Опыт организации единой беспроводной сети научного учреждения

Г.М. Михайлов, М.А. Жижченко, А.М. Чернецов

Вычислительный центр им. А.А. Дородницына ФИЦ ИУ РАН

Аннотация. В работе дано описание системы подключения пользователей к единому Wi-Fi - пространству ВЦ ФИЦ ИУ РАН в диапазонах 2.4 и 5 ГГц. При разработке проекта были проанализированы технические решения различных производителей. Система реализована на базе оборудования Cisco с использованием инфраструктурного режима (выбран вариант контроллера БЛВС и множества точек доступа). Исследованы и анализированы различные механизмы аутентификации пользователей (pre-shared keys, WPA2 и его модификации), обосновано использование web-based - аутентификации. Разработанная система обеспечивает персонифицированный и ограниченный доступ к Wi-Fi, что позволило соблюсти все требования действующего законодательства РФ в области предоставления услуг беспроводной связи. Выделяются три категории пользователей: администраторы ЛВС, пользователи организации и внешние пользователи. Соответственно, на оборудовании реализованы три независимых Wi-fi сегмента с разным уровнем доступа к ресурсам ЛВС и с различными настройками, включающими в себя время сеанса, доступ к внутренним ресурсам, запрет на просмотр каких-либо ресурсов. Это достигнуто за счет использования различных сервисных услуг (Service Set Identifier – SSID), для каждого из которых настроен свой класс обслуживания QoS.

Ключевые слова: вычислительные сети, беспроводные локальные вычислительные сети, информационная безопасность, ключи защиты, сетевые стандарты защиты информации.

Experience in organizing a unified wireless network of a scientific institution

G.M. Mikhaylov, M.A. Zyzchenko, A.M. Chernetsov

Computing Centre FRC CSC RAS

Abstract. The paper describes the system for connecting users to unified Wi-Fi space of the CC FRC CSC RAS in the 2.4 and 5 GHz bands. During the development of the project, technical solutions of various manufacturers were analyzed. The system is implemented on the basis of Cisco equipment with Infrastructure Mode

(WLAN Controller and Access Points mode). Various mechanisms of user authentication (pre-shared keys, WPA2 and its modifications) are investigated and analyzed, and the use of web-based authentication is justified. The developed system provides personalized and limited access to Wi-Fi, which allowed to comply with all the requirements of the current legislation of the Russian Federation in the provision of wireless communications services. There are three categories of users: LAN administrators, users of the organization and external users. Accordingly, the equipment implemented three independent Wi-fi segments with different levels of access to LAN resources and with different settings, including session time, access to internal resources, prohibition to view any resources. This is achieved through the use of various service services (Service Set Identifier - SSID), for each of which is configured its QoS service class.

Keywords: networks, wireless local area networks, information security, security keys, network information security standards.

Введение

Данная работа посвящена вопросам проектирования и развертывания беспроводных сетей Wi-Fi в учреждениях, в которых имеются и функционируют локальные вычислительные сети (ЛВС), базирующиеся на классических проводных стандартах **Ethernet.** ЛВС ВЦ РАН (далее Центра), созданная в 1995 году, до настоящего времени находилась в процессе непрерывного развития, обновления и развития программно-аппаратной среды в соответствии с требованиями современных IT- технологий. В этих условиях необходимость создания Wi-Fi – сети поверх и в дополнение к существующей – это усовершенствование и развитие телекоммуникационной и вычислительной среды учреждения в соответствии с требованиями времени. Исходя из этого, в работе главное внимание будет уделено основам организации беспроводной сети применительно к действующей ЛВС с сохранением полной функциональной целостности ее основных узлов и архитектуры. Учитывая 100% оснащенность рабочих мест пользователей точками доступа к **Internet** в стационарном режиме, основное внимание при проектировании Wi-Fi – сети было уделено оснащению аудиторий, конференц-залов и других помещений для проведения общественных и научных мероприятий. Так как беспроводная связь является принципиально широковещательной, при ее развертывании должны быть соблюдены и применены все разработанные к настоящему времени стандарты 802.11. Все методы этого стандарта используют радиосигналы ближнего радиуса действия в диапазоне частот ISM 2,4 ГГц или 5 ГГц, где не требуется лицензирования.

