

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ СЕТЕЙ Wi-Fi С ВЫСОКОЙ ПЛОТНОСТЬЮ ПОЛЬЗОВАТЕЛЕЙ

А. С. Викулов^{1*}, А. И. Парамонов¹

¹ СПбГУТ, Санкт-Петербург, 193232, Российская Федерация

* Адрес для переписки: asv012016@gmail.com

Аннотация

Планирование сетей стандарта IEEE 802.11 с высокой плотностью пользователей неотъемлемо связано с одной стороны с проектированием обеспечивающей инфраструктуры, а с другой с проработкой соответствующего применения функциональных возможностей точек доступа и контроллеров с целью построения решения, отвечающего поставленным требованиям. **Предмет исследования.** Статья посвящена функциональным особенностям БЛВС с высокой плотностью пользователей и их влиянию как на общую инфраструктуру ИТ, так и на процедуры внедрения. **Метод.** В основу данной работы положены руководства по проектированию БЛВС от компаний-производителей оборудования, рекомендации экспертов, ряд научных работ, а также более чем 5-летний личный опыт проектирования. **Основные результаты.** Рассмотрены ключевые функциональные особенности инфраструктуры, а также опции, предоставляемые производителями оборудования для планирования, развертывания и поддержки СВП. **Практическая значимость.** Проведенный анализ дает возможность сделать конкретные практические выводы и применить их при развертывании СВП.

Ключевые слова

IEEE 802.11, требования, инфраструктура, функциональность, Wi-Fi, высокая плотность пользователей.

Информация о статье

УДК 004.725.5

Язык статьи – русский.

Поступила в редакцию 23.05.18, принята к печати 01.07.18.

Ссылка для цитирования: Викулов А. С., Парамонов А. И. Функциональные особенности сетей Wi-Fi с высокой плотностью пользователей // Информационные технологии и телекоммуникации. 2018. Том 6. № 2. С. 49–61.

SPECIAL FEATURES OF HIGH DENSITY Wi-Fi NETWORKS

A. Vikulov^{1*}, A. Paramonov¹

¹ SPbSUT, St. Petersburg, 193232, Russian Federation

* Corresponding author: asv012016@gmail.com

Abstract—The high density wireless networks planning is closely connected to the IT infrastructure design as well as access point and wireless LAN controllers functionality choice in order to meet the solution requirements. **Research subject.** The present work is devoted to special features analysis of the high density Wi-Fi networks with attention to the implementation process of the WLAN. **Method.** The ground for this work is: Wi-Fi solution vendors design guides, recommendations of the experts, some scientific works and own more than 5-year design practice. **Core results.** The key special features of the IT infrastructure has been analyzed as well as several options provided by the solution vendors in order to plan, implement and support different high density WLANs. **Practical relevance.** The analysis gives practical recommendations for high density WLANs implementation.

Keywords—IEEE 802.11, requirements, functionality, high density, WLAN, Wi-Fi.

Article info

Article in Russian.

Received 23.05.18, accepted 01.07.18.

For citation: Vikulov A., Paramonov A.: Special Features of High Density Wi-Fi Networks // Telecom IT. 2018. Vol. 6. Iss. 2. pp. 49–61 (in Russian).

Введение

При работе с сетями Wi-Fi высокой плотности, важно обратить внимание на соответствующее планирование сети – соответствие имеющегося и планируемого к внедрению оборудования, как с позиций производительности, так и с позиций функциональности. Только путем всестороннего и полного сбора исходных данных, планирования сети, конфигурирования и эксплуатационной оптимизации, может быть успешно развернута сеть Wi-Fi, отвечающая задачам высокоплотной среды.

В процессе сбора требований, следует формализовать цели сетевого планирования таким образом, чтоб сеть отвечая бизнес-задачам, соответствовала имеющимся требованиям производительности и качества обслуживания. Соответствующее планирование требует понимания возможностей поддерживаемых клиентских устройств, достижимых плотностей размещения клиентов в каждой зоне радиопокрытия, развертываемых в сети сервисов и требований к сетевой инфраструктуре, как с позиции сетевых сервисов, так и с точки зрения оборудования Wi-Fi.

Проведение цикла радиообследований для сбора информации об объекте, равно как и для проверки принятых проектных решений, также является важнейшим фактором в проектировании сетей стандарта IEEE 802.11 с высокой плотностью пользователей (СВП).

