3.5 Описание настройки компонентов локальной сети

3.5.1 Настройка коммутатора

Для достижения большей степени административного контроля и логического разделения среды передачи данных было принято решение разделить устройства, подключенные к сети, на две группы: серверное оборудование и оборудование администраторов.

Для создания и настройки административного VLAN на коммутаторе необходимо создать его и назначить порты, к которым подключены конечные устройства, access портами с указанием номера VLAN.

Команды настройки VLAN №99 в Cisco IOS по алгоритму, описанному выше, выглядит так:

```
Switch(config)#vlan 99
Switch(config)#interface range g0/4-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
```

Аналогично конфигурируется VLAN №10 для серверной комнаты, разница в номере VLAN и в диапазоне интерфейсов (`interface range g0/1-3`).

Интерфейс g0/8, к которому подключена беспроводная точка доступа, необходимо назначить trunk портом и разрешите прохождение тегированного трафика VLAN №99:

```
Switch(config)#interface g0/8
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 99
```

Для настройки Inter-VLAN маршрутизации необходимо назначить порт, идущий к маршрутизатору, trunk портом и разрешить прохождение по нему тегированного трафика для 10 и 99 VLAN:

```
Switch(config)#interface g0/9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10, 99
```

На интерфейсе g0/7, к которому подключен принтер через порт f0, можно ограничить пропускную способность интерфейса для предотвращения некорректной работы:

```
Switch(config)#interface g0/7
Switch(config-if)#speed 1000
Switch(config-if)#srr-queue bandwidth limit 10
```

Для настройки сервера RADIUS необходимо перейти во вкладку «Network Resources», выбрать там подкатегорию «AAA», далее «AAA Servers and Groups», затем выбрать «Servers». Откроется список созданных серверов. Для создания нового сервера необходимо нажать кнопку «Add» и настроить новый сервер: выбрать тип сервера «RADIUS», назначить IP сервера 172.17.2.14, проверить порт авторизации и порт аккаунтинга (обычно это 1645 и 1646, стандартные порты для Cisco, рекомендуется использовать именно эти порты) и задайте ключ конфигурации («config_key_XcQ»). По нажатию «ОК» начинается процесс создания сервера, окно становится неактивно. В случае успешного создания сервера окно конфигурирования закроется, новый RADIUS-сервер появится в списке серверов.

Для управления пользователями необходимо нажать на вкладку «Users and Identity Stores», затем «Internal Identity Stores» и «Users». Для создания и добавления пользователя необходимо кликнуть на кнопку «Create» (рисунок 3.4).

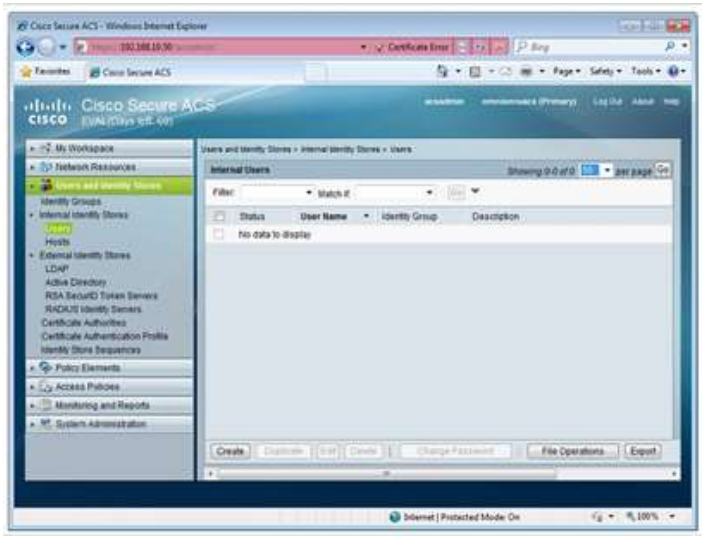

Рисунок 3.4 – Список пользователей в Cisco Secure ACS

Далее необходимо заполнить имя пользователя, выставить статус «Enabled» и ввести пароль пользователя (рисунок 3.5). При необходимости можно заполнить описание пользователя и определить для него группу, но для маленькой сети это имеет не много смысла.

По нажатию на кнопку «Submit» создание пользователя будет завершено, окно будет закрыто, отобразится список всех пользователей (рисунок 3.6). На этом процесс создания пользователя завершается.

На вкладке «General» необходимо ввести SSID точки доступа («Admin Wi-Fi»), VLAN ID (10), шлюз по умолчанию (172.17.0.1), IP-адрес точки доступа в рамках подсети в текстовом поле «Internet IP Address» (172.17.0.6) и адрес внутри WAN в текстовом поле «Router IP Address» (172.17.1.1).

Перейдём к настройке шифрования, для этого нужно перейти на вкладку WLAN и выбрать «Create New». В открывшемся окне нужно выбрать вкладку «Security», в ней «Layer 2». В окне настройки безопасности выбрать тип шифрования «WPA+WPA2», отметить чекбокс «WPA2 Policy-AES» и «802.1X Enable» (рисунок 3.7).

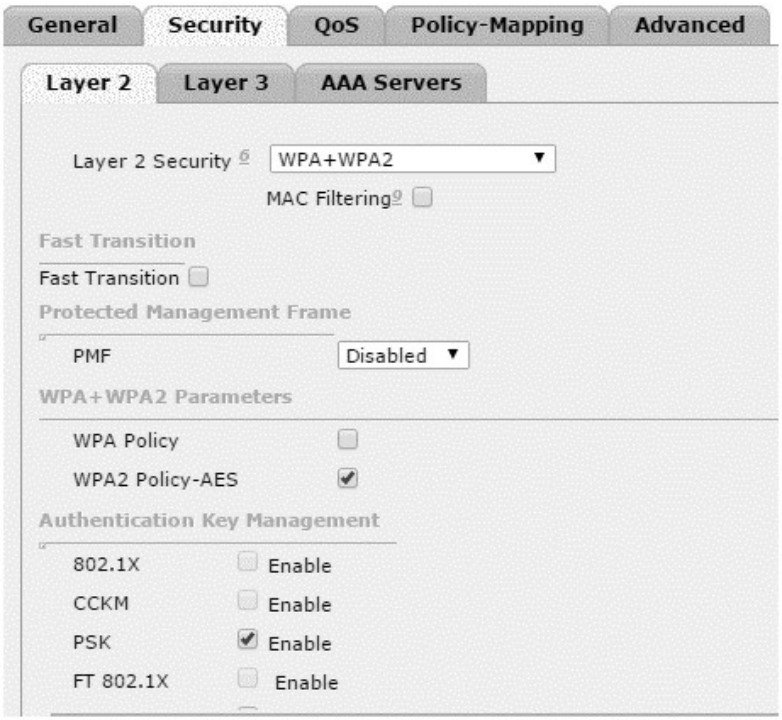

Рисунок 3.7 – Окно настройки WLAN

Далее необходимо настроить доступ к AAA-серверу на беспроводной точке доступа. Для этого, не покидая вкладки «Security», следует нажать на вкладку «AAA Servers», выбрать вид аутентификации «RADIUS Authentication», кликнуть «New», после чего перейти к настройке сервера (рисунок 3.8).

Здесь необходимо указать IP-адрес RADIUS-сервера (172.17.2.14), ввести ключ RADUIS-сервера («config_key_XcQ»), изменить порт по умолчанию на порт 1645, проверить статус сервера и после этого нажать «ОК».

Для автоматического назначения IP-адресов подключаемым устройствам нужно настроить работу DHCP. DHCP – это протокол, позволяющий раздавать IP-адреса подключаемым устройствам. Он позволяет упростить процесс выдачи адресов, перекладывая эту работу на сторону сервера.

Рисунок 3.8 – Окно настройки RADIUS-сервера

Точка доступа Cisco Aironet 1602I поддерживает протокол DHCP, для его настройки также необходимо воспользоваться графическим интерфейсом пользователя. Во вкладке «General» необходимо пролистать вниз до «DHCP Server Settings». В окне настройки нажать кнопку «Enable» напротив «DHCP Server», выбрать начальный IP-адрес для раздачи (172.17.1.5), и выбрать максимальное количество пользователей (с учётом размеров сети десяти пользователей будет достаточно).

На этом настройка беспроводной точки доступа закончена.

3.5.5 Настройка принтера

Для подключения принтера к локальной сети необходимо подключиться к нему с административной станции при помощи USB-кабеля и запустить установку драйверов с установочного диска, идущего в комплекте. В окне с предложением выбрать тип подключения выберите «Сетевое подключение» (рисунок 3.9).

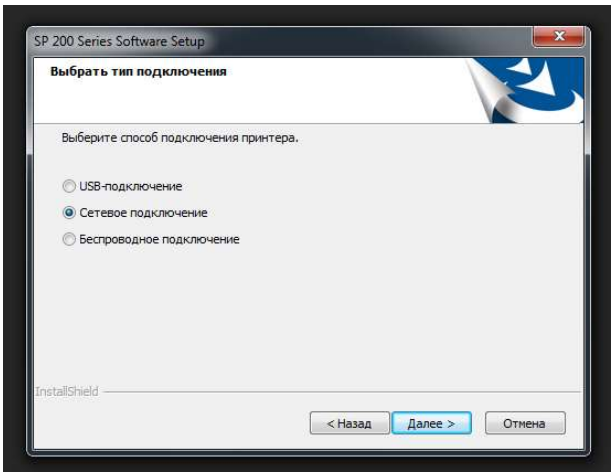

Рисунок 3.9 – Выбор типа подключения принтера

Для реализации Inter-VLAN Routing на интерфейсе маршрутизатора необходимо:

1. Создать подинтерфейсы для каждого VLAN.
2. Определить стандарт инкапсуляции.
3. Задать подинтерфейсу соответствующий IP-адрес.

Полный набор команд для настройки Inter-VLAN Routing выглядит следующим образом:

```
Router#configure terminal
Router(config)#interface g0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 172.17.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface g0/0.99
Router(config-subif)#encapsulation dot1q 99
Router(config-subif)#ip address 172.17.0.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface g0/1
Router(config-if)#no shutdown
Router(config-if)#exit
```

Для маршрутизации пакетов в подсеть 172.17.1.0/24 необходимо настроить на роутере путь в подсеть.

```
Router(config)#ip route 172.17.1.0 255.255.255.0 172.17.0.6
```

3.6 Адресация в локальной компьютерной сети

По условию задания в разрабатываемой ЛКС необходимо осуществить адресацию с применение протоколов IPv4 и IPv6. Протокол адресации IPv4 использует четырёхбайтные адреса, ограничивающие адресное пространство. Традиционно адрес IPv4 записывается четырьмя десятичными числами от 0 до 255, разделёнными точками, через дробь указывается длина маски подсети. Однако данный вид адресации столкнулся с проблемой исчерпания адресов. В ноябре 2019 года были распределены последние IPv4 адреса в Европе, странах бывшего СССР и на Ближнем Востоке. Решить эту проблему призвана новая версия протокола – IPv6. Протокол IPv6 отличается от своего предшественника использованием увеличенной в 4 раза длиной адреса. В связи с исчерпанием IPv4 адресов продвижение новой версии протокола началось активнее.

Сеть разделена на 2 виртуальные подсети:

1. VLAN №99 – административная подсеть.
2. VLAN №10 – серверная подсеть.

IPv6 адреса нужны лишь для некоторых приложений администраторов на их рабочих станциях, поэтому можно назначить эти адреса только на персональных компьютерах администраторов.