Конкурсное задание

Компетенция КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Конкурсное задание включает в себя следующие разделы:

1) Формы участия в конкурсе
2) Задание для конкурса
3) Модули задания и необходимое время
4) Критерии оценки
5) Необходимые приложения

Количество часов на выполнение задания: 15 ч.

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по пуско-наладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники соревнований получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Задание регионального чемпионат является утвержденным. В нем присутствуют 3 из 5 модулей, т.е. возможно набрать максимально 45 из 100 баллов

Конкурс включает в себя Пуско-наладку инфраструктуры на основе ОС семейства Linux; Пуско-наладку инфраструктуры на основе ОС семейства Windows; Пуско-наладку телекоммуникационного оборудования.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри, по согласованию с менеджером компетенции.

Конкурсное задание должно выполняться по модульно, циклически по модулям A-B-C. Оценка каждого модуля происходит Ежедневно.

Задания разработаны и протестированы группой сертифицированных экспертов:

Модуль конкурсного задания	Роль	ФИО Эксперта
Модуль A: «Пуско-наладка инфраструктуры на основе ОС семейства Linux»	Ведущий разработчик	М.М. Фучко
Модуль B: «Пуско-наладка инфраструктуры на основе ОС семейства Windows»	Ведущий разработчик	А.Б. Мананников
	Группа разработки	Д.В. Дюгуров
Модуль C: «Пуско-наладка телекоммуникационного оборудования»	Ведущий разработчик	Д.Н. Новиков

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 1

Таблица 1 – Время выполнение модуля

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Модуль А: «Пуско-наладка инфраструктуры на основе ОС семейства Linux»	В соответствии с жеребьёвкой по циклу А-В-С	5 ч.
2	Модуль В: «Пуско-наладка инфраструктуры на основе ОС семейства Windows»		5 ч.
3	Модуль С: «Пуско-наладка телекоммуникационного оборудования»		5 ч.

Модуль А: «Пуско-наладка инфраструктуры на основе ОС семейства Linux»

Версия 2019.1.0 от 28.02.19.

ВВЕДЕНИЕ

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном, интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

- Базовая конфигурация
- Конфигурация внутренней инфраструктуры ЦОД
- Конфигурация пограничной инфраструктуры ЦОД
- Конфигурация служб хранения данных ЦОД
- Конфигурация пользовательских служб ЦОД
- Конфигурация клиентских ВМ

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполнять поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает, что работа не будет оценена. Например, для удаленного доступа необходимо сконфигурировать IPsec-туннель, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже.

На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать

временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

В случае недоступности DNS-сервисов сформируйте файл **/etc/hosts** в соответствии с **Таблицей 1** на всех хостах. Проверка по IP-адресам версии 4 выполняться не будет. В случае корректной работы DNS-сервисов изменения в файле **/etc/hosts** не требуются и могут повлечь потерю баллов за настройку DNS.

Виртуальная машина ISP преднастроена и не требует доступа.

Доступ к остальным виртуальным машинам настроен по аккаунту root:toor

Доступ к клиентским виртуальным машинам настроен по аккаунту skill39:Skill39

Если при настройке служб у вас будет запрошен пароль, используйте Skill39

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Ожидается, что конкурсное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

Вам доступен диск debian-9.8.0-amd64-BD-1.iso

Вам доступен диск debian-9.8.0-amd64-BD-2.iso

Вам доступен диск debian-9.8.0-amd64-BD-3.iso

Внимание! Все указанные компоненты предоставляются участникам в виде ISO-файлов на локальном или удаленном хранилище.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

СХЕМА ОЦЕНКИ

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимающими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

Конфигурация хостов

1) Настройте имена хостов в соответствии с **Топологией**.
2) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Таблицей 1**.
   2.1) Интерфейсы хостов в ЦОД(за исключением внешнего интерфейса FW) не должны иметь IPv4 адресов!
3) Установите дополнительные пакеты программного обеспечения:
   3.1) dnsutils
   3.2) lynx
   3.3) vim

Конфигурация внутренней инфраструктуры ЦОД (Виртуальная машина CORE)

1) Реализуйте DNS-службу на основе пакета **BIND**:
   1.1) Сервер обслуживает зону **WSR.mv**
   1.2) Наполнение зоны организовать в соответствии с **Таблицей 2**
   1.3) Сервер реализует два отображения
      1.3.1 Внутреннее, для клиентов **CORE**, **STR**, **SRV-L**, **SRV-R**.
      1.3.2 Внешнее, для доступа **DNS-proxy** на **FW**
   1.4) Файлы зон расположить в **/var/dns**
   1.5) Сервер поддерживает прямое и обратное преобразование адресов для всех зон
2) Установите и настройте сервер каталогов LDAP на базе **OpenLDAP**:
   2.1) Создайте и распределите пользователей согласно **Таблице 4**
   2.2) Группы расположите в OU Groups
   2.3) Пользователей расположите в OU Users
      2.3.1 Пользователь сервиса VPN расположить в отдельном OU VPN
   2.4) Хосты **SRV-R. SRV-L**, **CORE** и и **STR** должны аутентифицироваться средствами LDAP
3) Установите и настройте службу синхронизации времени NTP на основе пакета **chrony**:
   3.1) Используется часовой пояс **MSK**(UTC+3)
   3.2) Время должно быть синхронизировано на всех хостах ЦОД
4) Реализуйте централизованный сбор и хранение сообщений журнала на основе пакета **Rsyslog**:
   4.1) Для хранения сообщений организовать файловую структуру в соответствии с **Таблицей 3**
   4.2) Все сообщения уровня **crit** и более критичных уровней дублировать в файл **/var/mylogs/CRIT.log**
5) Реализуйте центр сертификации на базе пакета **OpenSSL**
   5.1) В качестве базовой директории используйте /var/ca
   5.2) Атрибуты CA установите следующие:
      5.2.1 Страна RU
      5.2.2 Организация MV WSR
      5.2.3 CN CA установлен в MV WSR CA
   5.3) Создайте CA
   5.4) Все сертификаты должны быть выпущены данным CA
   5.5) Все компьютеры должны доверять данному CA.

Конфигурация пограничной инфраструктуры ЦОД (Виртуальная машина FW)

1) Выполните конфигурацию сервера удаленного доступа **sshd**

1.1) Прослушиваться должен только порт **1022**
1.2) Запретите вход пользователю **root**

2) Реализуйте сервис удаленного доступа на основе технологии **OpenVPN**:
   2.1) В качестве сервера выступает **BM FW**
   2.2) Параметры туннеля
      2.2.1) Устройство TAP
      2.2.2) Порт сервера 1194
      2.2.3) Применяется сжатие трафика
      2.2.4) Адресацию выполнить в соответствии с **Таблицей 1.**
         2.2.4.1) Пользователь с сертификатом CN=Admin получает статический IPv6 адрес в соответствии с **Таблицей 1.**
      2.2.5) Используется TLS-аутентификация
   2.3) Все сертификаты должны быть выданы собственным **CA** на **BM CORE**
   2.4) Реализуйте дополнительную аутентификацию с помощью сервера OpenLDAP
      2.4.1) Разрешите доступ только пользователям из OU=VPN
   2.5) В качестве клиента выступают следующие BM
      2.5.1) **CLI-ADM**, сертификат CN=Admin
      2.5.2) **CLI-OUT**, сертификат CN=Guest
   2.6) OpenVPN-туннель должен предоставлять клиентам доступ к внутренним ресурсам сети организации

3) Реализуйте службу **DNS-Proxy** на базе пакета **BIND**
   3.1) Служба должна прослушивать внешний IPv4 адрес виртуальной машины **FW**
   3.2) Служба должна обращаться к основному **DNS-серверу** на **CORE**
   3.3) Служба должна разрешать запросы только от сервера **ISP.**

4) Настройте межсетевой экран **iptables**
   4.1) Входящие подключения должны быть разрешены к следующим службам
      4.1.1) **HTTP, HTTPS**, **DNS**, **OpenVPN**, **SSH**
   4.2) Если служба не настроена в соответствии с заданием — доступ должен быть запрещен

Конфигурация служб хранения данных ЦОД (Виртуальная машина STR)

1) Настройте дисковый массив на основе технологии **RAID** на базе пакета **mdadm**
   1.1) Используйте два виртуальных диска
   1.2) Уровень массива RAID 1
   1.3) Используйте файловую систему ext4
   1.4) В качестве точки монтирования использовать **/mnt/storage**
   1.5) Массив должен автоматически монтироваться при запуске системы
2) Организуйте доступ к хранилищу данных с помощью технологии **NFS**
   2.1) Предоставьте доступ к каталогу **/mnt/storage**
   2.2) Доступ должен быть предоставлен на чтение и запись.
      2.2.1) Доступ предоставить машинам **CORE**, **SRV-R**, **SRV-L**
   2.3) Реализуйте объединение сетевых интерфейсов на **STR** и **CORE** по технологии **teaming** для достижения надежного канала и повышенной пропускной способности.

