1.1 Заметки

Логины и пароли для изначального входа в операционные системы
Минимальные альты: root - toor
Альт Workstation: user - resu
EcoRouter: admin - admin

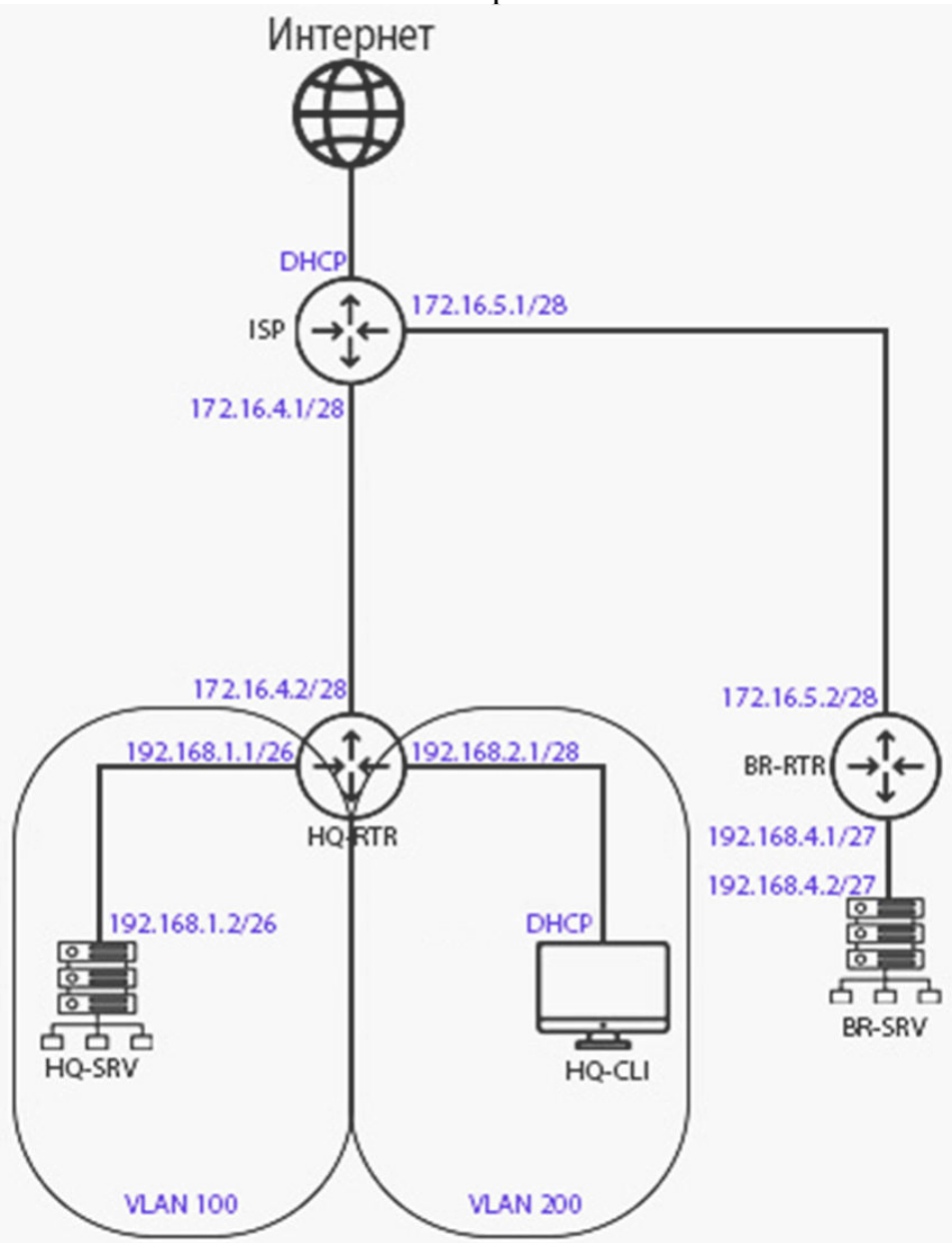
Команда для получения доступа к apt-get пакетам по прокси:
export http_proxy='http://10.1.1.11:3128/'
или можно ещё добавить в файл /etc/apt/apt.conf
Acquire::http::Proxy "http://10.1.1.11:3128";

После одного из двух сделать apt-get update чтобы получить доступ к репозиториям.

