения изоляции сети VPN, приведен на рисунке 15.

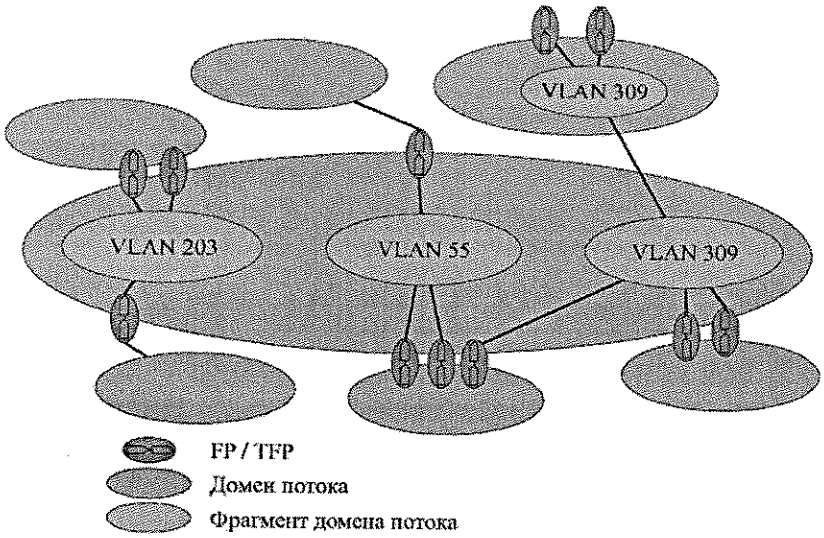


Рисунок 15 - Пример функциональной модели деления сети VPN

FDFr одного домена потока связан с FDFr в другом домене потока при помощи компонента – соединительной линии. Аналогично, SNC в одной подсети связан с SNC в другой подсети через соединительную линию. Это должно разделять или объединять элементы конструкции в соответствии с моделью подсети. Таким образом, модель является очень гибкой и позволяет изображать структуру VPN на любом уровне деления подсети.

5.8 VPN уровня равноправного взаимодействия

На рисунке 16 показана физическая топология VPN уровня равноправного взаимодействия. В этом примере «облако» сети изображает область совместно используемой сети, серая линия изображает VPN соединение P2P. Изоляция сети VPN должна быть обеспечена с использованием одного из подходов, определенных в разделе VPN равноправного взаимодействия.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH V.
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH MASHBARMAGI

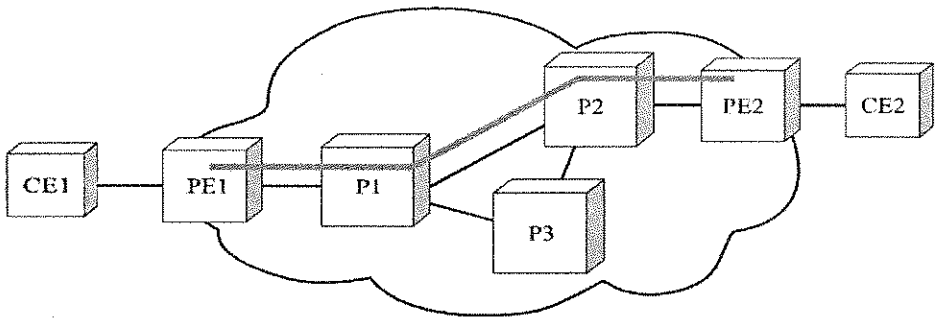


Рисунок 16 - Пример физической топологии VPN уровня равноправного взаимодействия

На рисунке 17 приведен уровень VPN и уровень сервера между точками PE. Уровень сервера работает CO, он также может работать CL.

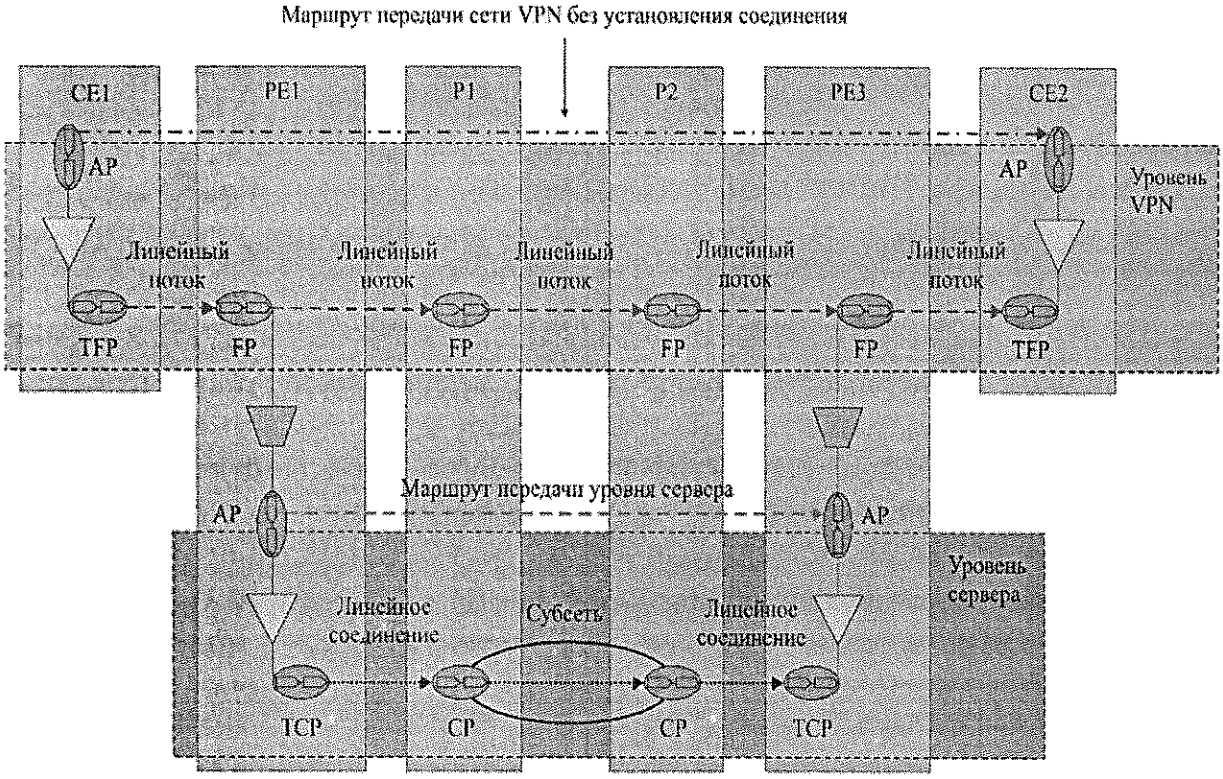


Рисунок 17 - Модель уровня для одного VPN уровня

В соответствии с рисунком 17, все узлы сети принадлежат уровню VPN и, они должны быть способны перенаправлять пакеты в нужном направлении, используя информацию из заголовков пакетов VPN соответствующего уровня. Многоуровневая модель не предоставляет столько информации, сколько предоставляется в том случае, когда она используется для сети VPN клиент-сервер. Формат представления на рисунке 16 не дает сведений о том, где начинается сеть VPN, и где она заканчивается. Одним из способов ввести эту информацию является расширение функций адаптации в сети VPN/уровня сервера. На рисунке 18 приведены два различных

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

примера функций адаптации сети VPN/уровня сервера, одна из которых использует метки IPsec, а другая – метки Ethernet VLAN.

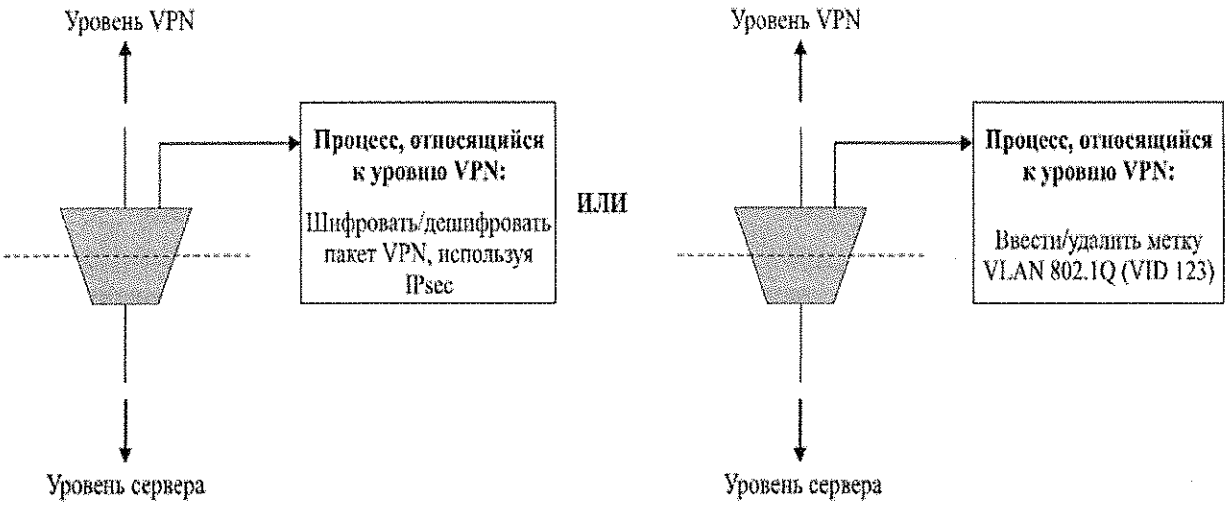


Рисунок 18 - Расширение функций адаптации в сети VPN/на уровне сервера

В VPN уровня равноправного взаимодействия используется концепция деления, приведенная в 5.7. Способ деления приведен на рисунке 19.

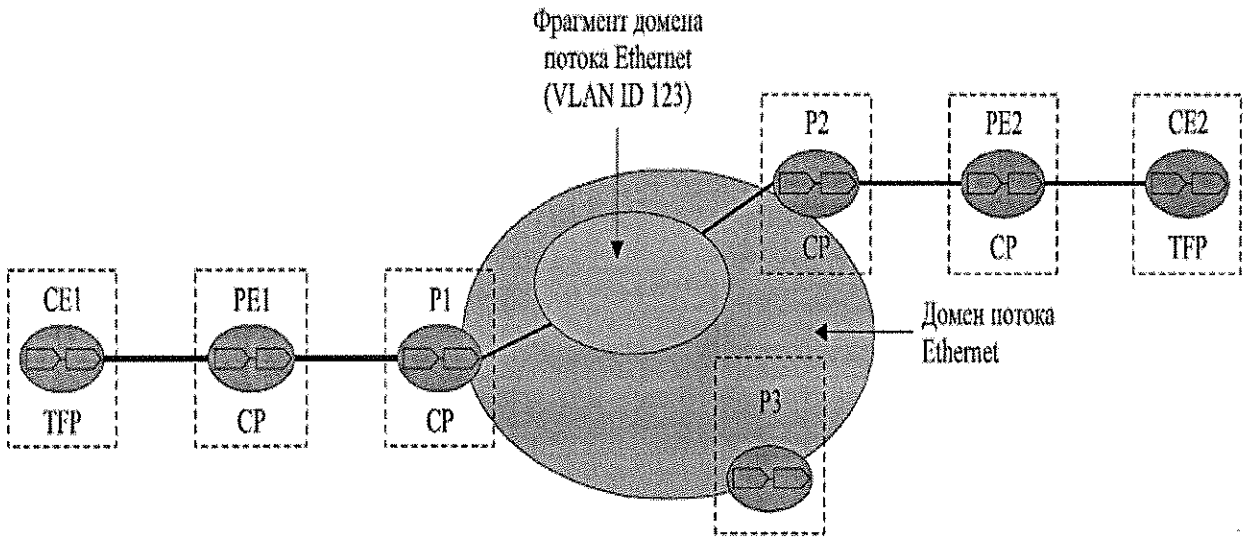


Рисунок 19 - Моделирование VPN уровня равноправного взаимодействия с использованием деления

На рисунке 19 приведена топология сети VPN равноправного взаимодействия, а также показана соответствующая VLAN (123), но не содержится сведений о том, где начинается сеть VPN, и где она заканчивается, т. е. где вводятся/удаляются VLAN метки. Согласно рисунку 19 узлы P1 и P2 входят в состав VLAN (123), но, несмотря на то, что PE1 и PE2 являются

© ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

точками начала/окончания для сети VPN, эта модель не дает такой информации. Однако, эту информацию можно получить, введя в модель деления функций адаптации сети VPN/уровня сервера и расширяя обработку, относящуюся к данному уровню VPN (в соответствии с рисунком 18).

6 Требования к поддержке VPN топологии

6.1 Топологии полносвязной ячеистой сети VPN

Соединение между сайтами VPN должно быт обеспечено с установлением маршрута VPN уровня сервера или уровня равноправного взаимодействия. Топология уровня n зависит от топологии, обеспечиваемой маршрутами уровня сервера на уровне n–1. После установления маршрутов в сети VPN уровня сервера или уровня равноправного взаимодействия, если технологией передачи в сети VPN уровня клиента или уровня равноправного взаимодействия является коммутация пакетов, то можно сократить топологию сети VPN, ограничив возможности соединения между определенными сайтами VPN.

Одним из способов ограничения возможностей соединения между составными частями VPN является управление распределением маршрутов передачи в сети VPN уровня клиента. Существует еще один метод ограничения возможностей соединения – фильтрация пакетов. Тремя основными топологиями VPN является – топологии полносвязной ячеистой сети VPN, топологии частичной ячеистой сети VPN и топологи и звездообразной сети VPN, они описаны в данном пункте, а также в 6.2 и 6.3.

В топологии полносвязной ячеистой сети VPN каждый сайт сети VPN имеет маршрут/соединение с каждым другим сайтом сети VPN, как приведено на рисунке 20.

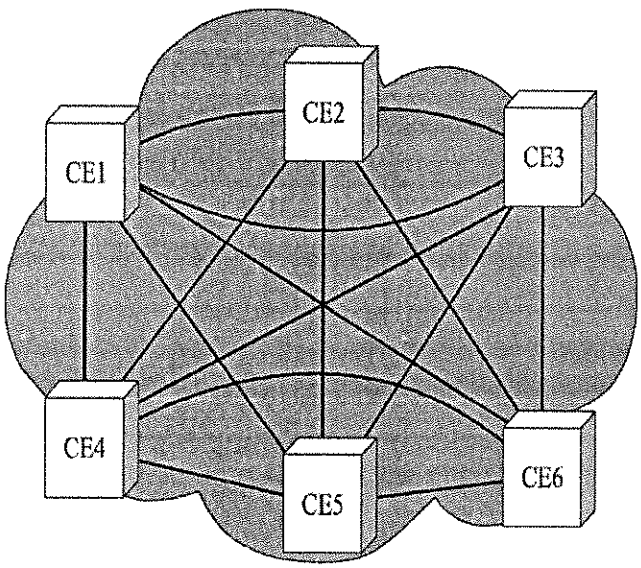


Рисунок 20 - Пример топологии полносвязной ячеистой сети VPN

STANDARTLASHTIRISH, RAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Топология полносвязной ячеистой сети VPN обеспечивает полную избыточность и может обеспечить эффективное использование сети и хорошие качественные показатели, поскольку сайты сети VPN используют для передачи данных между собой кратчайшие/наилучшие маршруты/пути. Недостаток подхода топологии полносвязной ячеистой сети в том, что полносвязная ячеистая сеть очень дорога в реализации, это зависит от применяемых режимов/технологий сети VPN. Другой недостаток, с увеличением числа сайтов сети, полностью построенной по топологии полносвязной ячеистой сети VPN, пропорционально увеличивается число соединений/маршрутов и общих границ плоскости управления (число соединений в полно связной ячеистой сети равно n(n–1)/2, где n – число сайтов сети VPN).

Поддержка большого числа соединений/маршрутов и соседних участков плоскости управления усложняет проблемы масштабирования из-за увеличения требуемых ресурсов пропускной способности и вычислительной мощности CPU.

6.2 Топологии частичной ячеистой сети VPN

В топологии частичной ячеистой сети VPN сайты VPN имеют соединения/маршруты с некоторыми сайтами VPN, но не со всеми. Пример топологии частичной ячеистой сети приведен на рисунке 21.

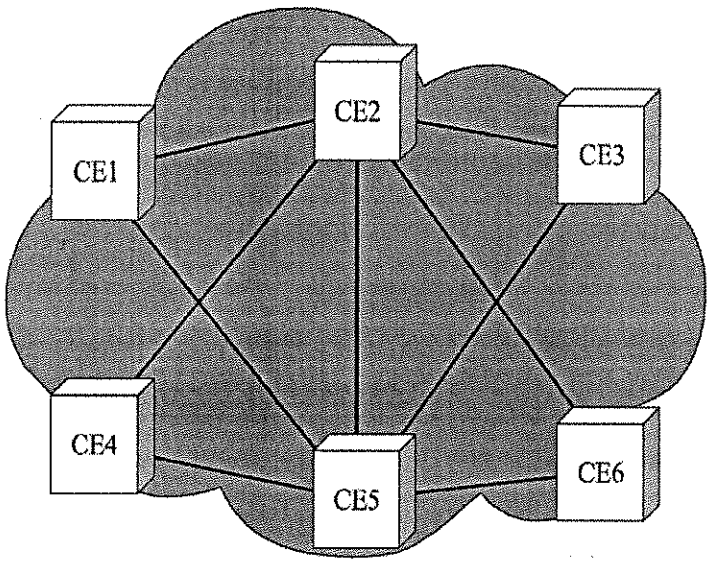


Рисунок 21 - Пример топологии частичной ячеистой сети VPN

Сайты сети VPN могут связываться с теми сайтами сети VPN, с которыми они не имеют прямых маршрутов/соединений, при помощи ретрансляции через транзитные сайты VPN.В других случаях при отсутствии у сайтов VPN прямых маршрутов/соединений с другими сайтами, связь между ними не может быть установлена. Возможность соединения между узлами, не имеющими между собой прямых маршрутов или соединений,

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

зависит от наличия соответствующих маршрутов в сети VPN уровня сервера или уровня равноправного взаимодействия и от ограничений, присущих определенной технологии (например, правил маршрутизации или параметров фильтров пакетов).

Топологии частичной ячеистой сети имеют более высокую степень масштабируемости, чем топологии полносвязной ячеистой сети, поскольку в ней уменьшены потребности в ресурсах пропускной способности и вычислительной мощности CPU, это сделано за счет снижения оптимальности маршрутизации и эффективности использования сети. Избыточность сети также уменьшена, несмотря на то, что частичные ячеистые сети, как правило, проектируются так, что избыточные маршруты/соединения используются там, где они более всего необходимы.

Например, на рисунке 21 CE узлы CE2 и CE5 должны быть основными узлами, а другие узлы CE могут быть пограничными узлами. В этой топологии пограничные узлы имеют избыточные маршруты/соединения для связи с центральной частью сети. Потребителям часто приходится использовать топологии частичной ячеистой сети из соображений стоимости и географических ограничений.

6.3 Топологии звездообразной сети VPN

В топологии звездообразной сети сайт VPN является либо центром, либо одним из лучей «звезды», образующей соединения для конкретной сети VPN. Все лучи в тополоти и звездообразной сети имеют прямые маршруты/соединения с центральным узлом, но не имеют маршрутов/соединений между собой. На рисунке 22 приведен пример топологии звездообразной сети, в которой узел CE2 является центральным, а все остальные узлы CE – лучами.

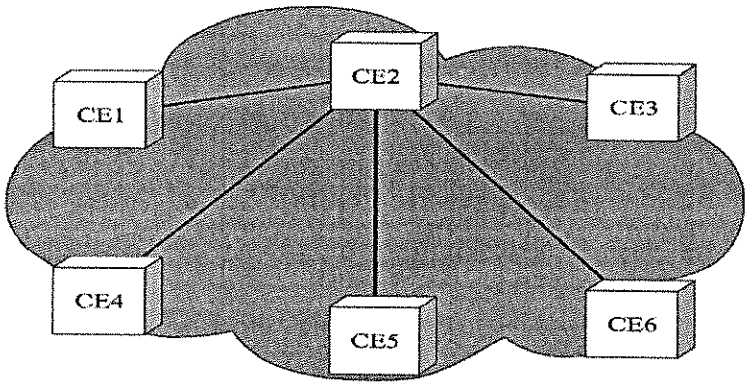


Рисунок 22 -Пример топологии звездообразной сети VPN

Центральный узел может быть сконфигурирован как транзитный узел, при этом лучи могут связываться друг с другом через центральный

O ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

узел. В других случаях, связь между узлами в лучах звезды может не быть допустимой. Наиболее широко топология звездообразной сети используется для соединения офисов со штаб-квартирой корпорации. Применение топологии звездообразной сети позволяет использовать централизованные сетевые ресурсы (*например, доступ в Интернет, защитное программное обеспечение, серверы электронной почты*), что может обеспечить снижение расходов по сравнению с подходом на основе распределенных сетевых ресурсов.

7 Требования по качеству обслуживания в VPN

7.1 Сети с коммутацией каналов

В сетях CO и с коммутацией каналов маршрут, построенный на основе физических линий, длин оптических волн, VC SDH/SONET или временных слотов TDM, формируется и выделяется для одного-единственного соединения между точками доступа сети на все время существования соединения. Когда запрашивается новое соединение, сеть должна принять решение о том, устанавливать ли это соединение, и, если устанавливать, то, как обеспечить его маршрутизацию в сети, и какие ресурсы зарезервировать для этого соединения. Механизмы CAC используются для создания соединения, если имеется необходимая пропускная способность, или для отказа в создании соединения, если пропускная способность, запрошенная для создания соединения, превышает имеющуюся в наличии пропускную способность.

Данные передаются по сети с постоянной скоростью и точно в том же порядке, в каком они были переданы. Соединения могут устанавливаться вручную с использованием статического выделения ресурсов или динамически, с использованием механизмов сигнализации или инструментов автоматического выделения ресурсов. Возможность установления новых соединений должна зависеть от наличия в сети свободной емкости. Если соединение установлено, то доставка данных по этому соединению гарантирована.

В сетях CO-CS задержка зависит от расстояния передачи. Задержка коммутации на узлах сетей CO-CS мала по сравнению с задержкой передачи сигнала.

7.2 Сети с коммутацией пакетов

7.2.1 Общее назначение сети с коммутацией пакетов

В сетях с коммутацией пакетов пакеты передаются в соответствии с данными в заголовке пакета. Коммутация пакетов реализует соединение, эффективно используя сетевые ресурсы, обеспечивая их совместное использование многими пользователями. Способ передачи пакетов в потоках или в соединениях можно описать набором параметров, которые называ-

O‘ZBEKISTON MILLIY STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

ются дескрипторами трафика. Примерами дескрипторов трафика являются средняя скорость передачи пакета/бита, максимальная длина импульса/размер пакета и вероятность доставки пакета в течение фиксированного интервала времени.

Требования пользователя к качеству часто выражаются в единицах приемлемости потери пакета, задержки или дрожания.

Для регулирования объема трафика, вводимого в сеть, могут применяться механизмы формирования трафика, они работают на базе очереди/потока на одно соединение или на один интерфейс.

Перегрузка в сетях с коммутацией пакетов может возникнуть, если объем трафика превышает возможности передачи сетевого элемента и пропускную способность сети. Когда сеть перегружается, пакеты могут храниться в буфере, что приводит к задержкам, или могут отбрасываться.

В сетях с коммутацией пакетов задержка зависит от расстояния передачи, связанного с нижележащим физическим уровнем сервера, и множества других факторов на уровне коммутации пакетов. Факторы, которые вносят задержку, это – размер пакета, скорости в канале, задержка на один пролет передачи и число пролетов.

В сетях с коммутацией пакетов необходимо управление приоритетами для того, чтобы гарантировать разные уровни QoS. Управление приоритетами реализуется за счет применения на каждом интерфейсе отдельных очередей, разделенных по соединениям, по потокам и по классам QoS и за счет регулирования приоритета в каждой очереди. Для распределения пакетов между этими очередями в соответствии с определенными правилами используются механизмы, регулирующие время передачи пакетов.

7.2.2 Сети с установлением соединения и с коммутацией пакетов

В сетях CO и с коммутацией пакетов соединения устанавливаются и поддерживаются до тех пор, пока не пропадает необходимость в этом соединении того, передаются ли по нему данные или нет. В сетях CO и с коммутацией каналов соединения могут устанавливаться вручную, с использованием системы управления или протокола сигнализации. Текущее состояние сети может быть определено путем контроля использования сетевых ресурсов и/или определения характеристик уже установленных соединений.

Механизмы CAC могут использоваться для сохранения пиковой пропускной способности, требуемого соединения для источников трафика с CBR.

В сети CO-PS, CBR задержки на один пролет остается постоянной и, можно рассчитать/гарантировать задержку/дрожание. Однако, если спрос на услуги намного выше предложения, и использование сети увеличивается на перегруженных узлах, пакеты будут задерживаться/теряться из-за буферизации или отбрасывания избыточного трафика. Несмотря на это величина задержки на пролет становится переменной, другие факторы, ско-

O'ZBEKISTON ALOQA VA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

рости в канале, расстояние передачи/число пролетов остаются постоянными.

7.2.3 Сети без установления соединения с коммутацией пакетов

В сетях CL-PS соединение должно разрываться после того, как данные переданы, и его не существует до момента передачи или приема следующей информации. Состояние соединения не сохраняется, и следующие пакеты не обязательно будут передаваться по тому же самому маршруту или прибывать в том же порядке, в каком они были переданы.

Трафик передается с переменной скоростью, и ресурсы выделяются по схеме «первый пришел – первый обслужен».

В сетях CL-PS факторы, определяющие задержку, – размер пакета, скорости в канале, количество пролетов и задержка передачи на одном пролете являются переменными, особенно, когда используются средства равномерного распределения нагрузки. На границе сети применяются механизмы ограничения скорости/формирования трафика для ограничения объема трафика, входящего в сеть. Из-за природы трафика в сети CL-PS, где все связаны со всеми (и роста числа равноправных сетевых соединений), трудно предсказать, какая емкость будет использована для каждого соединения в сети CL-PS.

Для формирования матрицы трафика должны использоваться методы контроля трафика и методы моделирования, а показатели IGP должен быть отрегулированы для повышения степени использования линии связи, но из-за импульсного и непредсказуемого характера CL-PS трафика, наиболее простым/наиболее безопасным способом гарантировать предоставление услуги является наличие в сети избыточных ресурсов.

При наличии в сети избыточных ресурсов, из-за неопределенного характера трафика в сети CL, узлы/каналы сети CL-PS должен оказаться перегруженными, особенно в случае неисправности узла/канала или отказа в обслуживании. Влияние неисправности узла/канала не ограничивается трафиком, передаваемым через неисправный узел/канал, изменение маршрутизации может вызвать перегрузку на другом участке сети. Общепринятый подход борьбы с перегрузкой сети – формирование приоритетных для управления характеристиками передачи в зависимости от класса обслуживания, трафик с наивысшим приоритетом получает предпочтение в обработке по отношению к трафику с меньшим приоритетом. Это позволит провайдеру предложить пользователю несколько уровней обслуживания с соответствующими расценками. Недостаток подхода дифференцированного обслуживания заключается в том, что емкость может резервироваться только в виде общего объема и невозможно гарантировать доставку отдельных потоков в этом общем объеме.

