УДК 32.95

А.Дж. Сатыбаев, А.Н. Ермаков
Д.ф.-м.н. ОшТУ,
A.Dj. Satybaev, A.N. Ermakov
D.ph.-m.s.OshTU

РАЗРАБОТКА И ВНЕДРЕНИЕ БЕСПРОВОДНОГО ПОДКЛЮЧЕНИЯ МЕЖДУ СЕГМЕНТАМИ СЕТИ УДАЛЕННЫХ ОФИСОВ И МЕТОДЫ ЕГО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В данной статье приведен пример успешного внедрения решения по объединению двух территориально разделенных офисов на расстоянии 300 метров с доработкой беспроводной антенны для вращения на 360 градусов. Данная задача была выполнена по средствам беспроводной технологии с использованием современных методов защиты информации от несанкционированного доступа.

Ключевые слова: беспроводное подключение, сеть удаленных офисов ,доступ, защита.

DEVELOPMENT AND IMPLEMENTATION OF WIRELESS CONNECTIVITY BETWEEN NETWORK SEGMENTS REMOTE OFFICES AND METHODS OF PROTECTION FROM UNAUTHORIZED ACCESS

This article is an example of the successful implementation of the decision to merge the two geographically separated offices at a distance of 300 meters c finalizing a wireless antenna to rotate 360 degrees. This task was carried out by means of wireless technology with the use of modern methods of information protection from unauthorized access.

Keywords: wireless, network, remote offices, access protection.

Актуальность: В наши дни из-за необходимости выполнения обширного числа задач, тесной коммуникации между офисами организаций, а так же за счет территориальной распределенности подразделений часто возникает проблема их объединения в одну общую компьютерную сеть. Данная ситуация легко решаема в случае небольшого расстояния между организациями по средствам монтажа проводного оборудования. Что делать в случае если удаленный офис находится за пределами 100 и более метров? Сегодня решение этой проблемы стало доступно посредством беспроводной технологии (Wi-Fi моста). Данное решение было внедрено авторами статьи, и успешно протестировано в локальной сети Общественного Фонда «Эм Эс Ди Эс Пи Кей Джи» (Инициатива Фонда Ага Хана).

Техническое задание: Связать два сегмента сети в единую локальную сеть посредством беспроводной технологии. В первом сегменте сети (головной офис) находится 50 рабочих станций и серверное оборудование, второй сегмент намного меньше и состоит из 5 рабочих станций. Необходимо настроить защищенное беспроводное соединение, а так же продумать механизм быстрой передислокации удаленного офиса, так как данный офис предполагает всего лишь трех месячную занятость, после чего переедет в большее здание в направлении примерно 180 градусов левее. Тем самым встанет вопрос о перенаправлении точки доступа в головном офисе.

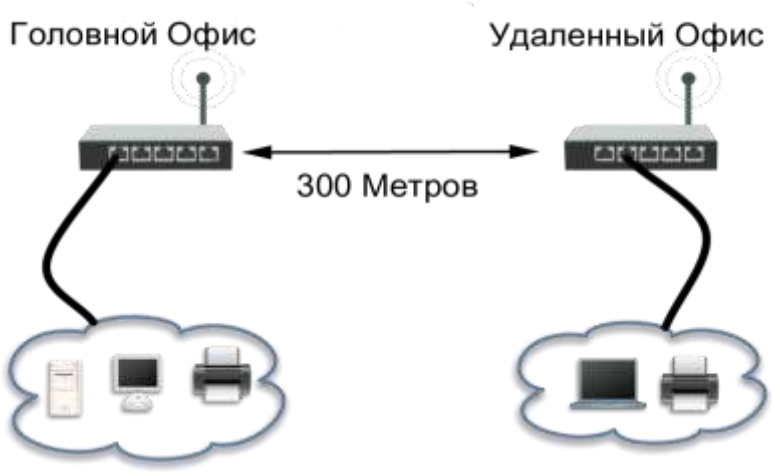

Рис.1. Схематичный рисунок объединения сегментов сети при помощи беспроводной технологии

Введение: В данном случае использования беспроводной технологии, очевидно. Во-первых - это простое и быстрое построение локальной сети; не нужно тянуть и укреплять кабели;
беспроводную сеть можно построить там, где нельзя протянуть кабели. Во-вторых - это снижение стоимости эксплуатации. Беспроводные сети снижают стоимость установки, поскольку не требуются кабельные соединения.

Разработка стандарта беспроводных локальных сетей (Wireless Local Area Network, WLAN), которая была начата вместе со стандартом 802.11, была окончательно сформирована IEEE (Инженерный институт электроники и электротехники) в 1997 году. Этот начальный стандарт поддерживает скорость передачи до 2 Мбит/с. Со временем стандарт был расширен. Расширение заключалось в добавлении информации к оригинальному стандарту, включая 802.11a и 802.11b. В списке ниже, детально рассмотрены стандарты, связанные со стандартом 802.11 и скорость обмена данными для каждого стандарта. [1], [2].

