КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

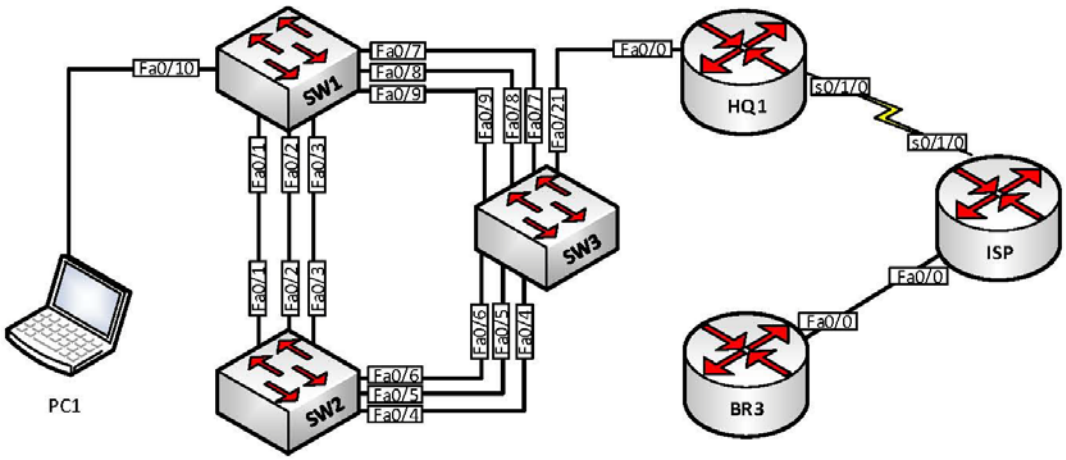
КОНКУРСНОЕ ЗАДАНИЕ

МОДУЛЬ С: NETWORKISLAND

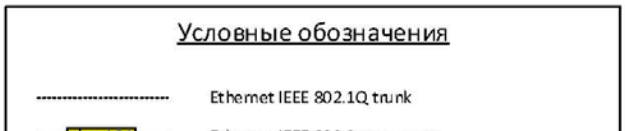
Разработано экспертами WSR:
Горбачев А.П.