Альтернативным подходом является использование архитектуры интегрированного обслуживания, в которой для резервирования емкости на сквозном маршруте используется RSVP, который сообщает о потребностях потока до начала передачи пакетов. В связи с этим емкость резервируется

O ‘ZBEKISTON ARXITEKTURA STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI

для каждого потока отдельно и обеспечивает гарантированную доставку отдельных потоков. Этот вариант повторяет модель CAC, используемую в сетях CO, где трафик не передается, пока не выполнены процедуры CAC для гарантии того, что сеть имеет достаточную емкость для передачи трафика. Главным недостатком этого подхода является то, что он добавляет заметную нагрузку по обработке RSVP на центральные маршрутизаторы, которая растет пропорционально числу потоков пакетов, для которых требуется резервирование ресурсов. Еще один подход, обеспечивающий резервирование ресурсов для отдельных потоков, – это применение потоковых маршрутизаторов. Потоковые маршрутизаторы поддерживают передачу отдельных потоков и принимают новый поток только тогда, когда для его передачи имеется достаточно ресурсов. Как и при подходе на основе RSVP, объем обработки растет с увеличением числа потоков.

8 Требования к функциям для создания VPN клиент-сервер

8.1 VPN уровня серверов

8.1.1 Основные этапы создания VPN уровня

При создании сети VPN клиент-сервер должен следует придерживаться строгого порядка выполняемых действий. Потоки/соединения VPN уровня клиента не могут быть установлены до установления потоков/соединений VPN уровня сервера. Точно также, потоки/соединения VPN уровня сервера не могут быть установлены, пока не установлены потоки/соединения уровня сервера. Этот порядок установления потоков/соединений определяется тем фактом, что топология уровня клиента определяется топологией, и такое положение дел сохраняется на все уровни вниз.

Имеется три основных этапа создания соединений VPN уровня сервера между элементами сети VPN уровня клиента:

1) определить элементы сети VPN и записать их данные;

2) рассчитать маршруты между элементами сети VPN уровня сервера;

3) установить соединения/туннели/сети VLAN между элементами VPN уровня сервера.

В таблице 4 описана каждая функция, необходимая для создания в VPN уровня сервера и поддержания его работы вместе с отдельными функциональными блоками.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, RAVLAT
RAZVITIYI MUVOFIQLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Таблица 4 -Функции VPN уровня сервера

Функции	Функциональные единицы	Сетевые элементы	Режим VPN уровня сервера
Определение элементов сети VPN	Определение элементов сети VPN (точки CP/FP VPN уровня клиента, принадлежащие одной VPN)	PE	Все
	Распространение/сбор данных об элементах сети VPN (включая присоединение, уход, доступность)	PE	Все
	Сохранение данных об элементах сети VPN	PE	Все
	Преобразование точек CP/FP сети VPN уровня клиента в точки AP сети VPN уровня сервера	PE	Все
Маршрутизация сети VPN уровня сервера	Распространение/сбор данных о возможности соединения/топологии/ресурсах VPN уровня сервера	PE,P	Все
	Сохранение данных о возможности соединения/топологии/ресурсах VPN уровня сервера	PE,P	Все
	Расчет наилучшего (их) маршрут(ов)а между точками AP сети VPN уровня сервера	PE,P	Все
Установление соединения/туннеля в сети VPN уровня сервера	Управление установлением соединений (CAC)	PE,P	Все
	Сообщение об успешном/безуспешном выполнении запроса соединения/туннеля	PE,P	Все
	Выделение и конфигурирование полей демультиплексирования VPN уровня сервера	PE,P	Все
	Распространение данных о соединении/туннеле, например, QoS, поля демультиплексирование, пропускная способность и т.д.	PE,P	Все

8.1.2 Определение элементов сети VPN

Для установления топологии сети VPN уровня сервера между узлами PE, необходимо определить какие узлы PE соединяются с узлами CE, принадлежащими конкретной сети VPN клиент-сервер. Эта функция должна

© O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BANDLIK
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

быть выполнена вручную человеком-оператором на основании знаний о топологии сети. Либо, эта функция может выполняться динамически через централизованный сервер/систему или распределенный протокол для того, чтобы автоматизировать/упростить процесс выделения ресурсов.

Для того чтобы поддержать динамическое определение элементов сети, узлы PE должны быть так сконфигурированы с идентификаторами VPN, чтобы было указано, что они соединены с одним или несколькими узлами CE, принадлежащими определенной сети VPN.

Примером централизованного сервера/системы для определения элементов сети является сервер аутентификации, служащий для распространения информации об элементах сети VPN, как части аутентификации клиента. Примером распределенного протокола является использование протокола BGP для сетей VPN, который использует адреса получателя маршрута как идентификаторы VPN для гарантии того, что узлы PE получают информацию только о тех сетях VPN, в состав которых они входят.

8.1.3 Маршрутизация в VPN уровня сервера

8.1.3.1 Необходимость маршрутизации

Уровень сервера между точками завершения источника/приемника сети VPN уровня сервера представляет собой однопролетное соединение/поток P2P, здесь маршрутизации не требуется, поскольку доступен только один маршрут. Если имеются альтернативные маршруты/пути в одну и ту же точку через различные промежуточные узлы, или если нижележащий уровень сервера формирует топологию P2MP, то в сети VPN уровня сервера должна быть выполнена маршрутизация для того, чтобы определить топологию и/или вычислить наилучший маршрут до пункта назначения.

В сетях CO сигнализация не может быть выполнена, пока не рассчитан маршрут/путь на данном уровне. В сетях CLпакет не может быть передан до тех пор, пока не рассчитан/сконфигурирован маршрут до пункта назначения. Для улучшения масштабирования используется сокращение сетевых адресов, совмещенное с иерархией домена маршрутизации. Основной формой сокращения адресов является использование маршрутов «по умолчанию», которые применяются как универсальный механизм для передачи пакета вне зависимости от адреса его пункта назначения.

Когда технология CL используется для радиовещательной передачи нет необходимости в предварительной конфигурации маршрута. Примером технологии, которая поддерживает такую возможность, является Ethernet. Радиовещательная передача - это копирование и передача пакетов с неизвестным адресом пункта назначения по всем имеющимся в топологии маршрутам уровня сервера (кроме того маршрута, откуда был получен пакет).

Для того чтобы многоуровневые сети охватывали множество узлов

STANDARTLASHTIRISH, RAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

на огромной географической территории, маршрутизация и иерархическая адресная структура являются основополагающими требованиями.

8.1.3.2 Примерные сетевые топологии, требующие маршрутизации

На рисунке 23 приведен пример сети, где имеется два альтернативных маршрута/пути до одного и того же пункта назначения (A и B).

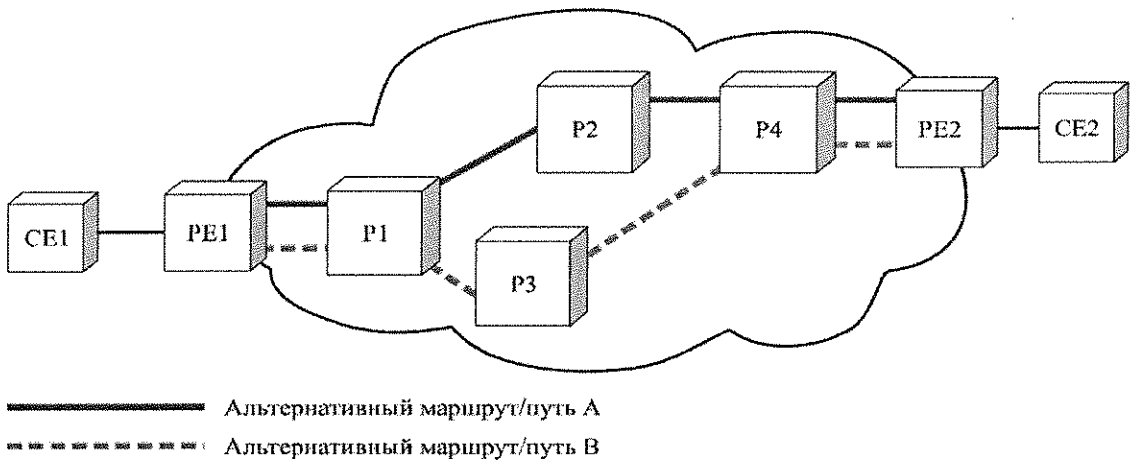


Рисунок 23 – Несколько маршрутов/путей до одного пункта назначения

Как видно из рисунка 23, маршрут A от CE1 до CE2 проходит через узлы PE1, P1, P2, P4 и PE2, тогда как маршрут B проходит через узлы PE1, P1, P3, P4 и PE2.

На рисунке 24 маршруты изображены в виде функциональной модели.

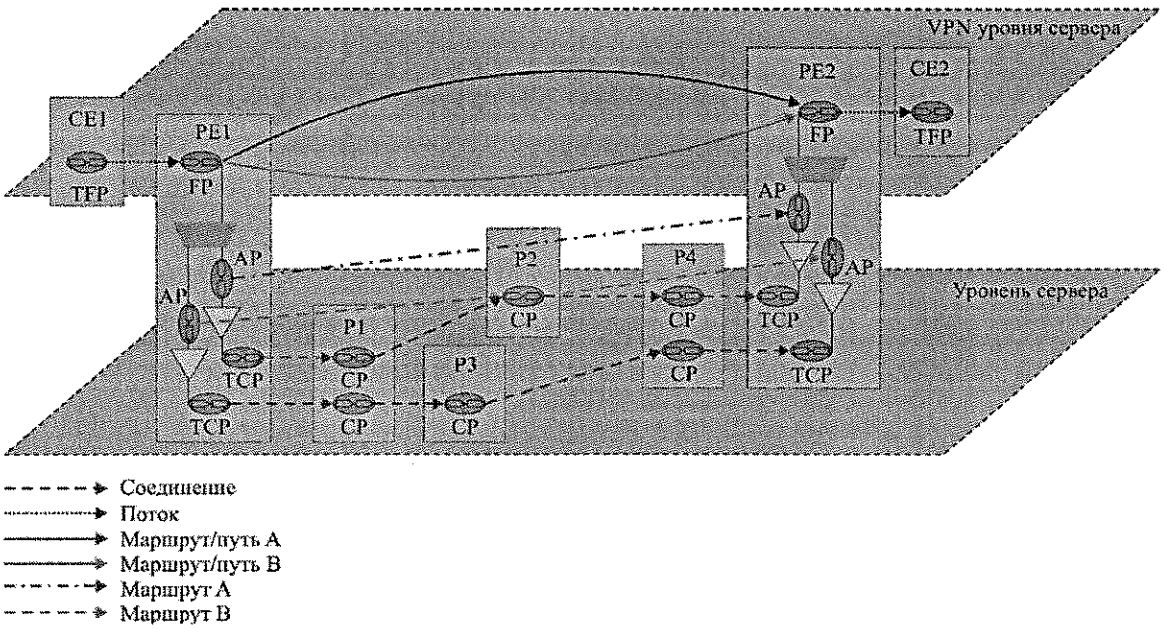


Рисунок 24 – Функциональная модель нескольких маршрутов/путей

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

На рисунке 24 показано два альтернативных маршрута на уровне сервера (A и B), которые могут использоваться сетью VPN уровня сервера.

На основании маршрутов, рассчитанных функцией маршрутизация в сети VPN уровня сервера, будет выбран один из маршрутов уровня сервера, чтобы передать поток в сети VPN уровня сервера между TFP источника сети VPN уровня сервера, расположенной в CE1, и TFP приемника, расположенной в CE2.

На рисунке 25 показано, когда на уровне сервера обеспечивается соединение P2MP от CE1 (источник) до CE2, CE3 и CE4 (разветвленные приемники в топологии P2MP).

