**ЭТО ГАЙД НА 3 ЛР ПО АОКС.**

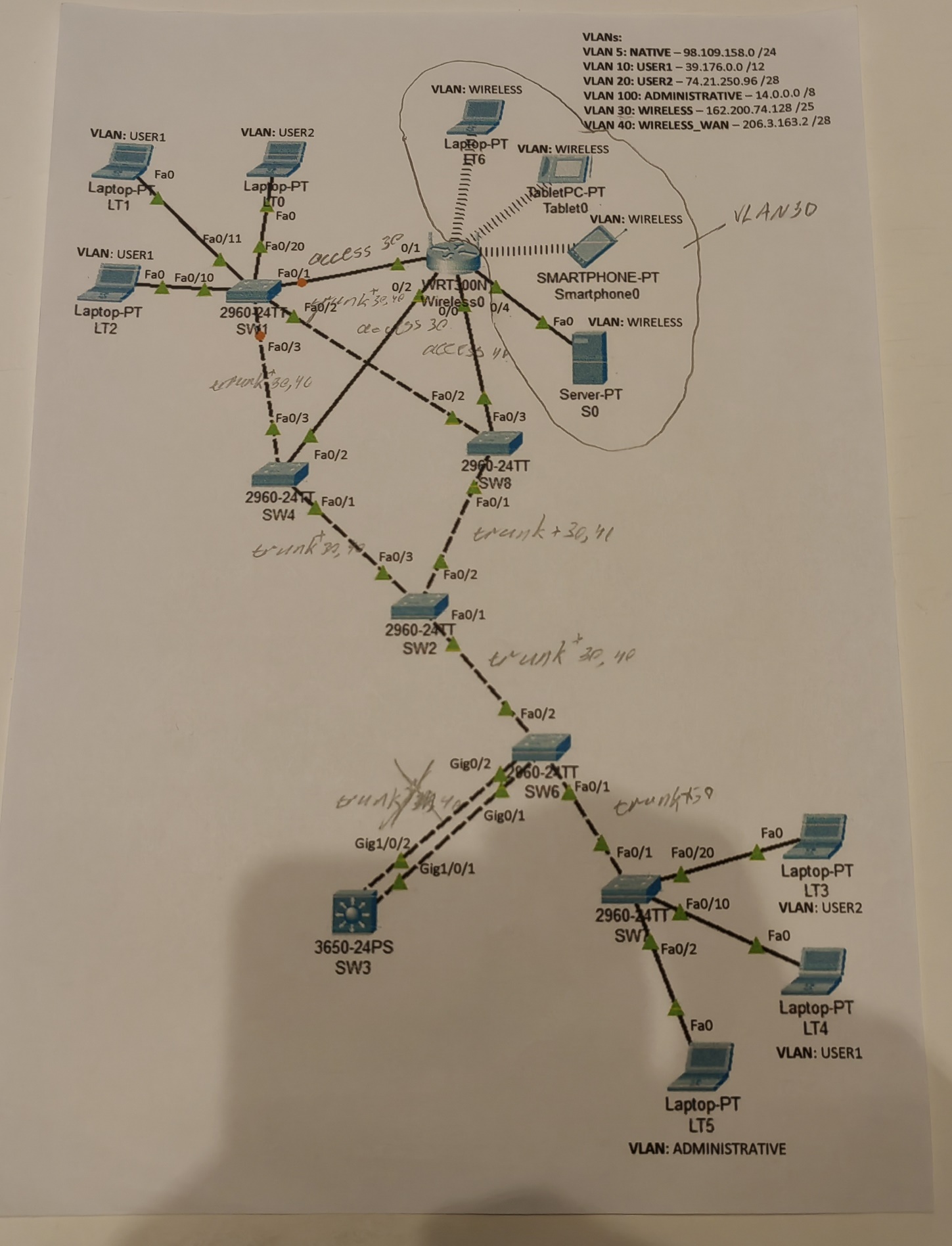
# Повторяем все как у этого замечательного человека

<https://github.com/andrejHurynovic/bsuirLabs/tree/main/term7/АОКС/АОКС%2C%20ЛР%20№%203>

**!!!** Уточнение мой гайд работает, если у вас не висящий беспроводной маршрутизатор. В случае висящего для вас будет актуальна ток та часть, где говорится про WAN. В случае если у вас все еще есть висящий 2960, то нужно именно его заменять беспроводным маршрутизатором

# **ТОПОЛОГИЯ**

# 1 порт LAN заменяем на WAN (0/0 это WAN)



# **2.3** Беспроводной маршрутизатор подключаем прямым кабелем

# **2.4** что касается сервера, то тут 3 варианта:

# **2.4.1** Можно как у меня (подключен к LAN). Обосновываем это как сервер только для авторизации. Но предпочтительнее следующий способ.

# **2.4.2** Подключить в Switch L2 который соединен с маршрутизатором (SW4, SW8). Обосновываем также как в 1 случае + безопасность т.к инфраструктура спрятана от пользователей. И в этом случае он не должен быть в VLAN беспроводных устройств, но об этом позже.

# **2.4.3** В третьем случае подразумевается, что сервер не ток для авторизации, и в этом случае его, вроде как, нужно поближе к Root или вообще в Root, но про этот способ я не могу ничего посоветовать.

# **3.** C ТОПОЛОГИЕЙ РАЗОБРАЛИСЬ ТЕПЕРЬ **НАСТРОЙКА**:

# **3.1 Подсети**

# Берем из варианта 2 подсети. Одна для LAN (VLAN 30 WIRELESS в моем случае), вторая для WAN (он же интернет для этого маршрутизатора, он же наш WAN. В моем случае VLAN 40 WIRELES\_WAN)

# **3.2** **Создаем виланы**

# У меня настроен VTP, поэтому в Root **создаем эти виланы:** VLAN 30 и VLAN 40, цифры можно и даже нужно менять на свои))).

>> conf t

>> vlan 30

>> name [name]

>> vlan 40

>> name [name]

# **3.3** **Теперь важно!!!**

Толька для WAN VLAN создаем виртуальный интерфейс

>> int vlan 40

>> ip address [ip address]

**3.4** **Настройка маршрутизации**

Если смотреть на нашу топологию только на L3 уровне, то у нас 2 маршрутизатора и подсеть для беспроводных устройств (Vlan 30) спрятана от root. Она для него не соседняя и он ее не видит. Поэтому нам нужно прописать static root.

>> conf t

>> ip route [адрес подсети для vlan 30] [маска для vlan 30] [тут нужно в качестве next hop указать **internet** address беспроводного маршрутизатора]

**3.5** **Транки на root**

В моем случае нет смысла доводить vlan 30 до root, поэтому trunk прописываем ток для vlan 40.

**4 НАСТРОЙКА ACCESS**

На коммутаторах соседних с БМ, для тех Switch, к которым подключены LAN, прописываем

[на интерфейсах] (SW1 fa0/1, SW4 fa0/2)

>> Switchport mode access

>> switchport access vlan 30.

Для WAN:

[на интерфейсе] (SW8 f0/3)

>> switchport mode access

>> switchport access vlan 40

**5** **ТРАНКИ**

!!! Транки **не** должный быть прописаны **везде** (хотя в специфичных случаях могут быть)

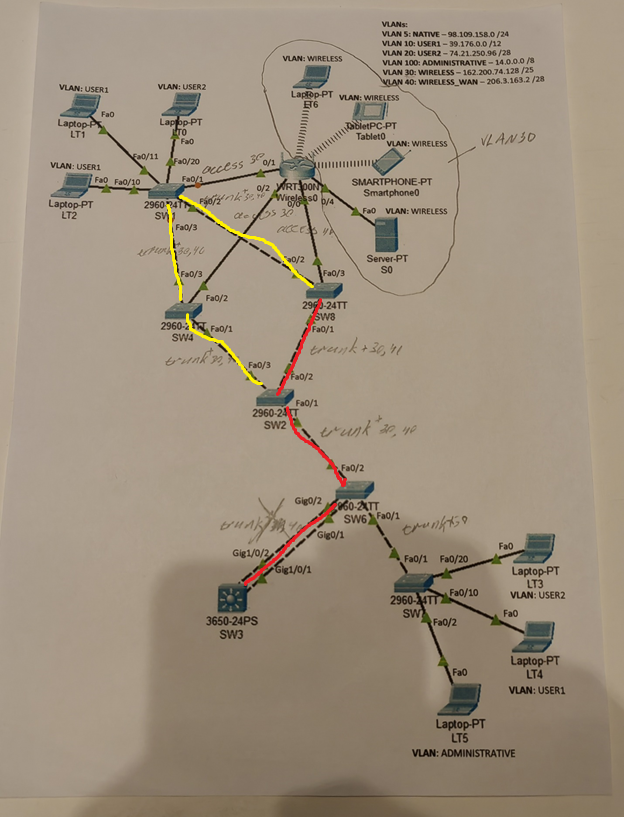
[на интерфейсе]

>> switchport trunk allowed vlan add [номер вилана]

**5.1 Trunk для WAN**

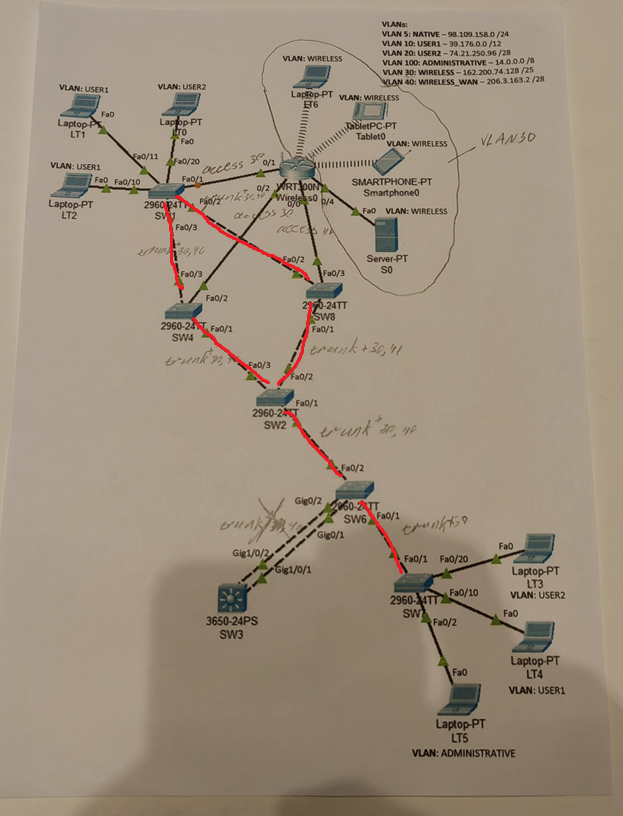
Идея здесь в следующем для WAN мы прописываем транки для **найкратчайшего пути** от Root до **беспроводного маршрутизатора (далее БМ**). Далее можем еще посмотреть **альтернативные пути** и там тож прописать, аргументируя это, как в случае, если сисадмин споткнется об кабель кратчайшего пути, то у пакетов будет альтернативный путь.

Красный это кратчайший путь, желтый это альтернативный



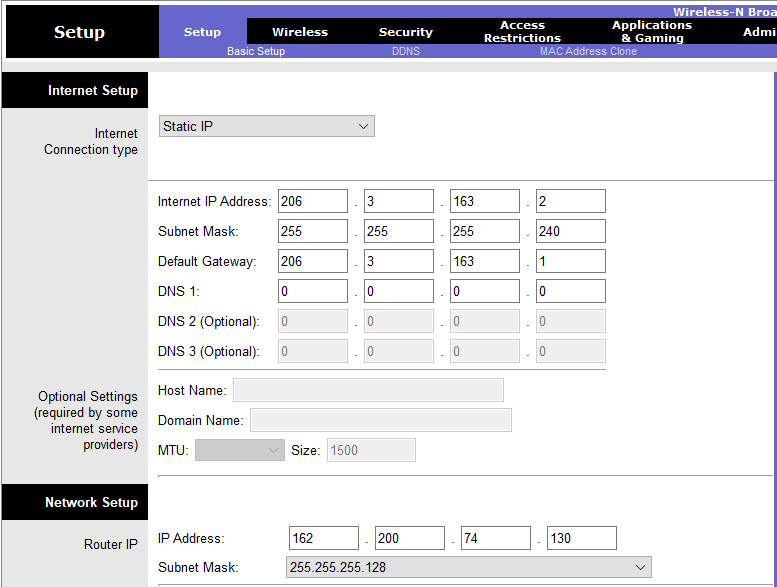
**5.2** **Транки для vlan 30 (он же LAN)**

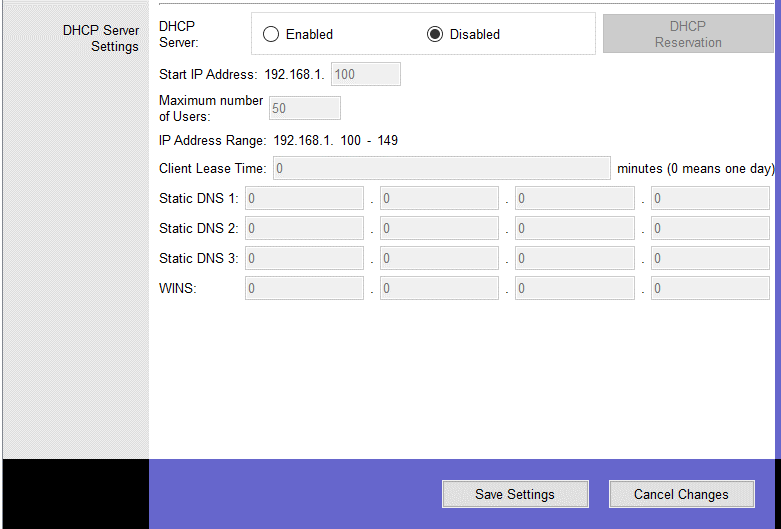
Здесь идея в следующем, т.к. у нас LAN порты подключены к 2960, то мы можем в наш vlan 30 подключать проводные устройства через эти же 2960. Поэтому мы можем разрешить trunk 30, по сути, везде кроме Root в похожих на мой случай.



Если на пальцах, то например мы вдруг захотели, чтобы в vlan 30 было еще 100 компов по проводу, а так как у нас есть LAN(БМ) подключения к 2960, то у нас этот VLAN 30 просачивается во всю сеть и это можно таким способом использовать (не баг, а фича). Подлючить компы к любому 2960 и прописать access 30. (кстати с этим был сввязан мой trick question см. в конце гайда, раздел защита)

**6. НАСТРОЙКА БМ**





**6.1 Internet**

Здесь задаем ему ip address из подсети для WAN. Gateway это ip address виртуального интерфейса Vlan 40 на Root.

**6.2 LAN**

Здесь назначаем ip address для БМ из подсети для Vlan 30.

6.2.1 Для беспроводных устройств можно использовать DHCP, задав пул из подсети для Vlan 30 и исключив адресс маршрутизатора.

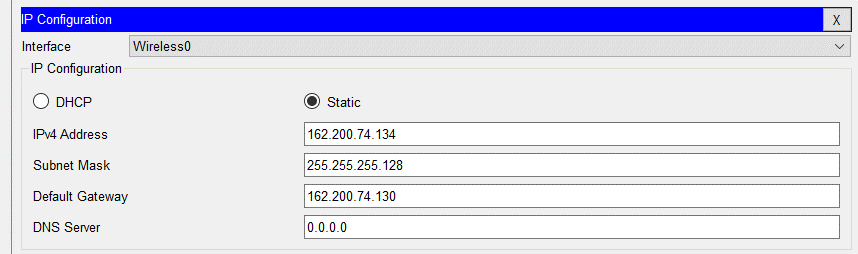
6.2.2 Или как я использовать статические в этом случае DHCP выключаем.

**7. Беспроводные устройства**

**7.1 DHCP**

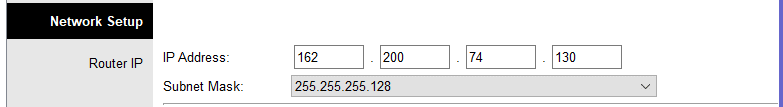
По идее в случае DHCP, нужно настроить ток авторизацию для Wi-fi. А IP Address он сам подтянет по DHCP.

**7.2 Static**



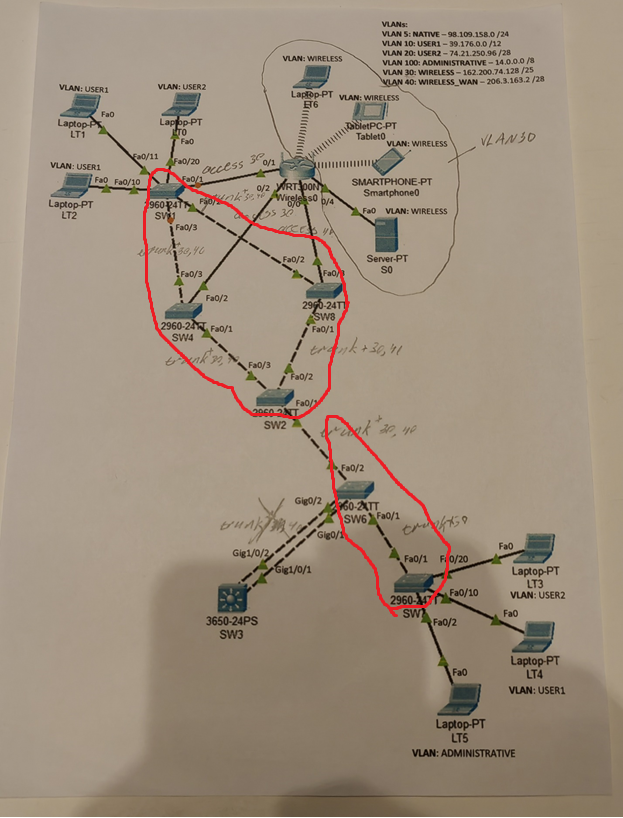
На примере LT6, назначаем IP address из vlan 30, в качестве Gateway ip address БМ (причем локальный, это значит из VLAN 30)

Вот этот:



**8. Сервер в WAN ~~и говорит…~~**

Если у вас сервер бахнут где-то здесь:



На самом деле хз где лучше, то могу предполагать, что в этом случае его лучше будет подключить в VLAN 40, тоесть в WAN.

Делается это просто как:

1)>> switchport access vlan 40

2) выдаем ip address из VLAN 40

3) Default Gateway, наверное, ip address Root (но тут не точно, но я бы сделал так)

3) на БМ указываем его адрес из 2 шага

И, по идее, все должно работать.

**9. НУ ВОТ ВЫ И СПРАВИЛИСЬ С ЛАБОЙ. CONGRATULATION!**

**🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳 🥳**

**10 А нет еще нужно защититься**

**11 Нюансы**

В 1 пункте задания мы должны были узнать про встроенный фаервол в БМ. Это означает, что даже не пытайтесь пинговать ни его, ни устройства в VLAN 30 из вне. Более того, вроде как, если пинг пройдет, то вы что-то сделали неверно. С беспроводных устройств, будет пинговаться все кроме административной станции.

**12 Самое сладкое защита**

1. **КлассЕка**

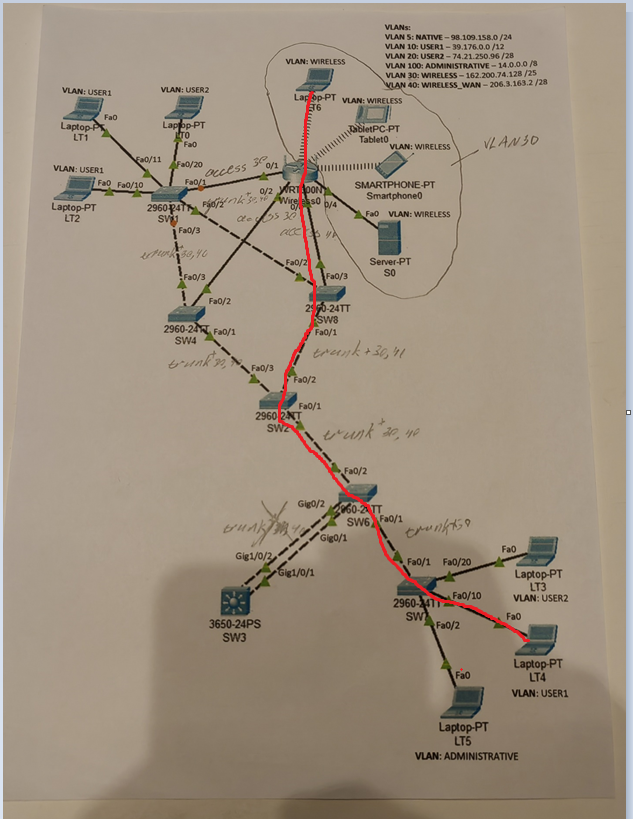
Tracerout из беспроводного устройства в тоже беспроводное:

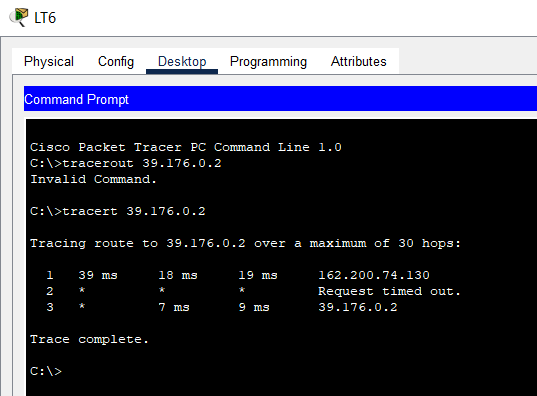


Например так. Итого должен быть 1 хоп.

1. **Тож база**

Tracerout до другого пользователького вилана из беспроводного





Итого 2 хопа (БМ, ROOT интерфейс соотв. vlan)

1. **Творчество**

Вопрос был таков:

Я админ. Мне нужно узнать какой тип авторизации используется для wi-fi.

Ответ:

(расскажу подробнее для понимания)

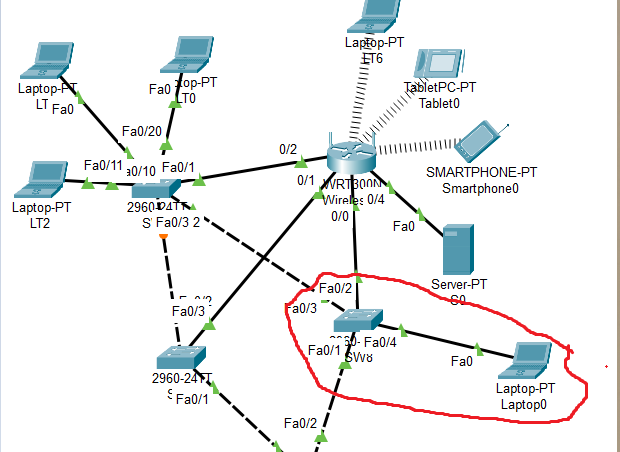
Даже не думайте тянуть ручки напрямую к БМ! Его GUI по клику существует ток в Packet Tracer.

Казалось бы, на первый взгляд, взять беспроводное устройство и в браузере вбить ip БМ и посмотреть. Но! Мы же не можем у пользователя отобрать устройство.

\* Вообще, я только что проверил, что можно из любого другого устройства (VLAN 10 или 20) по wan ip БМ достучаться до браузера, но хз…У меня была стрессовая ситуация и я думал следующим образом:

Возможно есть и другие решения, но мое было такое:

1. Если отобрать не можем, возмем свое.
2. Подключаем новый Laptop куда угодно, где доступен (транки) vlan 30



1. В жизни мы должны были бы залететь по SSH на SW8 (2960), к которому подключили, но для ускорения, он разрешил просто в CLI зайти.

Там мы не забывает поднять интерфейс

>> no shutdown

Затем access

>> sw mode access

>> sw access vlan 30

Но вот тут спорный момент, т.к. согласно, сейчас только выясненному, факту (\*), вроде как, и другой VLAN подойдет (например VLAN 40, он же WAN). Также те, у кого нет подключений LAN портов к 2960, тож подумать нужно.

1. Не забываем выдать ip address (В случае VLAN 30 и DHCP, тут хз), gateway в случае (vlan 30) необязателен, но на всякий случай прописать можно.
2. Теперь заходим в браузер и пишем LAN ip address беспроводного маршрутизатора
3. 