

Диагностика беспроводных соединений локальных вычислительных сетей

А.В. ВОРУЕВ, В.Н. КУЛИНЧЕНКО

Рассмотрена ситуация, сложившаяся при использовании близких частотных диапазонов различными сетевыми стандартами. Описан ряд путей по выходу из конфликтных ситуаций. Описывается применение программных и аппаратных средств для организации диагностики беспроводных сетей.

Ключевые слова: беспроводная сеть, несущая частота, диагностика.

The situation when using close frequency bands by different network standards are described. A number of ways to resolve the conflict are presented. The use of software and hardware for the organization of diagnosis of wireless networks are given.

Keywords: wireless network, carrier frequency, diagnosis.

Введение. В основе беспроводных сетей могут лежать разные технологии, но их объединяет общая для всех устройств среда, и это вносит существенное ограничение в механизмы их работы.

Для примера продемонстрируем типичную занятость частотного диапазона в районе частоты 2,4 ГГц (рисунок 1).

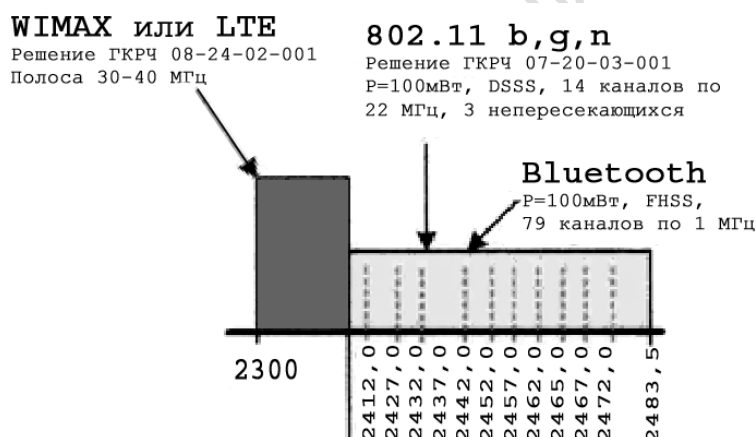


Рисунок 1 – Плотность использования частотного диапазона 2,4 ГГц

Основным международным документом, определяющим правила использования радиочастотной связи (РЧС), является Регламент радиосвязи, содержащий, в частности, международную таблицу распределения частот и определяющий основные правила координации и совместного использования частот для наземных и космических служб всех назначений.

В связи с ограниченностью РЧС встает задача повышения эффективности использования спектра. Перечислим некоторые меры, используемые в мировой практике при решении данного вопроса.

- Можно рекомендовать распределение ресурса на принципе аукционирования, поскольку конкурирующие операторы определяют стоимость спектра эффективнее, чем государственный орган. Ограничения этого подхода - должен быть достаточный спрос на данный участок спектра, а также важно не сделать слишком большим первичный взнос, поскольку это может негативно отразиться на способности операторов быстро вернуть свои инвестиции в РЧС.

- Разрешение на использование частот должно иметь ограничение по времени (не слишком короткое, чтобы оператор мог получить достаточную прибыль от деятельности и не слишком длительное, чтобы государство не лишалось возможности управлять частотным ресурсом). Обычно в качестве срока действия лицензии выбирается интервал 10-20 лет.

- Эффективность развития систем связи зависит от полосы частот, в узких полосах частот, как правило, эффективное развитие затруднено или невозможно. В США, например, принято решение, что в качестве лота на создание сети радиодоступа предоставляется полоса частот не менее 20 МГц и не более 45 МГц. В зависимости от доступного спектра оптимальным считается наличие 5 операторов в одной зоне обслуживания.

- Плата за использование спектра – еще один рычаг повышения эффективности использования частот.

- Известны успешные случаи, когда создание вторичного рынка частот позитивно сказывалось на эффективности их использования.

- Может применяться расширение прав пользователя в отношении выделяемых частот, например, выделение РЧС производится без определения, какую из технологий должен реализовывать пользователь для построения системы связи.

- Известны случаи, когда управление РЧС передается частному сектору, который демонстрирует эффективные подходы к управлению полученным ресурсом. Государство в этом случае оставляет за собой лишь стратегическое планирование, регистрирует сделки, получает за них налоги, решает конфликты и контролирует выполнение установленных требований.

Локальные сети в условиях необходимости поддержки увеличивающегося числа мобильных устройств увеличивают нагрузку на беспроводную среду. При этом системные администраторы постоянно сталкиваются с проблемой организации качественной и защищенной связи для своих абонентов.

