МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.1314

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(10/2005)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Аспекты межсетевого протокола – Транспортирование

Функциональная декомпозиция виртуальной частной сети

Рекомендация МСЭ-Т Y.1314

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	Y.100–Y.199
Общие положения	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	**Y.1300–Y.1399**
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты служб: возможности служб и архитектура служб	Y.2200–Y.2249
Аспекты служб: взаимодействие служб и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Y.1314

Функциональная декомпозиция виртуальной частной сети

Резюме

В настоящей Рекомендации описывается комплекс функций, необходимых для создания, эксплуатации и обслуживания виртуальных частных сетей (VPN) клиент-сервер и сетей равноправного взаимодействия. Функциональные средства сети описываются с точки зрения сетевого уровня, с учетом многоуровневой структуры сети VPN, данных о характеристиках клиента, связей клиент/сервер, топологии сети и функциональных средств сетевого уровня.

Функциональные модели описываются с использованием методики моделирования, изложенной в Рекомендациях МСЭ-Т G.805 и G.809. Используемая методика моделирования не зависит от сетевой технологии и, следовательно, описываемые функциональные модели и связанные с ними функции применимы ко всем VPN технологиям сетевого уровня.

Источник

Рекомендация МСЭ-Т Y.1314 утверждена 14 октября 2005 года 13-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Y.1314

Функциональная декомпозиция виртуальной частной сети

1 Сфера применения

В настоящей Рекомендации описывается комплекс функций, необходимых для создания, эксплуатации и обслуживания виртуальных частных сетей (VPN) клиент-сервер и сетей равноправного взаимодействия. Функциональные средства сети описываются с точки зрения сетевого уровня, с учетом многоуровневой структуры сети VPN, данных о характеристиках клиента, связей клиент/сервер, топологии сети и функциональных средств сетевого уровня. Функциональные модели описываются с использованием методики моделирования, изложенной в Рекомендациях МСЭ-Т G.805 и G.809.

2 Справочные документы

В нижеследующих Рекомендациях и других справочных документах содержатся положения, которые, с помощью ссылки в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются; поэтому всем пользователям данной Рекомендации настоятельно рекомендуется изучить возможность использования последних изданий перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает этому отдельному документу статуса рекомендации.

– ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

– ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks*.

– ITU-T Recommendation G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.

– ITU-T Recommendation Y.1311 (2002), *Network-Based VPNs – Generic architecture and service requirements*.

3 Определения

В настоящей Рекомендации используются термины, определенные в Рек. МСЭ-Т G.805:

3.1 точка доступа (access point)
3.2 группа доступа (access group)
3.3 адаптированная информация (adapted information)
3.4 характеристическая информация (characteristic information)
3.5 взаимосвязь клиент-сервер (client-server relationship)
3.6 соединение (connection)
3.7 точка соединения (connection point)
3.8 многоуровневая сеть (layer network)
3.9 линия (link)
3.10 линейное соединение (link connection)
3.11 матрица (matrix)
3.12 сеть (network)
3.13 сетевое соединение (network connection)
3.14 порт (port)
3.15 контрольная точка (reference point)
3.16 субсеть (subnetwork)
3.17 субсетевое соединение (subnetwork connection)
3.18 оконечная точка соединения (termination connection point)
3.19 маршрут (trail)

3.20 завершение маршрута (trail termination)
3.21 транспорт (transport)
3.22 транспортная единица (transport entity)
3.23 транспортная функция обработки (transport processing function)
3.24 однонаправленное соединение (unidirectional connection)
3.25 однонаправленный маршрут (unidirectional trail)

В настоящей Рекомендации используются термины, определенные в Рек. МСЭ-Т G.809:

3.26 точка доступа (access point)
3.27 группа доступа (access group)
3.28 адаптированная информация (adapted information)
3.29 характеристическая информация (characteristic information)
3.30 взаимосвязь клиент-сервер (client-server relationship)
3.31 маршрут без установления соединения (connectionless trail)
3.32 поток (flow)
3.33 домен потока (flow domain)
3.34 поток доменов потока (flow domain flow)
3.35 точка потока (flow point)
3.36 объединение точек потока (flow point pool)
3.37 завершение потока (flow termination)
3.38 получатель завершения потока (flow termination sink)
3.39 источник завершения потока (flow termination source)
3.40 многоуровневая сеть (layer network)
3.41 линейный поток (link flow)
3.42 сеть (network)
3.43 сетевой поток (network flow)
3.44 порт (port)
3.45 контрольная точка (reference point)
3.46 единица трафика (traffic unit)
3.47 транспорт (transport)
3.48 транспортная единица (transport entity)
3.49 транспортная функция обработки (transport processing function)
3.50 точка завершения потока (termination flow point)

В настоящей Рекомендации используется термин, определенный в Рек. МСЭ-Т G.8010/Y.1306:

3.51 фрагмент домена потока (flow domain fragment)

В настоящей Рекомендации используются термины, определенные в Рек. МСЭ-Т Y.1311:

3.52 VPN уровня 1 (VPN Level 1)
3.53 VPN уровня 2 (VPN Level 2)
3.54 VPN уровня 3 (VPN Level 3)

В настоящей Рекомендации определяются следующие термины:

3.55 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.

3.56 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.

3.57 VPN сеть 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.

4 Сокращения и аббревиатура

В настоящей Рекомендации используются следующие сокращения и акронимы:

AAA	Authentication, Authorization and Accounting	Аутентификация, авторизация и расчеты
AAL	ATM Adaptation Layer	Уровень адаптации ATM
AG	Access Group	Группа доступа
AI	Adapted Information	Адаптированная информация
AIS	Alarm Indication Signal	Сигнал индикации аварии
AP	Access Point	Точка доступа
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 Bit Rate	Постоянная скорость передачи
CC	Connectivity Check	Проверка возможности соединения
CE	Customer Edge	Сторона пользователя
CI	Characteristic Information	Характеристическая информация
CL-PS	Connectionless Packet-Switched	С коммутацией пакетов без установления соединения
CO-CS	Connection-Orientated Circuit-Switched	С коммутацией каналов с установлением соединения
CO-PS	Connection-Orientated Packet-Switched	С коммутацией пакетов 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
DSCP	Differentiated Services Code Point	Кодовая точка дифференцированного обслуживания
DWDM	Dense Wave Division Multiplexing	Мультиплексирование по длине волны повышенной плотности
EBGP	External Border Gateway Protocol	Расширенный пограничный межсетевой протокол
E-LMI	External LMI	Расширенный интерфейс локального управления
ES	End System	Оконечная система

FDF	Flow Domain Flow	Поток доменов потока
FDFr	Flow Domain Fragment	Фрагмент домена потока
FDI	Forward Defect Indication	Упреждающее обнаружение ошибки
FP	Flow Point	Точка потока
FPP	Flow Point Pool	Объединение точек потока
FR	Frame Relay	Ретрансляция кадров
FT	Flow Termination	Завершение потока
FTP	Flow Termination Point	Точка завершения потока
GRE	Generic Routing Encapsulation	Общее пакетирование для маршрута
IGP	Interior Gateway Protocol	Внутренний межсетевой протокол
IKE	Internet Key Exchange	Обмен ключами по сети Интернет
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 – промежуточная система
L2TP	Layer 2 Tunneling Protocol	Протокол туннелирования уровня 2
LDP	Label Distribution Protocol	Протокол распределения меток
LF	Link Flow	Поток в канале
LMI	Local Management Interface	Интерфейс локального управления
LOC	Loss Of Continuity	Потеря соединения
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
MP-BGP	Multi-Protocol BGP	Многопротокольный пограничный межсетевой протокол
MPLS	Multi-Protocol Label Switching	Многопротокольное переключение меток
MTU	Maximum Transmission Unit	Максимальный размер пакета
NE	Network Entity	Сетевой элемент
NF	Network Flow	Сетевой поток
NMS	Network Management System	Система управления сетью
NSAP	Network Service Access Point	Точка доступа к сетевому сервису
OAM	Operations, Administration and Maintenance	Эксплуатация, управление и обслуживание
OOB	Out Of Band	Внеполосный

OSI	Open Systems Interconnection	Взаимосвязь открытых систем	ВОС
OSPF	Open Shortest Path First	Открыть кратчайший путь первым	
OSS	Operational Support System	Система оперативной поддержки	
P	Provider (Node)	Провайдер (узел)	
P2P	Point-to-Point	Из пункта в пункт	
P2MP	Point-to-Multipoint	Из пункта во многие пункты	
PCR	Peak Cell Rate	Пиковая скорость передачи	
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	
PHP	Penultimate Hop Popping	Появление предпоследнего скачка	
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 ReserVation Protocol (with) Traffic Engineering (extensions)	Протокол резервирования ресурсов (с) управлением трафиком (расширения)	
SCR	Sustained Cell Rate	Поддерживаемая скорость передачи	
SDH	Synchronous Digital Hierarchy	Синхронная цифровая иерархия	СЦИ
SES	Severely Errored Second	Секунда с ошибками	
SLA	Service Level Agreement	Соглашение об уровне обслуживания	
SNC	SubNetwork Connection	Субсетевое соединение	
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления	
SONET	Synchronous Optical NETwork	Синхронная оптическая сеть	
SPVC	Switched Permanent Virtual Circuit	Коммутируемый постоянный виртуальный канал	
SSL	Secure Socket Layer	Протокол безопасных соединений	
STP	Spanning Tree Protocol	Протокол связующего дерева сети	
SVC	Switched Virtual Circuit	Коммутируемый виртуальный канал	
TCP	Termination Connection Point	Оконечная точка канала	
TDM	Time Division Multiplexing	Мультиплексирование с разделением по времени	

TFP	Termination Flow Point	Оконечная точка потока
TTL	Time-To-Live	Предписанное время жизни
TTSI	Trail Termination Source Identifier	Идентификатор источника завершения маршрута
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 выделенная сеть
WDM	Wavelength Division Multiplexing	Мультиплексирование с разделением по длине волны

5 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 Рекомендации МСЭ-Т Y.1311 описываются сети VPN клиент-сервер в понятиях типов VPN услуг и типов VPN транспорта, где термин "тип VPN услуги" означает сеть VPN уровня клиента, а термин "тип VPN транспорта" означает сеть VPN уровня сервера. Различные типы VPN услуги (клиента) и транспорта (сервера) классифицированы в Рекомендации. МСЭ-Т Y.1311, как показано в таблице 5-1.

Таблица 5-1/Y.1314 – Типы услуг Y.1311

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

Одним из недостатков метода классификации, использованного в Рекомендации МСЭ-Т Y.1311, является то, что MPLS не попадает ни в одну из этих категорий и, следовательно, должна рассматриваться как сетевая технология уникального уровня. Еще одним недостатком является то, что с функциональной точки зрения, сетевые технологии одного уровня могут иметь совершено различные характеристики и требования. Например, и Ethernet, и ATM являются технологиями уровня 2; однако Ethernet является технологией без установления соединения с радиовещательной передачей, а ATM – технологией с установлением соединения с нерадиовещательной передачей.

Еще одним способом классификации сетевых технологий является деление их по режимам сетей, к которым они принадлежат. Все сетевые технологии могут 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, поскольку у каждого режима свои характеристики. В таблице 5-2 показаны примеры технологий сетевых уровней VPN, и к какому режиму они принадлежат.

Таблица 5-2/Y.1314 – Режимы работы сети и примеры

Режим работы	Примеры
без установления соединения с коммутацией пакетов	IP, Ethernet, MPLS MP2P (Примечание 1)
с установлением соединения и с коммутацией пакетов	Ретрансляция кадров, MPLS P2P/P2MP (Примечание 2), ATM
с установлением соединения и с коммутацией каналов	SDH/SONET, TDM
ПРИМЕЧАНИЕ 1. – 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.	
ПРИМЕЧАНИЕ 2. – 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.	

5.1 Комбинации клиент-сервер

Существует девять возможных комбинаций клиент-сервер, основанных на трех режимах работы сети, хотя некоторые комбинации являются более совместимыми, чем другие. В таблице 5-3 показаны возможные комбинации клиент-сервер, и даны некоторые 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. Одним из важных требований по адаптации для VPN клиентов с коммутацией каналов, обслуживаемых VPN сервером с коммутацией пакетов, является то, что функция адаптации должна обеспечивать разграничение скоростей (т. е., заполнение пустых мест) и выявление пакетов уровня клиента VPN. Ключевое требование для ситуаций, когда и клиент и сервер работают с коммутацией пакетов (CO или CL) заключается в том, что функция адаптации должна поддерживать фрагментацию и выстраивание последовательности, если единица трафика уровня сервера VPN (т. е., MTU пакеты) меньше, чем единица трафика в сети VPN уровня клиента. Другими функциями адаптации, которые могут потребоваться в зависимости от конкретной используемой технологии клиент/сервер VPN, являются: кодирование, изменение скорости и синхронизация.

Таблица 5-3/Y.1314 – Комбинации режимов работы клиент-сервер

	CL-PS VPN уровня клиента	**CO-PS VPN уровня клиента**	**CO-CS VPN уровня клиента**
CL-PS уровня сервера VPN	– Идеален, хотя обеспечение гарантии доставки для каждого потока усложняет масштабирование – Общий подход, который гарантирует доставку каждого потока, должен использовать преимущественные и классовые решения по организации приоритета очередности для управления пакетным трафиком все-ко-всем и перегрузкой) *Пример: Серверный уровень Ethernet, поддерживающий уровень IP клиента*	– Обеспечение гарантии доставки для каждого потока усложняет масштабирование – Общий подход, который гарантирует доставку каждого потока, должен использовать преимущественные и классовые решения по организации приоритета очередности – Уровень клиента VPN должен быть способен к восстановлению от влияния единиц трафика, выбивающихся из общей последовательности (из-за возможности смены порядка следования пакетов на уровне сервера) *Пример: Серверный уровень IP, поддерживающий уровень ATM клиента*	– Обеспечение гарантии доставки для каждого потока усложняет масштабирование – Общий подход, который гарантирует доставку каждого потока, должен использовать преимущественные и классовые решения по организации приоритета очередности – Восстановление тактовой частоты очень сложно технически – 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-PS уровня сервера VPN	– Стоимость обслуживания предоставления каналов VPN по запросу с небольшим временем удержания, т. е. SPVC *Пример: Серверный уровень ATM , поддерживающий уровень IP клиента*	– Идеален *Пример: Серверный уровень A P2P MPLS, поддерживающий уровень ATM клиента*	– Восстановление тактовой частоты очень сложно технически *Пример: Серверный уровень ATM , 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 SDH , поддерживающий уровень Ethernet 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 ATM , поддерживающий уровень TDM клиента*	– Идеален *Пример: Серверный уровень оптической сети (например, канал DWDM) поддерживающий уровень клиента SDH/SONET*

5.2 Прозрачность уровня клиента VPN

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

Несмотря на то, что для сети VPN клиент-сервер можно разработать решения, в которых функциональные компоненты сети VPN уровня сервера взаимодействуют с функциональными компонентами сети VPN уровня клиента, этот подход имеет множество нежелательных последствий, например:

1) Если пользователь VPN изменит любые функциональные компоненты сети VPN уровня клиента, то предоставление услуги VPN может прерваться.
2) Провайдер услуг VPN должен отслеживать изменения в технологии сети VPN уровня клиента на стороне пользователя и соответствующим образом модернизировать технологию своей сети.
3) При возникновении неисправности, трудно установить, произошла ли ошибка в сети VPN уровня клиента или в сети VPN уровня сервера.

Требование того, чтобы сети VPN уровня клиента и уровня сервера имели бы возможность работать независимо друг от друга, естественно означает, что сеть VPN уровня сервера должна прозрачно передавать сигналы сети VPN уровня клиента. Например, если сеть VPN уровня клиента является сетью ATM, то сеть VPN уровня клиента может реализовывать патентованные приложения (например, AAL, маршрутизация и сигнализация без PNNI, OAM), которые, если их сигналы изменяются при передаче, могут нарушить предоставление услуги VPN.

Прозрачность уровня клиента является не только техническим требованием, она также имеет коммерческие последствия, так как провайдер услуг VPN, вероятно, учтет детали, делающие его сеть коммерчески уязвимой и, следовательно, пожелает скрыть эти подробности от любых сетей VPN уровня клиента. Например, для сети VPN уровня сервера было бы нежелательно, чтобы эта сеть в равноправном режиме обменивалась с сетью VPN уровня клиента сигналами маршрутизации и сигнализации (см. вышеприведенный пример).

6 VPN равноправного взаимодействия

Описанные в разделе 5 технологии VPN основаны на взаимоотношениях типа клиент-сервер между сетью VPN уровня клиента и сетью VPN уровня сервера. В сети VPN клиент-сервер, функция адаптации источника сети VPN уровня сервера адаптирует характеристическую информацию (CI) сети VPN уровня клиента в адаптированную информацию (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. В общих понятиях, такой адаптацией называют инкапсуляцию кадра/сигнала сети VPN уровня клиента в кадр/сигнал сети VPN уровня сервера.

Однако не все топологии VPN строятся по модели клиент-сервер. Сети VPN могут 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 настоящей Рекомендации такой тип сети VPN называется сетью VPN равноправного взаимодействия. Термин "уровень равноправного использования" обозначает тот факт, что провайдер передает пакеты пользователя VPN по совместно используемой инфраструктуре на том же самом 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, поскольку в случаях CO-PS и CO-CS, технология, основанная на установлении соединения, усиливает разграничение достижимости, т. е. сетевые элементы могут взаимодействовать только с сетевыми элементами, которые принадлежат одному и тому же соединению P2P или P2MP.

Для того чтобы поддерживать сети VPN в области совместного использования, используемая технология сети должна применять одни и те же средства разграничения сетей VPN, т. е., сетевые элементы должны иметь возможность соединения только с теми сетевыми элементами, которые принадлежат той же самой сети VPN, либо иметь возможность дешифровать пакеты от сетевых элементов, которые принадлежат той же самой VPN.

6.1 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. При таком подходе все узлы в сети провайдера услуг знают маршруты всех пользователей. Это относится к узлам на стороне провайдера (PE), которые работают с сайтами пользователей, и узлами провайдера (P) в центральной сети. 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 преодоления необходимости поддержания совместимых таблиц маршрутизации и фильтров пакетов для каждого пользователя и каждого сайта, имеется альтернативное решение, основанной на фильтрации маршрутов, а не фильтрации пакетов, и работающее совместно с соответствующими устройствами PE, т. е. по одному устройству PE на одну сеть VPN. В такой архитектуре узлы P содержат информацию обо всех маршрутах пользователя, а узлы PE содержат информацию о маршрутах только одного пользователя. Изоляция маршрутов пользователя достигается за счет фильтрации маршрутов. Узлы PE конфигурируются с фильтрами маршрута, которые позволяют пользователям узнать только те маршруты, которые относятся к ним. Пограничный межсетевой протокол (BGP) – это пример протокола, наиболее часто используемого для этой цели в магистральной сети провайдера, благодаря его универсальным свойствам по фильтрации маршрута. Альтернативой фильтрации маршрута является использование различных для каждой VPN экземпляров протокола маршрутизации. Однако в случае применения такого подхода совместно используемая сеть сможет поддерживать только небольшое количество сетей VPN, так как узлы P будут способны поддерживать ограниченное число экземпляров протокола маршрутизации, а также из-за эксплуатационной сложности управления множеством экземпляров протокола.

Для преодоления необходимости использования различных узлов PE для каждой сети VPN, имеется альтернативная возможность применения виртуальных маршрутизатором (VR). При таком подходе один физический узел объединяет несколько виртуальных маршрутизаторов. Конкретному пользователю может быть выделен один (или несколько) виртуальных маршрутизаторов. Таким образом, один узел может предоставить разделенные экземпляры протокола маршрутизации для нескольких пользователей. Индивидуальные виртуальные маршрутизаторы работают так же, как и отдельные узлы PE, выделенные для отдельной VPN. Как и при фильтрации маршрута, узлы P содержат все маршруты пользователей и, следовательно, требуется фильтрация маршрута на узлах PE[1].

6.2 Шифрование

Альтернативой фильтрации маршрутов/пакетов является обеспечение полной достижимости между всеми пользователями, присоединенными к совместно используемой инфраструктуре, вместе с шифрованием пакетов. Шифрование пакетов гарантирует, что, 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, следовательно, пользователь становится ответственным за управление VPN. При таком подходе, трафик в сети провайдера услуг маршрутизируется точно так же, как и любой другой IP трафик, а провайдер услуг не может видеть, что происходит в туннеле. Точно так же, сеть провайдера услуг не требует какой-либо особенной конфигурации. В ином случае пакеты VPN могут шифроваться с применением оборудования, управляемого провайдером (т. е. устройств PE или управляемые провайдером CE) на границе совместно используемой сети провайдера. При таком подходе ответственным за управление VPN становится провайдер.

---

[1] Естественное развитие этого подхода – применение MPLS или иных методов тунеллирования, в результате чего маршруты, свойственные VPN, не нуждаются в поддержке на магистральных линиях. Однако в результате этого создаются сети VPN с топологией клиент/сервер и, следовательно, этот подход применим к разделу 5, а не к данному разделу.

Примером архитектуры, которая поддерживает шифрование, является RFC 2401 – архитектура безопасности для Интернет-протокола (IPsec). IPsec определяет алгоритмы шифрования, аутентификации и правила управления ключами[2] при создании безопасных туннелей для передачи IP трафика между шлюзами/клиентами IPsec. IPsec гарантирует секретность, целостность и аутентификацию источника данных в сети VPN, когда информация передается по совместно используемой инфраструктуре. IPsec особенно полезен для создания сетей VPN с передачей информации по сетям общего пользования, таким как Интернет, с одного сайта на другой или для доступа к удаленным сетям VPN. Функционирование IPsec может обеспечиваться при помощи PE, CE или оконечных устройств пользователя (например, портативный компьютер с установленным программным обеспечением клиента IPsec).

Сети VPN с протоколом безопасных соединений (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 (например, Web-навигаторы, почтовые клиенты и т. д.). Также, сети VPN с SSL являются прозрачными для сетей VPN уровня равноправного взаимодействия (так как шифрование выполняется на прикладном уровне) и, следовательно, конфигурация узлов маршрутизации/коммутации не является необходимой для поддержки сетей VPN с SSL.

6.3 Виртуальные локальные сети (VLAN) Ethernet

В стандарте IEEE 802.1Q определяется функционирование мостов виртуальных локальных сетей (VLAN), которые позволяют выполнять определение, эксплуатацию и управление топологиями виртуальных локальных сетей в пределах мостовой инфраструктуры LAN. Сети VLAN дают возможность соединять оконечные станции в различных физических сегментах локальной сети так, будто они соединены с одним и тем же сегментом LAN. Оконечные пользователи и узлы/коммутаторы могут быть перенесены в различные сети VLAN путем изменения конфигурации VLAN на порту/интерфейсе 802.1Q-совместимом коммутационном устройстве, к которому подсоединена оконечная станция или узел/коммутатор. 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, 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 (VID). VID должен быть назначен каждой сети VLAN (от 1 до 4096) и должен быть уникальным в пределах одной и той же физической инфраструктуры. Один из недостатков этого подхода состоит в том, что пользователи также используют VLAN внутри своей собственной сети, которая вводит распределение VID и добавляет некоторые ограничения. Для решения этой проблемы к пакетам стандарта IEEE 802.1Q, направляемым в сеть провайдера, была добавлена вторая метка IEEE 802.1Q (термин Q-in-Q определен в IEEE 802.1ad). Он отделяет область сети VLAN провайдера от пользовательской области VLAN и позволяет пользователям применять любой VID[3].

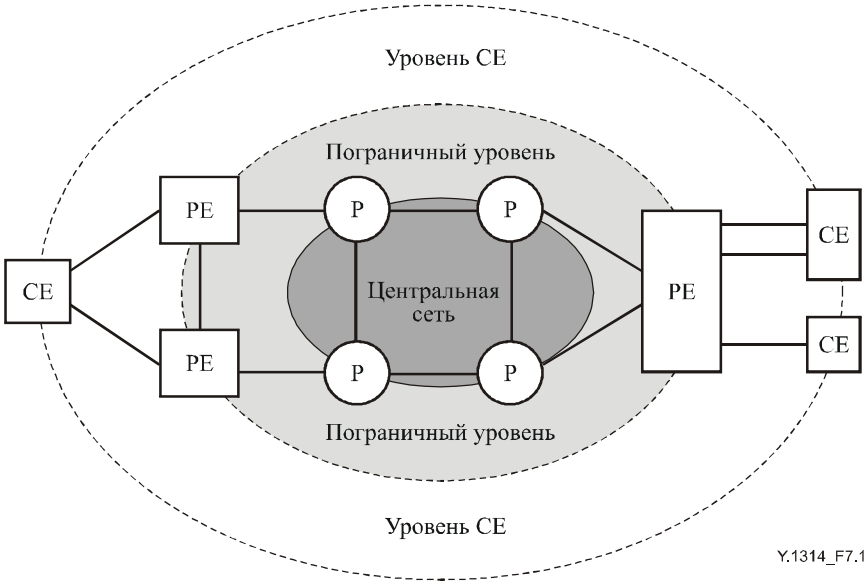
---

[2] Ключ – это блок информации, который управляет работой алгоритма шифрования/дешифрования.·

[3] Еще одна возможность – применение подхода MAC в MAC (определенного в IEEE 802.1ah), при котором провайдер добавляет к пакету пользователя второй Ethernet заголовок. Однако при этом варианте создается сеть клиент-сервер, а не VPN равноправного взаимодействия, так как кадр пользователя инкапсулируется в кадр провайдера.

7 Функциональная архитектура VPN

Эталонная модель VPN из Рекомендации МСЭ-Т Y.1311 показана на рисунке 7-1.



CE Сторона пользователя
PE Сторона провайдера
P Провайдер

Рисунок 7-1/Y.1314 – Эталонная модель VPN из Рек. МСЭ-Т Y.1311

Несмотря на физическую топологию этой модели и различные сетевые компоненты, она не показывает ни топологию различных сетей VPN уровня сервера и клиента, ни размещение функций адаптации между уровнями.

Альтернативным способом представления сети VPN клиент-сервер является метод функционального моделирования. Функциональная архитектура сетевых уровней с установлением соединения (CO-PS/CO-CS) и без установления соединения (CL-PS) может быть описана с применением "общей функциональной архитектуры транспортных сетей" из Рекомендации МСЭ-Т G.805 и "функциональной архитектуры сетевого уровня без установления соединения" из Рекомендации МСЭ-Т G.809, соответственно.

В Рекомендациях МСЭ-Т G.805 и G.809 описаны общие методы сетевого моделирования в функциональной и структурно-архитектурной плоскостях. Вводимая ими терминология не зависит от технологии и может использоваться для описания физических и логических компонентов любой заданной сети. Это особенно полезно для проверки комплектности сети и ее управления, поскольку можно смоделировать любой общий вид сети – от оптоволокна в кабеле до услуг VPN, предоставляемых с их использованием.

Сеть VPN можно разделить на независимые сетевые уровни, взаимодействие между которыми происходит по схеме клиент-сервер. Как указано в Рекомендации МСЭ-Т G.805, сетевые уровни, определенные с использованием функционального моделирования, не следует путать с уровнями из модели взаимосвязи открытых систем (ВОС) (Рек. МСЭ-Т X.200). Каждый уровень модели ВОС предоставляет конкретную услугу, а протокол, определенный для каждого уровня, выполняет конкретные функции, соответствующие этому уровню, например, транспортный уровень (Уровень 4) получает данные от уровня сеанса связи и передает их на сетевой уровень, предоставляя услугу сквозной доставки. В функциональной модели, основанной на Рекомендациях МСЭ-Т G.805 или G.809, наоборот, все сетевые уровни предоставляют одну и ту же услугу, т. е. транспортировку битов/кадров между входами и выходами. Как правило, используются абстрактные решения для сокрытия деталей и для сосредоточения внимания на интересующих сетевых уровнях/компонентах, но сети могут быть смоделированы непосредственно с обозначением сетевых элементов, таких как коммутаторы Ethernet, медные пары, кроссовые соединения СЦИ и т. д.

7.1 Сети VPN с установлением соединений (CO)

Каждая сеть VPN уровня клиента и сервера имеет собственный набор входов и выходов для установления соединений, называемых точками доступа (AP). Они могут объединяться 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 "из пункта в пункт" (P2P) и "из пункта во многие пункты" (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 с установлением соединения показаны на рисунке 7-2.

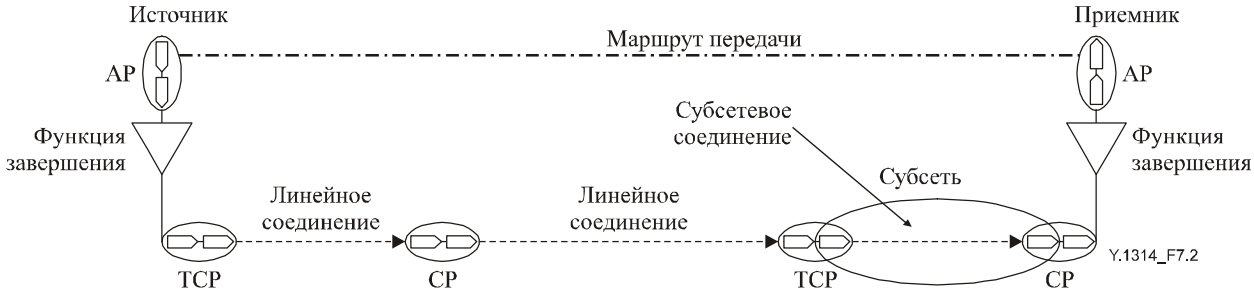


Рисунок 7-2/Y.1314 – Функциональные компоненты и контрольные точки в CO сети

Соединения – это транспортные единицы сетей с установлением соединения, которые состоят из связанной пары однонаправленных соединений, способных одновременно передавать информацию в двух противоположных направлениях между соответствующими входами и выходами. Сетевое соединение – это транспортная единица сети CO, образованная из нескольких смежных линейных соединений и/или субсетевых соединений между оконечными точками канала (TCP).

Субсеть – это компонент топологии сети CO, используемый для маршрутизации определенной характеристической информации и содержащий набор точек, связанных с функцией управления одного уровня сети CO. Субсетевое соединение передает информацию через субсеть и образовано путем соединения портов (выход оконечной точки источника сигнала на данном маршруте – вход оконечной точки получателя) на границах субсети.

Линейные соединения связывают смежные субсети, которые имеют общий набор точек. Точка, в которой вход канала соединен с выходом другого канала, является точкой соединения (CP). Точка, в которой выход оконечного источника маршрута сети CO соединен с входом сетевого соединения является оконечной точкой канала (TCP) источника, а точка, в которой вход оконечного приемника маршрута соединен с выходом сетевого соединения является оконечной точкой канала (TCP) приемника. С точками CP и TCP соединены управляемые объекты и, следовательно, в целях управления можно сгруппировать точки TCP и CP, принадлежащие одной и той же VPN.

7.2 Сети VPN без установления соединений (CL)

В отличие от сетей CO, сети CL поддерживают различные виды топологии соединения множества пунктов со множеством пунктов (MP2MP) или "все-со-всеми". Сети CL используют не каналы, а потоки, которые являются объединением одного или нескольких элементов трафика с элементом общей маршрутизации. Потоки могут быть однонаправленными или двунаправленными, при этом двунаправленные потоки состоят из двух противоположных однонаправленных потоков. Сетевой поток – это транспортная единица в сети CL, образованная множеством последовательных потоков между оконечными точками потока (TFP). Функциональные компоненты и контрольные точки сети CL показаны на рисунке 7-3.

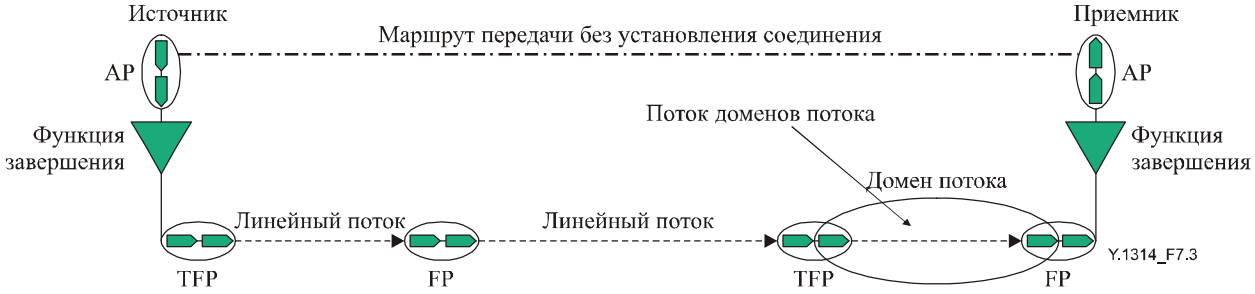


Рисунок 7-3/Y.1314 – Функциональные компоненты и контрольные точки в CL сети

Домен потока – это компонент топологии в сети CL, используемый для маршрутизации определенной характеристической информации. Поток доменов потока – это транспортная единица, которая переносит информацию через домен потока, она образована объединением портов на границе домена потока. 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 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. Как и для точек CP и TCP в случае CO, с точками FP и TFP для случая CL соединены управляемые объекты и, следовательно, в целях управления можно сгруппировать точки TFP и FP, принадлежащие одной и той же VPN.

7.3 Взаимосвязи между клиентами и сервером VPN

Говоря на языке функциональности, сеть VPN уровня клиента – это компонент топологии сети VPN клиент-сервер, который представляет собой набор точек доступа одного типа, соединенных для передачи характеристической информации сети VPN уровня клиента, которая поддерживается линией связи сети VPN уровня сервера, либо маршрутом без установления соединения. Оконечные точки канала/потока источника/приемника (TCP/TFP) для сети VPN уровня клиента могут располагаться в узлах на стороне пользователя (CE), или в узлах/оконечных устройствах в любом месте сети пользователя. Например, точки TCP в ATM сети VPN уровня клиента, вероятно, будут размещены на узлах CE, тогда как точки TFP в Ethernet сети VPN уровня клиента, вероятно, будут размещены на оконечных компьютерах пользователя или серверах. Место размещения оконечных точек канала/потока источника/приемника (TFP/TCP) сети VPN клиента является очень важным с точки зрения пользователя, поскольку это – та точка сети пользователя, где должна выполняться адаптация сетей VPN уровня клиента и сетей вышележащего уровня. Это место также 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 Дополнении I приведены примеры сетей VPN клиент-сервер с различными вариантами размещения точек TFP/TCP.

Сеть VPN уровня сервера – это компонент топологии сети VPN клиент-сервер, который представляет собой набор точек доступа одного типа, соединенных для передачи адаптированной информации уровня клиента для одного или нескольких каналов или потоков VPN уровня клиента. Сеть VPN уровня сервера содержит функции адаптации источника/приемника, которые адаптируют характеристическую информацию в сети VPN уровня клиента в/из адаптированной информации сети VPN уровня сервера. Сети VPN уровня клиента и сервера могут работать в одном и том же режиме (т. е. когда и уровень клиента, и уровень сервера работают без установления соединения, либо они оба работают с установлением соединения), но возможна также и комбинация этих двух режимов, т. е., 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 7-4 CL сеть VPN уровня сервера, поддерживающая CL сеть VPN уровня клиента, изображена с точки зрения функциональной перспективы, основанной на физической топологии сетевой модели из Рекомендации МСЭ-Т Y.1311, показанной на рисунке 7-1. Нижний уровень, показанный в модели, это – сеть VPN уровня сервера, а верхний уровень это – VPN уровня клиента. Для простоты картины показаны только уровни VPN клиент-сервер, уровень пользователя клиента выше VPN уровня клиента, и уровень сервера ниже VPN уровня сервера не показаны. В этом примере сеть VPN уровня сервера – это сеть с установлением соединения (CO) (например, ATM), тогда как сеть VPN уровня клиента это сеть без установления соединение (CL) (например, Ethernet), хотя возможны любые комбинации пар CO или CL.

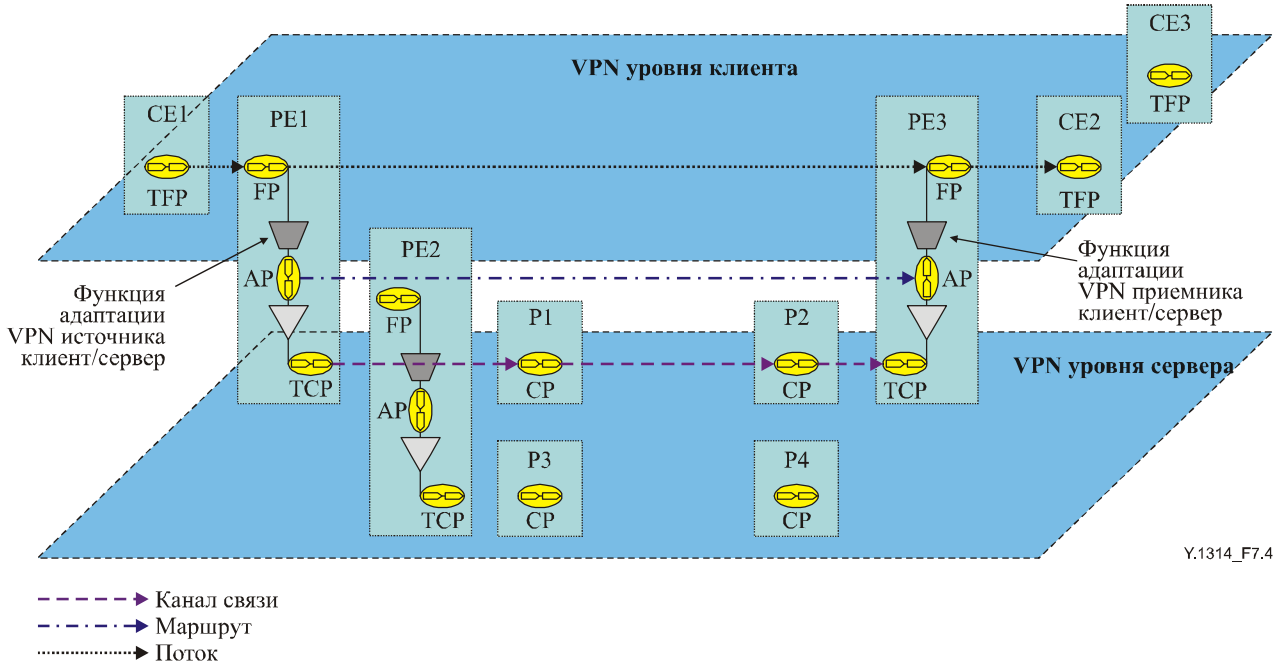


Рисунок 7-4/Y.1314 – Функциональная модель сети VPN клиент-сервер

На рисунке 7-4 показано, как функциональная модель связана с диаграммой сети, изображенной на рисунке 7-1 при помощи акцентирования внимания на том, какие функции и контрольные точки сети представлены в каком сетевом элементе (т. е. 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 (в данном случае – на каком узле CE) поток P2P сети VPN начинается (источник сети) и заканчивается (приемник сети), а точки FP определяют, через какие узлы PE проходит поток P2P. Аналогично, точки TFP в сети VPN уровня сервера определяют источник и приемник соединения VPN уровня сервера, а точки FP определяют, через какие узлы P проходит поток. Точки доступа (AP) в сети VPN уровня сервера определяют источник/приемник маршрута передачи в VPN уровня сервера.

В следующих параграфах показаны все четыре возможные комбинации сетей VPN клиент-сервер с использованием функциональных моделей и описана роль функций адаптации в сети VPN клиент-сервер.

7.3.1 Сеть VPN уровня клиента с установлением соединения (CO), поддерживаемая сетью VPN уровня сервера с установлением соединения (CO)

На рисунке 7-5 показан пример CO сети VPN уровня клиента, которая поддерживается CO сетью VPN уровня сервера.

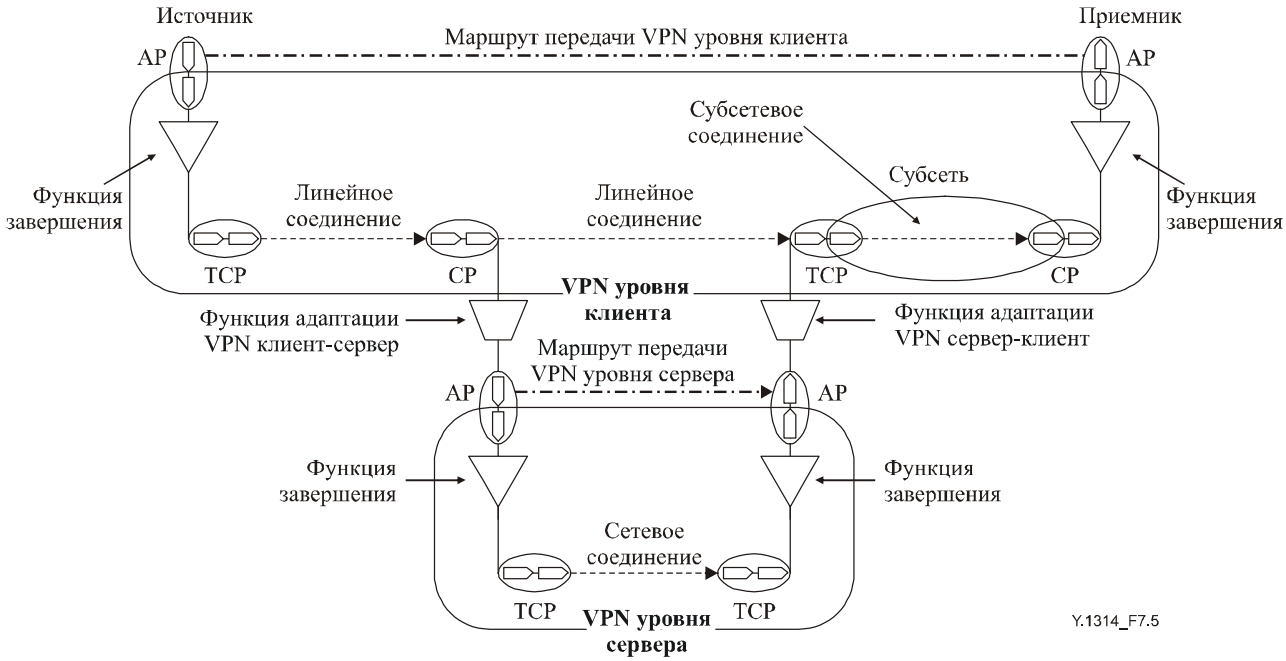


Рисунок 7-5/Y.1314 – CO сеть VPN уровня сервера с CO сетью VPN клиента

В этом примере CO соединение сети VPN уровня клиента поддерживается CO маршрутом передачи в сети VPN уровня сервера. Функция адаптации источника CO сети VPN уровня сервера адаптирует характеристическую информацию (CI) CO сети VPN уровня клиента, преобразуя ее в адаптированную информацию (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.

7.3.2 Сеть VPN уровня клиента без установления соединения (CL), поддерживаемая сетью VPN уровня сервера без установления соединения (CL)

На рисунке 7-6 показан пример CL сети VPN уровня клиента, которая поддерживается CL сетью VPN уровня сервера.

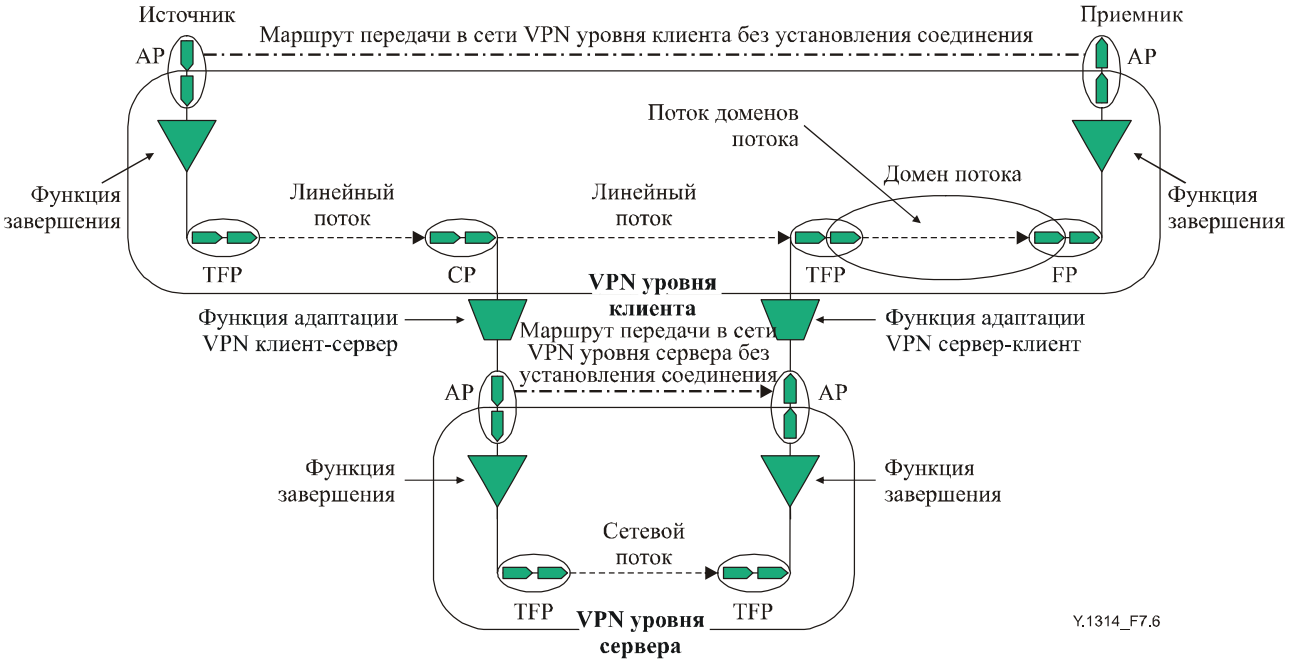


Рисунок 7-6/Y.1314 – CL сеть VPN уровня сервера с CL сетью VPN клиента

В этом примере CL поток сети VPN уровня клиента поддерживается маршрутом без установления соединения CL сети VPN уровня сервера. Функция адаптации источника CL сети VPN уровня сервера адаптирует характеристическую информацию (CI) CL сети VPN уровня, преобразуя ее в адаптированную информацию (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.

7.3.3 Сеть VPN уровня клиента с установлением соединения (CO), поддерживаемая сетью VPN уровня сервера без установления соединения (CL)

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

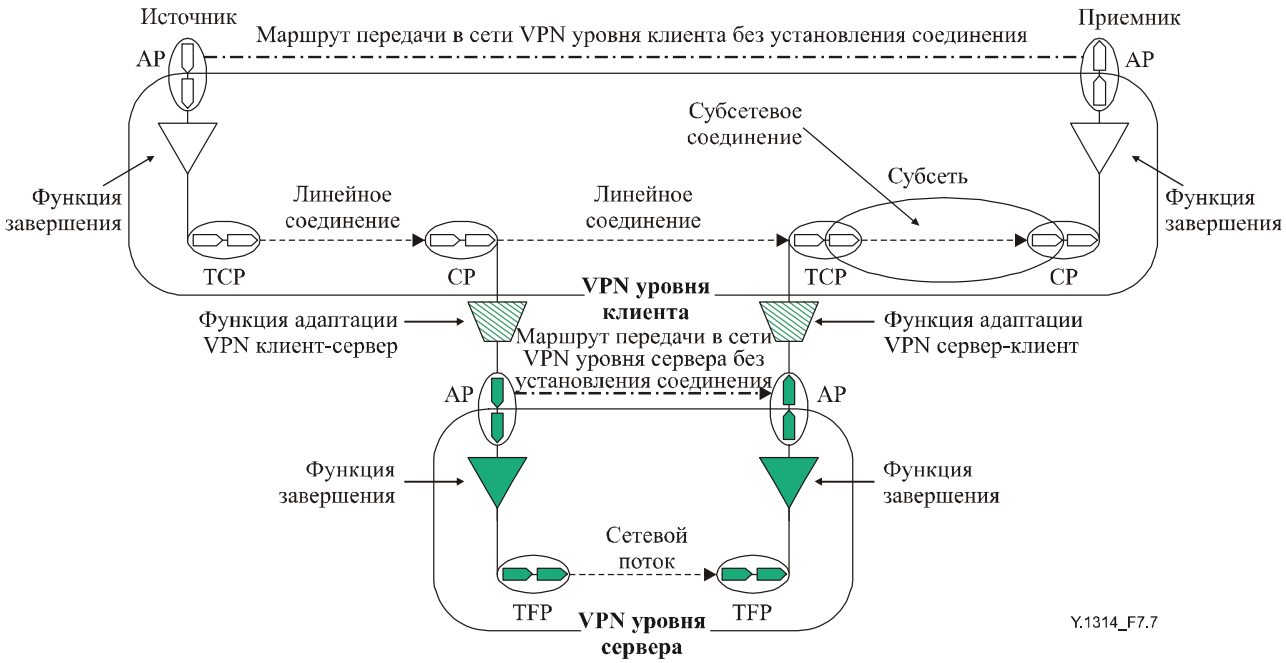


Рисунок 7-7/Y.1314 – CL сеть VPN уровня сервера с CO клиентом

В этом примере CO соединение сети VPN уровня клиента поддерживается маршрутом без установления соединения CL сети VPN уровня сервера. Функция адаптации источника CL сети VPN уровня сервера адаптирует характеристическую информацию (CI) CO сети VPN уровня, преобразуя ее в адаптированную информацию (AI) CL сети VPN уровня сервера. Функция адаптации получателя CL сети VPN уровня сервера адаптирует AI CL сети VPN уровня сервера, преобразуя ее в характеристическую информацию CO сети VPN уровня клиента.

7.3.4 Сеть VPN уровня клиента без установления соединения (CL), поддерживаемая сетью VPN уровня сервера с установлением соединения (CO)

На рисунке 7-8 показан пример CL сети VPN уровня клиента, которая поддерживается CO сетью VPN уровня сервера.

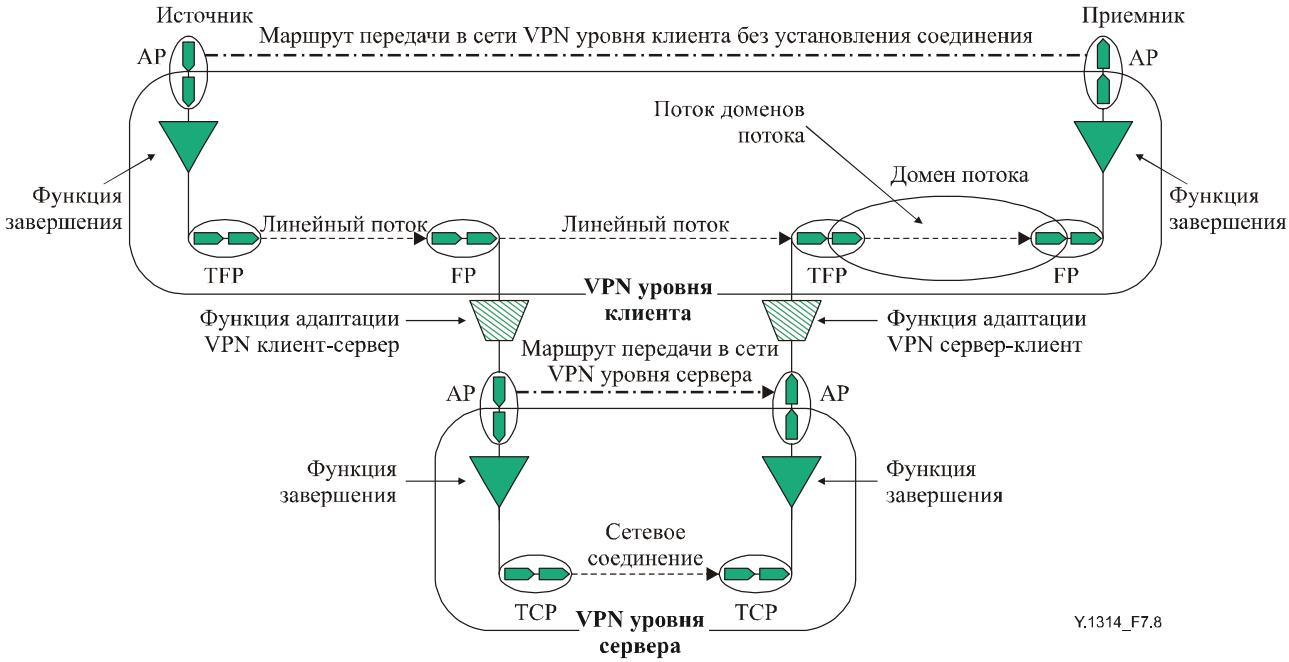


Рисунок 7-8/Y.1314 – CO VPN уровня сервера with a CL client

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 характеристическую информацию (CI) CL сети VPN уровня клиента, преобразуя ее в адаптированную информацию (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 CL сети VPN уровня клиента.

7.4 Несколько сетей уровня VPN клиента

В примерах, до сих пор рассматриваемых в этом разделе, для полного сквозного соединения использовалась одна-единственная сеть VPN уровня клиента. Однако, это не всегда так, пользователь может пожелать использовать на одной стороне сети VPN один тип сети VPN уровня клиента, а на другой стороне сети VPN – другой тип сети VPN уровня клиента. Например, на одной стороне может применяться IP сеть VPN уровня клиента, а на другой – это может быть MPLS, или на одной стороне может применяться технология ретрансляции кадров (Frame Relay – FR), а на другой – ATM. В таких случаях две различные сети VPN уровня клиента должна взаимодействовать на равных основаниях.

Следует отметить, что термин 'Сеть VPN уровня клиента', используемый здесь, представляет собой набор точек доступа одного типа, соединенных для передачи CI в сети VPN уровня клиента. Он не обозначает сетевые уровни Уровень 1, Уровень 2, Уровень 3, т. е. из двух сетевых технологий, взаимодействующие в VPN на уровне клиента, обе технологии могут быть технологиями Уровня 2 (например, одна может быть технологией ATM, а другая – FR), но они считаются разными сетевыми уровнями, поскольку в них находятся различные точки доступа, которые также являются точками разного типа.

Функция взаимодействия может выполняться либо до функции адаптации источника сети VPN уровня сервера, либо после функции адаптации приемника сети VPN уровня сервера. На рисунке 7-9 показана физическая топология сети VPN клиент-сервер, в которой на каждой стороне сети VPN используются различные сети VPN уровня клиента.

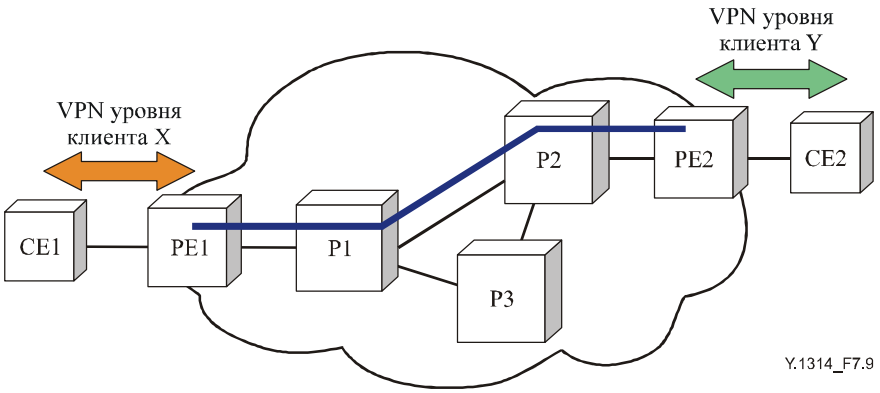


Рисунок 7-9/Y.1314 – Физическая топология сети VPN клиент-сервер уровня равноправного взаимодействия

На рисунке 7-10 представлена общая функциональная модель равноправного взаимодействия сети VPN уровня клиента, основанная на физической топологии, показанной на рисунке 7-9, где функция взаимодействия выполняется до функции адаптации источника сети VPN уровня сервера.

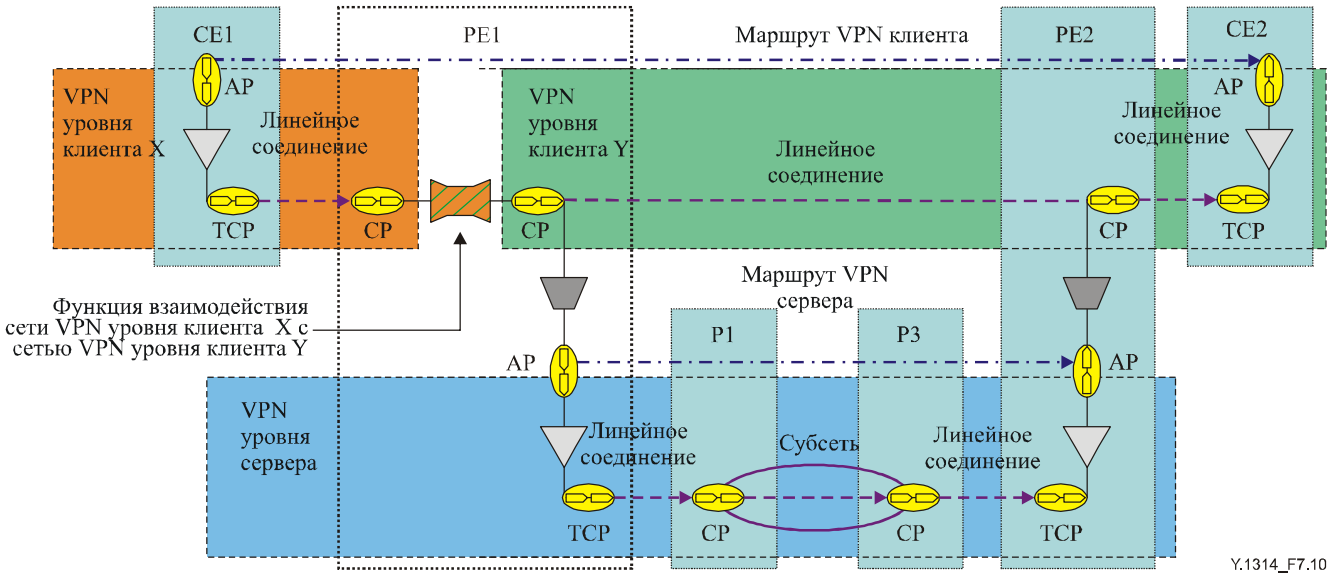


Рисунок 7-10/Y.1314 – Равноправное взаимодействие сети VPN клиента (адаптация до источника сервера VPN)

Две гетерогенных сети VPN уровня клиента в этой модели – это сеть VPN уровня клиента X и сеть VPN уровня клиента Y. В этом примере функцию взаимодействия выполняет PE, но она может также выполняться отдельным устройством. 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, если VPN уровня 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 (например, используя FRF.8), и трафик сети VPN уровня клиента будет передаваться по сети VPN уровня сервера как трафик ATM.

На рисунке 7-11 представлена общая функциональная модель равноправного взаимодействия сети VPN уровня клиента, где функция взаимодействия выполняется после функция адаптации приемника сети VPN уровня сервера.

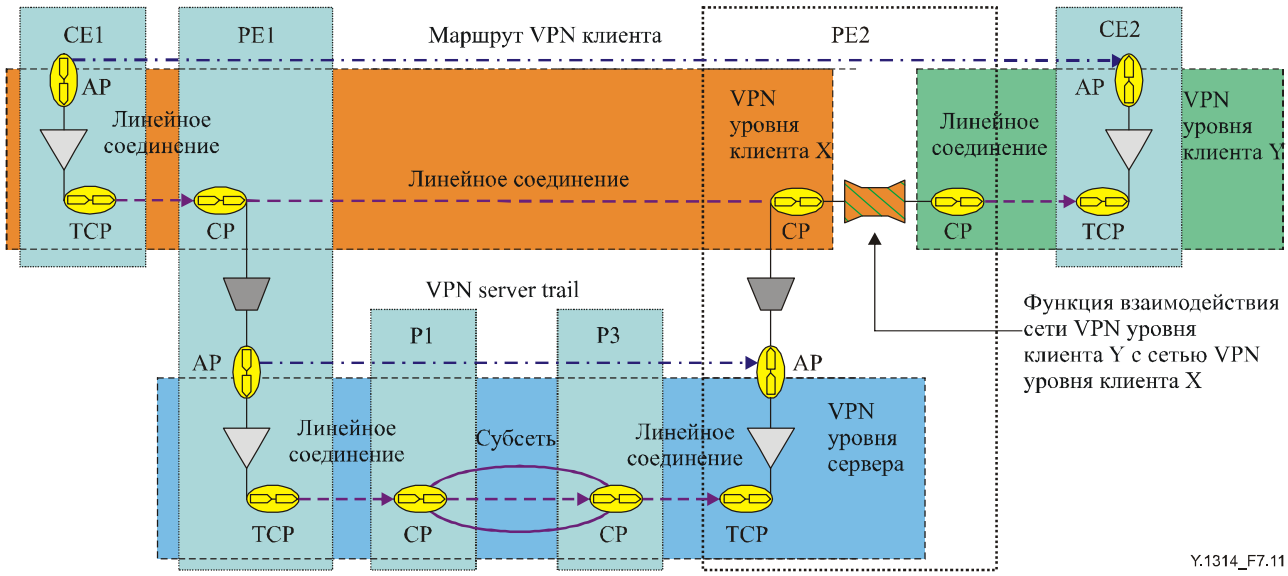


Рисунок 7-11/Y.1314 – Равноправное взаимодействие сети VPN клиента (адаптация после приемника сервера VPN)

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.

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

Хотя 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 Дополнении II приведены примеры равноправного взаимодействия и взаимодействия клиент-сервер для нескольких уровней сервера, а также некоторые соображения относительно этих вариантов.

Следует отметить, что 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 7-12, 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 (применяя вложенные метки MPLS) ниже сети VPN уровня сервера, и использовать сеть IP уровня сервера (например, применяя инкапсуляцию GRE) на другом участке сети.

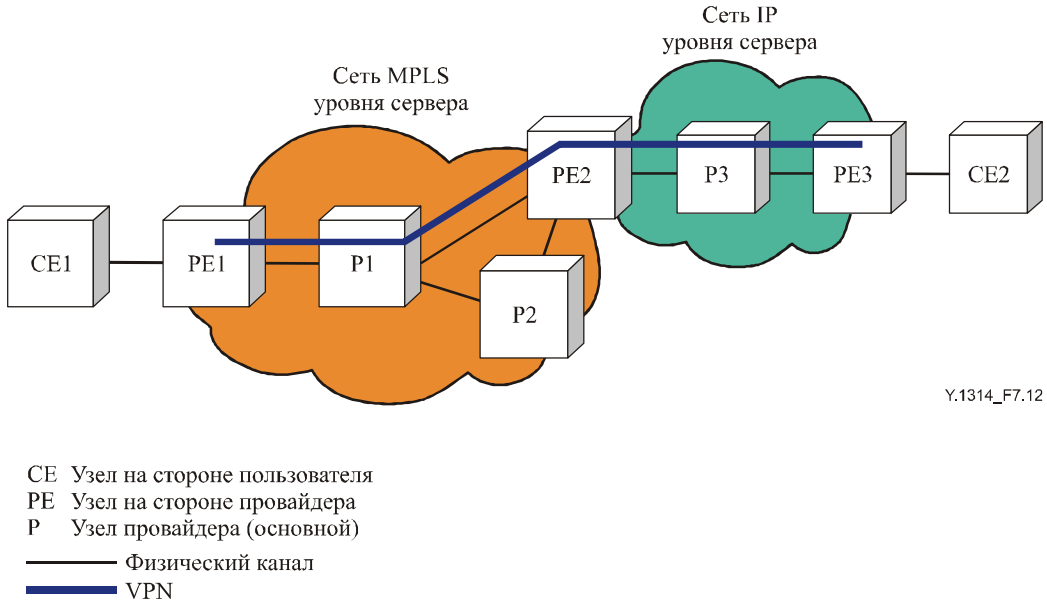


Рисунок 7-12/Y.1314 – Сеть VPN клиент-сервер с сетями MPLS и IP уровнями сервера

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, относящаяся к сети, показанной на рисунке 7-12, описывается на рисунке 7-13.

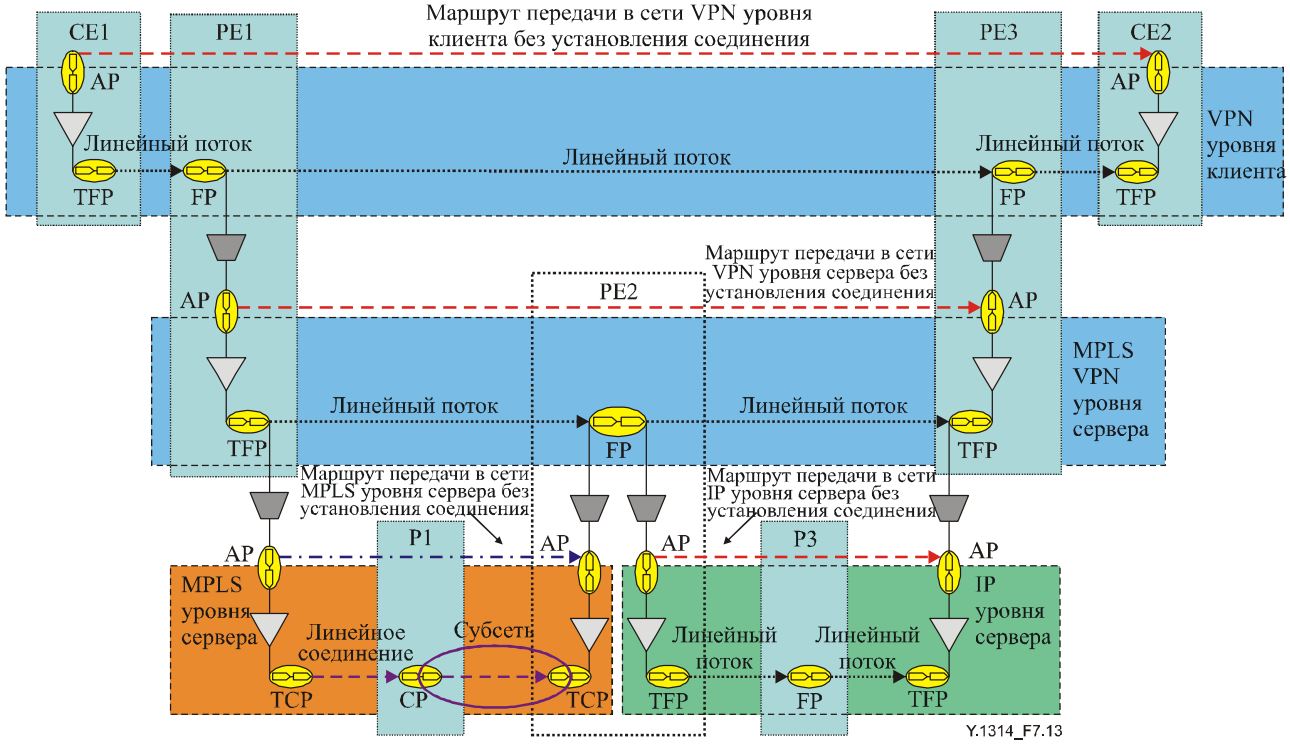


Рисунок 7-13/Y.1314 – Сеть VPN уровня сервера, поддерживаемая несколькими уровнями сервера

В этом примере функция адаптации источника сети MPLS уровня сервера преобразует характеристическую информацию (CI) MPLS сети VPN уровня сервера (которая является клиентом сети MPLS уровня сервера) в адаптированную информацию (AI) в сети MPLS уровня сервера, а функция адаптации приемника сети MPLS уровня сервера преобразует AI сети MPLS уровня сервера, в характеристическую информацию (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 характеристическую информацию (CI) MPLS сети VPN уровня сервера.

