



Конкурсное задание

Модуль С – Сети передачи данных

Сетевое и системное администрирование

Разработано:

Главный эксперт

Svetlana Lapenko

CONTENTS

Введение	3
Описание проекта и задач	4
Задачи конфигурации.....	6
Часть 1. Базовая конфигурация.....	7
Часть 2. Коммутация.....	7
Часть 3. EIGRP (для HQ2)	8
Часть 4. OSPF (для HQ1)	9
Часть 5. BGP	10
Часть 6. IP-сервисы.....	10
Часть 7. Безопасность и VPN.....	11

ВВЕДЕНИЕ

Соревнование имеет фиксированное время начала и окончания. Вы должны решить, как лучше распределить свое время.

Пожалуйста, внимательно прочтите следующие инструкции!

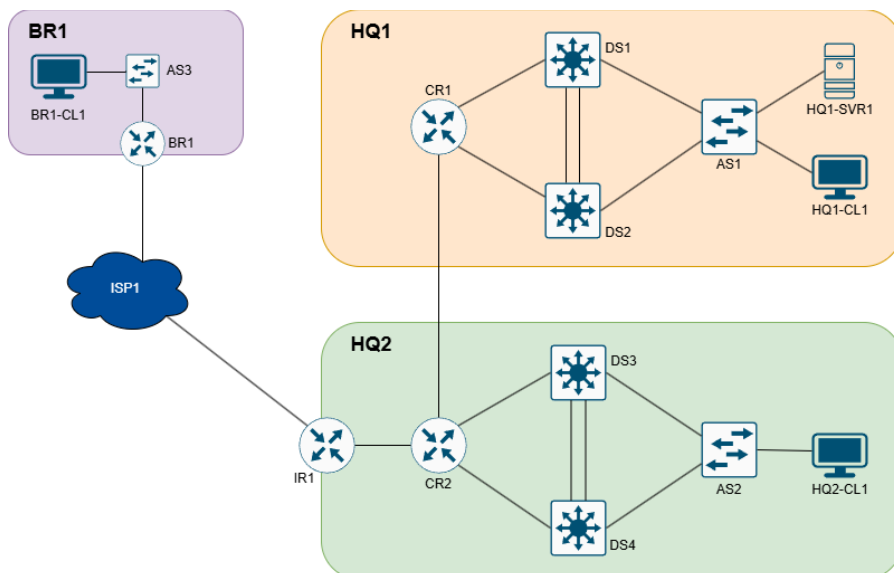
После окончания времени соревнования, пожалуйста, оставьте свою станцию в рабочем состоянии. Оценка будет проводиться в том состоянии, в котором она есть. Перегрузка не будет инициирована, а выключенные машины не будут включены!

Пожалуйста, используйте информацию ниже для всех серверов и клиентов.