Конфигурация пользовательских служб ЦОД

1) Реализуйте веб-службы на основе сервера **Apache**
   1.1) Раздается файл **/var/www/html/index.html**
   1.2) Файл должен содержать следующий текст
      1.2.1) «Served by <HOSTNAME>» где HOSTNAME — имя сервера
2) Реализуйте реверс-прокси сервер на базе пакета **nginx**
   2.1) Прослушивается внешний адрес **FW**
      2.1.1) Имя сайта **site.wsr.mv**
   2.2) Прослушиваются HTTP и HTTPS порты
      2.2.1) Выполняется перенаправление на HTTPS
   2.3) Запросы перенаправляются на сервера **SRV-R** и **SRV-L**
      2.3.1) Балансировка нагрузки осуществляется по принципу Round Robin
      2.3.2) Отключите кэширование ответов от серверов.

Конфигурация клиентских ВМ

1) На ВМ CLI-ADM
   1.1) Настройте разрешение DNS-имен через сервер ISP
   1.2) Установите автоматическое подключение к OpenVPN -серверу на ВМ FW
      1.2.1) Используйте сертификат CN=Admin
      1.2.2) Используйте имя пользователя VPNAdmin
      1.2.3) Подключение должно проходить по DNS-имени ВМ FW
      1.2.4) После подключения клиент должен перейти на использование сервера
      1.2.5) Выполнение авторизации должно быть автоматизировано
      1.2.6) Все конфигурационные файлы расположить в /etc/openvpn/
   1.3) Установить веб-браузер **IceWeasel\Firefox**
2) На ВМ CLI-OUT
   2.1) Настройте разрешение DNS-имен через сервер ISP
   2.2) Установите подключение к OpenVPN -серверу на ВМ FW
      2.2.1) Подключение должно включаться и отключаться по запуску скрипта
         2.2.1.1. **start_vpn.sh** и **stop_vpn.sh**
         2.2.1.2. Скрипт запрашивает учетные данные в ходе работы
      2.2.2) Используйте сертификат CN=GUEST
      2.2.3) Подключение должно проходить по DNS-имени ВМ FW
      2.2.4) После подключения клиент должен перейти на использование сервера
      2.2.5) Все конфигурационные файлы расположить в /etc/openvpn/
   2.3) Установить веб-браузер IceWeasel\Firefox

Таблица 1 – Сетевая адресация

Сеть	Хосты	Адреса/Подсети
SRV	SRV-L	2002:db:a::10/64
	SRV-R	2002:db:a::20/64
	CORE	2002:db:a::1/64
STR	STR	2002:db8:b::10/64
	CORE	2002:db8:b::1/64
INT	CORE	2002:db8:c::10/64
	FW	2002:db8:c::1/64
EXT	FW	10.10.10.10/24
	ISP	10.10.10.1/24
ADM	CLI-ADM	20.20.20.10/24
	ISP	20.20.20.1/24
OUT	CLI-OUT	30.30.30.10/24
	ISP	30.30.30.1/24
VPN	FW CLI-ADM CLI-OUT	2002:acca:a::1/64 2002:acca:a::100/64 2002:acca:a::X/64

Таблица 2 – Учетные записи LDAP

Хост	Внутреннее отображение	Внешнее отображение
SRV-R	AAAA: srv-r.wsr.mv AAAA: backend-l.wsr.mv	
SRV-L	AAAA: srv-l.wsr.mv AAAA: backend-r.wsr.mv	
CORE	AAAA: core.wsr.mv AAAA: ns.wsr.mv	
FW	AAAA: fw.wsr.mv AAAA: frontend.wsr.mv	A: fw.wsr.mv A: site.wsr.mv CNAME: access.wsr.mv
STR	AAAA: str.wsr.mv CNAME: storage.wsr.mv	

Таблица 3 – Правила журналирования

Источник	Уровень журнала	Файл
SRV-R, SRV-L	WARN и выше	/var/mylogs/<HOSTNAME>/journal.log
STR	NOTICE и выше	/var/mylogs/<HOSTNAME>/journal.log
CORE	WARN и выше	/var/mylogs/<HOSTNAME>/journal.log
FW	WARN и выше	/var/mylogs/<HOSTNAME>/journal.log

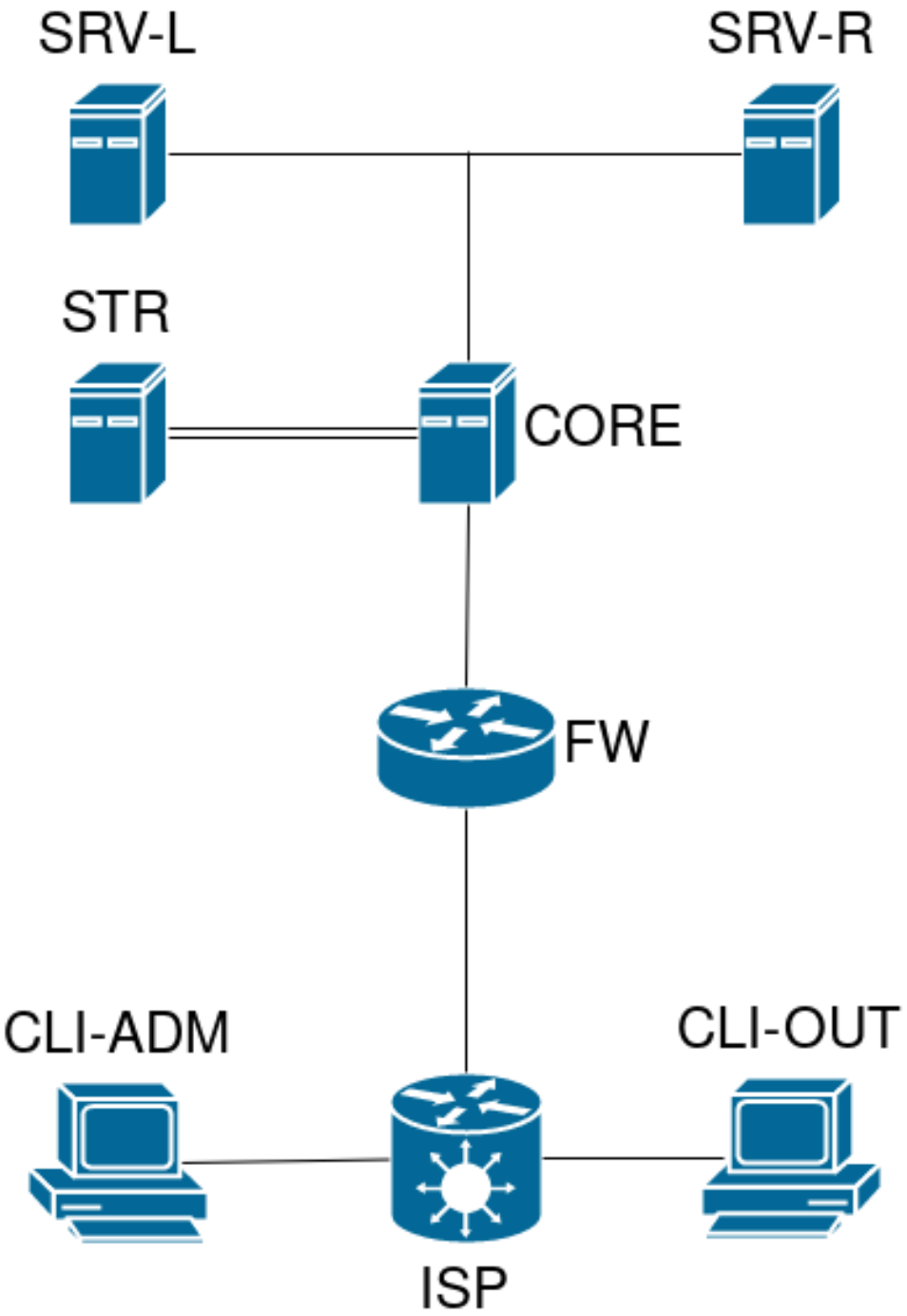
*<HOSTNAME> - название директории для журналируемого хоста