- 802.11 - Изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997)
- 802.11a - 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001)
- 802.11b - Улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999)
- 802.11e - Требование качества запроса, необходимое для всех радио интерфейсов IEEE WLAN.
- 802.11f - Описывает порядок связи между равнозначными точками доступа. Многократно разгружает распределенные между поставщиками сети WLAN.
- 802.11g - 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003)
- 802.11h - Распределенный по спектру 802.11a (5 GHz) для совместимости в Европе (2004)
- 802.11i - Исправляет существующие проблемы безопасности в областях аутентификации и протоколов шифрования. Стандарт затрагивает протоколы 802.1X, TKIP and AES.

Методы и способы решения задачи: Для решения поставленной задачи, то есть объединения сегментов сети головного офиса и удаленного на расстоянии 300 метров в единую локальную сеть необходимо выполнение некоторого ряда условий приведенных ниже:

- Выбор надежного оборудования, для монтажа вне помещения;
- Наличие прямой видимости между объектами, в противном случае сигнал между беспроводными точками доступа претерпевает изменения или рассеивается, что негативно влияет на качестве сигнала. В идеальных условиях, при прямой видимости

и отсутствии помех, максимальный диапазон бесперебойной работы Wi-Fi моста, составляет 5-10 км. ;

- Выбор беспроводного стандарта в качестве наиболее подходящего для выполнения поставленной задачи;
- Выбор протокола защиты от несанкционированного доступа, а так же реализация алгоритмов шифрования.
- Монтаж и настройка оборудования в режиме «точка-точка»;
- Доработка беспроводной точки доступа механизмом дистанционного вращения, для быстрого поворота в случае переезда офиса в иное место.

Рассмотрим вышеприведенные пункты по очереди.

В качестве беспроводного оборудования была выбрана точка доступа TL-WA5210G 2,4 ГГц – Это высокомощное наружное клиентское оборудование, а также решение при работе с беспроводными сетями на больших расстояниях. TL-WA5210G объединяет в себе функции беспроводной точки доступа, антенны с высоким коэффициентом усиления и защищённого от непогоды корпуса. Ключевыми особенностями TL-WA5210G являются 12dBi антенна с высоким коэффициентом усиления, высокая выходная мощность передатчика и высокая чувствительность приема. Это позволяет существенно расширить дальность передачи и получать более стабильные беспроводные соединения.

Наличие прямой видимости в большинстве случаях достигается установкой беспроводных точек доступа (Wireless Access Point) на мачту, высота которой может колебаться в зависимости от реализации поставленной задачи. До момента установки точку доступа необходимо было снабдить поворотным механизмом, которым можно было управлять на расстоянии. Точка доступа головного офиса будет постоянно находится на одном месте, а удаленный офис время от времени может менять место дислокации в радиусе от 300 метров до 1.5 километра.

Ни одна современная беспроводная точка доступа будь то внутренняя или внешняя не оснащена поворотным механизмом. Скорее всего, данная тенденция связанна с тем, что необходимости в решении проблем с поворотом антенн пока не возникало.

В данном случае для достижения максимальной прямой видимости точку доступа необходимо было закрепить на мачту высотой в 10 метров на крыше головного офиса. В случае переезда удаленного офиса необходимо будет поменять направление оборудования на 180 градусов, сделать это физически будет проблематично. Для решения данного вопроса было решено снабдить точку доступа поворотным механизмом, который был взаимствован, с обычной телевизионной антенны.

Рис.2. Поворотный механизм телевизионной антенны.

Данная антенна снабжена блоком питания, а так же кнопочным механизмом для поворота на 360 градусов, что вполне достаточно для реализации цели.

Снятие и установка поворотного механизма на беспроводную точку доступа проблем не составило, зато уберегло от дальнейших трудностей при развороте беспроводной точки доступа.

Вторая точка доступа была установлена в удаленном офисе и была направлена в сторону точки доступа головного офиса. Таким образом, вопрос о прямой видимости и разворотом антенны был решен.

В качестве беспроводного стандарта было решено использовать стандартз 802.11g. Данный стандарт идеально подходит под заданные нужды, так как позволяет передавать информацию по настроенному каналу связи до 54 Мбит/с, а так же поддерживает современные методы шифрования и защиты от несанкционированного доступа.

Так как беспроводная сеть будет функционировать вне здания, она будет являть собой широкий охват действия, тем самым, предоставляя возможность злоумышленнику получить несанкционированный доступ к локальной сети предприятия со всеми вытекающими негативными последствиями.

Для защиты созданного беспроводного соединения были использованы наиболее современные методы защиты от взлома и несанкционированного доступа.

В 2003 году был представлен стандарт безопасности — WPA (Wi-Fi Protected Access). Главной особенностью этого стандарта является технология динамической генерации ключей шифрования данных, построенная на базе протокола TKIP (Temporal Key Integrity Protocol). По протоколу TKIP сетевые устройства работают с 48-битовым вектором инициализации (в отличие от 24-битового вектора WEP (предыдущего протокола безопасности беспроводных сетей)) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей. В протоколе TKIP предусмотрена генерация нового 128-битного ключа для каждого передаваемого пакета. Кроме того, контрольные криптографические суммы в WPA рассчитываются по новому методу под названием MIC (Message Integrity Code). В каждый кадр здесь помещается специальный восьмибайтный код целостности сообщения, проверка которого позволяет отражать атаки с применением подложных пакетов. В итоге получается, что каждый передаваемый по сети пакет данных имеет собственный уникальный ключ, а каждое устройство беспроводной сети наделяется динамически изменяемым ключом [3].

Кроме того, протокол WPA поддерживает шифрование по стандарту AES (Advanced Encryption Standard), то есть по усовершенствованному стандарту шифрования, который отличается более стойким криптоалгоритмом, чем это реализовано в протоколах WEP и TKIP. Именно протокол WPA с шифрованием по стандарту AES будет достаточно для достижения цели.

На данном этапе использования протокола с возможностью шифрования данных будет не достаточно, поэтому необходима более тонкая конфигурация точек доступа для их безопасного взаимодействия.

Фильтрация MAC-адресов, которая поддерживается всеми современными точками доступа и беспроводными маршрутизаторами, хотя и не является составной частью стандарта 802.11, тем нее менее, позволяет повысить уровень безопасности беспроводной сети. Для реализации данной функции в настройках точки доступа создаётся таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы в данной сети. Таким образом в таблицу MAC-адресов каждой точки доступа необходимо добавить MAC-адрес другой точки доступа, тем самым защитив беспроводную сеть, от появления иного сетевого оборудования с MAC-адресом не совпадающим с таблицей.

Режим скрытого идентификатора сети SSID - одна из мер предосторожности, которую часто используют в беспроводных сетях. Каждой беспроводной сети назначается свой уникальный идентификатор (SSID), который представляет собой название сети. Когда пользователь пытается войти в сеть, то драйвер беспроводного адаптера прежде всего сканирует эфир на наличие в ней беспроводных сетей. При использовании режима скрытого идентификатора (как правило, этот режим называется Hide SSID) сеть не отображается в

списке доступных, и подключиться к ней можно только в том случае, если, во-первых, точно известен её SSID, и, во-вторых, заранее создан профиль подключения к этой сети.

Реализуя приведенные выше методы защиты беспроводного соединения, удается добиться практически максимальной защиты сегментов сети от несанкционированного доступа. Тем самым снизив риски проникновения злоумышленников.

Настройка беспроводных точек доступа осуществляется посредствам web-интерфейса. После проведенной конфигурации, сегменты сети необходимо протестировать и добиться максимального значения сигнала. Первоначальное тестирование было проведено используя команду ping из одного сегмента сети в другой. Результаты команды приведены ниже.

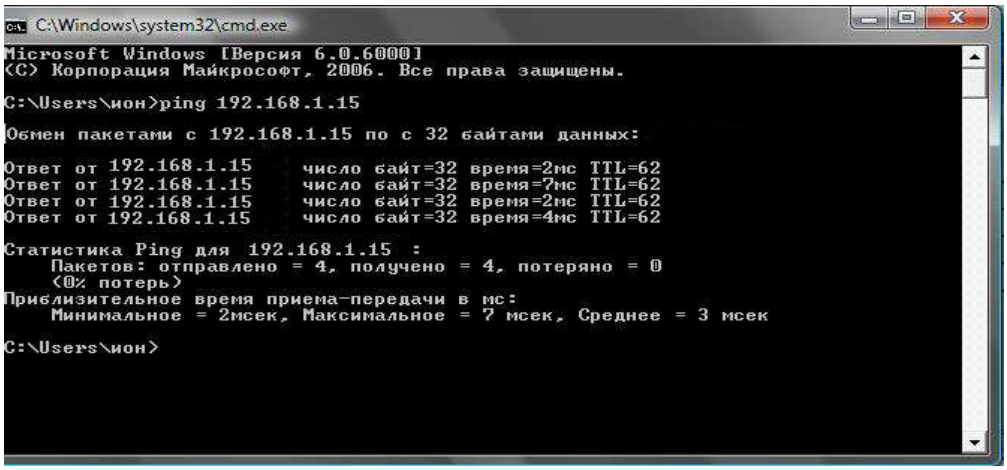

Рис. 3. Интерфейс командной строки

Как показано на рисунке 2 максимальная задержка пакета из одного сегмента сети в другой составляет максимально 7 милисекунд, что вполне достаточно для комфортной работы.

Таким образом, поставленная задача решена, мы реализовали объединение двух сегментов сети на расстоянии 300 метров, с защитой ее от несанкционированного доступа, с использованием современных методов шифрования, скрытия SSID, а также фильтрацией MAC-адресов. Так же беспроводная точка доступа головного офиса была доработана для быстрой смены направления, что позволило легко и просто передислоцировать удаленный офис.

Данный метод объединения сегментов сети возможно применить практически для любой сферы деятельности, в научных организациях, университетах, а так же территориально разделенных организациях.

Литература:

1. Джим Гейер, «Беспроводные сети. Первый шаг (Cisco)», 2005 г.
2. Денис Колисниченко, «Беспроводная сеть дома и в офисе», 2009 г.

Д. Росс, «Беспроводная компьютерная сеть Wi-Fi своими руками», 2009 г.