Таблица адресации (лучше просто запомнить 2^n - 2 = кол-во хостов)

Устройство	Интерфейс	IP-адрес	Маска	VLAN	Подсеть	Шлюз
ISP	eth0 (к интернету)	DHCP	DHCP	-	DHCP	DHCP
	eth1 (к HQ-RTR)	172.16.4.1	255.255.255.240	-	172.16.4.0/28	-
	eth2 (к BR-RTR)	172.16.5.1	255.255.255.240	-	172.16.5.0/28	-
HQ-RTR	eth0 (к ISP)	172.16.4.2	255.255.255.240	-	172.16.4.0/28	172.16.4.1
	eth1 (Trunk)	-	-	Trunk	-	-
	eth1.100	192.168.1.1	255.255.255.192	100	192.168.1.0/26	-
	eth1.200	192.168.2.1	255.255.255.240	200	192.168.2.0/28	-
	eth1.999	192.168.3.1	255.255.255.248	999	192.168.3.0/29	-
	gre1 (IP туннель)	10.10.10.1	255.255.255.252	-	10.10.10.0/30	-
HQ-SRV	enp0s3 (Trunk)	-	-	Trunk	-	-
	enp0s3.100	192.168.1.2	255.255.255.192	100	192.168.1.0/26	192.168.1.1
HQ-CLI	enp0s3.200	192.168.2.2	255.255.255.240	200	192.168.2.0/28	192.168.2.1
BR-RTR	eth0 (к ISP)	172.16.5.2	255.255.255.240		172.16.5.0/28	172.16.5.1
	eth1 (к BR-SRV)	192.168.4.1	255.255.255.224		192.168.4.0/27	-
	gre1 (IP туннель)	10.10.10.2	255.255.255.252		10.10.10.0/30	-
BR-SRV	enp0s3 (к BR-RTR)	192.168.4.2	255.255.255.224		192.168.4.0/27	192.168.4.1

Полная карта сети



Хостнеймы (DNS-адреса) устройств - moodle и wiki для докера

Устройство	Запись	Тип
HQ-RTR	hq-rtr.au-team.irpo	A,PTR
BR-RTR	br-rtr.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A,PTR
HQ-CLI	hq-cli.au-team.irpo	A,PTR
BR-SRV	br-srv.au-team.irpo	A
HQ-RTR	moodle.au-team.irpo	CNAME
HQ-RTR	wiki.au-team.irpo	CNAME

Таблица с масками подсети

Маска подсети	Маска в двоичной системе	Префикс	Количество адресов	Обратная маска
255.255.255.255	11111111.11111111.11111111.11111111	/32	1	0.0.0.0
255.255.255.254	11111111.11111111.11111111.11111110	/31	2	0.0.0.1
255.255.255.252	11111111.11111111.11111111.11111100	/30	4	0.0.0.3
255.255.255.248	11111111.11111111.11111111.11111000	/29	8	0.0.0.7
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	0.0.0.15
255.255.255.224	11111111.11111111.11111111.11100000	/27	32	0.0.0.31
255.255.255.192	11111111.11111111.11111111.11000000	/26	64	0.0.0.63
255.255.255.128	11111111.11111111.11111111.10000000	/25	128	0.0.0.127
255.255.255.0	11111111.11111111.11111111.00000000	/24	256	0.0.0.255

!!!! Заметки к конечному содержанию отчета

- В ходе проектирования и настройки сетевой инфраструктуры следует вести отчеты (**пять отчетов**) о своих действиях, включая таблицы и схемы, предусмотренные в задании. Отчеты по окончании работы следует сохранить на диске рабочего места.
- Сведения об адресах занесите в отчёт (**1**), в качестве примера, используйте Таблицу VVVVV.

Имя устройства	IP-адрес	Шлюз по умолчанию
BR-SRV	192.168.0.2/24	192.168.0.1

- Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт (**2**)
- Сведения о туннеле GRE/IPinIP занесите в отчёт (**3**)
- Сведения о настройке и защите протокола OSPF (через OSPF Authentication) занесите в отчёт (**4**)
- Сведения о настройке протокола динамической конфигурации (DHCP) занесите в отчёт (**5**)
- Отчёт нужно составлять в соответствии с ГОСТ Р 7.0.97-2016

1.2 Alt Linux

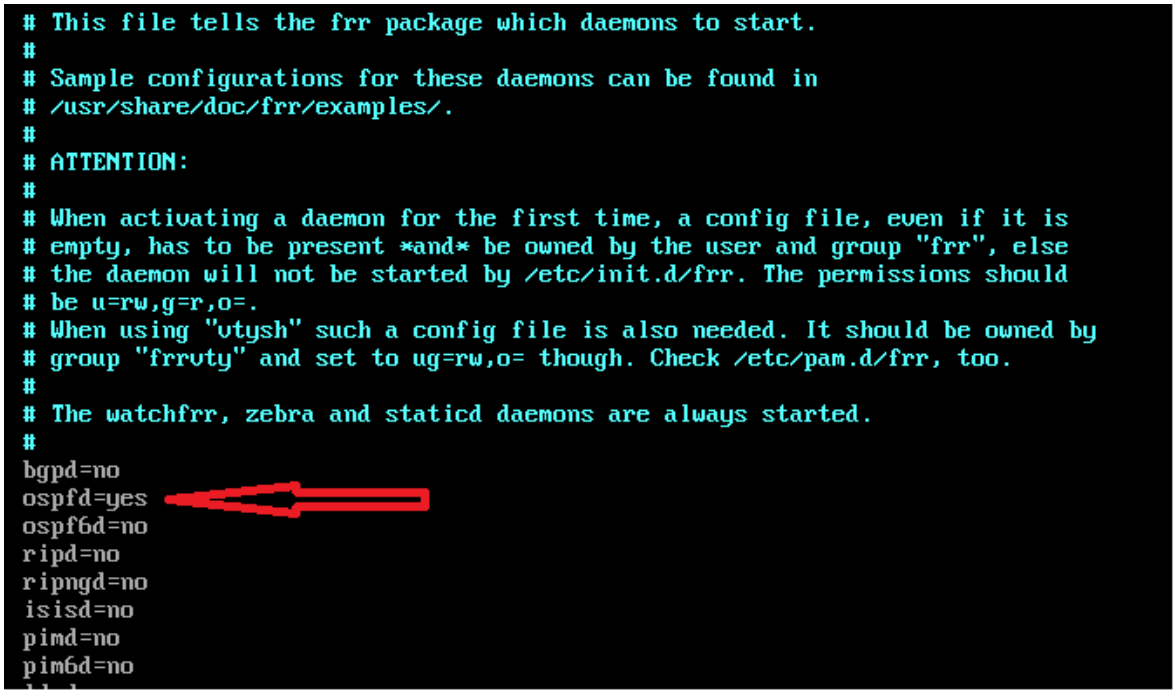
1.2.1 Базовая установка и настройка необходимого ПО

1.2.1.1 ISP (iptables, traceroute, net-tools и frr)

Пакеты можно устанавливать с помощью команды “apt-get install [имя пакета]”. Пакетам traceroute и net-tools конфигурация не нужна - они просто утилиты для устранения проблем в сети.

С пакетами frr (виртуальным маршрутизатором) и iptables (базовый firewall и перенаправлятель пакетов) - другая история, с помощью них мы имеем доступ к настройке OSPF и NAT.

После установки frr заходим в файл /etc/frr/daemons через любой адекватный текстовый редактор и изменяем значение “osfpd” на “yes” (для доступа к ospf)



iptables в нашем случае используется для настройки NAT, он приходит с несколькими командами.

iptables-save сохраняет текущие настройки (которые можно узнать через iptables -L) в указанный пользователем файл.
iptables-restore восстанавливает настройки iptables на основе файла.
iptables - утилита позволяющая манипулировать и проводить обзор текущих правил iptables.
В наших интересах использовать iptables для NAT. Вот команда:
iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
-t это table, через -A мы добавляем правило в цепочку “POSTROUTING” - цепочка которая решает что делать с пакетом после того как решение направить его уже было сделано, -o это output, или в других словах вывод и -j это действие, MASQUERADE заменяет отправляющий адрес всех пакетов которые выходят из интерфейса ens19 на его адрес.

Все остальное должно быть понятным.

1.2.1.2 HQ-SRV (dnsmasq/bind и bind-utils - на выбор, mdadm, openssh)

[ВСТАВИТЬ СЮДА ОБЪЯСНЕНИЕ О ДНС С BIND/DNSMASQ]

О настройке ssh есть своя статья. mdadm используется для RAID-а.

1.2.1.3 HQ-CLI (yandex-webbrowser-stable)

Тут по идее понятно.

1.2.1.4 BR-SRV (docker-engine, docker-compose-v2, openssh)

Docker нужен для второго модуля. О настройке ssh есть своя статья.