7.6 Моделирование сети VPN с применением деления на части

Функциональные модели, приведенные в предыдущих параграфах, были разработаны с применением многоуровневого подхода. Разделив сеть на множество независимых сетей различных уровней, можно смоделировать взаимодействие клиент-сервер между сетями смежных уровней, а также описывать соответствующие функции адаптации, 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 позволяет разделить субсеть одного уровня на несколько содержащихся в ней субсетей и каналы связи между ними. Такое деление может продолжаться до тех пор, пока не будет достигнут предел рекурсии, то есть, пока отдельные субсети не будут состоять из одного сетевого элемента. Этот подход известен как матрицирование, описанное в Рек. МСЭ-Т G.805. Деление на части показано на рисунке 7-14.

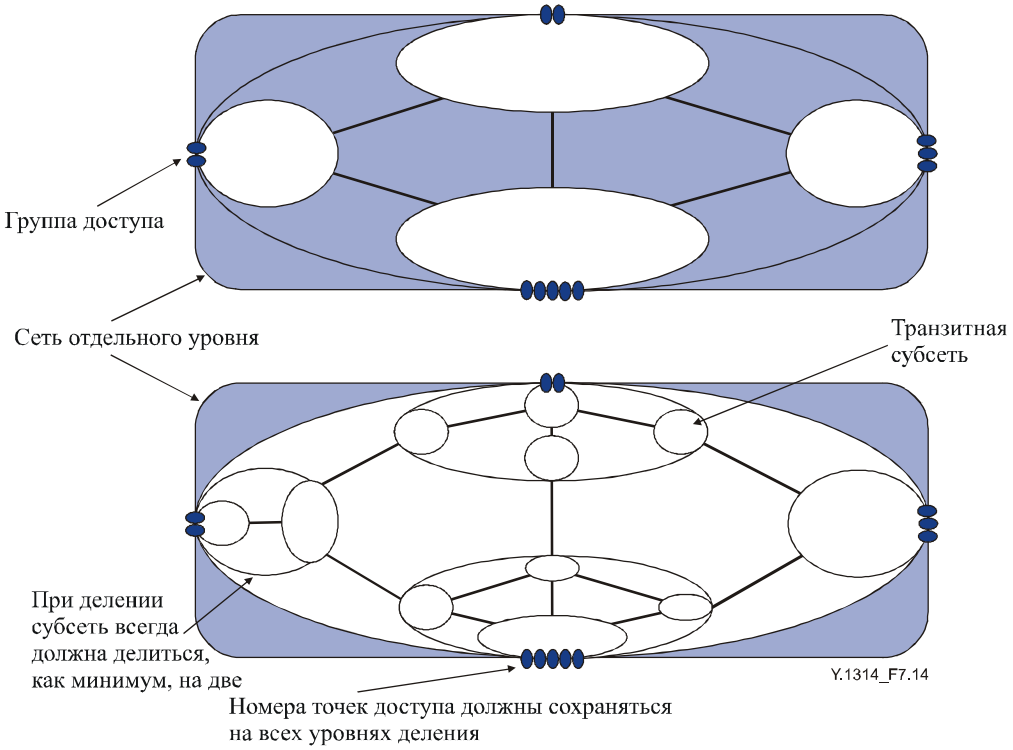


Рисунок 7-14/Y.1314 – Деление субсетей в пределах одного уровня сети

В ходе процесса деления сети на части, число точек потока/соединения в наибольшей субсети остается неизменным, при этом выявляются точки соединения, являющиеся внутренними на следующем уровне деления. С точки зрения соединения, субсеть (домен потока) представляет собой гибкое звено между входами и выходами соединения (например, точками доступа источника/приемника или точками потока/соединения). Как правило, такое положение дел позволяет любой вход соединить с любым выходом.

Эта модель достаточна для сетей общего пользования, где все ресурсы можно считать доступными для использования. Однако, она непригодна для виртуальных выделенных сетей. Причина этого – в том, что возможность установления соединения между входами и выходами в субсети/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 "Фрагмент домена потока" (FDFr), описанные в Рек. МСЭ-Т G.8010, и конструктивные единицы "Субсетевое соединение" (SNC). Единицы FDFr/SNC разбиваются на фрагменты при помощи выделения в различные группы их входов и выходов. Возможность установления соединения ограничена, оно может быть установлено только между членами одной группы. Такая группа может быть сетью VLAN на мосту Ethernet (домене потока Ethernet) или сетью VPN в субсети или домене потока. Отметим, что фрагмент не содержит точек потока; они связаны с доменом потока. Единица FDFr/SNC может носить 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, показан на рисунке 7-15.

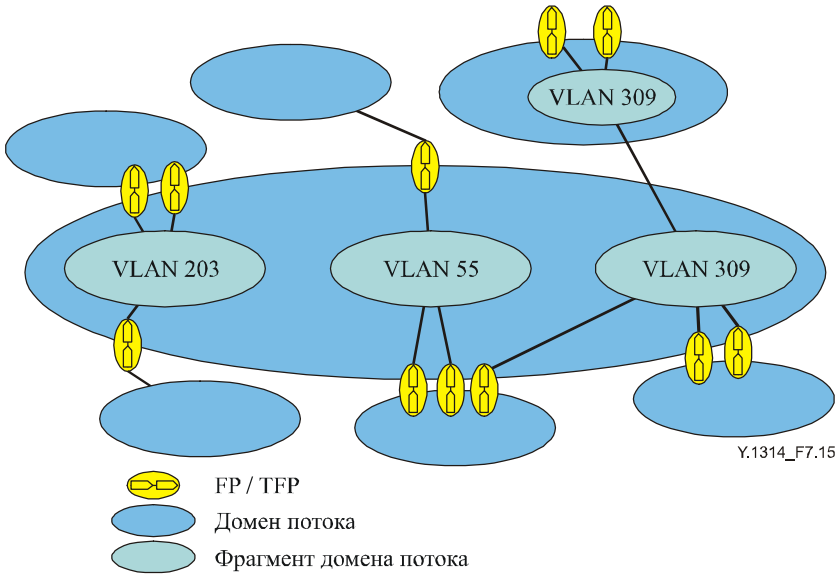


Рисунок 7-15/Y.1314 – Пример функциональной модели деления сети VPN

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

7.7 VPN уровня равноправного взаимодействия

На рисунке 7-16 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 может быть обеспечена с использованием любого из подходов, определенных в разделе 6, например, сеть VLAN Ethernet, туннель IPsec и т. д.

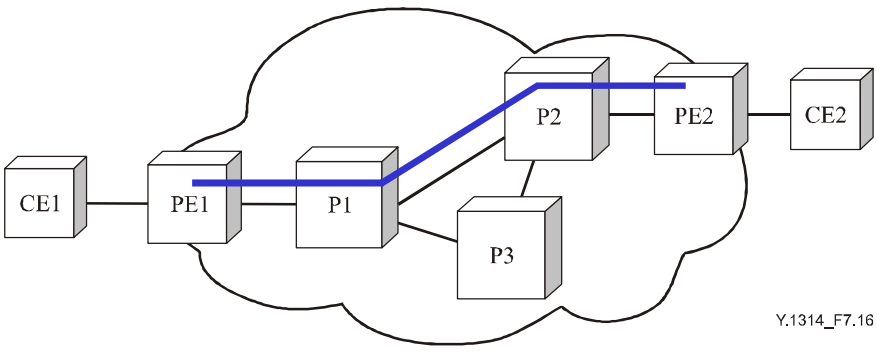


Рисунок 7-16/Y.1314 – Пример физической топологии VPN уровня равноправного взаимодействия

На рисунке 7-17 топология сети VPN, показанная на рисунке 7-1, описана с точки зрения функциональной перспективы, здесь изображен уровень VPN и один нижележащий уровень сервера между точками PE. В этом примере уровень сервера работает с установлением соединения (CO), но он *также может работать* и без установления соединения (CL).

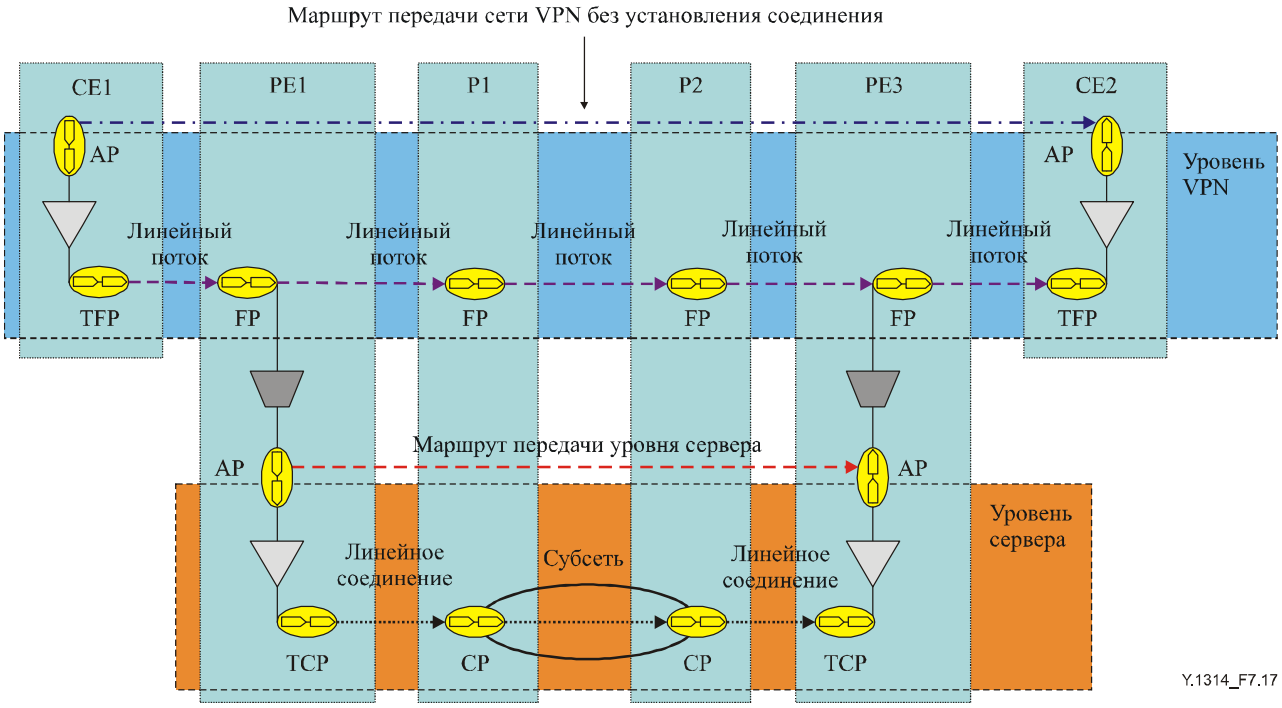


Рисунок 7-17/Y.1314 – Модель уровня для одного VPN уровня

Как показано на рисунке 7-17, все узлы сети (включая узлы P) принадлежат уровню VPN и, следовательно, они должны быть способны перенаправлять пакеты в нужном направлении, используя информацию из заголовков пакетов VPN соответствующего уровня. Благодаря архитектуре одного уровня VPN, многоуровневая модель не предоставляет столько информации, сколько предоставляется в том случае, когда она используется для сети VPN клиент-сервер. В частности, формат представления на рисунке 7-17 не дает никаких сведений о том, где начинается сеть VPN, и где она заканчивается. Одним из способов ввести эту информацию является расширение функций адаптации в сети VPN/уровне сервера. На рисунке 7-18 показано два различных примера функций адаптации сети VPN/уровня сервера, одна из которых использует метки IPsec, а другая – метки Ethernet VLAN.

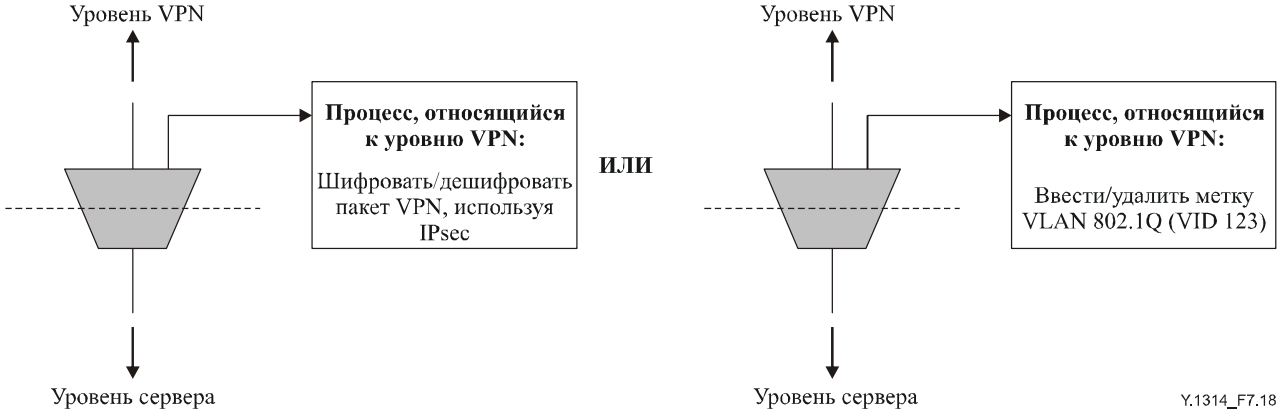


Рисунок 7-18/Y.1314 – Расширение функций адаптации в сети VPN/на уровне сервера

Другим способом для описания VPN уровня равноправного взаимодействия используется концепция деления, введенная в §7.6. Пример того, как может использоваться деление, приведен на рисунке 7-19.

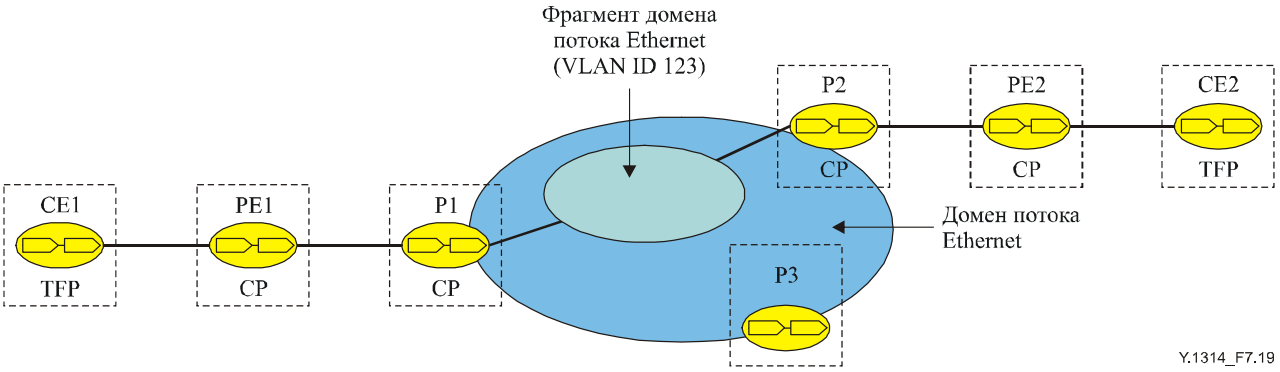


Рисунок 7-19/Y.1314 – Моделирование VPN уровня равноправного взаимодействия с использованием деления

На рисунке 7-19 показана 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 IEEE 802.1Q. Из модели на рисунке 7-19 легко увидеть, что узлы P1 и P2 входят в состав VLAN 123, но, несмотря на то, что PE1 и PE2 являются 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 (как показано на рисунке 7-18).

8 Поддержка VPN топологии

Термин 'VPN топология', используемый в тексте настоящей Рекомендации, обозначает топологию сети с точки зрения пользователя VPN, т. е., топологию между сайтами VPN, которые могут быть узлами CE или оконечными системами. Соединение между сайтами VPN может быть обеспечено, если только между ними были установлены маршруты VPN уровня сервера или уровня равноправного взаимодействия. Как правило, топология уровня n зависит от топологии, обеспечиваемой маршрутами уровня сервера на уровне n–1. После того, как установлены маршруты 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 (VPN сайты не могут связываться, если между ними нет маршрутов). Может использоваться еще один метод ограничения возможностей соединения – фильтрация пакетов (например, основанная на адресах источника/приемника сети VPN уровня клиента или уровня равноправного взаимодействия). Тремя основными топологиями VPN является – топологии полносвязной ячеистой сети VPN, топологии частичной ячеистой сети VPN и топологии звездообразной сети VPN , они описаны в параграфах 8.1, 8.2 и 8.3.

8.1 Топологии полносвязной ячеистой сети VPN

В топологии полносвязной ячеистой сети VPN каждый сайт сети VPN имеет маршрут/соединение с каждым другим сайтом сети VPN, как показано на рисунке 8-1.

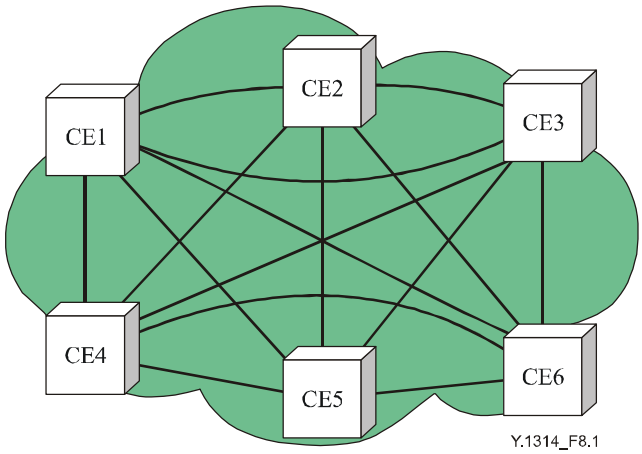


Рисунок 8-1/Y.1314 – Пример топологии полносвязной ячеистой сети VPN

Топология полносвязной ячеистой сети VPN обеспечивает полную избыточность и может также обеспечить эффективное использование сети и хорошие качественные показатели, поскольку сайты сети VPN могут использовать 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, хотя это зависит от применяемых режимов/технологий сети VPN (например, вероятно, что сеть VPN топологии полносвязной ячеистой сети VPN, созданная из виртуальных каналов (VC) технологии ATM, окажется дороже VPN сети Ethernet, поддерживающей соединение каждый-с-каждым). Другой недостаток заключается в том, что 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 полносвязной 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.

8.2 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 показан на рисунке 8-2.

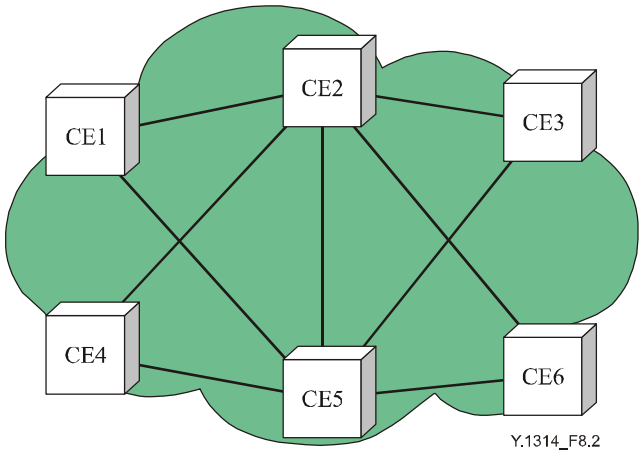


Рисунок 8-2/Y.1314 – Пример топологии частичной ячеистой сети VPN

В некоторых случаях 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. Однако, 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, 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, хотя это сделано за счет снижения оптимальности маршрутизации и эффективности использования сети (если некоторые узлы CE используются как транзитные узлы). 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 8-2 CE узлы CE2 и CE5 могут быть основными узлами, а другие узлы CE могут быть пограничными узлами. В таком случае, 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 (т. е. сети топологии полносвязной ячеистой сети стоят намного дороже) и географических ограничений.

8.3 Топологии звездообразной сети VPN

В топологии звездообразной сети сайт VPN может быть либо центром, либо одним из лучей "звезды", образующей соединения для конкретной сети VPN (хотя, если сайт VPN входит в состав нескольких сетей VPN, в некоторых из них он может быть центром, а в других – лучом). Все лучи в топологии звездообразной сети имеют прямые маршруты/соединения с центральным узлом, но не имеют маршрутов/соединений между собой. На рисунке 8-3 показан пример топологии звездообразной сети, в которой узел CE2 является центральным, а все остальные узлы CE – лучами.

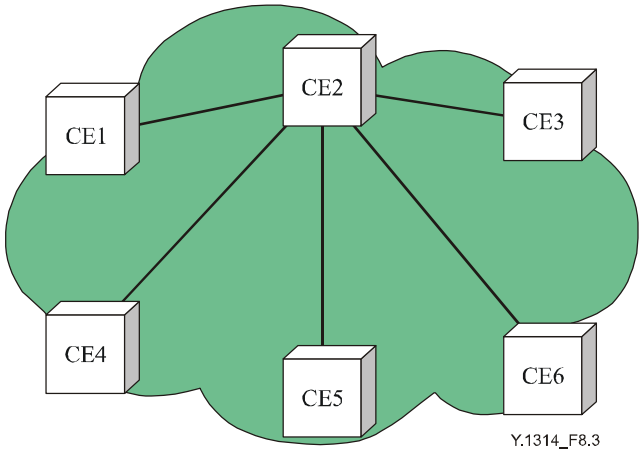


Рисунок 8-3/Y.1314 – Пример топологии звездообразной сети VPN

В некоторых случаях, центральный узел может быть сконфигурирован как транзитный узел, при этом лучи могут связываться друг с другом через центральный узел. Однако, в других случаях, связь между узлами в лучах звезды может не быть допустимой. Наиболее широко топология звездообразной сети используется для соединения офисов (лучи) со штаб-квартирой корпорации (центральный узел). 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.

9 Аспекты качества обслуживания (QoS) в VPN

Имеется множество источников информации о качестве обслуживания (QoS), которые содержат различные определения того, что же, на самом деле, означает QoS. В Рекомендации МСЭ-Т E.800 QoS определяется как суммарный эффект от характеристик услуги, который определяет степень удовлетворенности пользователя услуги. В Рекомендации МСЭ-Т G.1000 приведены основные сведения и определения качестве услуги связи, а в Рекомендации МСЭ-Т G.1010 определена модель

категорий качества (QoS) мультимедиа услуг с точки зрения оконечного пользователя. Функции, требуемые для удовлетворения требований по качеству обслуживания, определенных в этих Рекомендациях и в других документах, зависят от режима работы сети. Следовательно, требования по качеству обслуживания могут влиять на выбор провайдером VPN услуг технологий сетей VPN уровня сервера и уровня клиента, которые он будет поддерживать.

9.1 Сети с коммутацией каналов

В сетях с установлением соединения и с коммутацией каналов маршрут, построенный на основе физических линий, длин оптических волн, виртуальных контейнеров (VC) СЦИ/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 управления установлением соединений (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 зависит от наличия в сети свободной емкости. Если соединение установлено, то доставка данных по этому соединению гарантирована.

В сетях с установлением соединения и с коммутацией каналов (CO-CS), таких как КТСОП, задержка зависит, главным образом, от расстояния передачи. Задержка коммутации на узлах сетей CO-CS относительно мала по сравнению с задержкой передачи (распространения) сигнала, особенно, когда вызовы передаются по магистральным линиям дальней связи.

9.2 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 (на основании предположения о том, что не всем пользователям ресурсы необходимы постоянно). Способ передачи пакетов в потоках или в соединениях можно описать набором параметров, которые называются 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, как правило, 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 (NE) 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 (которая распределяется между процессами пакетирования, компрессии/декомпрессии, коммутации/маршрутизации, записи в буфер и извлечения из буфера) и число пролетов. В сетях с коммутацией пакетов необходимо управление приоритетами для того, чтобы гарантировать разные уровни качества обслуживания. Как правило, 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.

9.2.1 Сети с установлением соединения и с коммутацией пакетов

В сетях с установлением соединения и с коммутацией пакетов соединения устанавливаются и поддерживаются до тех пор, пока не пропадает необходимость в этом соединении (вне зависимости от

того, передаются ли по нему данные или нет). Также как и в сетях с установлением соединения 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 постоянной скоростью передачи (CBR). Альтернативно, могут использоваться схемы статистического мультиплексирования с механизмами CAC для выделения меньшей, чем требуется пиковой емкости для повышения эффективности работы сети. Однако, может быть непросто оценить емкость запрашиваемого соединения, поскольку требуемая пропускная способность может существенно меняться с течением времени.

В сети CO-PS (например, ATM), CBR (без подписки) относительно задержки на один пролет остается постоянной и, следовательно, можно рассчитать/гарантировать задержку/дрожание. Однако, если спрос на услуги намного выше предложения, и использование сети увеличивается (что обычно и бывает), то на перегруженных узлах пакеты будут задерживаться/теряться из-за буферизации или отбрасывания избыточного трафика. Несмотря на то, что величина задержки на пролет становится переменной, другие факторы, например, скорости в канале, расстояние передачи/число пролетов (и размер пакета в сети ATM) остаются постоянными.

9.2.2 Сети без установления соединения с коммутацией пакетов

В сетях без установления соединения с коммутацией пакетов (CL-PS) соединение разрывается после того, как данные переданы, и его не существует до момента передачи или приема следующей информации (пакет можно рассматривать как соединение, которое существует на протяжении того времени, которое требуется для передачи или приема этого пакета). Никакого состояния соединения не сохраняется и, следовательно, 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, как правило, выделяются по схеме "первый пришел – первый обслужен".

В сетях CL-PS (например, сетях IP), 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 могут применяться механизмы ограничения скорости/формирования трафика для ограничения объема трафика, входящего в сеть, однако из-за природы трафика в сети CL-PS, где все связаны со всеми (и роста числа равноправных сетевых соединений), очень трудно предсказать, какая емкость будет использована для каждого соединения в сети CL-PS. Для формирования матрицы трафика могут использоваться методы контроля трафика и методы моделирования, а показатели Внутреннего межсетевого протокола (IGP) могут 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.

Однако, даже при наличии в сети избыточных ресурсов, из-за неопределенного характера трафика в сети без установления соединения, узлы/каналы сети CL-PS могут оказаться перегруженными, особенно в случае неисправности узла/канала или отказа в обслуживании (DoS). Кроме того, 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 очередей (например, по принципу, описанному в RFC 2475 "Архитектура дифференцированного обслуживания для IP) для управления характеристиками передачи в зависимости от класса обслуживания, т. е. трафик с наивысшим приоритетом получает предпочтение в обработке по отношению к трафику с меньшим приоритетом. Это позволит провайдеру предложить пользователю несколько уровней обслуживания (например, высший приоритет, связь в реальном времени, предоставление наилучших условий) с соответствующими расценками. Недостаток подхода дифференцированного обслуживания (Diffserv) заключается в том, что емкость может резервироваться только в виде общего объема и, следовательно, невозможно гарантировать доставку отдельных потоков в этом общем объеме.

Альтернативным (или дополнительным) подходом является использование Архитектуры интегрированного обслуживания (основанной на RFC 1633), в которой для резервирования емкости на сквозном маршруте используется Протокол резервирования ресурсов (RSVP, RFC 2205), который сообщает о потребностях потока до начала передачи пакетов. Благодаря тому, что емкость резервируется для каждого потока отдельно, можно обеспечить 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, проблема здесь заключается в том, что объем обработки растет с увеличением числа потоков. Однако, сегодня имеются маршрутизаторы, поддерживающие режим потоковой маршрутизации большого числа потоков.

10 Функции, требуемые для создания VPN клиент-сервер

При создании сети VPN клиент-сервер 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 (для которого сеть VPN уровня сервера является клиентом). Этот порядок установления потоков/соединений определяется тем фактом, что топология уровня клиента определяется топологией, и такое положение дел сохраняется на все уровни вниз.

10.1 Создание уровня сервера в VPN

Предполагая, что топология нижележащего уровня сервера установлена, и точки TCP/TFP и CP/FP сети VPN уровня сервера сконфигурированы с адресами, имеется три основных этапа создания соединений VPN уровня сервера между элементами сети VPN уровня клиента:

Этап 1: Определить элементы сети VPN и записать их данные.

Этап 2: Рассчитать маршруты между элементами сети VPN уровня сервера.

Этап 3: Установить соединения/туннели/сети VLAN между элементами VPN уровня сервера.

В таблице 10-1 подробно описана каждая функция, необходимая для создания в VPN уровня сервера и поддержания его работы вместе с отдельными функциональными блоками.

Таблица 10-1/Y.1314 – 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) маршрута(ов) 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 демультиплексирования, пропускная способность и т. д.	PE, P	Все

10.1.1 Определение элементов сети VPN

Для установления топологии сети VPN уровня сервера между узлами PE, необходимо сначала определить, какие узлы PE соединяются с узлами CE, принадлежащими конкретной сети VPN клиент-сервер. Эта функция может 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 (например, RADIUS), служащий для распространения информации об элементах сети VPN, как части аутентификации клиента. Примером распределенного протокола является использование протокола BGP для сетей VPN RFC 2547, 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.

10.1.2 Маршрутизация в VPN уровня сервера

Если нижележащий уровень сервера (уровень ниже VPN уровня сервера) между точками завершения источника/приемника сети VPN уровня сервера представляет собой однопролетное соединение/поток P2P, то здесь никакой маршрутизации не требуется, поскольку доступен только один маршрут. С другой стороны, если имеются альтернативные маршруты/пути в одну и ту же точку через различные промежуточные узлы, или если нижележащий уровень сервера формирует топологию P2MP[4], то в сети VPN уровня сервера должна быть выполнена маршрутизация для того, чтобы определить топологию и/или вычислить наилучший(е) маршрут(ы) до пункта назначения.

10.1.2.1 Необходимость маршрутизации

В сетях с установлением соединения сигнализация не может быть выполнена, пока не рассчитан маршрут/путь на данном уровне. В сетях без установления соединения пакет не может быть передан до тех пор, пока не рассчитан/сконфигурирован маршрут до пункта назначения. Это не означает, что для каждого узла в сети должен быть явным образом прописан маршрут к каждому другому узлу в сети. Для улучшения масштабирования широко используется сокращение сетевых адресов, совмещенное с иерархией домена маршрутизации. Основной формой сокращения адресов является использование маршрутов "по умолчанию", которые могут применяться как универсальный механизм для передачи пакета вне зависимости от адреса его пункта назначения.

Одно исключение из того правила, состоящее в том, что пакет CL не может быть передан до тех пор, пока не рассчитан маршрут (или не сконфигурирован маршрут "по умолчанию"), реализуется, когда технология CL используется для радиовещательной передачи. 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). Примером технологии, которая поддерживает такую возможность, является Ethernet. Еще одним исключением из этого правила является способ работы сетей технологии token ring (маркерное кольцо). В сетях token ring, когда какой-либо узел принимает пакет, он передает этот пакет следующему узлу в кольце, это продолжается до тех пор, пока пакет не вернется на создавший его узел, где он удаляется. Узел, являющийся пунктом назначения для этого пакета, сохраняет его копию, и сообщает о получении пакета, вводя биты ответа в кадры пакета. Несмотря на то, что существуют технологии, в которых не требуется маршрутизации, следует отметить, что эти технологии не являются идеальными технологиями для сети VPN уровня сервера. Для того чтобы многоуровневые сети охватывали множество узлов на огромной географической территории, маршрутизация и иерархическая адресная структура являются основополагающими требованиями. Такие механизмы, как радиовещательная передача и token ring, с точки зрения сети VPN, являются незащищенными и малоэффективными для передачи однонаправленного (P2P) трафика.

---

[4] Ссылка на топологию P2MP здесь указывает на топологию вешнего сервера с точки зрения единственного PE источника· Реальная общая топология данного сетевого уровня может быть "все-ко-всем", основанная на полной/частичной "mesh"-топологии двунаправленных соединений/потоков между различными PE.

10.1.2.2 Примерные сетевые топологии, требующие маршрутизации

На рисунке 10-1 показан пример сети, где имеется два альтернативных маршрута/пути до одного и того же пункта назначения (A и B).

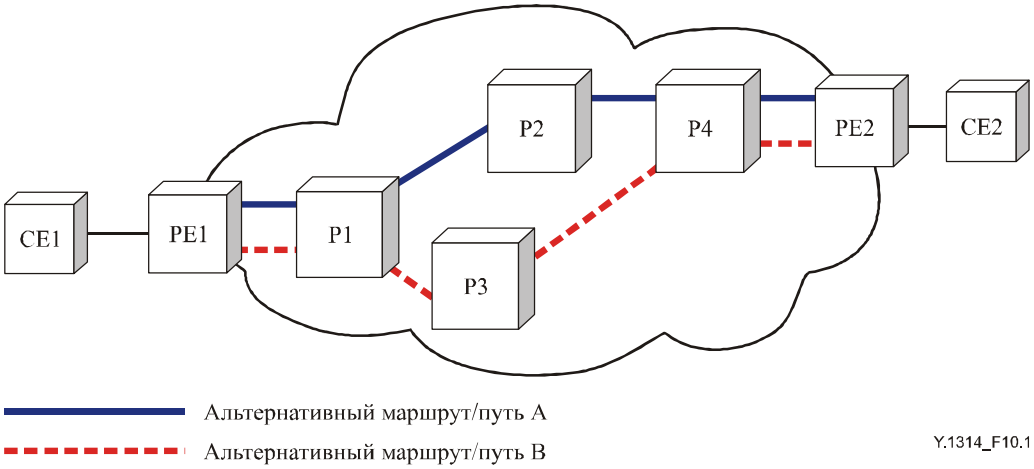


Рисунок 10-1/Y.1314 – Несколько маршрутов/путей до одного пункта назначения

Как видно из рисунка 10-1, 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 10-2 это изображено в виде функциональной модели.

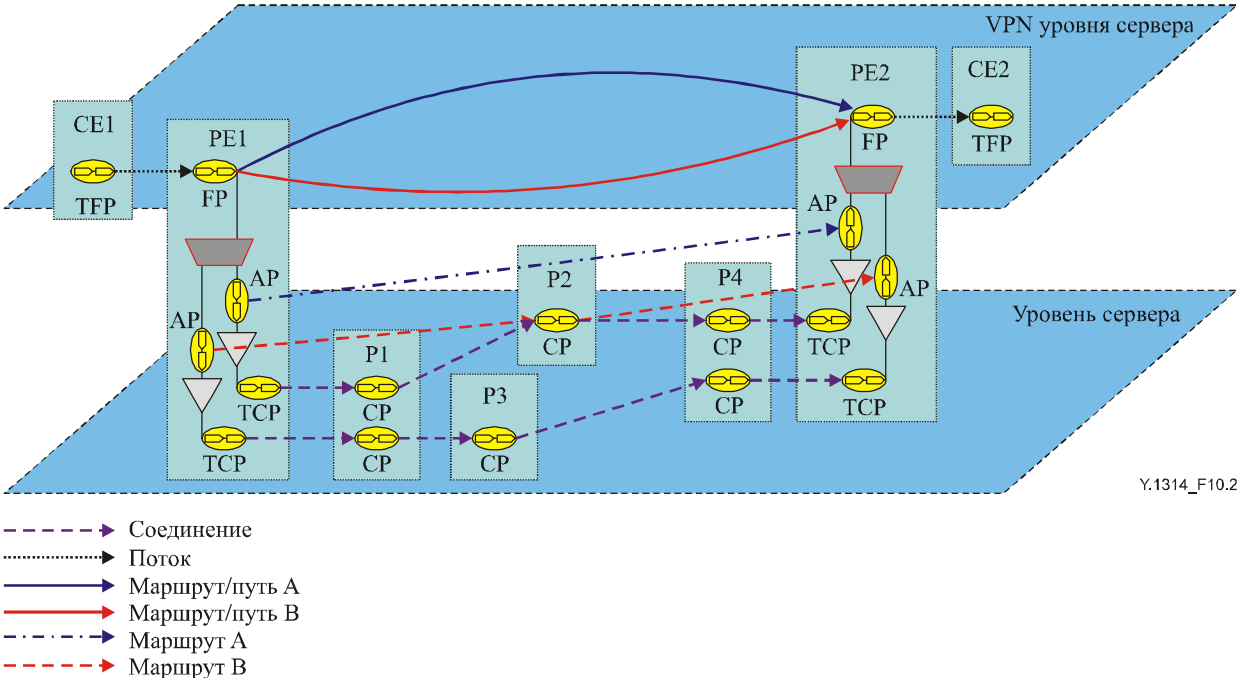


Рисунок 10-2/Y.1314 – Функциональная модель нескольких маршрутов/путей

На рисунке 10-2 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 (или оба, если требуется уравновесить нагрузку) для того, чтобы передать поток(и) в сети VPN уровня сервера между TFP источника сети VPN уровня сервера, расположенной в CE1, и TFP приемника, расположенной в CE2.

На рисунке 10-3 показан случай, когда на уровне сервера обеспечивается соединение P2MP от CE1 (источник) до CE2, CE3 и CE4 (разветвленные приемники в топологии P2MP).

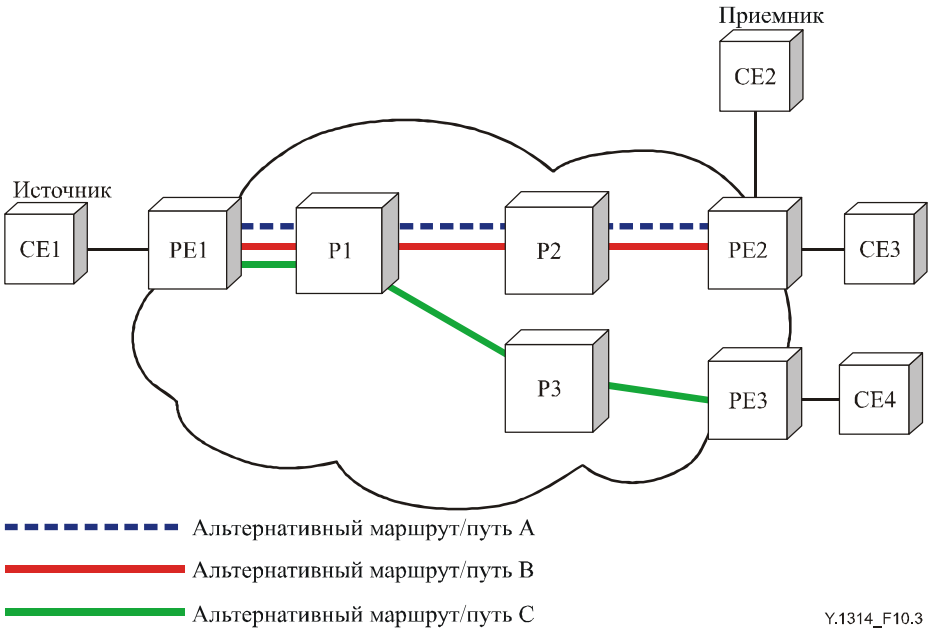


Рисунок 10-3/Y.1314 – Топология P2MP на уровне сервера

Сеть, изображенная на рисунке 10-3, показана на рисунке 10-4 как функциональная модель.

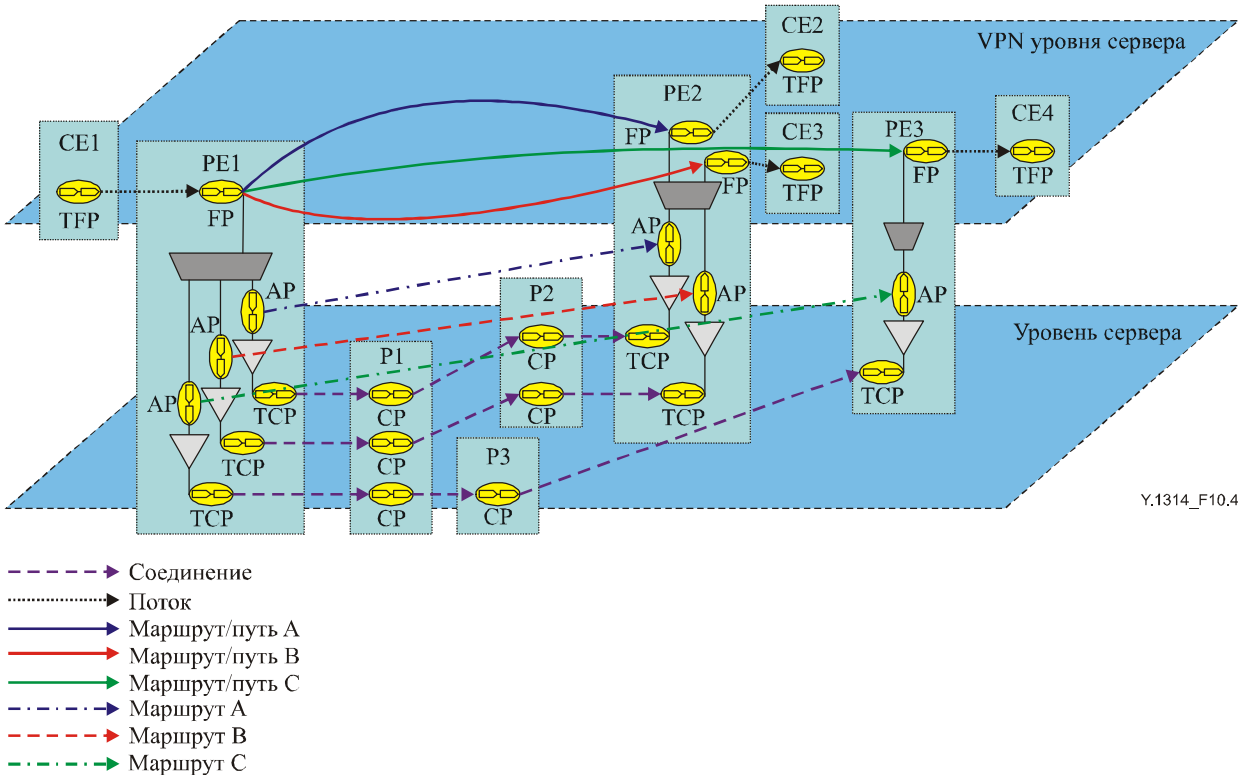


Рисунок 10-4/Y.1314 – Функциональная модель топологии P2MP на уровне сервера

Если CE1 – источник, а CE2 – приемник для определенного потока в сети VPN уровня сервера, то CE1 должен знать, каков путь до CE2. Однако, маршруты/пути в сети VPN уровня сервера, показанные на рисунке 10-4, поддерживаются маршрутами P2P на нижележащем уровне сервера, т. е., в топологии P2MP существует только один путь от TFP источника до TFP каждого разветвленного приемника. Это значит, что функция маршрутизации требуется только для определения топологии, она не требуется для расчета маршрута (поскольку существует только один путь до приемника). После определении топологии, потоки от CE1 в направлении CE2 будут использовать маршрут/путь A, поддерживаемый маршрутом A на уровне сервера.

10.1.2.3 Альтернативные способы маршрутизации

Когда требуется маршрутизация, оператор может выполнить маршрутизацию вручную, в таком случае он вычисляет маршруты по сети на основании известной топологии сети и информации об использовании ресурсов. Одним из примеров ручного выполнения маршрутизация является конфигурирование двусторонних узлов CE, когда сеть VPN уровня клиента является IP сетью. В этом примере может оказаться разумным применение статических маршрутов (т. е. с одним основным и одним "плавающим" маршрутами "по умолчанию"), поскольку существует только два альтернативных маршрута.

Если для выполнения функции маршрутизации используется система управления сетью (NMS), то эта 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 примеров выполнения маршрутизация при помощи NMS, является установление P2P соединений на СЦИ уровне сети. До того как соединение может быть установлено, NMS должна сначала рассчитать наилучший(е) маршрут(ы) в сети.

Если для выполнения маршрутизации используется динамический протокол маршрутизации, то 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 примеров динамического протокола маршрутизации является составная часть маршрутизации через интерфейс между выделенной сетью и сетью общего пользования (PNNI), используемая в сетях ATM (хотя он также может использоваться с другими сетевыми технологиями) для определения топологии сети и расчета маршрутов для динамических соединений. Другой пример – отказоустойчивая сеть передачи пакетов (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 (во избежание петель топология сети усекается) и прозрачные мосты (основанные на выяснении адреса источника) в плоскости данных для передачи пакетов в нужный пункт назначения без необходимости их передачи на все узлы/оконечные станции. Однако, если используется выяснение адреса в плоскости данных, то сетевая технология должна поддерживать также и радиовещательную передачу пакетов с еще не выясненными адресами пункта назначения. Из-за того, что до тех пор, пока не получены пакеты с соответствующими адресами, маршруты не известны в сетях CO выяснение адреса в плоскости данных не может быть использовано для выполнения функции маршрутизации, оно пригодно только для сетей CL.

10.1.3 Сигнализация в сети VPN уровня сервера

В настоящей Рекомендации сигнализацией называется обмен информацией, необходимой для создания CL туннелей (например, туннелей L2TP) и CO соединений (например, ATM соединений VPI/VCI). Требуемая информация включает в себя такие параметры, как поля мультиплексирования/демультиплексирования, QoS (например, задержка, дрожание), полоса пропускания, ключи шифрования и способность к восстановлению (например, резерв 1+1).

Одним из ключевых отличий между туннелями и соединениями является тот факт, что для установления соединения до передачи данных всегда требуется сигнализация (или ручное выделение ресурса). Хотя некоторые методы туннелирования (например, L2TP туннели, явно сконфигурированные GRE туннели) также требуют сигнализации для передачи данных о параметрах туннеля до того, как можно будет передавать данные пользователя, другие методы, такие как программные/динамические GRE туннели и туннели IP-в-IP никакой сигнализации не требуют. Эти методы туннелирования просто вводят пакет VPN уровня клиента внутрь заголовка пакета VPN уровня сервера на основании информации о местных правилах/маршрутизации. Промежуточные (P) узлы, встречающиеся между завершающими точками источника/приемника туннеля, просматривают только заголовок пакета VPN уровня сервера для того, чтобы определить, следует ли передавать этот пакет в направлении приемника VPN уровня сервера (PE пункта назначения) и как это сделать. Заголовки VPN уровня клиента используются только, 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 (например, маршрутизации) во внутренних заголовках VPN уровня клиента.

Управление установлением соединений (CAC) выполняется во время установления соединения для определения того, имеется ли на нижележащем уровне сервера достаточная полоса пропускания для удовлетворения потребностей QoS уровня клиента. Дескрипторы трафика (например, для ATM это – пиковая скорость передачи (PCR) и поддерживаемая скорость передачи (SCR)) 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.

В том случае, когда уровни сервера имеют конфигурацию CO-CS, функция CAC основывается на физическом объеме полосы пропускания, имеющемся в наличии на том сетевом уровне, где она запрашивается (например, свободные слоты времени для сетей TDM или свободные длины волн для WDM). В том случае, когда 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 (например, объеме используемого ресурса для восходящих и нисходящих соединений) каждого соединения на каждом узле для конкретного сетевого уровня. В отличие от сетей CO-CS, где доступная полоса пропускания ограничивается физической полосой пропускания, в сетях CO-PS на каждом узле в сети могут быть реализованы различные правила для каждого соединения (особенно, если предполагается статистическое мультиплексирование) для гарантии того, что каждое соединение передает/принимает только тот объем трафика, который был согласован во время установления соединения.

В том случае, когда 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. Как и для сетей CO-PS, на каждом узле в сети должны быть реализованы правила, основанные на величине запрошенной полосы пропускания. Однако, в отличие от сетей CO-PS, где для каждого соединения поддерживается информация о текущем состоянии, аналогичная (т. е., для каждого потока) информация в сетях CL, как правило, не поддерживается[5]. Это положение дел, вместе с не детерминистической природой трафика CL "все-со-всеми" означает, что функция CAC в сетях CL опирается на интенсивный контроль трафика и его моделирование для создания матрицы трафика, вместе с тем, что в сети предусмотрена избыточность ресурсов для гарантии необходимой полосы пропускания, особенно в условиях неисправности. Если для каждой VPN требуются четкое управление установлением соединений (CAC) и жесткие Соглашения об уровне обслуживания (SLA), то должна использоваться сеть CO уровня сервера, а не сеть CL уровня сервера.

---

[5] Исключением является использование RSVP RFC 2205 (решение, основанное на сквозной сигнализации) и маршрутизации потоков (решение для каждого пролета), когда поддерживается состояние каждого потока, и при отсутствии достаточной полосы пропускания новые потоки отбрасываются.

10.2 Конфигурация/аутентификация VPN уровня клиента

Функции, требуемые для установления соединения между узлами CE и PE в сети VPN уровня клиента, могут быть выполнены с использованием статического выделения ресурсов или с использованием динамических протоколов. Статическое выделение ресурсов может быть выполнено вручную или с помощью автоматических систем управления сетью. Функциональные единицы, вовлеченные в установление соединения сети VPN уровня клиента, показаны в таблице 10-2.

Таблица 10-2/Y.1314 – Функции аутентификации и конфигурации VPN уровня клиента

Функция	Функциональные единицы	Сетевые элементы	Режим работы VPN уровня клиента
Аутентификация CE/пользователя, санкционирование доступа и расчеты (AAA)	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

10.2.1 Аутентификация CE/пользователя, санкционирование доступа и расчеты (AAA)

Функция AAA CE/пользователя 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 могут выполняться устройством PE, которое соединяет CE с другим устройством или ими обоими.

В некоторых случаях может потребоваться централизованный сервер аутентификации для аутентификации пользователя/CE, а в других – в процесс аутентификации могут быть вовлечены только CE и PE. Примером первого является случай, когда для аутентификации CE устройства в сети Ethernet используется IEEE 802.1X. В этом примере PE может быть аутентификатором, а для выполнения аутентификации используется централизованный сервер аутентификации. Примером последнего является аутентификация управляющих сообщений (например, сообщений BGP) от CE для аутентификации источника сообщений и защиты от мошенничества.

10.2.2 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: адреса сети VPN уровня клиента, поля демультиплексирования сети VPN уровня клиента, идентификаторы VPN и профили/правила работы для каждой сети VPN. Конфигурация может быть выполнена в ходе аутентификации/разрешения доступа, либо независимо. Примером первого является случай, когда после успешной аутентификации CE может быть автоматически сконфигурирован с выделением ему конкретной полосы пропускания и профиля меток пакетов на основании данных, полученных от сервера аутентификации. Примером последнего является использования для назначения IP адресов CE ручной конфигурации или протокола динамической конфигурации сетевого узла (DHCP).

Адреса сети VPN уровня клиента, которые 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 (например, IP адреса для IP сети VPN уровня клиента, или адреса в соответствии с Рекомендацией МСЭ-Т E.164/NSAP для ATM 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, если используемая технология сети VPN уровня клиента всегда содержит поля демультиплексирования. Примером первого является Ethernet сеть VPN уровня клиента, которой требуется использовать

только VLAN метки, если необходимо поддерживать множество VPN. Примером последнего является сеть ATM, которая всегда использует значения VPI/VCI в заголовках пакетов. В некоторых случаях, конфигурация полей демультиплексирования будет зависеть от физической конфигурации, а не от значения конфигурации в заголовке пакета (например, присоединение кабеля к правильному входному интерфейсу на PE, соответствующему правильной длине волны выходного DWDM).

Хотя идентификатор VPN – это имя, используемое для идентификации конкретной сети VPN, и его необходимо назначать/конфигурировать только, если требуется поддержка динамического подтверждения участия в VPN и сигнализации, он может оказаться полезным для эксплуатации (например, для разрешения проблем с оплатой). Примером идентификатора VPN, используемого для динамического подтверждения участия и сигнализации, является атрибут "Цель маршрута", используемый в сетях VPN RFC 2547. Идентификатор VPN может быть статистически сконфигурирован на PE при помощи ручного/OSS выделения ресурсов или динамически (например, как часть процесса аутентификации, с использованием протокола RADIUS). Если идентификатор VPN должен использоваться для подтверждения участия/сигнализации, то он должен быть уникальным, как минимум, в пределах одного домена маршрутизации/сигнализации (и, в идеале, глобально уникальным, если требуется поддержка сетей VPN inter-AS/провайдера).

В устройстве CE, устройстве 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 и выбор маршрута/соединения для сайтов с несколькими домашними сетями (одной – основной, и одной – резервной).

10.3 Маршрутизация и сигнализация в VPN уровня клиента

Как и 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 в ней поддерживается динамическое выделение ресурсов для VPN уровня клиента, то требуется еще и сигнализация.

Важно отметить, что 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, следовательно, невозможно выполнить расчет маршрута и невозможно 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 вместе с отдельными функциональными единицами описаны в таблице 10-3.

Таблица 10-3/Y.1314 – 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(их) маршрута(ов) между точками доступа VPN уровня клиента	CE, PE	Все
Сигнализация в туннелях/соединениях VPN уровня клиента	Управление установлением соединения (CAC)	PE, P	CO-CS, CO-PS
	Сообщение об успешном/безуспешном выполнении запроса на установление туннеля/соединения	PE, P	Все
	Назначение и конфигурация полей демультиплексирования VPN уровня клиента	PE, P	Все
	Распространение информации о соединении/ туннеле VPN уровня клиента, например, QoS, полях демультиплексирования, полосе пропускания и т. д.	PE, P	Все

10.3.1 Соединение "все-со-всеми" в VPN уровня клиента без установления соединения с коммутацией пакетов (CL-PS)

Если маршруты VPN уровня сервера образуют топологию полносвязной/частичной ячеистой сети "все-со-всеми" для сети CL-PS VPN уровня клиента с несколькими сайтами, то узлы, содержащие точки TFP/FP сети VPN уровня клиента (т. е. узлы PE/CE, но не узлы P) должны принимать решения о дальнейшей передаче пакетов на основании адресной информации сети VPN уровня клиента. Это значит, что 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. Альтернативой применению динамических протоколов маршрутизации или статической маршрутизации является выяснение адреса в плоскости данных, как для сети Ethernet, которая для передачи трафика в нужный пункт назначения использует выяснение адреса на основании данных об источнике.

Информация о маршрутизации для каждой сети VPN должна быть изолирована от информации о маршрутизации других сетей VPN. То есть, необходимо обеспечить разделение передачи в VPN (т. е. гарантировать, что 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 PE – для каждой сети VPN свои, либо общие PE с логически/виртуально разделенными базами данных о маршрутизации. Альтернативой является использование общих устройств и таблиц маршрутизации, но выделение в них раздельных адресных пространств для каждого клиента VPN[6]. Примером решения на основе VPN, которое поддерживает маршрутизацию на уровне клиента VPN, является RFC 2547. RFC 2547 использует динамическую или статическую маршрутизацию от CE к PE вместе с MP-BGP для распространения информации о маршрутизации в VPN уровня клиента между PE и отдельные виртуальные таблицы маршрутизации для обеспечения изоляции маршрутов в сети VPN уровня клиента.

10.3.2 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. Однако, если требуется динамическое установление соединения по запросу, то между всеми точками CP и TCP (т. е., между узлами PE и CE) должно выполняться равноправное взаимодействие в плоскости управления (маршрутизация и сигнализация) в сети VPN уровня клиента. Кроме того, 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 значит, что функция CAC должна равноправно взаимодействовать с плоскостями управления как в сети VPN уровня сервера, так 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.

10.3.3 Управляемые пользователями соединения по запросу

Управляемые пользователями динамические соединения по запросу относятся к случаю, когда пользователи имеют некоторый или полный контроль над узлом CE, что позволяет им создавать новые соединения VPN уровня клиента. Преимущество этой возможности с точки зрения пользователя состоит в том, что она дает им гибкость динамически создавать сети VPN, когда требуется и если требуется, и платить за их использование соответственно. Например, пользователь может пожелать создать на короткий промежуток времени соединение по запросу для загрузки/перекачки большого файла (например, приложения или видеофайла) или создать надежное соединение для видеоконференции. Примером динамических, устанавливаемых по запросу, соединений VPN уровня клиента является использование PNNI для создания/разъединения SPVC соединений на маршрутах VPN уровня сервера при условии использования виртуальных маршрутов.

Одним важным фактором, который следует учитывать при рассмотрении дополнительной поддержки динамических, устанавливаемых по запросу, соединений в сетях VPN уровня клиента, является распространение информации об адресе/топологии. Маловероятно, что провайдер услуг пожелает

---

[6] Недостатки этого подхода: требуется управление адресным пространством со стороны провайдера услуг, требуется согласие пользователя использовать адрес, назначенный ему провайдером (он может пожелать использовать собственные адреса) и требуется фильтрация пакетов для изоляции сетей VPN, что является сложной и подверженной ошибкам задачей.

раскрыть пользователям топологию своей сети или внутреннюю адресацию сети из соображений безопасности. Следовательно, желательно, чтобы функция маршрутизация на PE передавала сведения о достижимости только на CE. Еще одним важным условием является принятие решения о том, какие действия должны быть предприняты во время установления соединений, если достаточной полосы пропускания нет в наличии. Способность создавать новые соединения в сети VPN уровня клиента зависит от наличия маршрутов на уровне сервера между точками завершения источника и приемника. Если маршрутов нет, то свободной полосы пропускания тоже нет, и в установлении этих соединений должно быть отказано, либо должны быть установлены новые соединения/туннели сети VPN уровня сервера (или увеличена полоса пропускания для существующих соединений/туннелей). Для того, чтобы создать новые соединения/туннели сети VPN уровня сервера или увеличить полосу пропускания для существующих соединений/туннелей, для гарантии того, что имеется полоса пропускания на нижележащем уровне сервера должна быть выполнена функция CAC.

Следовательно, если уровень сервера работает в режиме CL, тот 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 то, что он требует тщательного планирования сети и управления/контроля для гарантии того, 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 гарантии того, что имеется в наличии полоса пропускания для создания новых соединений/туннелей сети VPN уровня сервера. Однако, каждый запрос на соединение на уровне n влияет на полосу пропускания, доступную на уровне n–1, и так далее до самого низа. С приближением к нижнему уровню, повышается дробность полосы пропускания и время предоставления/удержания ресурсов для соединения. В общем, если на сервере нижележащего уровня недостаточно емкости для создания нового соединения, то 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.

10.3.4 Управляемые провайдером услуг соединения по запросу

Управляемые провайдером услуг динамические соединения по запросу относятся к тому сценарию, когда провайдер услуг руководит узлом CE и использует данные маршрутизации/сигнализации для динамического создания новых соединений в сети VPN уровня клиента. Преимущество этой возможности, с точки зрения провайдера услуг, состоит в том, что она позволяет динамически создавать сквозные соединения в сети VPN уровня клиента, а не использовать статическую конфигурацию (т. е., ручное или OSS выделение ресурсов). Пример ситуации, когда динамическое установление соединения может быть полезным, это – когда две и более сетей ATM соединяются через центральную сеть MPLS. В этом примере, PNNI может использоваться для создания/разъединения SPVC в сети VPN уровня клиента через маршруты MPLS в сети VPN уровня сервера. Как и для сетей VPN уровней клиента и сервера, технологии уровня сервера могут быть различным. Должно обязательно быть обеспечено равноправное взаимодействие в плоскости управления.

В случае управляемых провайдером услуг динамические соединения по запросу, даже, если провайдер управляет узлом CE от лица пользователя, распределение внутренней адресации и информации о топологии для CE связано с риском, например, CE расположен в помещении пользователя, а не в помещении провайдера. Одним из способов избежать этих рисков является применение статического/ручного выделения ресурсов для устройства CE и близлежащего промежуточного узла сети провайдера, и применение динамической маршрутизации/сигнализации от этого узла назад к PE. Например, если сеть VPN является сетью ATM, то может быть вручную создан VC между CE и ATM коммутатором провайдера, который соединит их, а затем соединит с КТСОП, используя сквозные соединения между ATM коммутаторами. Что касается управления установлением соединения/туннеля на различных уровнях в иерархии многоуровневой сети, то, поскольку соединениями по запросу управляет провайдер, провайдер, по большей части, и контролирует все происходящее в сети. Однако, должно обязательно оставаться тщательное 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 (и всеми уровнями сервера, расположенными под ним).

11 Функции, требуемые для создания VPN с равноправными пользователями

Предполагая, что топология нижележащего уровня сервера определена, а точки TFP и FP на уровне равноправного взаимодействия VPN сконфигурированы и имеют адреса, необходимо выполнить три основных этапа по созданию соединений между участниками VPN в сети VPN уровня равноправного взаимодействия:

Этап 1: Определить и аутентифицировать участников VPN, и сохранить информацию о принадлежности сети VPN.

Этап 2: Рассчитать маршруты между участниками VPN в сети VPN уровня равноправного взаимодействия.

Этап 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 далее подробно описаны в таблице 11-1.

Таблица 11-1/Y.1314 – 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
Аутентификация CE/пользователя, санкционирование доступа и расчеты (AAA)	Аутентификация: Идентификация CE/пользователя на основании параметров аутентификации, например, 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(их) маршрута(ов) 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 шифрования для каждой VPN/CE	ES, CE, PE
	Назначение и конфигурация идентификаторов (ID) сетей VLAN	CE, PE, P

11.1 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 посредством централизованного сервера/системы или распределенного протокола.

11.2 Аутентификация CE/пользователя, санкционирование доступа и расчеты (AAA)

Функция AAA для CE/пользователя используется в предоставленных провайдером сценариях для управления доступом к ресурсам сети VPN уровня равноправного взаимодействия. Кроме того, функция AAA используется для обеспечения выполнения правил, поддержки контроля использования и для предоставления информации, необходимой для выставления пользователю счетов за услуги VPN. Функция AAA может выполняться элементом PE, отдельным устройством, или с использованием объединения обоих методов. Например, если для аутентификации CE устройства для VPN, построенной на основе VLAN Ethernet, используется IEEE 802.1X, то PE может быть аутентификатором, а для выполнения аутентификации используется централизованный сервер аутентификации.

11.3 Маршрутизация в сети VPN равноправного взаимодействия

В том случае, когда между участниками VPN существуют альтернативные маршруты/пути, должна быть выполнена маршрутизация на VPN уровне равноправного взаимодействия для того, чтобы определить топологию и/или рассчитать наилучший(ие) маршрут(ы) между участниками VPN. Поскольку все узлы CE, PE и P принадлежат сети VPN уровня равноправного взаимодействия, в расчете маршрут/пути участвуют все три типа узлов. Функция маршрутизации может выполняться вручную оператором или может выполняться динамически посредством централизованного сервера/системы или распределенного протокола маршрутизации. В тексте настоящей Рекомендации маршрутизация включает в себя прозрачный процесс создания мостовых соединений на основании выяснения адреса источника в плоскости данных.

11.4 Конфигурация сетевых элементов в сетях VPN равноправного взаимодействия

Имеется множество альтернативных функций, обеспечивающих изоляцию VPN. Одной из возможностей является конфигурирование фильтров пакетов для каждой VPN в отдельности на совместно используемых узлах PE для обеспечения полной доступности между сайтами отдельного пользователя, и, в то же время, сохранения изоляции между пользователями. Другой возможностью является использование выделенных узлов PE и конфигурация фильтров/маршрутов, так, чтобы, несмотря на то, что узлы P содержат маршруты всех пользователей, узлы PE содержали бы только маршруты одного-единственного пользователя. Сортировка пакетов/маршрутов применима только в сценариях VPN, предоставленных провайдером, и, следовательно, должна выполняться узлами PE.

Альтернативой применению фильтрации маршрутов/пакетов там, где установлено соединение между пользователями, (например, через Интернет) является шифрование пакетов. Применение шифрования пакетов гарантирует, что, если пользователь принимает пакеты от VPN, участником которой он не является, то 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.

Наиболее широко используемыми типами криптографии для шифрования/дешифрования, является криптография с секретным ключом и криптография с открытым ключом. Криптография с секретным ключом лучше всего подходит для закрытых групп пользователей, члены которых могут знать секретный ключ, и он может распространяться одним-единственным органом, ответственным за безопасность, например, для корпоративной сети VPN. Преимущество криптографии с открытым ключом состоит в том, что она позволяет пользователю устанавливать безопасные соединения, не имея предварительного доступа к секретному ключу. В этом подходе используется два ключа, частный ключ, который хранится в секрете, и открытый ключ, который должен быть распространен между всеми участниками VPN. Частный ключ и открытый ключ математически связаны и, не зная нужного частного ключа, никто не может расшифровать информацию в зашифрованном пакете. Обычно криптография с открытым ключом используется для обмена секретными ключами, которые затем используются для криптографии с секретным ключом.

В том случае, когда технологией, используемой для создания сети VPN уровня равноправного взаимодействия, является Ethernet, изоляция VPN может быть обеспечена при помощи назначения и конфигурации отдельных сетей VLAN. Сети VLAN, как правило, назначаются и конфигурируются вручную или при помощи OSS, хотя может применяться и динамический протокол. Для формирования сквозного соединения межу элементами CE, сети VLAN должны быть правильно сконфигурированы на узлах CE, PE и P.

12 Функции VPN по эксплуатации, управлению и обслуживанию

Инструменты и функции по эксплуатации, управлению и обслуживанию (OAM) чрезвычайно важны для поддержания эффективности работы в широкомасштабных сетях. Примерами важных характеристик сетевых соединений/потоков, обеспечиваемых при помощи функций OAM, являются качество, целостность и достоверность. Если сеть какого-либо уровня не поддерживает функций OAM вообще или частично, то сеть этого уровня является функционально неполноценной в отношении этих функций OAM. В качестве замещения/замены отсутствующих функций на данном уровне не могут использоваться аналогичные функции/инструменты более высокого/более низкого уровней, в частности, это приводит к ошибке определения положения. Это не означает, что невозможно предоставлять услуги VPN с применением сетевых технологий, в которых функции OAM не предусмотрены. Однако, вполне вероятно, что отсутствие функций OAM значительно повысит эксплуатационные расходы и сложность эксплуатации.

В таблице 12-1 приведены некоторые ключевые функции OAM и определено, какие сетевые элементы должны поддерживать соответствующие функции.

