УДК 004.771:004.932

А.Д. Калюжный, Г.В. Табунщик, В.Ф. Онищенко

Запорожский национальный технический университет, Запорожье

СРЕДСТВА ПЕРЕДАЧИ ИНФОРМАЦИИ В ТЕРМИНАЛЬНЫХ СИСТЕМАХ

В статье проанализирована терминальная схема построения сети предприятия, выделены преимущества и недостатки данной сетевой структуры. Авторами проанализированы протоколы обмена данными, использующиеся в терминальных системах, и проведено сравнение продуктов основанных на протоколах удаленного доступа. Рассмотрена реализация средств передачи видео-потока с использованием протокола RDP, приведено обоснование использования x264 кодека для сжатия видеопотока.

Ключевые слова: *терминальная система, протокол удаленного доступа, сжатие, передача видео-потока.*

Введение

Построение информационных систем предприятия при заданном наборе функциональных возможностей требует достижения оптимального соотношения стоимости, производительности и надежности. Говоря о стоимости информационной системы предприятия следует учитывать не только стоимость создания, но и стоимость владения системой на ее жизненном цикле [1].

Как следствие, при развертывании дополнительных компьютеризированных рабочих мест, основное назначение которых – стандартное офисное применение, не целесообразно устанавливать полнофункциональные персональные компьютеры (ПК). Экономически обоснованным решением является применение терминальных станций.

При разработке приложений уровня предприятий, возникает задача передачи видео-потока, например в системах наблюдения за персоналом, и системах организации телеконференций. Также примером может выступать система дистанционного обучения, в которых изображение с web-камеры используется для подтверждения личности студента, а также для контроля над процессом сдачи экзамена.

Разрабатывая приложения данного класса, необходимо учитывать особенности архитектуры терминальных систем, протоколов взаимодействия, а также обеспечить эффективность передачи данных.

Архитектура терминальных систем

Архитектура терминальной системы основывается на принципах построения адаптивной инфраструктуры, которая в свою очередь основана на следующих принципах: простота; уменьшение количества составляющих; упрощение настройки под специфические требования; автоматизация изменений; стандартизация; использование стандартных технологий и интерфейсов; заимствование общей архитектуры; применение стандартных процессов; модульность; избавление от монолитной структуры; создание повторно используемых компонентов; применение логических архитектур; интеграция; связь бизнеса и информационных технологий (IT); связь приложений и бизнес-процессов внутри и вне предприятия.

Существует большое множество вариантов построения сетевых структур на основе терминальных решений. Вариант решения зависит от потребностей конкретной организации. Например, на основе терминальных систем возможно построить архитектуру, узлами которой будут являться тонкие клиенты с поддержкой работы с различными видами оборудования такими как принтеры, web-камеры, устройства передачи звука и пр. Также в качестве клиентов в терминальных системах могут использоваться портативные устройства и рабочие станции с различными операционными системами. Связь клиента с сервером может осуществляться через различные виды соединений, например это может быть Wi-Fi

или GPRS-соединение [2].

Современные средства терминального доступа, применяющиеся на персональных компьютерах, специализированных терминальных рабочих станциях и портативных устройствах, основаны на принципе централизации вычислений и коллективизации ресурсов похожем на мэйнфреймы. В данном случае, пользователем на рабочей станции запускается клиентская часть средства терминального доступа и происходит обращение к удаленному серверу, содержащему соответствующую серверную часть данного средства. При успешной аутентификации серверная часть средства терминального доступа создает для пользователя собственную сессию, в которой в адресном пространстве сервера запускаются нужные ему приложения. Пользовательский интерфейс приложений, запущенных таким образом, доступен на рабочей станции в окне клиентской части средства терминального доступа. Пользователь, с помощью клавиатуры и мыши рабочей станции, может управлять данными приложениями — сведения о нажатых клавишах и движении мыши (а также содержимое буфера обмена) передаются сеансу данного пользователя на сервере, а обратно поступают изменения в пользовательском интерфейсе приложений. По закрытии сессии все выполнявшиеся в ней приложения закрываются.

Преимущества и недостатки использования терминальных систем. Преимущества применения терминального доступа, такие как: высокая надежность, повышенный уровень безопасности, быстрая и эффективная модернизация, возможность использования старых ПК, экономия на стоимости ПО, простота администрирования, простая масштабируемость информационных систем (ИС), удаленный доступ к рабочим данным и приложениям, и нечувствительность к пропускной способности сети становятся очевидны при наличии большого количества рабочих станций или при повышенных требованиях к безопасности и к централизации хранения данных [3].

Высокая надежность. Все данные хранятся и обрабатываются на серверах, на которых регулярно и централизованно создаются резервные копии, что сводит к минимуму риск потери информации. Отсутствие для пользователей возможности самостоятельной установки новых приложений минимизирует риск возникновения программных конфликтов и заражения вирусами. Замена вышедшего из строя ПК, работающего в терминальном режиме, сводится к установке вместо него другого стандартного системного блока или "тонкого клиента" - при этом не требуется перенос данных, переустановка операционной системы (ОС) и приложений.

Повышенный уровень безопасности. При работе по терминальной схеме сервер, на котором хранятся все данные, может находиться достаточно удаленно. На рабочих местах пользователей никакие конфиденциальные данные храниться не будут, а отсутствие съемных накопителей не позволит скопировать важные данные на внешний носитель.

Быстрая и эффективная модернизация. Устройства, установленные на клиентских местах, не требуют модернизации. Модернизация всех рабочих мест в компании сводится к модернизации одного или нескольких серверов, что обходится во много раз дешевле и выполняется несравненно быстрее, чем обновление (а тем более замена) сотни ПК.

Возможность использования старых ПК. В качестве терминальных клиентов можно использовать устаревшие компьютеры, уже не поддерживающие современные приложения в обычном режиме.

Экономия на стоимости программного обеспечения (ПО). Приобретение терминальной лицензии для одного рабочего места дешевле чем приобретение полной копии ОС [4].

Простота администрирования. Поскольку все используемые приложения установлены на сервере, их сопровождение может выполняться одним системным администратором. Обновление ПО и установка новых приложений производится централизованно (после инсталляции на сервер и минимальной настройки новое ПО становится доступным всем подключенным клиентам). Терминальные системы предусматривают также разграничение прав пользователей относительно используемого ПО. Терминальные системы позволяют администратору подключаться к клиентской сессии пользователя и дистанционно оказывать помощь и решать возникающие проблемы. Поскольку рабочие места могут находиться в другом здании, или даже в другом городе, данные системы позволяют сэкономить времена и средства при их администрировании.

Простая масштабируемость ИС. Добавление новых рабочих мест производится простой установкой новых терминалов и их быстрым конфигурированием на сервере. На новом рабочем месте не требуется ни установка и настройка операционной системы, ни инсталляция приложений и их конфигурирование. Если с ростом числа клиентов становится недостаточно мощности сервера, можно произвести его модернизацию или установить дополнительный сервер, создав терминальный кластер и настроив схему балансировки нагрузки между его узлами. Такой шаг повысит быстродействие всей ИС - приложения у всех подключенных клиентов будут выполняться быстрее и с меньшими задержками.

Удаленный доступ к рабочим данным и приложениям. Возможности системы позволяют настроить конфигурацию так, что отдельные пользователи смогут получать доступ к своим рабочим данным и приложениям из любого места, где есть канал связи – из дома через модем, из другого офиса

через Internet или даже из "чистого поля", имея с собой ноутбук или портативный ПК плюс мобильный телефон.

Нечувствительность к пропускной способности сети. Между клиентским рабочим местом и сервером передается минимум информации (нажатия клавиш и движения мыши от клиента и команды на обновление экрана с сервера). Для этого достаточно порядка 10 KB/сек для каждого клиента, и пропускной способности одного 100-мегабитного сегмента сети хватит для поддержания работы до 1000 пользователей. При переходе на большие объемы обрабатываемых данных обновление всей сетевой структуры может и не потребоваться - достаточно будет нарастить мощность серверного парка и, может быть, пропускную способность канала между серверами.

К недостаткам использования терминальных систем можно отнести то, что требования к аппаратной части сервера во многом зависят от количества пользователей одновременно работающих с терминальным сервером и от типа приложений, с которыми они работают. Однако, современные средства терминального доступа способны работать с кластерами серверов и осуществлять баланс загрузки.

К приложениям, которые не желательно использовать в терминальном режиме, можно отнести продукты, которые требуют очень больших вычислительных ресурсов в монопольном режиме – это системы обработки изображений, графического моделирования, "тяжелые" САПР, средства разработки и отладки программного обеспечения. Однако это зависит от мощности сервера и характера работы приложений.

Доступ клиентов к приложениям осуществляется через терминальный сервер с использованием одного из известных протоколов терминального доступа.

Рассмотрим наиболее популярные: протокол RDP разработанный Microsoft, протокол ICA корпорации Citrix, и протокол VNC который был создан в Olivetti & Oracle Research Lab.

Анализ используемых протоколов удаленного доступа в терминальных системах

Принцип работы протоколов состоит в следующем: для выполняющихся на сервере программ эмулируется устройство вывода изображения (GDI). Программа выполняет обычный вывод на экран, а протоколы упаковывают эти данные в удобный для передачи по сети формат, и передают клиенту. Клиент производит форматирование команд и выполняет на локальном экране у пользователя. В обратном порядке, все действия пользователя (движения мышью, нажатия клавиш) передаются от приложения на тонком клиенте на сервер, где соответствующий драйвер «подкладывает» их как будто они пришли с локальной мыши и клавиатуры.

RDP (англ. Remote Desktop Protocol) – протокол прикладного уровня, использующийся для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений. Клиенты существуют практически для всех версий Windows (включая Windows CE и Mobile), Linux, FreeBSD, Mac OS X [5].

Microsoft предполагает два режима использования протокола RDP:

– для администрирования (Remote administration mode);

– для доступа к серверу терминалов (Terminal Server mode).

RDP в режиме администрирования**,** используется всеми современными операционными системами Microsoft. Серверные версии Windows поддерживают одновременно два удаленных подключения и один локальный вход в систему, в то время как клиентские – только один вход (локальный или удаленный).

Режим доступа к серверу терминалов возможен только в серверных версиях Windows. Количество удаленных подключений в данном случае не лимитируется, но требуется настройка сервера лицензий (License server) и его последующая активация. Сервер лицензий может быть установлен как на сервер терминалов, так и на отдельный сетевой узел. Возможность удаленного доступа к серверу терминалов открывается только после установки соответствующих лицензий на License server.

При использовании кластера терминальных серверов и балансировки нагрузки требуется установка специализированного сервера подключений (Session Directory Service). Данный сервер индексирует пользовательские сессии, что позволяет выполнять вход, а также повторный вход на терминальные серверы, работающие в распределенной среде.

Принцип работы RDP. Протокол является прикладным, базирующимся на TCP. После установки соединения на транспортном уровне инициализируется RDP-сессия, в рамках которой согласуются различные параметры передачи данных. Передача вывода с помощью примитивов является приоритетной для протокола RDP, так как значительно экономит трафик; а изображение передается лишь в том случае, если иное невозможно по каким-либо причинам (не удалось согласовать параметры передачи примитивов при установке RDP-сессии). RDP-клиент обрабатывает полученные команды и выводит изображения с помощью своей графической подсистемы. Пользовательский ввод по умолчанию передается при помощи скан-кодов клавиатуры.

RDP поддерживает несколько виртуальных каналов в рамках одного соединения, которые могут

использоваться для обеспечения дополнительного функционала:

– использование принтера или последовательного порта;

– перенаправление файловой системы;

– поддержка работы с буфером обмена;

– использование аудио- подсистемы.

Характеристики виртуальных каналов согласуются на этапе установки соединения.

Работа протокола при стандартных настройках сжатия и глубине цвета 32 бит занимает максимум 160 Кбайт/сек ширины пропускания канала, и данная цифра уменьшается со снижением глубины цвета. При глубине цвета 8 бит для работы протокола необходимо максимум 60 Кбайт/сек [6].

Обеспечение безопасности при использовании RDP. Спецификация протокола RDP предусматривает использование одного из двух подходов к обеспечению безопасности:

– Standard RDP Security (встроенная подсистема безопасности);

– Enhanced RDP Security (внешняя подсистема безопасности).

Standard RDP Security**.** При данном подходе аутентификация, шифрование и обеспечение целостности реализуется средствами, заложенными в RDP-протокол. Рассмотрим данные этапы подробнее.

1. Аутентификация. Аутентификация сервера выполняется следующим образом:

1) при старте системы генерируется пара RSA-ключей;

2) создается сертификат (Proprietary Certificate) открытого ключа;

3) сертификат подписывается RSA-ключом, зашитым в операционную систему (любой RDP-клиент содержит открытый ключ данного встроенного RSA-ключа);

4) клиент подключается к серверу терминалов и получает подписанный сертификат;

5) клиент проверяет сертификат и получает открытый ключ сервера (данный ключ используется в дальнейшем для согласования параметров шифрования).

Аутентификация клиента проводится при вводе имени пользователя и пароля.

2. Шифрование. В качестве алгоритма шифрования выбран потоковый шифр RC4. В зависимости от версии операционной системы доступны различные длины ключа от 40 до 168 бит.

Максимальная длина ключа для операционных систем Winodws:

– Windows 2000 Server – 56 бит;

– Windows XP, Windows 2003 Server – 128 бит;

– Windows Vista, Windows 2008 Server – 168 бит.

При установке соединения после согласования длины генерируется два различных ключа: для шифрования данных от клиента и от сервера.

3. Целостность. Целостность сообщения достигается применением алгоритма генерации MAC (Message Authentication Code) на базе алгоритмов MD5 и SHA1.

Начиная с Windows 2003 Server, для обеспечения совместимости с требованиями стандарта FIPS (Federal Information Processing Standard) 140-1 возможно использование алгоритма DES для шифрования сообщений и алгоритма генерации MAC, использующего только SHA1, для обеспечения целостности.

Enhanced RDP Security. В данном подходе используются внешние модули обеспечения безопасности: TLS 1.0 и CredSSP [5].

Протокол TLS можно использовать, начиная с версии Windows 2003 Server, но только если его поддерживает RDP-клиент. Поддержка TLS добавлена, начиная с RDP-клиента версии 6.0.

При использовании TLS, сертификат сервера можно генерировать средствами Terminal Sercives или выбирать существующий сертификат из хранилища Windows.

Протокол CredSSP представляет собой совмещение функционала TLS, Kerberos и NTLM.

Рассмотрим основные достоинства протокола CredSSP [5]:

– проверка разрешения на вход в удаленную систему до установки полноценного RDP-соединения, что позволяет экономить ресурсы сервера терминалов при большом количестве подключений;

– надежная аутентификация и шифрование по протоколу TLS;

– использование однократного входа в систему (Single Sign On) при помощи Kerberos или NTLM.

Технологии и возможности, предоставляемые приложениями на основе RDP. Решения для серверов приложений активно продвигаются компанией Microsoft, расширяется функционал, вводятся дополнительные модули. Наибольшее развитие получили технологии, упрощающие установку приложений и компоненты, отвечающие за работу сервера терминалов в глобальных сетях [7].

К последней версии протокола, которая вышла в составе Windows 7, добавлены следующие возможности:

– поддержка аутентификации сетевого уровня (NLA);

– увеличение производительности ядра RDP;

– поддержка технологии Windows Aero (Aero over Remote Desktop);

– поддержка технологий Direct2D и Direct3D 10.1 в приложениях;

– полноценная поддержка мультидисплейных конфигураций;

– улучшения в работе с мультимедиа;

– поддержка технологии Media Foundation;

– поддержка технологии DirectShow;

– снижена длительность задержки при воспроизведении аудио;

– поддержка двунаправленных аудиопотоков.

В Terminal Services для Windows 2008 Server введены следующие возможности [5]:

– Terminal Services Printing – позволяет использовать принтер клиента для печати из приложений на сервере терминалов;

– Terminal Services RemoteApp – обеспечивает доступ к любым приложениям через службу терминалов. Для пользователя в данном случае сервер терминалов становится совершенно прозрачным;

– Terminal Services Web Access – позволяет клиентам подключаться к приложениям RemoteApp при помощи обычного браузера. В роли связующего звена для RemoteApp выступает Web –сервер;

– Terminal Services Gateway – данная технология организует работу RDP поверх установленного HTTPS- соединения. TS Gateway дает возможность удаленным пользователям подключаться к серверу приложений через региональные сети или Internet с использованием безопасного SSL- туннеля и с минимальной настройкой сетевых устройств;

– Terminal Services Session Broker – позволяет организовывать подключения пользователей к серверным платформам, использующим балансировку сетевой нагрузки;

VNC (англ. Virtual Network Computing) – система базирующаяся на концепции *RFB* (англ. Remote FrameBuffer, удалённый кадровый буфер). В основе системы VNC лежит протокол RFB [8].

Принцип работы протокола VNC**.** Данные о нажатии клавиш и движении мыши, выполняемых пользователем на собственном компьютере передаются по сети на удаленный компьютер и воспринимаются им действия с его собственными клавиатурой и мышью. Схема при которой вывод с удаленного компьютера на экран пользователя основывается на графических примитивах (прямоугольник пиксельных данных выводится в заданной координатами позиции) в своей примитивной форме потребляет большую часть пропускной возможности канала. Существуют различные кодировки — методы определения наиболее эффективного способа передачи этих прямоугольников. Протокол VNC позволяет клиенту и серверу «договориться» о том, какая кодировка будет использована. Самый простой метод кодирования, поддерживаемый всеми клиентами и серверами — «raw encoding», при котором пиксели передаются в порядке слева-направо, сверху-вниз, и после передачи первоначального состояния экрана передаются только изменившиеся пиксели. Этот метод работает очень хорошо при незначительных изменениях изображения на экране (движения указателя мыши по рабочему столу, набор текста под курсором), но загрузка канала становится очень высокой при одновременном изменения большого количества пикселей, например, при просмотре видео в полноэкранном режиме.

Для работы требуется ширина пропускания канала от 32 Кбит/сек до 2 Мбит/сек. Для комфортной работы в полноцветном режиме при разрешении экрана 1024x768 скорость канала должна быть 1-2 Мбит/сек. При снижении качества графики, при уменьшении числа цветов и при некоторых дополнительных способах оптимизации, приемлемое удобство может обеспечить скорость 128 Кбит/сек. Канал занимается полностью только при обновлении больших участков экрана, при печати текста трафик заметно меньше, а в остальное время канал практически не используется. Если при передаче по каналу возникают большие задержки передачи пакетов (медленные каналы, спутниковая связь, большие расстояния), это вызывает ухудшение времени реакции на нажатие клавиш и движение мыши, что значительно снижает комфортность работы.

Обеспечение безопасности при использовании VNC. Метод обеспечения безопасности (security type) определяется на стадии «рукопожатия», после согласования версии протокола, который будет использоваться. Спецификация протокола описывает следующие методы обеспечения безопасности:

– отсутствие аутентификации и шифрования трафика;

– VNC аутентификация – шифрование трафика не используется, однако пароль не передается в открытом виде, а используется алгоритм «вызов-ответ» с DES-шифрованием (эффективная длина ключа составляет 56-бит).

Также многие современные реализации VNC поддерживают расширения стандартного протокола, которые реализуют шифрование и/или сжатие VNC-трафика, разграничения по спискам доступа ACL и различные методы аутентификации.

При необходимости надежного шифрования всей VNC-сессии, она может быть установлена через SSL, SSH или VPN-туннель, а также поверх IPSec. Технология IPSec поддерживается подавляющим большинством современных ОС и используется как при соединении через Интернет, так и в локальных сетях. SSH-клиенты позволяют создавать SSH-туннели как со всех основных платформ (UNIX, Windows, Macintosh и др.), так и для менее популярных [8].

Данным протоколом предоставляются следующие технологии и возможности [9]:

– обмен файлами;

– весомое увеличение скорости отрисовки экрана удаленного компьютера, в локальной сети;

– подключение плагина шифрования для улучшения безопасного обмена данными;

– поддержка доменной атентификации;

– поддержка чата с удаленным компьютером для обмена сообщениями;

– ViewerToolbar, JavaViewer с поддержкой передачи файлов;

– автомасштабирование для подгонки размера изображения удаленного компьютера;

– поддержка нескольких мониторов;

– Repeater/Proxy-support;

– печать файлов с VNC-сервера на принтер по умолчанию, подключенный к компьютеру VNC-клиента;

– возможность обслуживания VNC клиента, для Java и VNC сессий, через один TCP порт, что упрощает NAT и конфигурацию файрвола;

– возможность подключения VNC клиента через различные web-прокси сервера и фильтры, что делает его использование таким же простым как и использование браузера.

ICA (англ. Independent Computing Architecture) – это закрытый протокол для сервера приложений, разработанного компанией Citrix Systems. Протокол определяет спецификацию обмена данными между сервером и клиентами, но не встроен ни в одну из платформ. ICA выполняет задачи, во многом схожие с X Window System [10].

Протокол ICA обеспечивает стандартную поддержку графического вывода и ввода данных с клавиатуры, мыши. Базовый механизм передачи между сервером и клиентом графических данных и данных, вводимых с клавиатуры/мыши, по протоколу ICA почти идентичен тому, который используется в протоколе RDP. Обеспечение безопасности при использовании ICA. Так как спецификация протокола является закрытой, следует говорить о шифровании в продуктах на основе данного протокола. Например, Citrix Metaframe поставляется только с минимальными функциями шифрования для ICA-подключений и поддерживает только режим простейшего шифрования, который задействует простой экспортируемый алгоритм с менее чем 40-разрядным ключом. Если необходимо организовать защиту для подключений ICA, то следует приобрести дополнительный пакет SecureICA для MetaFrame. В SecureICA использован алгоритм шифрования RSA RC5 и поддерживаются 40-, 56- и 128-разрядные ключи.

Для шифрования коммуникация между сервером и клиентом ICA может использоваться Citrix SSL Relay, который обеспечивает шифрование по протоколу Secure Sockets Layer/Transport Layer Security (SSL/TLS) [10].

Ниже перечислены многие возможности клиентского программного обеспечения Citrix ICA, которые присутствуют в MetaFrame [10]:

– интеграция локального и удаленного буферов обмена;

– отображение клиентских устройств (принтеров, дисков, COM-портов и звуковых плат);

– эмуляция локальных окон;

– приложение Program Neighborhood;

– запуск и внедрение приложений (Application Launching and Embedding, ALE);

– отображение сеансов;

– Business Recovery Client;

– постоянный кэш растровой графики.

Более широкие функциональные возможности предоставляются такими продуктами как Citrix XenServer, XenDesktop и XenApp, которые предназначения для решения задач виртуализации. Например, среди возможностей Citrix XenServer 5.6 присутствуют следующие [11]:

– Distributed Virtual Switching**.** Эта возможность позволяет использовать средства управления распределенным сетевым взаимодействием хост-серверов и виртуальных машин;

– VM Protection & Recovery. использование снятия мнгновенных снимков и экспорта виртуальных машин по расписанию. Новая версия XenServer включает в себя простую утилиту для бэкапа виртуальных машин и их восстановления;

– Web Self-Service. Портал самообслуживания для пользователей виртуальных машин на основе привилегий, определенных администратором. Создание машин прямо из портала данной версией не поддерживается;

– HA Restart Priority. Возможность настройки политик механизма отказоустойчивости таким образом, чтобы расставить приоритеты по старту виртуальных машин отказавшего хост-сервера;

– Improved XenDesktop VDI scalability. Улучшения под виртуализацию настольных ПК (VDI) – увеличение коэффициента консолидации виртуальных машин на хост-серверах посредством использования компонентом control domain (Dom0) нескольких процессоров и других улучшений;

– XenDesktop platform enhancements. Технология локального кэширования образов виртуальных машин для экономии дискового пространства в инфраструктуре виртуальных ПК (VDI). Будет использоваться в следующей версии Citrix XenDesktop.

Так как в протоколе VNC отсутствуют изначально-интегрированные каналы передачи данных, то без дальнейшего улучшения данного протокола, он не может использоваться при реализации собственных приложений, в отличие от протоколов ICA и RDP.

Протокол ICA по сравнению с RDP позволяет:

– обеспечить бесшовный режим (с сервера передаются данные не обо всём рабочем столе, а только о содержимом конкретного окна);

– уменьшить потребление трафика при работе;

– улучшить субъективные впечатления от скорости ответа сервера за счёт эмуляции поведения курсора и полей ввода текста на локальном клиенте (введённые символы отображаются на экране раньше, чем их обработает сервер);

– лучшая адаптация к линиям с плохой связью (в частности, за счёт эмуляции ответа сервера локально, за счёт согласования времени повторной отправки не дошедших данных);

Главными минусами ICA по сравнению с RDP являются:

– необходимость установки отдельного дорогостоящего ПО на терминальный сервер, при этом расходы на лицензирования терминального сервера у компании Microsoft остаются прежними;

– необходимость дополнительного конфигурирования, что является недостатком в случае сетей малого и среднего размера, из-за увеличения сложности обслуживании;

– необходимость приобретения лицензии для пользователей (помимо лицензий Microsoft), что увеличивает цену лицензии «на пользователя» в несколько раз (без учёта остального ПО), а также раздельная (не полностью совместимая) система учёта лицензий пользователей [12].

Было проведено сравнение продуктов основанных на протоколах удаленного доступа (табл. 1).

На основании проведенного анализа было решено выделить для использования протокол RDP, поскольку данный протокол обеспечивает высокий уровень безопасности, практически не влияет на пропускную способность канала [6], а также имеет полную документацию и является простым в администрировании.

Таблица 1

Сравнение продуктов основанных на протоколах удаленного доступа

Продукт	Remote Desktop Services/ Terminal Services	RealVNC Enterprice	Citrix XenApp
Протокол	RDP	VNC	ICA, RDP
Лицензирование	Собственность	Собственность	Собственность
Режим Работы	Клиент & Сервер	Клиент & Сервер & Прослушивание	Клиент & Сервер
Шифрование	RC4	AES-128	SSL, TLS
Поддержка звука	+	–	+
Многоклиентный режим	+	+	+
Бесшовные окна	+	–	+
Удаленный помощник	+	?	?
Запрос прав	+	?	?
Linux клиент	+	+	+
Mac OS X клиент	+	+	+
Microsoft Windows клиент	+	+	+
Windows Mobile клиент	+	–	+
Java клиент	+	+	+
Android клиент	+	–	+

Реализация средств передачи видео-потока с использованием RDP протокола

При разработке приложений уровня предприятия, возникает задача передачи видео-потока, например в системах наблюдения за персоналом, и системах дистанционного обучения.

Разрабатываемое приложение должно обладать следующими функциональными возможностями: создание виртуальной камеры на стороне сервера; определения камер подключенных к стороне клиен-

та (физическая сторона); возможность работы с виртуальной камерой нескольким приложениям одновременно; возможность одновременной работы в нескольких RDP-сессиях с одной и той же веб-камерой; предоставление пользователю на виртуальной стороне списка камер, подключенных к физической стороне, для их дальнейшей эмуляции; обеспечение RGB24 формата видео-потока и размера изображения 320*240 с веб-камеры на стороне сервера; возможность сохранения выбранной пользователем веб-камеры, между переключениями RDP-сессиий; возможность сохранения камеры как выбранной, на виртуальной стороне, при ее переключении с одного USB-порта в другой; ведение журнала ошибок во время работы программы, для каждого отдельного модуля системы.

Для передачи видео-потока, получаемого с Web-камеры, по сети, требуется большая пропускная способность канала. Недостаточная пропускная способность канала приводит к потере актуальности передаваемого видеосигнала, а также снижает его информативность. Решением данной проблемы является эффективное сжатие передаваемого видеосигнала.

Сжатие и декомпрессия видеосигнала выполняется с использованием кодеков, которые могут быть выполнены программно или аппаратно. В работе было проведено сравнение по скорости, требуемым ресурсам процессора (ЦП) и качеству компрессии таких распространенных кодеков как MJPEG, x264, и XviD кодек, при формате видео изображения RGB24 320*240. Также для каждого из кодеков было рассчитано среднеквадратическое отклонение элементов кодируемого потока (табл. 2) [13].

Из таблицы можно сделать следующие выводы [13]:

1. По качеству компрессии: MJPEG значительно уступает x264 и XviD кодекам. Отношение сжатого кадра изображения к несжатому составляет 40%. У x264 кодека коэффициент сжатия видеопотока составляет 1%. XviD кодек также имеет коэффициент сжатия 1%.

2. По времени сжатия: x264 выполняет компрессию видео-потока на 25% быстрее чем XviD кодек. Скорость сжатия MJPEG кодека в среднем равна скорости сжатия x264 кодека.

3. Для процесса сжатия наименьшее число ресурсов ЦП требует x264 кодек, и составляет 6-8% загрузки ЦП. XviD кодек требует 7-9% загрузки ЦП при выполнении процесса сжатия. MJPEG кодек требует 19-21%. Исследование проводилось на ЦП с тактовой чистотой 2,71 ГГц.

Таблица 2

Сравнительная характеристика кодеков

Кодек	Количество элементов видеопотока	Средний размер сжатого элемента (байт)	Среднеквадратичное отклонение размеров элементов	Время сжатия одного элемента (секунд)	Требуемый Ресурс ЦП для сжатия (%)
MJPEG	1420	68702	2673	0,009	19-21
x264		1021	367	0,009	6-8
XviD		1200	667	0,012	7-9

Была проанализирована эффективность применения разработанного приложения, для целей эмуляции веб-камер в терминальных системах.

Входными данными для анализа эффективности являлись: пропускная способность канала; количество переданных на сторону сервера кадров; загрузка ЦП на стороне клиента и сервера. Для анализа эффективности приложения была взята пропускная способность канала равная 10мбит/с. Размер получаемого сжатого видео-кадра при этом варьировался от 1 кбайта до 2,5 кбайт, следует заметить что, в данном случае, под видео-кадром понимается буфер байт указанного выше размера.

Следовательно, для обеспечения стандартной скорости отображения кадров (25 кадров/с) потребуется передавать в среднем 44 кбайта/с. Был произведен подсчет получаемых на стороне сервера видео-кадров, который показал что количество принимаемых сервером кадров равно 25 кадрам в секунду, при производительности веб-камеры 25 fps. Что свидетельствует об отсутствии отброса кадров, из-за недостаточности сетевого трафика, что в свою очередь подтверждает эффективности сжатия, и актуальность изображения на стороне сервера.

Было произведено измерение загрузки ЦП на стороне клиента и на стороне сервера, которое показало, что при передаче видео-изображения в одну удаленную сессию, ЦП на стороне клиента был загружен на 15-20%, а на стороне сервера на 23-29%, при частоте процессора клиентской стороны 2,71 Ггц, и частоте процессора серверной стороны 2,13 Ггц. Как было показано при анализе средств сжатия видео-сигнала, требуемая загрузка процессора при сжатии составляет 8-12%, при частоте 2,71 Ггц.

Выводы

Выполнен анализ схемы реализации сетевой IT-инфраструктуры в виде терминальной системы, который показал эффективность использования данной архитектуры для большинства предприятий.

Выполнен анализ таких протоколов удаленного доступа как: RDP, VNC, ICA. Анализ проводился по следующих характеристикам: принцип работы, обеспечение безопасности при использовании протокола, технологии и возможности предоставляемые приложениями на основе протокола.

Проведенный анализ позволил выделить следующие преимущества RDP протокола: открытая спецификация протокола; полная документация, аспекты реализации протокола доступны на сайте MSDN; простота развертывания и администрирования; лицензирование терминального сервера не требует приобретения дополнительных лицензий как в случае с лицензиями Citrix. Это свидетельствует о том, что данный протокол подходит для использования в рамках малого и среднего бизнеса.

Был проведен анализ средств сжатия видеосигнала, который доказал эффективность использования x264 кодека. Наибольший коэффициент сжатия и наименьшее среднеквадратическое отклонение, размеров элементов сжатого потока, и наименьшая загрузка ЦП данного кодека свидетельствуют о том, что для передачи видео-потока, потребуется наименьшая пропускная способность канала, и наименьший объем вычислительных ресурсов.

Практической ценностью работы является реализованная система, которая предназначена для передачи видео-потока, с физической стороны на виртуальную средствами RDP-протокола, в системах терминального доступа. На виртуальной стороне был обеспечен формат видео изображения RGB24 320*240.

При использовании данного приложения пользователь получает возможность использовать локально подключенные web-камеры на удаленном компьютере, при этом обеспечивается актуальность изображения получаемого с web-камеры на виртуальной стороне и уменьшается объем передаваемых данных по отношению к объему данных передаваемых без эффективного сжатия.

Список литературы

1. Тонкие клиенты и терминальные системы Citrix и Windows [Электронный ресурс]. – Режим доступа к ресурсу: http://www.uw.ru/thin_client/.

2. Переход на терминальные системы в условия экономического кризиса [Электронный ресурс]. – Режим доступа к ресурсу: http://omsk.narod.ru/documents/5_prichin.html

3. Терминальные решения [Электронный ресурс]. – Режим доступа к ресурсу: http://www.onix.kiev.ua/terminal_advantages.asp

4. Windows Shop [Электронный ресурс]. – Режим доступа к ресурсу: http://www.microsoft.com /windows/buy/default.aspx

5. Security Lab by Positive Technologies [Электронный ресурс]. – Режим досутпа к ресурсу: http://www.securitylab.ru/analytics/367591.php

6. Remote Desktop Protocol Performance [Электронный ресурс]. – Режим доступа к ресурсу: http://download.microsoft.com/download/4/d/9/4d9ae285-3431-4335-a86e-969e7a146d1b/rdp_performance_whitepaper.docx.

7. Принцип работы Microsoft Terminal Services [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/en-us/library/ cc755399(WS.10).aspx

8. The RFB Protocol [Электронный ресурс]. – Режим доступа к ресурсу: http://www.tigervnc.com/cgi-bin/rfbproto#tight-security-type.

9. Управление «Институт информатики ИжГТУ» [Электронный ресурс]. – Режим доступа к ресурсу: http://www.pro-spo.ru/index.php

10. Мазерс Т.В. Архитектура тонкого клиента в Windows NT/2000. Реализация терминальных служб и Citrix MetaFrame / Т.В. Мазерс. – М.: Вильямс, 2001. – 800 с.

11. Виртуализация Citrix XenServer, XenDesktop и XenApp [Электронный ресурс]. – Режим доступа к ресурсу: http://www.vmgu.ru/citrix-xen.

12. «Норма: Терминальные решения» [Электронный ресурс]. – Режим доступа к ресурсу: http://www.normats.ru/support_info_04.shtml.

13. Калюжный А.Д. Анализ средств сжатия видеосигнала / А.Д. Калюжный, Г.В. Табунщик // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2010. – Вип. 7(88). – С. 200.

Поступила в редколлегию 11.04.2011

Рецензент: д-р техн. наук, проф. С.И. Гоменюк, Запорожский национальный университет, Запорожье.

ЗАСОБИ ПЕРЕДАЧА ІНФОРМАЦІЇ В ТЕРМІНАЛЬНИХ СИСТЕМАХ

О.Д. Калюжний, Г.В. Табунщик, В.Ф. Оніщенко

В статті проаналізована термінальна схема побудови мережі підприємства, виділені переваги та недоліки даної мережевої структури. Авторами проаналізовані протоколи обміну даними, що використовуються в термінальних системах, та проведено порівняння продуктів заснованих на протоколах віддаленого доступу. Розглянута реалізація засобів передачі відео-потоку з використанням протоколу RDP. Приведено обґрунтування використання x264 кодека для компресії відеопотоку.

Ключові слова: *термінальна система, протокол віддаленого доступу, компресія, передача відео-потоку.*

INFORMATION TRANSMISSION MEANS IN TERMINAL SYSTEMS

A.D. Kaliuzhnyi, G.V. Tabunshchik, V.F. Onyshchenko

In article the on-structure enterprise terminal network are analysed. The advantages and disadvantages of such network are defined. Authors analysed the terminal system communication protocols. The protocol based product comparison is made by the authors. The video image transmission means implementation using RDP is considered. The usage of x264 codec for purposes of video image compression is grounded by the authors.

Keywords: *terminal system, remote access protocol, compression, video image transmission.*