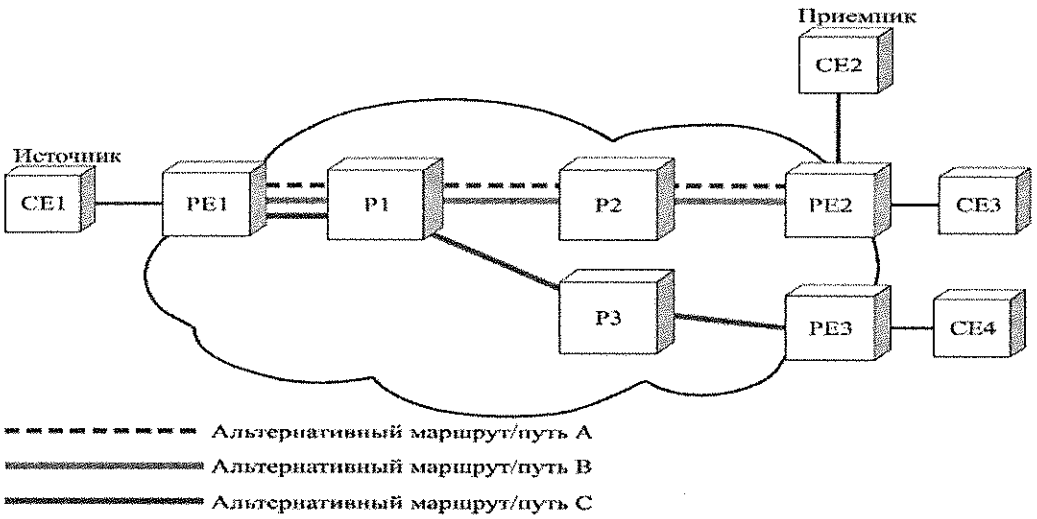


Рисунок 25 – Топология P2MP на уровне сервера

Сеть, изображенная на рисунке 25, приведена на рисунке 26 как функциональная модель.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, MAVLAI
NAZORATINI MUVOFIQLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

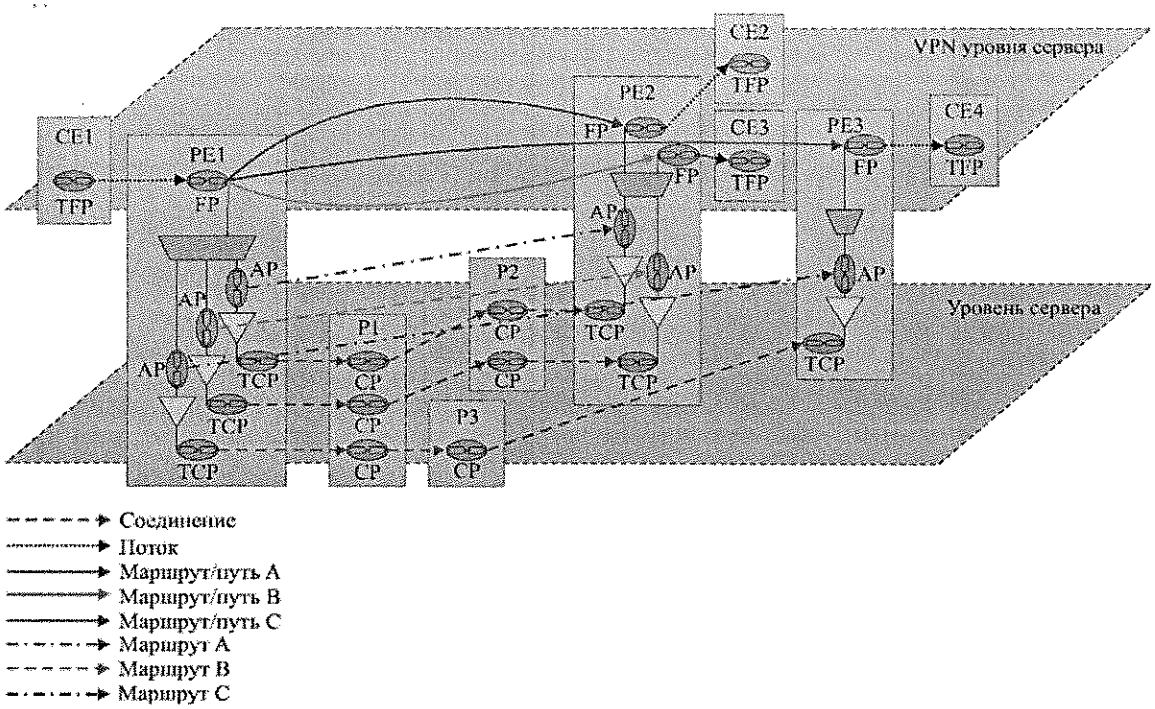


Рисунок 26 - Функциональная модель топологии P2MP на уровне сервера

Здесь CE1 – источник, CE1 должен знать каков путь до CE2, а CE2 – приемник для определенного потока в сети VPN уровня сервера.

Маршруты/пути в сети VPN уровня сервера, показанные на рисунке 26, поддерживаются маршрутами P2P на нижележащем уровне сервера, в топологии P2MP существует только один путь от TFP источника до TFP каждого разветвленного приемника. Это означает, что функция маршрутизации требуется только для определения топологии, она не требуется для расчета маршрута. После определения топологии, потоки от CE1 в направлении CE2 будут использовать маршрут/путь A, поддерживаемый маршрутом A на уровне сервера.

8.1.3.3 Альтернативные способы маршрутизации

Когда необходима маршрутизация, оператор должен выполнить маршрутизацию вручную и вычислять маршруты по сети на основании известной топологии сети и информации об использовании ресурсов. Одним из примеров ручного выполнения маршрутизации является конфигурирование двусторонних узлов CE.

Если для выполнения функции маршрутизации используется NMS, система должна определить топологию сети, запрашивая или собирая информацию о достижимости/топологии/ресурсах, а затем использовать эту информацию для расчета маршрутов и доставки информации маршрутизации на узлы сети. Одним из видов выполнения маршрутизация при помощи NMS, является установление P2P соединений на SDH уровне сети. До того как соединение может быть установлено, NMS должна сначала рас-

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

считать наилучший(е) маршрут(ы) в сети.

Если для выполнения маршрутизации используется динамический протокол маршрутизации, при помощи этого протокола информация о достижимости/топологии/ресурсах передается по сети на каждый узел и используется для расчета наилучшего маршрута/пути до пункта назначения. Одним из видов динамического протокола маршрутизации является составная часть маршрутизации через PNNI.

Другой вид маршрутизации – RPR, в которой для определения топологии кольца используются сообщения о топологии. Когда узел принимает сообщение о топологии, он дополняет его MAC адрес и передает на следующий узел в кольце, в конце концов, пакет возвращается обратно к источнику с топологической картой (списком адресов) кольца.

Альтернативой динамическому протоколу маршрутизации в плоскости управления является выяснение адреса в плоскости данных, примером сетевой технологии, использующей такой режим работы, является Ethernet.

Ethernet использует структуру дерева и прозрачные мосты в плоскости данных для передачи пакетов в нужный пункт назначения без необходимости их передачи на все узлы/оконечные станции.

8.1.4 Сигнализация в сети VPN уровня сервера

В сети VPN сигнализацией называется обмен информацией, необходимой для создания CL туннелей и CO соединений. Требуемая информация включает в себя, поля мультиплексирования/демультиплексирования, QoS (задержка, дрожание), полоса пропускания, ключи шифрования и способность к восстановлению (резерв 1+1).

Отличий между туннелями и соединениями является, установления соединения до передачи данных всегда требуется сигнализация. Некоторые методы туннелирования также требуют сигнализации для передачи данных о параметрах туннеля до того, как будет передавать данные пользователя, другие методы, такие как программные/динамические GRE туннели и туннели IP-в-IP сигнализации не требуют. Эти методы туннелирования вводят пакет VPN уровня клиента внутрь заголовка пакета VPN уровня сервера на основании информации о местных правилах маршрутизации.

Промежуточные узлы, встречающиеся между завершающими точками источника/приемника туннеля, просматривают заголовок пакета VPN уровня сервера, чтобы определить, следует ли передавать этот пакет в направлении приемника VPN уровня сервера.

Заголовки VPN уровня клиента используются, когда пакет достигает PE пункта назначения, где расположен приемник VPN уровня сервера. Отметим также, что промежуточные узлы часто не будут иметь возможности выполнения какого-либо действия (маршрутизации) во внутренних заголовках VPN уровня клиента.

CAC выполняется во время установления соединения для определе-

O‘ZBEKISTON ALOQA VA
STANDARTLASHTIRISH, MAYDAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ния, имеется ли на нижележащем уровне сервера достаточная полоса пропускания для удовлетворения потребностей QoS уровня клиента. Дескрипторы трафика используются в процессе обмена сообщениями сигнализации уровня клиента для запроса необходимых ресурсов от нижележащего уровня сервера. Способность определить, какая пропускная способность имеется в наличии на уровне сервера, на основании запроса, поступившего с уровня клиента, означает, что функция CAC должна равноправно взаимодействовать в плоскости управления, как с уровнем клиента, так и с уровнем сервера.

Способы организации сигнализации в сети VPN уровня сервера:

- уровни сервера имеют конфигурацию CO-CS, функция CAC основывается на физическом объеме полосы пропускания, имеющемся в наличии на том сетевом уровне, где она запрашивается (свободные слоты времени для сетей TDM или свободные длины волн для WDM);

- уровни сервера имеют конфигурацию CO-PS, функция CAC основывается на свободном объеме полосы пропускания, не используемом для поддержания существующих соединений. Эти данные становятся доступными за счет сохранения информации о текущем состоянии каждого соединения на каждом узле для конкретного сетевого уровня.

В отличие от сетей CO-CS, доступная полоса пропускания ограничивается физической полосой пропускания, в сетях CO-PS на каждом узле в сети могут быть реализованы различные правила для каждого соединения для гарантии того, что каждое соединение передает/принимает только тот объем трафика, который был согласован вовремя установления соединения;

- уровни сервера имеют конфигурацию CL-PS, функция CAC может быть выполнена на основании данных о полосе пропускания, доступной на физическом/логическом интерфейсе, или об очередности/потоке/классе уровня обслуживания для данного соединения. Для сетей CO-PS, на каждом узле в сети должны быть реализованы правила, основанные на величине запрошенной полосы пропускания. В отличие от сетей CO-PS, для каждого соединения поддерживается информация о текущем состоянии, аналогичная информация в сетях CL. Если в VPN требуются четкое CAC и жесткие SLA, то должна использоваться сеть CO уровня сервера, а не сеть CL уровня сервера.

8.2 Конфигурация/аутентификация VPN уровня клиента

8.2.1 Основные функции уровня клиента

Функции, требуемые для установления соединения между узлами CE и PE в сети VPN уровня клиента, должны быть выполнены с использованием статического выделения ресурсов или с использованием динамических протоколов. Статическое выделение ресурсов должны быть выполнено вручную или с помощью автоматических систем управления сетью. Функциональные единицы в установление соединения сети VPN уровня клиента, показаны в таблице 5.

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI

Таблица 5 – Функции аутентификации и конфигурации VPN уровня клиента

Функция	Функциональные единицы	Сетевые элементы	Режим работы VPN уровня клиента
Аутентификация CE/пользователя, санкционирование доступа и расчеты	Аутентификация: идентификация CE/пользователя на основании параметров аутентификации, например, правильных имени пользователя и пароле	CE, PE	Все
	Санкционирование доступа: разрешение или отказ в доступе к ресурсам /услугам сети VPN уровня клиента	CE, PE	Все
	Выставление счетов: измерение использованных ресурсов/услуг	CE, PE	Все
Конфигурация элемента в сети VPN уровня клиента	Назначение и конфигурация адресов сети VPN уровня клиента для точек CP/FP и TCP/TFP в VPN уровня клиента	CE, PE	Все
	Назначение и конфигурация идентификаторов VPN для точек CP/FP одной и той же сети VPN уровня клиента	PE	Все
	Конфигурация профилей и правил работы VPN	CE, PE	CO-PS, CL-PS

8.2.2 Аутентификация CE/пользователя, санкционирование доступа и расчеты

Функция AAA управляет доступом к сети VPN уровня клиента, выполняет установленные правила, поддерживает контроль использования и предоставляет информацию, необходимую для выставления счетов за услуги VPN. Функции AAA должны выполняться устройством PE, которое соединяет CE с другим устройством или ими обоими.

8.2.3 Конфигурация элементов сети VPN уровня клиента

Во время формирования сети VPN уровня клиента сетевые элементы на стороне пользователя и на стороне провайдера сети должны быть сконфигурированы со следующими параметрами:

STANDARTLASHTIRISH, RAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

- адреса сети VPN уровня клиента;
- поля демультиплексирования сети VPN уровня клиента;
- идентификаторы VPN;
- профили/правила работы для каждой сети VPN.

Конфигурация должна быть выполнена в ходе аутентификации/разрешения доступа. После успешной аутентификации CE должен быть автоматически сконфигурирован с выделением конкретной полосы пропускания и профиля меток пакетов на основании данных, полученных от сервера аутентификации.

Адреса сети VPN уровня клиента, должны конфигурироваться в точках CP/FP на PE и в точках TCP/TFP или CP/FP на CE, это – адреса, принадлежащие сети VPN уровня клиента (IP адреса для IP сети VPN уровня клиента).

Поля демультиплексирования сети уровня клиента должны конфигурироваться только, если по одной и той же линии между CE и PE передаются сигналы множества VPN клиентов или используемая технология сети VPN уровня клиента всегда содержит поля демультиплексирования.

Идентификатор VPN – имя, используемое для идентификации конкретной сети VPN, и его необходимо назначать/конфигурировать, если требуется поддержка динамического подтверждения участия в VPN и сигнализации.

Идентификатор VPN должен быть статистически сконфигурирован на PE при помощи ручного/OSS выделения ресурсов или динамически (протокол RADIUS). Если идентификатор VPN должен использоваться для подтверждения участия/сигнализации, то он должен быть уникальным, как минимум, в пределах одного домена маршрутизации/сигнализации.

В устройстве CE, PE или в них обоих могут потребоваться профили и правила конфигурации каждой сети VPN уровня клиента с коммутацией пакетов. Примеры профилей и правил VPN, которые могут потребоваться для конфигурации в зависимости от услуги VPN, включают в себя:

- ограничение скорости/формирование трафика;
- установка меток на пакеты/классификация пакетов;
- выбор маршрута/соединения для сайтов с несколькими домашними сетями (основной, резервной).

8.3 Маршрутизация и сигнализация в VPN уровня клиента

8.3.1 Функции маршрутизации и сигнализации в VPN

В сетях VPN уровня сервера, маршрутизация в VPN уровня клиента требуется, когда между точками TCP/TFP источника и приемника существует несколько маршрутов или если маршруты сети VPN уровня сервера создают топологию P2MP на уровне клиента VPN.

Если сеть VPN уровня клиента работает с установлением соединений и вней поддерживается динамическое выделение ресурсов для VPN уровня клиента, то требуется сигнализация.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI

Маршруты VPN уровня сервера должны быть установлены до выполнения маршрутизации/сигнализации в сети VPN уровня клиента. Топология плоскости данных VPN уровня клиента основана на топологии нижележащих маршрутов сети VPN уровня сервера и невозможно выполнить расчет маршрута и установить соединение/туннель для передачи информации сигнализации до тех пор, пока не сформированы маршруты сети VPN уровня сервера.