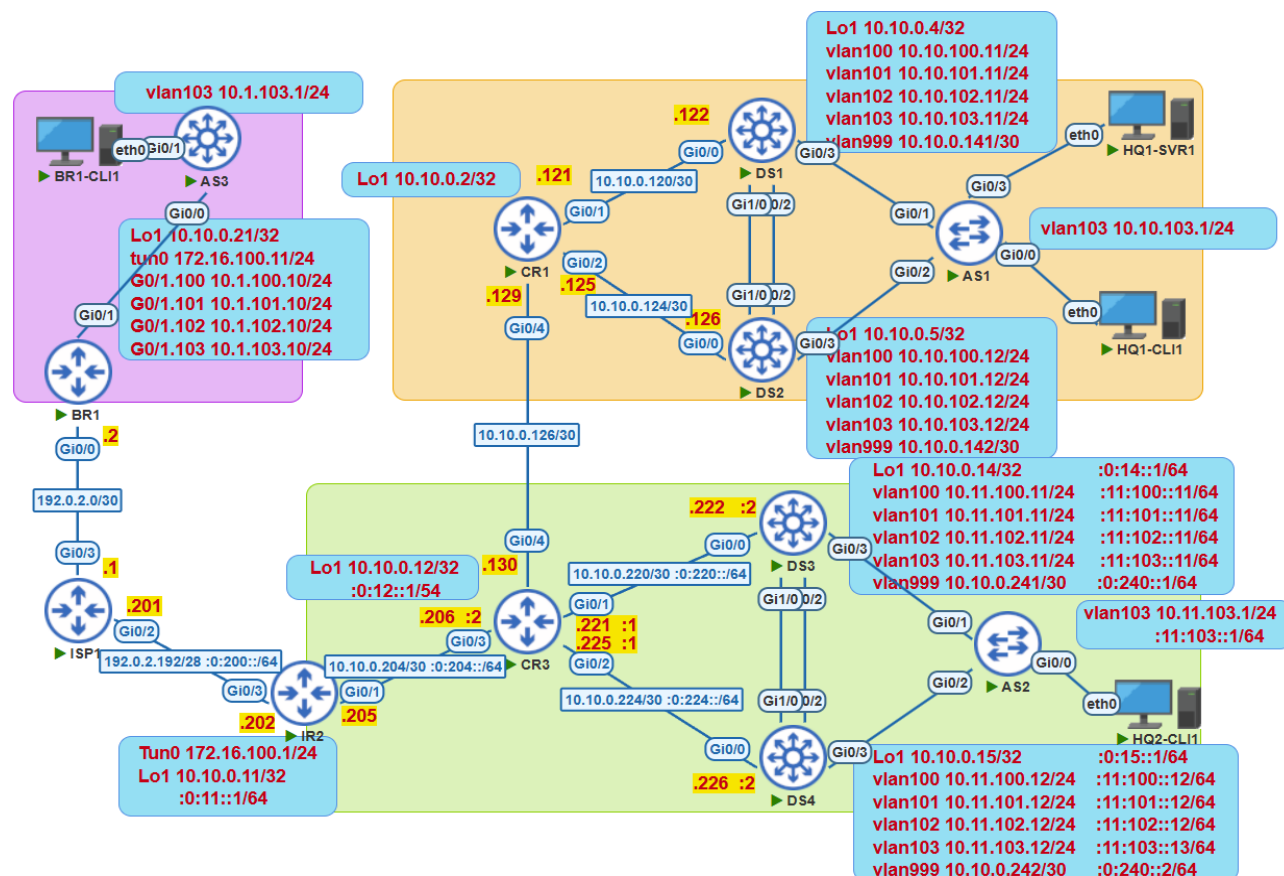
ОПИСАНИЕ ПРОЕКТА И ЗАДАЧ

В современной IT-среде знание сетевых технологий становится всё более необходимым для специалистов в области IT-инжиниринга. Данный тестовый проект включает ряд задач, основанных на реальных сценариях, с акцентом на IT-сетевые технологии и интеграцию.

Физическая топология



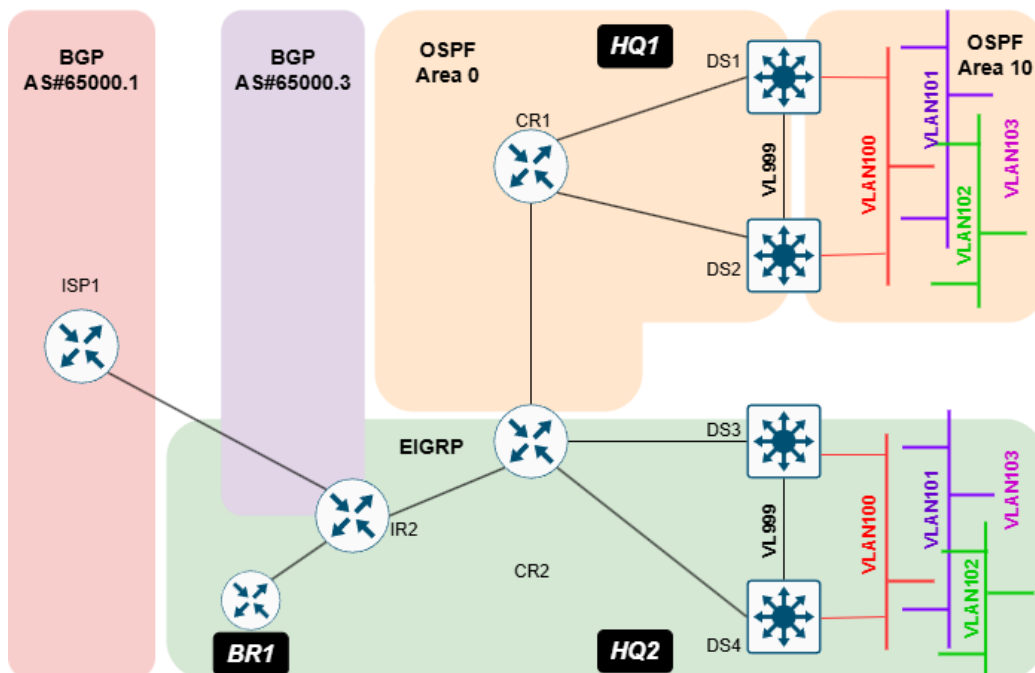
Логическая топология и адресации



Все IPv6-адреса начинаются с 2001:DB8:X:X::X/64

Топология маршрутизации

На схеме приведена топология маршрутизации, включающая BGP, EIGRP и OSPF.



ЗАДАЧИ КОНФИГУРАЦИИ

Пожалуйста, внимательно ознакомьтесь с инструкциями перед началом работы:

1. Конфигурация ISP1:

- Не вносите изменения в конфигурацию устройства ISP1. Все настройки ISP1 уже выполнены, и это устройство должно оставаться неизменным.

2. Базовые настройки:

- Ваша конфигурация будет проверяться с помощью скриптов, поэтому должны быть сохранены следующие два базовых параметра на всех маршрутизаторах и коммутаторах:

- `no ip domain lookup`
- `exec-timeout 0 0` для консоли

Эти параметры уже предустановлены – изменения не допускаются.

3. Порядок выполнения задач:

- Перед началом конфигурационных работ внимательно прочтите все задачи в каждом разделе. Некоторые задачи могут зависеть от выполнения предыдущих или последующих шагов.

4. Работающие конфигурации:

- Баллы начисляются только за корректно работающие конфигурации. Перед сдачей проекта обязательно протестируйте работоспособность всех требований, так как при внесении изменений можно нарушить ранее выполненные настройки.

5. Полное выполнение требований:

- За отдельный аспект нельзя получить частичные баллы – все требования должны быть полностью выполнены. Некоторые задачи зависят от выполнения других, как до, так и после текущего этапа.

6. Частое сохранение конфигурации:

- Сохраняйте конфигурацию регулярно – непредвиденные ситуации могут привести к потере данных.

7. Доступ к клиентским устройствам и серверу:

- Все клиентские устройства (например, HQ1-CLI1, HQ2-CLI1, BR1-CLI1, BR2-CLI1) и сервер (HQ1-SVR1) преднастроены для доступа по учётным данным `admin\Skill139@2025`. Не изменяйте эти пароли.

8. Проверка конфигураций хостов:

- Хотя хосты поставляются с базовыми настройками, проверьте их и при необходимости внесите корректировки.

9. Состояние интерфейсов:

- Если для тестирования какие-либо интерфейсы были отключены, убедитесь, что они включены перед сдачей проекта.

10. Статическая маршрутизация:

- Конфигурация статических маршрутов не допускается, если они не сгенерированы автоматически в рамках настроек OSPF/EIGRP.

Часть 1. Базовая конфигурация

Устройства: DS1–DS4, AS1–AS3, BR1

1. IP-адресация

- Настроить IPv4 адреса на указанных устройствах в соответствии со схемой адресации.

2. Конфигурация времени

- Настроить на всех устройствах HQ1, HQ2 и BR1 часовой пояс PKT (UTC+5)

3. Доменные и учетные записи

- Установить доменное имя **wsa2025.net** на всех устройствах.
- Настроить enable-пароль **Skill39@2025** и создать локального пользователя **admin** с этим же паролем на всех маршрутизаторах и коммутаторах. Все пароли должны использовать шифрование типа 9.

Часть 2. Коммутация

1. VTP:

- Настроить VTP домен **WSA2025** на коммутаторах DS1, DS2, DS3, DS4, AS1, AS2, AS3 и AS4.
- Запретить распространение VTP сообщений на этих устройствах.

2. VLAN:

- Создать на всех коммутаторах следующие VLAN:

VLAN ID	НАЗВАНИЕ VLAN	УСТРОЙСТВА
100	SERVER	DS1, DS2, DS3, DS4, AS1, AS2, AS3
101	CLIENT_1	DS1, DS2, DS3, DS4, AS1, AS2, AS3
102	CLIENT_2	DS1, DS2, DS3, DS4, AS1, AS2, AS3
103	MGMT	DS1, DS2, DS3, DS4, AS1, AS2, AS3
999	L3_P2P	DS1, DS2, DS3, DS4

3. STP:

- В офисе HQ1 сделать DS1 корневым мостом для всех VLAN (включая будущие) и DS2 – резервным (в случае отказа DS1).

- В офисе HQ2 сделать DS3 корневым мостом и DS4 – резервным.
- Выбрать режим STP с максимально быстрой сходимостью.

4. Trunk-порты:

- На всех распределительных коммутаторах (DS1–DS4) настроить порты, соединяющие их с AS1 и AS2, как trunk-порты с native VLAN 888.
- На коммутаторе AS3 интерфейс GigabitEthernet0/0 настроить как trunk, оставив VLAN 1 в качестве native.

5. Логические интерфейсы (EtherChannel):

- **Между DS1 и DS2:**
 - Создать логический интерфейс (номер 12) для передачи трафика всех VLAN, объединяя физические интерфейсы G0/2 и G1/0, используя протокол LACP с возможностью инициирования согласования обеими сторонами.
- **Между DS3 и DS4:**
 - Создать логический интерфейс (номер 34) для передачи трафика, без динамического согласования, объединяя интерфейсы G0/2 и G1/0.

6. HSRP:

- Настроить HSRP для VLAN 100–103:
 - В каждом /24 сегменте виртуальный IP-адрес должен оканчиваться на .10 (например, 10.10.100.10 для VLAN 100).
 - DS1 (в HQ1) и DS3 (в HQ2) должны быть активными, а DS2 и DS4 – резервными, с автоматическим возвратом активной роли при восстановлении основного устройства.
- Для HQ2: дополнительно настроить IPv6 HSRP для VLAN 101 и 102 на DS3 и DS4 с группами 1101 и 1102 соответственно; виртуальный IPv6 адрес – FE80::10.

Часть 3. EIGRP (для HQ2)

1. Запуск процесса:

- Настроить на устройствах IR1, CR2, DS3 и DS4 единый процесс EIGRP с именем **WSA2025**, включающим поддержку IPv4 и IPv6.
- Для IPv4 использовать автономную систему номер 100. Loopback1 должен использоваться в качестве router-id.

2. Объявление маршрутов:

- Объявить все Loopback-интерфейсы и /30 point-to-point сети на IR1, CR2, DS3 и DS4.
- На DS3 и DS4 дополнительно объявить VLAN-сети 100–103.

3. Управление hello-сообщениями:

- По умолчанию подавлять hello-сообщения на всех интерфейсах, разрешив их только там, где необходимы EIGRP-смежности.
- 4. **Дефолт-маршрут:**
 - На IR1 настроить объявление дефолтного маршрута в EIGRP, если он получен от ISP1 через BGP.
- 5. **Суммаризация:**
 - На CR2 настроить суммаризацию для VLAN 100–103 в HQ2 и объявить суммарный маршрут IR1.
- 6. **IPv6 EIGRP:**
 - Настроить IPv6 EIGRP в том же процессе (WSA2025, AS 100) на HQ2.
 - На DS3 и DS4 не должны устанавливаться смежности по IPv6 для VLAN 100, 101, 102 и 103.
- 7. **Проверка:**
 - Убедитесь, что с устройства HQ2 можно выполнить ping до Loopback1 IR1 (например, 2001:DB8:0:11::1/64).

Часть 4. OSPF (для HQ1)

1. **Запуск процесса:**
 - Запустить OSPF процесс 100 на IR1, CR1, DS1 и DS2.
 - Использовать Loopback1 в качестве router-id.
2. **Объявление маршрутов:**
 - Объявить все /30 point-to-point сети и Loopback1 в area 0.
3. **Включение VLAN-сетей:**
 - На DS1 и DS2 добавить сети VLAN 100–103 в area 10.
4. **Hello-сообщения:**
 - Настроить OSPF так, чтобы hello-сообщения отправлялись только по /30 соединениям.
5. **DR/BDR:**
 - При установлении смежностей OSPF не проводить выбор DR/BDR.
6. **Дефолт-маршрут:**
 - Настроить на CR2 объявление дефолтного маршрута в OSPF.
7. **Перераспределение OSPF в EIGRP:**
 - На CR2 настроить перераспределение сетей OSPF в EIGRP, чтобы обеспечить доступ между подсетями HQ1 и HQ2.
8. **Суммаризация:**

- На ABR и ASBR настроить суммаризацию так, чтобы в OSPF объявлялась только сеть 10.10.100.0/22.