**В директории /var/mylogs/мне должно быть файлов, кроме тех, которые указаны в таблице

Таблица 4 – Пользователи LDAP

Группа	OU	CN	Пароль	Доступ
Administrators	Users	admin	toor	CORE, STR, SRV-L, SRV-R
Users	Users	user01-user10	P@ssw0rd	SRV-L, SRV-R
VPN	VPN	VPNAdmin, vpn01-vpn02	P@ssw0rd	OpenVPN на BM FW

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль B: «Пуско-наладка инфраструктуры на основе ОС семейства Windows»

Версия 2.2 от 13.03.2019

ВВЕДЕНИЕ

На выполнение задания отводится ограниченное время – подумайте, как использовать его максимально эффективно. Составьте план выполнения работ. Вполне возможно, что для полной работоспособности системы в итоге действия нужно выполнять не строго в той последовательности, в которой они описаны в данном конкурсном задании.

В рамках легенды конкурсного задания вы – системный администратор одного из университетов, в котором есть административное управление и кампус. Вы управляете доменом vuz.ru. Вам, в том числе, необходимо настроить сервисы в локальной сети административного управления университета. Также вам придется настроить необходимую инфраструктуру в кампусе.

Безусловно вам необходимо настроить канал связи между сетевыми сегментами с помощью интерфейсов вызовов по требованию.

Внимательно прочтите задание от начала до конца – оно представляет собой целостную систему. При первом доступе к операционным системам либо следуйте указаниям мастера, либо используйте следующие реквизиты: ***Administrator/P@ssw0rd***.

Если предоставленные виртуальные машины начнут самопроизвольно отключаться в процессе работы, попробуйте выполнить на них команду ***slmgr /rearm*** или обратитесь к техническому эксперту.

КОМПЛЕКТАЦИЯ КОНКУРСНОГО ЗАДАНИЯ

1) Текстовые файлы:
   1.1) данный файл с конкурсным заданием;
2) Предоставляемые конкурсантам компоненты проекта:
   2.1) файл для геренации пользователей в домене vuz.ru (.txt);
   2.2) стартовая страница сайта it.vuz.ru (.htm);
   2.3) стартовая страница сайта www.vuz.ru (.htm).
3) Программное обеспечение:
   3.1) Microsot Windows server 2016;
   3.2) Microsoft Windows 10 Enterprise;
   3.3) Windows 10 and Windows Server 2016 ADMX.

Внимание! Все указанные компоненты предоставляются участникам в виде ISO-файлов на локальном или удаленном хранилище.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

Настройка DC1

Базовая настройка

- переименуйте компьютер в DC1;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping).

Active Directory

- сделайте сервер основным контроллером домена vuz.ru.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – FS1, state switchover – 15 min, сообщения между серверами должны быть зашифрованы;
- область для административного сегмента vuz.ru: диапазон выдаваемых адресов: 10.0.19.155-200/24;
- область для кампуса vuz.ru: диапазон выдаваемых адресов: 10.0.20.155-200/24;
- настройте дополнительные свойства областей (адреса обоих DNS-серверов и основного шлюза).

DNS

- настройте необходимые зоны прямого и обратного просмотра, обеспечьте их согласованную работу со службой DNS на FS1;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов.

GPO

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;

- в браузерах Internet Explorer и Edge должна быть настроена стартовая страница – https://www.vuz.ru;
- для членов группы Teachers настройте перенаправление папок Documents и Desktop по адресу FS1→d:\shares\redirected;
- члены группы Teachers должны иметь повышенные требования к сложности пароля – не менее 12 символов.

Элементы доменной инфраструктуры

- создайте подразделения: IT, Teachers, Students, ITF;
- в соответствующих подразделениях создайте доменные группы: IT, Teachers, Students, ITF;
- также в подразделении Students создайте необходимые доменные группы учитывая информацию в файле Groups.txt.

Внимание! Указанные выше подразделения и группы должны быть созданы в домене обязательно. Если вы считаете, что для выполнения задания необходимы дополнительные элементы доменной инфраструктуры, вы можете создать их.

- создайте скрипт, при помощи которого сгенерируйте по 25 пользователей учебных групп (список групп в файле Groups.txt) в формате <group>-0N (например ad11-01) с паролем P@ssw0rd; поместите этих пользователей в подразделение Students, сделайте их членами указанных в файле групп. Также поместите всех созданных пользователей в группу Students; все созданные учетные записи должны быть включены и доступны;
- если создать пользователей из файла не удается, создайте вручную по одному пользователю в каждой группе с паролем P@ssw0rd;
- для каждого пользователя, члена группы Students, создайте домашнюю папку в папке по адресу FS1→d:\shares\users\Students, автоматически подключаемую в качестве диска Z:\;
- создайте пользователей adm и sup с паролем P@ssw0rd, поместите их в подразделение и группу IT;
- создайте пользователей adm1 и sup1 с паролем P@ssw0rd, поместите их в подразделение и группу ITF;
- создайте пользователей t1 и t2 с паролем P@ssw0rd, поместите их в подразделение и группу Teachers, для обоих пользователей создайте домашнюю папку по адресу FS1→d:\shares\users\Teachers, автоматически подключаемую в качестве диска Z:\.

Настройка FS1

Базовая настройка

- переименуйте компьютер в FS1;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru;
- из трех имеющихся жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

Active Directory

- сделайте сервер дополнительным контроллером домена vuz.ru;
- контроллер не должен выполнять функцию глобального каталога;
- передайте на него роль Infrastructure master.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – DC1, state switchover – 15 min, сообщения между серверами должны быть зашифрованы.

DNS

- сделайте сервер дополнительным DNS-сервером в домене vuz.ru;
- загрузите с DC1 все зоны прямого и обратного просмотра.

Общие папки

- создайте общие папки, настройте разрешения и обеспечьте их подключение пользователям согласно таблице 2;
- пользователи на любых сетевых дисках должны видеть только те папки, к которым им разрешен доступ.

Квоты/Файловые экраны

- установите максимальный размер в 50 Mb для каждой домашней папки пользователей группы Students;
- запретите хранение в всех домашних папках пользователей файлов с расширениями .mp4, .avi, .vob; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

DFS

- создайте корень под именем FILES, он должен поддерживаться FS1 и FS2;
- создайте под этим корнем папку с именем shares, ссылающуюся на директорию с тем же именем (shares), созданную Вами на диске D:\;

- настройте репликацию между папками средствами DFS (для этого на FS2 создайте папку c:\shares), исключите из репликации файлы с расширениями *.avi.