Количество подключенных устройств к концу 2014 г. составит 16 млрд, что на 20 % больше, чем было в 2013 г., а к 2020 г. их численность возрастет более чем вдвое и достигнет 40,9 млрд, сообщает аналитическая компания ABI Research. Другие аналитические организации, например Международный телекоммуникационный союз (The International Telecommunications Union, ITU), склоняются к более скромной цифре около 30 млрд устройств. Напротив, компании производители, например Cisco Inc., склоняются к большей цифре около 50 млрд.

Эксперты считают, что рост числа устройств будет происходить за счет подключений M2M-устройств или устройств, предназначенных для обмена информацией между машинами. Этот сетевой трафик необходимо пропустить через инфраструктуру каналов связи, а значит их развитие является сдерживающим фактором.

Для реализации клиентского подключения беспроводным способом необходимо иметь резерв в радиочастотном спектре. Такой резерв достигается за счет уплотнения: частотного, временного или пространственного (в случае с MIMO). Опыты в данном направлении продолжаются.

Например, компанией Ubiquiti Networks была разработана и запатентована в 2012 г. технология AirMAX. Суть ее в том, что прием-передача сигнала несколькими антеннами на одном канале упорядочивается и структурируется протоколом TDMA с аппаратным ускорением: пакеты данных разнесены в отдельные временные слоты, очереди передачи координируются.

Диагностика беспроводного соединения на стороне пользователя долгое время не учитывалась как актуальная задача. Низкая мощность устройств, задействованных в обмене данными, позволяла организовать разделение одного частотного канала несколькими пользовательскими устройствами за счет затухания сигнала от соседних устройств.

К середине 2014 г. ситуация изменилась:

- требование к увеличению дальности связи и скорости передачи данных потребовало увеличения мощности устройств;

- плотность размещения пользователей беспроводных сетей возросла;

- одновременная эксплуатация несколькими сетевыми стандартами соседних частот приводит к общему снижению качества обслуживания.

В результате внедрение, а в некоторых случаях и просто поддержка эксплуатации, беспроводных сегментов локальных вычислительных сетей упирается в необходимость проведения обследования радиочастотного диапазона.

Простейшие программы диагностики доступны пользователям в виде всевозможных модулей, осуществляющих отображение беспроводных сетей, сигнал которых распознается достаточно хорошо. Примером такой программы является Wifi Analyzer (рисунок 2).

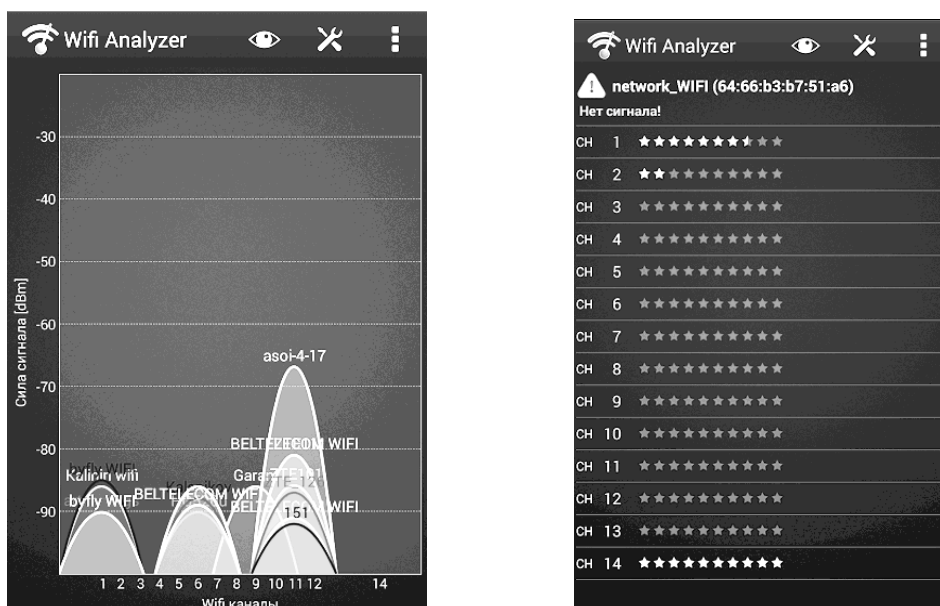


Рисунок 2 – Пример реального заполнения частотного диапазона 2,4 ГГц

Приведенный график (левая часть рисунка 2) показывает накладки частотных диапазонов при их эксплуатации соседними станциями. Программа вырабатывает рекомендацию по рейтингу частот свободных на текущий момент для дальнейшего использования (правая часть рисунка 2). В зависимости от интенсивности работы каждой из беспроводных сетей можно получить графики загруженности частот (рисунок 3).

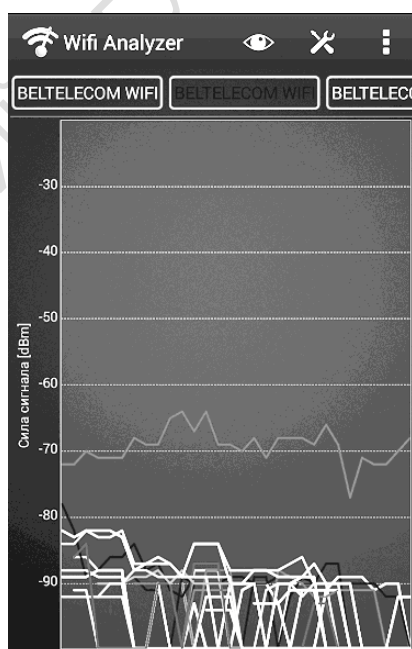


Рисунок 3 – График изменения мощности сигнала станций WiFi

Даже такой поверхностный анализ уже дает возможность принимать решения по установке и настройке новых беспроводных точек доступа.

Профессиональное оборудование позволяет получить намного более детальную картину (рисунки 4, 5).

Access Points Summary

Name: 98f537-3464e7 Channels: 8 (2,447GHz) #APs: 1 Security: No Security SSIDs: byfly WIFI Notes: Unexpected country from access point,	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -88dBm Authorization (ACL): Unauthorized
Name: 98f537-3e440f Channels: 6 (2,437GHz) #APs: 2 Security: Mixed SSIDs: Kalenikov, Notes: Unexpected country from access point	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -88dBm Authorization (ACL): Unauthorized
Name: c864c7-3c25c5 Channels: 1 (2,412GHz) #APs: 2 Security: Mixed SSIDs: Kalinin wifi, Notes: Unexpected country from access point	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -89dBm Authorization (ACL): Unauthorized
Name: cc7b35-262c79 Channels: 10 (2,457GHz) #APs: 2 Security: Mixed SSIDs: ZTE044, Notes: Possible Interference - overlaps standard channels	802.11 Types: b,g,n AP Country Setting: TW Best AP Signal Strength: -84dBm Authorization (ACL): Unauthorized
Name: cc7b35-272339 Channels: 10 (2,457GHz) #APs: 1 Security: No Security SSIDs: BELTELECOM WIFI Notes: Possible Interference - overlaps standard channels	802.11 Types: b,g,n AP Country Setting: TW Best AP Signal Strength: -87dBm Authorization (ACL): Unauthorized
Name: D-Link:002191-88b2ad Channels: 11 (2,462GHz) #APs: 1 Security: WPA2-P(AES-CCMP) SSIDs: asoi-4-17 Notes:	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -58dBm Authorization (ACL): Unauthorized
Name: D-Link:1caff7-2ded50 Channels: 1 (2,412GHz) #APs: 1 Security: No Security SSIDs: Garant Notes: Unexpected country from access point,	802.11 Types: b,g AP Country Setting: GB Best AP Signal Strength: -87dBm Authorization (ACL): Unauthorized
Name: D-Link:1caff7-2deda8 Channels: 1 (2,412GHz) #APs: 1 Security: No Security SSIDs: Garant Notes: Unexpected country from access point,	802.11 Types: b,g AP Country Setting: GB Best AP Signal Strength: -88dBm Authorization (ACL): Unauthorized
Name: D-Link:1caff7-2dedc8 Channels: 1 (2,412GHz) #APs: 1 Security: No Security SSIDs: Garant Notes: Unexpected country from access point,	802.11 Types: b,g AP Country Setting: GB Best AP Signal Strength: -84dBm Authorization (ACL): Unauthorized
Name: Infint:f81a67-ec7bf8 Channels: 9 (2,452GHz) #APs: 1 Security: WPA2-P(AES-CCMP) SSIDs: Garant Notes: 40 MHz 802.11n is not recommended on 2.4 GHz,	802.11 Types: b,g,n AP Country Setting: TW Best AP Signal Strength: -81dBm Authorization (ACL): Unauthorized
Name: IntIn:00e04d-66a3e4 Channels: 1 (2,412GHz) #APs: 1 Security: No Security SSIDs: BELTELECOM WIFI Notes:	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -90dBm Authorization (ACL): Unauthorized
Name: IntIn:00e04d-762515 Channels: 6 (2,437GHz) #APs: 2 Security: Mixed SSIDs: BELTELECOM WIFI, Notes:	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -84dBm Authorization (ACL): Unauthorized
Name: Openbr:fa150e-a3f0bc Channels: 11 (2,462GHz) #APs: 1 Security: WPA2-P(AES-CCMP) SSIDs: NOKIA Lumia 630_8138 Notes:	802.11 Types: b,g,n AP Country Setting: TW Best AP Signal Strength: -85dBm Authorization (ACL): Unauthorized
Name: Pima:5422f8-1b7e13 Channels: 11 (2,462GHz) #APs: 2 Security: Mixed SSIDs: ZTE 101, Notes:	802.11 Types: b,g,n AP Country Setting: TW Best AP Signal Strength: -83dBm Authorization (ACL): Unauthorized
Name: Pima:5422f8-1bef5e Channels: 11 (2,462GHz) #APs: 2 Security: Mixed SSIDs: BELTELECOM WIFI, Notes:	802.11 Types: b,g,n AP Country Setting: TW Best AP Signal Strength: -76dBm Authorization (ACL): Unauthorized
Name: ZTE :0026ed-a85051 Channels: 11 (2,462GHz) #APs: 2 Security: Mixed SSIDs: ZTE_126, Notes:	802.11 Types: b,g AP Country Setting: TW Best AP Signal Strength: -88dBm Authorization (ACL): Unauthorized

Рисунок 4 – Часть журнала опроса частот стандарта IEEE 802.11 с Flucke AirCheck



Рисунок 5 – Экраны работы Fluke AirCheck

Учитывая данные, отсеиваемые ранее как незначительный фон, появляется возможность принимать более взвешенные решения. Например:

- выработка рекомендаций по физическому переносу источников сигнала;
- выработка рекомендаций по равномерному заполнению частотного диапазона источниками сигнала;
- возможный отказ от использования нескольких устройств с большим перекрытием зон вещания дублирующего трафика;
- выработка рекомендаций по замене оборудования.

Материал для статьи был собран устройством AirCheck™ Wi-Fi Tester.

Вот некоторые из его возможностей:

- просмотр данных об использовании сети Wi-Fi, отсортированных по каналам, и быстрое определение наличия трафика стандарта 802.11 или помех, не относящихся к трафику 802.11;
- быстрая идентификация беспроводных точек доступа, авторизованных или неавторизованных, и определение их местонахождения;
- полное документирование результатов поиска неполадок для быстрого разрешения неполадки или передачи проблемы следующему уровню технического обслуживания.

Применение данного устройства и его аналогов обеспечивает процедуру диагностики планируемых и эксплуатируемых беспроводных соединений дополнительными данными.

Литература

1. Демиденко, О.М. Функциональные возможности программного комплекса адаптивной идентификации пользователей корпоративной сети // О.М. Демиденко, В.Д. Левчук, А.И. Кучеров / Проблемы, физики, математики и техники. – 2010. – № 3 (4). – С. 69–73.
2. Воруев, А.В. Удаленный контроль и управление процессами в локальных сетях / О.М. Демиденко, А.В. Воруев, А.И. Кучеров // Известия Гомельского государственного университета им. Ф. Скорины. – 2007. – № 5 (44). – С. 98–100.
3. Диваков, Н.Н. IPv6 протоколы : в 2 ч. / Диваков Н.Н., А.В.Воруев // Материалы III Республиканской научной конференции студентов, магистрантов и аспирантов «Актуальные вопросы физики и техники», 17 апреля 2014 г. : ч. 2 / редкол. : А.В.Рогачев (гл. ред.) [и др.]. – Гомель : ГГУ им. Ф. Скорины, 2014. – С. 60–62.
4. AirCheck™ Wi-Fi Tester. Простой поиск и устранение неисправностей в специализированном тестовом инструменте Wi-Fi. [Электронный ресурс]. – Режим доступа : <http://ru.flukenetworks.com/enterprise-network/network-testing/AirCheck-Wi-Fi-Tester#sthash.UNBaDH3A.dpuf>. – Дата доступа : 15.09.2014.

Гомельский государственный
университет им. Ф. Скорины

Поступила в редакцию 06.10.2014