Важнейшим условием при реализации беспроводной сети является соблюдение действующих постановлений правительства РФ №738 от 31.07.2014 года и №801 от 12.08.2014 года [1,2].

1. Основная часть

1.1 Выбор топологии и платформы реализации сети.

Исходим из того, что беспроводные сети, используемые для подключения к сети **Internet,** появились еще в 1997 году [3], и к настоящему времени уже существуют стандарты 802.11(a,b,c, g, n, i. ad), применение которых определяется в каждом отдельном случае в соответствии с задачами учреждения. Нет необходимости останавливаться на их описании и на отличительных особенностях каждого из перечисленных методов. Применение очевидно – это обеспечение работы мобильных устройств, быстрое развертывание новой системы и сворачивание по мере необходимости.

Самый популярный режим использования сетей 802.11 — это подключение их клиентов к другой сети, например, внутренний сети учреждения или Интернету. В таком инфраструктурном режиме (**infrastructure mode)** каждый режим связывается с точкой доступа (**Access Point, AP**), которая, в свою очередь, подключена к сети. Клиент отправляет и получает пакеты через точку доступа. Несколько точек доступа можно соединить вместе, обычно в кабельную сеть под названием распределительная система (distribution system). Так формируется расширенная сеть 802.11. При реализации проекта важно определиться с выбором аппаратной платформы и соответствующего программного обеспечения для этого оборудования. Здесь у каждого разработчика проекта могут быть свои обоснованные предпочтения в выборе производителя сетевых устройств. В нашем проекте эта проблема решалась однозначно в пользу компании **Cisco.** так как вся базовая **Ethernet**–сеть в части сетевых компонентов была построена на **Cisco**- платформе.

Исходя из концепции, положенной в основу проекта развертывания **wi-fi,** как дополнение к существующей ЛВС, была поставлена задача обеспечить доступ к Интернет с использованием беспроводной сети во всех аудиторных помещениях, в рабочих кабинетах, в конференц-зале института, где регулярно проводятся научные конференции, лекции, семинары и другие научно-практические занятия для студентов и аспирантов.

При проектировании архитектуры беспроводной сети были рассмотрены два варианта ее организации:

1) создание сети на базе контроллера сети и с использованием интегрированного контроллера на управляемом коммутаторе (**свитче**);
2) создание сети с использованием отдельного контроллера беспроводной сети.

Первый вариант с использованием интегрированного контроллера на **свитче** требует, чтобы все беспроводные клиенты подключались к свитчу напрямую без промежуточного сетевого оборудования. С учетом локальных условий удаленности помещений, охватываемых Wi-Fi – сетью, подобное

решение невозможно из-за больших расстояний между коммутатором и конечными точками доступа AP. Кроме того, в этом варианте исполнения нет резервирования, а при использовании отдельного контроллера БЛВС возможно построение топологии сети с резервированием, что достигается установкой резервных контроллеров по мере необходимости.

1.2 Аутентификация и обеспечение информационной безопасности

Беспроводная передача принципиально является широковещательной. Учитывая эту особенность, обеспечивающую доступность к сети **wi-fi** широкому кругу лиц независимо от того, является пользователь сотрудником института или не является, доступ к ней должен быть персонифицирован и ограничен. Исходя из этого принципа, было принято решение о развертывании нескольких Wi-Fi - сетей с разными идентификаторами (Service Set Identifier - SSID) и уровнями доступа:

1) сеть CCAS_GUEST (гостевая) предназначена для гостевого доступа. Из нее есть доступ в Интернет, но невозможно попасть в локальную сеть Центра;

2) сеть CCAS_EMP (корпоративная) предназначена для доступа сотрудников Центра к ресурсам Интернет и локальной сети Центра;

3) сеть CCAS_SER предназначена для управления сегментом БЛВС Центра.

С целью оптимизации доступа к ресурсам сети Интернет реализованы классы QoS для всех трех идентификаторов SSID (Service Set Identifier) и установлены соответствующие приоритеты. Были рассмотрены различные способы обеспечения безопасности беспроводной сети. Протокол WPA2 обеспечивает самый высокий уровень защиты данных и контроль доступа в беспроводную сеть для корпоративных (WPA2-Enterprise) и индивидуальных пользователей (WPA2-Personal). WPA2 (Wireless Protected Access ver. 2.0) – это вторая версия набора алгоритмов и протоколов, обеспечивающих защиту данных в беспроводных сетях Wi-Fi. Новый стандарт предусматривает, в частности, обязательное использование более мощного алгоритма шифрования AES (Advanced Encryption Standard) и аутентификации 802.1X. На сегодняшний день для обеспечения надежного механизма безопасности в корпоративной беспроводной сети необходимо и обязательно использование устройств и программного обеспечения с поддержкой WPA2. Протоколы WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise). В режиме WPA2-Personal из введенной открытым текстом парольной фразы генерируется 256-разрядный ключ PSK (PreShared Key). Ключ PSK совместно с идентификатором SSID используются для генерации временных сеансовых ключей PTK (Pairwise Transient Key) для взаимодействия беспроводных устройств. Как и статическому протоколу WEP, протоколу WPA2-Personal присущи определенные проблемы, связанные с

необходимостью распределения и поддержки ключей на беспроводных устройствах сети, что делает его более подходящим для применения в небольших сетях из десятка устройств, в то время как для корпоративных сетей оптимален WPA2-Enterprise.

В режиме WPA2-Enterprise решаются проблемы, касающиеся распределения статических ключей и управления ими, а его интеграция с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в этом режиме требуются такие регистрационные данные, как имя и пароль пользователя, сертификат безопасности или одноразовый пароль. Аутентификация же осуществляется между рабочей станцией и центральным сервером аутентификации. Точка доступа или беспроводной контроллер проводят мониторинг подключений и направляют запросы аутентификации на соответствующий сервер аутентификации. В качестве такого сервера могут использованы RADIUS- сервер, LDAP-сервер, сервер Active Directory. Базой для обеспечения режима WPA2-Enterprise служит стандарт 802.1X, поддерживающий аутентификацию пользователей и устройств, пригодную как для проводных коммутаторов, так и для беспроводных точек доступа. Как правило, совместно со стандартом 801.1X взаимодействует расширенный протокол EAP (Extendable Authentication Protocol), предоставляющий среду для других сопутствующих стандартов по созданию сообщений. К сожалению, авторизация WPA2-Enterprise не позволяет подключаться к сети устройствам типа смартфонов.

Решается эта задача следующим образом. Авторизация WPA2-Enterprise требует получения и установки на клиенте пользовательских сертификатов для обеспечения SSL-соединения. Такое защищенное соединение может создаваться разными способами, но преимущественно с помощью протокола EAP-TLS (Extendable Authentication Protocol-Transport Layer Security). Для всех категорий внешних пользователей выполнять подобные настройки неудобно, трудоемко и небезопасно. Как правило, срок действия такого сертификата составляет один год. Следовательно, использование WPA2-Enterprise для аутентификации в сетях CCAS_GUEST недопустимо. Для решения этой проблемы использована технология ***web-based***-аутентификации, при которой при обращении к ЛВС происходит перенаправление запроса на блок авторизации специального Web-сервера. Контроллеры БЛВС компании **Cisco** содержат такой встроенный Web - сервер. При отсутствии такой возможности должен быть предусмотрен внешний (отдельный) Web - сервер. Страница авторизации при этом чрезвычайно проста – запрос логина и пароля. Учетные данные выдаются сотрудниками сетевой службы учреждения конкретным посетителям индивидуально. В этом случае процесс аутентификации заключается в передаче введенных данных (логин, пароль) для авторизации в Active Directory. В целях обеспечения запрета внешнему Wi-Fi - пользователю авторизоваться с данной учетной записью в локальной сети Центра были

созданы специальные учетные записи, для которых произведена смена первичной группы Domain Users на специально созданную группу со своим именем. В нашем решении это имя - **«wi-fi»**.

Для сети CCAS_SER, в силу стоящих задач, была выбрана авторизация по ключу WPA2 PSK (Pre-Shared-Key), как наиболее предпочтительная система защиты, предназначенная системному администратору.

1.3 Программно-аппаратная платформа

Инфраструктура локальной сети после включение в ее архитектуру БЛВС - сегмента претерпевает значительные изменения. Эти изменения связаны не только с добавлением нового оборудования, но и с необходимостью перенастройки части основных узлов и соответствующего программного обеспечения сети в целом. Учитывая ограничения объема текста представляемой работы, выделим следующие главные элементы:

1) в качестве контроллера БЛВС выбрано оборудование Cisco AIR-CT2504-15, как наиболее предпочтительный вариант на рынке сетевых устройств;

2) в качестве коммутатора БЛВС выбрано Cisco Catalyst WS-C3560X-48PF-S, сохраняя концепцию архитектуры сети в целом, включая ее проводную составляющую;

3) Wi-Fi - точки доступа выполнены на Cisco AIR-CAP16-21(I)-R-K9 со встроенными антеннами и с внешними антеннами; AIR-CAP16-21(E)-R-K9;

4) в соответствии с необходимостью распределения пользователей БЛВС в зависимости от прав доступа, а также для реализации транзитных обменов и управления беспроводными устройствами в схеме реализованы сети WLAN_Service, WLAN_Employees, WLAN_Guests, Transit_Net, Management_Net.

5) в сеть добавлены два инжектора питания POE (Power over Ethernet) Cisco AIR-PWRINJ5 для обеспечения электропитанием устройств точек доступа, не подключенных напрямую к коммутатору БЛВС.

В такой конфигурации с учетом особенностей разводки точек доступа, их количества и других условий запущен в эксплуатацию описанный Wi-Fi-сегмент, интегрированный в единую сеть института.

Анализ радиоэфира, проведенный средствами контроллера БЛВС, показал крайне высокую степень «зашумленности». Установленное в сеть оборудование Cisco позволило достаточно тонко нивелировать взаимные влияния излучателей и приемников сети и получить положительные результаты работы развернутой БЛВС. Апробация и вслед за ней полученные в процессе нормальной эксплуатации результаты подтвердили все параметры, заложенные в основу проекта.

Заключение

В заключение отметим, что разработка и выполнение такого масштаба проектов по созданию корпоративных БЛВС очень сильно привязаны к местным локальным условиям. В первую очередь, это правильное развертывание точек доступа, учет пространственных факторов в зданиях, определение количества планируемых пользователей, оценка необходимого оборудования для реализации проекта и, наконец, выбор производителя этой программно-аппаратной платформы. Исключительно важным условием при этом является необходимость привязки создаваемого БЛВС - сегмента к уже существующей проводной ЛВС, как это имеет место быть в представленной работе. Здесь особо следует отметить важность работ по установке и наладке дополнительных компонентов ПО применительно к основным узлам ЛВС Центра [4].

В целом работа по созданию сегмента БЛВС Центра была проведена успешно, что подтверждается устойчивой работой как в повседневном режиме работы института, так и при проведении регулярных конференций и других научных мероприятий.

Работа выполнена в рамках темы «Математические методы анализа данных и прогнозирования».

Раздел: *Информационно-вычислительные системы и среды в науке и образовании.*

Литература

1. Постановление правительства РФ №758 от 31 июля 2014 г. URL: https://rg.ru/2014/08/05/svyaz-site-dok.html.
2. Постановление правительства РФ №801 от 12 августа 2014 г. URL: https://rg.ru/2014/08/19/svyaz-site-dok.html.
3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: 2012. – С. 960
4. Михайлов Г.М., Жижченко М.А., Чернецов А.М. Обеспечение плавной перенумерации сети при смене провайдера // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18-23 сентября 2017 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2017. — С. 351-355. — URL: http://keldysh.ru/abrau/2017/44.pdf.

References

1. Postanovlenie pravitelstva RF №758 ot 31 iiulia 2014 g. URL: https://rg.ru/2014/08/05/svyaz-site-dok.html.
2. Postanovlenie pravitelstva RF №801 ot 12 avgusta 2014 g. URL: https://rg.ru/2014/08/19/svyaz-site-dok.html.

3. Tanenbaum E., Uezeroll D. Kompiuternye seti. 5-e izd. — SPb.: 2012. – S. 960
4. Mikhailov G.M., Zhizhchenko M.A., Chernetsov A.M. Obespechenie plavnoi perenumeratsii seti pri smene provaidera // Nauchnyi servis v seti Internet: trudy XIX Vserossiiskoi nauchnoi konferentsii (18-23 sentiabria 2017 g., g. Novorossiisk). — M.: IPM im. M.V.Keldysha, 2017. — S. 351-355. — URL: http://keldysh.ru/abrau/2017/44.pdf.