Варианты изменений в задание по острову Network

Пояснительная записка:

Данный комплект изменений призван сделать проще процесс внесения изменений в конкурсное задание в день С-2.

Практика 30% изменений позволяет исключить «вызубривание» и бездумное выполнение задания за счёт воспроизведения заранее выученной последовательности команд, не вникая в их смысл или в принципы работы связанных с ними технологий.

Обеспечить полноценные изменения в задание в С-2, соблюдая при этом единообразие с другими региональными чемпионатами с одной стороны, и не нарушая выполнимости задания с другой стороны, является достаточно сложной и трудоёмкой задачей.

Предложенные ниже готовые комплекты изменений максимально оптимизируют этот процесс для команды экспертов. Принятие решений о выборе того или иного изменения можно оперативно провести, сгенерировав случайные числа (либо вручную, либо с помощью имеющейся в комплекте таблицы).

Помимо изменений в задание меняется также и таблица адресации.

Такой метод не исключает подготовку к выполнению задания заранее, но усложняет тотальное вызубривание всех конфигураций. В качестве побочного эффекта такой подход требует более внимательного чтения задания.

Принцип работы:

Всего предложено 10 независимых друг от друга изменений. Для каждого изменения предложен вариант №1 (как в текущем шаблоне) и вариант №2 (изменённая версия).

В день С-2 команда, состоящая из всех экспертов, должна провести выбор всех 10 значений случайным образом. Для этого можно воспользоваться готовой таблицей в файле RC1718_Random_Generator. Каждое значение будет либо 1 (вариант №1, ничего не меняем), либо 2 (вариант №2, заменяем в тексте задание согласно предложенному).

В итоге должен получиться список правок, которые следует внести в шаблон вместе с актуальной схемой адресации. В соответствии с этими правками также вносятся коррективы в схему оценки острова Network.

Важно!

- Выбор производится в С-2. После этого никаких изменений не вносится.
- В рамках одного чемпионата все участники должны получить идентичное задание с идентичными изменениями и схемой адресации.
- Следует внимательно проверять использование правильных адресов и идентификаторов. Использование участником идентификаторов, отличных от приведённых в задании, следует считать ошибкой.
- До проверки необходимо ещё раз убедиться, что экспертам доступна актуальная версия задания и схемы адресации. При проверке эксперты сами должны тщательно следить за использованием правильных адресов и идентификаторов, чтобы корректно оценить работу участника.
- Внесение изменений в задание должно быть задокументировано в соответствующем протоколе

Изменение 1

Вариант 1 (по умолчанию)

Настройки коммутации, пункт 5:

5. На порту Fa0/5 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 root-inconsistent.

Вариант 2

Настройки коммутации, пункт 5:

5. На порту Fa0/5 коммутатора SW1 включите защиту от нежелательных BPDU. При получении BPDU на этом порту, порт должен переводиться в состояние err-disabled.

Изменение 2

Вариант 1 (по умолчанию)

Настройка подключений к глобальным сетям, пункт 2a:

2. На маршрутизаторе BR3 настройте подключение к ISP через PPPoE.
    a. Используйте протокол PAP для аутентификации

Вариант 2

Настройка подключений к глобальным сетям, пункт 2a:

3. На маршрутизаторе BR3 настройте подключение к ISP через PPPoE.
    a. Используйте протокол CHAP для аутентификации

Изменение 3

Вариант 1 (по умолчанию)

Настройка подключений к глобальным сетям, пункт 2c:

c. Аутентификация должна быть двусторонней (клиент и сервер проверяют подлинность друг друга).

Вариант 2

Настройка подключений к глобальным сетям, пункт 2c:

c. Аутентификация должна быть односторонней (только сервер проверяет подлинность клиента).

Изменение 4

Вариант 1 (по умолчанию)

Настройка маршрутизации, пункты 1 и 2

1. На маршрутизаторах ISP, HQ1 и BR3 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2018.
    a. Включите маршрутизацию для сетей INET1, INET3, а также на интерфейсе Loopback100 маршрутизатора HQ1 и на интерфейсах Loopback101 и Loopback102 маршрутизатора BR3.
    b. Используйте алгоритм аутентификации md5 с ключом WSR.
    c. Настройте суммаризацию для сетей на интерфейсах Loopback101 и Loopback102 маршрутизатора BR3 таким образом, чтобы BR3 анонсировал вместо этих двух сетей только одну суммарную сеть минимально возможного размера.
    d. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. На маршрутизаторах HQ1 и BR3 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
    a. Используйте область с номером 0.
    b. Включите в обновления маршрутизации сети LAN, Tunnel100, Loopback101 и Loopback103.
    c. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

Вариант 2

Настройка маршрутизации, пункты 1 и 2

1. На маршрутизаторах ISP, HQ1 и BR3 настройте протокол динамической маршрутизации OSPFv2 с номером процесса 1.
    a. Включите маршрутизацию для сетей INET1, INET3, а также на интерфейсе Loopback100 маршрутизатора HQ1 и на интерфейсах Loopback101 и Loopback102 маршрутизатора BR3.
    b. Используйте алгоритм аутентификации md5 с ключом WSR.
    c. Используйте область 0 для всех интерфейсов, кроме Loopback101 и Loopback102 на маршрутизаторе BR3.
    d. Настройте суммаризацию для сетей на интерфейсах Loopback101 и Loopback102 маршрутизатора BR3 таким образом, чтобы BR3 анонсировал вместо этих двух сетей только одну суммарную сеть минимально возможного размера. Используйте для этих интерфейсов область 1.
    e. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. На маршрутизаторах HQ1 и BR3 настройте протокол динамической маршрутизации EIGRPv6 с номером автономной системы 2018.
    a. Включите в обновления маршрутизации сети LAN, Loopback101 и Loopback103.
    b. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

Изменение 5

Вариант 1 (по умолчанию)

Настройка маршрутизации, пункт 4

4. Оптимизируйте сходимость протоколов OSPF и EIGRP.
    a. Для протокола EIGRP настройте интерфейсы между маршрутизаторами так, чтобы hello-пакеты отправлялись раз в секунду, а соседство считалось недействительным после 4 пропущенных hello-пакетов.
    b. Для протокола OSPF настройте интерфейсы между маршрутизаторами так, чтобы соседство разрывалось после 15 секунд простоя, и за эти 15 секунд маршрутизатор должен бы был отправить 3 hello-пакета.

Вариант 2

Настройка маршрутизации, пункт 4

4. Оптимизируйте сходимость протоколов OSPF и EIGRP.
    a. Для протокола EIGRP настройте интерфейсы между маршрутизаторами так, чтобы соседство разрывалось после 10 секунд простоя, и за эти 10 секунд маршрутизатор должен бы был отправить 3 hello-пакета.
    b. Для протокола OSPF настройте интерфейсы между маршрутизаторами так, чтобы hello-пакеты отправлялись раз в две секунды, а соседство считалось недействительным после 5 пропущенных hello-пакетов.

Изменение 6

Вариант 1 (по умолчанию)

Базовая настройка, пункт 8:

8. На маршрутизаторе HQ1 установите правильное время с учётом часового пояса.

Настройка служб, пункт 1:

1. Назначьте в качестве сервера синхронизации времени маршрутизатор HQ1.
    a. Настройте временную зону с названием MSK, укажите разницу с UTC +3 часа.
    b. Настройте сервер синхронизации времени. Используйте стратум 2.
    c. Настройте маршрутизатор BR3 в качестве клиента NTP
    d. Используйте аутентификацию MD5 с ключом WSR

Вариант 2

Базовая настройка, пункт 8:

8. На маршрутизаторе BR3 установите правильное время с учётом часового пояса.

Настройка служб, пункт 1:

1. Назначьте в качестве сервера синхронизации времени маршрутизатор BR3.
    e. Настройте временную зону с названием MSK, укажите разницу с UTC +3 часа.
    f. Настройте сервер синхронизации времени. Используйте стратум 3.
    g. Настройте маршрутизатор HQ1 в качестве клиента NTP
    h. Используйте аутентификацию MD5 с ключом WSR

Изменение 7

Вариант 1 (по умолчанию)

Настройка механизмов безопасности, пункт 1:

1. На маршрутизаторе BR3 настройте пользователей с ограниченными правами.
    a. Создайте пользователей user1 и user2 с паролем cisco.
    b. Пользователь user1 должен быть авторизован выполнять все команды пользовательского режима, а также иметь возможность осуществлять перезагрузку, включать и выключать отладку и удалять стартовую конфигурацию.
    c. Создайте view-контекст “show_view”. Включите в него
        i. Команду show version
        ii. Все команды show ip *
        iii. Команду who
    d. Создайте view-контекст “ping_view”. Включите в него
        i. Команду ping
        ii. Команду traceroute
    e. Создайте superview-контекст, объединяющий эти 2 контекста. При входе на маршрутизатор пользователь user2 должен попадать в данный контекст
    f. Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.

Вариант 2

Настройка механизмов безопасности, пункт 1:

1. На маршрутизаторе BR3 настройте пользователей с ограниченными правами.
    a. Создайте пользователей user1 и user2 с паролем cisco.
    b. Пользователь user1 должен быть авторизован выполнять все команды пользовательского режима, а также иметь возможность осуществлять перезагрузку, настраивать время и сохранять стартовую конфигурацию.
    c. Создайте view-контекст “show_view”. Включите в него

iv. Команду show clock
v. Все команды show ip route *
vi. Команду show ip interface brief

d. Создайте view-контекст “ping_view”. Включите в него
iii. Команду ping

e. Создайте superview-контекст, объединяющий эти 2 контекста. При входе на маршрутизатор пользователь user2 должен попадать в данный контекст
f. Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.

Изменение 8

Вариант 1 (по умолчанию)

Настройка механизмов безопасности, пункт 2:

2. На порту коммутатора SW1, к которому подключен PC1, включите и настройте Port Security со следующими параметрами:
   a. не более 2 адресов на интерфейсе
   b. адреса должны динамически пополняться, но не сохраняться в текущей конфигурации
   c. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.

Вариант 2

Настройка механизмов безопасности, пункт 2:

2. На порту коммутатора SW1, к которому подключен PC1, включите и настройте Port Security со следующими параметрами:
   d. не более 2 адресов на интерфейсе
   e. адреса должны динамически пополняться и автоматически сохраняться в текущей конфигурации
   f. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт должен быть отключен.

Изменение 9

Вариант 1 (по умолчанию)

Настройка механизмов безопасности, пункт 5:

5. На коммутаторе SW3 настройте зеркалирование трафика, проходящего через порт 0/21 в оба направления, на порт 0/11.

Вариант 2

Настройка механизмов безопасности, пункт 5:

5. На коммутаторе SW3 настройте зеркалирование трафика, приходящего на порт 0/21, на порт 0/12.

Изменение 10

Вариант 1 (по умолчанию)

Конфигурация виртуальных частных сетей, пункт 2:

2. На маршрутизаторах HQ1 и BR3 настройте IKEv1 IPsec Site-to-Site VPN и примените его к созданному GRE-туннелю
    a. Параметры политики первой фазы:
        i. Проверка целостности – MD5
        ii. Шифрование – DES
        iii. Группа Диффи-Хэлмана – 5
    b. Параметры преобразования трафика для второй фазы:
        i. Протокол – ESP
        ii. Шифрование – DES
        iii. Проверка целостности – MD5

Вариант 2

Конфигурация виртуальных частных сетей, пункт 2:

2. На маршрутизаторах HQ1 и BR3 настройте IKEv1 IPsec Site-to-Site VPN и примените его к созданному GRE-туннелю
    c. Параметры политики первой фазы:
        iv. Проверка целостности – SHA1
        v. Шифрование – AES-128
        vi. Группа Диффи-Хэлмана – 5
    d. Параметры преобразования трафика для второй фазы:
        iv. Протокол – ESP
        v. Шифрование – AES-128
        vi. Проверка целостности – SHA1