Функции маршрутизации и сигнализации VPN уровня клиента с отдельными функциональными единицами описаны в таблице 6.

Таблица 6 – Функции маршрутизации и сигнализации VPN уровня клиента

Функция	Функциональные единицы	Сетевые элементы	Режим работы VPN уровня клиента
Маршрутизация VPN уровня клиента	Распространение/сбор данных о доступности/топологии/ресурсах сети VPN уровня клиента	CE, PE	Все
	Поддержание информации о доступности/топологии/ресурсах сети VPN уровня клиента	CE, PE	Все
	Расчет наилучшего маршрута между точками доступа VPN уровня клиента	CE, PE	Все
Сигнализация в туннелях/соединениях VPN уровня клиента	Управление установлением соединения	PE, P	CO-CS, CO-PS
	Сообщение об успешном/безуспешном выполнении запроса на установлении туннелях/соединения	PE, P	Все
	Назначение и конфигурация полей демультиплексирования VPN уровня клиента	PE, P	Все
	Распространение информации о соединении/туннеле VPN уровня клиента, (QoS, полях демультиплексирования, полосе пропускания)	PE, P	Все

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

8.3.2 Соединение «все-со-всеми» в VPN уровня клиента без установления соединения с коммутацией пакетов

Маршруты VPN уровня сервера образуют топологию полносвязной ячеистой сети «все-со-всеми» для сети CL-PS VPN уровня клиента с несколькими сайтами, узлы содержащие точки TFP/FP сети VPN уровня клиента должны принимать решения о дальнейшей передаче пакетов на основании адресной информации сети VPN уровня клиента.

Узлы CE и PE должны обмениваться информацией о маршрутизации в плоскости управления сети VPN уровня клиента, используя динамические протоколы маршрутизации, или статические маршруты должны конфигурироваться с использованием ручного или OSS выделения ресурсов.

Информация о маршрутизации для каждой сети VPN должна быть изолирована от информации о маршрутизации других сетей VPN. Необходимо обеспечить разделение передачи в VPN (гарантировать, пакеты не будут переданы на узлы, принадлежащие другой сети VPN) и разрешить перекрытие используемых адресных пространств сетей VPN уровня клиента. Этого можно достичь, используя физически разделенные или способом с логически/виртуально разделенными PE базами данных о маршрутизации.

8.3.3 Создание/разъединение динамических соединений в сети VPN уровня клиента по запросу

В большинстве случаев соединения CO-CS и CO-PS в VPN уровня клиента будут статически конфигурироваться путем ручного или OSS выделения ресурсов.

В динамическом установление соединения по запросу, между всеми точками CP и TCP и между узлами PE и CE должно выполняться равноправное взаимодействие в плоскости управления (маршрутизация и сигнализация) в сети VPN уровня клиента. Во время установления соединения должна выполняться функция CAC для определения того, имеется ли в наличии в VPN уровня сервера достаточная полоса пропускания для соединения в сети VPN уровня клиента. Это означает функция CAC должна равноправно взаимодействовать с плоскостями управления в сети VPN уровня сервера и в сети VPN уровня клиента. Если в сетях VPN уровня сервера и уровня клиента используются различные технологии, то равноправное взаимодействие в плоскости управления сетью должно иметь место между уровнями клиента и сервера сети VPN.

8.3.4 Управляемые пользователями соединения по запросу

Управляемые пользователями динамические соединения по запросу имеют полный контроль над узлом CE, позволяет создавать новые соединения VPN уровня клиента.

Пользователь может пожелать создать на короткий промежуток времени соединение по запросу для загрузки/перекачки большого файла (приложения или видео файла) или создать надежное соединение для ви-

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI

деоконференции.

Способность создавать новые соединения в сети VPN уровня клиента зависит от наличия маршрутов на уровне сервера между точками завершения источника и приемника.

Если маршрутов и свободной полосы пропускания не имеется, в установлении этих соединений должно быть отказано, либо должны быть установлены новые соединения/туннели сети VPN уровня сервера. Для того, чтобы создать новые соединения/туннели сети VPN уровня сервера или увеличить полосу пропускания для существующих соединений/туннелей, должна быть гарантия того, что имеется полоса пропускания на нижележащем уровне сервера а также должна быть выполнена функция CAC.

Если уровень сервера работает в режиме CL, то невозможно выполнить жесткую функцию CAC и, следовательно, для того, чтобы получить возможность установить новые туннели, сеть должна быть обеспечена избыточными ресурсами сети VPN уровня сервера.

Недостатком этого подхода является требование тщательного планирования сети и управления/контроля для гарантии, что существующие туннели в сети VPN уровня сервера не подвергаются никакому влиянию. Если нижележащий уровень сервера работает в режиме CO, то может быть выполнена жесткая функция CAC для создания новых соединений/туннелей сети VPN уровня сервера. Каждый запрос на соединение на уровне n влияет на полосу пропускания, доступную на уровне n–1. С приближением к нижнему уровню, повышается дробность полосы пропускания и время предоставления/удержания ресурсов для соединения. Если на сервере нижележащего уровня недостаточно емкости для создания нового соединения, в установлении соединения должно быть отказано. Должна быть предусмотрена полоса пропускания на уровне сервера как результат действий по планированию пропускной способности, включая моделирование сети и использование аналитической информации/прогнозирования.

8.3.5 Управляемые провайдером услуг соединения по запросу

Управляемые провайдером услуг динамические соединения по запросу относятся к сценарию, провайдер услуг руководит узлом CE и использует данные маршрутизации/сигнализации для динамического создания новых соединений в сети VPN уровня клиента.

Это позволяет провайдерам услуг создавать сквозные соединения в сети VPN уровня клиента, а не использовать статическую конфигурацию (ручное или OSS выделение ресурсов). Динамическое установление соединения используется когда две и более сетей ATM соединяются через центральную сеть MPLS, а PNNI должен использовать для создания/разъединения SPVC в сети VPN уровня клиента через маршруты MPLS в сети VPN уровня сервера.

В сети VPN уровня клиента и сервера, технологии уровня сервера могут быть различными. Должно обязательно быть обеспечено равноправ-

O‘ZBEKISTON RESPUBLIKASI STANDARTLASHTIRISH, BAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI ...

ное взаимодействие в плоскости управления.

Провайдер управляет и контролирует все происходящее в сети с установлением соединения/туннеля на различных уровнях в иерархии многоуровневой сети VPN.

Провайдер должен тщательно организовать планирование сети и контроль соединений на каждом уровне при помощи NMS, особенно, если управляющее подразделение компании, ответственное за управление сетью VPN уровня клиента, не является одновременно подразделением, ответственным за управление сетью VPN уровня сервера.

9 Требования к функциям для создания VPN равноправного взаимодействия

9.1 Этапы уровня равноправного взаимодействия

В сети VPN с равноправными пользователями необходимо выполнить три основных этапа по созданию соединений между участниками VPN в сети VPN уровня равноправного взаимодействия:

1) определить и аутентифицировать участников VPN и сохранить информацию о принадлежности сети VPN;

2) рассчитать маршруты между участниками VPN в сети VPN уровня равноправного взаимодействия;

3) сконфигурировать сетевые элементы сети VPN уровня равноправного взаимодействия для обеспечения изоляции VPN.

Каждая функция необходимая для обеспечения создания и дальнейшей эксплуатации сети VPN уровня равноправного взаимодействия, а также отдельные функциональные элементы подробно описаны в таблице 7.

Таблица 7 – Функции в сети VPN уровня сервера

Функция	Функциональные единицы	Сетевые элементы
Уточнение участников VPN	Определение участников VPN	CE/PE
	Распространение/сбор данных об участниках VPN (включая присоединение, уход, доступность)	CE/PE
	Поддержание информации об участниках VPN	CE/PE

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BANDLAT
MAZMUNINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

Окончание таблицы 7

Функция	Функциональные единицы	Сетевые элементы
Аутентификация, CE/пользователя, санкционирование доступа и расчеты (AAA)	Аутентификация: идентификация CE/пользователя на основании параметров аутентификации, правильных имени пользователя и пароле	CE, PE
	Санкционирование доступа: разрешение или отказ в доступе к ресурсам/услугам сети VPN уровня равноправного взаимодействия	CE, PE
	Выставление счетов: измерение использованных ресурсов/услуг	CE, PE
Маршрутизация в сети VPN равноправного взаимодействия	Распространение/сбор данных о доступности/топологии/ресурсах сети VPN уровня равноправного взаимодействия	CE, PE, P
	Поддержание информации о доступности/топологии/ресурсах сети VPN уровня равноправного взаимодействия	CE PE, P
	Расчет наилучшего маршрута между точками доступа VPN уровня равноправного взаимодействия	CE PE, P
Конфигурация сетевых элементов в VPN с равноправными пользователями	Конфигурация пакетных фильтров для каждой VPN	PE
	Конфигурация фильтров маршрутов для каждой VPN	PE
	Конфигурация и обмен ключами шифрование для каждой VPN/CE	ES, CE, PE
	Назначение и конфигурация идентификаторов (ID) сетей VLAN	CE, PE, P

9.2 Определение принадлежности сети VPN

В предоставленных пользователем сценариях услуг для сети VPN равноправного взаимодействия, где сеть VPN прозрачна для провайдера (например, IPsec сеть VPN через Интернет), до создания VPN необходимо, прежде всего, определить, какие CE принадлежат этой сети VPN. В предоставленных провайдером сценариях услуг для VPN (например, сети VPN, построенные на VLAN сетях Ethernet), провайдеру требуется уточнить, какие PE соединены с теми CE, которые являются участниками данной сети VPN. Уточнение может выполняться вручную оператором на основании известной топологии сети, или может выполняться динамически посред-

O ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ством централизованного сервера/системы или распределенного протокола.

9.3 Аутентификация CE/пользователя, санкционирование доступа и расчеты

Функция AAA для CE/пользователя используется в предоставленных провайдером сценариях для управления доступом к ресурсам сети VPN уровня равноправного взаимодействия. Функция AAA используется для обеспечения выполнения правил, поддержки контроля использования и для предоставления информации, необходимой для выставления пользователю счетов за услуги VPN.

9.4 Маршрутизация в сети VPN равноправного взаимодействия

В сети VPN между участниками существуют альтернативные маршруты/пути и должна быть выполнена маршрутизация на VPN уровне равноправного взаимодействия, чтобы определить топологию и/или рассчитать наилучший маршрут между участниками VPN.

Узлы CE, PE и P принадлежат сети VPN уровня равноправного взаимодействия, в расчете маршрут/пути участвуют все три узла. Функция маршрутизации должна выполняться вручную оператором или динамически, посредством централизованного сервера/системы или распределенного протокола маршрутизации.

9.5 Конфигурация сетевых элементов в сетях VPN равноправного взаимодействия

В сети VPN обеспечивается изоляция способом конфигурирования фильтров пакетов для каждой VPN в отдельности на совместно используемых узлах PE для обеспечения полной доступности между сайтами отдельного пользователя и сохранения изоляции между пользователями. Другой возможностью является использование выделенных узлов PE и конфигурация фильтров/маршрутов, узлы P содержат маршруты всех пользователей, узлы PE -только маршруты одного пользователя. Сортировка пакетов/маршрутов применима только в сценариях VPN, предоставленных провайдером и должна выполняться узлами PE.

Альтернативой применению фильтрации маршрутов/пакетов, где установлено соединение между пользователями является шифрование пакетов. Применение шифрования пакетов гарантирует, если пользователь принимает пакеты от VPN, участником которой он не является, что он не сможет получить данные, содержащиеся в пакете. Шифрование пакетов выполняется на узлах PE в сетях VPN, предоставленных провайдером и на узлах CE или на оконечных системах в сетях VPN, предоставленных пользователем.

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAYLAT
RAZORATINI MUVOFIQLASHTIRISHGA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

10 Требования к функциям VPN по эксплуатации, управлению и обслуживанию

10.1 Основные характеристики и функции OAM

Инструменты и функции по OAM необходимы для поддержания эффективности работы в широкомасштабных сетях.

Основными характеристиками сетевых соединений/потоков, обеспечиваемых при помощи функций OAM, являются:

- качество;
- целостность;
- достоверность.

В качестве замещения/замены отсутствующих функций на данном уровне не используются аналогичные функции/инструменты более высокого/более низкого уровней.

В таблице 8 приведены ключевые функции OAM и сетевые элементы должны поддерживать соответствующие функции.

Таблица 8 – Функции OAM в сетях VPN клиент-сервер

Функция	Функциональные единицы	Сетевые элементы
OAM в сети VPN уровня клиента	Управление обработкой/обнаружение отказов в VPN уровня клиента	CE и PE
	Контроль качества VPN уровня клиента	CE и PE
	Включение и отключение функций OAM в сети VPN уровня клиента	CE и PE
OAM в сети VPN уровня сервера	Управление обработкой/обнаружение отказов в VPN уровня сервера	PE и P
	Контроль качества VPN уровня сервера	PE и P
	Включение и отключение функций OAM в сети VPN уровня сервера	PE и P
OAM в сети VPN уровня равноправного взаимодействия	Управление обработкой/обнаружение отказов в VPN уровня равноправного взаимодействия	CE, PE, P
	Контроль качества VPN уровня равноправного взаимодействия	CE, PE, P
	Включение и отключение функций OAM в сети VPN уровня равноправного взаимодействия	CE, PE, P

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, RAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

10.2 Управление обработкой отказов

Управление обработкой отказов включает в себя обнаружение отказа, определение его местоположения, исправление и диагностическое тестирование по запросу. Дефекты могут быть обнаружены и обработаны в точке завершения приемника соединения/потока на том уровне сети, где они возникли.

Если своевременно не устранить дефекты, то они приводят к неоднозначному обозначению отказа, что увеличивает сложность эксплуатации и время, требуемое для устранения неисправности.

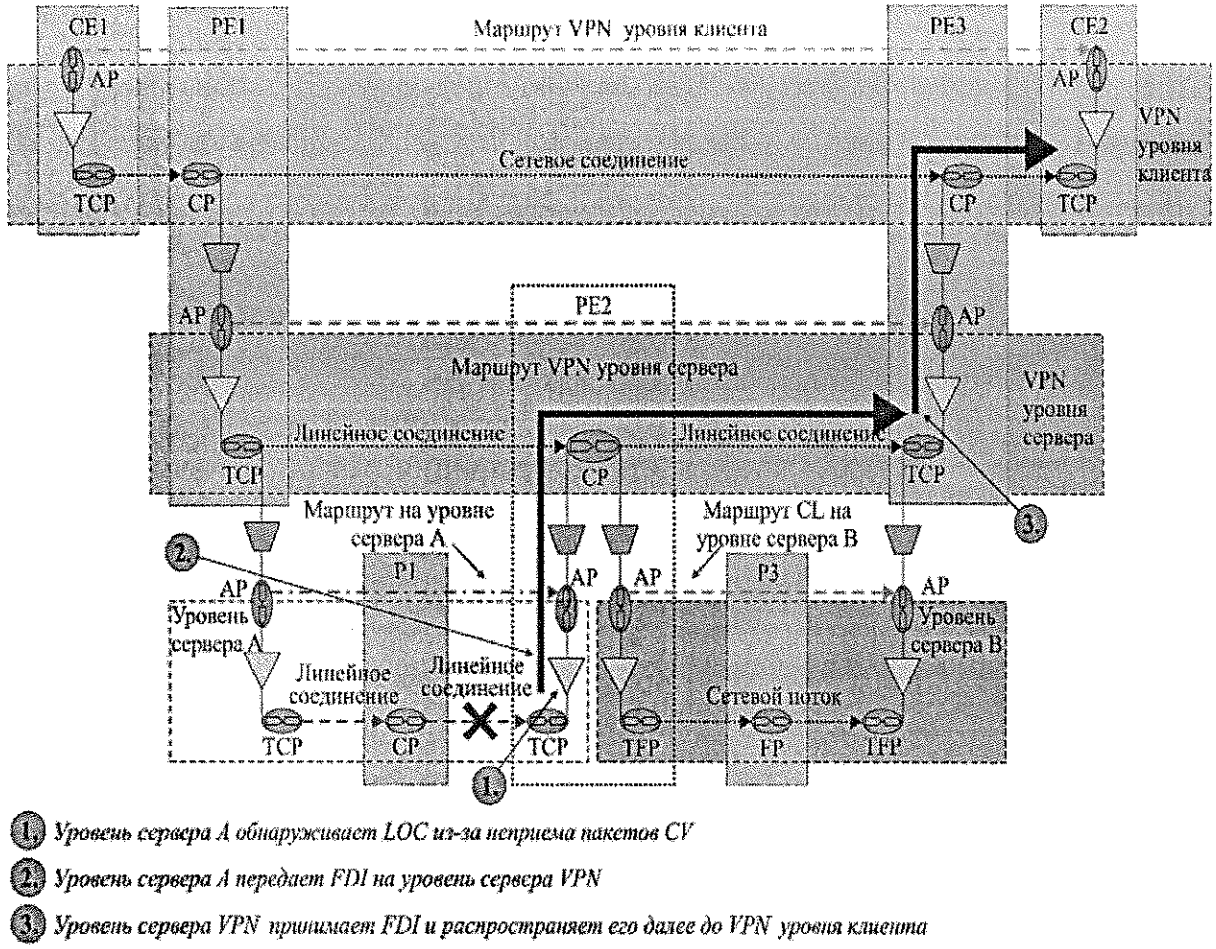
После обнаружения неисправности, создания и передачи сигналов оповещения в систему NMS, для предотвращения лавины аварийных сигналов в сетях уровня клиента, в сети уровня клиента должен быть передан сигнал FDI или AIS с применением соответствующего синтаксиса функций OAM.

Наиболее важный механизм обнаружения ошибки – использование CV, является общим требованием для всех трех режимов работы сети. Источник потока трафика должен определенно идентифицировать себя на приемнике.

Обнаружение местоположения ошибки – это ключевое требование для всех трех режимов работы сети, оно позволяет определить корень проблемы. Кроме исходной информации об ошибке, для определения местоположения ошибки могут использоваться инструменты диагностики по запросу.

Пример сценария ошибки в сети VPN уровня сервера с точки зрения функциональной перспективы описывается на рисунке 27.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, MAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
[illegible]



1. *Уровень сервера A обнаруживает LOC из-за неприема пакетов CV*
2. *Уровень сервера A передает FDI на уровень сервера VPN*
3. *Уровень сервера VPN принимает FDI и распространяет его далее до VPN уровня клиента*

Рисунок 27 – Распространение FDI на уровне клиент-сервер

Сигнал FDI распространяется до функции завершения приемника сети VPN уровня сервера, который передает сигнал FDI на уровень клиента. Эти действия продолжаются, пока сигнал не достигнет того уровня сети, который не поддерживает FDI. Приняв сигнал FDI, сеть VPN уровня клиента может передать его на вышестоящий уровень.

Единственным местом, где должен быть создан сигнал тревоги, это – точка завершения маршрута на том уровне сети, где обнаружена исходная ошибка. Если необходим контроль обоих направлений из одной точки, то в другом направлении может быть передан BDI.

Исправление неисправности применяется для восстановления работы и для управления процедурами, использующими избыточные ресурсы для замены вышедшего из строя оборудования или средств передачи.

Инструменты диагностического тестирования по запросу, используются для локализации неисправности, а также для проверки правильности соединения/конфигурации соединения/туннеля до их ввода в эксплуатацию. Проверка по шлейфу – один из примеров диагностического тестирования, в ходе которого создается петля для сетевого соединения от источника обратно к источнику через соединение или завершающую точку соединения.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

10.3 Управление рабочими характеристиками

PM используются для доступа и обслуживания сети, а также для документирования качественных показателей для пользователей. Если поддерживается несколько уровней класса обслуживания, то контроль качества должен выполняться для каждого класса обслуживания в отдельности. Контроль качества включает в себя обнаружение ухудшения характеристик сигнала, контроль запаздывания/дрожания и подсчет потерянных пакетов. Имеется несколько целей контроля качества, включая обслуживание SLA, поддержку формирования трафика, выставление счетов для конкретных пользователей, и восстановление обслуживания/переключение на резерв. Очень важно установить взаимосвязь между ошибками, доступностью и контролем качества.

Установлен определенный порядок, который кратко можно описать следующим образом:

1) режим работы сети определяет неисправности и требуемые функции OAM;

2) все неисправности должны быть определены в стандартизованных терминах критериев входа/выхода и последующих действиях;

3) сеть входит в состояние недоступности, неисправность или недопустимое ухудшение качества продолжается в течение нескольких последовательных секунд;

4) PM для целей SLA достоверен только, когда она находится в состоянии доступности и, соответственно PM для целей SLA должен быть приостановлен, когда сеть входит в состояние недоступности.

10.4 Включение/отключение OAM

В режиме CO-CS и CO-PS основные механизмы OAM по обнаружению/обработке отказов должны включаться/выключаться синхронно с установлением/разрывом маршрута, выполняется системами NMS/OSS или посредством сигнализации. Создание CV на источнике должно быть включено до включения обнаружения CV на приемнике, чтобы избежать появления бессмысленных сигналов тревоги.

Метод NMS/OSS или сигнализация, используемые для установления маршрута, также должны быть способны сообщить приемнику в точке завершения маршрута, какого идентификатора источника следует ожидать в плоскости данных конкретного маршрута, какому маршруту принадлежит принимаемый пакет OAM.

10.5 Дефекты, относящиеся к каждому сетевому режиму

10.5.1 Сети CL-PS

Дефекты транспортировки могут появиться в сети VPN уровня клиента или сервера и зависят от режима работы сети, к которому принадле-

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

жит технология данного уровня сети.

Виды возможных дефектов зависящих от режима работы:

– CL-PS: только разрывы;

– CO-PS: разрывы, перестановки и объединения;

– CO-CS: разрывы, перестановки (но только между похожими единицами).

Дефекты, вызванные неправильными соединениями в сетях CL-PS, проявиться не могут. Каждый пакет содержит и адрес источника и адрес пункта назначения, который содержит всю необходимую информацию для корректной маршрутизации пакета на каждом узле сети. В сети CL-PS возможен один-единственный дефект – разрыв сети (из-за неисправности функции маршрутизации, линии или узла).

В сетях CL-PS функция CV является составной частью заголовка пакета, каждый пакет содержит уникальный для данной сети адрес источника/пункта назначения. В сетях CL-PS данные управления и данные пользователя, передаются по одному пути передачи данных и, при неисправности в плоскости управления можно предположить, что соединение разорвано и данные пользователя также не могут быть переданы. Таким путем обнаруживаются и исправляются неисправности в сетях CL-PS.

10.5.2 Сети CO-PS

В CO-PS уникальные адреса, используемые функцией маршрутизации для расчета наилучшего для данного соединения маршрута/пути в сети, известны только в точках доступа данного уровня сети.

Когда маршрут/путь рассчитан, используется сигнализация для выделения и конфигурации входных/выходных полей мультиплексирования/демультиплексирования.

Поля мультиплексирования/демультиплексирования имеют только местное значение, одни и те же значения могут использоваться узлами восходящей/нисходящей связи как для одного и того же соединения, так и для различных соединений. Многократное использование полей мультиплексирования/демультиплексирования вместе с отсутствием уникальной системы сетевой адресации в плоскости данных означает, что в сетях CO-PS, кроме разрывов могут возникать дефекты перестановки и объединения. Поскольку пакеты в сетях CO-PS передаются асинхронно и не содержат уникальных для данной сети адресов источника/пункта назначения, необходимо добавить функцию CV, в виде передачи пакетов CV с определенной частотой. Необходимо тщательно подобрать скорость передачи пакетов CV для гарантии того, что не будет предпринято никаких ненужных действий при появлении ошибочных переходных импульсов.

10.5.3 Сети CO-CS

Сети CO-CS не страдают от дефектов объединения, в них поля мультиплексирования/демультиплексирование основаны на физических иден-

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

тификаторах линейных соединений времени/пространстве/частоте, передаваемых с постоянной скоростью.

В сети CO-CS, и в сетях CO-PS должна быть добавлена функция CV.

В сети кадры CO-CS передаются с постоянной скоростью, информация CV может передаваться в каждом кадре со скоростью передачи кадров. В сетях CO-CS управляющий трафик всегда передается через OOB и, функции OAM должны быть предоставлены в отдельности для каждого соединения в плоскости данных пользователя и в плоскости управления.

10.5.4 Разделение плоскости данных управления и плоскости данных пользователя

Данные управления и данные пользователя в сетях CO-PS могут передаваться в различных плоскостях данных, а также в режиме CO-CS эти действия предписываются во всех случаях.

Это разделение плоскости данных управления и плоскости данных пользователя имеет ряд преимуществ, обусловленных множеством причин и в частности, соображениями безопасности и стабильности работы сети, поскольку оно защищает плоскость управления от атак со стороны плоскости данных пользователя и от проблем перегрузки/блокировки, вызванных трафиком в плоскости пользователя.

Без наличия в плоскости данных OAM механизмов обнаружения источник будет продолжать передачу данных, создавая черную дыру для трафика, или нарушая безопасность данных пользователя за счет передачи трафика в ошибочный пункт назначения.

Для того чтобы однозначно определить, где возникла ошибка, и для выполнения правильных действий по ее устранению, как для соединений P2P, так и для соединений P2MP, функции OAM должны действовать в одном направлении. Кроме того, по возможности должен поддерживаться контроль неисправностей, выполняемый в обоих направлениях с одной стороны. Это особенно важно, когда пользователь или провайдер контролирует одну сторону соединения/туннеля, но не другую его сторону, например, в сценарии межпровайдерской VPN. когда стороны соединения P2P в сети VPN уровня клиента расположены в сетях различных провайдеров.

11 Требования к функциональным конвергенциям и сценариям услуг

11.1 Сценарии услуг в сети VPN клиент-сервер

Функции (механизмы/протоколы) необходимые для поддержания сети VPN клиент-сервер зависят от режимов работы сети клиент-сервер, а также от предлагаемых услуг VPN.

В таблицах С.1 и С.2 приведены сценарии услуг и механизмы/протоколы, которые могут использоваться для выполнения требуемых

STANDARTLASHTIRISH, BAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

функций.

11.2 Сценарии услуг в сети VPN равноправного взаимодействия

Функции, необходимые для поддержания сети VPN равноправного взаимодействия, зависят от технологии сети уровня равноправного взаимодействия и типа предоставляемых в сети VPN услуг. В таблице С.3 приведены примеры различных сценариев услуг и определены примерные механизмы/протоколы, которые используеюся для выполнения требуемых функций.

12 Требования безопасности к сети VPN

При проектировании сетей VPN безопасность должна быть рассмотрена в обязательном порядке для того, чтобы выбрать сетевые технологии и функциональные компоненты, которые соответствуют требованиям пользователя к безопасности сети. Существуют риски в отношении безопасности, присущие всем технологиям VPN, их причиной является совместное использование инфраструктуры для передачи трафика множеству пользователей. Должен быть также предотвращен дистанционный несанкционированный доступ к инфраструктуре сети (используя программные средства обеспечения безопасности для защиты от атак из Интернета).

В сети VPN клиент-сервер, сеть VPN уровня сервера должна поддерживать мультиплексирование/демультиплексирование в целях разделения плоскостей данных клиентов VPN нескольких уровней. Такое разделение трафика должно комбинироваться с эффективным контролем доступа к VPN на стороне сети, основанным на правилах, определенных пользователем VPN.

В сети VPN равноправного взаимодействия, чтобы поддерживать несколько сетей VPN в совместно используемом домене, используемая сетевая технология должна содержать средства для изоляции VPN.

Элементы CE должны быть способны взаимодействовать только с другими CE той же сети VPN, или расшифровывать только пакеты от других CE той же сети VPN.

Безопасность, в сети VPN клиент-сервер и в сети VPN равноправного взаимодействия, можно улучшить путем применения криптографии для шифрования блоков трафика пользователя/управления, и использовать аутентификацию для идентификации пользователей и сетевых узлов.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Приложение А
(рекомендуемое)

Расположение точек TCP/TFP в VPN уровня клиента

На рисунке А.1 показана физическая топология сети VPN клиент-сервер, которая использует две различные сети VPN уровня сервера – X и Y. Узлы PE1, P1 и P2 принадлежат сети VPN уровня сервера X, а узлы P3 и PE3 принадлежат сети VPN уровня сервера Y. Узел PE2 принадлежит обеим сетям уровня сервера и действует как шлюз между ними.

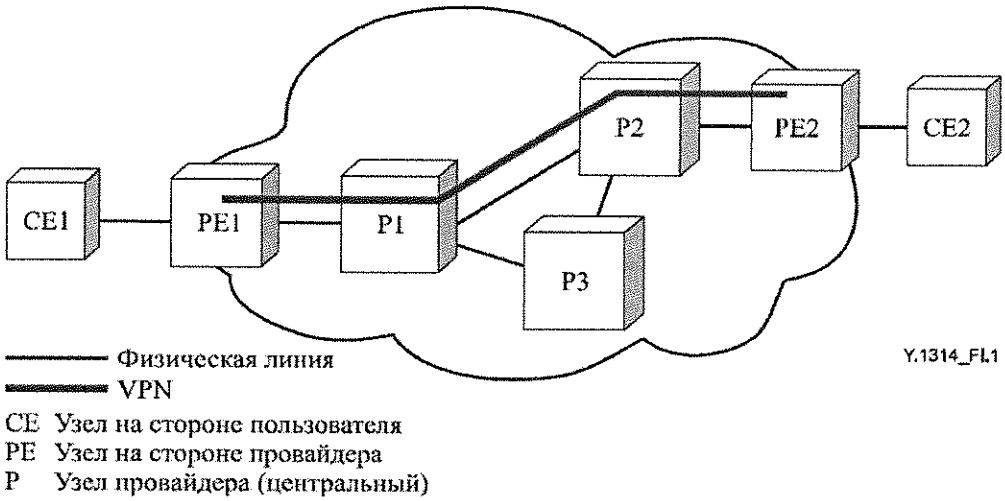


Рисунок А.1 – Физическая топология взаимодействия сетей VPN уровня сервера

На рисунке А.2 представлена функциональная модель, основанная на физической топологии, изображенной на рисунке А.1, в которой точки TFP располагаются в узлах CE.

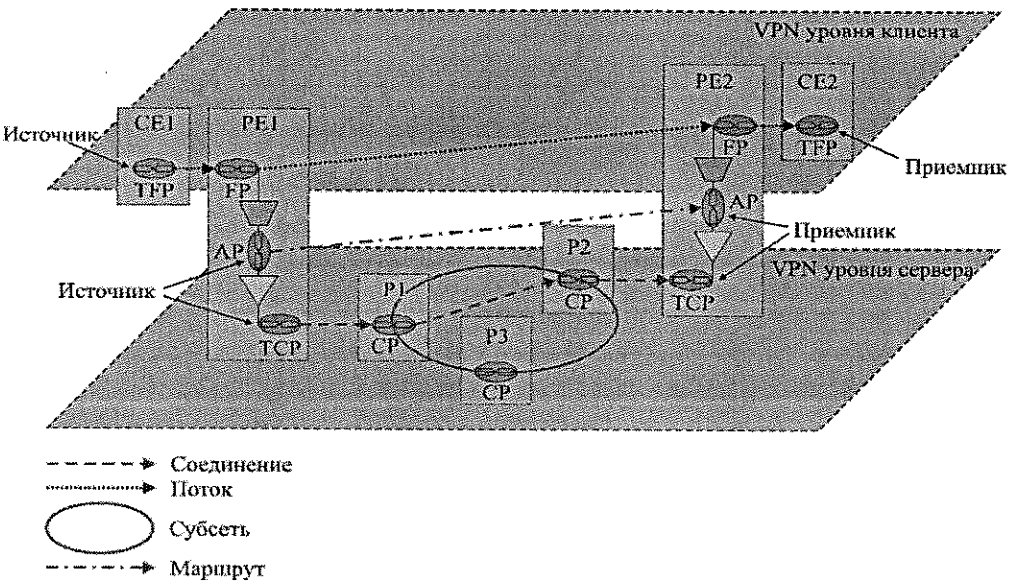


Рисунок А.2 – VPN уровня клиента – точки TFP расположены в узлах CE

O‘ZSTANDART AGENTLIGIDA
STANDARTLASHTIRISH, BAYLAY
AZORATINI MUVOFIQLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH RO‘YXATIDAN O‘TKAZILGAN

Узлы CE и P принадлежат сети VPN уровня клиента и сервера, узлы PE принадлежат обоим уровням. Точки TFP в сети VPN уровня клиента определяют, где поток P2P в сети VPN уровня клиента начинается и заканчивается, а точки FP определяют, через какие узлы PE проходит поток P2P.

Точки TFP в сети VPN уровня сервера определяют источник и приемник для соединения сети VPN уровня сервера, а точки FP определяют, через какие узлы P проходит поток. AP в сети VPN уровня сервера определяют источник/приемник для маршрута в сети VPN уровня сервера.

На рисунке А.3 показана физическая топология сети VPN клиент-сервер.

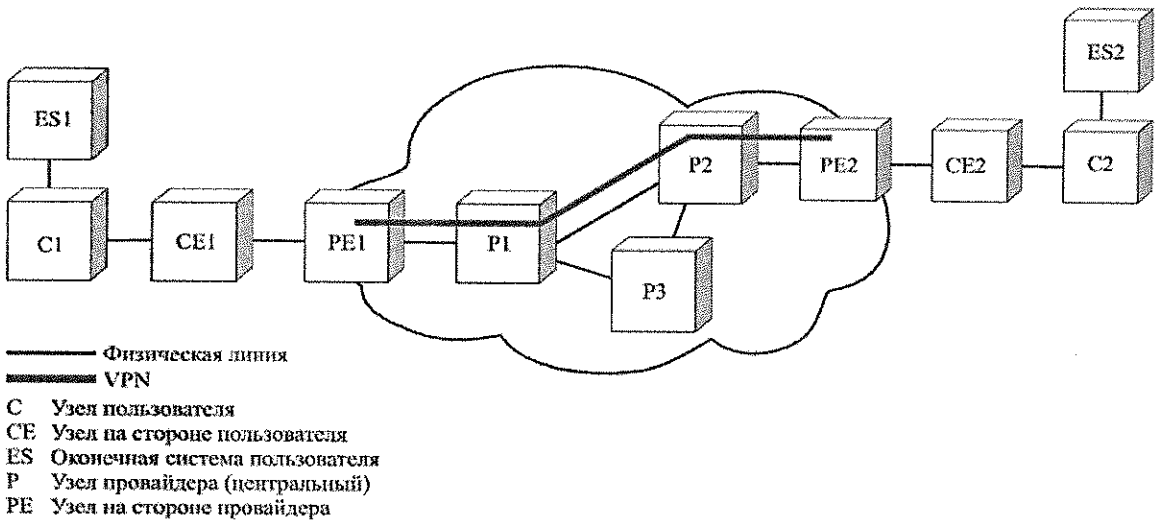


Рисунок А.3 – Физическая топология сети VPN клиент-сервер

Функциональная модель, основанная на физической сети изображенной на рисунке А.4 - точки TFP/TCP сети VPN уровня клиента расположены на оконечных системах/хостах, а не в CE.

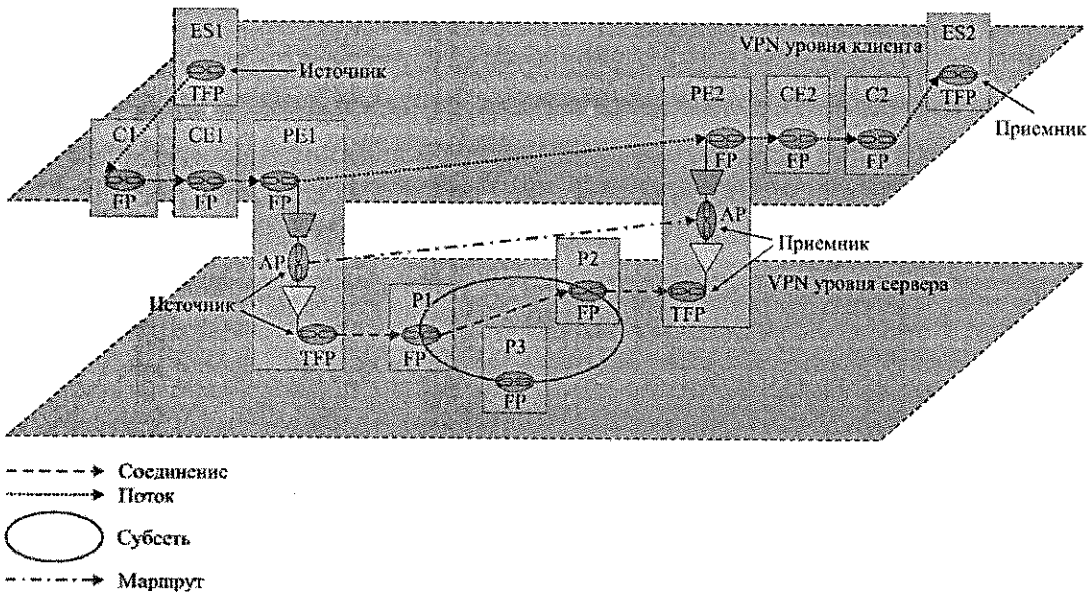


Рисунок А.4 – VPN уровня клиента – точки TFP расположены на оконечных системах/хостах.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Узлы C и CE, а также ES принадлежат сети VPN уровня клиента. Узлы PE принадлежат сетям VPN уровня сервера и уровня клиента, а узлы P принадлежат только сети VPN уровня сервера. Точки TFP в сети VPN уровня клиента определяют источник и приемник (ES1 и ES2) для потока в сети VPN уровня клиента, а точки FP определяют, через какие узлы C, CE и PE проходит поток.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

Приложение В
(рекомендуемое)

Сеть VPN клиент-сервер с несколькими VPN уровня сервера

На рисунке В.1 показана физическая топология сети VPN клиент-сервер, которая использует две различных сети VPN уровня сервера – X и Y. Узлы PE1, P1 и P2 принадлежат сети VPN уровня сервера X, а узлы P3 и PE3 принадлежат сети VPN уровня сервера Y. Узел PE2 принадлежит обеим сетям уровня сервера и действует как шлюз между ними.

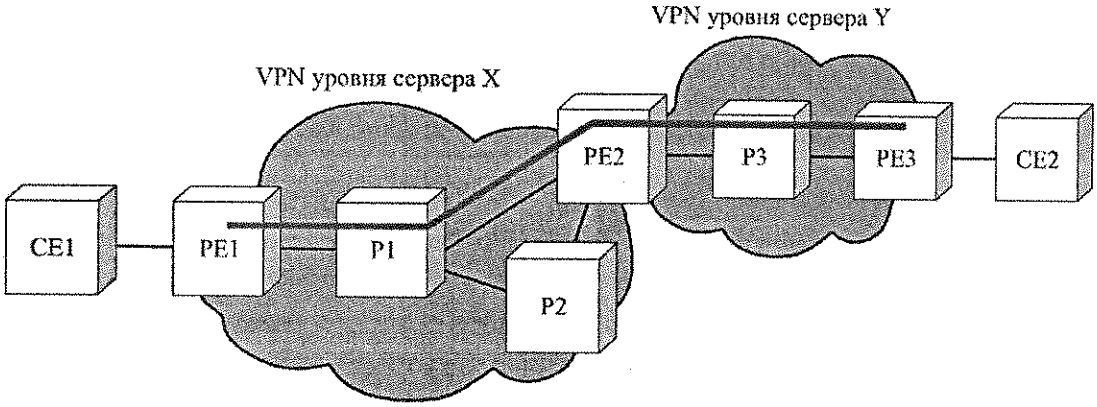


Рисунок В.1 - Физическая топология взаимодействия сетей VPN уровня сервера

Один из методов взаимодействия сетей VPN уровня сервера X и Y заключается в использовании взаимодействия клиент-сервер, как показано на рисунке В.2. В этой модели узел PE2 принадлежит обеим сетям VPN уровня сервера X и Y, а все три узла PE принадлежат сети VPN уровня клиента.

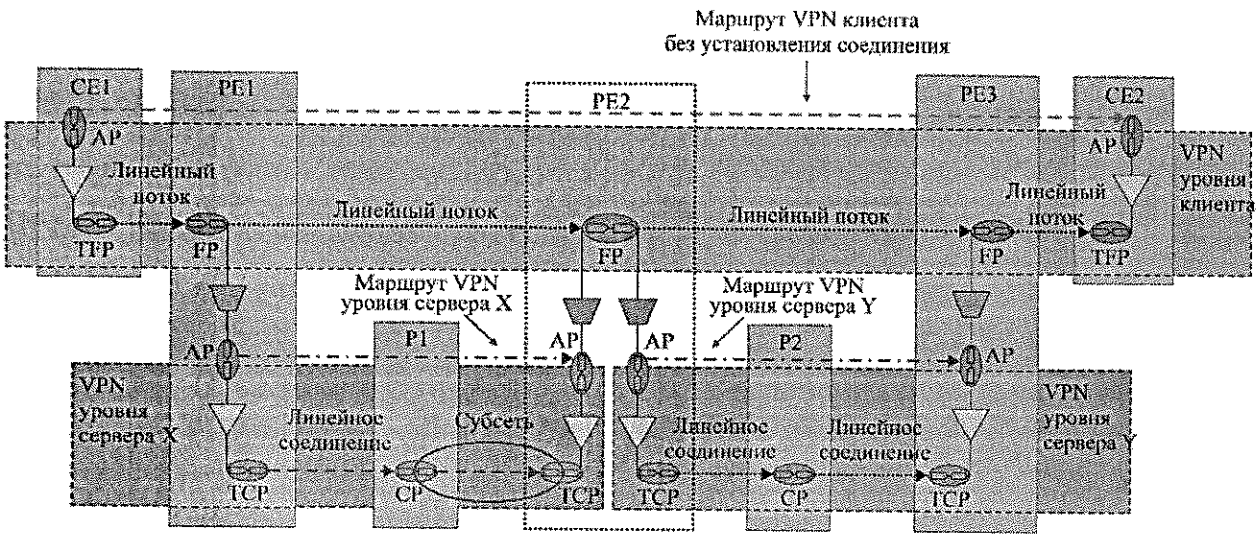


Рисунок В.2 – Взаимодействие сетей VPN уровня сервера

STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Функция адаптации источника сети VPN уровня сервера X трансформирует CI сети VPN уровня клиента в AI сети VPN уровня сервера X, а функция адаптации приемника трансформирует AI сети VPN уровня сервера X в CI сети VPN уровня клиента.

Функция адаптации источника сети VPN уровня сервера Y трансформирует CI сети VPN уровня клиента в AI сети VPN уровня сервера Y, а функция адаптации приемника трансформирует AI сети VPN уровня сервера Y в CI сети VPN уровня клиента.

Сетевые элементы, на которых выполняется адаптация клиент-сервер, содержат точки FP или CP, принадлежащие сети VPN уровня клиента, которую нужно идентифицировать адресами VPN уровня клиента.

Использование нескольких сетей VPN уровня сервера с адаптацией клиент-сервер для VPN уровня клиента CO означает, что маршрут/путь должен быть динамически/вручную рассчитан через все точки CP, и должно быть установлено два сквозных линейных соединения в сети VPN уровня клиента.

Использование нескольких сетей VPN уровня сервера с адаптацией клиент-сервер для уровня клиента CL означает, что маршрут/путь должен быть динамически/вручную рассчитан через все точки FP, и единицы трафика CL должны передаваться на основе адресной информации сети VPN уровня клиента.

Альтернативный метод взаимодействия между сетями VPN уровня сервера X и Y показан на рисунке B.3, он заключается в использовании равноправного взаимодействия.

В этой модели узел PE2 принадлежит сетям VPN уровня сервера X и Y, но не принадлежит сети VPN уровня клиента. Узлы PE1 и PE3 принадлежат сетям VPN уровня сервера X и Y соответственно, а также принадлежат сети VPN уровня клиента.

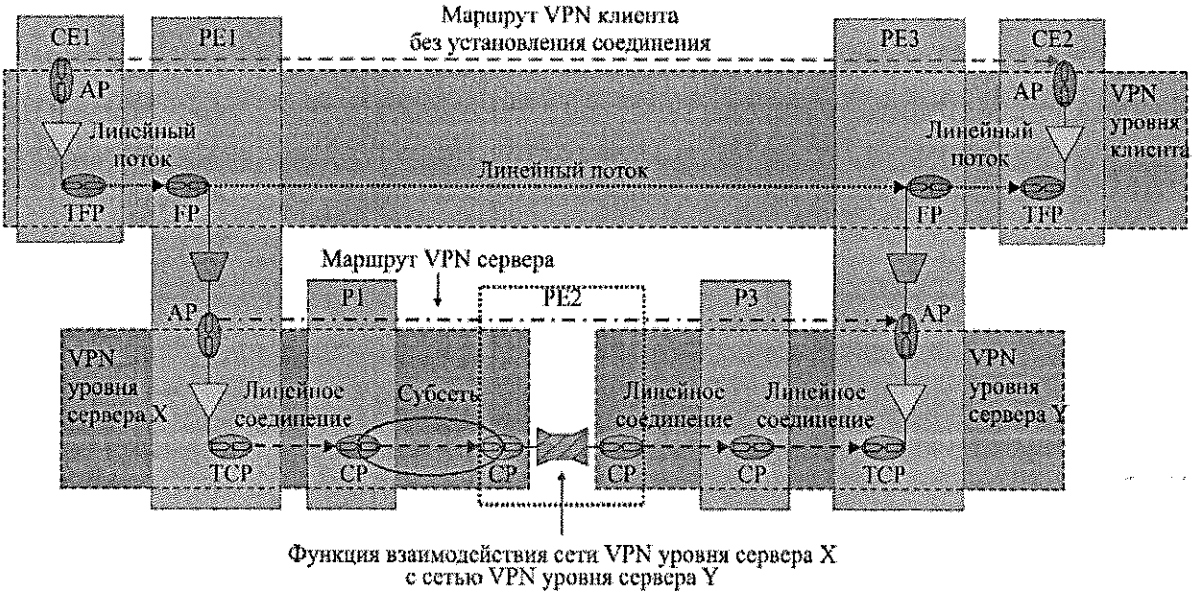


Рисунок B.3 – Равноправное взаимодействие сетей VPN уровня сервера

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Функция адаптации источника сети VPN уровня сервера X трансформирует CI сети VPN уровня клиента в AI в сети VPN уровня сервера X.

Функция взаимодействия сети VPN уровня сервера X с сетью VPN уровня сервера Y трансформирует AI сети VPN уровня сервера X в AI сети VPN уровня сервера Y. Функция адаптации приемника VPN уровня сервера Y трансформирует AI сети VPN уровня сервера Y AI в CI сети VPN уровня клиента.

Взаимодействие на равноправной основе требует осуществлять взаимодействие не только в плоскости данных, и в плоскости управления для таких функций как маршрутизация, сигнализация и OAM.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Приложение С
(рекомендуемое)

Примеры сценариев услуг в сетях VPN клиент-сервер и в сетях VPN равноправного взаимодействия

В таблицах С.1 - С.3 приведены примеры различных сценариев предоставления услуг VPN и определены примеры механизмов/протоколов, которые могут использоваться для выполнения необходимых функций.

Таблица С.1 – Сценарии предоставления услуг VPN клиент-сервер № 1

Функции VPN	Уровень 2 услуга передачи кадров по сети MPLS	Уровень 2 услуга Ethernet VPWS по сети P/L2TPv3	Уровень 2 услуга IP передачи в сети VPN RFC 2547
VPN уровня клиента	Frame Relay	Ethernet	IP
VPN уровня сервера	MPLS PW	IP/L2TPv3	MPLS
Определение принадлежности сети VPN	RADIUS, BGP, вручную, NMS	RADIUS,BGP, LDP, RSVP-TE, вручную, NMS	BGP
Маршрутизация в VPN уровня сервера	IGP, BGP, вручную, NMS	IGP, BGP, вручную, NMS	BGP
Создание туннеля/соединения в VPN уровня сервера	LDP, BGP, вручную, NMS	Сигнализация L2TPv3	BGP
Аутентификация CE/пользователя, санкционирование доступа и расчеты	RADIUS, RMON, SNMP, NMS	RADIUS, RMON, SNMP, NMS	Протокол маршрутизации CE-PE (EBGPcMD5), RMON, SNMP, NMS
Конфигурация элементов сети VPN уровня клиента	NMS, вручную	NMS, вручную, E-LMI	DHCP, NMS, вручную
Маршрутизация в VPN уровня клиента	NMS, вручную	Выяснение MAC адреса	EBGP, OSPF, вручную/статически

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Окончание таблицы С.1

Функции VPN	Уровень 2 услуга передачи кадров по сети MPLS	Уровень 2 услуга Ethernet VPWS по сети P/L2TPv3	Уровень 2 услуга IP передачи в сети VPN RFC 2547
Передача сигнализации по туннлю/соединению VPN уровня клиента	NMS, вручную	Не требуется, так как клиент-CL-PS	Не требуется, так как клиент-CL-PS
Функции OAM в VPN уровня клиента	Frame Relay LMI	E-LMI,	IP переброска/трассировка маршрута
Функции OAM в VPN уровня сервера	MPLS,VCCV,BFD/LSP переброска	IP переброска/трассировка маршрута	LSP переброска/трассировка маршрута

Таблица С.2 – Сценарии предоставления услуг VPN клиент-сервер № 2

Компоненты сети VPN	Уровень 1 SDH услуги в сети VPN посредством OTN	Уровень 1 TDM услуги в сети VPN посредством MPLS	Уровень 2 ATM услуги в сети VPN посредством SDH
VPN уровня клиента	SDH (STM-16)	TDM (E1)	ATM
VPN уровня сервера	Светово-вод/оптический	MPLS PW	SDH (VC4)
Определение принадлежности сети VPN	Вручную, NMS	RADIUS, BGP, LDP, вручную, NMS	Вручную, NMS
Маршрутизация в VPN уровня сервера	GMPLS/ASON протоколы маршрутизации, вручную, NMS	IGP,BGP, вручную, NMS	GMPLS/ASON, протоколы маршрутизации, вручную, NMS
Создание туннеля/соединения в VPN уровня сервера	GMPLS/ASON протоколы сигнализации, вручную, NMS	LDP, BGP, вручную, NMS	GMPLS/ASON протоколы сигнализации, вручную, NMS
Аутентификация CE/пользователя, санкционирование доступа и расчеты	Протоколы GMPLS/ASON, SNMP, NMS	RMON, SNMP, NMS,	ATM, безопасность, PNNI/UNI, RMON, SNMP, NMS

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH MASHQARMASI

Окончание таблицы С.2

Компоненты сети VPN	Уровень 1 SDH услуги в сети VPN посредством OTN	Уровень 1 TDM услуги в сети VPN посредством MPLS	Уровень 2 ATM услуги в сети VPN посредством SDH
Конфигурация элементов сети VPN уровня клиента	NMS, вручную	NMS, вручную	ATM UNI, вручную, NMS
Маршрутизация в VPN уровня клиента	GMPLS/ASON,протоколы сигнализации, вручную, NMS	Вручную, NMS	Вручную, NMS, PNNI
Передача сигнализации по тунелю/соединению VPN уровня клиента	GMPLS/ASON, протоколы сигнализации, вручную, NMS	Вручную, NMS	Вручную, NMS, PNNI
Функции OAM в VPN уровня клиента	Заголовок к SDH	AIS/LOS	F4 и F5 управления обработкой отказов, обратная петля, и контроль непрерывности
Функции OAM в VPN уровня сервера	Заголовок OCh	MPLS,VCCV, BFD/LSP переброска	Заголовок SDH

Таблица С.3 – Сценарии предоставления услуг VPN равноправного взаимодействия

Компоненты сети VPN	IPsec VPN через Интернет	VPN сеть VLAN Ethernet
VPNравноправного взаимодействия	IP	Ethernet
Определение принадлежности сети VPN	Вручную, NMS	Вручную, NMS, RADIUS
Аутентификация CE/пользователя, санкционирование доступа и расчеты	Основная аутентификация IKE, RMON, SNMP, NMS	RADIUS, RMON, SNMP, NMS

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Окончание таблицы С.3

Компоненты сети VPN	IPsec VPN через Интернет	VPNсетьVLAN Ethernet
Маршрутизация в VPN равноправного взаимодействия	IGP протоколы маршрутизации (ISIS, OSPF, RIP), BGP, вручную, NMS	Усечение топологии STP и выяснение адреса в плоскости данных
Конфигурация сетевых элементов в VPN равноправного взаимодействия	Конфигурирование совместного использования ключа, или запрос сертификата от органа сертификации	Конфигурирование сетей VLAN вручную, используя NMS или динамические протоколы
Функции OAM в VPN равноправного взаимодействия	IP переброска, трассировка маршрута	E-LMI

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAYLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

УДК 621.37/39.004 ОКС 35.110 Э 08

Ключевые слова: инициализация, пакетная передача данных, пакетная коммутация, протокол, сессия, сети с пакетной коммутацией

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

Заместитель директора
ГУП «UNICON.UZ» А.Кадиров

Начальник
научно-исследовательского
отдела телекоммуникационных
технологий и почтовой связи А.Мирхабибов

Инженер
научно-исследовательского
отдела телекоммуникационных
технологий и почтовой связи С.Сайдиакбаров

Нормоконтроль Л.Шаймарданова
14.09.2016

СОГЛАСОВАНО

Начальник отдела
телекоммуникационных
технологий и услуг
Министерства по развитию
информационных технологий
и коммуникаций Республики
Узбекистан

З.Зияев
письмо от 16.10.2015
№ 09-8/5678

СОГЛАСОВАНО

Заместитель
генерального директора
АК «Узбектелеком»

Ж.Махсудов
письмо от 10.09.2015
№ 07-03-46/3510

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI