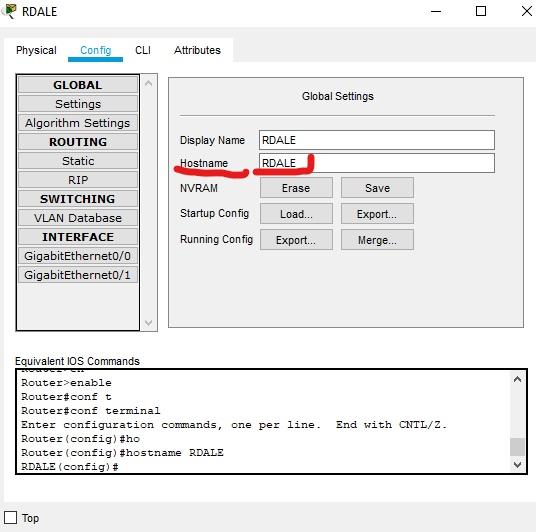
Отборочные на регион

**Настройка административного доступа**

1 Задайте имена устройств согласно их топологии

| (conf t) hostname <Имя устройства согласно топологии > | В режим конфигурирования даём имя устройству |
| --- | --- |

или



Остальных устройств в Config (Global > Setting). В пункте Display name изменяем имя.

2 Настройте учетную запись администратора на всех сетевых устройствах.

Используйте логин **admin** и пароль **cisco**.

Пароль должен храниться в виде хеш функции.

Задайте максимальные полномочия

| (conf t) username admin privilege 15 secret cisco | Создаем admin максимальными привилегиями и паролем cisco |
| --- | --- |

3 Настройте пароль на enable

Создайте пароль wsr

Пароль не должен храниться в виде хэш функции

| (conf t) enable password wsr | Создали не зашифрованный пароль на enable |
| --- | --- |

4 Настройте режим при котором все пароли хранятся в зашифрованном виде.

| (conf t) service password-encryption | Шифруем все пароли |
| --- | --- |

5 Настройте проверку пользователя на консоли

При подключении устройство должно запрашивать учетную запись пользователя

| (conf t) line console 0  login local | Заходим в настройки виртуальной консоли  Команда на проверку при входе в консоль |
| --- | --- |

6 Настройте IP-адреса для управления:????????

Настройте на SW1CHIP, SW2CHIP, COREDALE, SW1DALE, SW2DALE адрес

из сети LANMGMT. (Нудно и утомительно прописываем всем ip-шники)

|  |  |
| --- | --- |

Настройте на маршрутизаторах PCHIP и RDALE интерфейс Loopback1 и дайте ему адрес из сети LANMGMT.

| (conf t) interface loopback 1  no sh  (conf int) ip address <адрес который указан в таблице для данного маршрутизатора> | Создаём loopback 1 и поднимаем его  Добавляем адрес loopback |
| --- | --- |

7 Настройте подключение по [SSH](https://wiki.merionet.ru/seti/13/nastrojka-dostupa-k-cisco-po-ssh/)

1 Все сетевые устройства CISCO должны быть доступными по адресу из

сети LANMGMT для пользователя AdminCHIPnDALE

2 Настройте доменное имя chipndale.ru

3 Используйте ключ длиной 2048 бит.

4 Используйте версию 2

5 Запретить подключение по telnet.

tr vty 0 15

tra \_\_ ssh

login local 0

| (conf t) ip domain name <chipndale.ru>  //при том что у вас должно быть заранее прописанное имя хоста  hostname <имя\_хоста> //  crypto key generate rsa  // Потом спросят какой ключи использовать мы указваем//  2048  ip ssh version 2  line vty 0 14  transport input ssh | Указываем доменное имя для подключения по ssh прямо на сетевом оборудовании  Генерируем ключ шифрования  Подключаем ssh второй версии  Указываем подключение только по SSH |
| --- | --- |

8 Включите защиту от перебора на RCHIP. ПОМОГИТЕ

1. При попытке подключиться по SSH с неправильным паролем после 3 попыток за 10 секунд маршрутизатор должен блокировать удаленные подключения на 1 минуту.

**Настройка локальной сети**

1 Создайте VLAN согласно топологии.

1. Создайте номера и имена VLAN согласно топологии
2. Создайте VLAN 10 с именем WIFI
3. Создайте VLAN 20 с именем MANAGER
4. Создайте VLAN 30 с именем WORKER
5. Создайте VLAN 40 с именем BOSS
6. Создайте VLAN 50 с именем SERVER
7. Создайте VLAN 101 с именем LANMGMT
8. Создайте VLAN 1111 с именем SHUTDOWN

| (conf t) vtp mode transparent  vlan 10  name WIFI  vlan 20  name MANAGER  vlan 30  name WORKER  vlan 40  name BOSS  vlan 50  name SERVER  vlan 101  name LANMGMT  vlan 1111  name SHUTDOWN | Передаем vtp команду на то чтобы Vlan были прозрачными и мы могли создавать блатные Vlan  Создаем Vlan |
| --- | --- |

2 Настройте порты доступа.

1. Настройте порты на коммутаторах для подключения клиентов в соответствии с топологией

1 VLAN 10 с именем WIFI

2 VLAN 20 с именем MANAGER

3 VLAN 30 с именем WORKER

4 VLAN 40 с именем BOSS

5 VLAN 50 с именем SERVER

Просто заходишь на порт и протягиваешь в ту сторону access

switchport mode access

switchport access vlan <Указываешь нужный тебе vlan>

1. Все неиспользуемые порты поместите в Vlan 1111

Просто

1. Выключите все неиспользуемые порты

Посмотри какие порты не работают потом через range

interface range <тип интерфейса> <диапазон интерфейсов>

switchport mode access

switchport access vlan 1111

shutdown

3 Настройте транки между коммутаторы. ([Доп](https://habr.com/ru/post/319080/))

1. Офис CHIP :

1 На коммутаторе SW1CHIP порт в сторону RCHIP переведите в маршрутизируемый режим и дайте ip-адрес согласно таблице.

Создай vlan (новый) и кинь его в виде access на RCHIP. Не забудь дать

ip-шник vlan согласно топологии сети(Vlan - нет в таблице, но ip-шник есть)

2 Настройте режим динамического согласования транков ([Источник](https://ru.bmstu.wiki/DTP_(Dynamic_Trunking_Protocol))):

1 Коммутатор SW1CHIP инициализирует согласование

параметров магистрального соединения

| (conf t) interface gigabitEthernet 0/2  switchport mode dynamic desirable | Вроде только этот порт указываем. Сам порт делаем активным чтобы он был в поиске других  Делаем его активным |
| --- | --- |

2 Коммутатор SW2CHIP ожидает начало согласования

параметров от соседа, но сам не инициализирует согласование

| (conf t) interface gigabitEthernet 0/1  switchport mode dynamic auto | Вроде только этот порт указываем. Сам порт делаем пассивным чтобы он был в поиске других и не мог ничего сделать сам  Делаем его пассивным |
| --- | --- |

1. Офис DALE:

1 На коммутаторе COREDALE порт в сторону RDALE переведите в маршрутизируемый режим и дайте ip-адрес согласно таблице.

Создай vlan (новый) и кинь его в виде access на RDALE. Не забудь дать

ip-шник vlan согласно топологии сети(Vlan - нет в таблице, но ip-шник есть)

2 На всех коммутаторов офиса используйте режим без динамического согласования отключите TDP в явном виде.

| (conf t) interface gigabitEthernet <Порт>  switchport nonegotiate | Указываем порт на устройстве  Отключаем TDP в явном его виде |
| --- | --- |

1. Ограничьте список разрешенных VLAN. Должны разрешаться только VLAN 10, 20, 30, 40,50 и 101

Мы это автоматически делаем указывая на физических интерфейсов как мы будем работать с vlan

4 Настройте выдачу ip-адресов клиентам:

1. Клиенты сетей WIFI, MANAGER, WORKER и BOSS должны получать ip-адреса по DHCP.
2. В офисе CHIP в качестве DHCP-сервера SW1CHIP:

1 DNS-сервер c портом 8.8.8.8

2 Шлюз по умолчания и SW1CHIP в соответствующих сетях

3 Устройство WIFICHIP переведите в точку доступа

1. Пользователи SmartphoneCHIP и LaptopCHIP должны получать ip-адрес по беспроводному соединению автоматически.
2. В офисе DALE используйте в качестве DHCP-сервера COREDALE:

1 DNS-сервер 8.8.8.8

2 Шлюз по умолчания COREDALE в соответсвующих сетях.

1. Запретите выдачу первых и последних десяти адресов в соответствующих подсетях.
2. Настройте ip-адреса на устройствах AdminCHIPnDALE и ServerCHIP согластно таблице. //Просто статически прописываем ip-шники не забывая к ним привести соответствующие vlan

5 Настройте протокол остовного дерева в офисе DALE:

1. На всех коммутаторов в офисе DALE используйте протокол Rapid PVST

| (conf t) spanning-tree mode rapid-pvst  // Прописываем на всех коммутаторов в треугольнике// | Настройка протокола. Выбор его во всех коммутаторов которые его будут использовать. То есть в треугольнике коммутаторов |
| --- | --- |

1. На всех коммутаторов COREDALE должен являться корневым связующем дерева во всех VLAN. В случае его отказа, корнем должен стать коммутатор SW1DALE.

| (conf t) spanning-tree vlan 1-4094 root primary  (conf t) spanning-tree vlan 1-4094 root secondary | Настраиваем на COREDALE и указываем его в треугольнике главным  Настраиваем на SW1DALE и делаем его вторым после COREDALE |
| --- | --- |

6 Настройте маршрутизацию между VLAN на COREDALE и SW1CHIP

1. Включите шаблон [SDM](https://wiki.merionet.ru/seti/45/pro-cisco-shablony-sdm-switching-database-manager/) с поддержкой маршрутизации.

| (conf t)sdm prefer vlan  write memory  reload  // Для проверки можете использовать # show sdm prefer | Включаем SDM. Нам будет сказано что нужна перезагрузка(Не переживайте)  !!!Не забываем сохраниться!!!  После перезагрузки SDM включится |
| --- | --- |

1. Настройте интерфейсы SVI для сетей WORKER, MANAGER, BOSS, SEVER, LANMGMT и WIFI на комутаторе COREDALE и SW1CHIP.

1 Задайте им адреса в соответствующих подсетях.

Создаёшь vlan и даёшь им соответствующие ip(смотри в таблицу)

7 Настройте OSPF в офисе DALE: // Не сложнее чем EIGRP

1. Используйте номер процесса 1 и область 0
2. В маршрутизации участвуют устройства RDALE и COREDALE
3. Добейтесь связанности в сетях LANMGMT, MANAGER, WORKER, BOSS и SERVER.
4. Все интерфейсы должны находиться в пассивном режиме.

Отключить пассивный режим на интерфейсах между RDALE и COREDALE. Провайдер не должен получать hello пакеты OSPF.

1. Распространите статические маршруты и маршрут по умолчанию в OSPF.

8 Настройте протокол маршрутизации [EIGRP](https://wiki.merionet.ru/seti/40/passivnye-interfejsy-v-eigrp/) в офисе CHIP.

1. Используйте номер AS 65000 (AS - автономная система )
2. В маршрутизации участвуют два устройства RCHIP и SW1CHIP
3. Добейтесь связности в сетях WORKER, MANAGER, BOSS, SEVER, LANMGMT и WIFI.
4. Все интерфейсы должны находиться в пассивном режиме.

Отключить пассивный режим на интерфейсах между RCHIP и SW1CHIP. Провайдер не должен получать hello пакеты EIGRP.

| (config-router) network 192.168.10.0 0.0.0.255  network 192.168.20.0 0.0.0.255  network 192.168.30.0 0.0.0.255  network 192.168.50.0 0.0.0.255  network 192.168.101.0 0.0.0.7  network 192.168.0.0 0.0.0.3 | vlan 10 name WIFI  vlan 20 name MANAGER  vlan 30 name WORKER  vlan 40 name BOSS  vlan 50 name SERVER  vlan 101 name LANMGMT  Vlan между RCHIP и SW1CHIP |
| --- | --- |

passive-interface default (не работает, лучше не надо)

| На SW1CHIP  (conf eigrp)  passive-interface <>  На RCHIP  (conf eigrp)  passive-interface <> | Переводим все интерфейсы в пассивный режим  Делаем исключение в пассивном режиме  Переводим все интерфейсы в пассивный режим  Делаем исключение в пассивном режиме |
| --- | --- |

1. Распространите статические маршруты и маршрут по умолчанию EIGRP.

9 Настройте [статические маршруты](https://wiki.merionet.ru/seti/45/pro-cisco-shablony-sdm-switching-database-manager/) на RCHIP и RDALE для обеспечения связности в локальной сети.

1. Настройте на RCHIP статические маршруты через туннель до всех сетей офиса DALE.

| ip route <В какую сеть хочешь попасть .0> <Маска сети в которую хочешь попасть > <Физически ip который идёт на пути>(без .0) | Долго и нудно пишешь пальчиками  Прописываешь весь маршрут |
| --- | --- |

1. Настройте на RDALE статические маршруты через туннель до всех сетей офиса CHIP.

| ip route 3.3.3.0 255.255.255.0 192.168.23.3 | Пример |
| --- | --- |

1. Настройте редистрибуцию статических маршрутов в EIGRP и OSPF

**Настройка глобальной сети** (Ваше задание оставшуюся часть зданий выполнить самим используя материалы из интернета или посмотрев реализацию в готовой сети)

1 Включите интерфейсы маршрутизаторах RCHIP и RDALE и настройте на них ip-адреса согласно таблице:

1. Задайте описания всех интерфейсов в маршрутизатора.
2. Для интерфейсов в сторону провайдера используйте в качестве описания название провайдеров.
3. Для интерфейсов в сторону коммутаторов используйте название согласно таблицы.
4. Для интерфейсов Loopback используйте название LO-MGMT.

2 Настройте на роутерах RCHIP и RDALE маршрут по умолчанию в сторону провайдера ISP.

ip route 0.0.0.0 0.0.0.0 <isp>

3 Настройте доступ в интернет (PAT) клиентами сетей WIFI, MANAGER, WORKER и BOSS. [PAT\_1](https://habr.com/ru/post/351332/)  [PAT\_2](https://www.sysnettechsolutions.com/en/configure-nat-pat-in-cisco-packet-tracer/)

1. Сеть LANMGMT не должна иметь доступ в интернет.

4 Настройте туннель между роутерами RCHIP и RDALE:

1. Используйте в качестве VTI интерфейс Tunnel100
2. Используйте адресацию 5.5.5.0/30

5 Настройте проброс портов на RCHIP.

1. При подключении на порт 80 на внешний IPv4 адрес RCHIP трафик должен пересылаться на адрес ServerCHIP на порт 80.