Лекция 08

Сеансовый уровень.
Протоколы L2TP и PPTP.

Сеансовый уровень

Сеансовый уровень (Session layer) — 5-й уровень сетевой модели OSI, отвечает за поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений. Синхронизация передачи обеспечивается помещением в поток данных контрольных точек, начиная с которых возобновляется процесс при нарушении взаимодействия.

Сеансы передачи составляются из запросов и ответов, которые осуществляются между приложениями. В случае потери соединения этот протокол может попытаться его восстановить. Если соединение не используется длительное время, то протокол сеансового уровня может его закрыть и открыть заново. Он позволяет производить передачу в дуплексном или в полудуплексном режимах и обеспечивает наличие контрольных точек в потоке обмена сообщениями.

В эталонной модели DOD (TCP/IP) отсутствует рассмотрение затронутых в модели OSI вопросов применения семантики транспортного протокола и поэтому сеансовый уровень не рассматривается. Управление сеансами OSI в соединении с типичными транспортными протоколами (TCP, SCTP) содержится в протоколах транспортного уровня или же в противном случае затрагивает область протоколов прикладного уровня. Слои модели DOD являются описаниями рамок функционирования (приложение, соединение хост-хост, сеть, связь), но не подробными предписаниями в отношении способа функционирования или семантики данных.

Протокол PPTP

PPTP (Point-to-Point Tunneling Protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

Спецификация протокола была опубликована как «информационная» RFC 2637 в 1999 году. Она не была ратифицирована IETF. Протокол считается менее безопасным, чем IPSec[1]. PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation[2]. Второе соединение на TCP-порте 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий.

PPTP-трафик может быть зашифрован с помощью MPPE[3]. Для аутентификации клиентов могут использоваться различные механизмы, наиболее безопасные из них — MS-CHAPv2 и EAP-TLS.

Cisco первой реализовала PPTP и позже лицензировала эту технологию корпорации Microsoft.

PPTP удалось добиться популярности благодаря тому, что это первый протокол туннелирования, который был поддержан корпорацией Microsoft. Все версии Microsoft Windows, начиная с Windows 95 OSR2, включают в свой состав PPTP-клиент, однако существует ограничение на два одновременных исходящих соединения.

PPTP был объектом множества анализов безопасности, в нём были обнаружены различные серьёзные уязвимости. Известные относятся к используемым протоколам аутентификации PPP, устройству протокола MPPE, и интеграции между аутентификациями MPPE и PPP для установки сессионного ключа. Краткий обзор данных уязвимостей:

---

1 **IPsec (IP Security)** — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации vpn-соединений.

2 **GRE (Generic Routing Encapsulation — общая инкапсуляция маршрутов)** — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP пакеты. Номер протокола в IP — 47. Туннелирование подразумевает три протокола:

- пассажир — инкапсулированный протокол (IP, IPX, AppleTalk, ...)
- протокол инкапсуляции (GRE)
- транспортный протокол (UDP)

3 **Microsoft Point-to-Point Encryption (MPPE)** — протокол шифрования данных, используемый поверх соединений PPP. Использует алгоритм RSA RC4. MPPE поддерживает 40-, 56- и 128-битные ключи, которые меняются в течение сессии.