Планирование СВП в части требуемой функциональности включает в себя следующие основные этапы:

- Определение возможностей клиентского устройства и требований сетевых сервисов.
 - Определение необходимой пользовательской емкости радиоканала.
 - Определение типа требуемых точек доступа и необходимых опций (антенн, например) и мест их размещения.
 - Определение требований к сетевой инфраструктуре.
- Далее рассмотрим эти вопросы подробнее.

Возможности клиентских устройств

Важнейшим вопросом для планирования сети высокой плотности является количество каналов для каждого диапазона, требуемое для соответствия проектному числу пользователей. Ответ может быть неочевидным, поскольку даже те клиенты, которые формально поддерживают работу в двух диапазонах, не всегда на практике предпочитают работу в диапазоне 5 ГГц. Почти все современные ноутбуки и смартфоны оснащены двухдиапазонными Wi-Fi адаптерами. Это, однако, не означает, что каждый ноутбук или смартфон является двухдиапазонным клиентом. Из этого также не следует, что клиентом будет отдано предпочтение 5 ГГц диапазону несмотря на тот факт, что большинство современных операционных систем сканируют в первую очередь именно 5 ГГц диапазон в поисках точки доступа. Плюс не каждое клиентское устройство поддерживает MIMO – подобный функционал все еще остается прерогативой наиболее дорогих устройств, в то время как большинство устройств работают в режиме SISO.

Одно из основных требований любой СВП – управление мощностью передачи в условиях перемещающихся в пространстве клиентов. Число клиентских устройств значительно превосходит совокупное число радиомодулей точек доступа, поэтому они являются серьезным источником внутри- и межканальных помех (CCI/ACI). Значение протокола 802.11h и протокола управления мощностью передачи (TPC) здесь имеют ощутимое значение, но они полностью зависят от драйвера радиомодуля клиентского устройства. Поэтому крайне желательна полноценная поддержка клиентскими устройствами этих протоколов.

В высокоплотной среде обычно имеет место разнородная и плохо управляемая смесь самых разных типов клиентов. За исключением случаев централизованного внедрения систем управления мобильными устройствами (*Mobile Device Management* – MDM), или различных вариантов систем внутренней идентификации устройства (*Identity Services*), в типовых задачах гостевого доступа клиентские устройства не контролируются эксплуатантом сети, поэтому они не всегда имеют все последние обновления драйверов и ПО. В сети могут быть устройства 802.11a, 802.11b, 802.11g, 802.11n и 802.11ac протоколов. Многие современные клиентские устройства часто уходят в «спящий режим», при «пробуждении» устанавливая Wi-Fi соединение заново, что создает дополнительную нагрузку на сеть служебными кадрами (*control-traffic*).

В первую очередь необходимо уточнить предполагаемый спектр клиентских устройств, использование которых предполагается в развертываемой инфраструктуре. Ввиду того, что радиомодули клиентов и точек доступа исполь-

зуют одну и ту же общую среду передачи сигнала, конфигурация сети должна в известной мере балансировать доступ к сети между всеми клиентами. Такими характеристиками радиомодулей являются:

- Версия стандарта 802.11.
- Предпочтительный частотный диапазон работы.
- Число пространственных потоков (SS) 802.11n/802.11ac (если SS используется).
- Максимальные скорости установки соединения (*data rate*).

Последнее особенно важно ввиду того, что более высокие номинальные скорости передачи данных автоматически обозначают меньшее время, требуемое для передачи того же объема данных.

Плюс ко всему в оценке плотности клиентов, необходимо учесть фактор типа клиентов. Руководства производителей содержат в целом близкие рекомендации на предмет реально достижимых различными типами клиентских устройств значений пропускной способности. Подобные рекомендации содержат, в частности, документы^{1,2} [1].

СВП, поддерживающая максимальную пропускную способность для максимального числа клиентов должна иметь проассоциированными только самые новейшие клиентские устройства, работающие на самых последних драйверах. Как только в сети появляются клиентские устройства с разными конфигурациями MIMO, с разными версиями стандарта 802.11, совокупная пропускная способность сети начнет заметно падать.

Соотношения между типами клиентских устройств в реальной сети исследовались, в частности в работах [2, 3, 4, 5], где показано, что даже в корпоративных сетях, где особую роль имеет централизованное управление устройствами, велико разнообразие устройств.

