Министерство образования Республики Беларусь

Учреждение Образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

по дисциплине: «Аппаратное обеспечение компьютерных сетей»

на тему: «Проектирование компьютерной локальной сети»

Выполнил:

студент гр. 550504

Тишук В. М.

Руководитель проекта:

Глецевич. И. И.

МИНСК 2018

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 4](#_Toc535025233)

[1 ОБЗОР ЛИТЕРАТУРЫ 5](#_Toc535025234)

[1.1 Общие требования, предъявляемые к ЛВС 5](#_Toc535025235)

[1.2 Требования к беспроводной локально-вычислительной сети 6](#_Toc535025236)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 9](#_Toc535025237)

[2.1 Выбор способа организации локальной сети 9](#_Toc535025238)

[3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 10](#_Toc535025239)

[3.1 Обоснование выбора логической структуры сети, используемых сетевых технологий 10](#_Toc535025240)

[3.2 Обоснование выбора оборудования ЛВС 11](#_Toc535025241)

[3.2.1 Общие сведения 11](#_Toc535025242)

[3.2.2 Обоснование выбора пассивного сетевого оборудования и аксессуаров 12](#_Toc535025243)

[3.2.3 Обоснование выбора активного сетевого оборудования 12](#_Toc535025244)

[3.2.4 Адресация в локальной сети 16](#_Toc535025245)

[4 ПРОЕКТИРОВАНИЕ СКС 19](#_Toc535025246)

[4.1 Настройка и конфигурирование коммутатора Cisco SG220-50P Cisco Smart Plus PoE+. 19](#_Toc535025247)

[4.1.1 Монтаж. 19](#_Toc535025248)

[4.1.2 Подключение к сети. 20](#_Toc535025249)

[4.1.3 Настройка VLAN. 21](#_Toc535025250)

[4.1.4 Настройка Trunk и Access портов. 22](#_Toc535025251)

[4.1.5 Настройка Host Name и Login Banner. 22](#_Toc535025252)

[4.1.6 Настройка IP-адреса устройства и управляющей VLAN сети. 23](#_Toc535025253)

[4.2 Настройка и конфигурирование точки доступа Cisco AIR-CAP1602I. 23](#_Toc535025254)

[4.2.1 Монтаж. 24](#_Toc535025255)

[4.2.2 Конфигурирование. 24](#_Toc535025256)

[4.3 Настройка и конфигурирование маршрутизатора Cisco ME4624-ONT-RGW 26](#_Toc535025257)

[4.4 Настройка веб-сервера. 27](#_Toc535025258)

[ЗАКЛЮЧЕНИЕ 29](#_Toc535025259)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 30](#_Toc535025260)

[ПРИЛОЖЕНИЕ А 31](#_Toc535025261)

[ПРИЛОЖЕНИЕ Б 32](#_Toc535025262)

[ПРИЛОЖЕНИЕ В 33](#_Toc535025263)

[ПРИЛОЖЕНИЕ Г 34](#_Toc535025264)

[ПРИЛОЖЕНИЕ Д 35](#_Toc535025265)

[ПРИЛОЖЕНИЕ Е 36](#_Toc535025266)

ЗАДАНИЕ НА ПРОЕКТИРОВАНИЕ

|  |  |
| --- | --- |
| Вариант | 19 |
| Сфера деятельности | Небольшая гостиница. |
| Помещения и пользователи | В трехэтажном здании.  Первый этаж: вдоль одной стороны коридора: 3 однокомнатных номера (21, 22, 27 м2 ) -- по 3 стац. и по 3 моб. подкл.; вдоль другой стороны коридора: комната приема и размещения (18 м2 ) -- 2 стац. и 2 моб. подкл., дирекция (18 м2 ) -- 3 стац. и 3 моб. подкл., комната для персонала (34 м2 ) -- 5 стац. и 10 моб. подкл., буфет (20 м2 )-- 20 моб. подкл.  Второй и третий этажи: аналогично, только все комнаты отведены под номера. |
| Оборудование | ? без ПК, личные ноутбуки, смартфоны, web-сервер, 17 телевизоров с Wi-Fi, цветное МФУ. |
| Подключение к Internet | Оптоволоконный Ethernet. |
| Адресация | IPv4 (публичная подсеть из 4 адресов от провайдера), IPv6 (блок глобальных адресов от провайдера). |
| Безопасность | Подключение к сети (проводной и беспроводной) персонала гостиницы и посетителей -- с целью выхода в Internet. Удаленное администрирование. |
| Финансы | Полноценная коммерческая сеть. |
| Дополнительные требования заказчика | В номерах обеспечить выход в Internet посредством телевизоров. |

# ВВЕДЕНИЕ

Локальная сеть (далее ЛВС) является коммуникационной системой, включающей в себя рабочие станции и периферийный устройства на территории, объединяющей несколько зданий или одного предприятия, позволяющей одновременно использовать, различные сетевые ресурсы. В современное время ЛВС стала незаменимым инструментом во многих информационных структурах, включающих в себя более 1 компьютера.

Основные достоинства, реализуемые при использовании локальной сети – возможность совместной эксплуатации и быстрого обмена файлами, централизованное хранение файлов, распределяемый доступ к общим ресурсам, таким как принтеры, сеть Internet и другие.

Одной из главных функций, воплощаемых при создании и конструировании локальной сети, является обеспечение отказоустойчивости системы, то есть системы продолжающей функционировать (пусть и не в полном объеме) при выходе из строя некоторых входящих в них элементов. В ЛВС отказоустойчивость гарантируется путем избыточности, резервирования; а также пластичность работы входящих в сеть элементов (компьютеров).

Главной целью разработки и строительства локальной сети для организации является повышение производительности предприятия в целом.

Проектирование ЛВС, будет преследовать следующие цели:

* изучение физических сред передачи данных;
* ознакомление с принципами конструирования локальной вычислительной сети;
* анализ способов построения физической структуры ЛВС;
* ознакомление с правилами адресации в сети и моделями сетевого взаимодействия;
* изучение способов защиты информации в ЛВС.

# 1 ОБЗОР ЛИТЕРАТУРЫ

## Общие требования, предъявляемые к ЛВС

Вычислительная сеть создается для обеспечения потенциального доступа к любому ресурсу сети для любого пользователя сети. Качество доступа к ресурсу как глобальная характеристика функционирования сети может быть описана многими показателями, выбор которых зависит от задач, стоящих перед вычислительной сетью. Рассмотрим основные требования, предъявляемые к ЛВС.

1. Главным требованием, является выполнение сетью ее основной функции - обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть. Все остальные требования - производительность, надежность, совместимость, управляемость и масштабируемость - связаны с качеством выполнения этой основной задачи.
2. Производительность - это свойство обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. Существуют следующие основные характеристики производительности сети - время реакции, пропускная способность и задержка передачи на сетевом устройстве. Время реакции сети является интегральной характеристикой производительности с точки зрения пользователя. В общем случае время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос. Пропускная способность отражает объем данных, переданных сетью или ее частью в единицу времени. Задержка передачи определяется как задержка между моментом поступления пакета на вход какого-либо сетевого устройства или части сети и моментом появления его на выходе этого устройства.
3. Надежность ЛВС определяется следующими показателями:

* Готовностью или коэффициентом готовности, который означает долю времени, в течение которого система может быть использована.
* Вероятностью доставки пакета узлу назначения без искажений (вероятность потери пакета, вероятность искажения отдельного бита передаваемых данных, отношение потерянных пакетов к доставленным)
* Способностью системы защитить данные от несанкционированного доступа (безопасностью).

1. Отказоустойчивость - способностью «скрыть» от пользователя отказ отдельных элементов сети.
2. Расширяемость – означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений и служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной.
3. Масштабируемость - означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается.
4. Прозрачность сети достигается в том случае, когда сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени.
5. Поддержка разных видов трафика. Сеть должна обеспечить совместную передача традиционного компьютерного и мультимедийного трафика (в том числе видео и речи).
6. Управляемость – подразумевает собой возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности сети и планировать ее развитие.
7. Совместимость или интегрируемость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие различные стеки коммуникационных протоколов, и работать аппаратные средства и приложения от различных производителей [8].

## Требования к беспроводной локально-вычислительной сети

Так же в проектируемой ЛВС планируется использовать и беспроводные технологии, следовательно, необходимо определить общие требования к беспроводной локально вычислительной сети.

Внедряемая беспроводная локально-вычислительная сеть (далее БЛВС) предназначена для обеспечения доступа постояльцев и сотрудников гостиницы, к существующей корпоративной сети передачи данных (СПД), построенной на оборудовании Cisco. Пользователями БЛВС являются постояльцы и сотрудники гостиницы.

БЛВС должна отвечать следующим функциональным требованиям:

* активное оборудование БЛВС должно размещаться на территории подключаемого здания (уровни распределения и доступа);
* обеспечивать одновременную работу пользователей в диапазонах 2.4 ГГц и 5 ГГц (частоты маршрутизатора TP-LINK N750);
* обеспечивать пользователю возможность беспроводного доступа в корпоративную сеть по технологии Wi-Fi стандарта IEEE 802.11 g/n с иерархией скоростей от 11 Мбит/с до 450 Мбит/с;
* в качестве основного протокольного стека БЛВС используется TCP/IP;
* в качестве основного протокола сетевого уровня должен использоваться IPv4. Необходима так же поддержка протокола IPv6;
* оборудование радиодоступа БЛВС должно отвечать требованиям международных стандартов (Общие требования к радиоканалам: EN 300.328, EN 301.893, EN 301.489-1, EN 301.489-17, EN 60601-1-2; Радиосоединения: IEEE 802.11 b/g, IEEE 802.11n, IEEE 802.11d; Защита соединений: 802.11i (WPA, WPA2), 802.1X; Аутентификация: EAP-TLS, TTLS, PEAP v0, EAP-FAST, PEAPv1, EAP-SIM) в соответствующих отраслях техники, иметь сертификаты, разрешающие его применение в Республики Беларусь, в том числе «Сертификат соответствия Системы сертификации в области связи», и соответствовать стандартам ТР ТС 004/2011 «О безопасности низковольтного оборудования» и ТР ТС 020/2011 «Электромагнитная совместимость технических средств»;
* предоставление услуг БЛВС должно производиться круглосуточно, в режиме 24х7. Допускаются технологические паузы в функционировании оборудования БЛВС продолжительностью не более часа. Количество пауз в течение года – не более двух на каждый опорный узел сети;
* оборудование ядра должно обеспечивать коммутацию трафика третьего и четвертого уровней эталонной модели OSI на скоростях каналов связи [6].

Требования к программному обеспечению оборудования:

1. Программное обеспечение оборудования БЛВС на момент установки не должно иметь задокументированных критических ошибок, приводящих, при определенных условиях, к сбоям в работе оборудования и сети в целом;
2. Программное обеспечение оборудования должно быть модернизируемым без необходимости изменения аппаратной части оборудования, за исключением необходимости обновления съемных носителей, если такая процедура предусмотрена производителем оборудования;
3. Обновление программного обеспечения на оборудовании не должно требовать выведения оборудования из эксплуатации, за исключением одного цикла перезагрузки системы;
4. Программное обеспечение оборудования должно обеспечивать поддержку следующих основных протоколов на оборудовании уровня распределения – ARP, Proxy ARP, STP (IEEE 802.1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), IEEE 802.1q, IEEE 802.1p, LACP (IEEE 802.3ad), IP v.4, HSRP, OSPF, client DNS, SNMP, SSH [5].

Главным требованием к зоне действия БЛВС является его уверенный радиоприем в пределах всех помещений гостиницы. Под уверенным радиоприемом подразумевается прием радиосигнала, уровень мощности которого составляет не менее 50 дБм.

Структура БЛВС должна удовлетворять следующим требованиям:

* инфраструктура БЛВС должна включать уровни распределения и доступа. Не допускается совмещение функций любых двух уровней на одном оборудовании;
* точки доступа должны подключаться Ethernet-интерфейсами к коммутаторам доступа локально-вычислительной сети [3].

К функциям (задачам) БЛВС предъявляются следующие требования:

* БЛВС должна предоставлять защищенный беспроводной доступ пользователей к ресурсам корпоративной сети гостиницы на основе метода аутентификации и авторизации по согласованию с Заказчиком;
* БЛВС должна вещать все беспроводные сети гостиницы, доступные в остальных зданиях (не более 5). Подробная проработка способов аутентификации и авторизации беспроводных пользователей, сегментирования беспроводных (WLAN) и виртуальных (VLAN) сетей, а также информационного взаимодействия со смежными системами, должна выполняться на этапе пусконаладочных работ совместно с Заказчиком.

Требования по надежности и отказоустойчивости БЛВС.

Для исключения сбоев системы, вызванных нарушениями работы телекоммуникационного оборудования, необходимо:

* максимально унифицировать предлагаемое оборудование;
* точки доступа должны быть совместимы с системой управления Cisco Prime 2.0;
* предусмотреть использование механизмов, обеспечивающих автоматическое переключение на резервное оборудование;
* предусмотреть наличие встроенных в оборудование средств диагностики и устранения неисправностей.

Требования по размещению оборудования.

Все телекоммуникационное оборудование (кроме точек доступа) должно размещаться в специализированных монтажных шкафах с 19'' профилями. Размещение оборудования должно предусмотреть исключение несанкционированного доступа к нему.

# 2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описывается структура и порядок ее выбора, локальной сети, а также способ подключения её к Internet.

2.1 Выбор способа организации локальной сети

При организации WLAN-сетей значительную роль играет размер покрытия. При идеальных условиях распространения радиоволн зона покрытия одной точки доступа будет иметь следующие значения:

1. Сеть стандарта IEEE 802.11a - 50 м

2. Сети 802.11b, g, n - порядка 100 м.

Для разрабатываемой сети гостиницы характерны небольшие расстояния до всех беспроводных устройств. Исходя из этого, будет использоваться стандарт 802.11а.

Все пользовательские станции будут подключены к беспроводным точкам доступа, находящимся на соответствующем этаже, которые в свою очередь через проектируемую кабельную структуру соединены с соответствующими коммутаторами, соединенными через web-сервер с маршрутизатором, имеющим доступ во внешнюю сеть Internet.

Провайдером предоставляется четыре IPv4 адреса. Для доступа всех устройств в глобальную сеть интернет на маршрутизаторе настраивается механизм Network Address Translation (NAT), который позволяет подменять IP адреса проходящих пакетов. Каждый из трех VLAN, будет подменятся своим IP адресом, и один IP адрес будет использоваться для сервера.

Проектируемая локальная сеть будет состоять из личных ноутбуков, смартфонов, веб-сервера, 17 телевизоров с Wi-Fi.

Структурная схема представлена в приложении «А».

# 3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

## 3.1 Обоснование выбора логической структуры сети, используемых сетевых технологий

Топология сети – геометрическая форма и физическое расположение компьютеров по отношению к друг другу. Топология сети позволяет сравнивать и классифицировать различные сети. Для реализации данного проекта самым оптимальным выбором будет использование топологии «Звезда».

В звездообразной сети все коммуникации между узлами проходят через центральное устройство. Кабели, которыми компьютеры подключаются к сети, расходятся от этого устройства наподобие лучей звезды (рис. 3.1). Сети такого типа преобладают там, где используются мэйнфреймы. Собственно, центральное устройство с подключенными к нему терминалами и есть мэйнфрейм (говоря очень упрощенно).

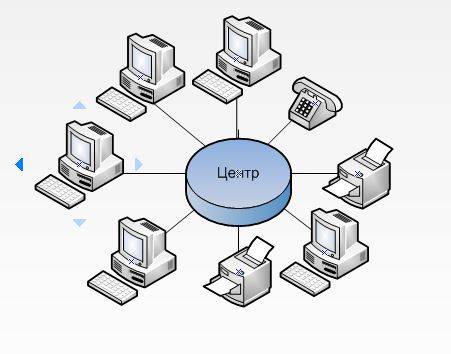


Рисунок 3.1. Топология типа «Звезда»

Несмотря на то, что у такой конструкции есть уязвимое место — центральное устройство, — на практике она исключительно стабильна и надежна, одновременно позволяя без труда подключать и отключать клиентские машины. Кроме того, сбой одного компьютера обычно не наносит ущерба всей сети, так как задерживается центральным устройством. К недостаткам этой топологии относятся необходимость прокладки отдельного кабеля от каждого компьютера к центральному устройству даже тогда, когда два компьютера расположены рядом друг с другом.

Если в центре звезды поместить мощный, интеллектуальный концентратор, можно использовать его защитные функции для фильтрации аппаратных адресов [9].

Передача данных осуществляется с использованием сетевого уровня согласно сетевой модели OSI.

Основная причина создания сетевой модели OSI - стандартизация используемых протоколов и технологий. Независимость технологий каждого уровня позволяет разработчикам новых приложений и технологий абстрагироваться от реализаций тех протоколов, которые не затрагивают внедряемый или разрабатываемый объект.

Физический уровень. На данном уровне основной рассматриваемой единицей передачи информации является бит (bit), передаваемый тем или иным способом. В контексте данного уровня рассматривается среда передачи (например, витая пара, оптоволоконный кабель), протоколы организации передачи (к примеру, DSL, протокол работы оптики NRZ). К устройствам, работающим на данном уровне можно отнести регенераторы, репитеры, сетевые адаптеры. Пример протокола данного уровня -G703, описывающий стандарт передачи проводного 2-мегабитного потока.

Канальный уровень. Основной рассматриваемой единицей является фрейм(frame). Фрейм – особым образом сгруппированная группа битов физического уровня, к которому добавляется битовый заголовок, содержащий аппаратные адреса отправителя и получателя, контрольную сумму для определения целостности фрейма и некоторые флаги, управляющие процессом передачи. На данном уровне работает процесс коммутации фреймов. Сам термин коммутация следует понимать, как процесс проключения канала от получателя к отправителю. К функциям данного уровня можно отнести также контроль целостности фрейма (защиту от помех и ошибок). Как пример протоколов можно привести протоколы Ethernet (IEEE 802.3), WLAN (IEEE 802.11a/b/g/n).

Сетевой уровень. Основной рассматриваемой единицей является пакет. Функцией данного уровня является объединение сетей. Под сетью в данном контексте понимается группа устройств - узлов (хостов) сети, которые объединены с помощью единой технологии канального уровня. На данном уровне работает процесс маршрутизации – выбора оптимального маршрута передачи пакета. Пакет представляет собой информационный блок, содержащий информацию вышестоящего уровня в качестве нагрузки, плюс заголовок, содержащий сетевые адреса отправителя и получателя и служебную информацию.

Уровень представлений. На данном уровне обеспечивается кодирование исходного сообщения.

Уровень приложений. Основной задачей данного уровня является организация интерфейса между объектом – отправителем сообщения, представление сообщения в машинно-обрабатываемом виде, и передача его на более низкие уровни модели [12].

## 3.2 Обоснование выбора оборудования ЛВС

### 3.2.1 Общие сведения

Для размещения коммутационного оборудования, необходимо использовать специально оборудованное помещение, но при строительстве и проектировании здания гостиницы, данные помещения не были учтены. Поэтому для размещения оборудования предполагается использование настенных шкафов, расположенных на высоте примерно двух с половиной метров от пола, что затруднит свободный доступ к оборудованию, для предотвращения несанкционированного доступа двери шкафов оснащены запорными устройствами, замками.

Прокладка кабелей должна осуществляться с учетом стандартов: TIA/EIA-568B, ISO/IEC\_11801 (СНГ аналоги ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008).

При параллельной прокладке информационных кабелей категории 5е и силовых кабелей, необходимо руководствоваться требованиями стандарта EN 50174-2.

### 3.2.2 Обоснование выбора пассивного сетевого оборудования и аксессуаров

Пассивное сетевое оборудование - вид сетевого оборудования, которое, в отличии от активного, не питается от электросети и сигнал передаётся без усиления.

Оно разделяется между собой на две условные группы: оборудование, которое служит трактом передачи данных, и оборудование, которое представляет собой своеобразную трассу для кабелей. К первой группе в большинстве своем относятся: розетки, кабели и др. Ко второй группе: кронштейны, кабель каналы, клипсы и прочее оборудование.

Пассивное оборудование необходимо для работоспособности сети и для её эстетичного вида. С помощью розеток и коммутационных панелей достигается удобство подключения, с помощью кабель-каналов достигается красота размещения проводов на стенах, потолках и полу [13].

Расходные материалы помогают в процессе монтажа и демонтажа сети. Нейлоновые стяжки самый необходимый материал для работы с сетью, который помогает закрепить провода и стянуть их в единый пучок практически в любом месте.

Учитывая нестандартные длины кабелей Ethernet, необходимо их укоротить до нужной длины и сделать обжим витой пары.

Поскольку кабели, которые придется укорачивать, соединяют коммутаторы и персональные компьютеры, необходимо использовать вариант разводки, называющийся прямой кабель.

Из двух вариантов обжима витой пары был выбран вариант T568B, так как он является более распространенным.

### 3.2.3 Обоснование выбора активного сетевого оборудования

3.2.3.1 Расчет показателя использования сети.

Рассчитаем показатель использования сети. Этот параметр показывает процентное соотношение реальной нагрузки на сеть к максимальной пропускной способности оборудования. Для соблюдения требований отказоустойчивости этот параметр должен быть ниже 100%.

Для проведения расчетов и выводов следует рассчитать производительность в каждом сегменте сети.

Вычислим полезную нагрузку Pп (формула 2.1):

|  |  |
| --- | --- |
| , Мбит/с, | (2.1) |

где N – количество пользовательских станций в сегменте;

G1, G2 – производительность рабочей станции первого и второго видов соответственно;

R1, R2 – количество рабочих станций первого и второго видов, поддерживающих производительность G1 и G2 соответственно.

Pп = (54\*36)\*0,3 + (54\*18)\*0,3 = 583,2 + 291,6= 874,8 Мбит/с

Далее необходимо определить общую нагрузку Pо (формула 2.2):

|  |  |
| --- | --- |
| , Мбит/с, | (2.2) |

где n – количество сегментов проектируемой сети.

P0 = 874,8 \* 1= 874,8 Мбит/сек

Полная фактическая нагрузка Pф (формула 2.3) рассчитывается с учетом коллизий и величины задержек доступа к среде передачи данных:

|  |  |
| --- | --- |
| , Мбит/с, | (2.3) |

где к – задержка доступа к среде передачи данных: для семейства технологий Ethernet – 0,4, для Token Ring – 0,6, для FDDI – 0,7.

Рф = 874,8\*(1+0.4) = 876,2 Мбит/с

Так как фактическая нагрузка Pф > 10 Мбит/с, то, как и предполагалось ранее, данную сеть невозможно реализовать с помощью стандарта Ethernet, необходимо применить технологию Fast Ethernet (100 Мбит/с).

В связи с тем, что в данной сети мы не используем концентраторы, то рассчитывать время двойного оборота сигнала не требуется. Сигнал коллизий отсутствует.

3.2.3.2 Выбор соответствующего оборудования

Активное сетевое оборудование – это оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников и выполняющее функции усиления, преобразования сигналов и иные. Это означает способность такого оборудования обрабатывать сигнал по специальным алгоритмам. В сетях происходит пакетная передача данных, каждый пакет данных содержит также техническую информацию: сведения о его источнике, цели, целостности информации и другие, позволяющие доставить пакет по назначению.

Активное сетевое оборудование не только улавливает и передает сигнал, но и считывает техническую информацию, используя её для перенаправления и распределения поступающих потоков данных в соответствии с заложенными в устройство алгоритмами. Эта особенность, являются признаком активного сетевого оборудования.

Коммутаторы, концентраторы и другое подобное оборудование позволяет объединить несколько компьютеров в одну сеть, то есть образуют так называемое логическое соединение между устройствами. Маршрутизаторы, в свою очередь, распределяют пакеты данных по компьютерам, сегментам сети [2].

К активному оборудованию относятся:

Маршрутизатор (рис. 3.2) ‑ сетевое устройство, перенаправляющее пакеты данных в одной или нескольких подсетях в соответствие с некоторым заранее определенным принципом. В отличие от концентратора (хаба) и коммутатора (switch), которые просто соединяют компьютеры физической линией.



Рисунок 3.2. Маршрутизатор Cisco 2911

Характеристики маршрутизатора (рис.3.2):

- Поддержка Fiber optic, 802.3af PoE;

- Порты: 3x 10/100/1000 Ethernet;

- Защита информации: 64/128-битное WEP, WPA/WPA2, WPA-PSK/WPA2-PSK шифрование, фильтрация MAC-адресов;

- Температура: от -5 до 45⁰C;

- Влажность: от 5 до 95%.



Рисунок 3.3. Коммутатор Cisco SG220-50P 50-Port   
Gigabit PoE Smart Plus Switch

Выбор данного коммутатора (рис. 3.3) обусловлен тем, что он соответствует следующим характеристикам:

* Поддержка объединения оборудования в стек.
* Пропускная способность аппаратной шины стека – не менее 480 Гбит/с.
* Поддержка режима работы в качестве маршрутизирующего устройства.
* Поддержка режима работы в качестве коммутирующего устройства.
* Поддержка передачи пакетов размером не менее 9198 байт.
* Количество поддерживаемых VLAN-ов – не менее 4000 шт.
* Количество поддерживаемых MAC-адресов в MAC-таблице в режиме коммутирующего устройства – не менее 32000 шт.
* Количество поддерживаемых маршрутизирующих интерфейсов в режиме маршрутизирующего устройства – не менее 1000 шт.
* Возможность обеспечения работы беспроводной сети (режим агента и режим контроллера беспроводной сети).
* Количество поддерживаемых беспроводных сетей – не менее 64 шт.
* Поддержка протокола Control and Provisioning of Wireless Access Points (CAPWAP) для взаимодействия с беспроводными точками доступа.
* Поддержка протоколов агрегации физических интерфейсов Port Aggregation Protocol (PAgP) и Link Aggregation Control Protocol (LACP).
* Поддержка протокола Dynamic Trunking Protocol (DTP).
* Поддержка протокола Unidirectional Link Detection Protocol (UDLD).
* Поддержка протоколов класса Spanning Tree: IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), а также IEEE 802.1w Rapid Spanning-Tree для каждого VLAN-а в отдельности.
* Поддержка протоколов резервирования шлюза сети Hot Standby Router Protocol (HSRP) Virtual Router Redundancy Protocol (VRRP) как для IPv4-адресов, так и для IPv6-адресов.
* Поддержка протоколов маршрутизации Routing Information Protocol version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF).
* Поддержка протокола Flexible NetFlow на каждом физическом порту.

Количество поддерживаемых очередей на каждом физическом порту для обработки трафика – не менее 8 штук.

Поддержка протоколов аутентификации Terminal Access Controller Access-Control System Plus (TACACS+), RADIUS (Remote Authentication Dial-In User Service).

Точка доступа ‑ это беспроводная базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети (беспроводной или проводной) или создания новой беспроводной сети. Точки доступа призваны выполнять самые разнообразные функции, как для подключения группы компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные сети (режим Ad-hoc), так и для выполнения функции моста между беспроводными и кабельными участками сети (режим Infrastructure).



Рисунок 3.4. WiFi точка доступа Cisco AIR-CAP1602I

Самыми популярными стандартами для точек доступа являются Wi-Fi (IEEE 802.11) и Bluetooth. В технологии Bluetooth существует специальный профиль PAN (PersonalAreaNetwork) для этих целей.

WiFi точка доступа Cisco AIR-CAP1602I (рис. 3.4) является передовой технологией компании Cisco, предназначенной для небольшого и среднего бизнеса. Серию точек доступа Cisco Aironet 1600 выпустили на рынок в декабре 2012 года. До этого уже были представлены серии точек доступа Cisco Aironet 2600 и 3600, которые отличились высокой надежностью работы и теплыми отзывами пользователей. Cisco AIR-CAP1602I является неуправляемой. Другими словами, автономное управление в ней не предусмотрено, однако консольный порт для базовой настройки все же присутствует. AIR-CAP1602I управляется от общего контроллера. Это привносит дополнительные удобства при использовании нескольких точек доступа. При наличии контроллера не стоит переплачивать за автономные точки доступа, а все неавтономные точки можно полноценно настраивать с одного контроллера, не уходя с рабочего места. WiFi точка AIR-CAP1602I может содержать до 3 внутренних Wi-Fi антенн. Внутренние антенны имеют немного меньший радиус действия по сравнению с внешними, однако потребляют меньше мощности и точки доступа Cisco AIR-CAP1602I со встроенными антеннами лучше вписываются в общий дизайн помещения. Wi-Fi точка доступа поддерживает такие стандарты беспроводной передачи данных, как 802.11a, 802.11g, 802.11n. Стандарт 802.11b поддерживается для взаимосвязи со старыми беспроводными устройствами, однако открыто не анонсируется. Максимальная заявленная скорость при использовании технологии 3х3 MIMO составляет 300 Мбит/с.

3.2.4 Адресация в локальной сети

Адресация осуществляется с помощью протоколов IPv4 и IPv6. Сеть гостиницы разделена на три виртуальные сети:

* Сеть первого этажа – VLAN 101.
* Сеть второго этажа – VLAN 102.
* Сеть третьего этажа – VLAN 103.

В таблице 3.1 указаны номера виртуальных сетей и соответствующие им IP адреса и маски.

Таблица 3.1— Соответствие номеров виртуальных сетей IP адресам и маскам

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN № | ip address | subnet mask | IPv6 address |
| 101 | 192.168.1.0 | 255.255.255.0 | 2001:0aa8:2239:0101::/64 |
| 102 | 192.168.2.0 | 255.255.255.0 | 2001:0aa8:2239:0102::/64 |
| 103 | 192.168.3.0 | 255.255.255.0 | 2001:0aa8:2239:0103::/64 |

В таблице 3.2 указаны номера телевизоров и соответствующие им IP адреса и маски.

Таблица 3.2— Соответствие номеров хабов умного дома IP адресам и маскам

|  |  |  |  |
| --- | --- | --- | --- |
| hub № | ip address | subnet mask | IPv6 address |
| 1 | 192.168.1.11 | 255.255.255.0 | 2001:0aa8:2239:0101::b/64 |
| 2 | 192.168.1.12 | 255.255.255.0 | 2001:0aa8:2239:0101::c/64 |
| … | … | … | … |
| 5 | 192.168.2.12 | 255.255.255.0 | 2001:0aa8:2239:0102::c/64 |
| 6 | 192.168.2.13 | 255.255.255.0 | 2001:0aa8:2239:0102::d/64 |
| 7 | 192.168.2.14 | 255.255.255.0 | 2001:0aa8:2239:0102::e/64 |
| … | … | … | … |
| 17 | 192.168.3.17 | 255.255.255.0 | 2001:0aa8:2239:0103::10/64 |

В таблице 3.3 указаны другие устройства и соответствующие им IP адреса и маски.

Таблица 3.3— Адреса и маски маршрутизаторов и сервера.

|  |  |  |  |
| --- | --- | --- | --- |
| device | ip address | subnet mask | IPv6 address |
| Router 1 | 192.168.1.1 | 255.255.255.0 | 2001:0aa8:2239:0101::1/64 |
| Router 2 | 192.168.2.1 | 255.255.255.0 | 2001:0aa8:2239:0102::1/64 |
| Router 3 | 192.168.3.1 | 255.255.255.0 | 2001:0aa8:2239:0103::1/64 |
| Server | 192.168.4.1 | 255.255.255.0 | 2001:0aa8:2239:0104::1/64 |

Беспроводные устройства получают адреса из пулов адресов, предоставляемых точками доступа.

Провайдером предоставляется 4 IPv4 адреса. Для доступа всех устройств в глобальную сеть интернет на маршрутизаторе настраивается механизм NAT. Для этого в конфигурации маршрутизатора прописываются следующие команды:

Router#configure terminal

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)#ip nat pool vlan101pool 10.0.58.1 10.0.58.1 netmask 255.255.255.254

Router(config)#ip nat inside source list 1 pool vlan101pool

Router(config)#access-list 2 permit 192.168.2.0 0.0.0.255

Router(config)#ip nat pool vlan102pool 10.0.58.2 10.0.58.2 netmask 255.255.255.254

Router(config)#ip nat inside source list 2 pool vlan102pool

Router(config)#access-list 3 permit 192.168.3.0 0.0.0.255

Router(config)#ip nat pool vlan103pool 10.0.58.3 10.0.58.3 netmask 255.255.255.254

Router(config)#ip nat inside source list 3 pool vlan103pool

Router(config)#access-list 4 permit 192.168.4.0 0.0.0.255

Router(config)#ip nat pool serverpool 10.0.58.4 10.0.58.4 netmask 255.255.255.254

Router(config)#ip nat inside source list 4 pool serverpool

Router(config)#int fa0/0

Router(config-if)#ip nat outside

Router(config)#int range fa0/1-3

Router(config-if-range)#ip nat outside

Router(config-if-range)#end

cisco-wifi#write memory

Building configuration...

[OK]

# 4 ПРОЕКТИРОВАНИЕ СКС

Спроектировав расположение комнат на первом этаже, было принято решение отделить небольшую свободное пространство под лестничным пролетом, ведущим на второй этаж, под специальную комнату для активного сетевого оборудования такого, как маршрутизатор, сервер и коммутатор. Это позволит обеспечить лучшую безопасность для сети и скрыть дорогостоящее оборудование от лишних глаз.

На втором и третьем этажах коммутаторы будут располагаться в коридорах, однако для безопасности будут монтироваться в специальные стойки, оснащенные запорным устройством.

Планы этажей представлены в приложениях «В», «Г» и «Д».

## 4.1 Настройка и конфигурирование коммутатора Cisco SG220-50P Cisco Smart Plus PoE+.

Рассмотрим необходимые конфигурации элементов сети, представленных на схемах.

Коммутатор Cisco SG220-50P Cisco Smart Plus PoE+, устанавливается на всех этажах.

### 4.1.1 Монтаж.

Установить коммутатор можно двумя способами:

- Разместить коммутатор на плоской поверхности. Чтобы разместить коммутатор на столе, следует закрепить четыре резиновые ножки (входят в комплект поставки) на днище коммутатора.

- Монтировать коммутатор в стандартной стойке (высотой 1 RU).

Выбран способ монтажа коммутатора в стойку.

Советы по размещению:

- Температура окружающей среды — во избежание перегрева коммутатора не следует использовать его при температурах выше 50 °C.

- Воздушный поток — следует убедиться, что коммутатор окружает достаточный воздушный поток.

- Механическая нагрузка — следует убедиться, что коммутатор располагается ровно и устойчиво, чтобы избежать возникновения опасных условий.

- Перегрузка цепи — при включении коммутатора в розетку нужно следить за тем, чтобы цепь не оказалась перегруженной.

Информация для монтажа коммутатора в стойку:

- Коммутатор можно монтировать в стойку любого стандартного размера шириной около 48 см. Для коммутатора требуется пространство 1 RU, что эквивалентно высоте 44,45 мм.

### 4.1.2 Подключение к сети.

После того как коммутатор был вмонтирован, требуется подключить коммутатор к сети. Для этого необходимо:

1. Подключить кабель Ethernet к порту Ethernet на компьютере или другом сетевом устройстве.

2. Другой конец кабеля Ethernet соединить с одним из пронумерованных портов Ethernet на коммутаторе. Индикатор порта горит, когда подключенное устройство активно.

3. Повторить шаги Шаг 1 и Шаг 2 для каждого устройства, которое нужно подключить к коммутатору.

При подключении сетевых устройств не стоит превышать максимальную длину прокладки кабеля — 100 м. Устройства или локальная сеть будут готовы к эксплуатации примерно через минуту после подключения. Это нормальное поведение.

Устройство подключено к сети, теперь требуется произвести необходимые настройки.

Осуществлять доступ к коммутатору и управлять им можно двумя разными способами: по IP-сети при помощи веб-интерфейса или через порт консоли при помощи интерфейса командной строки коммутатора.

Далее будет производится настройка коммутатора через веб-интерфейс:

1. Включить компьютер и коммутатор.

2. Соединить компьютер с коммутатором. Можно подключиться к той же IP-подсети, которую использует коммутатор, соединив его с компьютером напрямую кабелем Ethernet либо через другие коммутаторы подключившись к той же локальной сети, в которой находится коммутатор. Можно также соединить компьютер с коммутатором из другой IP-подсети через один или несколько IP-маршрутизаторов.

3. Определить IP-адрес коммутатора.

a. Для доступа к коммутатору и управления им можно использовать сетевые средства и сервисы Cisco, в том числе утилиту сетевого обнаружения Cisco FindIT, которая позволяет автоматически определять все поддерживаемые устройства Cisco, находящиеся в одном сегменте локальной сети с компьютером. Можно получить информацию о текущем состоянии каждого устройства или запустить средство настройки продукта для просмотра и настройки параметров.

b. Определить IP-адрес, назначенный DHCP-сервером, обратившись с запросом к маршрутизатору или DHCP-серверу. Проверить работоспособность и доступность DHCP-сервера.

4. Настроить конфигурацию IP-адреса на своем компьютере.

a. Если коммутатор использует статический IP-адрес по умолчанию (192.168.1.254), выбрать свободный IP-адрес в диапазоне от 192.168.1.2 до 192.168.1.253.

b. Если IP-адреса будут назначены DHCP-сервером, проверьте его работоспособность и доступность с коммутатора и компьютера. Возможно, потребуется отключить и заново подключить устройства, чтобы они определили свои новые IP-адреса, полученные с DHCP-сервера.

5. Открыть окно веб-браузера. Ввести IP-адрес коммутатора в адресную строку и нажать клавишу Enter. При первой настройке http://192.168.1.254.

6. Когда откроется страница входа, выбрать язык веб-интерфейса и ввести имя пользователя и пароль. Имя пользователя по умолчанию — cisco. Пароль по умолчанию — cisco. Имена пользователей и пароли вводятся с учетом регистра.

7. Нажать Log In (Вход в систему). При первом входе в систему с именем пользователя и паролем по умолчанию откроется страница Change Password (Смена пароля).

8. Ввести новый пароль и подтвердить его. Пароль должен соответствовать стандартным правилам сложности, либо его можно временно выключить, выбрав Disable Password Strength Enforcement (Отключить требование надежного пароля).

9. Нажать кнопку Apply (Применить).

### 4.1.3 Настройка VLAN.

На активных портах необходимо настроить VLAN и настроить скоростной режим работы портов.

В меню VLAN Managment нужно выбрать Create VLAN, т.к. настроек для VTP нет, придется создавать VLAN-ы вручную. Далее нужно нажать кнопку add, ввести ID и имя, нажать Apply. VLAN создан. Аналогично можно добавить остальные VLAN, которые будут использоваться на данном коммутаторе (рисунок 4.1).

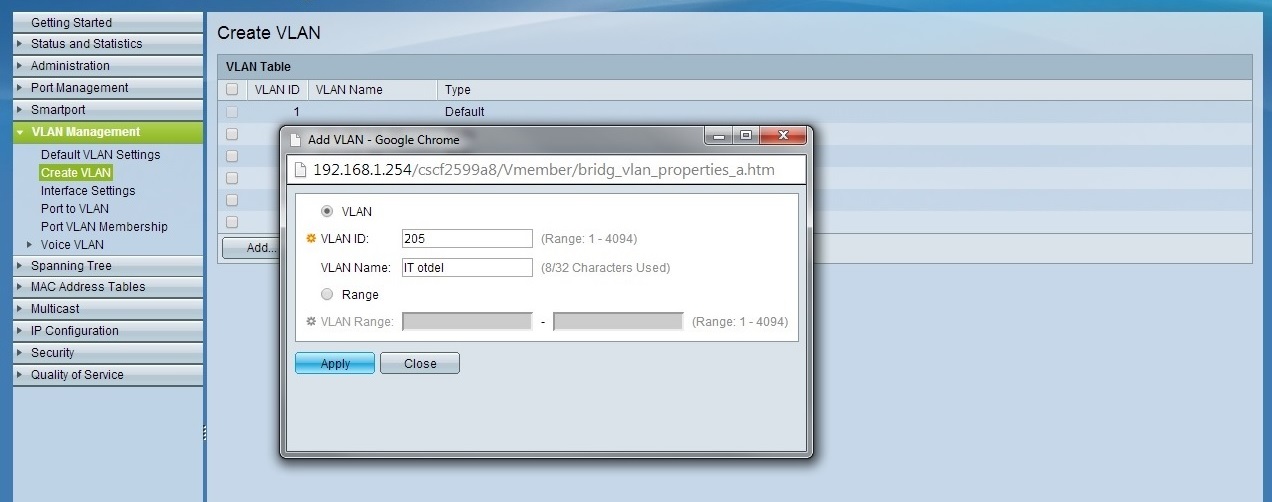


Рисунок 4.1. Создание VLAN

### 4.1.4 Настройка Trunk и Access портов.

Чтобы увидеть режим работы порта или поменять его, необходимо зайти в меню VLAN Managment, перейти на вкладку Interface Settings, выбрать необходимый порт, нажать Edit и настроить необходимый режим работы (рисунок 4.2).

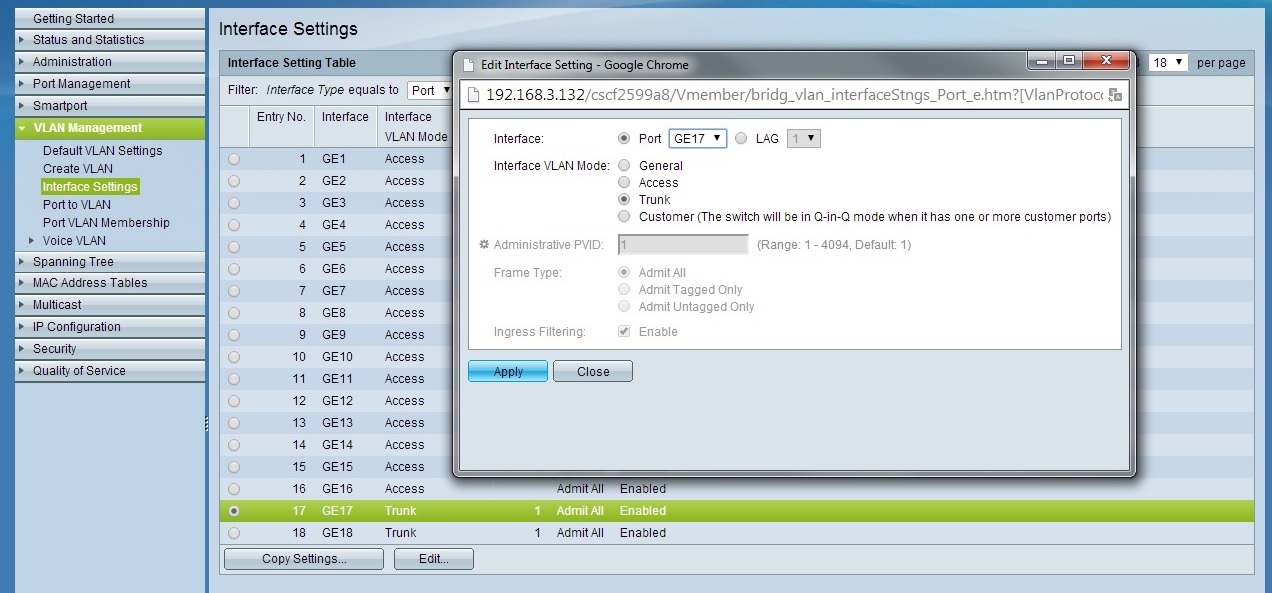


Рисунок 4.2. Редактирование настроек интерфейса

Чтобы связать VLAN с интерфейсом нужно зайти в меню VLAN Managment, перейти на вкладку Port to VLAN, выбрать необходимый VLAN в поле VLAN ID equals to, нажать Go. Переставить переключатель необходимого нам порта из Excluded в Untagged, также, если необходимо, чтобы пакеты переходили через Trunk порт переставить переключатель Trunk порта в режим Tagged из Excluded (рисунок 4.3)

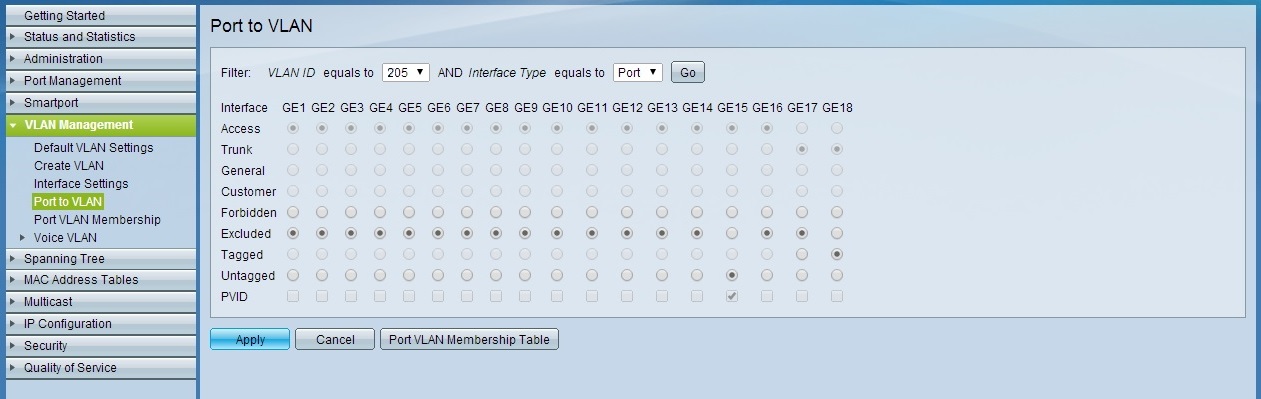


Рисунок 4.3. Связывание Port и VLAN

### 4.1.5 Настройка Host Name и Login Banner.

Зайти в меню Administration и выбрать пункт System Settings (рисунок 4.4). Изменить Host Name с Use Default на User Defined и назначить ему имя. Все, что будет введено в поле Login Banner, будет отображено на странице авторизации.

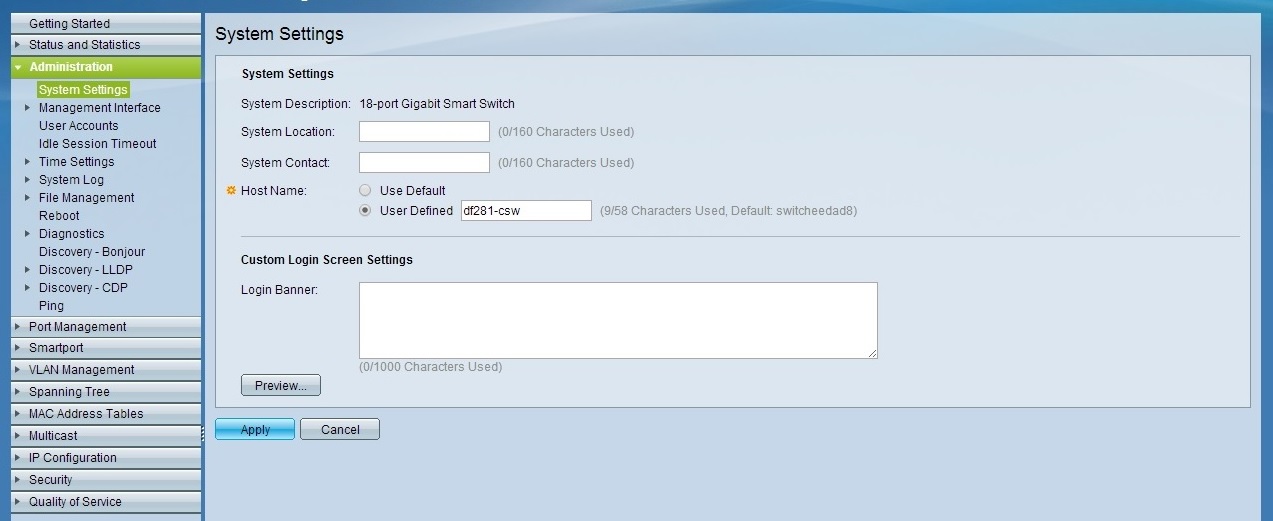


Рисунок 4.4. Настройка Host Name и Login Banner

### 4.1.6 Настройка IP-адреса устройства и управляющей VLAN сети.

Необходимо зайти в меню Administration, выбрать пункт Management Interface и перейти в IPv4 Interface (рисунок 4.5). В поле с выпадающим списком Management VLAN выбрать VLAN ID, в котором будет находиться данный коммутатор. Если адрес задается динамически, то дальше не нужно никаких настроек, иначе - переключить IP Address Type в Static и настроить IP-адрес коммутатора, маску и шлюз.

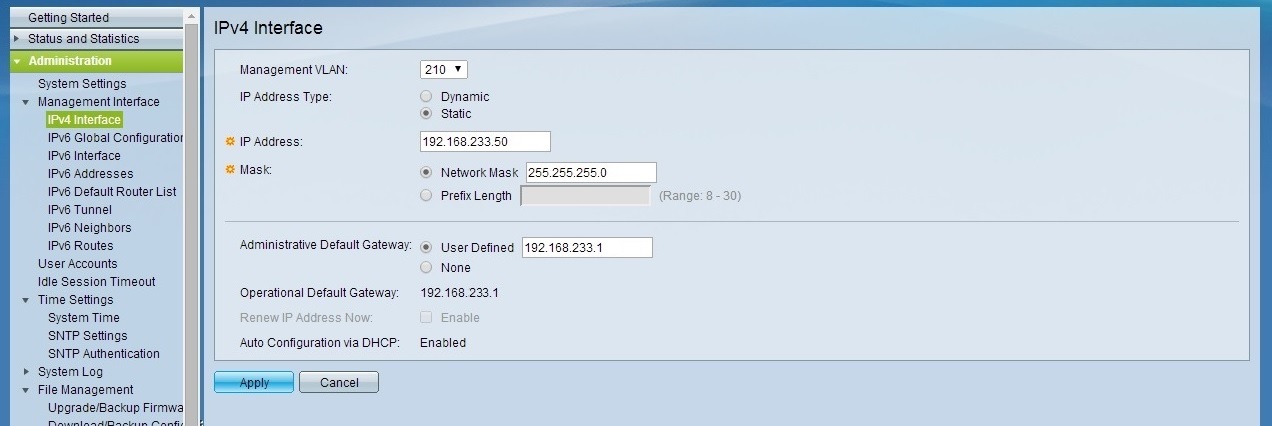


Рисунок 4.5. Настройка IP-адреса для VLAN

Далее необходимо записать Running configuration в Startup configuration и на этом настройка коммутатора завершена [14], [15].

## 4.2 Настройка и конфигурирование точки доступа Cisco AIR-CAP1602I.

Устанавливается на всех этажах. Необходимо настроить доступ к беспроводной сети, для чего выставим название данной сети «Hotel-1» и выставить настройки безопасности сети WPA2/PSK.

### 4.2.1 Монтаж.

Для данных точек доступа предусмотрено несколько вариантов монтажа: монтаж на подвесном потолке, на твердом потолке или стене, на электрощите или сетевой коробке, а также за подвесным потолком. Поскольку неизвестны заранее тонкости отделки помещений гостиницы, можно предположить размещение точек доступа на потолке или же за потолком, если он подвесной.

Для монтажа необходимо стандартное монтажное оборудование, представленное в таблице 4.1.

Таблица 4.1. Кронштейны и фиксаторы для монтажа точки доступа

|  |  |  |
| --- | --- | --- |
|  | Номер по каталогу | Описание |
| Кронштейны | AIR-AP-BRACKET-1 | Низкопрофильный наружный кронштейн |
| AIR-AP-BRACKET-2 | Универсальный кронштейн |
| Фиксаторы | AIR-AP-T-RAIL-R | Фиксатор для потолочной сетки (утопленный монтаж) |
| AIR-AP-T-RAIL-F | Фиксатор для потолочной сетки (монтаж заподлицо) |
| AIR-CHNL-ADAPTER | Дополнительный адаптер для швеллерных направляющих потолочной сетки. |

### 4.2.2 Конфигурирование.

Для начала следует сбросить все возможно сохраненные настройки. Для этого необходимо нажать на кнопку MODE на задней панели в углублении рядом с гнездом подключения консольного провода, и, не отпуская, подать на устройство электропитание. После того, как загорятся постоянным красным цветом (секунд через 20-ть) два светодиода System и Radio, отпустить кнопку. Произойдет сброс устройства до начальных установок, при этом логин пароль для входа в него станет стандартным: Cisco – Cisco (логин/пароль – регистрозависимы).

Далее необходимо подключить устройство с помощью консольного провода к компьютеру и войти в него. Для пущей надежности можно стереть содержимое nvram и перезагрузить устройство:

ap>enable

ap#erase nvram

ap#reload

Теперь необходимо задать hostname, domain name, сгенерировать ssh-ключи, сменить пароли, добавить/удалить пользователей:

ap#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ap(config)#hostname cisco-wifi

cisco-wifi(config)#ip domain name newdomain.ru

cisco-wifi(config)#crypto key generate rsa general-keys modulus 1024

The name for the keys will be: cisco-wifi.newdomain.ru

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

cisco-wifi(config)#

\*Mar 1 00:04:20.063: %SSH-5-ENABLED: SSH 1.99 has been enabled

cisco-wifi(config)#enable secret PASSWORD1

cisco-wifi(config)#username USER privilege 15 secret PASSWORD2

cisco-wifi(config)#no username Cisco

cisco-wifi(config)#exit

cisco-wifi#write memory

Building configuration...

[OK]

Присвоим интерфейсу BVI1 ip-адрес из подсети 192.168.1.0 вручную:

cisco-wifi#configure terminal

cisco-wifi(config)#interface BVI1

cisco-wifi(config-if)#ip address 192.168.200.38 255.255.255.0

cisco-wifi(config-if)#exit

cisco-wifi(config)#exit

cisco-wifi#write memory

Building configuration...

[OK]

В режиме конфигурирования зададим и настроим SSID (Service Set Identifier – уникальный идентификатор беспроводной сети). Присвоим нашей будущей сети имя NAME, включим авторизацию с помощью алгоритма шифрования wpa, установим ключ сети KEY (именно в таком виде, в каком его необходимо будет вводить при авторизации в Wi-Fi сети):

cisco-wifi#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

cisco-wifi(config)#dot11 ssid NAME

cisco-wifi(config-ssid)#authentication open

cisco-wifi(config-ssid)#authentication key-management wpa

cisco-wifi(config-ssid)#guest-mode

cisco-wifi(config-ssid)#wpa-psk ascii KEY

cisco-wifi(config-ssid)#exit

cisco-wifi(config)#

Настроим радио-интерфейс. Установим описание для интерфейса, укажем с каким SSID он должен работать, обозначим роль нашей беспроводной точки, «поднимем» интерфейс. Строкой speed basic-54.0 54.0 устанавливаются позволенные радио-скорости передачи данных.

cisco-wifi(config)#interface Dot11Radio1

cisco-wifi(config-if)#description WiFi

cisco-wifi(config-if)#encryption mode ciphers tkip

cisco-wifi(config-if)#ssid NAME

cisco-wifi(config-if)#speed basic-54.0 54.0

cisco-wifi(config-if)#station-role root access-point

cisco-wifi(config-if)#no shutdown

cisco-wifi(config-if)#exit

cisco-wifi(config)#exit

cisco-wifi#write memory

Building configuration...

[OK]

Точка доступа готова к работе. Осталось с помощью какого-нибудь устройства обнаружить настроенную сеть и подключиться к ней [16].

## 4.3 Настройка и конфигурирование маршрутизатора Cisco ME4624-ONT-RGW

Устанавливается на первом этаже.

Схема подключения приведена на рисунке 4.6.

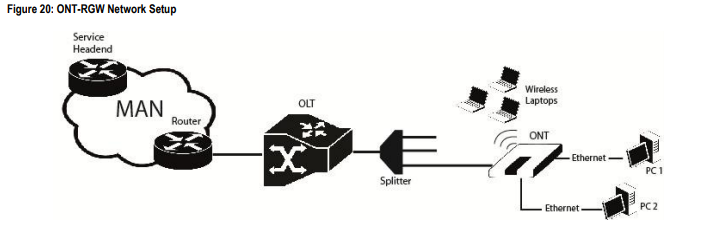


Рисунок 4.6. Схема подключения

Чтобы сконфигурировать данное устройство переходим в браузере по адресу 192.168.1.1. Далее требуется войти как администратор. Для этого вводим Login: admin, Password: admin (рисунок 4.7).

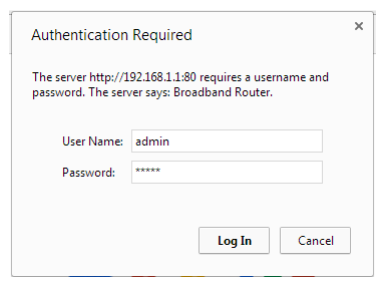


Рисунок 4.7. Аутентификация

* 1. Настройка веб-сервера.

Проведем настройку веб-сервера. Для начала включаем компоненты службы IIS в операционной системе Windows. Требуется включить Службы Интернет и Средства управления веб-сайтом. Используя Средства управления веб-сайтом, в дальнейшем можно подключаться к веб-серверу с другого устройства, на котором установлен клиент управления IIS, и осуществлять удаленное администрирование. Используя Диспетчер служб IIS устанавливаем необходимые компоненты веб-сервера (например, php + SQL сервер). Диспетчер служб IIS автоматически устанавливает и интегрирует выбранные версии продуктов.

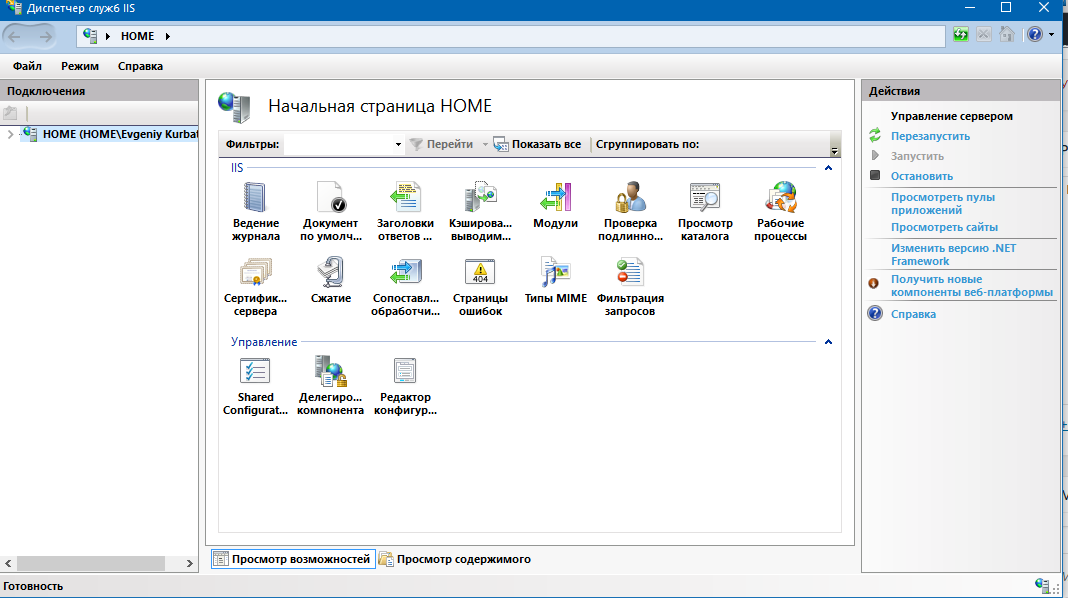


Рисунок 4.8. Диспетчер служб IIS

Также нам нужно произвести настройку PPP протокола (рис.4.9), указать VLAN идентификатор, выбрать протокол сети и произвести другие настройки WAN сервиса [14].

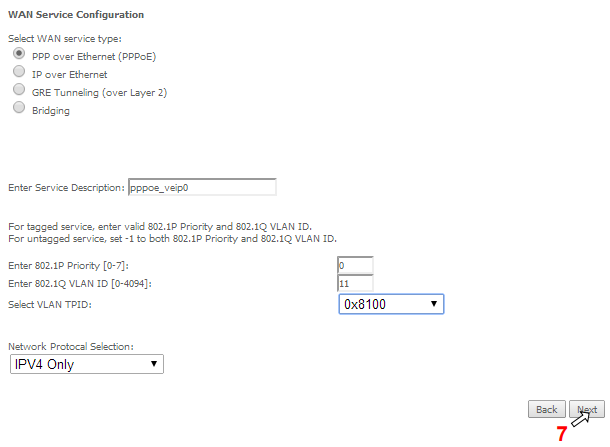


Рисунок 4.9. Настройка PPP протокола

# ЗАКЛЮЧЕНИЕ

Информатизация общества предлагает доступ к тем ресурсам, которые благодаря интеграции становится общественным достоянием. Такой доступ, не зависящий от расстояний до источника информации, возможен потому, что существует LAN - локальные сети, решающие проблемы транспорта данных. Сети обеспечивают возможность совместной работой над документами, оперативность принятий управленческих решений, доступ к глобальной сети Internet. Сегодня успех работы организации во многом будет зависеть от того, будет ли устойчиво работать её сеть или нет.

При выполнении проекта организации локальной вычислительной сети трехэтажной гостиницы был разработан проект сети, соответствующий всем требованиям задания. Были проанализированы все помещения, в которых проходила сеть, т. е. выбраны места для размещения сетевого оборудования: веб-сервера, маршрутизатора, коммутаторов, точек доступа wi-fi, коммутационных розеток, проводной сети. Дорогостоящее оборудование, такое как веб-сервер, маршрутизатор и коммутатор первого этажа, были размещены в отдельном помещении, предназначенном специально для их размещения. Были настроены и сконфигурированы активные устройства, находящиеся в локальной сети. Соблюдена адресация провайдера, а именно все пользователи получают доступ в глобальную сеть интернет по четырем предоставляемым IPv4 адресам с помощью механизма NAT. Поставленная цель выполнена в полном объёме

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации / В.Л. Бройдо. – 2-е изд. – СПб.: Питер, 2008. – 703 с.
2. Кузин А.В. Компьютерные сети / А.В. Кузин, В.М. Деминю. – М.: Инфра-М, 2005. – 192 с.
3. [Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы](http://www.internet-biblioteka.ru/67-olifer-kompyuternye-seti.html) / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с.
4. Руденков Н. А. Основы сетевых технологий / Н. А. Руденков, Л. И. Долинер. – Екатеринбург: УрФУ, 2014. – С. 27-30.
5. Семенов А.Б. Проектирование и расчет структурированных кабельных систем и их компонентов / А.Б. Семенов – М.: ДМК Пресс Компания АйТи, 2016. – 416 с.
6. Семенов А.Б. Структурированные кабельные системы / А.Б.Семенов, С.К. Стрижаков, И.Р. Сунчелей. – М.: ДМК Пресс Компания АйТи, 2014. – 482 с.
7. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – СПб.: Питер, 2003. – 992 с.
8. Чекмарев Ю. В. Локальные вычислительные сети / Ю. В. Чекмарев. –М.: ДМК-Пресс, 2014. – 250 с.
9. Нагибин П. Выбор топологии сети в реальных условиях [Электронный ресурс] / П. Нагибин. – Режим доступа: http://citforum.ru/nets/hard/street/
10. Проектирование локальной вычислительной сети (ЛВС) [Электронный ресурс]. – Режим доступа: https://mosproject-eng.ru/proektirovanie-lvs.html.
11. Проектирование локальной сети [Электронный ресурс]. – Режим доступа: https://2hpc.ru/проектирование-локальной-сети/
12. Уровни модели OSI [Электронный ресурс]. – Режим доступа: http://nastroyvse.ru/net/inter/urovni-modeli-osi.html
13. Шашлов С. Азбука сисадмина [Электронный ресурс] / С. Шашлов. – Режим доступа: <https://www.ixbt.com/editorial/sysadmin/bible-black-0.shtml>.
14. CISCO DATASHEET [Электронный ресурс]. – Режим доступа: <https://www.cisco.com>
15. Настройка коммутаторов CISCO [Электронный ресурс] – Режим доступа: <https://r.edbox.ru/настройка-коммутаторов>
16. Настройка точки доступа CISCO [Электронный ресурс] / М. Боголепов – http://www.maxblogs.ru/articles/nastroika-tochki-dostupa-cisco-air-ap1252g-a-k9

ПРИЛОЖЕНИЕ А

(обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б

(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В

(обязательное)

План первого этажа

ПРИЛОЖЕНИЕ Г

(обязательное)

План второго этажа

# ПРИЛОЖЕНИЕ Д

(обязательное)

План третьего этажа

ПРИЛОЖЕНИЕ Е

(обязательное)

Перечень оборудования, изделий и материалов