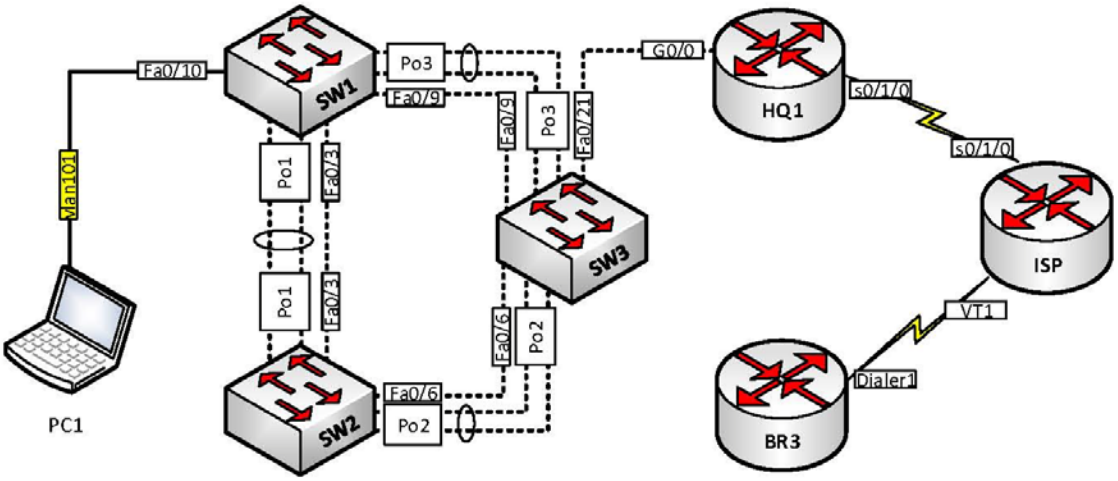
Дата: 20.09.16
Версия: 8

Network Island.
L1 diagram

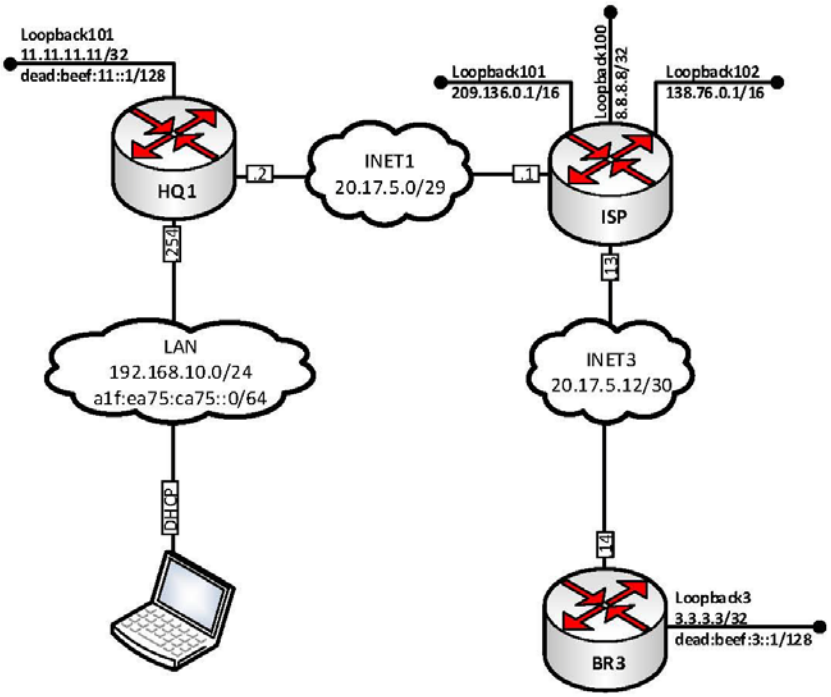


Network Island.
L2 diagram

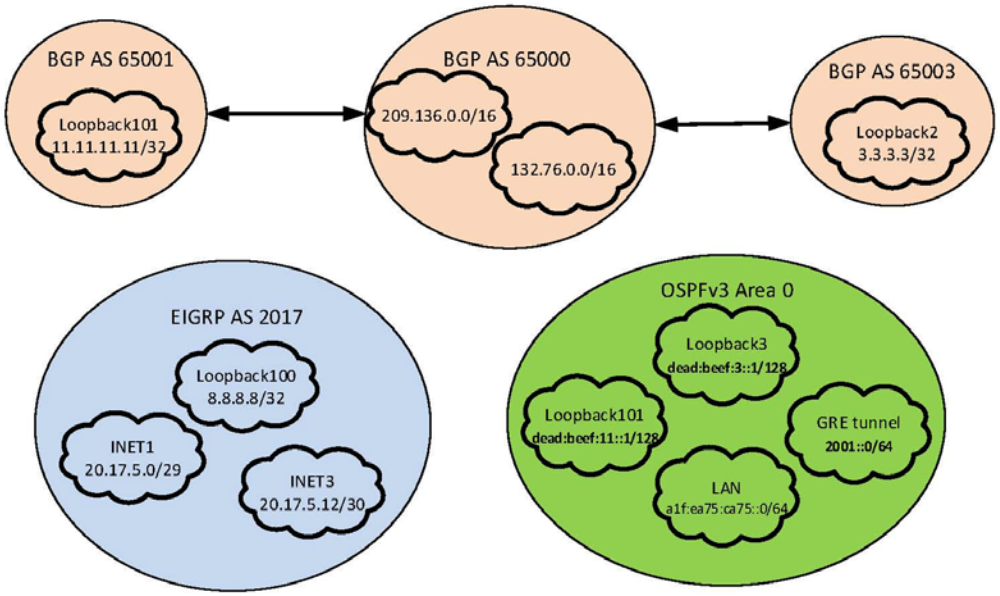




Network Island.
L3 diagram



Network Island.
Routing diagram



Базовая настройка

1. Задайте имя ВСЕХ устройств в соответствии с топологией.
2. Назначьте для ВСЕХ устройств доменное имя wsr2017.ru.
3. Создайте на ВСЕХ устройствах пользователя wsr2017 с паролем cisco:
    a. пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
    b. пользователь должен обладать максимальным уровнем привилегий.
4. Для ВСЕХ устройств реализуйте модель AAA:
    a. аутентификация на удаленной консоли должна производиться с использованием локальной базы данных;
    b. после успешной аутентификации при входе с удаленной консоли пользователь сразу должен попадать в режим с максимальным уровнем привилегий;
    c. настройте необходимость аутентификации на локальной консоли;
    d. при успешной аутентификации на локальной консоли пользователь должен попадать в режим с минимальным уровнем привилегий;
    e. на BR3 при успешной аутентификации на локальной консоли пользователь должен попадать в режим с максимальным уровнем привилегий.
5. На ВСЕХ устройствах установите пароль wsr на вход в привилегированный режим:
    a. пароль должен храниться в конфигурации НЕ в виде результата хэш-функции;
    b. настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
6. На ВСЕХ устройствах создайте виртуальные интерфейсы, подинтерфейсы и интерфейсы типа петля. Назначьте ip-адреса в соответствии с L3-диаграммой:
    a. для коммутаторов SW1, SW2 и SW3 создайте виртуальные интерфейсы в ВЛВС 101.
    b. назначьте им ip-адреса .51, .52 и .53 из подсети LAN соответственно.
    c. используйте автоматическую генерацию IPv6 адресов в сети LAN на интерфейсе маршрутизатора HQ1;
    d. на ВСЕХ коммутаторах отключите ВСЕ неиспользуемые порты.
7. Все устройства должны быть доступны для управления по протоколу SSH версии 2.
8. На маршрутизаторе HQ1 установите правильное локальное время.

Настройкакоммутации

1. На ВСЕХ коммутаторах создайте ВЛВС:
    a. под номером 101, назначьте имя LAN для этой подсети.
2. На коммутаторах SW1, SW2 и SW3 выполните настройку протокола динамического согласования параметров магистральных соединений (DTP):
    a. на коммутаторе SW3 переведите порты в Fa0/4-9 в режим, при котором коммутатор на данных портах будет инициировать согласование параметров магистрального соединения.
    b. переведите порты Fa0/7-9 на SW1 и Fa0/4-6 на SW2 в режим, при котором каждый коммутатор ожидает начала согласования параметров от соседа, но сам не инициирует согласование.
    c. переведите порты Fa0/1-3 на SW1 и SW2 в режим передачи трафика по протоколу IEEE 802.1q. Явно отключите динамическое согласование магистральных соединений.
3. Настройте агрегирование каналов связи между коммутаторами:
    a. номера портовых групп:

i. 1 — между коммутаторами SW1 <-> SW2;
ii. 2 — между коммутаторами SW2 <-> SW3;
iii. 3 — между коммутаторами SW3 <-> SW1.

b. коммутатор SW3 должен быть настроен в режиме активного согласования по обеим портовым группам по протоколу LACP;
c. коммутаторы SW1 и SW2 должны быть настроены в пассивном режиме LACP с коммутатором SW3;
d. коммутатор SW2 должен быть настроен в режиме активного согласования по протоколу PAgP с коммутатором SW1;
e. коммутатор SW1 должен быть настроен в режиме пассивного согласования по протоколу PAgP с коммутатором SW2.

4. Конфигурация протокола остовного дерева:
   a. на всех коммутаторах используйте вариант протокола STP, совместимый со стандартом 802.1w.
   b. коммутатор SW1 должен являться корнем связующего дерева в VLAN 101. В случае его отказа, корнем должен стать коммутатор SW2. В случае отказа SW2 — коммутатор SW3.
   c. на коммутаторах SW1, SW2 и SW3 в VLAN 101 используйте для передачи данных порты, не состоящие в портовых группах.
5. На порту Fa0/10 коммутатора SW1 включите защиту от атаки на смену корня остовного дерева. При получении информации о том, что на этом порту находится потенциальный корень дерева в VLAN 101, порт должен переводиться в состояние err-disable.
6. Настройте порт Fa0/10 коммутатора SW1 таким образом, чтобы порт переходил в состояние Forwarding не дожидаясь пересчета оставного дерева.
7. Трафик сети LAN между HQ1 и SW3 должен передаваться без тэга IEEE 802.1Q.

Настройка подключений к глобальным сетям

1. На маршрутизаторе HQ1 настройте PPP для подключения к маршрутизатору ISP. Для аутентификации используйте протокол CHAP с паролем cisco.
2. На маршрутизаторе BR3 настройте подключение к ISP через PPPoE;
   a. Используйте протокол PAP для аутентификации;
   b. используйте учетную запись cisco\cisco.

Настройка маршрутизации

1. На маршрутизаторах ISP, HQ1 и BR3 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2017:
   a. включите в обновления маршрутизации сети в соответствии с Routing-диаграммой;
   b. используйте алгоритм аутентификации md5 с ключом WSR.
2. На маршрутизаторах ISP, HQ1 и BR3 настройте протокол динамической маршрутизации BGP:
   a. номера автономных систем 65000, 65001 и 65003 для ISP, HQ1 и BR3 соответственно;
   b. включите в обновления маршрутизации сети в соответствии с Routing-диаграммой;
   c. настройте фильтрацию маршрутов на HQ1 таким образом, чтобы в таблице маршрутизации отсутствовал маршрут 209.136.0.0/16.

3. на маршрутизаторах HQ1 и BR3 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
    a. включите в обновления маршрутизации сети LAN, Loopback101 и Loopback3;
    b. используйте зону с номером 0.

Настройка служб

1. Назначьте в качестве сервера синхронизации времени маршрутизатор HQ1:
    a. настройте временную зону с названием SAMT;
    b. настройте сервер синхронизации времени. Используйте стратум 2;
    c. настройте маршрутизатор BR3 в качестве клиента сервера;
    d. используйте аутентификацию MD5 с ключом WSR.
2. На маршрутизаторе HQ1 настройте динамическую трансляцию портов (PAT) в адрес интерфейса, подключенного к сети INET1 для сети LAN.
3. Настройте протокол динамической конфигурации хостов со следующими характеристиками:
    a. на маршрутизаторе HQ1 для подсети LAN:
        i. адрес сети – 192.168.10.0/24;
        ii. адрес шлюза по умолчанию — адрес интерфейса в данной подсети;
        iii. адрес сервера службы доменных имен — 192.168.10.100;
        iv. исключите из раздачи первые 100 адресов.

Настройка механизмов безопасности

1. На маршрутизаторе BR3 настройте ролевое управление доступом:
    a. создайте пользователей user1, user2, user3, user4 и user5с паролем cisco:
        i. пользователь user1 должен быть авторизован выполнять все команды привилегированного режима кроме show version и show ip route, но должен быть авторизован выполнять все остальные команды show ip *;
        ii. пользователь user2 должен быть авторизован выполнять все команды непривилегированного режима включая showversion, но не show ip route.
    b. создайте view-контекст “show_view”. Включите в него:
        i. команду show version;
        ii. все команды show ip *;
        iii. команду who;
        iv. при входе на маршрутизатор пользователь user3 должен попадать в данный контекст.
    c. создайте view-контекст “ping_view”. Включите в него:
        i. команду ping;
        ii. команду traceroute;
        iii. при входе на маршрутизатор пользователь user4 должен попадать в данный контекст.
    d. создайте superview-контекст, объединяющий эти 2 контекста. Создайте пользователя user5 с паролем cisco. При входе на маршрутизатор пользователь user5 должен попадать в данный контекст.
    e. убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов.
2. На порту коммутатора SW1, к которому подключен PC1, включите и настройте PortSecurity со следующими параметрами:
    a. не более 2 адресов на интерфейсе;

b. адреса должны быть динамически сохранены в текущей конфигурации;
c. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.

3. На коммутаторе SW1 включите DHCP-snooping для подсети LAN. Используйте флеш-память в качестве места хранения базы данных
4. На коммутаторе SW1 включите динамическую проверку ARP-запросов в сети LAN.

Конфигурация виртуальных частных сетей

1. На маршрутизаторах HQ1 и BR3 настройтеGRE-туннель:
   a. используйте в качестве VTI интерфейс Tunnel100;
   b. используйте адресацию 2001::0/64.
2. На маршрутизаторах HQ1 и BR3 настройте IKEv1 IPsecSite-to-SiteVPN и примените его к созданномуGRE-туннелю:
   a. параметры политики первой фазы:
      i. проверка целостности – MD5;
      ii. шифрование – AES-128;
      iii. группа Диффи-Хэлмана – 5.
   b. параметры преобразования трафика для второй фазы:
      i. протокол – ESP;
      ii. шифрование – AES-128;
      iii. рроверка целостности – MD5.