9. Проверка маршрутов:

- После настройки маршрутизации для BR1 и BR2 убедитесь, что в таблице маршрутов OSPF на устройствах HQ1 присутствуют:
 - Суммарные маршруты: 10.1.100.0/22 и 10.2.100.0/22.
 - Loopback-адреса: 10.10.0.21 и 10.10.0.22.

Часть 5. BGP

1. eBGP:

- Настроить eBGP-сессию на IR1 (AS 65000.3) с использованием IP-адреса интерфейсов G0/2 (192.0.2.201).
- ISP1 уже настроен с параметрами: keepalive – 10 с, holddown – 30 с, аутентификация – пароль **Skill39@2025**.

2. Обработка префиксов от ISP1:

- На IR1 принимаются префиксы 198.51.100.0/24 и 203.0.113.0/24 от ISP1.
- Для тестирования используйте IP-адреса 198.51.100.1 и 203.0.113.1 (проверка с HQ-CLI1 и HQ2-CLI1 с помощью ping и traceroute).

Часть 6. IP-сервисы

1. NAT:

- Для пользователей из VLAN 101 и 102 (около 400 пользователей в HQ1, HQ2, BR1 и BR2) настроить source NAT:
- При проходе через IR1 – трансляция в диапазоне 192.0.2.104–192.0.2.110.
- Для сервера HQ1-SVR1 (IP 10.10.100.101) настроить NAT так, чтобы исходящий IP был: 192.0.2.205 при маршрутизации через IR1
- Тестирование можно выполнить, настроив интерфейс AS1 G0/3 в VLAN 100.

2. NTP:

- Интернет-маршрутизатор IR1 должен синхронизировать время с адресом ISP1 (192.0.2.201).
- Остальные устройства (HQ1, HQ2 и BR1) используют IR1 (10.10.0.11) в качестве NTP-сервера.
- Для NTP-коммуникаций использовать Loopback-интерфейсы (за исключением AS1–AS3, где можно использовать IP SVI 103).

3. DHCP:

- На DS1:
 - Для VLAN 101 – пул адресов 10.10.101.101–10.10.101.254, шлюз – 10.10.101.10.

- Для VLAN 102 – пул адресов 10.10.102.101–10.10.102.254, шлюз – 10.10.102.10.
- **На DS3:**
 - Для VLAN 101 – пул адресов 10.11.101.101–10.11.101.254, шлюз – 10.11.101.10.
 - Для VLAN 102 – пул адресов 10.11.102.101–10.11.102.254, шлюз – 10.11.102.10.
- **На филиале (BR1):**
 - для VLAN 101 – пул 10.1.101.101–10.1.101.254, шлюз – 10.1.101.10.

Часть 7. Безопасность и VPN

1. VPN (GRE):

- **На IR1 (HQ2):** настроить для подключения филиала с использованием следующих параметров:
 - Tunnel-интерфейс 0 с IP-адресом 172.16.100.1/24
- **BR1:**
 - Tunnel-интерфейс 0 с IP 172.16.100.11/24
 - Дополнительно разрешены статические маршруты:

```
ip route 192.0.2.192 255.255.255.240 192.0.2.1
```

2. EIGRP между филиалом и HQ2:

- Настроить EIGRP на BR1 и IR1 так, чтобы филиальный маршрутизатор объявлял суммарный маршрут для сетей VLAN (100–103) своего сайта.

3. SSH:

- Включить SSH на IR1 с использованием самой безопасной доступной версии.
- Использовать учётные данные admin/Skill139@2025.
- Отключить Telnet.

4. Ограничение доступа по SSH:

- Разрешить SSH-подключения к IR1 только с устройства HQ1-SVR1 (IP 10.10.100.101/24).

5. Безопасность портов:

- Включить port security на switch-портах, к которым подключены клиентские устройства HQ1-CLI и HQ2-CLI1.
- Настроить ограничение числа MAC-адресов до минимально необходимого.
- При нарушении port security порт должен быть отключён, с генерацией syslog-сообщения, и автоматически восстановлен через 3 минуты.

6. ACL:

- Реализовать ACL, блокирующий доступ пользователей VLAN 102 (на HQ1, HQ2, BR1 и BR2) к серверу HQ1-SVR1, при этом не нарушая исходящий доступ сервера к другим устройствам.