Таблица 12-1/Y.1314 – Функции OAM в сетях VPN клиент-сервер

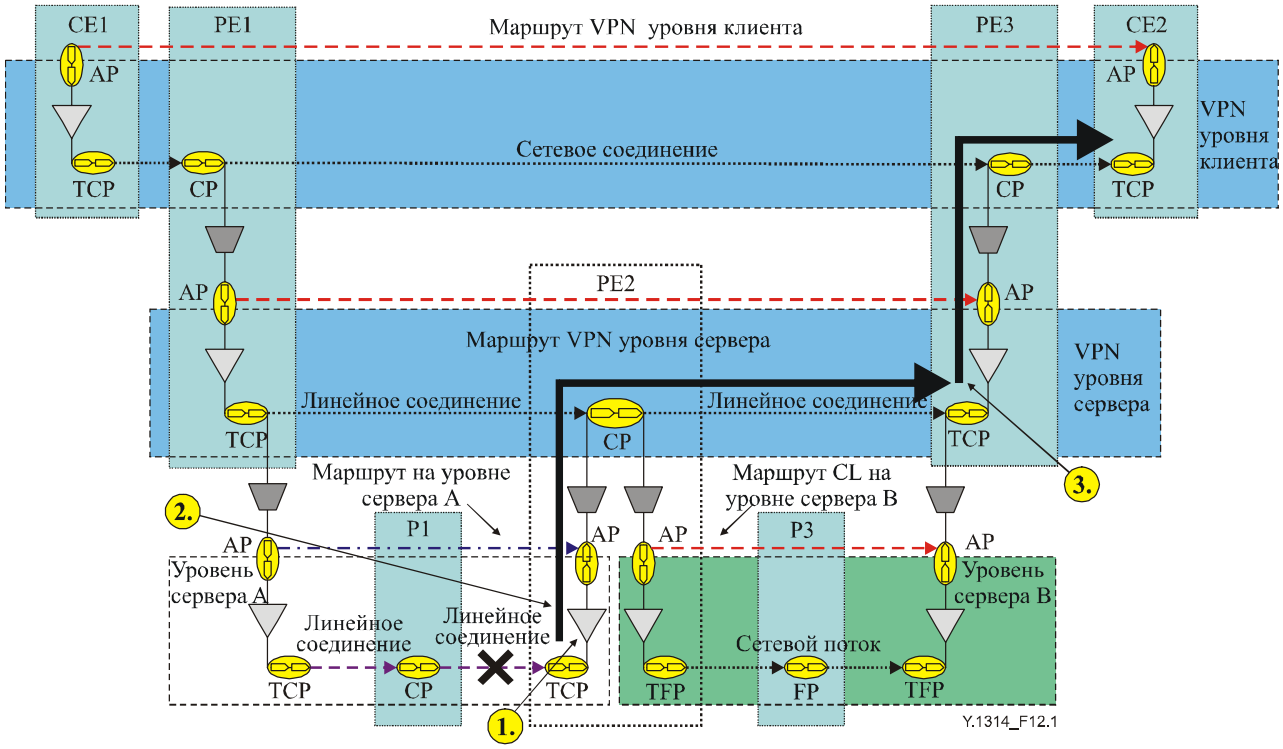
Функция	Функциональные единицы	Сетевые элементы
OAM в сети VPN уровня клиента	Управление обработкой/обнаружение отказов в VPN уровня клиента	CE и PE
	Контроль качества VPN уровня клиента	CE и PE
	Включение и отключение функций OAM в сети VPN уровня клиента	CE и PE
OAM в сети VPN уровня сервера	Управление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

12.1 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 этого сделать не удается, то это приводит к неоднозначному обозначению отказа, что существенно увеличивает сложность эксплуатации и время, требуемое для устранения неисправности. После обнаружения неисправности, кроме 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 (Упреждающего обнаружения ошибки) или AIS (Сигнал индикации аварии) с применением соответствующего синтаксиса функций OAM, используемого технологией конкретного затронутого уровня клиента (если таковой существует).

Наиболее важный механизм обнаружения ошибки – использование проверки возможности соединения (CV), что является общим требованием для всех трех режимов работы сети. Говоря проще, источник потока трафика должен определенно (некоторым образом) идентифицировать себя на приемнике. Способ достижения этого зависит от режима сети и разъясняется в последующих параграфах. Обнаружение местоположения ошибки – это еще одно 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 12-1.



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 12-1/Y.1314 – Распространение FDI на уровне клиент-сервер

В этом примере обнаружение неисправности на линии посредством функции завершения приемника на уровне сервера A приводит к созданию сигнала FDI/AIS и его передаче на уровень сервера VPN. Сигнал FDI распространяется до функции завершения приемника сети VPN уровня сервера, который, в свою очередь, передает сигнал FDI на уровень клиента. Эти действия продолжаются до тех пор, пока сигнал не достигнет того уровня сети, который не поддерживает FDI. Следовательно, хотя этого здесь не показано, но, приняв сигнал FDI, сеть VPN уровня клиента может передать его на вышестоящий уровень, в зависимости от технологии этого вышестоящего уровня (например, ATM, Ethernet, IP и т. д.).

Единственным местом, где должен быть создан сигнал тревоги, это – точка завершения маршрута на том уровне сети, где обнаружена исходная ошибка. В частности, не должно создаваться сигналов тревоги ни на одном из уровней клиента (это является главной целью, преследуемой при передаче сигнала FD)I. Далее, если необходим контроль обоих направлений из одной точки, то в другом направлении может быть передан BDI (индикатор неисправности в обратном направлении). Подробнее о том, какие индикаторы ошибки/сигналы тревоги (включая подробности записей об ошибках и недоступности ресурса, а также существующие критерии последующих действий) можно прочесть в Рекомендациях, касающихся функций OAM для сетевых технологий конкретных уровней, например, Рек. МСЭ-Т Y.1711 – для функций OAM в сети MPLS.

Исправление неисправности применяется для восстановления работы и для управления процедурами, использующими избыточные ресурсы для замены вышедшего из строя оборудования или средств передачи. Например, при обрыве кабеля или неисправности узла, для восстановления/поддержания обслуживания может использоваться переключение на резерв или изменение маршрута.

Инструменты диагностического тестирования по запросу, как правило, используются для локализации неисправности, но могут использоваться 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, и, таким образом, эта часть соединения изолируется.

12.2 Управление рабочими характеристиками

Контроль качества (PM) – это процесс сбора, анализа и обобщения данных о качественных показателях. Эти данные используются для доступа и обслуживания сети, а также для документирования качественных показателях для пользователей. Если поддерживается несколько уровней класса обслуживания (например, на основе архитектуры дифференциального обслуживания (Diffserv)), то контроль качества должен выполняться для каждого класса обслуживания в отдельности. Контроль качества, кроме прочего, включает в себя обнаружение ухудшения характеристик сигнала, контроль запаздывания/дрожания и подсчет потерянных пакетов. Имеется несколько различных целей контроля качества, включая обслуживание SLA, поддержку формирования трафика, выставление счетов для конкретных пользователей, и восстановление обслуживания/переключение на резерв (например, в результате ухудшения сигнала).

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, которые могут возникнуть (которые различны для различных режимов) и требуемые функции OAM.

2) Все неисправности должны быть определены в стандартизованных терминах критериев входа/выхода и последующих действий.

3) Сеть входит в состояние недоступности, когда неисправность или недопустимое ухудшение качества продолжается в течение нескольких последовательных секунд. В режиме СЦИ сеть входит в состояние недоступности после 10 последовательных секунд с ошибками[7] (SES) и выходит из него после 10 последовательных секунд без ошибок (non SES). В целях гармонизации, период недоступности должен быть одинаковым на всех уровнях сети, т. е. 10 секунд.

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

Если сеть находится в состоянии доступности, то PM для целей SLA – это однонаправленное измерение. Однако, поскольку для большей части приложений требуется работа обоих направлений (восходящего и нисходящего), то неисправность работы приложения регистрируется при выходе из строя любого направления. Это значит, что недоступность – это функция "ИЛИ" для каждого направления и, следовательно, если какое-либо направление входит в состояние недоступности, то PM для целей SLA должен быть приостановлен в обоих направлениях.

12.3 Включение/отключение OAM

Для режимов работы CO-CS и CO-PS, основные механизмы OAM по обнаружению/обработке отказов должны включаться/выключаться синхронно с установлением/разрывом маршрута, что может выполняться системами NMS/OSS или посредством сигнализации. Например, создание CV на источнике должно быть включено до включения обнаружения CV на приемнике для того, 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 (например, TTSI из Рек. МСЭ-Т Y.1711) следует ожидать в плоскости данных конкретного маршрута для того, чтобы определить, какому маршруту принадлежит принимаемый пакет OAM.

---

[7] SES – это период времени длиной в одну секунду, в котором коэффициент ошибок по битам больше или равен 1-3, или в течение которого обнаруживается появление LOS или AIS.

12.4 Дефекты, относящиеся к каждому сетевому режиму

Возможные дефекты транспортировки, которые могут появиться в сети VPN уровня клиента или сервера, зависят от режима работы сети, к которому принадлежит технология данного уровня сети. Далее приводится обзор зависящих от режима возможных дефектов:

– **CL-PS**: только разрыва;

– **CO-PS**: разрывы, перестановки и объединения;

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

В последующих разделах подробно описывается каждый режим работы сети, для понимания того, каковы основные требования и аспекты OAM для каждого конкретного режима. Следует отметить, что этот обзор не является исчерпывающим перечнем требований для каждого режима OAM. Рассматриваются только основополагающие различия, позволяющие определить, как режим работы сети, к которому принадлежат уровни клиента и сервера VPN, влияет на то, какие требуются функции/инструменты OAM.

12.4.1 Сети CL-PS

Предполагая наличие согласованной и достоверной информации маршрутизации (что относится ко всем режимам), дефекты, вызванные неправильными соединениями, (т. е. перестановки и объединения) в сетях CL-PS проявиться не могут. Каждый пакет содержит и адрес источника (то есть, функцию CV), и адрес пункта назначения, который содержит всю необходимую информацию для корректной маршрутизации пакета на каждом узле сети. Следовательно, в сети CL-PS возможен один-единственный дефект – разрыв сети (например, из-за неисправности функции маршрутизации, линии или узла). В сетях CL-PS функция CV является составной частью заголовка пакета, поскольку каждый пакет содержит уникальный для данной сети адрес источника/пункта назначения. В сетях CL-PS данные управления и данные пользователя, как правило, передаются по одному пути передачи данных и, следовательно, при неисправности в плоскости управления (например, вышел из строя смежный участок маршрутизации), можно предположить, что соединение разорвано и данные пользователя также не могут быть переданы. Именно так обычно обнаруживаются и исправляются неисправности в сетях CL-PS, например, отсутствие на приеме вызовов маршрутизация плоскости управления означает наличие ошибки в плоскости данных и, следовательно, должны быть предприняты корректирующие действия (например, выбран альтернативный маршрут). Однако, может возникнуть ситуация, когда это не так, одним из таких случаев является ситуация, когда в сетях уровня IP используется балансировка нагрузки. В этом случае существует несколько маршрутов к одному и тому же пункту назначения, следовательно, если один из маршрутов становится недоступным, то плоскость управления этого может и не обнаружить, поскольку для передачи трафика управления может использоваться один из оставшихся доступных маршрутов. Для обнаружения неисправностей, когда используется балансировка нагрузки, должен применяться такой механизм OAM, который проверяет существование соединений на всех доступных маршрутах.

12.4.2 Сети CO-PS

В случае 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. После того, как маршрут/путь рассчитан, используется сигнализация (или действия оператора) для выделения и конфигурации входных/выходных полей мультиплексирования/демультиплексирования (или идентификаторов линейного соединения), которые используются для коммутации пакета с целью его передачи в заданный пункт назначения. Поскольку 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 заранее известным способом добавить функцию проверки возможности соединения (CV), как правило, 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.

12.4.3 Сети CO-CS

Сети CO-CS не страдают от дефектов объединения, поскольку в них поля мультиплексирования/демультиплексирование основаны на физических идентификаторах линейных соединений времени/пространстве/частоте, передаваемых с постоянной скоростью. Неисправности, которые могут возникнуть в сети CO-CS, включают в себя разрыв и перестановку, однако, перестановка соединений может возникнуть только между одинаковыми маршрутами, например, она может возникнуть в СЦИ между VC12 и VC4. В сети CO-CS, как и в сетях CO-PS, некоторым заранее известным способом должна быть добавлена функция проверки возможности соединения (CV). Поскольку кадры CO-CS передаются с постоянной скоростью (вне зависимости от того, есть ли в них данные или нет), информация CV может передаваться в каждом кадре со скоростью передачи кадров, например, след сообщения J0 в кадре VC4 СЦИ имеет базовую скорость подачи 125 мкс. В сетях CO-CS управляющий трафик всегда передается вне полосы пропускания (OOB) и, следовательно, функции OAM должны быть предоставлены в отдельности для каждого соединения в плоскости данных пользователя и в плоскости управления.

12.4.4 Разделение плоскости данных управления и плоскости данных пользователя

Данные управления и данные пользователя в сетях CO-PS могут передаваться в различных плоскостях данных (это положение дел часто называется управлением вне полосы пропускания (OOB)); и, как отмечено в предыдущем параграфе, 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. Ясно, что когда плоскости данных управления и пользователя разделены, невозможно предположить, что неисправность в плоскости управления указывает на неисправность в плоскости данных пользователя (и наоборот). Следовательно, механизмы OAM в сетях уровня CO-PS, в которых применяется управление вне полосы пропускания (OOB), должны быть своими для каждой плоскости (т. е. различными для различных соединений). Существует также случай, когда для передачи трафика управления может использоваться та же самая плоскость, что и для передачи некоторого трафика пользователей, но не всего (например, механизм формирования трафика (TE) в сети MPLS может применяться для выполнения явной маршрутизации для определенных типов трафика и, следовательно, трафик данных пользователей не должен передаваться по пути, который используется пакетами управления при создании туннелей TE).

Ошибка в использовании механизмов OAM, основанных на плоскости данных пользователя, может привести к таком сценарию, когда возникают ошибки в соединениях, по которым передаются пакеты данных, но, поскольку трафик управления передается по другому соединению, управляющая информация продолжает передаваться и, следовательно, плоскость управления не видит неисправности. Без наличия в плоскости данных OAM механизмов обнаружения источник будет продолжать передачу данных, создавая черную дыру для трафика, или, что значительно хуже, нарушая безопасность данных пользователя за счет передачи трафика в ошибочный пункт назначения.

Для того чтобы однозначно определить, где возникла ошибка, и для выполнении 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 меж-провайдерской VPN. когда стороны соединения P2P в сети VPN уровня клиента расположены в сетях различных провайдеров.

13 Функциональная конвергенция и сценарии услуг

Сопоставляя требования к услугам VPN с функциями, описанными в настоящей Рекомендации, оператор может выбрать наиболее приемлемые сетевые технологии и механизмы, необходимые для предоставления тех услуг VPN, которые он планирует предложить клиенту. Выбор наилучших среди аналогов механизмов/протоколов для каждой функции позволяет развивать отдельные функциональные компоненты независимо друг от друга. Это подход также предусматривает многократное использование различными VPN сетевыми технологиями общих механизмов/протоколов (там, где возможно) для снижения цены и уменьшения сложности.

13.1 Сценарии услуг в сети VPN клиент-сервер

Функции (и, следовательно, механизмы/протоколы), необходимые для поддержания сети VPN клиент-сервер, зависят от режимов работы сети клиент-сервер, а также от предлагаемых услуг VPN. Например, некоторые пользователи могут захотеть иметь возможность установления по запросу коммутируемых виртуальных каналов (SVC) между несколькими сайтами таким образом и когда требуется, тогда как другие пользователи могут захотеть просто иметь постоянные соединения, построенные на известной статической топологии. Другой пример – некоторые пользователи могут захотеть использовать аутентификацию каждого CE/пользователя для повышения степени безопасности, тогда как другие пользователи могут посчитать достаточным обеспечить ограничение физического доступа к инфраструктуре сети. В таблицах III.1 и III.2 приведены некоторые примеры различных сценариев услуг и определены некоторые примерные механизмы/протоколы, которые могут использоваться для выполнения требуемых функций.

13.2 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. Например, аутентификация в случае VPN, работающей с шифрованием, обязательна для того, чтобы использовались правильные ключи, тогда как в случае VPN на основе VLAN сети, аутентификация (например, с применением IEEE 802.1X) обеспечивает дополнительную защиту и не является основным требованием. В таблице III.3 приведены некоторые примеры различных сценариев услуг и определены некоторые примерные механизмы/протоколы, которые могут использоваться для выполнения требуемых функций.

14 Аспекты безопасности VPN

В настоящей Рекомендации не вводится никаких новых положений безопасности. Однако, при разработке/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.

Безопасность сети – это сама по себе огромная область и, следовательно, в настоящей Рекомендации она не рассматривается подробно. Рассматривая вопросы безопасности с верхнего уровня, физическую инфраструктуру сети можно VPN защитить от несанкционированного доступа или от злонамеренных воздействий (например, ограничив доступ и разрешив его только для оборудования, находящегося в данном здании). Кроме того, должен быть также предотвращен дистанционный несанкционированный доступ к инфраструктуре сети (например, используя программные средства обеспечения безопасности для защиты от атак из Интернета).

Как показано в §5.1, 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, как показано в разделе 6, для того, 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, как в сети VPN клиент-сервер, так и в сети VPN равноправного взаимодействия, можно улучшить путем применения криптографии для шифрования блоков трафика пользователя/управления, и можно использовать аутентификацию для идентификации пользователей и сетевых узлов. Более подробно аутентификация в сетях VPN клиент-сервер и в сетях VPN равноправного взаимодействия описывается в §10.2.1 и §11.2 соответственно. Шифрование подробно описывается в §6.2 и §11.4.

Дополнение I

Расположение точек TCP/TFP в VPN уровня клиента

На рисунке I.1 показан пример сети VPN клиент-сервер, то есть, физическая топология сети, в которой черные линии показывают сеть VPN уровня сервера, а серые линии показывают физическую линию между узлами.

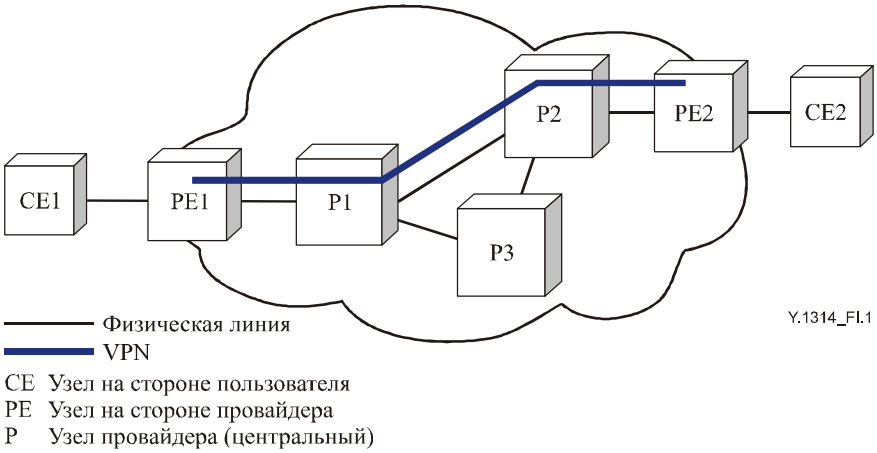


Рисунок I.1/Y.1314 – Физическая топология сети VPN клиент-сервер – Пример 1

Несмотря на то, что рисунок I.1 изображает физическую топологию и сеть VPN уровня сервера, на нем отдельно не представлены топологии VPN уровня клиента и уровня сервера или расположение точек TCP/TFP. На рисунке I.2 представлена функциональная модель, основанная на физической топологии, изображенной на рисунке I.1, в которой точки TFP располагаются в узлах CE. В этом примере сеть VPN уровня сервера – это сеть с установлением соединения (CO) (например, ATM), тогда как сеть VPN уровня клиента – это сеть без установления соединения (CL) (например, Ethernet), хотя возможны любые комбинации пары CO или CL.

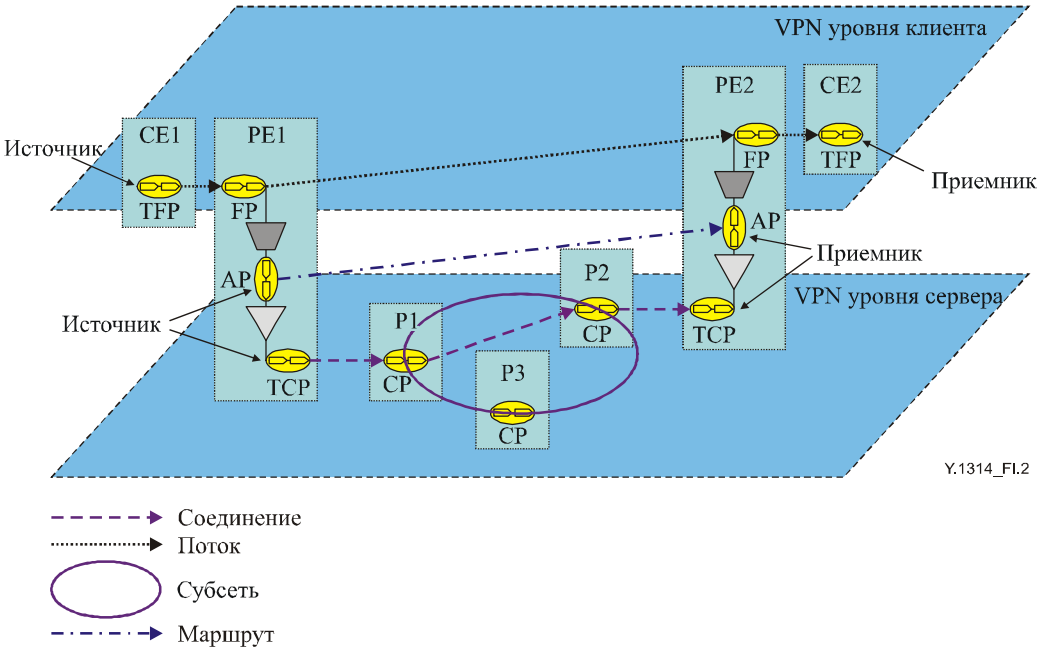


Рисунок I.2/Y.1314 – VPN уровня клиента – точки TFP расположены в узлах CE

Узлы CE и P принадлежат сети VPN уровня клиента и сервера соответственно, тогда как узлы PE принадлежат обоим уровням. Точки TFP в сети VPN уровня клиента определяют, где (в данном случае – в каком узле CE) поток P2P в сети VPN уровня клиента начинается (его источник) и заканчивается (его приемник), а точки FP определяют, через какие узлы PE проходит поток P2P. Аналогично, 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. Точки доступа (AP) в сети VPN уровня сервера определяют источник/приемник для маршрута в сети VPN уровня сервера.

В предыдущем примере точки TFP в сети VPN уровня клиента располагались на узлах CE (CE1 и CE2), однако это относится не ко всем случаям взаимосвязи между клиентами и сервером в сети VPN. Например, сеть VPN уровня клиента может быть сетью Ethernet или сетью IP, где точки TFP располагаются на хостах/оконечных системах.

