4️⃣ LabWork4

Контроллер + легковесные точки доступа.

Перейти на более новую версию Cisco Packet Tracer 8.0.

Более ходовая версия WLC — 2504.

Контроллер надо располагать как можно ближе к точкам доступам.

Точки доступа непосредственно к контроллеру подключать не надо, они подключаются к коммутатору.

Защита веб-интерфейса и т.п., как в третьей лабе, не прописана в требованиях, но подразумевается, ибо иначе не получится.

Источники

https://www.packettracernetwork.com/tutorials/pt71-wlc-configuration.html#:~:text=Connect to the WLC 2504,HTTPS%2C for this first connection.

https://youtu.be/QrwN_I_t558?si=DoicnL23EjvAjQLz

https://www.youtube.com/watch?v=ZBTEC35f6eY&t=372s

Теория

Легковесные точки доступа (Lightweight Access Points, LAP) — это точки доступа, которые функционируют как часть централизованной беспроводной сети, управляемой контроллером беспроводной локальной сети (Wireless LAN Controller, WLC). Они отличаются от автономных (или «толстых») точек доступа тем, что значительная часть их функциональности передается на контроллер, а сами устройства выполняют минимальные операции.

Active Rogue APs (Активные Rogue точки доступа) — это несанкционированные или нежелательные точки доступа, обнаруженные в сети, которые активно передают данные или пытаются взаимодействовать с устройствами в пределах вашего беспроводного окружения.

Ad-hoc — точка-точка.

Authentication Key Management (AKM) — 802.1X — это метод управления ключами аутентификации, который используется в беспроводных сетях для обеспечения безопасного доступа. Он основан на стандарте IEEE 802.1X и применяется в корпоративных беспроводных сетях, где требуется высокая степень безопасности.

NAC (Network Access Control) — это система, которая управляет доступом устройств к сети, обеспечивая соблюдение политик безопасности. NAC определяет, какие устройства могут подключаться к сети, какие ресурсы им доступны и при каких условиях.

Dynamic AP Management — это механизм, который позволяет точкам доступа взаимодействовать с контроллером через выделенные IP-интерфейсы (динамические интерфейсы). Динамический интерфейс используется для:

1. Передачи управляющих сообщений между точками доступа и контроллером (например, настройка параметров, обновление прошивки).
2. Подключения точек доступа к контроллеру в процессе регистрации.
3. Разгрузки трафика между точками доступа и контроллером для масштабирования сети.

CAPWAP-запрос (Control and Provisioning of Wireless Access Points) — это сообщение, отправляемое точкой доступа (Access Point, AP) к контроллеру беспроводной сети (Wireless LAN Controller, WLC) в процессе настройки, управления или обмена данными. Работает на основе UDP**.**

FlexConnect — это режим работы точек доступа (Access Points, AP) в сети с контроллером беспроводной сети (**WLC**, Wireless LAN Controller). Он позволяет точкам доступа продолжать предоставлять услуги даже при потере соединения с контроллером.

Local Switching (Локальная коммутация) — точки доступа могут направлять пользовательский трафик напрямую в локальную сеть филиала, минуя контроллер.

Local Authentication (Локальная аутентификация) — точки доступа могут выполнять аутентификацию клиентов локально, без передачи данных на контроллер.

Выполнение работы

▼ Беспроводной контроллер 2504 (137.134.137.140/25):

Не подходят:

- S3 — корневой;
- S2, S7, S6 — соединены с агрегацией каналов;
- S8, S5 — соединены с оконечными устройствами.

Подходят, оба в любом случае будут иметь транзитный трафик, соответственно равнозначны:

- S1;
- S4 — менее нагружен.

▼ Беспроводные точки доступа 3702i:

Подключены к Switch2 (137.134.137.142/25) и Switch5 (137.134.137.143/25), чтобы быть в достаточной близости от контроллера.

Для включения питания нужно подтянуть кабель снизу.

Primary Controller: 137.134.137.140.

▼ Виланы для беспроводных устройств:

- 50 — Wireless1 (177.58.12.0/22);
- 60 — Wireless2 (19.44.0.0/14).

Создаются виртуальные интерфейсы: .1 и .1.

Для достижимости вилана на Root-коммутаторе прописано:

`spanning-tree vlan 10,20,50,60,100,999 priority 24576`.

На всех trunk-портах в список разрешенных виланов добавлены Vlan50, Vlan60.

На портах коммутаторов, соединенных с точками доступа, в качестве нативного вилана прописан административный (Vlan100).

▼ Первоначальная настройка WLC:

Для доступа к настройке контроллера через браузер, необходимо подключить к нему физически компьютер, которому далее назначить адрес из той же подсети.

Учетная запись администратора:

- логин: admin_lab
- пароль: wabrej-7qeczy-gUkdom

Настройка контроллера:

- System Name: WLC-Lab
- Management IP Address: 137.134.137.140
- Subnet Mask: 255.255.255.128
- Default Gateway: 137.134.137.129 (корневой коммутатор)
- Management VLAN ID: 1

Настройка беспроводной сети Wireless_emp: WPA2 Enterprise.

Сохранение конфигурации длится вечность... вечность... вечность, поэтому, не дожидаясь тщетно окончания, следует закрыть окно. Для подключения использовать протокол https.

▼ Создание BSS:

> Создание двух WLAN (WLANs → WLANs → Create New (21)):

- General: Profile Name, SSID, Status — Enabled;
- Security → Layer 2: Layer 2 Security — WPA+WPA2, WPA+WPA2 Parameters: WPA2 Policy, WPA2 Encryption — AES; 802.1x — Enable.
- Advanced → FlexConnect: FlexConnect Local Switching — Enabled, FlexConnect Local Auth — Enabled.

1. Wireless_emp. Wireless_emp.
2. Wireless_guest. Wireless_guest.

> Создание двух групп точек доступа (WLANs → Advances → AP Groups):

AP Group Name. [Description].

1. Employee.
2. Guest.

Редактирование точек доступа:

- WLANs → Add New. Выбрать соответствующий WLAN SSID.
- APs → Add APs. Выбрать соответствующие группе.
- General → Apply.

▼ Сервер (137.134.137.143/25):

Входит в Vlan100.

Services → AAA (Authentication, Authorization, Accounting) → Network Configuration:

- Client Name: Wireless
- Client IP: адрес контроллера;
- Secret: пароль AAA в Passwords;
- ServerType: Radius.

Добавить пользователей для беспроводных устройств, для них ввести тот же Secret.

Включить сервер.

> ## Для добавления на WLANs в контроллере:

Security → AAA → Radius Authentication Servers → New...

- Server Index (Priority): 1;
- Server IP Address(Ipv4/Ipv6): 137.134.137.143
- Shared Secret: magnan-jipziv (не больше 16 символов)
- Port Number: 1645.

Отредактировать WLANS: Security → AAA Services → Authentication Servers: Server 1 — выбрать добавленный ранее сервер.

▼ Настройка интерфейсов (Controller → Interfaces → New...):

Interface Name — LWAP1, VLAN Id — 50.

Physical Information: Port Number — 1.

Interface Address: VLAN Identifier — 50, IP Address — 177.58.12.2, Netmask — 255.255.252.0, Gateway — 177.58.12.1.

Аналогично для LWAP2.

Созданные интерфейсы выбрать для соответствующих WLANs в General → Interface/Interface Group(G).

▼ Обеспечение достижимости добавленных устройств:

Laptop3 (заменить сетевую карту) и Table PC0 относятся к WLAN Wireless_emp и Vlan50, Smartphone0 — к Wireless_guest и Vlan60.

Беспроводным устройствам указаны SSID, ip-адреса, а также шлюз (интерфейс соответствующего вилана, созданный на корневом коммутаторе).

▼ Аутентификация WPA2 Enterprise:

Для аутентификации беспроводных устройств во вкладке Config ввести все аналогичным образом:

Вопросы на защите

Добавить точку доступа.

Добавить беспроводное устройство.

Как сделать так, чтобы точка доступа обслуживала выбранную BSS?

Как настраивали административное управление контроллером?

Продемонстрировать, что доступ к контроллеру защищен.