Даже при относительно низкой клиентской плотности, смена пары активных 802.11ac устройств на более старые значительно влияет на общую скорость работы сети, по сравнению с сетью, построенной целиком на 802.11ac устройствах. Некоторые подходы, например, ATF (*Air Time Fairness*) помогают снизить эффекты такого поведения, но не в силах полностью решить данной проблемы, поскольку клиенты, которые могут передавать только на низких скоростях будут занимать большой временной ресурс, который мог бы быть использован более скоростными устройствами. Наличие в сети старых устройств означает, что сеть будет:

- Использовать механизм защиты передачи 802.11 (RTS/CTS).
- Передавать кадры broadcast, multicast и управления 802.11 на сниженных скоростях.
- Клиенты 802.11n/ac будут вынуждены занимать меньший временной ресурс канала.

При этом важно не забывать, что, например, не все клиенты, номинально поддерживающие стандарт 802.11n, фактически могут работать с номинальными скоростями передачи в 300–450 Мбит/с. Стремясь получить приемлемое ав-

¹ Meru Networks Best Practices Guide for High-Density Design and Deployment. 2012.

² Aruba VHD 802.11ac Networks VRD. Theory Guide v1. Chuck Lukaszewski. 2015.

тономное время работы, производители порой, с целью энергосбережения, ограничивают номинальные скорости величинами порядка 65 Мбит/с³.

Требования сетевых приложений

После определения возможностей клиентских устройств, необходимо определить сетевые приложения и их требования к производительности (скорость и QoS) в расчете на клиентское устройство. Понимание требований сетевого приложения даст необходимую информацию для проектирования отвечающей поставленным задачам сети. При этом возможно выделение нескольких приложений (как критичных для работы, так и нет) используемых на каждом устройстве, что позволит корректнее определить целевую пропускную способность в расчете на устройство.

В сетях СВП в сценарии гостевого доступа пользовательский трафик обладает большим разнообразием. Наиболее распространены приложения, представляющие собой HTTP/HTTPS, e-mail, передача видео и разнообразные сервисы совместной работы. Кроме потокового видео, все эти сетевые сервисы имеют «взрывной» характер нагрузки и требуют одновременной работы всех клиентов сети.

Далее необходимо формализовать требования к пропускной способности с позиции развернутых в сети сервисов (клиентских приложений) в расчете на каждое клиентское устройство. Ввиду разнообразных сетевых накладных расходов на полосу пропускания, номинальная скорость установки соединения не соответствует реальному пиковому максимуму скорости передачи прикладных данных. Для получения точного значения объема издержек необходимо провести измерения в реальной сети. В среднем же непроизводительные затраты пропускной способности составляют 40–60 %⁴.

В работах Aerohive⁵, Aruba High Density Wireless networks for Auditoriums⁶, [1] приведены типовые рекомендации относительно типов сетевых приложений согласно Aerohive Networks, Cisco Systems, Aruba Networks.

Во всех случаях настоятельно рекомендуется протестировать целевое приложение для определения реально создаваемой сетевой нагрузки. Разработчики ПО часто берут среднюю величину пропускной способности для оценки производительности приложением нагрузки на сеть, хотя часто существует множество режимов и нюансов внедрения, от которых зависит точное значение. В дополнение, не все устройства, операционные системы и браузеры удовлетворятся одной и той же имеющей пропускной способностью.

Размер блока данных приложения также имеет немаловажное значение. Так объем служебной информации в расчете на кадр является примерно постоянным, в то время как собственно размер кадра может сильно меняться. В таком контексте номинальные требования двух приложений к скорости могут быть идентичны, в то время как используемый средний размер кадра данных может значительно повлиять на это соотношение, не будучи в явном виде задекларирован. Эффективность использования сети «чатообразными» протоколами

³ Motorola High Density Design with WiNG 5. Motorola Solutions. 2013.

⁴ Aerohive. High Density Wi-Fi Design Principles. 2012.

⁵ Там же.

⁶ Aruba High Density Wireless networks for Auditoriums. VRD. 2010.

в среднем всегда ниже по сравнению с протоколами, передающими данные сплошным потоком (например, мультимедийный трафик). Под «чатообразными» протоколами подразумеваются протоколы, посылающие сообщения небольшого размера с большой частотой. Небольшие пакеты дают самое неэффективное использование временного ресурса, поэтому их использование должно быть минимизировано где это возможно, либо прямо запрещено. К таким протоколам в числе прочих относятся: netbios-ns, netbios-dgm, Bonjour, mDNS, UPnP, SSDP и IPv6, если последний прямо не задействован⁷.

В работе [3], среди прочих параметров БЛВС исследовалось распределение среднего размера кадра в пользовательском трафике, из которого видно, что в практических примерах трафик чаще всего имеет бимодальное распределение с двумя модами, составляющими порядка 300 и 800 Байт. Иными словами, в сети сосуществуют несколько приложений с различными размерами среднего кадра, соответственно веб-доступ и мультимедиа.

В работе Aruba High Density Wireless networks for Auditoriums показано, что кадры с полезными данными составляют лишь 24 % от общего числа кадров, т. е. нельзя забывать, что высокая занятость временного ресурса радиоканала сама по себе не обозначает высокую его загруженность полезным трафиком.

Рабочий цикл клиентского устройства (*Client Duty Cycle*)

До сих пор рассматривался сценарий, в котором все клиенты ячейки «состязаются» за доступ к среде одновременно. В этом случае все пользователи одновременно пытаются получить доступ к одному ресурсу, выстраиваясь в очередь. Однако, в большом числе случаев проектным требованием является эпизодический доступ к сетевым ресурсам во время какого-то события. Планирование и масштабирование такого типа событий будет достаточно разнообразно и будет сильно зависеть от рабочего цикла клиентского устройства.

Например, на стадионе определенные участки зоны покрытия будут требовать постоянного доступа в течение всего времени. Зоны кассового обслуживания, служебные помещения, помещения для прессы обычно требуют максимального качества доступа. Среди них только зона работы прессы будет требовать именно высокой плотности. Среди зрителей мероприятия только некоторый процент устройств будет ассоциирован с сетью. По мнению и опыту большинства производителей эта величина лежит в пределах 20–30 %^{8, 9, 10, 11}, с выраженными максимумами во время перерывов в проводимых мероприятиях, например, футбольных матчах. Согласно требованию технических регламентов большинства организаторов, процент же одновременно активных устройств обычно принимается в пределах 15–20 %. Во время самого мероприятия очень небольшое количество зрителей пользуется сетью. Однако последнее утверждение уже довольно спорно, поскольку для пользователя становятся доступны разнообразные онлайн-сервисы, такие, например, как видеоповтор.

⁷ Aruba High Density Wireless networks for Auditoriums. VRD. 2010.

⁸ Meru Networks Best Practices Guide for High-Density Design and Deployment. 2012.

⁹ Motorola High Density Design with WiNG 5. Motorola Solutions. 2013.

¹⁰ Aerohive. High Density Wi-Fi Design Principles. 2012.

¹¹ Aruba High Density Wireless networks for Auditoriums. VRD. 2010.

Вообще говоря, перечислить все возможные сервисы, которые могут быть предоставлены, например зрителю стадиона посредством его мобильного устройства, крайне затруднительно. Помимо названных, это могут быть и рекламные сообщения, и баннеры, синхронизированные с постами цифровых вывесок (*digital signage*), и разнообразные информационные сервисы, помогающие ориентироваться в большом незнакомом комплексе, и многое другое. Поэтому перед проектированием сети 802.11, крайне желательно определить не только планируемые сервисы, но и примерный перечень предполагаемых задач, которые могут потребовать решение специфических подходов по интеграции.

Например, ситуация, в которой 500 пользователей находятся в одном помещении с необходимостью одновременного доступа к одному ресурсу и ситуация с 1 500 пользователей, которые эпизодически используют Wi-Fi сеть – это определенно разные цели планирования. Помимо этого, шаблоны работы пользователей меняются со временем. Например, растет число клиентских устройств в расчете на пользователя. Мониторинг, статистика и отчетность о сетевой активности – ключ к пониманию этого фактора [1].

Технические требования к проводной ЛВС и сетевой инфраструктуре

Перечисленные выше сложности с разнообразием клиентских устройств и протоколов, осложненные высокой плотностью их размещения выдвигает ряд требований к проводной инфраструктуре. Некоторыми из них являются:

- Порты доступа 1000BaseT с поддержкой 802.3af или (чаще всего) 802.3at. В СВП стандарта 802.11ac возможны скорости передачи, достигающие 200–300 Мбит/с, что делает гигабитные порты доступа обязательным условием.

- Необходимо помнить, что номинально скорости передачи WLAN уже превысили 1 Гбит/с, что заставляет думать о соответствующей поддержке на стороне проводной инфраструктуры. Вместе с тем нужно понимать, что в отличие от БЛВС невысокой плотности, для точек доступа (ТД) в СВП в обозримом будущем маловероятно, что пиковые пропускные способности превысят 1 Гбит/с.

- Современные ТД поддерживают резервированное подключение к портам коммутатора доступа, и потому хорошей практикой является подключение ТД агрегированным каналом к паре коммутаторов.

- Порты 10 Гбит/с на восходящих каналах коммутаторов доступа в сторону уровня распределения/ядра. По перечисленной выше причине, совокупная скорость работы клиентов растет, и пропускная способность восходящих каналов должна отвечать этим требованиям.

- Одновременный вход в сеть. RADIUS или любой другой метод аутентификации должен выдерживать массовый вход в сеть пользователей за короткий промежуток времени. Для сети Wi-Fi развернутой на большой площади с большим количеством клиентов – это типовой сценарий работы.

- Адресное пространство третьего уровня должно быть спроектировано исходя из адекватной оценки числа ассоциированных устройств.

- DHCP сервис для нужд сети высокой плотности также должен поддерживать работу в условиях серьезных пиковых нагрузок. Время жизни адреса

при этом должно быть оптимизировано исходя из планируемого сценария работы пользователей.

Функциональность беспроводной инфраструктуры

Высокоплотные сети Wi-Fi обычно предполагают наличие специфических функциональных возможностей беспроводной инфраструктуры, которые не всегда оказываются востребованы в традиционных сетях Wi-Fi. Перечислим основные из этих функций.

- **Динамическое управление радиоресурсами.** Для минимизации нагрузки на IT службу и наличия возможности адаптироваться к меняющимся радиочастотным условиям, возможность динамического выбора канала и уровня мощности в современных реалиях можно считать обязательным условием. Такими же обязательными являются механизмы распределения клиентов для равномерного размещения клиентов по имеющимся каналам. Последнее в большей степени касается 5 ГГц радиомодулей. Избыточные в некоторых схемах радиомодули диапазона 2,4 ГГц во избежание высокой интерференции могут быть либо отключены, либо использованы для мониторинга среды различными средствами. Как один из вариантов, в диапазоне 2,4 ГГц может использоваться статическая схема использования каналов, с предпочтением динамической в диапазоне 5 ГГц.

- **«Честность» доступа к сети (ATF).** Для сети с большим числом разнообразных (в том числе и устаревших) клиентских устройств под этим термином понимается возможность их работы без заметного ущерба клиентам с современными версиями стандарта. Явление по своей сути связано с тем, что клиенту сети 802.11a/b/g требуется большее время для передачи того же объема информации, чем клиенту с новыми версиями стандарта. Реализация подобных алгоритмов учитывает типы трафика, активность клиентов, объем трафика в расчете на клиента для всех соединений. Это позволяет всем клиентам иметь приемлемую скорость работы, даже при наличии большого числа клиентов со старыми и медленными реализациями стандарта. Клиент стандарта 802.11n, поддерживающий работу с тремя пространственными потоками, может посылать большие объемы трафика в пределах выделенного времени, чем клиент с одним потоком. Однако оба клиента получают один и тот же по продолжительности временной ресурс. Этого можно избежать, если контроллер БЛВС поддерживает использование динамических методов выделения канального ресурса клиентам, что даст возможность более скоростной работы для «быстрых» клиентов без отрицательного эффекта на «медленных».

- **Пулы виртуальных локальных сетей (VLAN Pooling).** В крупномасштабных СВП необходимо иметь достаточное адресное пространство для всех клиентских устройств, включая резерв на пиковые нагрузки. В то же самое время ограничение размера широковеб-адресного домена является обязательным условием любой LAN. Например, различные реализации этого подхода от разных производителей предоставляют возможность построить множество сетей /24 для одной сети Wi-Fi любого размера с возможной балансировкой пользователей между ними.

- **Dynamic Multicast Optimization (DMO).** Динамическая оптимизация мультикаст-пакетов повышает качество мультикастовых передач в БЛВС.

При небольшом числе клиентов, мультикаст передается как уникаст, с соответствующим механизмом подтверждения получения и повышенной надежности передачи. При росте числа клиентов, делающем такую конверсию неэффективной, передачи снова ведутся в мультикасте. Данный вопрос рассматривался, в том числе в работе [6].

- IGMP Snooping. Данный, широко применяющийся в проводной инфраструктуре протокол, отвечает за то, что мультикаст трафик передается по проводной инфраструктуре только до тех ТД, с которыми ассоциированы подписчики.

- Multicast-Rate-Optimization (MRO). Согласно требованию стандарта 802.11 мультикаст потоки при передаче по БЛВС должны передаваться на минимально поддерживаемой скорости, чтобы все клиенты могли их декодировать. MRO отслеживает все поддерживаемые клиентами скорости и использует максимально возможную скорость для мультикаст-передач.

- Quality of Service (QoS). Если в высокоплотной сети Wi-Fi передается голос или видео, то крайне важно, чтобы QoS (WMM, или IEEE 802.11e) был внедрен и настроен как на проводной, так и беспроводной части сети, между ТД и на уровне распределения. Использование WMM, являющееся обязательным для задействования скоростей 802.11n/ac, позволяет применять приоритезацию трафика на канальном уровне и методы агрегирования кадров, что заметно увеличивает пропускную способность сети для клиента, снижает занятость канала и увеличивает общую сетевую емкость.

- Подстройка чувствительности приема. Может быть использована для ТД с целью запрета ассоциации клиентов, чей уровень сигнала меньше определенного порога для покрываемой зоны. Это позволяет повысить устойчивость сети в случае внешних помех или попыток ассоциации со стороны клиентов, чей сигнал слаб, что в итоге не позволит совокупной пропускной способности ячейки упасть ниже установленного критерия. Однако, ввиду высоких погрешностей измерения уровня сигнала точками доступа, данной опцией следует пользоваться с большой осторожностью.

Ограничения режимов модуляции и кодирования

Сети высокой плотности требуют, чтобы клиенты передавали данные на максимально возможных скоростях. Более высокие скорости, помимо очевидных преимуществ для клиента, уменьшают время, требуемое каждому клиенту для передачи данных и увеличивают общую сетевую емкость. Отключение низких скоростей ограничивает клиентские устройства возможностью работы только на высоких скоростях модуляции и кодирования, стимулирует хендовер клиентов между ТД и уменьшает число устройств, «прилипших» к одной точке доступа. Под «прилипшими» устройствами понимаются клиенты, по какой-то причине не осуществляющие хендовер в процессе своего перемещения по зоне покрытия и продолжающие работать через далеко расположенную ТД, доступную со слабым уровнем сигнала и, как следствие, на минимальной скорости. Уменьшение числа доступных номиналов скоростей также уменьшает число смен скоростных режимов клиентами, что в свою очередь снижает объем служебного трафика в сети.

В руководствах производителей оборудования, например Aerohive¹², рекомендуется целиком отключать номиналы стандарта 802.11b ввиду использования ими старой модуляции DSSS и HR/DSSS, при использовании которой сильно загружается временной ресурс радиоканала по сравнению с более современной OFDM модуляцией. Помимо этого, устаревшие виды модуляции сигнала, требуют применение механизмов защиты, таких как RTS/CTS и CTS-to-Self, которые сами по себе вносят до 40 % избыточной нагрузки на сеть. Следовательно, отключая номиналы скоростей 1, 2, 5.5 и 11 Мбит/с, мы увеличим общую сетевую емкость, снижая нагрузку на каналный ресурс от каждого клиента. Однако, если поддержка клиентов 802.11b необходима, то нужно оставить хотя бы один номинал доступным для работы.

Чтобы удостовериться, что клиенты используют высокие скорости, необходимо детально настроить поддержку для диапазонов 2,4 и 5 ГГц. В высокоплотных сетях необходимо настроить приемлемо минимальную скорость – например 18 Мбит/с и отключить низкие номиналы. Это заставит клиентов активно выбирать точки доступа с более высоким уровнем сигнала и поддерживать работу в высокоскоростных режимах¹³.

Если актуальны проблемы совместимости клиентов, рекомендуется установить скорости 6, 12 и 24 Мбит/с как базовые (это, фактически, – требование); установить скорости 24, 48 и 54 Мбит/с как опциональные; и отключить все прочие номиналы. Если же требуется поддержка клиентов 802.11b, то необходимо установить 11 Мбит/с как единственную базовую скорость, а номиналы 18, 24, 36, 48 и 54 Мбит/с установить, как опциональные, отключив все прочие. Необходимо помнить, что некоторые виды устройств могут вести себя непредсказуемо, в случае недоступности скорости в 24 Мбит/с¹⁴.

Ввиду того, что преамбула всегда передается в режиме BPSK, т. е. на скорости 6 Мбит/с, размер домена коллизий от выбранных номиналов скоростей передачи не зависит, поэтому расстояние от ТД, на котором будут заметны эффекты интерференции нельзя уменьшить, запрещая подключение к сети на низких скоростях¹⁵.

Для использования номинальных скоростей стандарта 802.11n необходимо использовать WPA2-CCMP/AES или Open security. Следует избегать применения WEP или TKIP, что ограничит работу клиентов только скоростями 802.11a/b/g. Необходимо помнить, что в стандарте 802.11ac этих методов аутентификации больше нет. На сегодняшний день необходимо применять один из следующих способов обеспечения безопасности:

- WPA2 802.1X (*Enterprise*),
- WPA2 PSK (*Personal*),
- Private PSK (PPSK),
- Open Security.

¹² Aerohive. High Density Wi-Fi Design Principles. 2012.

¹³ Там же.

¹⁴ Motorola High Density Design with WiNG 5. Motorola Solutions. 2013.

¹⁵ Aruba VHD 802.11ac Networks VRD. Theory Guide v1. Chuck Lukaszewski. 2015.

Управление диапазонами (*Band Steering*)

При проектировании сетей, работающих в двух диапазонах, полезно будет стимулировать клиентов подключаться к точкам в диапазоне 5 ГГц, если они его поддерживают. Это обычно улучшает скорость их работы, особенно, если речь идет о клиентах 802.11n, которые таким образом уходят с каналов, где они делят каналный ресурс с клиентами старых стандартов.

Этот подход также улучшает производительность сети для клиентов диапазона 2,4 ГГц, снижая число клиентов в этих каналах и активность борьбы за каналный ресурс. Указанные механизмы работают при радиопланировании, исходящем в первую очередь из покрытия в диапазоне 5 ГГц, что является де-факто требованием.

Управление диапазонами (*band steering*) позволяет более широко использовать диапазон 5 ГГц, снижая внутриканальную интерференцию и улучшая повторное использование каналов. Несмотря на то, что с точки зрения стандарта, только клиентское устройство определяет рабочий диапазон, различные производители по разному алгоритмически разрешают эту задачу, но суть у всех примерно одна – распределять клиентские устройства по диапазонам, не просто форсируя работу клиента в 5 ГГц диапазоне, если он поддерживает таковую, и равномерно распределяя клиентов между диапазонами, а дополнительно учитывая многие другие факторы такие как – доступные скорости, требуемая производительность, статистика ошибок и др.

Балансировка нагрузки

Для оптимизации клиентских ассоциаций с группой точек доступа может использоваться балансировка нагрузки. Это полезно, когда ТД оказываются перегружены трафиком. Точки доступа обмениваются с контроллером информацией о клиентской нагрузке, объеме ошибок CRC, условиях интерференции в окружающей среде и строят базу радиочастотных условий в сети. Основываясь на этих данных, контроллер может избирательно отвечать через ТД на запросы probe и association от новых клиентов таким образом, чтобы они устанавливали связь с теми ТД, у которых имеются наиболее благоприятные возможности с точки зрения установления ассоциации с дополнительным клиентом. Балансировку нагрузки с позиций занятости временного каналного ресурса определяет радиомодуль, основываясь на объеме трафика и нагрузке на канал, предоставляя лучшую индикацию доступности сетевой емкости, чем балансировка нагрузки, основанная на числе ассоциированных клиентов. Использование числа клиентов как критерия для балансировки нагрузки крайне нежелательно, поскольку на практике велика вероятность ситуации, когда с точкой ассоциировано много неактивных клиентов.

