ВИРТУАЛЬНЫЕ ЧАСТЫЕ СЕТИ VPN НА ОСНОВЕ ТЕХНОЛОГИИ MPLS

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Скрипелёва А.А.

Саломатин С.Б. – к.т.н.,доцент

На сегодняшний день большинство организаций и предприятий имеют территориально распределенную структуру, вследствие чего возникает необходимость объединения локальных вычислительных сетей территориально распределенных филиалов в одну корпоративную сеть. Кроме того, существуют проблемы защиты информации, аутентификации и авторизации пользователей, предоставления доступа к ресурсам, обеспечение независимости адресных пространств. Эти задачи в настоящее время помогает решить технология виртуальных частных сетей VPN (Virtual Privat Network).

Под термином VPN понимают круг технологий, обеспечивающих безопасную и качественную связь в пределах контролируемой группы пользователей по открытой глобальной сети.

Построение виртуальной частной сети учреждения, например, для обеспечения документооборота устанавливает следующие задачи: обеспечение защиты соединения, требуемого качества обслуживания, низкую стоимость и расширяемость инфраструктуры. Для решения поставленных задач построения VPN используют технологию MPLS (MultiProtocol Label Switching).

Цель создания VPN на основе технологии MPLS для обеспечения документооборота предприятия — моделирование системы массового обслуживания с входящим самоподобным потоком, которая предоставляет необходимую пропускную способность канала передачи, а так же размер выходного буфера, в соответствии с интенсивностью поступающей нагрузки, требуемым задержкам и вероятностью потерь пакетов.

Защита соединения в сетях MPLS-VPN поддерживается с помощью сочетания протокола BGP и системы разрешения IP-адресов. BGP-протокол отвечает за распространение информации о маршрутах. Он определяет, кто и с кем может связываться. Членство в VPN зависит от логических портов, которые объединяются в сеть VPN и которым BGP присваивает уникальный параметр (RD). Параметры RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. В состав VPN входят только определенные назначенные порты. В сети VPN с функциями MPLS протокол BGP распространяет таблицы FIB (Forwarding Information Base) с информацией о VPN только участникам данной VPN, обеспечивая таким образом безопасность передачи данных с помощью логического разделения трафика. Именно провайдер, а не заказчик присваивает порты определенной VPN во время ее формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. Пользователи могут работать в сети интранет или экстранет, только если они связаны с нужным физическим или логическим портом и имеют нужный параметр RD. Эта схема придает сетям MPLS-VPN очень высокий уровень защищенности.

Для обеспечения дополнительной защиты соединения со стороны клиента могут устанавливаться межсетевые экраны (например, Cisco ASA).

На рисунке 1 приведен пример VPN-сети, создаваемой провайдером.

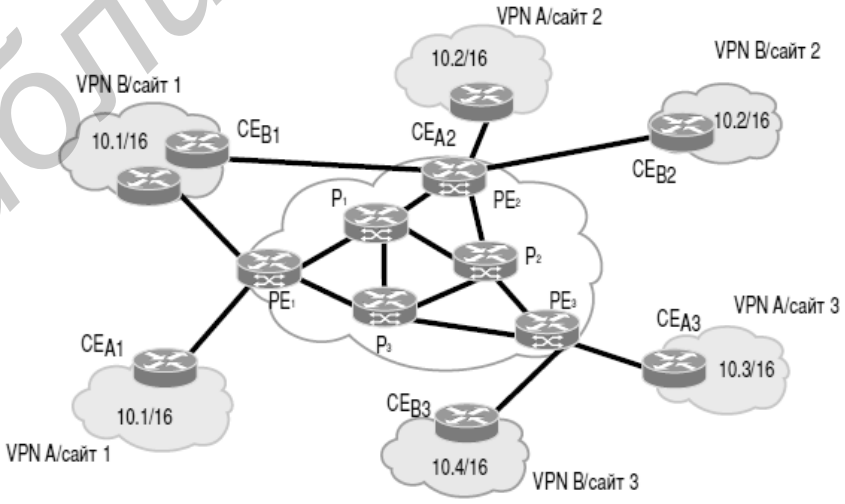

Рис. 1 - Виртуальная частная сеть MPLS

Информационные потоки в пакетной транспортной сети проявляют свойства самоподобия. Задачей выбора параметров магистрального канала является расчет необходимой пропускной способности канала

передачи, а так же размера выходного буфера.

Работу магистрального канала с выходным буфером можно описать моделью систем массового обслуживания с входящим самоподобным потоком и детерминированным временем обслуживания: $f_{BM}/D/1$ (f_{BM} – фрактальное броуновское движение, являющееся самоподобным процессом; D – детерминированный процесс обслуживания; 1 – одно устройство обслуживания, в нашем случае - канал передачи с буфером).

Данная система - $f_{BM}/D/1$ имеет аналитическое решение в виде формулы Норроса:

$$x = \frac{p^{1/(2(1-H))}}{(1-p)^{H/(1-H)}}$$, где p = λ/μ – коэффициент использования ресурса сети; λ – интенсивность поступающей нагрузки; μ – интенсивность обслуживания нагрузки, а в нашем случае и есть искомая пропускная способность; H – параметр Херста, для самоподобных процессов H = 0,9; x – необходимый объем выходного буфера.

$$T = \frac{1}{\lambda}\left[(y * \left(\frac{1}{c} + \frac{y}{c} * \frac{(y*c)^{\frac{2H-1}{2(1-H)}}}{(c-y)^{\frac{H}{1-H}}}\right)\right]$$, где T – задержка пакета, складывающаяся из времени нахождения пакета в очереди и времени передачи пакета по каналу связи.

Таким образом, исходя из параметра входящего информационного потока, мы можем выбрать такую пропускную способность канала, при которой рассчитанный размер буфера будет обеспечивать требуемые задержки пакетов в канале связи.

Для осуществления документооборота учреждения рассчитаем параметр информационного потока передачи данных:

$$\lambda_{DATA} = \frac{y_{DATA}}{n}$$, где n – длина пакета (примем n = 1500 байт = 12000 бит).

При самоподобном входящем потоке резкое возрастание задержек пакетов происходит уже при ρ = 0,6. Рассчитаем необходимый размер буфера и задержку пакета для ρ Є [0,6:1), с шагом 0,1, результаты приведем в таблицу:

y, Мб/с	λ, пак/с	c, Мб/с	μ, пак/с	ρ	x, пак	T, с
774,9	58002	1160,04	96670	0,6	297	0,031264
774,9	58002	994,32	82860	0,7	8539	3,112616
774,9	58002	870,036	72503	0,8	640001	3850,691
774,9	58002	782,052	65171	0,89	236818632	3,64662E+13

По полученным значениям построим график зависимости задержки от величины пропускной способности канала при фиксированной нагрузке y, Мб/с:

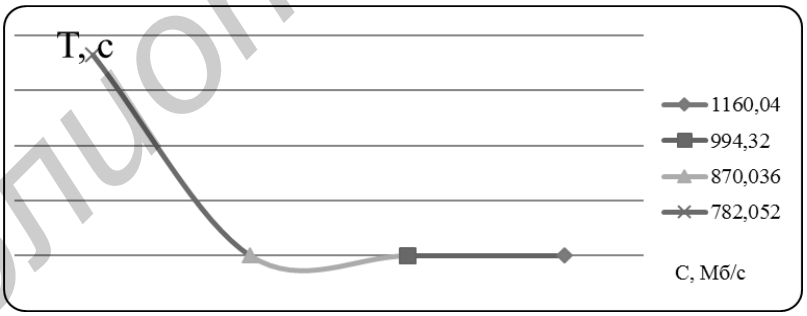

Рис. 2 - График зависимости задержки на передачу от пропускной способности канала

Как видно из таблицы необходимое значение пропускной способности лежит в пределах c = 994,32-1160,04 Мб/с.

Рассчитаем параметры задержки и необходимый размер буфера для ρ Є [0,6:0,7], с шагом 0,01 аналогичным образом и получим, что необходимо выделить для передачи данных полосу пропускания со скоростью не менее 1141,032 Мб/с.

Данная модель VPN MPLS предоставляет необходимую полосу пропускания, позволяет избежать перегрузок канала, роста задержки передачи пакетов и потерь в соответствии с качеством обслуживания QoS.

Список использованных источников:

1. Cisco Systems, Построение виртуальных частных сетей (VPN) на базе технологии MPLS
2. Бехингер М. Безопасность MPLS VPN. – Индианаполис: Cisco Press, 2005. – 312с.
3. Гейн Л. Основы MPLS. – Индианаполис: Cisco Press, 2007. – 651 с.