Построение современной беспроводной корпоративной сети

ТЕКСТ: **Боцман Я.В., ДП «ЭС ЭНД ТИ УКРАИНА»**

Мобильные беспроводные устройства прочно вошли в жизнь современного человека. Границы рабочего места размываются и мигрируют в сторону повышения мобильности офисной среды. Основные средства в коммерческих компаниях обновляются значительно реже и по удобству использования редко соответствуют собственным устройствам сотрудников. Смартфоны и планшетные компьютеры постепенно вытесняют стационарные компьютеры и ноутбуки с рабочих столов.

В сложившихся условиях, самой актуальной задачей в корпоративной сети является реализация концепции «использования собственных устройств» (BYOD – Bring your own device). Ключевым элементом концепции является внедрение системы управления политиками и построение безопасной корпоративной беспроводной сети.

В большинстве случаев вопрос разворачивания беспроводной сети решается установкой нескольких точек доступа, и является как бы надстройкой над проводной инфраструктурой, управляемой отдельно. Такой подход оправдывает себя в домашнем сегменте и является недостаточным для применения в корпоративном сегменте.

Требования к беспроводным сетям 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 связность и безопасность, обладать высокой масштабируемостью, простотой развертывания, управления и улучшенными эксплуатационными характеристиками, а также предоставлять расширенный функционал по добавлению и кастомизации пользовательских сервисов. 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. Наиболее оптимальным по соотношению стоимости и доступного

функционала беспроводной системы является решение компании Juniper Networks. Оборудование позволяет осуществить построение системы корпоративного класса, обладающей высокой отказоустойчивостью и соответствующей всем требованиям по безопасности, производительности и масштабируемости.

В основу архитектуры решения (см. рисунок) положен принцип централизованного управления и расширения беспроводных сервисов. 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.

Для организации радиопокрытия в решении присутствует широкая линейка точек доступа. Их можно условно разделить 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) и 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 применяется 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 решениях точки доступа используют собственные приватные протоколы производителей оборудования и 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. 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, и особенно ценна 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 более экономно расходовать лицензии на подключение точек доступа. Нет необходимости держать неиспользованные лицензии на случай выхода из строя первичного контроллера. Ключевым 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.

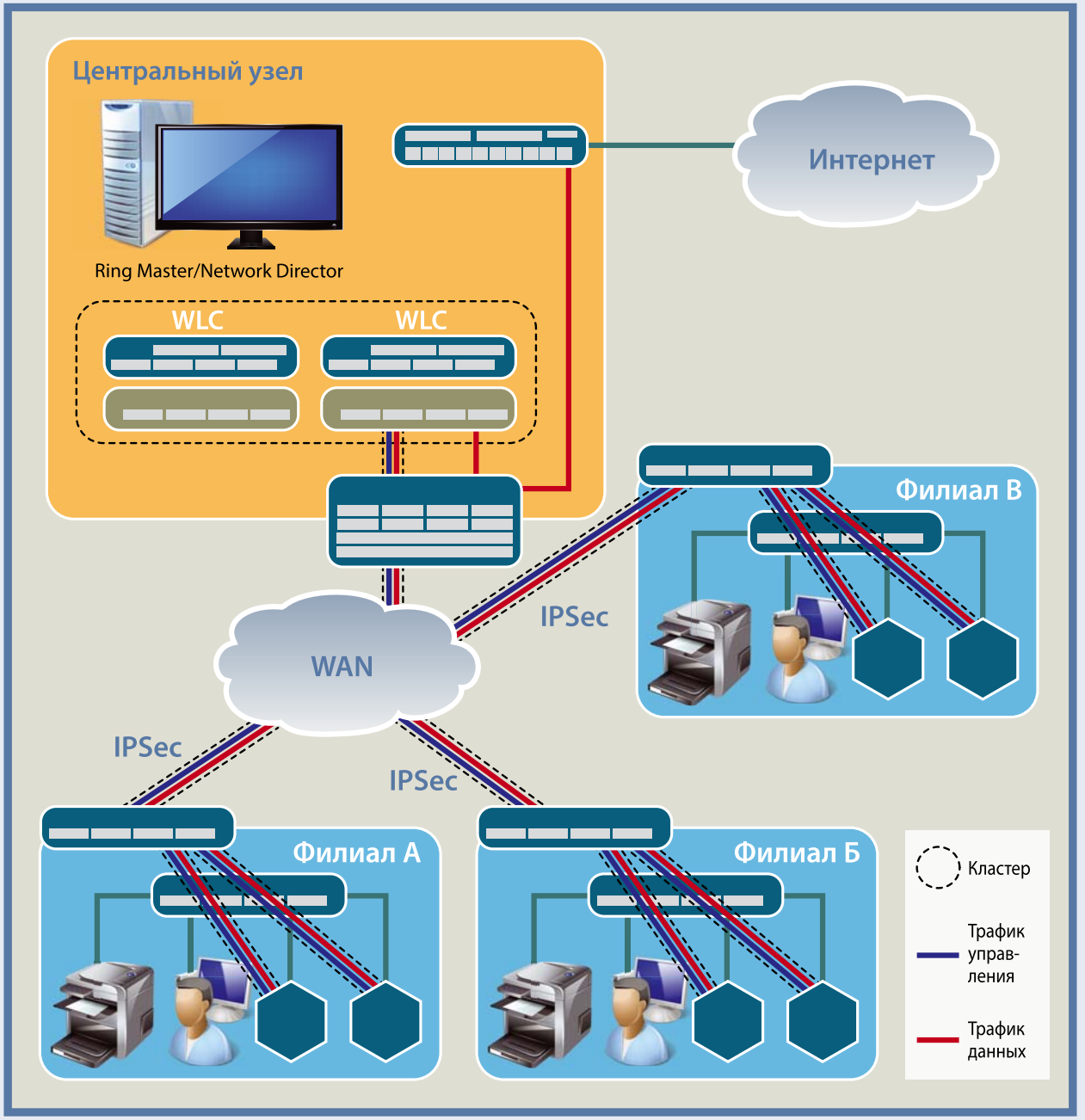
Большинство современных беспроводных устройств поддерживает работу в двух диапазонах – 2,4 ГГц и 5 ГГц. Исторически диапазон 2,4 ГГц начал использоваться раньше и на данный момент значительно более загружен, по сравнению с диапазоном 5 ГГц. Система беспроводной связи компании Juniper обеспечивает автоматическую 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 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 и отчетность, а также определение местоположения.

Отслеживание местоположения пользователей, реализация бесшовного перехода между точками доступа и обеспечение заданного ка-

Архитектура беспроводной сети



чества обслуживания требуют более плотного размещения точек доступа. Функции самовосстановления и качество работы сервисов обеспечивается централизацией управления с помощью контроллера и зависит от правильного планирования беспроводной сети.

На начальном этапе разворачивания сети используется 3D-планировщик, учитывающий затухание радиосигнала в различных видах материалов и взаимное расположение точек доступа и предназначенный для проведения рас-

четов как внутри помещения, так и на открытой местности. Данный этап очень важен для дальнейшей работы системы, и 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. Применение радиолокации предоставляет возможность реализовать периметр безопасности и предотвратить доступ в сеть за территорией предприятия. В этом случае, даже обладая действующими аутентификационными данными (логин/пароль), злоумышленник не сможет получить доступ к сети, находясь на прилегающей к офису территории. Также этот функционал небезынтересен при выделении зон с запретом на использование беспроводного доступа, например на территории процессингового центра или серверной, или отслеживании перемещений излучающего устройства по территории предприятия, предоставляя возможность поиска дорогостоящего мобильного оборудования, снабженного RFID меткой, и осуществление контроля перемещений пользователей.

Повышение 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. А 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 обеспечивая 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 приложения 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, уведомлении 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 кастомизированый 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, поддерживают 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.

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 и адаптированную под потребности практически любой организации, оптимизируя при этом стоимость владения беспроводным сегментом. СТ