Нередки случаи, когда «узким местом» становится именно контроллер (в той или иной его архитектурной реализации), который не справляется с пиковыми нагрузками. Таким образом, даже грамотно рассчитанная радиочастотная часть проекта сети 802.11 не является гарантом высокого конечного качества инфраструктуры в целом, если по каким-то причинам были недооценены пиковые нагрузки. В последнее время реализации БЛВС, в которых весь

пользовательский трафик идет через контроллер, постепенно уходят в прошлое. Тем не менее, необходимо помнить про те ограничения, которые имеет контроллер Wi-Fi в случае применения подобной архитектуры.

Выводы

1) В работе рассмотрены вопросы функциональных требований сетей с высокой плотностью пользователей по отношению к внешней инфраструктуре.

2) Показана важность учета возможностей клиентских устройств и клиентского состава БЛВС для планирования СВП.

3) Рассмотрены ключевые опции технологии беспроводного доступа, предоставляемые производителями оборудования, являющиеся ключевыми для планирования, развертывания и поддержки СВП.

4) Проведено обобщение конкретных рекомендаций относительно выбора номинальных скоростей передачи (MCS) в свете решения задач построения СВП.

5) Проведен анализ возможностей СВП для балансировки клиентов как между диапазонами (радиомодулями), так и между точками доступа БЛВС.

Литература

1. Florwick J., Whiteaker J., Amrod A. C., Woodhams J. *Wireless LAN Design Guide for High Density Environments in Higher Education*. Cisco Systems. 2017.

2. Викулов А. С., Парамонов А. И. Исследование клиентского состава в сети беспроводного доступа // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методической конференция. 2017. Т. 2. С. 136–139.

3. Paramonov A., Vikulov A., Scherbakov S. Practical Results of WLAN Traffic Analysis // *Lecture Notes in Computer Science*. 2017. Vol. 10531. PP. 721–733.

4. Викулов А. С., Парамонов А. И. Анализ трафика в сети беспроводного доступа стандарта IEEE 802.11 // Труды учебных заведений связи. 2017. Т. 3. № 3. С. 21–27.

5. Викулов А. С., Парамонов А. И. Анализ эффективности использования канала сети беспроводного доступа стандарта IEEE 802.11 по результатам наблюдений // 3-я Международная научно-техническая конференция студентов, аспирантов и молодых ученых «Интернет Вещей и 5G». 2017. С. 68–73.

6. Makolkina M., Vikulov A., Paramonov A. The Augmented Reality Service Provision in D2D Network // *Communications in Computer and Information Science*. 2017. Vol. 700. PP. 281–290.

References

1. Florwick J., Whiteaker J., Amrod A. C., Woodhams J. *Wireless LAN Design Guide for High Density Environments in Higher Education*. Cisco Systems. 2017.

2. Vikulov A., Paramonov A. WLAN Client Diversity Analysis // 6th International Conference on Advanced Infotelecommunication (ICAIT). 2017. Vol. 2. pp. 136–139.

3. Paramonov A., Vikulov A., Scherbakov S. Practical Results of WLAN Traffic Analysis // *Lecture Notes in Computer Science*. 2017. Vol. 10531. pp. 721–733.

4. Vikulov A., Paramonov A. IEEE 802.11 WLAN Traffic Analysis // *Proceedings of Telecommunication Universities*. 2017. Vol. 3. Iss. 3. pp. 21–27.

5. Vikulov A., Paramonov A. IEEE 802.11 WLAN Channel use Efficiency Analysis Based on Monitoring Results // III International Conference on the Internet of Things and Its Enablers "IoT and 5G". 2017. pp. 68–73.

6. Makolkina M., Vikulov A., Paramonov A. The Augmented Reality Service Provision in D2D Network // *Communications in Computer and Information Science*. 2017. Vol. 700. pp. 281–290.

Викулов Антон Сергеевич

– аспирант, СПбГУТ, Санкт-Петербург, 193232,
Российская Федерация, asv012016@gmail.com

Парамонов Александр Иванович

– доктор технических наук, профессор, СПбГУТ,
Санкт-Петербург, 193232, Российская Федерация,
alex-in-spb@yandex.ru

Vikulov Anton

– Postgraduate, SPbSUT, St. Petersburg,
193232, Russian Federation, asv012016@gmail.com

Paramonov Alexander

– Doctor of Engineering Sciences, Full Professor,
SPbSUT, St. Petersburg, 193232, Russian Federation,
alex-in-spb@yandex.ru