IIS

- создайте сайт университета www.vuz.ru (используйте предоставленный html-файл в качестве документа по умолчанию); сайт должен быть доступен только по протоколу https;
- создайте сайт для ИТ-службы университета it.vuz.ru (используйте предоставленный html-файл в качестве документа по умолчанию); сайт должен быть доступен только по протоколу https исключительно для членов группы IT по их пользовательским сертификатам.

Настройка RCA

Базовая настройка

- переименуйте компьютер в RCA;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru.

Службы сертификации

- установите службы сертификации;
- настройте доменный корневой сервер сертификации (длина ключа и алгоритмы шифрования значения не имеют);
- имя центра сертификации – VuzRootCA;
- срок действия сертификата – 15 лет.
- настройте шаблон выдаваемого сертификата для клиентских компьютеров *VuzClients*: *subject name=common name*, автозапрос для всех клиентских компьютеров домена;
- настройте шаблон выдаваемого сертификата для группы IT *ITUsers*: *subject name=common name*, автозапрос только для пользователей – членов группы IT.

Настройка CLI1

Базовая настройка

- переименуйте компьютер в CLI1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);

- присоедините компьютер к домену vuz.ru;
- запретите любое использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
- используйте компьютер для тестирования настроек в домене vuz.ru: пользователей, общих папок, групповых политик и т.д.

Настройка BR1

Базовая настройка

- переименуйте компьютер в BR1;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru.

Настройка RRAS

- установите службу RRAS;
- настройте защищенное vpn-соединение с кампусом с обязательным использованием сертификатов компьютеров; весь трафик между сегментами сети должен передаваться через это соединение, сертификаты должны быть выданы компьютерам автоматически по шаблону VuzClients.

Настройка DC2

Базовая настройка

- переименуйте компьютер в DC2;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru.

AD

- сделайте сервер дополнительным контроллером домена vuz.ru в режиме RODC;
- не устанавливайте и не используйте на этом компьютере службу DNS-сервера;
- разрешите локальную авторизацию пользователей группы ITF.

WDS

- разверните роль WDS, она должна отвечать на запросы любых клиентских компьютеров;
- для локального хранения образов используйте папку E:\RemoteInstall, для этого используйте дополнительный жесткий диск;
- подготовьте для развертывания Windows 10 Enterprise, образ которой вам доступен;
- членам группы IT предоставьте полный доступ к образу распространяемой ОС;
- установите на компьютер CLI2 операционную систему с помощью настроенной службы развертывания;
- компьютер CLI2 должен стать членом домена vuz.ru сразу при установке ОС с помощью службы развертывания.

Настройка RDS

Базовая настройка

- переименуйте компьютер в RDS;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru.

Службы удаленных рабочих столов

- разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования.
- сконфигурируйте web-доступ RemoteApp к службам терминалов сервера;
- опубликуйте программу *Notepad* на web-портале RemoteApp для членов группы IT;
- опубликуйте программу *Paint* на web-портале RemoteApp для членов группы Students;
- web-интерфейс сервера должен быть настроен таким образом, чтобы пользователи могли автоматически получать доступ к форме входа на web-интерфейс удаленных рабочих столов при указании адресов http://rds.vuz.ru и https://rds.vuz.ru;
- с помощью доменного центра сертификации на сервере RCA сгенерируйте и используйте для терминальных служб соответствующий SSL-сертификат. Сертификат должен быть использован для всех установленных компонентов терминальных служб. При обращении с любого компьютера в домене vuz.ru к сайту по имени https://rds.vuz.ru сертификат должен распознаваться как доверенный и действительный.

Настройка FS2

Базовая настройка

- переименуйте компьютер в FS2;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- средствами виртуализации добавьте жесткий диск объемом 2 Гб; присвойте ему букву D: в ОС;
- присоедините компьютер к домену vuz.ru.

Общие папки

- создайте общие папки, настройте разрешения и обеспечьте их подключение пользователям согласно таблице 2;
- пользователи на любых сетевых дисках должны видеть только те папки, к которым им разрешен доступ.

Квоты/Файловые экраны

- установите максимальный размер в 50 Mb для каждой домашней папки пользователя группы Students, полученной в результате работы DFS;
- запретите хранение в домашних папках пользователей, полученных в результате работы DFS, файлов с расширениями .mp4, .avi, .vob; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

DFS

- обеспечьте функционирование системы в соответствии с проведенными ранее настройками на FS1.

Настройка CLI2

Базовая настройка

- установите операционную систему с помощью службы развертывания;
- дайте имя компьютеру CLI2;
- IP-адрес должен назначаться сервером DHCP из административного сегмента сети;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru;
- запретите любое использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;

- используйте компьютер для тестирования настроек, в первую очередь, чтобы самостоятельно убедиться в работоспособности настроенной вами WDS.

Настройка CLI3

- Не выполняйте никаких действий. Данная виртуальная машина будет использоваться экспертами для проверки работоспособности настроенной вами WDS в сети.

Настройка BR2

Базовая настройка

- переименуйте компьютер в BR2;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
- присоедините компьютер к домену vuz.ru.

Настройка RRAS

- установите службу RRAS;
- настройте проброс запросов и ответов DHCP из административного сегмента сети в сеть кампуса;
- настройте защищенное vpn-соединение с административным сегментом, весь трафик между сегментами сети должен передаваться через это соединение.

Таблица 1 – Адресация сети

Имя компьютера	IP-адреса
DC1	10.0.19.1/24
FS1	10.0.19.2/24
RCA	10.0.19.3/24
BR1	10.0.19.254/24 200.100.50.100/24
CLI1	DHCP
DC2	10.0.20.1/24
FS2	10.0.20.2/24
RDS	10.0.20.3/24
BR2	10.0.20.254/24 200.100.50.101/24
CLI2, CLI3	DHCP