На рисунке I.3 показана физическая топология сети VPN клиент-сервер. Если бы сетью VPN уровня клиента была сеть Ethernet, то узлы C били бы коммутаторами Ethernet, а оконечными системами/хостами были бы компьютеры/серверы с интерфейсами Ethernet.

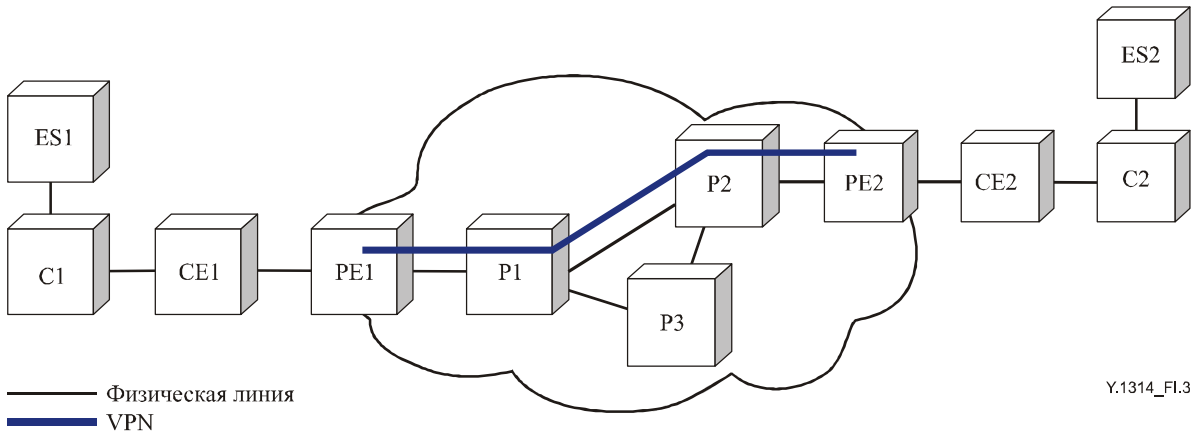


Рисунок I.3/Y.1314 – Физическая топология сети VPN клиент-сервер – Пример 2

Функциональная модель, основанная на физической сети, изображенной на рисунке I.3, показана на рисунке I.4, где точки TFP/TCP сети VPN уровня клиента расположены на оконечных системах/хостах, а не в CE.

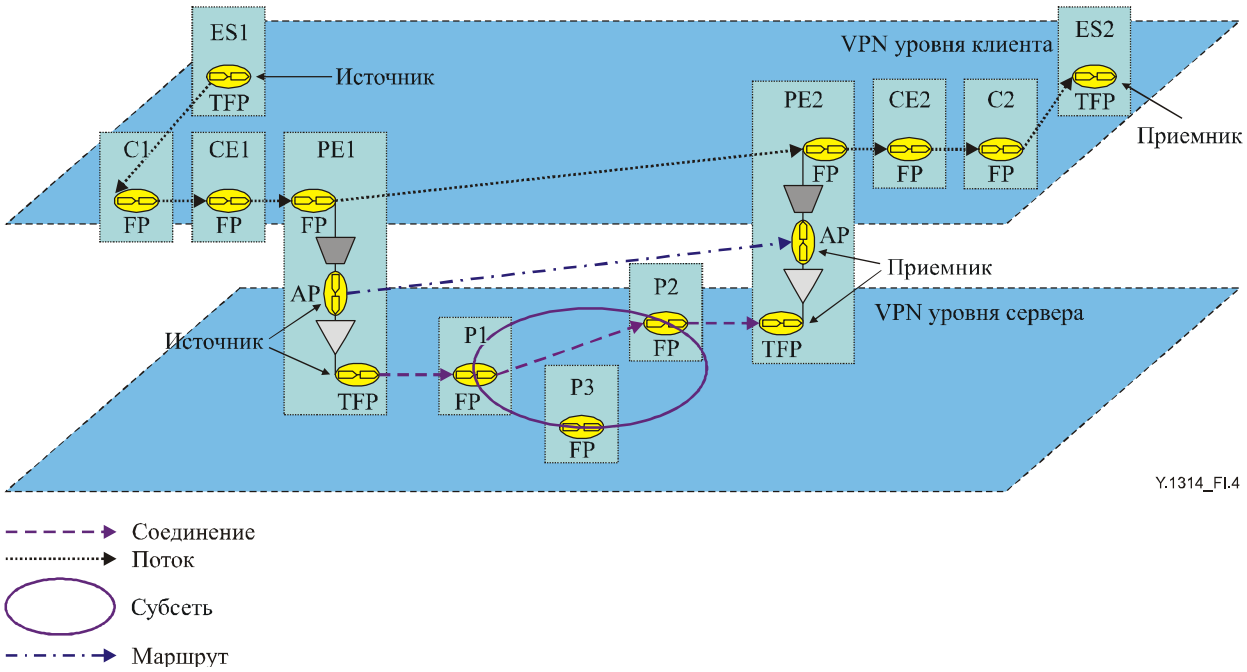


Рисунок I.4/Y.1314 – VPN уровня клиента – точки TFP расположены на оконечных системах/хостах

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 (т. е. ES1 и ES2, соответственно) для потока в сети VPN уровня клиента, а точки FP определяют, через какие узлы C, CE и PE проходит поток.

Хотя это и не показано в рассмотренных ранее примерах, возможно также, чтобы на одной стороне сети VPN точка TFP/TCP источника или приемника располагалась в CE, а на другой стороне – точка не располагается в CE, т. е. точка CP/FP располагается в CE, а точка TFP/TCP располагается в узле пользователя или ES.

Дополнение II

Сеть VPN клиент-сервер с несколькими VPN уровня сервера

На рисунке II.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.

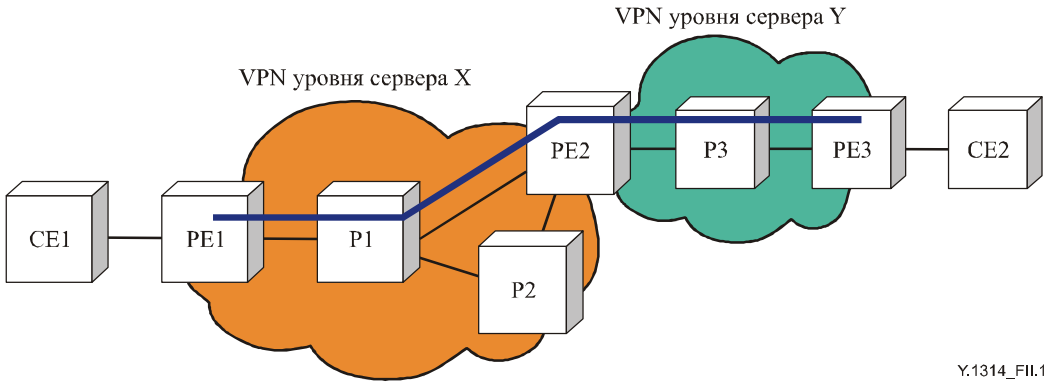


Рисунок II.1/Y.1314 – физическая топология взаимодействия сетей VPN уровня сервера

Один из методов взаимодействия сетей VPN уровня сервера X и Y заключается в использовании взаимодействия клиент-сервер, как показано на рисунке II.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.

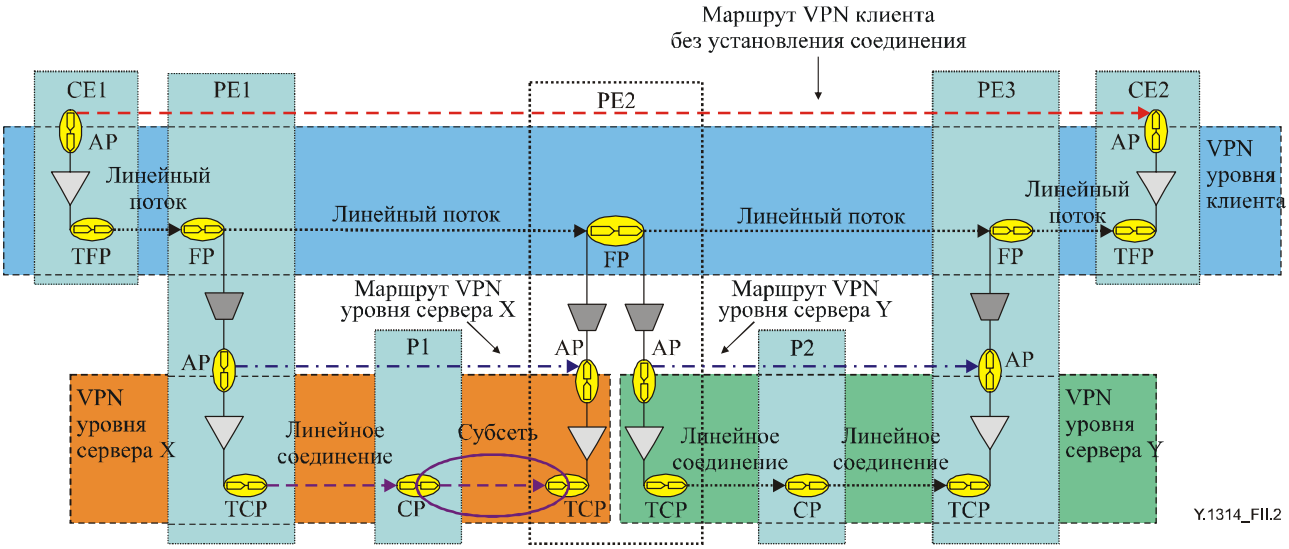


Рисунок II.2/Y.1314 – Взаимодействие сетей VPN уровня сервера

Функция адаптации источника сети VPN уровня сервера X трансформирует характеристическую информацию (CI) сети VPN уровня клиента в адаптированную информацию (AI) сети VPN уровня сервера X, а функция адаптации приемника трансформирует AI сети VPN уровня сервера X в CI сети VPN уровня клиента. Аналогично, 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 можно идентифицировать адресами VPN уровня клиента. Так например, если бы сеть VPN уровня клиента была бы сетью IP, то на узлах PE1, PE2 и PE3 требовались бы IP адреса, принадлежащие сети VPN уровня клиента .

Использование нескольких сетей VPN уровня сервера с адаптацией клиент-сервер для VPN уровня клиента с установлением соединений означает, что маршрут/путь должен быть динамически/вручную рассчитан через все точки CP, и должно быть установлено, как минимум, два сквозных линейных соединения в сети VPN уровня клиента в пределах сети провайдера. Использование несколько сетей VPN уровня сервера с адаптацией клиент-сервер для уровня клиента без установления соединений означает, что маршрут/путь должен быть динамически/вручную рассчитан через все точки FP, и единицы трафика без установления соединений (CL) (т. е. пакеты) должны передаваться на основе адресной информации сети VPN уровня клиента. Это противоречит случаю, когда создавалось одно-единственное сквозное соединение VPN уровня сервера в сети провайдера между двумя точками CP/FP в сети VPN уровня клиента. В этом случае в сети провайдера требуется одно-единственное линейное соединение/поток от источника до приемника маршрута сети VPN уровня сервера и, следовательно, не требуется рассчитывать маршрут/путь в сети провайдера для VPN уровня клиента.

Альтернативный метод взаимодействия между сетями VPN уровня сервера X и Y показан на рисунке II.2, он заключается в использовании равноправного взаимодействия, как показано на рисунке II.3. 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.

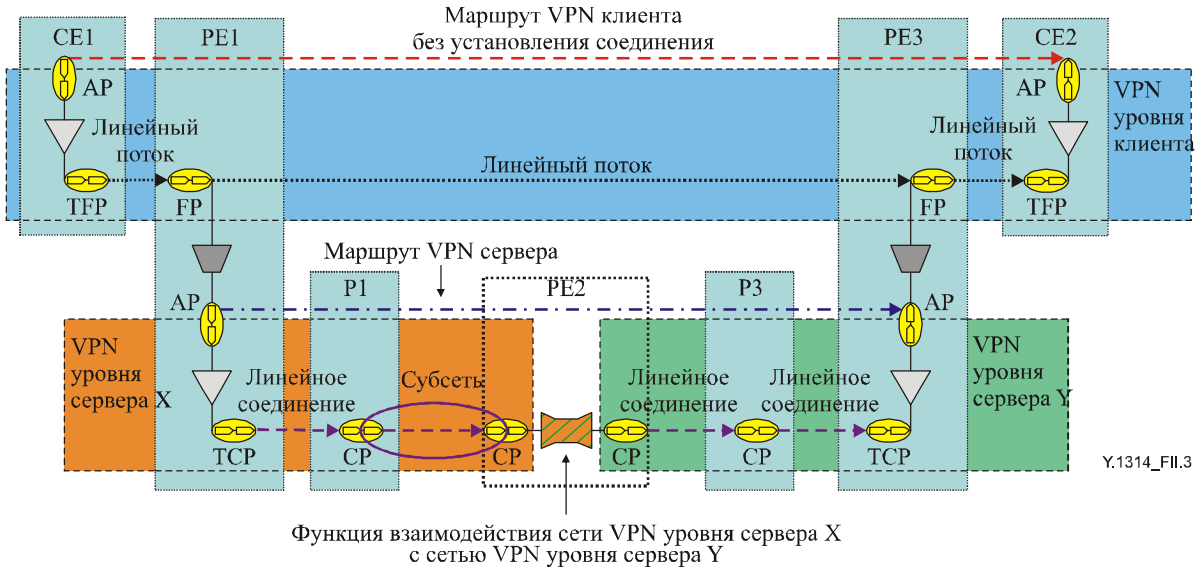


Рисунок II.3/Y.1314 – Равноправное взаимодействие сетей VPN уровня сервера

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.

Основным фактором, который следует учитывать при определении равноправного взаимодействия, является то, что только определенные технологии способны взаимодействовать на равноправной основе, например, сети ATM и Frame Relay могут взаимодействовать на равноправной основе (используя FRF.8), но сети IP и TDM не могут. Взаимодействие на равноправной основе требует осуществлять взаимодействие не только в плоскости данных, но также и в плоскости управления для таких функций как маршрутизация, сигнализация и OAM.

Дополнение III

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

В таблицах далее приведены некоторые примеры различных сценариев предоставления услуг VPN и определены некоторые примеры механизмов/протоколов, которые могут использоваться для выполнения необходимых функций.

ПРИМЕЧАНИЕ. – Дополнительные справки, относящиеся к таблицам данного Дополнения, приводятся в списке литературы.

Таблица III.1/Y.1314 – Сценарии предоставления услуг VPN клиент-сервер №1

	Уровень 2 услуга передачи кадров по сети MPLS	**Уровень 2 услуга Ethernet VPWS по сети IP/L2TPv3**	**Уровень 3 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 (AAA)	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	Протокол маршрутизации CE-PE (например, EBGP с MD5), 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
Передача сигнализации по туннелю/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	IEEE 802.1ag, E-LMI, IEEE 802.3ah, Рек. МСЭ-T Y.1731	IP переброска/ трассировка маршрута
Функции OAM в VPN уровня сервера	Рек. МСЭ-T Y.1711, Рек. МСЭ-T Y.1713, MPLS, VCCV, BFD/LSP переброска	IP переброска/ трассировка маршрута	Рек. МСЭ-T Y.1711, Рек. МСЭ-T Y.1713, LSP переброска/ трассировка маршрута

Таблица III.2/Y.1314 – Сценарии предоставления услуг VPN клиент-сервер № 2

	Уровень 1 СЦИ услуги в сети VPN посредством OTN	**Уровень 1 TDM услуги в сети VPN посредством MPLS**	**Уровень 2 ATM услуги в сети VPN посредством СЦИ**
VPN уровня клиента	СЦИ (например, STM-16)	TDM (например, E1)	ATM
VPN уровня сервера	Световод/ оптический канал (OCh)	MPLS PW	SDH (например, VC4)
Определение принадлежности сети VPN	Рек. МСЭ-Т G.7714.1/Y.1705.1, 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 СЕ/пользователя, санкционирование доступа и расчеты (AAA)	Протоколы GMPLS/ASON, SNMP, NMS	RMON, SNMP, NMS	ATM, Безопасность PNNI/UNI, RMON, SNMP, NMS
Конфигурация элементов сети VPN уровня клиента	NMS, вручную	NMS, вручную	ATM UNI, вручную, NMS
Маршрутизация в VPN уровня клиента	GMPLS/ASON протоколы маршрутизации, вручную, NMS	Вручную, NMS	Вручную/статически, NMS, PNNI
Передача сигнализации по туннелю/соединению VPN уровня клиента	GMPLS/ASON протоколы сигнализации, вручную, NMS,	Вручную, NMS	Вручную, NMS, PNNI
Функции OAM в VPN уровня клиента	Заголовок СЦИ (например, следы байтов J0/J1/J2, байт состояния трассы G1)	Рек. МСЭ-Т G.775, AIS/LOS	F4 и F5 управления обработкой отказов, обратная петля, и контроль непрерывности (CC)
Функции OAM в VPN уровня сервера	Заголовок OCh (например, идентификатор следа маршрута (TTI), используемый для контроля маршрута/участка (PM/SM))	Рек. МСЭ-Т Y.1711, Рек. МСЭ-Т Y.1713, MPLS, VCCV, BFD/LSP переброска	Заголовок СЦИ (например, следы байтов J0/J1/J2, байт состояния трассы G1)

Таблица III.3/Y.1314 – Сценарии предоставления услуг VPN равноправного взаимодействия

	IPsec VPN через Интернет	**VPN сеть VLAN Ethernet**
VPN равноправного взаимодействия	IP	Ethernet
Определение принадлежности сети VPN	Вручную, NMS	Вручную, NMS, RADIUS
Аутентификация CE/пользователя, санкционирование доступа и расчеты (AAA)	Основная аутентификация IKE (основанная на предварительно распределенных ключах или цифровых подписях), RMON, SNMP, NMS	IEEE 802.1x, RADIUS, RMON, SNMP, NMS
Маршрутизация в VPN равноправного взаимодействия	IGP протоколы маршрутизации (например, ISIS, OSPF, RIP), BGP, вручную, NMS	Усечение топологии STP и выяснение адреса в плоскости данных (прозрачные мосты)
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	IEEE 802.1ag, E-LMI, IEEE 802.3ah, Рек. МСЭ-T Y.1731

БИБЛИОГРАФИЯ

Указанная здесь справочная литература постоянно пересматривается. Читателям данной Рекомендации рекомендуется обратиться к самым последним версиям/проектам этой литературы.

ATM UNI: ATM Forum UNI 4.1 (2002), "*ATM User Network Interface (UNI) Signalling Specification version 4.1*", af-sig-0061.001.

ATM Forum PNNI 1.1 (2002), *Private Network-Network Interface Specification v.1.1*, af-pnni-0055.001.

IEEE 802.1ad (2005, Draft 6.0), *Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges*.

IEEE 802.1ag (2005, Draft 4.1), *Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management*, status: PAR approved, Task Group ballot in progress.

IEEE 802.1ah (Aug 2005, Draft 1.2), *Virtual Bridged Local Area Networks – Amendment 6: Provider Backbone Bridges*, status: PAR approved, Task Group ballot.

IEEE 802.1Q (2005), *Virtual Bridged Local Area Networks*, status: published.

IEEE 802.1X (2004), *Port-Based Network Access Control*, status: published.

IEEE 802.17 (2004), *Specific requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specifications*, status: published.

IEEE 802.3ah (2004), *Specific requirements – Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications* Amendment: *Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*, Ethernet in the First Mile amendment to IEEE Std 802.3.

IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview*.

IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

IETF RFC 3036 (2001), *LDP Specification*.

IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

IETF draft-ietf-bfd-base-03.txt (2005), *Bidirectional Forwarding Detection,* work in progress.

IETF draft-ietf-bfd-mpls-02.txt (2005), *BFD For MPLS LSPs*, work in progress.

IETF draft-ietf-l2tpext-l2vpn-05.txt (2005), *L2VPN Extensions for L2TP*, work in progress.

IETF draft-ietf-l2vpn-radius-pe-discovery-01.txt (2005), *Using RADIUS for PE-Based VPN Discovery,* work in progress.

IETF draft-ietf-l3vpn-bgpvpn-auto-06.txt (2005), *Using BGP as an Auto-Discovery Mechanism for Network-based VPNs*, work in progress.

IETF draft-ietf-l3vpn-rfc2547bis-03.txt (2004), *BGP/MPLS VPNs*, work in progress.

IETF draft-ietf-mpls-lsp-ping-09.txt (2005), *Detecting MPLS Data Plane Failures*, work in progress.

IETF draft-ietf-pwe3-control-protocol-17.txt (2005), *Pseudowire Setup and Maintenance using the Label Distribution Protocol*, work in progress.

IETF draft-ietf-pwe3-frame-relay-05.txt (2005), *Encapsulation Methods for Transport of Frame Relay Over MPLS Networks*, work in progress.

IETF draft-ietf-pwe3-vccv-06.txt (2005), *Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)*, work in progress.

ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan*.

ITU-T Recommendation E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*.

ITU-T Recommendation G.775 (1998), *Loss of Signal (LOS), Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) defect detection and clearance criteria for PDH signals*.

ITU-T Recommendation G.826 (2002), *End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections*.

ITU-T Recommendation G.827 (2003), *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*.

ITU-T Recommendation G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

ITU-T Recommendation G.1010 (2001), *End-user multimedia QoS categories*.

ITU-T Recommendation G.7714.1/Y.1705.1 (2003), *Protocol for automatic discovery in SDH and OTN networks*.

ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

ITU-T Recommendation Q.933 (2003), *ISDN Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*.

ITU-T Recommendation Q.2931 (1995), *Digital Subscriber Signalling System No. 2 – User-Network Interface (UNI) layer 3 specification for basic call/connection control*.

ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

ITU-T Recommendation Y.1413 (2004), *TDM-MPLS network interworking – User plane interworking*.

ITU-T Recommendation Y.1415 (2005), *Ethernet-MPLS network interworking – User plane interworking*.

ITU-T Recommendation Y.1711 (2004), *Operation & Maintenance mechanism for MPLS networks*.

ITU-T Recommendation Y.1713 (2004), *Misbranching detection for MPLS networks*.

ITU-T Recommendation Y.1731 (2006), *OAM functions and mechanisms for Ethernet based networks*.

MEF ETH OAM (2003), *Ethernet Services OAM*, Draft.

Frame Relay Forum FRF.8 (1995), *Frame Relay/ATM PVC Service Interworking Implementation Agreement*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.