1.2.2 Базовая Адресация (Чеплаков)

Для того чтобы узнать какой адрес совпадает с каким мостом нужно совмещать MAC-адреса и мосты vmbr, которые можно видеть в панели “hardware” на любой виртуальной машине.

1.2.2.1 ISP

!!!!! В любой момент можно скопировать и подредактировать файл /etc/net/ifaces/default/options чтобы не запоминать все настройки.

На ISP есть 2 интерфейса - один интерфейс (обычно ens19), который получает IP адрес с через DHCP и один статический интерфейс (ens20?), имеющий доступ в локальную сеть.
Для настройки DHCP интерфейса хватает лишь наличие файла options с нижеуказанными параметрами:
TYPE=eth
BOOTPROTO=dhcp
ONBOOT=yes
Для статического интерфейса добавляются несколько файлов, а именно ipv4address, ipv4route и resolv.conf. Также меняется параметр BOOTPROTO на static вместо dhcp (BOOTPROTO=static).
ipv4address содержит в себе ipv4 адрес интерфейса в данном виде:
x.x.x.x/м - где x - октет адреса и м - маска в десятичном виде.
Т.е например 192.168.1.1/24 - адрес 192.168.1.1 с маской 255.255.255.0.
ipv4route содержит шлюз по умолчанию. Содержание выглядит так.
default via x.x.x.x
Да, тут без маски, и да, все время пишется “default via”.
resolv.conf имеет следующий вид:
nameserver x.x.x.x, тут наверное объяснять больше не надо.

1.2.2.2 HQ-SRV

Другие гайды показывают что нужно создавать дополнительный интерфейс типа как ens20.100 для обеспечения 100-ого vlan-а, но в условиях proxmox-а это не нужно. Proxmox мост автоматически добавляет vlan tag 100 к исходящим пакетам, так что тут обычная настройка статического интерфейса.
Если вы это делаете в VBox или VMware нужно будет оставить обычный интерфейс почти пустым (ничего кроме файла options с BOOTPROTO=static и TYPE=eth) и добавить новый интерфейс, с таким-же именем только с точкой и цифрой VLAN-а после него. В его файле параметров также требуется сменить TYPE на vlan и добавить строчки

VID=[айди вашего vlan-a] и HOST=[интерфейс на котором едет весь VLAN, типа как ens20]

1.2.2.3 HQ-CLI

Получает адрес по DHCP.

1.2.2.4 BR-SRV

Обычный статический адрес.

1.2.3 Настройка SSH - создание sshuser и настройка openssh

1.2.3.1 HQ-SRV и BR-SRV

Создания пользователя на системе alt:

sudo useradd -u 1010 -m sshuser
echo "sshuser:P@ssw0rd" | sudo chpasswd
или passwd sshuser и просто ввести пароль

Настройка доступа без аутентификации:

Файл : /etc/sudoers

sudo usermod -aG wheel sshuser
sudo visudo или vim /etc/sudoers как root
Добавляем или раскомменчиваем убирая # : WHEEL_USERS ALL=(ALL) NOPASSWD: ALL

Настройка openssh:
Основной каталог : /etc/openssh
Файл настроек : /etc/openssh/sshd_config

EcoRouter:
router ospf
network <адрес_сети/префикс> area 0

Это в режиме conf t надо писать

Ну и так же через network просто добавляешь все сетки которые к роутеру подкючены

Для аутентификации ospf заходишь в конфигурацию интерфейса который подключается к соседу ospf и пишешь ip ospf authentication (включает аутентификацию ospf)
ip ospf message-digest-key 1 md5 <пароль>
Ни и далее на другом роутере тоже самое

Чтобы dhcp сервак настроить сначала создаешь пул адресов с помощью ip pool <имя_пула> 1.1.1.1-2.2.2.2 (ни через тире просто диапазон прописываешь короче)

Потом пишешь dhcp-server <id> и потом пишешь dns <ip_dns_севака_для_раздачи> потом mask <маска сети> и gateway <адрес_шлюза> и pool <имя_пула> <приоритет> и потом там внутри так же dns, mask, gateway прописываешь

Потом просто на интерфейс нужный заходишь тебе и там пишешь dhcp-server <айдишник_который_ты_дал_своему_dhcp_серверу>

Включение форвардинга
echo 1 > /proc/sys/net/ipv4/ip_forward

NAT для HQ-RTR и BR-RTR
iptables -t nat -A POSTROUTING -s 172.16.4.0/28 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 172.16.5.0/28 -o eth0 -j MASQUERADE

