Лабораторная работа №7 Исследование сложной беспроводной сети Wi-Fi с сегментацией, roaming и безопасностью

1. Тема

Проектирование и исследование сложной корпоративной беспроводной сети Wi-Fi с сегментацией трафика, обеспечением roaming и многоуровневой безопасностью в Cisco Packet Tracer.

2. Цель работы

- **Теоретическая:** Изучить архитектуру корпоративных Wi-Fi сетей, принципы сегментации (VLAN), механизмы быстрого и безопасного roaming (802.11r/k), а также современные методы обеспечения безопасности (WPA3, изоляция клиентов).
- **Практическая:** Приобрести навыки проектирования многослойной беспроводной сети, настройки нескольких SSID с разным уровнем доступа, оптимизации радиоканалов и диагностики проблем в беспроводной среде.

3. Задачи

1. Спроектировать и построить физическую и логическую топологию корпоративной Wi-Fi сети для трехэтажного офиса.
2. Настроить контроллер беспроводной сети (WLC) в режиме автономного или на базе роутера.
3. Настроить несколько беспроводных точек доступа (WAP) с поддержкой roaming между ними.
4. Создать и настроить три отдельных SSID (Service Set Identifier) для различных групп пользователей с привязкой к разным VLAN.
5. Настроить многоуровневую систему безопасности для каждого SSID.
6. Реализовать проводную инфраструктуру (коммутаторы, маршрутизатор) для поддержки беспроводных клиентов и серверов.
7. Провести всестороннюю диагностику и тестирование работы сети, включая анализ roaming, безопасность и производительность.
8. Смоделировать и устранить типовые неисправности в беспроводной сети.

4. Оборудование и программное обеспечение

- **Программное обеспечение:** Cisco Packet Tracer (версия, поддерживающая беспроводные устройства).
- **Оборудование (в эмуляторе):**
  - **Беспроводное:**
    - Точки доступа Cisco (например, `PT-Host-NM-1W`) или беспроводные маршрутизаторы (`Wireless Router`) – 3-4 шт. (имитируют точки доступа на разных этажах).
    - Беспроводные конечные устройства (ноутбуки, смартфоны) – не менее 4 шт.
  - **Проводное:**
    - Многоуровневый коммутатор (`Switch-PT`) или коммутатор уровня L3 – 2 шт. (распределенный и ядровой).
    - Маршрутизатор (`Router-PT`) – 1-2 шт. (для выхода в интернет и межVLAN маршрутизации).
    - Сервер (`Server-PT`) – 2 шт. (DNS/DHCP-сервер, сервер аутентификации).
  - Кабельная инфраструктура.

5. Теоретическое введение (Ключевые аспекты для исследования)

- **SSID и VLAN:** Один физический AP может транслировать несколько логических беспроводных сетей (SSID), каждая из которых связана с отдельным VLAN для изоляции трафика (сотрудники, гости, IoT-устройства).
- **Безопасность Wi-Fi:**
  - **WPA2/WPA3-Enterprise:** Использование сервера RADIUS (например, на базе встроенных возможностей маршрутизатора или отдельного сервера) для индивидуальной аутентификации пользователей по логину/паролю или сертификатам.
  - **WPA2/WPA3-Personal:** Использование общего пароля (PSK) для менее критичных сетей.
  - **Изоляция клиентов:** Функция, предотвращающая прямое взаимодействие беспроводных клиентов друг с другом в рамках одного SSID.
- **Roaming (Беспрерывный переход):** Механизм, позволяющий клиенту перемещаться между зонами покрытия разных AP, сохраняя активные сессии. Зависит от совпадения SSID, типа безопасности и правильной настройки VLAN.
- **Планирование радиоканалов:** Распределение неперекрывающихся каналов (1, 6, 11 для 2.4 ГГц) между соседними AP для минимизации интерференции.
- **Контроллер беспроводной сети (WLC):** В Packet Tracer его роль часто имитируется настройками на маршрутизаторе или коммутаторе. Концептуально

он централизованно управляет AP, политиками безопасности и roaming.

6. Сценарий и порядок выполнения работы

Сценарий: Вы - сетевой инженер IT компании. Вам необходимо развернуть безопасную Wi-Fi сеть в новом трехэтажном офисе. Требования:

1. Сеть для сотрудников (SSID: `Corp-Net`): Высокий уровень безопасности (WPA2-Enterprise), доступ к внутренним ресурсам (сервер).
2. Гостевая сеть (SSID: `Guest-Net`): Изолированный доступ только в Интернет, аутентификация по паролю (WPA2-Personal), клиенты не должны "видеть" друг друга.
3. Сеть для IoT устройств (SSID: `IoT-Net`): Отдельный, сильно ограниченный сегмент.
4. Обеспечить беспрерывный Wi-Fi (roaming) для сотрудников при перемещении между этажами.
5. Все беспроводные сети должны быть привязаны к отдельным VLAN.

Этап 1: Проектирование и построение топологии

1. Создайте физическую схему: разместите 3 точки доступа (AP1, AP2, AP3), имитируя их расположение на разных этажах. Разместите коммутаторы, маршрутизатор, серверы и беспроводных клиентов.
2. Создайте логическую схему сети, продумав IP-адресацию и VLAN:
   - VLAN 10 (Сотрудники): 192.168.10.0/24
   - VLAN 20 (Гости): 192.168.20.0/24
   - VLAN 30 (IoT): 192.168.30.0/24
   - VLAN 99 (Management): 172.16.99.0/24 (для управления сетевым оборудованием)

Этап 2: Настройка проводной инфраструктуры

1. **На маршрутизаторе (выполняет роль шлюза, межVLAN маршрутизатора и упрощенного контроллера):**
   - Настройте интерфейсы (порт к коммутатору - trunk, порт к WAN).
   - Создайте сабинтерфейсы для VLAN 10, 20, 30, 99 и назначьте им IP-адреса (шлюзы по умолчанию).
   - Настройте DHCP-пулы для каждой из пользовательских VLAN.
   - Настройте статический маршрут/NAT для выхода в Интернет (имитацию WAN можно сделать через Cloud).
2. **На коммутаторе уровня L3 (ядро):**
   - Создайте VLAN 10, 20, 30, 99.

- Настройте SVIs (интерфейсы VLAN) с IP-адресами и активируйте их.
- Настройте межVLAN маршрутизацию (если не используется маршрутизатор).

3. **На коммутаторах доступа:**
   - Создайте необходимые VLAN.
   - Настройте порты, подключенные к AP, в режиме **trunk** и разрешите прохождение всех пользовательских VLAN и управляющего VLAN.
   - Порт, подключенный к коммутатору ядра, также настройте как trunk.

Этап 3: Настройка беспроводной инфраструктуры

1. **На каждой точке доступа (AP):**
   - **Физическое подключение:** Подключите AP к коммутатору доступа через порт, настроенный как trunk.
   - **Настройка в графическом интерфейсе (GUI) Packet Tracer:** Перейдите на вкладку `Wireless` для каждого AP.
   - **SSID 1 (`Corp-Net`):**
     - SSID Name: `Corp-Net`
     - Network Mode: `WPA2-Enterprise` (в Packet Tracer часто реализован через `WPA2` с указанием RADIUS-сервера). В поле `RADIUS Server` укажите IP-адрес вашего маршрутизатора или сервера.
     - VLAN: `10`.
   - **SSID 2 (`Guest-Net`):**
     - SSID Name: `Guest-Net`
     - Network Mode: `WPA2-Personal`. Установите сложный пароль.
     - Включите опцию **Client Isolation** (Изоляция клиентов), если доступна.
     - VLAN: `20`.
   - **SSID 3 (`IoT-Net`):**
     - SSID Name: `IoT-Net`
     - Network Mode: `WPA2-Personal` (с другим паролем).
     - VLAN: `30`.
   - **Радионастройки:** Для AP1 установите канал 1 (2.4 ГГц), для AP2 - канал 6, для AP3 - канал 11. Мощность передатчика можно установить на средний уровень. Убедитесь, что все AP транслируют одни и те же три SSID с одинаковыми настройками безопасности.
2. **Настройка беспроводных клиентов:** На каждом беспроводном устройстве (ноутбук, телефон) выберите нужный SSID и введите соответствующие учетные данные (пароль для Guest/IoT).

Этап 4: Диагностика, тестирование и моделирование неисправностей

1. **Базовое тестирование:**

- С клиента в `Corp-Net` выполните `ping` на шлюз (VLAN 10), на внутренний сервер, на публичный IP (8.8.8.8). Убедитесь в доступности.
- С клиента в `Guest-Net` выполните `ping` на шлюз (VLAN 20) и 8.8.8.8. Попытка `ping` клиента в `Corp-Net` должна завершиться неудачей (изоляция).

2. **Исследование Roaming:**
   - Поместите два ноутбука сотрудника (`Corp-Net`) в зону покрытия AP1 и AP3.
   - Начните непрерывный `ping` с одного ноутбука на другой.
   - В **режиме симуляции (Simulation)** физически переместите (перетащите) ноутбук из зоны AP1 в зону AP3.
   - **Задание:** Проследите в Simulation, какие кадры передаются во время перемещения. Зафиксируйте, теряются ли ICMP-пакеты (пинги) и на какое время. Объясните, почему roaming сработал или не сработал идеально. Сделайте вывод о необходимости настройки 802.11r/k (которая в PT может быть недоступна).

7. Контрольные вопросы:

1. Объясните разницу между режимами безопасности WPA2-Personal и WPA2-Enterprise. В каком сценарии предпочтительнее каждый из них?
2. Почему для портов, подключенных к точкам доступа, необходимо использовать режим **trunk**, а не **access**?
3. Каким образом достигается изоляция трафика между гостевой сетью и сетью сотрудников на **беспроводном** и **проводном** уровнях?
4. Опишите по шагам процесс, который происходит в сети, когда ноутбук сотрудника, подключенный к `Corp-Net`, пытается открыть сайт google.com (DHCP, ARP, DNS, маршрутизация, NAT).
5. Что такое "co-channel interference" (совмещаемая помеха) и как правильное планирование каналов помогает ее избежать в вашей спроектированной сети?
6. Какие факторы в Packet Tracer ограничивают реализацию "идеального" seamless roaming, и как эта проблема решается в реальном оборудовании (упомяните 802.11r, k, v)?
7. Предложите архитектурное решение, если бы точек доступа было не 3, а 30. Как изменилась бы роль маршрутизатора и коммутаторов?

8. Содержание отчета

1. **Цель и задачи работы.**
2. **Физическая и логическая схемы сети** (скриншоты из PT и нарисованная схема с IP-адресацией и VLAN).

3. **Конфигурации ключевых устройств** (выдержки из running-config маршрутизатора и коммутатора или скриншоты основных настроек из GUI).
4. **Результаты этапа тестирования:**
    - Таблица с результатами ping-тестов между различными сегментами сети.
    - Скриншот процесса roaming из режима Simulation с описанием наблюдений и выводов.
    - Описание действий по диагностике и устранению смоделированных неисправностей.
5. **Ответы на контрольные вопросы.**
6. **Выводы:** Обобщение полученных навыков, оценка адекватности инструментов Packet Tracer для моделирования сложных Wi-Fi сценариев, предложения по улучшению спроектированной сети.