Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По лабораторной работе №11**

Студент: Смирнов Алексей Игоревич

Дисциплина/Профессиональный модуль: Инфокоммуникационные системы и сети

Группа: 3ПКС-220

Вариант: 22

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2023г.**

**Лабораторная работа №11**

**Описание протокола RDP**

**Цель работы:** ознакомиться с протоколом удаленного рабочего стола RDP.

**Задание:** дать описание протоколу и рассказать о его подключении

**Выполнение работы:**

Протокол RDP основан на семействе стандартов протокола T-120 и является его расширением. Протокол, поддерживающий несколько каналов, позволяет использовать отдельные виртуальные каналы для передачи следующих сведений:

* данные презентации
* последовательная связь с устройством
* сведения о лицензировании
* строго зашифрованные данные, такие как активность клавиатуры и мыши

RDP — это расширение основного протокола T.Share. Некоторые другие возможности сохраняются как часть RDP, например, архитектурные особенности, необходимые для поддержки многоточечных (многосторонних) сеансов. Доставка данных из нескольких точек позволяет в реальном времени доставлять данные из приложения нескольким сторонам, таким как виртуальные доски. Не требуется отправлять одинаковые данные в каждый сеанс по отдельности.

В этом первом выпуске Windows Terminal Server мы будем концентрироваться на обеспечении надежного и быстрого обмена данными «точка–точка» (один сеанс). В первоначальном выпуске Terminal Server 4.0 используется только один канал данных. Однако гибкость протокола RDP предоставляет достаточно места для функциональных возможностей в будущих продуктах.

Одна из причин, по которой корпорация Майкрософт решила реализовать RDP в целях подключения в Windows NT Terminal Server, заключается в том, что он предоставляет расширяемую базу для создания множества дополнительных возможностей. RDP предоставляет 64 000 отдельных каналов для передачи данных. Однако в настоящее время для передачи данных используется только один канал (для клавиатуры, мыши и данных презентации).

Протокол RDP предназначен для поддержки различных типов сетевых топологий, таких как ISDN и POTS. Протокол RDP также предназначен для поддержки многих протоколов локальной сети, таких как IPX, NetBIOS и TCP/IP. Текущая версия RDP будет работать только по протоколу TCP/IP. Благодаря отзывам клиентов в будущих версиях может быть добавлена поддержка других протоколов.

Действия, связанные с отправкой и получением данных через стек RDP, по сути, аналогичны стандартам семиуровневой модели OSI для распространенных сегодня сетей LAN. Данные от приложения или службы, которые необходимо передать, передаются через стеки протоколов. Они разделяются, направляются в канал (через MCS), шифруются, структурируются и упаковываются в сетевой протокол и, наконец, обрабатываются и отправляются клиенту по сети. Возвращение данных выполняется так же, только в обратном направлении. Пакет удаляется из адреса, а затем распаковывается, расшифровывается и т. д. Наконец, данные представляются приложению для использования. Основные части изменений стека протокола происходят между четвертым и седьмым уровнями, где данные являются:

* зашифрованными;
* упакованными;
* систематизированными;
* направленными в канал;
* приоритезированными.

Одним из ключевых моментов для разработчиков приложений является то, что при использовании RDP корпорация Майкрософт абстрагируется от сложностей работы со стеком протоколов. Это позволяет им создавать 32-разрядные продуманные, корректно написанные приложения. Затем стек RDP, реализованный сервером терминалов и его клиентскими подключениями, берет на себя остальные операции.

В составе стека RDP стоит рассмотреть четыре компонента:

* Служба связи Multipoint (MCSMUX)
* Общее управление конференцией (GCC)
* Wdtshare.sys
* Tdtcp.sys

MCSmux и GCC являются частью семейства T.120 Международного союза электросвязи (ITU). MCS состоит из двух стандартов:

* T.122: определяет службы multipoint
* T.125: указывает протокол передачи данных.

MCSMux управляет:

* назначением каналов путем мультиплексирования данных на предопределенные виртуальные каналы в протоколе
* уровнями приоритета
* сегментацией отправляемых данных

По сути, MCSMux объединяет несколько стеков RDP в единую сущность с точки зрения GCC. GCC отвечает за управление этими каналами. GCC позволяет создавать и удалять сеансы подключения и управляет ресурсами, предоставляемыми MCS. Для каждого протокола сервера терминалов (в настоящее время поддерживаются только ICA Citrix и RDP) будет загружен экземпляр стека протоколов (стек прослушивателя, ожидающий запроса на подключение). Драйвер устройства сервера терминалов координирует действия протокола RDP и управляет ими. Он состоит из более мелких компонентов:

* драйвер RDP (Wdtshare.sys) для передачи с помощью пользовательского интерфейса, сжатия, шифрования, кадрирования и т. д.
* транспортный драйвер (Tdtcp.sys) для упаковки протокола в базовый сетевой протокол TCP/IP.

Протокол RDP был разработан для полной независимости от базового транспортного стека, в данном случае TCP/IP. Это обеспечивает возможность добавлять другие транспортные драйверы для других сетевых протоколов, которые по мере их роста могут понадобиться клиентам, без внесения значительных изменений в основные части протокола. Они являются ключевыми элементами производительности и расширяемости RDP в сети.

**Подключение к удаленному рабочему столу**

Для [подключения по RDP](http://www.dprotricks.com/remote-desktop-access-computer-remotely/) необходимо, на удаленном компьютере была учетная запись с паролем, в системе должны быть разрешены удаленные подключения, а чтобы не менять данные доступа при постоянно меняющемся динамическом IP-адресе, в [настройках сети](http://spvcomp.com/stat/rdp_nastroit_udaalennij_rabochij_stol.php) можно присвоить статический IP-адрес. Удаленный доступ возможен только на компьютерах с Windows Pro, Enterprise или Ultimate.  
Для удаленного подключения к компьютеру нужно разрешить подключение  в «Свойствах Системы» и задать пароль для текущего пользователя, либо создать для RDP нового пользователя. Пользователи обычных аккаунтов не имеют права самостоятельно предоставлять компьютер для удаленного управления. Такое право им может дать администратор. Препятствием использования протокола RDP может стать его блокировка антивирусами. В таком случае RDP нужно разрешить в настройках антивирусных программ.

При подключении к удаленному рабочему столу через командную строку (MSTSC) можно задать дополнительные параметры RDP:

|  |  |
| --- | --- |
| /v:<сервер[: порт]> | Удаленный компьютер, к которому выполняется подключение. |
| /admin | Подключение к сеансу для администрирования сервера. |
| /edit | Редактирование RDP-файла. |
| /f | Запуск удаленного рабочего стола на полном экране. |
| /w:<ширина> | Ширина окна удаленного рабочего стола. |
| /h:<высота> | Высота окна удаленного рабочего стола. |
| /public | Запуск удаленного рабочего стола в общем режиме. |
| /span | Сопоставление ширины и высоты удаленного рабочего стола с локальным виртуальным рабочим столом и развертывание на несколько мониторов. |
| /multimon | Настраивает размещение мониторов сеанса RDP в соответствии с текущей конфигурацией на стороне клиента. |
| /migrate | Миграция файлов подключения прежних версий в новые RDP-файлы. |

**Вывод:** в ходе выполнения практической работы я познакомился с протоколом удаленного рабочего стола RDP, узнал, как подключиться к удаленному рабочему столу