Ручное сохранение:

iptables-save > /etc/iptables.rules

1.3.1 Настройка учетной записи net_admin

en
conf t
username net_admin
password P@$$word
role admin
exit

1.3.2 Настройка маршрутизации - адресация, VLAN и OSPF

Заходим на HQ-RTR, логинимся и выполняем следующие команды:
en (Входит в привилегированный режим)
conf t (Входит в режим конфигурации)
do show port brief (Выводит список всех подключенных портов, должно быть два порта te0, и te1, te0 - это порт к ISP, te1 - это порт к HQ-CLI и HQ-SRV)

Далее настраиваем интерфейсы с помощью следующих команд:
interface eth0 (Переход в режим конфига интерфейса eth0)
ip address 172.16.4.2/28 (Задаем IP адрес)
exit
interface eth1.100
ip address 192.168.1.1/26
exit
interface eth1.200
ip address 192.168.2.1/28
exit
interface eth1.999
ip address 192.168.3.1/29
exit

Далее настраиваем порты с помощью команд:
port te1 (Переход в режим конфига порта te1)
service-instance VLAN100 (Создаем инстанс с именем VLAN100)
encapsulation dot1q 100 (Инкапсуляция трафика с VLAN 100)
rewrite pop 1 (Снимаем VLAN тег 100 с трафика)
connect ip interface eth1.100 (Подключаем интерфейс к данному инстансу)
exit
service-instance VLAN200
encapsulation dot1q 200
rewrite pop 1
connect ip interface eth1.200
exit
exit
port te0
service-instance ISP

encapsulation untagged (Инкапсуляция не тегированного трафика)
connect ip interface eth0
exit
exit
write (сохраняем конфигурацию)

Заходим на BR-RTR логинимся если нужно и выполняем следующие команды:
en
conf t
do show port brief (Должны также отобразится также два интерфейса te0 и te1)

Далее конфигурируем интерфейсы с помощью команд:
interface eth1
ip address 192.168.4.1/27
exit
interface eth0
ip address 172.16.5.2/28
exit

Далее настраиваем порты с помощью команд:
port te1
service-instance BR-SRV
encapsulation untagged
connect ip interface eth1
exit
exit
port te0
service-instance ISP
encapsulation untagged
connect ip interface eth0
exit
exit
write (Сохраняем конфигурацию)

Базовая настройка:

Хостнеймы:

- EcoRouter

enable

conf t

hostname имя

- Для CLI

su hostname имя

- Для остальных

hostnamectl set-hostname имя

IP адреса:

ls /etc/net/ifaces - (ls - просмотр содержимого файлов ls)

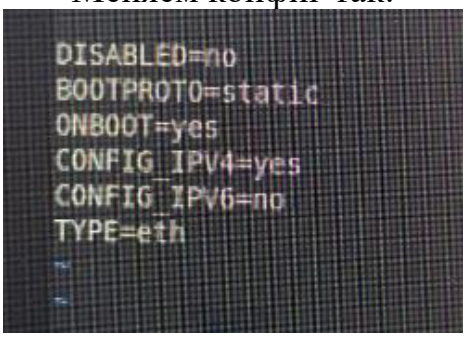
mkdir /etc/net/ifaces/ens19 (ens19 для всего кроме RTR, для них 20 и 21) (mkdir - создание папки)

cp /etc/net/ifaces/default/options /etc/net/ifaces/ens19/ - Перемещение (cp) конфигурации из стандартной директории в директорию интерфейса

rm -rf /etc/net/ifaces/ens18 - удаляем ens18 (rm команда удаления) (можно не делать)

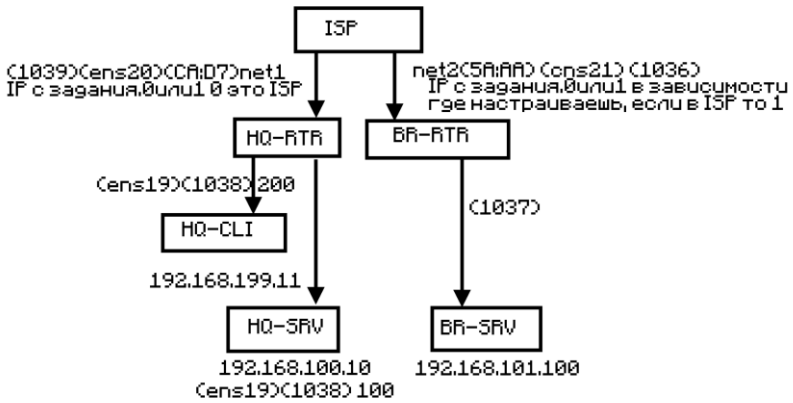
vim /etc/net/ifaces/ens19/options (vim - текстовый редактор)