Таблица 2 – Файловые ресурсы

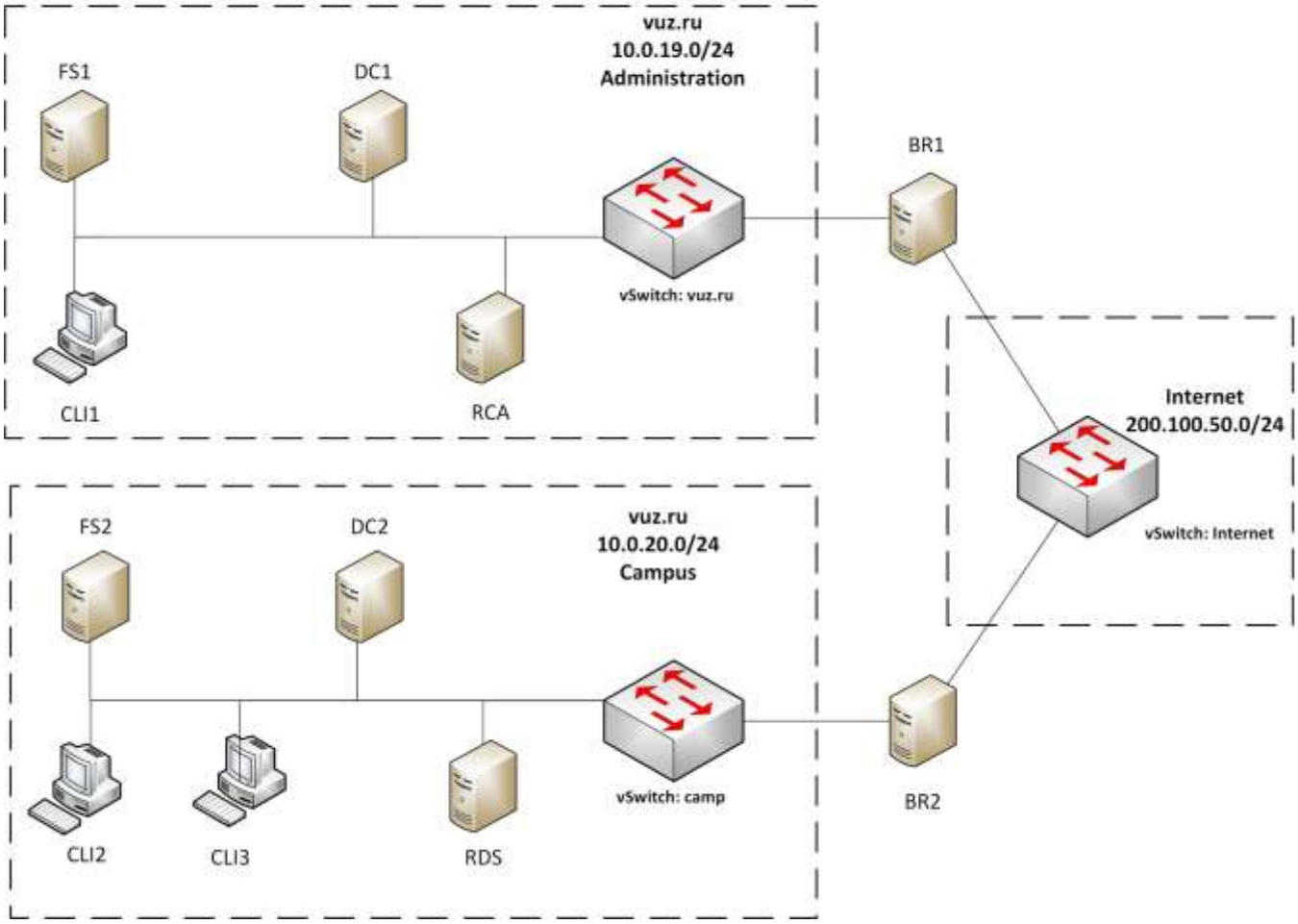
Имя общего ресурса	Расположение	Доступ только для чтения	Доступ для чтения и записи	Буква диска
Documents	FS1→D:\shares\documents FS2→D:\shares\documents	Students	Teachers IT	Y:
Teachers	FS1→D:\shares\users\teachers FS2→D:\shares\users\teachers	-	Teachers IT	Z:
Students	FS1→D:\shares\users\students FS2→D:\shares\users\students	Teachers	Students IT	Z:

Таблица 3. Характеристики виртуальных машин.

Имя компьютера	**Операционная система**	**Объем оперативной памяти, Гб**	**Количество и объем жестких дисков**
DC1	Windows Server 2016 Standard GUI	1,5	1 диск на 20 ГБ
FS1	Windows Server 2016 Standard Core	1	1 диск на 20 ГБ, 3 диска на 2 ГБ
RCA	Windows Server 2016 Standard GUI	1,5	1 диск на 20 ГБ
BR1	Windows Server 2016 Standard Core	1	1 диск на 20 ГБ
CLI1, CLI2, CLI3	Windows 10 Enterprise	1	1 диск на 20 ГБ
DC2	Windows Server 2016 Standard GUI	1,5	2 диска на 20 ГБ
FS2	Windows Server 2016 Standard Core	1	1 диск на 20 ГБ
RDS	Windows Server 2016 Standard GUI	1,5	1 диск на 20 ГБ
BR2	Windows Server 2016 Standard GUI	1,5	1 диск на 20 ГБ

На всех виртуальных машинах, кроме CLI2 и CLI3, операционные системы должны быть предустановлены без установки каких бы то ни было ролей.
После установки операционных систем на всех виртуальных машинах должна быть выполнена системная программа *Sysprep* с опциями *Generalize* и *Shutdown*.

Диаграмма виртуальной сети



Версия: 1.0 от 28.02.19.

ВВЕДЕНИЕ

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с учетом различных сетевых технологий, соответствующих уровням сертификации CCNA, CCNA Security. Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- Конфигурация виртуальных частных сетей

Все секции являются независимыми друг от друга но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх Frame-Relay и PPPoE и т.д. Очень важно понимать, что если вам не удается решить какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 3 в секции «Настройка служб» предписывает вам настроить службу протокола автоматической конфигурации хостов, которая, разумеется, не будет работать пока не будут выполнены необходимые настройки в секции «Конфигурация коммутации». На вас возлагается ответственность за распределение своего рабочего времени.

Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

В начале работы убедитесь в том, что оборудование сохранит ваши настройки.

ПО окончании работы убедитесь в том, что ваши настройки на всех устройствах функционируют после перезагрузки всего оборудования.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Ожидается, что конкурсное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

СХЕМА ОЦЕНКИ

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимающими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

ПОДКЛЮЧЕНИЕ К УСТРОЙСТВАМ

Для настройки всех устройств кроме маршрутизатора BR1 используется удаленное подключение по протоколу Telnet.

ПРЕДНАСТРОЙКА

На маршрутизаторе ISP преднастроены протоколы PPP, PPPoE и SSH. Поэтому при настройке оборудования будьте внимательны, чтобы не сбить настройки.

ИСПОЛЬЗОВАНИЕ LINUX

На узле RTR2 установлена операционная система Linux Centos7. На нем предустановлено следующее программное обеспечение: freeradius, keepalived. Его необходимо будет настроить. Настроено: bind, ntp. Настройки сервисов будут выполняться участниками во время острова Networking, а учтены при оценивании острова Linux.

Базовая настройка

1. Задайте имена ВСЕХ устройств в соответствии с топологией

2. Назначьте для BCEX устройств доменное имя **wsrvuz19.ru**
3. Создайте на BCEX устройствах пользователя **wsrvuz19** с паролем **cisco**

a. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
b. Пользователь должен обладать максимальным уровнем привилегий.

4. Для BCEX устройств реализуйте модель AAA.

a. Аутентификация на удаленной консоли должна производиться с использованием локальной базы данных (кроме устройства RTR1 и RTR2)
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 BCEX 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 маршрутизаторе RTR1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.

a. Порядок аутентификации:
   i. По протоколу RADIUS
   ii. Локальная
b. Используйте общий ключ **cisco**
c. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
d. Адрес RADIUS-сервера **2001:300::3**
e. Настройте авторизацию при успешной аутентификации
f. Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору RTR1, используя учетную запись **radius** с паролем **cisco**

7. На BCEX устройствах создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля. Назначьте IP-адреса в соответствии с топологией

a. Включите механизм SLAAC для выдачи IPv6-адресов в сети MNG на интерфейсе маршрутизатора RTR1
b. На виртуальных интерфейсах в ВЛВС 100 (MNG) на коммутаторах SW1, SW2, SW3 включите режим автоконфигурации IPv6
c. На BCEX устройствах (кроме PC1 и WEB) вручную назначьте link-local адреса.
d. На BCEX коммутаторах отключите BCE неиспользуемые в задании порты и переведите в VLAN 99.
e. На коммутаторе SW1 включите блокировку на 1 минуту в случае двукратного неправильного ввода пароля в течение 30 секунд

8. Все устройства должны быть доступны для управления по протоколу SSH версии 2.

Настройка коммутации

1. На ВСЕХ коммутаторах создайте ВЛВС:
    a. под номером 99 с именем UNUSED
    b. под номером 100 с именем MNG
    c. под номером 300 с именем OFFICE
2. На коммутаторах SW1, SW2 и SW3 выполните настройку протокола динамического согласования транков (DTP).
    a. На коммутаторе SW3 переведите порты в Fa0/3-6 в режим, при котором коммутатор на данных портах будет инициировать согласование параметров транка.
    b. Переведите порты Fa0/3-4 на SW1 и Fa0/5-6 на SW2 в режим, при котором каждый коммутатор ожидает начала согласования параметров от соседа, но сам не инициирует согласование.
    c. Переведите порты Fa0/1-2 на SW1 и SW2 в режим передачи трафика по протоколу IEEE 802.1q. Явно отключите динамическое согласование транков.
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 пассивного согласования по обеим портовым группам по протоколу PAgP;
    c. Коммутаторы SW1 и SW2 должны быть настроены в активном режиме PAgP с коммутатором SW3.
    d. Коммутатор SW2 должен быть настроен в режиме активного согласования по протоколу LACP с коммутатором SW1.
    e. Коммутатор SW1 должен быть настроен в режиме пассивного согласования по протоколу LACP с коммутатором SW2.
4. Конфигурация протокола остовного дерева:
    a. Используйте протокол Rapid STP.
    b. Коммутатор SW1 должен являться корнем связующего дерева в VLAN 100,300. В случае его отказа, корнем должен стать коммутатор SW2.
5. На портах Fa0/10, Fa0/9 коммутатора SW1 включите защиту от нежелательных BPDU. При получении BPDU на этом порту, порт должен переводиться в состояние err-disabled.
6. Обеспечить автоматическое восстановление работоспособности указанных портов с интервалом 60 секунд
7. Настройте порты Fa0/9, Fa0/10 коммутатора SW1 таким образом, чтобы порт переходил в состояние Forwarding, не дожидаясь пересчета остовного дерева.

Настройка подключений к глобальным сетям

1 Настройте подключение PPPoE между ISP и маршрутизатором BR1.

1.1 Настройте PPPoE клиент на BR1.

1.2 Используйте имя пользователя **cisco** и пароль **cisco**

1.3 Устройства проходят одностороннюю аутентификацию по протоколу CHAP, только ISP проверяет имя пользователя и пароль.

1.4 BR1 должен автоматически получать адрес от ISP.

2 Настройте подключение RTR1 к провайдеру ISP с помощью протокола PPP.

2.1 Настройте Multilink PPP с использованием двух Serial-интерфейсов.

2.2 Используйте 1 номер интерфейса.

2.3 Не используйте аутентификацию.

2.4 RTR1 должен автоматически получать адрес от ISP.

Настройка маршрутизации

1. На маршрутизаторах RTR1 и BR1 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.

a. Включите маршрутизацию для сетей BR1, OFFICE, MNG, Tunnel100, Tunnel101 а также на интерфейсе Loopback100 маршрутизатора RTR1 и на интерфейсе Loopback101 маршрутизатора BR1.

b. Используйте области согласно диаграмме маршрутизации

c. Настройте суммаризацию для сетей на интерфейсах Loopback101 и сети WEB маршрутизатора BR1 таким образом, чтобы BR1 анонсировал вместо этих двух сетей только одну суммарную сеть минимально возможного размера. Используйте для этих интерфейсов область 1.

d. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

2. На маршрутизаторах RTR1 и BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2019.

a. Включите в обновления маршрутизации сети Tunnel100, Loopback100 и Loopback101,

b. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

c. Используйте аутентификацию md5 с ключом **wsrvuz**

3. На маршрутизаторе RTR2 настройте статический маршрут для обеспечения доступности сети 10.10.10.0/30.

4. На маршрутизаторе BR1 настройте статический маршрут для обеспечения доступности сети 2001:300::/64 в случае неработоспособности OSPFv3

Настройка служб

1. В сетевой инфраструктуре сервером синхронизации времени является RTR2. Все остальные сетевые устройства должны использовать в качестве сервера времени RTR1.
    1. Передача данных между RTR1 и RTR2 осуществляется без аутентификации.
    2. Настройте временную зону с названием EKB, укажите разницу с **UTC +5** часов.
    3. Настройте сервер синхронизации времени. Используйте стратум **2**.

4. Используйте для синхронизации клиентов с RTR1 аутентификацию MD5 с ключом **WSR**.

2. Настройте на RTR1 DHCPv6 сервер с отслеживанием состояния для сети OFFICE со следующими характеристиками:

a. Имя домена **wsrvuz19.ru**

DNS – сервер – адрес RTR2.

3. Обеспечить копирование с коммутатора SW1 на BR1 файла SW1_backup, являющийся копией стартовой конфигурации SW1

4. На маршрутизаторе RTR2 настройте RADIUS – сервер (программное обеспечение предустановлено):

a. Используйте общий ключ **cisco**
b. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
c. Адрес сети **2001:300::/64**
d. Учетная запись **radius** с паролем **cisco**

Примечание: Настройка RADIUS – сервера на RTR2 оценивается в составе острова Linux

Настройка механизмов отказоустойчивости

1. На шлюзе RTR1 и узле RTR2 настроить протокол VRRP в сети OFFICE:

a. Номер группы 1
b. IPv6 адрес виртуального шлюза 2001:300::1/64
c. Включить вытеснение
d. Master – RTR1

Backup – RTR2

Примечание: Настройка VRRP на RTR2 оценивается в составе острова Linux

Настройка механизмов безопасности

1. На порту F0/9 коммутатора SW1, включите и настройте Port Security со следующими параметрами:

a. не более 3 адресов на интерфейсе;
b. адреса должны динамически пополняться и сохраняться в текущей конфигурации
c. при попытке подключения устройства с адресом, нарушающим политику, порт не должен быть отключен, уведомления не передаются;

2. На маршрутизаторе RTR1 настройте список контроля доступа со следующими свойствами:

a. ACL не должен позволять пользователям сети MNG обращаться к сайтам на устройстве WEB;
b. ACL не должен нарушать работу настроенных сервисов и протоколов

c. ACL должен позволять отправлять эхо-запросы из внутренней сети и получать на них ответы;
d. ACL должен позволять удаленный доступ к PC1 с узла WEB только по ssh;

Конфигурация виртуальных частных сетей

1. На маршрутизаторах RTR1 и BR1 настройте GRE-туннель:

a. Используйте в качестве VTI интерфейс Tunnel100
b. Используйте адресацию согласно диаграмме.

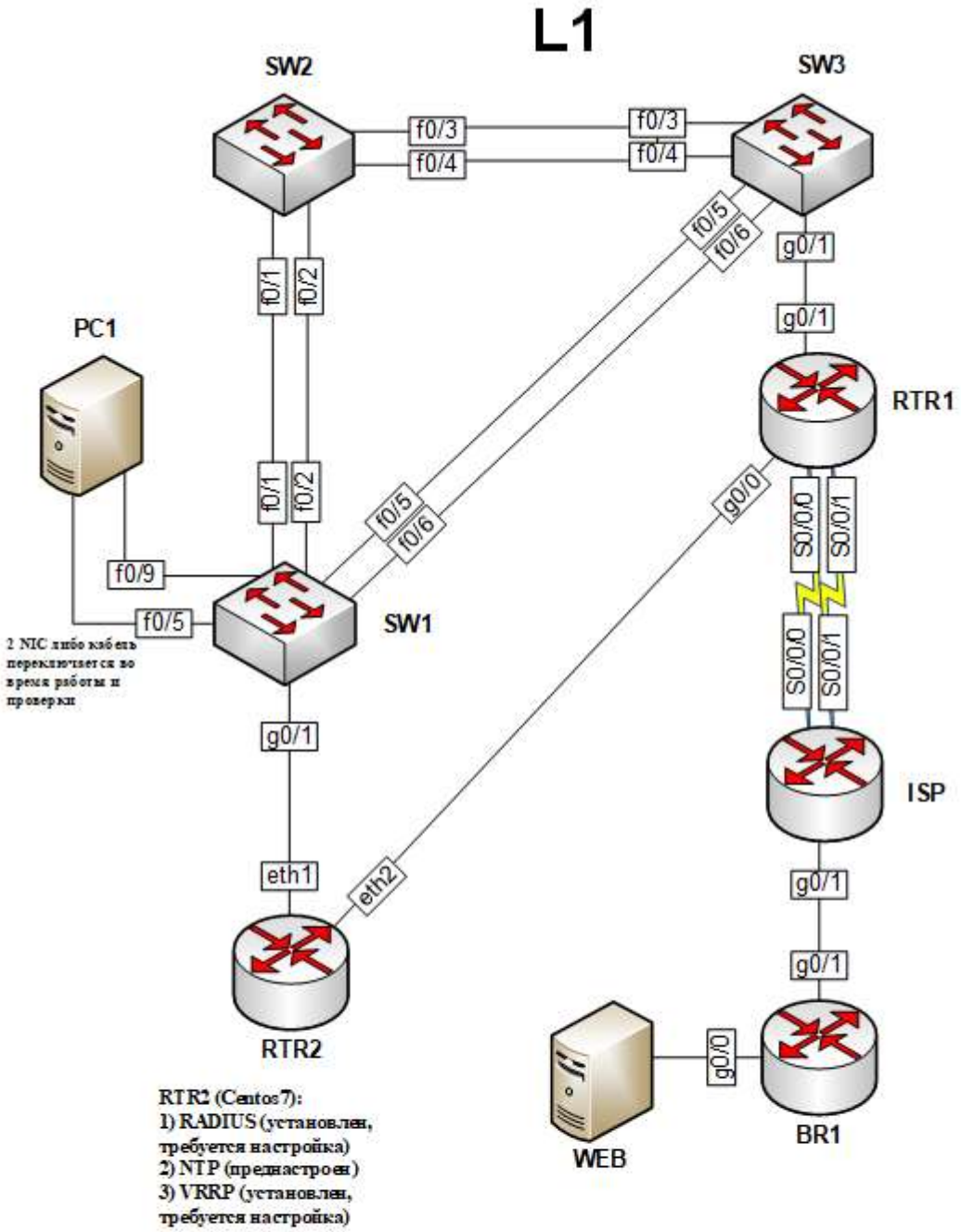
2. На маршрутизаторах RTR1 и BR1 настройте IKEv1 IPsec Site-to-Site VPN и примените его к созданному GRE-туннелю

a. Параметры политики первой фазы:
   i. Проверка целостности – MD5
   ii. Шифрование – DES
   iii. Группа Диффи-Хэлмана – 14
   iv. Ключ - cisco
b. Параметры преобразования трафика для второй фазы:
   i. Протокол – ESP
   ii. Шифрование – DES
   iii. Проверка целостности – MD5

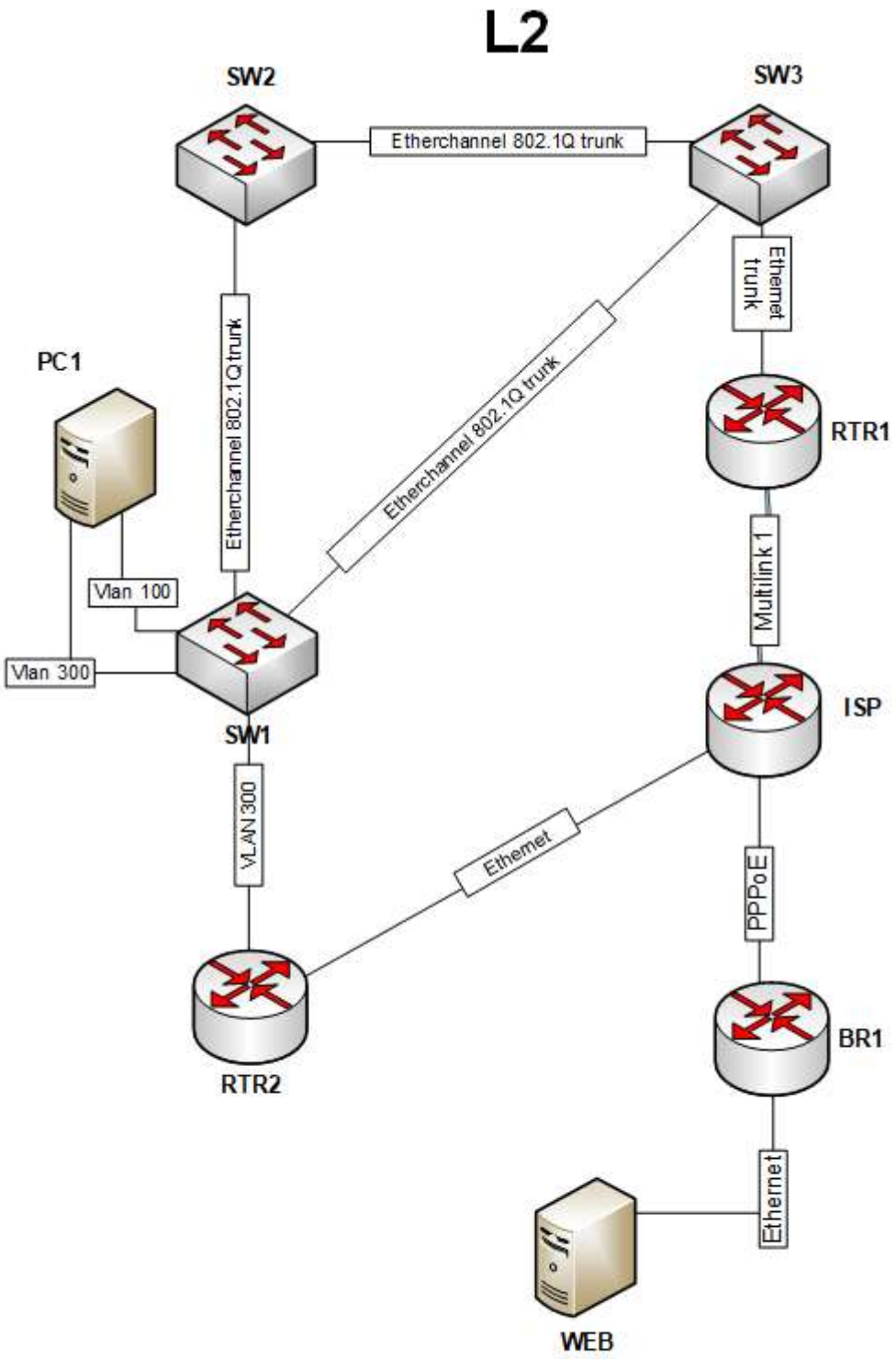
3. На маршрутизаторах RTR2 и BR1 настройте GRE-туннель:

c. Используйте интерфейс Tunnel101
d. Используйте адресацию согласно диаграмме.

Топология L1

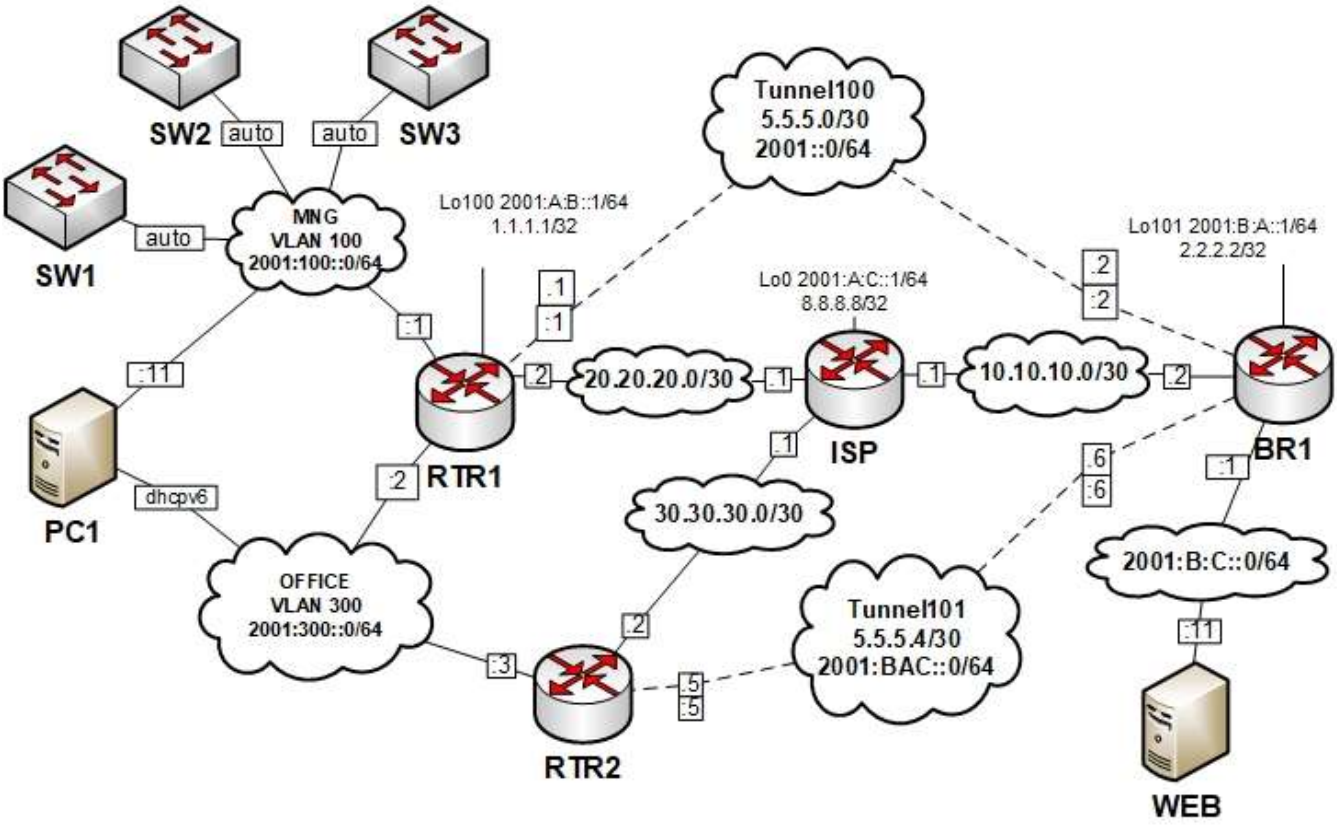


Топология L2

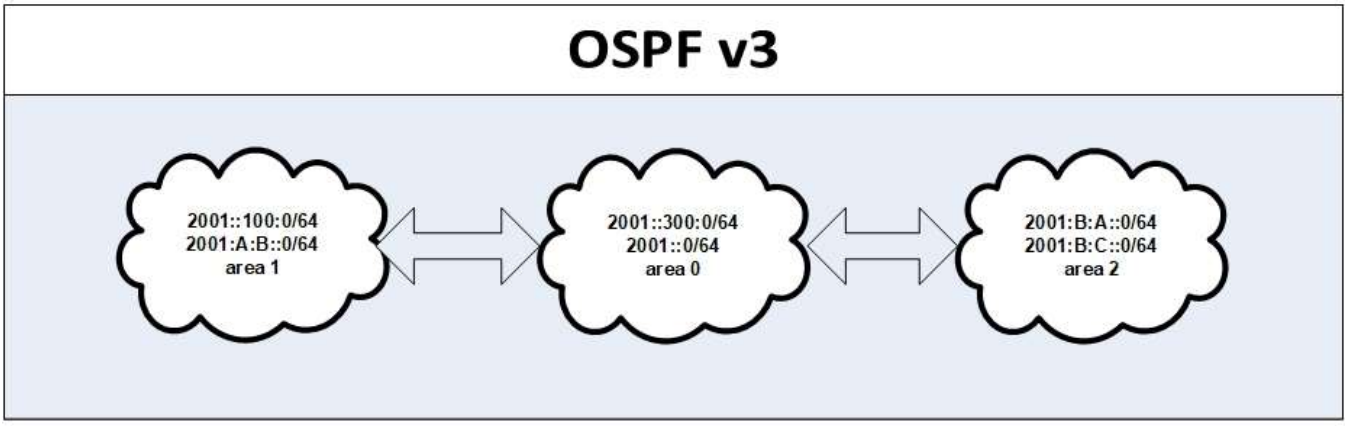


Топология L3

L3


SW2
auto
auto
SW3
Tunnel100
5.5.5.0/30
2001::0/64
SW1
auto
MNG
VLAN 100
2001:100::0/64
Lo100 2001:A:B::1/64
1.1.1.1/32
Lo101 2001:B:A::1/64
2.2.2.2/32
Lo0 2001:A:C::1/64
8.8.8.8/32
:11
:1
:1
:1
:2
:2
20.20.20.0/30
:1
:1
10.10.10.0/30
:2
PC1
dhcpv6
:2
RTR1
ISP
BR1
:1
:6
:6
30.30.30.0/30
2001:B:C::0/64
OFFICE
VLAN 300
2001:300::0/64
Tunnel101
5.5.5.4/30
2001:BAC::0/64
:3
:2
:5
:5
:11
RTR2
WEB

Routing-диаграмма



4. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 45.

Таблица 2 – Критерии оценки

Раздел	Критерий	Оценки		
		Субъективная (если это применимо)	Объективная	Общая
A	Модуль A: «Пуско-наладка инфраструктуры на основе ОС семейства Linux»	0	15	15
B	Модуль B: «Пуско-наладка инфраструктуры на основе ОС семейства Windows»	0	15	15
C	Модуль C: «Пуско-наладка телекоммуникационного оборудования»	0	15	15
Итого =		0	45	45

Субъективные оценки - Не применимо.

5. ПРИЛОЖЕНИЯ К ЗАДАНИЮ

1) Шаблон виртуальных машин Linux
   https://nextcloud.wsr39.ru/index.php/s/ZJEZ5yyBeKdKrdz
2) Шаблон виртуальных машин Windows
   https://nextcloud.wsr39.ru/index.php/s/7MeggDCktWM8yD3
3) Шаблон виртуальных машин RTR2
   https://nextcloud.wsr39.ru/index.php/s/as84qAxq2D9q5jp
4) Преднастрой ISP

```
hostname ISP
!
aaa new-model
!
aaa authentication login default local
aaa authentication ppp default local
!
no ip domain lookup
ip domain name wsrvuz19.ru

ipv6 unicast-routing

username cisco password 0 cisco
!
bba-group pppoe global
 virtual-template 1
!
!
interface Loopback0
 ip address 8.8.8.8 255.255.255.255
 ipv6 address 2001:A:C::1/64
!
interface Multilink1
 ip address 20.20.20.1 255.255.255.252
 peer default ip address pool PPP
 ppp multilink
 ppp multilink group 1
!

!
interface GigabitEthernet0/0
 description to RTR2
 ip address 30.30.30.1 255.255.255.252
 duplex auto
```

```
 SPEED AUTO
!
INTERFACE GIGABITETHERNET0/1
 DESCRIPTION TO BR1
 IP ADDRESS 10.10.10.1 255.255.255.252
 DUPLEX AUTO
 SPEED AUTO
 PPPOE ENABLE GROUP GLOBAL
!
INTERFACE SERIAL0/0/0
 NO IP ADDRESS
 ENCAPSULATION PPP
 PPP MULTILINK
 PPP MULTILINK GROUP 1
INTERFACE SERIAL0/0/1
 NO IP ADDRESS
 ENCAPSULATION PPP
 PPP MULTILINK
 PPP MULTILINK GROUP 1
!
INTERFACE VIRTUAL-TEMPLATE1
 DESCRIPTION PPPOE FOR BR1
 IP UNNUMBERED GIGABITETHERNET0/1
 IP MTU 1492
 PEER DEFAULT IP ADDRESS POOL PPPOE
 PPP AUTHENTICATION CHAP
!
!
IP LOCAL POOL PPPOE 10.10.10.2
IP LOCAL POOL PPP 20.20.20.2

!
IP ROUTE 0.0.0.0 0.0.0.0 NULL0


LINE CON 0
 PASSWORD CISCO

LINE VTY 0 4
 TRANSPORT INPUT TELNET SSH
```