Протокол L2TP

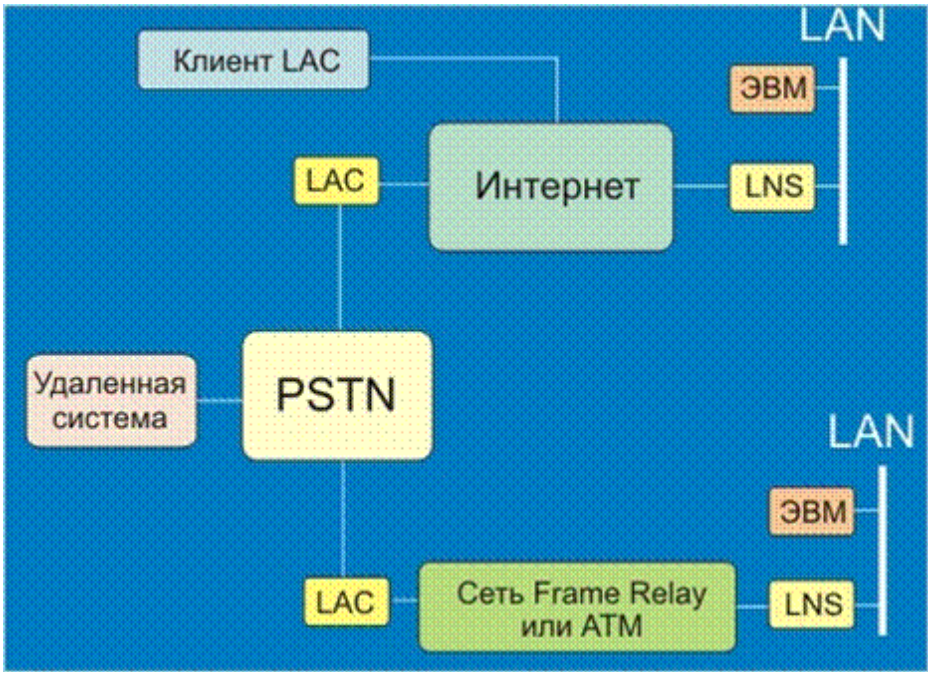
L2TP (Layer 2 Tunneling Protocol — протокол туннелирования второго уровня) — в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей. Главное достоинство L2TP состоит в том, что этот протокол позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay.

RFC 2661

Несмотря на то, что L2TP действует наподобие протокола Канального уровня модели OSI, на самом деле он является протоколом Сеансового уровня и использует зарегистрированный UDP-порт 1701.

Схема работы

На диаграмме показана схема работы протокола L2TP. Целью здесь является туннелирование кадров PPP между удаленной системой или клиентом LAC (L2TP Access Concentrator) и LNS (L2TP Network Server), размещенной в LAN.



Удаленная система инициирует PPP-соединение с LAC через коммутируемую телефонную сеть PSTN (Public Switched Telephone Network). LAC затем прокладывает туннель для PPP-соединения через Интернет, Frame Relay или ATM к LNS, и таким образом осуществляется доступ к исходной LAN. Адреса удаленной системе (как и аутентификация/авторизация) предоставляются исходной LAN через согласование с PPP NCP.

LAC-клиент (ЭВМ, которая исполняет программу L2TP) может также участвовать в туннелировании до исходной LAN без использования отдельного LAC, если ЭВМ, содержащая программу LAC-клиента, уже имеет соединение с Интернет. Создается «виртуальное» PPP-соединение, и локальная программа L2TP LAC формирует туннель до LNS. Как и в вышеописанном случае, адресация, аутентификация и авторизация будут обеспечены областью управления исходной LAN.

Обзор протокола

L2TP использует два вида пакетов: управляющие и информационные сообщения. Управляющие сообщения используются при установлении, поддержании и аннулировании туннелей и вызовов. Информационные сообщения используются для инкапсуляции PPP-кадров, пересылаемых по туннелю. Управляющие сообщения используют надежный контрольный канал в пределах L2TP, чтобы гарантировать доставку. Информационные сообщения при потере не пересылаются повторно.

Управляющее сообщение имеет порядковый номер, используемый в управляющем канале для обеспечения надежной доставки. Информационные сообщения могут использовать порядковые номера, чтобы восстановить порядок пакетов и детектировать потерю кадров.

Протокольные операции

Необходимая процедура установления PPP-сессии туннелирования L2TP включает в себя два этапа:

- установление управляющего канала для туннеля
- формирование сессии в соответствии с запросом входящего или исходящего вызова.

Туннель и соответствующий управляющий канал должны быть сформированы до инициализации входящего или исходящего вызовов. L2TP-сессия должна быть реализована до того, как L2TP сможет передавать PPP-кадры через туннель. В одном туннеле могут существовать несколько сессий между одними и теми же LAC и LNS.

PPP-туннелирование: