ОСОБЕННОСТИ ПОСТРОЕНИЯ СОВРЕМЕННОЙ БЕСПРОВОДНОЙ КОРПОРАТИВНОЙ СЕТИ

Юрий Лисецкий, Наталья Каревина

Аннотация: *Представлено построение современной беспроводной корпоративной сети, реализующей концепцию использования собственных устройств. Сформулированы требования к современным беспроводным сетям корпоративного уровня, изложены принципы их построения и особенности архитектуры. Рассмотрены вопросы организации информационной безопасности в беспроводных корпоративных сетях.*

Ключевые слова: *беспроводная сеть, инфраструктура, пользовательские сервисы, профилирование устройств, точки доступа, коммутация, отказоустойчивость, триангуляция, аутенфикация, контроль доступа, информационная безопасность.*

ACM Classification Keywords: *H. Information Systems. H.1 Models and Principles. H.1.1 Systems and Information Theory. F.1.2 Models of Computation. 1.6.1 Simulation Theory.*

Введение

За последние несколько лет мобильные беспроводные устройства прочно проникли в жизнь современного человека [Палагин, 2006]. Границы рабочего места “размываются” и “мигрируют” в сторону мобильности офисной среды. Компьютерный парк на предприятиях и в организациях обновляется значительно реже по сравнению с личными (персональными) устройствами сотрудников, да и по удобству использования существенно им уступает. Массовое распространение смартфонов и планшетных компьютеров приводит к постепенному вытеснению стационарных компьютеров и ноутбуков с рабочих мест. В сложившихся условиях одна из наиболее актуальных задач в беспроводной корпоративной сети – реализация концепции использования собственных устройств (BYOD – Bring your own device). Ключевым элементом концепции является внедрение системы управления политиками и построение безопасной корпоративной беспроводной сети.

Требования к сети

В большинстве случаев вопрос развёртывания беспроводной сети решается установкой нескольких точек доступа и является как бы надстройкой над проводной инфраструктурой, управляемой отдельно [Богомолов, 2004]. Такой подход оправдывает себя в домашнем сегменте и является недостаточным для применения в корпоративном [Букин, 2007]. Требования к беспроводным сетям уже давно не ограничиваются только организацией интерфейса между беспроводным клиентским устройством и проводной инфраструктурой.

Современная корпоративная сеть должна иметь возможность передачи мультимедийных данных (данные, голос и видео), обеспечивать высокую производительность и безопасность, обладать хорошей масштабируемостью, простотой развертывания, управления и улучшенными эксплуатационными характеристиками, а также предоставлять дополнительный функционал по расширению спектра

пользовательских сервисов и их адаптации. Кроме того, при построении корпоративной беспроводной сети внедряемое решение должно обладать возможностями профилирования подключаемых устройств, выполнять процедуру гостевого доступа и иметь возможность отслеживать местоположение излучающих устройств [Лисецкий, 2008].

Построение беспроводной сети

В основу архитектуры беспроводной сети (рис. 1) положен принцип централизованного управления и расширения беспроводных сервисов [Бобров, 2004]. Основной функционал возлагается на контроллер беспроводной сети, а точки доступа работают в «облегченном режиме». Точки доступа обеспечивают радиоинтерфейс и шифрование пользовательских данных, передавая все пользовательские данные на контроллер в зашифрованном туннеле, а также предоставляют широкие функции по диагностике и отчетности.

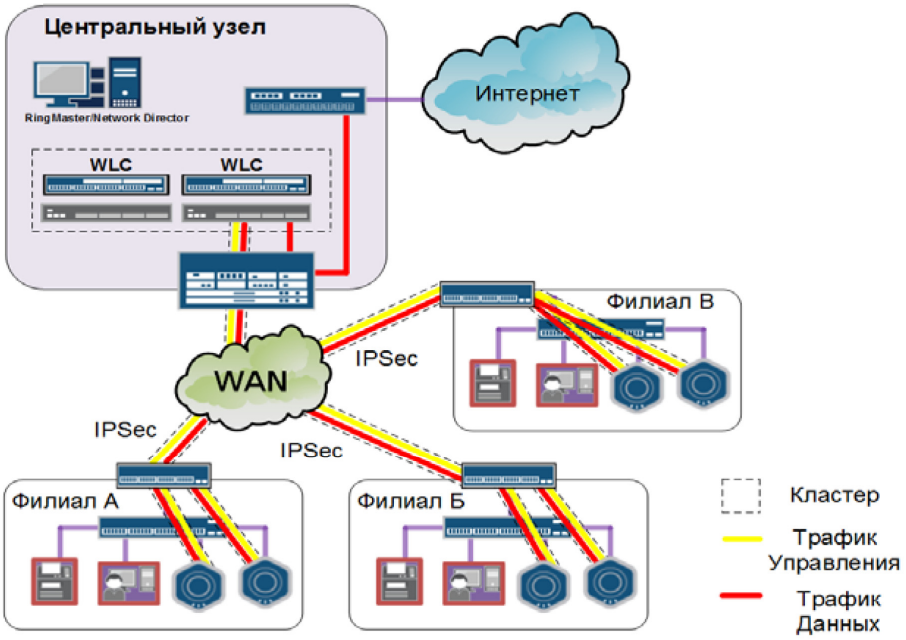

Рисунок 1. Архитектура беспроводной сети

Для организации радиопокрытия в решении присутствует широкая линейка точек доступа. Их можно условно разделены на три группы: системы начального уровня, корпоративного уровня и точки доступа во внешнем исполнении. Все предлагаемые производителем точки доступа поддерживают стандарт 802.11n и отличаются количеством радиомодулей, поддерживаемых потоков передачи данных и возможностью подключения внешней антенны. Предлагаемые устройства поддерживают три режима работы:

- точка доступа (обслуживание абонентов в режиме точка-многоточка);
- мост (реализация линии связи точка – точка);
- полносвязный режим (MESH-сеть, предусматривающая беспроводную линию связи между точками).

Применение универсальных устройств в соответствующих режимах работы делает возможным построение распределенной беспроводной сети под любые требования абонентов.

Традиционно применяются два типа архитектуры: размещение контроллера на центральном узле и в филиалах. При размещении контроллера на центральном узле применяется централизованная коммутация. При этом весь трафик проходит через контроллер, что ведет к значительной загрузке WAN-каналов. В представленных на рынке промышленных наборах программных и аппаратных средств для беспроводной сети точки доступа используют собственные приватные протоколы производителей оборудования, имеют возможность продолжать обрабатывать обращения пользователей и осуществлять взаимодействие с RADIUS-сервером в случае отказа WAN-канала. Несмотря на отсутствие перерыва в предоставлении сервиса, данные протоколы носят частный характер и предназначены для ограниченного числа удаленных офисов. Так, например, решение компании Juniper Networks свободно от данного недостатка и позволяет использовать локальную коммутацию. При этом через контроллер проходит только служебный трафик, а все данные коммутируются точкой доступа непосредственно на шлюз назначения. В системе реализована предпочтительная для предоставления мобильности модель оптимальной передачи пользовательского трафика при сохранении централизованного контроля и учета. Распределенная коммутация обеспечивает беспрецедентное качество беспроводного канала, реализуя минимальную в отрасли задержку передачи данных, что особенно важно для передачи «голосового» трафика.

Необходимость повышения отказоустойчивости сети вызвала отказ от идеи использования горячего резервирования и привела к кластеризации контроллеров. Объединение контроллеров в кластер позволяет существенно оптимизировать количество используемых лицензий на подключение точек доступа. Нет необходимости держать неиспользуемые лицензии на случай выхода из строя первичного контроллера. Основным отличием данного решения является возможность объединения в кластер любых типов контроллеров как разных аппаратных серий, так и виртуальных. Реализация общей программной платформы дает администраторам возможность проводить обновление программного обеспечения без перерыва в предоставлении сервисов.

Большинство современных беспроводных устройств поддерживает работу в двух диапазонах – 2,4 ГГц и 5 ГГц. Исторически диапазон 2,4 ГГц начал использоваться раньше и на данный момент значительно более загружен по сравнению с диапазоном 5 ГГц. Система беспроводной связи компании Juniper обеспечивает автоматическую балансировку клиентов между точками, а функция группирования клиентов осуществляет приоритетное подключение клиентских устройств в диапазон 5 ГГц, и только при невозможности присоединения происходит подключение в диапазоне 2,4 ГГц. Функционал балансирования и группирования абонентов обеспечивает оптимальное использование пропускной способности радиосети.

Для обеспечения максимальной пропускной способности данное решение позволяет обнаруживать, классифицировать и локализовать источники помех в режиме реального времени в обоих рабочих диапазонах. Вся информация по помехам консолидируется в системе управления Network director, предоставляя графический интерфейс для устранения неполадок.

С помощью системы управления Network director также осуществляется управление жизненным циклом беспроводной сети: планирование и развертывание, конфигурирование и отладка, мониторинг, отчетность и определение местоположения.

Отслеживание местоположения пользователей, реализация бесшовного перехода между точками доступа и обеспечение заданного качества обслуживания требуют более плотного размещения точек

доступа. Функции самовосстановления и качество работы сервисов обеспечиваются централизацией управления с помощью контроллера и зависят от правильного планирования беспроводной сети.

На начальном этапе разворачивания сети используется 3D-планировщик, который учитывает затухание радиосигнала в различных видах материалов, взаимное расположение точек доступа и предназначен для проведения расчетов как внутри помещения, так и на открытой местности. Данный этап очень важен для дальнейшей работы системы. В результате его выполнения осуществляется частотно-территориальное планирование беспроводной сети.

Основываясь на плане размещения точек доступа и используя метод триангуляции, система позволяет определять точное местоположение пользователя и осуществлять поиск специализированных RFID-меток.

Безопасность беспроводной сети

Применение радиолокации предоставляет возможность организовать периметр безопасности и предотвратить доступ в сеть за территорией предприятия (рис. 2). В этом случае, даже обладая действующими аутентификационными данными (логин/пароль), злоумышленник не сможет получить доступ к сети, находясь на прилегающей к офису территории.

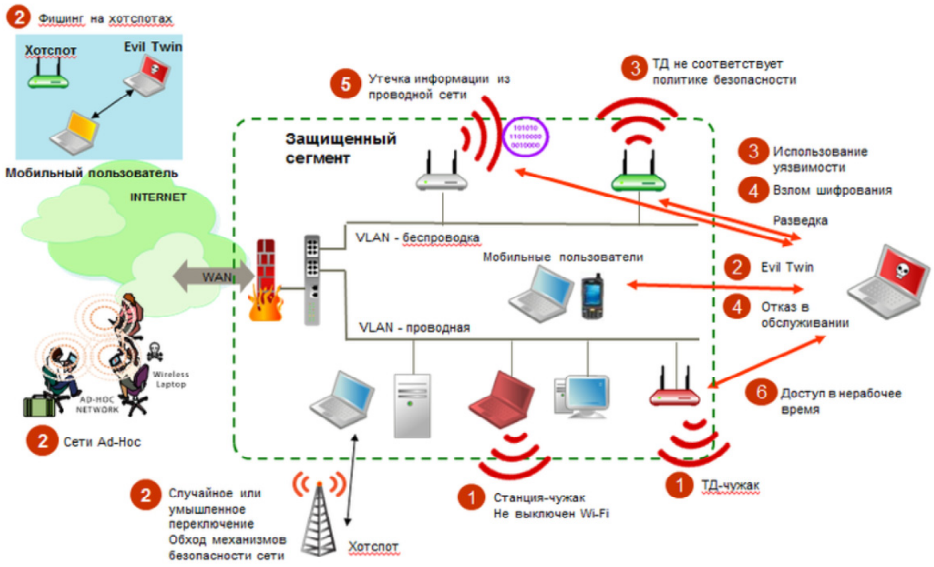

Рисунок 2. Организация безопасности беспроводной сети

Также этот функционал является интересным при выделении зон с запретом на использование беспроводного доступа, например, на территории процессингового центра или серверной, или же при отслеживании перемещений излучающего устройства по территории предприятия, предоставляя возможность поиска дорогостоящего мобильного оборудования, снабженного RFID-меткой, и осуществление контроля перемещений пользователей [Пастоев, 2006].

Повышение уровня безопасности сети осуществляется применением беспроводной системы предотвращения (обнаружения) вторжений (IPS/IDS). Система проводит внутренний анализ на наличие атак на беспроводную сеть и имеет возможность отправлять интересующий трафик на внешнюю систему

предотвращения вторжений. Возможность исторического анализа делает систему незаменимой при расследовании инцидентов.

В современной корпоративной беспроводной сети важно осуществлять динамический контроль доступа пользователей. Для этих целей служит приложение управления безопасностью SmartPass. Программное обеспечение интегрируется с системой управления Network director и системой отслеживания местоположения, обеспечивая контроль доступа на основе физического положения и возможность расширенных отчетов.

Платформа SmartPass Connect предназначена для реализации концепции использования собственных устройств. При необходимости обеспечения доступа к корпоративной сети затраты труда администраторов значительно возрастают, а при их значительных объемах могут требовать наличие в организационной структуре выделенных менеджеров. Платформа позволяет автоматизировать процедуру регистрации устройства и организацию доступа к сети с помощью корпоративных учетных данных. SmartPass интегрируется с контроллером домена и имплементирует на подключаемое устройство необходимые сертификаты. При этом система осуществляет профилирование устройства – определяется его тип, операционная система, ее версия, информация о приложениях клиента (совместно с SRX AppTrack и UAC) и т.д. Получаемая информация используется в корпоративных политиках и дает возможность предоставлять гранулированный доступ к сети.

Для доступа незарегистрированных пользователей на предприятиях необходимо внедрить процедуру гостевого доступа. SmartPass реализует полный жизненный цикл управления гостевым доступом (регистрация пользователя, уведомление о выделенных учетных данных, проведение аутентификации и авторизации, осуществление ограничения доступа, логирование событий безопасности и предоставление подробной отчетности).

Для каждого идентификатора беспроводной сети (SSID) может быть реализован адаптированный Web-портал с возможностью самообслуживания. После регистрации пользователь получает уведомление одним из трех возможных вариантов: учетные данные распечатываются на принтере, отправляются на электронную почту или отправляется СМС на указанный номер мобильного телефона. Гостевые сессии могут быть ограничены по длительности и времени использования, иметь разные политики доступа, но в то же время могут поддерживать мониторинг активных сессий, аккаунтинг, логирование и детальные отчеты. Решение поддерживает RFC 3576 предусматривающие изменение авторизации и динамическое изменение параметров во время сессии, включая качество обслуживания QoS, списки доступа ACLs, выделяемую пропускную способность и т.д.

Стандартизованный интерфейс программирования приложений API обеспечивает значительное расширение функционала беспроводной системы за счет интеграции с системами биллинга, различными платформами аналитики и отчетности.

Таким образом, решение компании Juniper Networks для построения беспроводной сети является одним из наиболее оптимальных по соотношению стоимости и доступности функционала. Предлагаемый набор промышленных программных и аппаратных средств позволяет создавать беспроводные системы корпоративного класса, обладающие высокой отказоустойчивостью и соответствующие всем требованиям по безопасности, производительности и масштабируемости.

Заключение

В настоящее время корпоративные беспроводные сети переживают период расцвета. Развитие бизнес-процессов переносит критически важные приложения в беспроводную среду, делая необходимым

реализацию интерактивных бизнес-приложений. Требования мобильности, повышения конкурентоспособности и производительности труда увеличивают требования к сервисам, предлагаемым в беспроводной сети. Описанный в данной статье подход позволяет построить универсальную корпоративную беспроводную сеть, основанную на стандартных протоколах, адаптированную под потребности практически любой организации и позволяющую оптимизировать стоимость владения беспроводным сегментом.

Литература

[Палагин, 2006] Палагин А.В., Алишов Н.И., Громовский А.В. Средства удаленного доступа на базе мобильной персональной системы // УСиМ. – 2006. – № 6. – С. 26 – 32, 51.

[Богомолов, 2004] Богомолов Ю. О беспроводных решениях // Экспресс-Электроника. – 2004. – № 12. – С. 33 – 40.

[Букин, 2007] Букин М. WiMAX на корпоративном рынке // PC WEEK/RE. – 2007. – № 20. – С. 24 – 27.

[Лисецкий, 2008] Лисецкий Ю.М., Бобров С.И. WiMax сети. Реализации и перспективы // Управляющие системы и машины. – 2008. – № 4. – С. 88 – 93.

[Бобров, 2004] Бобров С.И. Принципы проектирования корпоративных сетей // Материалы третьей научно-практической конференции «Информационные технологии в энергетике»: сб. науч. тр. – К.: НАН Украины, Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, 2004. – С. 34 – 37.

[Пастоев, 2006] Пастоев А., Петров Н. Безопасность беспроводных сетей // Директор информационной службы. – 2006. – № 4. – С. 17 – 19.

Информация об авторах

Лисецкий Юрий *- Киев, Институт проблем математических машин и систем НАН Украины, к.т.н., докторант. E-mail: Iurii.Lysetskyi@ snt.ua.*

Основные области научных исследований: проблемы принятия решений и управления в технических и экономических системах, математические методы, модели и технологии исследования сложных систем, информационные технологии поддержки принятия решений, проблемно и функционально-ориентированные компьютерные системы и сети.

Каревина Наталья *- Киев, Институт проблем математических машин и систем НАН Украины, к.и.н., н.с. E-mail: Natka_Kn@ukr.net.*

Основные области научных исследований: системы поддержки принятия решений в сложных системах, прогрессивные информационные технологии в социальных науках.

Building Peculiarities of the Modern Wireless Corporate Network

Iurii Lysetskyi, Natalia Karevina

Abstract: *Under consideration is the building of the modern wireless corporate network that implements the concept of using their own devices. Represented the requirements for the modern wireless networks of the enterprise-level, set out the principles of their building and architectural peculiarities. The questions of the organization of the information security in the wireless corporate networks are considered in the article.*

Keywords: *wireless network, infrastructure, user services, profiling devices, access point, commutation, fail-safe feature, triangulation survey, authentication, access audit, information security.*