Меняем конфиг так:



vim /etc/net/ifaces/ens19/ipv4address

(сюда пишем айпи по схеме, все айпи можно самому придумать, айпи для RTR прописаны в задании. Маски сети можно посмотреть в таблице в самом начале) RTR настраивать через CLI машину



systemctl restart network - перезапускаем сеть

Настройка DHCP НЕПРАВИЛЬНО

- Откройте файл на редактирование:

sudo nano /etc/dhcp/dhcpd.conf

- Пример конфиг файла:

Параметры по умолчанию
default-lease-time 600;
max-lease-time 7200;
authoritative;
# Сеть HQ (192.168.100.0/24)
subnet 192.168.100.0 netmask 255.255.255.0 {
range 192.168.100.20 192.168.100.80;
option routers 192.168.100.1;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.100.10; # HQ-SRV как DNS
option domain-name "hq.work";
}
# Резервирование адреса для HQ-SRV
host hq-srv {
hardware ethernet 00:11:22:33:44:55; # MAC-адрес HQ-SRV
fixed-address 192.168.100.10;
}

- MAC-адрес нужно заменить на реальный MAC HQ-SRV, его можно узнать командой: ip a | grep ether

Указать интерфейс, на котором работает DHCP

Файл:/etc/sysconfig/dhcpd или /etc/default/isc-dhcp-server (в зависимости от сборки ALT Linux)

Добавьте/укажите интерфейс: INTERFACES="ens19"

Интерфейс ens19 используется для HQ-сети согласно топологии.

- Запуск и автозагрузка службы DHCP

sudo systemctl start dhcpd
sudo systemctl enable dhcpd

- Проверьте статус: sudo systemctl status dhcpd
- Проверка работы:

sudo dhclient ens19
ip a

1. Произведите базовую настройку устройств
● Настройте имена устройств согласно топологии. Используйте полное доменное имя
● На всех устройствах необходимо сконфигурировать IPv4 ● IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918
● Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов
● Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов
● Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов
● Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов
● Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3 2.
2. Настройка ISP
● Настройте адресацию на интерфейсах:
o Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
o Настройте маршруты по умолчанию там, где это необходимо o Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28
o Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28
o На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет
3. Создание локальных учетных записей
● Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV o Пароль пользователя sshuser с паролем P@ssw0rd
o Идентификатор пользователя 1010
o Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.
● Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR
o Пароль пользователя net_admin с паролем P@$$word
o При настройке на EcoRouter пользователь net_admin должен обладать максимальными привилегиями
o При настройке ОС на базе Linux, запускать sudo без дополнительной аутентификации
4. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:
● Сервер HQ-SRV должен находиться в ID VLAN 100
● Клиент HQ-CLI в ID VLAN 200
● Создайте подсеть управления с ID VLAN 999
● Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт
5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BRSRV:
● Для подключения используйте порт 2024
● Разрешите подключения только пользователю sshuser
● Ограничьте количество попыток входа до двух
● Настройте баннер «Authorized access only»
6. Между офисами HQ и BR необходимо сконфигурировать ip туннель
• Сведения о туннеле занесите в отчёт
• На выбор технологии GRE или IP in IP
7. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.

● Разрешите выбранный протокол только на интерфейсах в ip туннеле
● Маршрутизаторы должны делиться маршрутами только друг с другом
● Обеспечьте защиту выбранного протокола посредством парольной защиты
● Сведения о настройке и защите протокола занесите в отчёт
8. Настройка динамической трансляции адресов.
● Настройте динамическую трансляцию адресов для обоих офисов.
● Все устройства в офисах должны иметь доступ к сети Интернет
9. Настройка протокола динамической конфигурации хостов.
● Настройте нужную подсеть
● Для офиса HQ в качестве сервера DHCP выступает маршрутизатор HQ-RTR.
● Клиентом является машина HQ-CLI.
● Исключите из выдачи адрес маршрутизатора
● Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR.
● Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV.
● DNS-суффикс для офисов HQ – au-team.irpo
● Сведения о настройке протокола занесите в отчёт
10. Настройка DNS для офисов HQ и BR.
● Основной DNS-сервер реализован на HQ-SRV.
● Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
● В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер
11. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена