ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Иркутский государственный университет путей сообщения»

Сибирский колледж транспорта и строительства

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРАКТИЧЕСКИМ РАБОТАМ

МДК.01.02. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

для специальности
09.02.06 Сетевое и системное администрирование

базовая подготовка среднего профессионального образования

Иркутск 2022

РАССМОТРЕНО:
ЦМК специальности 09.02.06
«Сетевое и системное
администрирование»
Протокол №9 от «23 » мая 2023 г.
Председатель ЦМК: Саквенко Т.В.

Разработчик:
Помазкина Л.И. преподаватель Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения»,
Саквенко Т.В., преподаватель первой категории Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения»

Практическая работа № 1.

Развертывание коммутируемой сети с резервными каналами

Топология

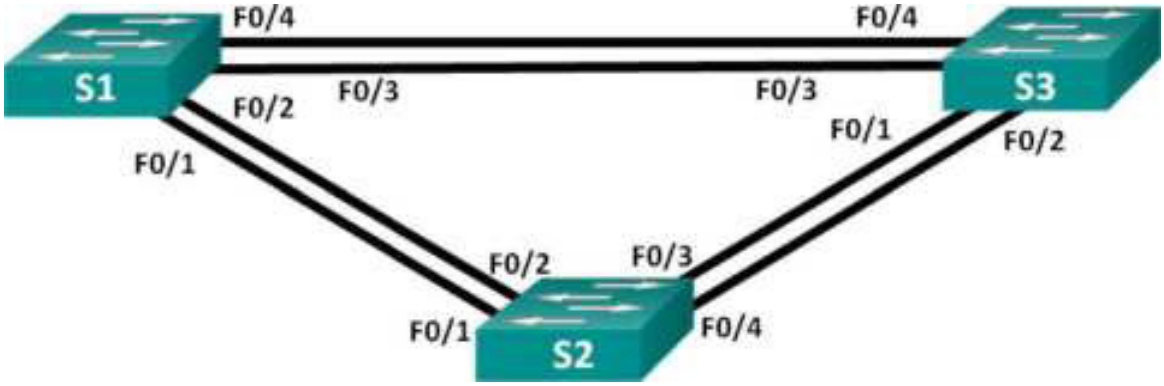


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
S3	VLAN 1	192.168.1.3	255.255.255.0

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Выбор корневого моста

Часть 3. Наблюдение за процессом выбора протоколом STP порта, исходя из стоимости портов

Часть 4. Наблюдение за процессом выбора протоколом STP порта, исходя из приоритета портов

Исходные данные/сценарий

Избыточность позволяет увеличить доступность устройств в топологии сети за счёт устранения единой точки отказа. Избыточность в коммутируемой сети обеспечивается посредством использования нескольких коммутаторов или нескольких каналов между коммутаторами. Когда в

проекте сети используется физическая избыточность, возможно возникновение петель и дублирование кадров.

Протокол spanning-tree (STP) был разработан как механизм предотвращения возникновения петель на 2 уровне для избыточных каналов коммутируемой сети. Протокол STP обеспечивает наличие только одного логического пути между всеми узлами назначения в сети путем намеренного блокирования резервных путей, которые могли бы вызвать петлю.

В этой лабораторной работе команда **show spanning-tree** используется для наблюдения за процессом выбора протоколом STP корневого моста. Также вы будете наблюдать за процессом выбора портов с учетом стоимости и приоритета.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.

Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 вам предстоит настроить топологию сети и основные параметры маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с диаграммой топологии и выполните разводку кабелей по необходимости.

Шаг 2: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 3: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

d. Назначьте **cisco** в качестве паролей консоли и VTY и активируйте вход для консоли и VTY каналов.

e. Настройте logging synchronous для консольного канала.

f. Настройте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

g. Задайте IP-адрес, указанный в таблице адресации для VLAN 1 на обоих коммутаторах.

h. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Проверьте соединение.

Проверьте способность компьютеров обмениваться эхо-запросами. Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S3? Успешно ли выполняется эхо-запрос от коммутатора S2 на коммутатор S3? Выполняйте отладку до тех пор, пока ответы на все вопросы не будут положительными.

Часть 2: Определение корневого моста

Для каждого экземпляра протокола spanning-tree (коммутируемая сеть LAN или широковещательный домен) существует коммутатор, выделенный в качестве корневого моста. Корневой мост служит точкой привязки для всех

расчётов протокола spanning-tree, позволяя определить избыточные пути, которые следует заблокировать.

Процесс выбора определяет, какой из коммутаторов станет корневым мостом. Коммутатор с наименьшим значением идентификатора моста (BID) становится корневым мостом. Идентификатор BID состоит из значения приоритета моста, расширенного идентификатора системы и MAC-адреса коммутатора. Значение приоритета может находиться в диапазоне от 0 до 65535 с шагом 4096. По умолчанию используется значение 32768.

Шаг 1: Отключите все порты на коммутаторах.

Шаг 2: Настройте подключенные порты в качестве транковых.

Шаг 3: Включите порты F0/2 и F0/4 на всех коммутаторах.

Шаг 4: Отобразите данные протокола spanning-tree.

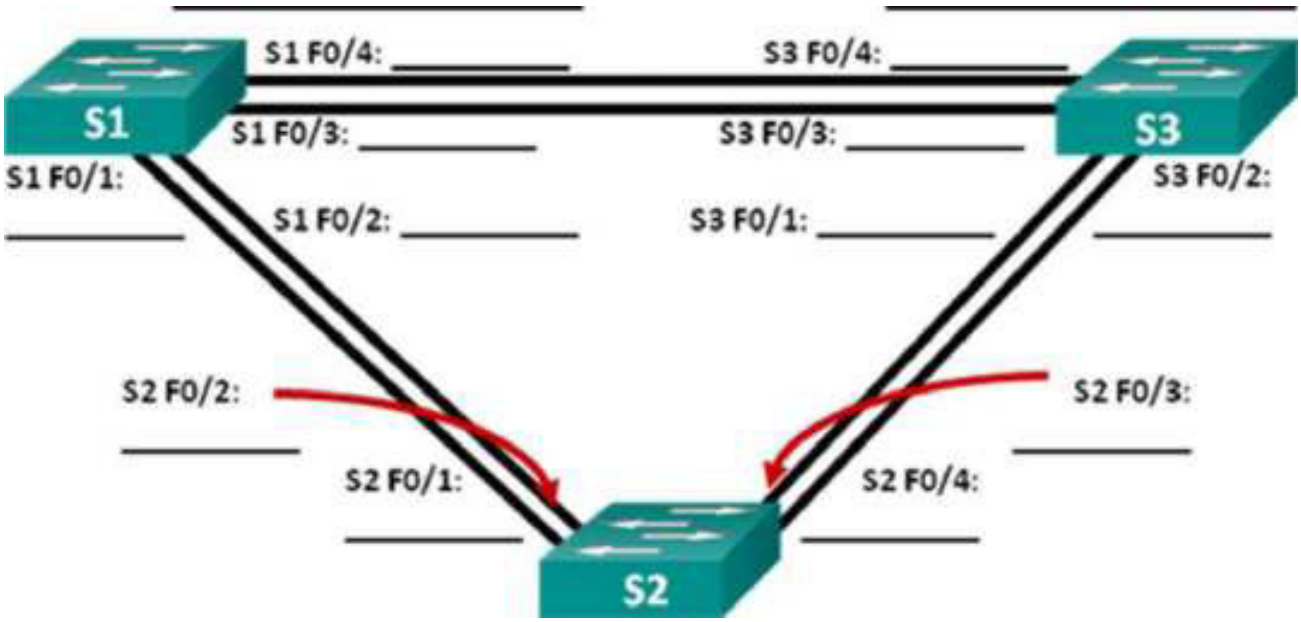
Введите команду **show spanning-tree** на всех трех коммутаторах. Приоритет идентификатора моста рассчитывается путем сложения значений приоритета и расширенного идентификатора системы. Расширенным идентификатором системы всегда является номер сети VLAN. В примере ниже все три коммутатора имеют равные значения приоритета идентификатора моста (32769 = 32768 + 1, где приоритет по умолчанию = 32768, номер сети VLAN = 1); следовательно, коммутатор с самым низким значением MAC-адреса становится корневым мостом (в примере — S2).

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Altn BLK 19        128.4    P2p

S2# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
```

```
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96d2.4000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Desg FWD 19        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.7400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p
```

Примечание. Режим STP по умолчанию на коммутаторе 2960 — протокол STP для каждой сети VLAN (PVST).

В схему ниже запишите роль и состояние (Sts) активных портов на каждом коммутаторе в топологии.



SI MAC: S3 MAC

S2 MAC: _____

С учетом выходных данных, поступающих с коммутаторов, ответьте на следующие вопросы. Какой коммутатор является корневым мостом?

Почему этот коммутатор был выбран протоколом spanning-tree в качестве корневого моста? Какие порты на коммутаторе являются корневыми портами? Какие порты на коммутаторе являются назначенными портами?

Какой порт отображается в качестве альтернативного и в настоящее время заблокирован?

Почему протокол spanning-tree выбрал этот порт в качестве невыделенного (заблокированного) порта?

Часть 3: Наблюдение за процессом выбора протоколом STP порта, исходя из стоимости портов

Алгоритм протокола spanning-tree (STA) использует корневой мост как точку привязки, после чего определяет, какие порты будут заблокированы, исходя из стоимости пути. Порт с более низкой стоимостью пути является предпочтительным. Если стоимости портов равны, процесс сравнивает BID. Если BID равны, для определения корневого моста используются приоритеты портов. Наиболее низкие значения являются предпочтительными. В части 3 вам предстоит изменить стоимость порта, чтобы определить, какой порт будет заблокирован протоколом spanning-tree.

Шаг 1: Определите коммутатор с заблокированным портом.

При текущей конфигурации только один коммутатор может содержать заблокированный протоколом STP порт. Выполните команду **show spanning-tree** на обоих коммутаторах некорневого моста. В примере ниже протокол spanning-tree блокирует порт F0/4 на коммутаторе с самым высоким идентификатором BID (S1).

```
S1# show spanning-tree

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Altn BLK 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.7400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec
```

Примечание. В конкретной топологии корневой мост может отличаться от выбора порта.

Шаг 2: Измените стоимость порта.

Помимо заблокированного порта, единственным активным портом на этом коммутаторе является порт, выделенный в качестве порта корневого моста. Уменьшите стоимость этого порта корневого моста до 18, выполнив команду **spanning-tree cost 18** режима конфигурации интерфейса.

```
S1(config)# interface f0/2
S1(config-if)# spanning-tree cost 18
```

Шаг 3: Просмотрите изменения протокола spanning-tree.

Повторно выполните команду **show spanning-tree** на обоих коммутаторах некорневого моста. Обратите внимание, что ранее заблокированный порт (S1 - F0/4) теперь является назначенным портом, и протокол spanning-tree теперь блокирует порт на другом коммутаторе некорневого моста (S3 - F0/4).

S1# show spanning-tree

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        18
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 18        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
           Address     0cd9.96e8.7400
           Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
```

Почему протокол spanning-tree заменяет ранее заблокированный порт на назначенный порт и блокирует порт, который был назначенным портом на другом коммутаторе?

Шаг 4: Удалите изменения стоимости порта.

a. Выполните команду **no spanning-tree cost 18** режима конфигурации интерфейса, чтобы удалить запись стоимости, созданную ранее.

```
S1(config)# interface f0/2
S1(config-if)# no spanning-tree cost 18
```

b. Повторно выполните команду **show spanning-tree,** чтобы подтвердить, что протокол STP сбросил порт на коммутаторе некорневого моста, вернув исходные настройки порта. Протоколу STP требуется примерно 30 секунд, чтобы завершить процесс перевода порта.

Часть 4: Наблюдение за процессом выбора протоколом STP порта, исходя из приоритета портов

Если стоимости портов равны, процесс сравнивает BID. Если BID равны, для определения корневого моста используются приоритеты портов. Значение приоритета по умолчанию — 128. STP объединяет приоритет порта с номером порта, чтобы разорвать связи. Наиболее низкие значения являются предпочтительными. В части 4 вам предстоит активировать избыточные пути до каждого из коммутаторов, чтобы просмотреть, каким образом протокол STP выбирает порт с учетом приоритета портов.

a. Включите порты F0/1 и F0/3 на всех коммутаторах.

b. Подождите 30 секунд, чтобы протокол STP завершил процесс перевода порта, после чего выполните команду **show spanning-tree** на

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

коммутаторах некорневого моста. Обратите внимание, что порт корневого моста переместился на порт с меньшим номером, связанный с коммутатором корневого моста, и заблокировал предыдущий порт корневого моста.

```
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
```

Fa0/1	Root	FWD 19 12		P2p
Fa0/2	Altn	BLK 19 12	8.2	P2p
Fa0/3	Altn	BLK 19 12	8.3	P2p
Fa0/4	Altn	BLK 19 12	8.4	P2p
protocol ieee **S3#** show spanning-tree				
VLAN0001				
Spanning	tree enabled			
Root ID	Priority	32769		
	Address	0cd9.96d2.4000		
	Cost	19		
	Port	1 (FastEthernet0/1)		
	Hello Time	2 sec Max Age	20 sec	Forward Delay 15 sec
Bridge ID	Priority	32769 (priority	32768	sys-id-ext 1)
	Address	0cd9.96e8.7400		
	Hello Time	2 sec Max Age	20 sec	Forward Delay 15 sec
	Aging Time	15 sec		
Interface	Role	Sts Cost Prio.Nbr		Type
Fa0/1	Root	FWD 19 12	8.1	P2p
Fa0/2	Altn	BLK 19 12	8.2	P2p
Fa0/3	Desg	FWD 19 12	8.3	P2p
Fa0/4	Desg	FWD 19 12	8.4	P2p

Какой порт выбран протоколом STP в качестве порта корневого моста на каждом коммутаторе некорневого моста?

Почему протокол STP выбрал эти порты в качестве портов корневого моста на этих коммутаторах?

Вопросы на закрепление

1. Какое значение протокол STP использует первым после выбора корневого моста, чтобы определить выбор порта?

2. Если первое значение на двух портах одинаково, какое следующее значение будет использовать протокол STP при выборе порта?

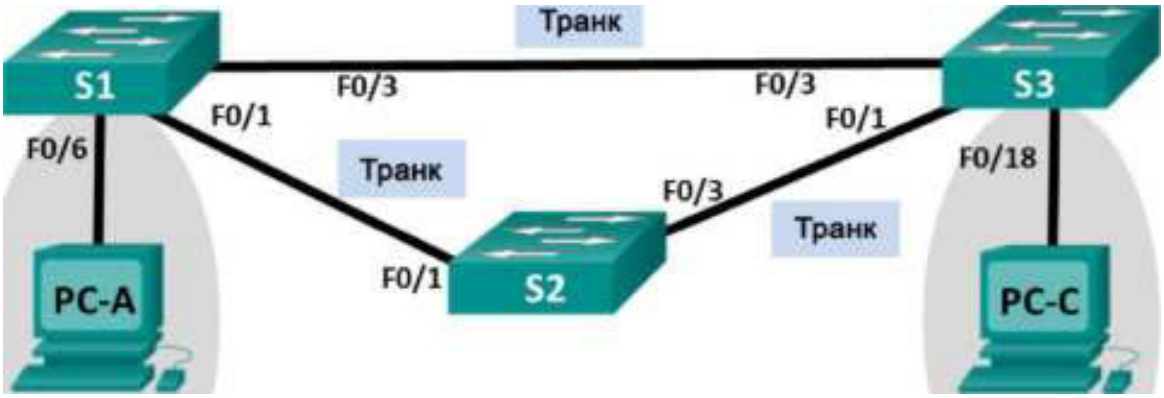
3. Если оба значения на двух портах равны, каким будет следующее значение, которое использует протокол STP при выборе порта?

Практоическая работа 2

Настройка Rapid PVST+, PortFast и BPDU Guard

Лабораторная работа . Настройка Rapid PVST+, PortFast и BPDU Guard

Топология



VLAN 10 VLAN 10

Пользователь Пользователь

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	Пользователь
99	Management (Руководство)

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка сетей VLAN, native VLAN и транковых каналов

Часть 3. Настройка корневого моста и проверка сходимости PVST+

Часть 4. Настройка Rapid PVST+, PortFast, BPDU guard и проверка сходимости

Исходные данные/сценарий

Протокол spanning-tree для VLAN (PVST) является проприетарным протоколом Cisco. По умолчанию коммутаторы Cisco используют протокол PVST. Rapid PVST+ (IEEE 802.1w) является усовершенствованной версией PVST+ и обеспечивает более быстрые вычисления протокола spanning-tree и более быструю сходимость после изменений топологии 2 уровня. Rapid PVST+ определяет три состояния порта: отбрасывание, обучение и пересылка, а также представляет ряд нововведений в целях оптимизации производительности сети.

В этой лабораторной работе вам предстоит настроить основной и вспомогательный корневые мосты, изучить сходимость PVST+, настроить Rapid PVST+ и сравнить его сходимость с PVST+. Кроме того, необходимо будет настроить пограничные порты для немедленного перехода в состояние пересылки с помощью PortFast, а также блокировать пересылку BDPU из пограничных портов, используя BDPU guard.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки. Список требуемых команд приведен в приложении А. Проверьте свои знания: настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.

Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В первой части вам предстоит настроить топологию сети и настроить базовые параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 4: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Установите **cisco** в качестве пароля консоли и виртуального терминала VTY и включите вход по паролю.

d. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

e. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

f. Отключите все порты коммутатора.

g. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Часть 2: Настройка сетей VLAN, native VLAN и транковых каналов

В части 2 рассматриваются создание сетей VLAN, назначения сетям VLAN портов коммутатора, настройка транковых портов и изменение native VLAN для всех коммутаторов.

Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы, приведены в приложении А. Чтобы проверить свои знания, попробуйте настроить сети VLAN, native VLAN и транковые каналы, не обращаясь к приложению.

Шаг 1: Создайте сети VLAN.

Используйте соответствующие команды, чтобы создать сети VLAN 10 и 99 на всех коммутаторах. Присвойте сети VLAN 10 имя **User,** а сети VLAN 99 — имя **Management.**

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management

S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management

S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
```

Шаг 2: Переведите пользовательские порты в режим доступа и назначьте сети VLAN.

Для интерфейса F0/6 S1 и интерфейса F0/18 S3 включите порты, настройте их в качестве портов доступа и назначьте их сети VLAN 10.

Шаг 3: Настройте транковые порты и назначьте их сети native VLAN 99.

Для портов F0/1 и F0/3 на всех коммутаторах включите порты, настройте их в качестве транковых и назначьте их сети native VLAN 99.

Шаг 4: Настройте административный интерфейс на всех коммутаторах.

Используя таблицу адресации, настройте на всех коммутаторах административный интерфейс с соответствующим IP-адресом.

Шаг 5: Проверка конфигураций и возможности подключения.

Используйте команду **show vlan brief** на всех коммутаторах, чтобы убедиться в том, что все сети VLAN внесены в таблицу VLAN и назначены правильные порты.

Используйте команду **show interfaces trunk** на всех коммутаторах, чтобы проверить транковые интерфейсы.

Используйте команду **show running-config** на всех коммутаторах, чтобы проверить все остальные конфигурации.

Какие настройки используются для режима протокола spanning-tree на коммутаторах Cisco?

Проверьте подключение между PC-A и PC-C. Удалось ли выполнить эхо-запрос?

Если эхо-запрос выполнить не удалось, следует выполнять отладку до тех пор, пока проблема не будет решена.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Настройка корневого моста и проверка сходимости PVST+

В части 3 вам предстоит определить корневой мост по умолчанию в сети, назначить основной и вспомогательный корневые мосты и использовать команду **debug** для проверки сходимости PVST+.

Примечание. Команды, необходимые для выполнения заданий третьей части лабораторной работы, приведены в приложении А. Проверьте свои знания: попробуйте настроить корневой мост, не обращаясь к приложению.

Шаг 1: Определите текущий корневой мост.

С помощью какой команды пользователи определяют состояние протокола spanning-tree коммутатора Cisco Catalyst для всех сетей VLAN? Запишите команду в строке ниже.

Выполните команду на всех трех коммутаторах, чтобы ответить на следующие вопросы:

Примечание. На каждом коммутаторе доступно три экземпляра протокола spanning-tree. По умолчанию на коммутаторах Cisco используется конфигурация STP PVST+, которая позволяет создавать отдельный экземпляр протокола spanning-tree для каждой сети VLAN (VLAN 1 и все остальные настроенные пользователем сети VLAN).

Какой приоритет моста используется для коммутатора S1 в сети VLAN 1?

Какой приоритет моста используется для коммутатора S2 в сети VLAN 1?

Какой приоритет моста используется для коммутатора S3 в сети VLAN 1?

Какой коммутатор является корневым мостом?

Почему этот коммутатор выбран в качестве корневого моста?

Шаг 2: Настройте основной и вспомогательный корневые мосты для всех существующих сетей VLAN.

При выборе корневого моста (коммутатора) по MAC-адресу может образоваться условно оптимальная конфигурация. В этой лабораторной работе вам необходимо настроить коммутатор S2 в качестве корневого моста и коммутатор S1 — в качестве вспомогательного корневого моста.

a. Настройте коммутатор S2 в качестве основного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

b. Настройте коммутатор S1 в качестве вспомогательного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

Используйте команду **show spanning-tree** для ответа на следующие вопросы: Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _ Какой интерфейс в сети находится в состоянии блокировки?

Шаг 3: Измените топологию 2 уровня и проверьте сходимость.

Чтобы проверить сходимость PVST+, необходимо создать изменение топологии 2 уровня, используя команду **debug** для отслеживания событий протокола spanning-tree.

a. Выполните команду **debug spanning-tree events** в привилегированном режиме на

```
S3# debug spanning-tree events
Spanning Tree event debugging is on
```

b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

```
S3(config)# interface f0/1
S3(config-if)# shutdown
*Mar  1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/
*Mar  1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0
*Mar  1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0
*Mar  1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vl
state to down
*Mar  1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vl
state to down
*Mar  1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, change
administratively down
*Mar  1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface Fa
changed state to down
*Mar  1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar  1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar  1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
*Mar  1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/
*Mar  1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar  1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0
*Mar  1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar  1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
```

```
*Mar  1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar  1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
*Mar  1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Примечание. Прежде чем продолжить, исходя из выходных данных команды **debug** убедитесь, что все сети VLAN на интерфейсе F0/3 перешли в состояние пересылки, после чего используйте команду **no debug spanning-tree events,** чтобы остановить вывод данных командой **debug.**

Через какие состояния портов проходит каждая сеть VLAN на интерфейсе F0/3 в процессе схождения сети?

Используя временную метку из первого и последнего сообщений отладки STP, рассчитайте время (округляя до секунды), которое потребовалось для схождения сети. **Рекомендация.** Формат временной метки сообщений отладки: чч.мм.сс.мс

Часть 4: Настройка Rapid PVST+, PortFast, BPDU Guard и проверка сходимости

В части 4 вам предстоит настроить Rapid PVST+ на всех коммутаторах. Вам необходимо будет настроить функции PortFast и BPDU guard на всех портах доступа, а затем использовать команду debug для проверки сходимости Rapid PVST+.

Примечание. Команды, необходимые для выполнения заданий в четвертой части, приведены в приложении А. Проверьте свои знания. Для этого попробуйте настроить Rapid PVST+, PortFast и BPDU guard, не обращаясь к материалам в приложении.

Шаг 1: Настройте Rapid PVST+.

a. Настройте S1 для использования Rapid PVST+. Запишите команду в строке ниже.

b. Настройте S2 и S3 для Rapid PVST+.

c. **Проверьте конфигурации с помощью команды** show running-config | include spanning-tree mode.

S1# show running-config | include spanning-tree mode

```
spanning-tree mode rapid-pvst

S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst

S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Шаг 2: Настройте PortFast и BPDU Guard на портах доступа.

PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения. Эту функцию рекомендуется использовать при подключении узлов, чтобы они могли начать обмен данными по сети VLAN немедленно, не дожидаясь протокола spanning-tree.

Чтобы запретить портам, настроенным с использованием PortFast, пересылать кадры BPDU, которые могут изменить топологию протокола spanning-tree, можно включить функцию BPDU guard. После получения BPDU функция BPDU Guard отключает порт, настроенный с помощью функции PortFast.

a. Настройте F0/6 на S1 с помощью функции PortFast. Запишите команду в строке ниже.

b. Настройте F0/6 на S1 с помощью функции BPDU Guard. Запишите команду в строке ниже.

c. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции PortFast. Запишите команду в строке ниже.

d. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции BPDU. Запишите команду в строке ниже.

Шаг 3: Проверьте сходимость Rapid PVST+.

a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
*Mar  1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar  1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar  1 01:28:37.588: RSTP(99): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar  1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar  1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
*Mar  1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar  1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar  1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar  1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar  1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar  1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar  1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
```

```
*Mar  1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar  1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar  1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar  1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar  1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a resp
proposal
*Mar  1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a res
proposal
*Mar  1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a res
proposal
*Mar  1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastE
```

cnangea state to up

Используя временную метку из первого и последнего сообщений отладки RSTP, рассчитайте время, которое потребовалось для схождения сети.

Вопросы на закрепление

1. В чем заключается главное преимущество Rapid PVST+?

2. Каким образом настройка порта с помощью функции PortFast обеспечивает более быстрое схождение?

3. Какую защиту обеспечивает функция BPDU Guard? **Приложение А. Команды настройки коммутатора**

Коммутатор S1

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/1
```

```
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface f0/3
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# exit
S1(config)# spanning-tree vlan 1,10,99 root secondary
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

Коммутатор S2

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# exit
S2(config)# spanning-tree vlan 1,10,99 root primary
S2(config)# spanning-tree mode rapid-pvst
```

Коммутатор S3

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
S3(config-vlan)# exit
S3(config)# interface f0/18
S3(config-if)# no shutdown
S3(config-if)# switchport mode access
```

S3	config- if)	#	switchport access vlan 10
S3	config- if)	#	spanning-tree portfast
S3	config- if)	#	spanning-tree bpduguard enable
S3	config- if)	#	interface f0/1
S3	config- if)	#	no shutdown
S3	config- if)	#	switchport mode trunk
S3	config- if)	#	switchport trunk native vlan 99
S3	config- if)	#	interface f0/3
S3	config- if)	#	no shutdown
S3	config- if)	#	switchport mode trunk
S3	config- if)	#	switchport trunk native vlan 99
S3	config- if)	#	interface vlan 99
S3	config- if)	#	ip address 192.168.1.13 255.255.255.0
S3	config- if)	#	exit
S3	**config)#** spanning-tree mode rapid-pvst		

Практическая работа 3 Настройка протокола GLBP
Лабораторная работа. Настройка протоколов HSRP и GLBP

Топология

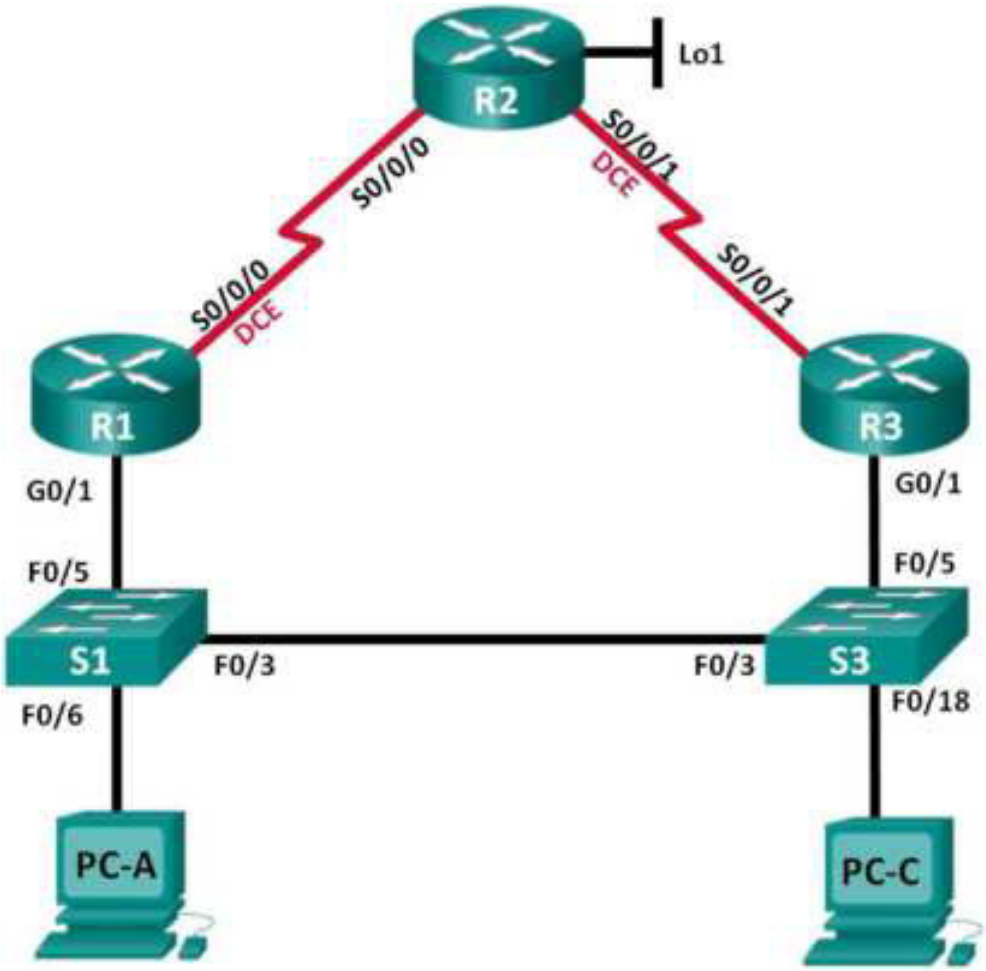


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo1	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.1.3	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка обеспечения избыточности на первом хопе с помощью HSRP Часть 3. Настройка обеспечения избыточности на первом хопе с помощью GLBP

Исходные данные/сценарий

Протокол spanning-tree обеспечивает беспетлевую избыточность между коммутаторами в пределах сети LAN. Однако оно не предоставляет избыточные шлюзы по умолчанию для устройств оконечных пользователей в пределах сети на случай сбоя одного из маршрутизаторов. Протоколы обеспечения избыточности на первом хопе (First Hop Redundancy Protocols, FHRP) предоставляют избыточные шлюзы по умолчанию для оконечных устройств. При этом конфигурация оконечного пользователя не требуется.

В этой лабораторной работе вам предстоит выполнить настройку двух протоколов FHRP. В части 2 необходимо настроить протокол Cisco Hot Standby Routing Protocol (HSRP), а в части 3 — настроить протокол Cisco Gateway Load Balancing Protocol (GLBP).

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена и в них нет начальной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и проверка соединения

В первой части вам предстоит настроить топологию сети и выполнить базовые настройки, например, IP-адреса интерфейса, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с диаграммой топологии и выполните разводку кабелей по необходимости.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.

d. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора DCE.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

f. Назначьте **cisco** в качестве пароля виртуального терминала VTY и активируйте вход.

g. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

h. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте **cisco** в качестве пароля виртуального терминала VTY и активируйте вход.

g. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

h. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 6: Проверьте подключение между PC-A и PC-C.

Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C. Успешно ли выполнен эхо-запрос?

Если эхо-запросы не проходят, выполните отладку основных настроек устройства.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг 7: Настройте маршрутизацию.

a. Настройте протокол EIGRP на маршрутизаторах и используйте значение административной дистанции, равное 1. Добавьте в процесс EIGRP все сети, кроме 209.165.200.224/27.

b. Настройте маршрут по умолчанию на R2, используя Lo1 в качестве выходного интерфейса к сети 209.165.200.224/27, и перераспределите этот маршрут в процесс EIGRP.

Шаг 8: Проверьте соединение.

a. Эхо-запросы, отправленные от PC-A в каждый интерфейс на R1, R2, R3 и PC-C, должны быть успешными. Все эхо-запросы выполнены успешно?

b. Эхо-запросы, отправленные от PC-C в каждый интерфейс на R1, R2, R3 и PC-A., должны быть успешными. Все эхо-запросы выполнены успешно?

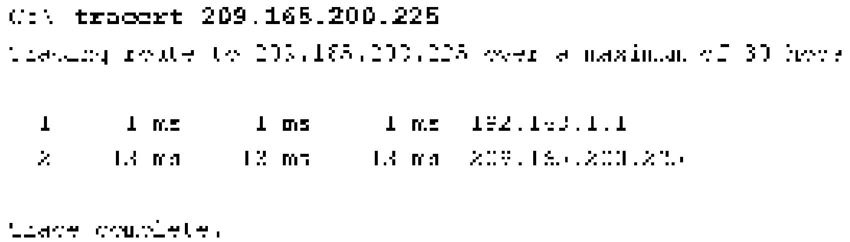
Часть 2: Настройка обеспечения избыточности на первом хопе с помощью HSRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза. PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет.

В части 2 вам предстоит изучить поведение сети до и после настройки протокола HSRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь loopback-адрес на R2.

Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.

a. В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.



```
C:\ tracert 209.165.200.225
Tracing route to 209.165.200.225 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    13 ms    13 ms    13 ms  209.165.200.225

Trace complete.
```

Какой путь прошли пакеты от PC-A до 209.165.200.225?

b. В командной строке на PC-C введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

Какой путь прошли пакеты от PC-C до 209.165.200.225?

Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.

a. В командной строке на PC-A введите команду **ping -t** для адреса **209.165.200.225** на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

Примечание. Чтобы прервать отправку эхо-запросов, нажмите комбинацию клавиш **Ctrl+C** или закройте окно командной строки.

`C:\ ping -t 209.165.200.225`

Pinging *209*		.165	.2 0C	.225	with 32 bytes			of	data	
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
Reply	from	209.	165.	200.	225:	bytes	=32	time	=9ms	TTL
<Данные опущены>										

b. В процессе эхо-тестирования отсоедините кабель Ethernet от интерфейса F0/5 на S1. Отключение интерфейса F0/5 на S1 приведет к тому же результату.

Что произошло с трафиком эхо-запросов?

c. Повторите шаги 2a и 2b на PC-C и S3. Отсоедините кабель от интерфейса F0/5 на S3. Какие получены результаты?

d. Повторно подсоедините кабели Ethernet к интерфейсу F0/5 или включите интерфейс F0/5 на S1 и S3, соответственно. Повторно отправьте эхо-запросы на 209.165.200.225 с компьютеров PC-A и PC-C, чтобы убедиться в том, что подключение восстановлено.

Шаг 3: Настройте HSRP на R1 и R3.

В этом шаге вам предстоит настроить HSRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для HSRP. R1 назначается активным маршрутизатором с помощью команды приоритета HSRP.

a. Настройте протокол HSRP на маршрутизаторе R1.

```
R1(config)# interface g0/1
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
```

b. Настройте протокол HSRP на маршрутизаторе R3.

```
R1# show standby
GigabitEthernet0/1   Group 1
  State is Active
    1 state change, last state change 00:02:11
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.784 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3, priority 100 (expires in 9.568 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)

R3# show standby
GigabitEthernet0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:02:20
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.128 secs
  Preemption disabled
  Active router is 192.168.1.1, priority 150 (expires in 10.592 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp Gi0/1 1" (default)
R3(config)# interface g0/1
R3(config-if)# standby 1 ip 192.168.1.254
```

c. Проверьте HSRP, выполнив команду **show standby** на R1 и R3.

Используя указанные выше выходные данные, ответьте на следующие вопросы:

Какой маршрутизатор является активным?

Какой MAC-адрес используется для виртуального IP-адреса?

Какой IP-адрес и приоритет используются для резервного маршрутизатора?

d. Используйте команду **show standby brief** на R1 и R3, чтобы просмотреть сводку состояния HSRP. Пример выходных данных приведен ниже.

```
R1# show standby brief
                     P indicates configured to preempt.

Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       1    150 P Active  local           192.168.1.3     192.168.1.254
```

```
R3# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/        1    100   Standby 192.168.1.1     local           192.168.1.254
```

e. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?

Проверьте новые настройки. Отправьте эхо-запрос с PC-A и с PC-C на loopback-адрес маршрутизатора R2. Успешно ли выполнены эхо-запросы?

Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение с

коммутатором, подключенным к активному маршрутизатору HSRP (R1).

a. В командной строке на PC-A введите команду **ping -t** для адреса 209.165.200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

b. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

Что произошло с трафиком эхо-запросов?

Шаг 5: Проверьте настройки HSRP на маршрутизаторах R1 и R3.

На коммутаторах R1 и R3 выполните команду **show standby brief.** Какой маршрутизатор является активным?

Повторно подсоедините кабель, соединяющий коммутатор и маршрутизатор, или включите интерфейс F0/5.

Отключите команды конфигурации HSRP на маршрутизаторах R1 и R3.

```
R1(config)# interface g0/1
R1(config-if)# no standby 1

R3(config)# interface g0/1
R3(config-if)# no standby 1
```

Часть 3: Настройка обеспечения избыточности на первом хопе с помощью GLBP

По умолчанию HSRP НЕ выполняет распределение нагрузки. Активный маршрутизатор всегда обрабатывает весь трафик, а резервный задействуется только в случае сбоя канала. Подобное использование ресурсов не является эффективным. GLBP обеспечивает непрерывную избыточность пути для IP за счёт использования общих для всех шлюзов IP-адреса и MAC-адреса. GLBP также позволяет группе маршрутизаторов использовать распределение нагрузки шлюзов по умолчанию в сети LAN. Настройка GLBP выполняется аналогично настройке HSRP. Существует несколько

способов распределения нагрузки с помощью GLBP. В рамках данной лабораторной работы вы будете использовать метод циклического обслуживания.

Шаг 1: Настройте GLBP на R1 и R3.

a. Настройте протокол GLBP на маршрутизаторе R1.

```
R1(config)# interface g0/1
R1(config-if)# glbp 1 ip 192.168.1.254
R1(config-if)# glbp 1 preempt
R1(config-if)# glbp 1 priority 150
R1(config-if)# glbp 1 load-balancing round-robin
```

b. Настройте протокол GLBP на маршрутизаторе R3.

```
R3(config)# interface g0/1
R3(config-if)# glbp 1 ip 192.168.1.254
R3(config-if)# glbp 1 load balancing round robin
```

Шаг 2: Проверьте настройки GLBP на маршрутизаторах R1 и R3.

a. На коммутаторах R1 и R3 выполните команду **show glbp brief.**

```
R1# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
G0/1        1    -   100 Active   [illegible]     local           [illegible]
G0/1        1    1       Active   [illegible]     local
G0/1        1    2       Listen   0007.b400.0102  [illegible]

R3# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
G0/1        1        100 Standby  [illegible]     [illegible]     local
G0/1        1    1       Listen   0007.b400.0101  192.168.1.1
G0/1        1    2   -   Active   0007.b400.0102  local           -
```

Шаг 3: Сформируйте поток трафика от PC-A и PC-C на интерфейс loopback R2.

a. Из командной строки на PC-A отправьте эхо-запрос на адрес 209.165.200.225 R2. C:\> ping 209.165.200.225

b. Выполните команду **arp -a** на PC-A. Какой MAC-адрес используется для адреса 192.168.1.254?

c. Сгенерируйте еще больше трафика на loopback-интерфейс маршрутизатора R2. Выполните еще раз команду **arp -a.** Изменился ли MAC-адрес шлюза по умолчанию 192.168.1.254?

Как вы видите, R1 и R3 принимают участие в пересылке трафика на интерфейс loopback маршрутизатора R2. Ни один из маршрутизаторов не остается незадействованным.

Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение с коммутатором, подключенным к R1.

a. В командной строке на PC-A введите команду **ping -t** для адреса 209.165.200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

b. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

Что произошло с трафиком эхо-запросов?

Вопросы на закрепление

1. Для чего в локальной сети может потребоваться избыточность?

2. Если бы у вас был выбор, какой протокол вы бы реализовали в своей сети: HSRP или GLBP? Поясните свой выбор.

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	П оследо вател ьный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 4

Определение типовых ошибок конфигурации STP

Общие сведения и настройка конфигурации протокола связующего дерева (STP) на коммутаторах Catalyst

Содержание

Введение

Протокол STP (Spanning Tree Protocol) - это протокол второго уровня, выполняемый на мостах и коммутаторах. Спецификация для STP называется IEEE 802.1D. Основная цель STP - предотвращение создания петель при наличии в сети избыточных путей. Петли приводят к серьезным сбоям в сети.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Хотя в данном документе используются коммутаторы Cisco Catalyst 5500/5000, представленные принципы связующего дерева применимы практически ко всем устройствам, поддерживающим STP.

В представленных примерах используются следующие устройства:

• Кабель консоли, подходящий для модуля управления в данном

коммутаторе

Шесть коммутаторов Catalyst 5509

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по умолчанию. В рабочей сети необходимо понимать последствия выполнения всех команд.

Условные обозначения

Дополнительная информация об используемых в документах условных обозначениях представлена в Технические советы Cisco. Условные обозначения.

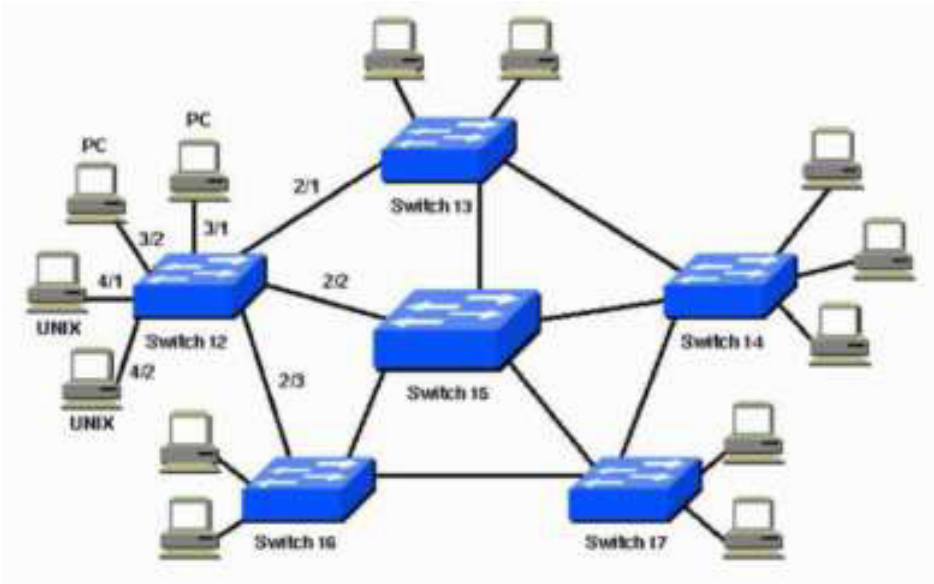
Теоретические сведения

Конфигурации данного документа применяются к коммутаторам Catalyst 2926G, 2948G, 2980G, 4500/4000, 5500/5000 и 6500/6000 под управлением ОС Catalyst (CatOS). Информация о настройке STP на других платформах коммутаторов представлена в следующих документах:

- Настройка STP и IEEE 802.1s MST (коммутаторы Catalyst 6500/6000, использующие ПО Cisco IOS®)
- Общие сведения и настройка STP (коммутаторы Catalyst 4500/4000, использующие ПО Cisco IOS)
- *раздел "Настройка STP"* документа Настройка системы (коммутаторы Catalyst 2900XL/3500XL)
- Настройка STP (коммутаторы Catalyst 3550)
- Настройка STP (коммутаторы Catalyst 2950)

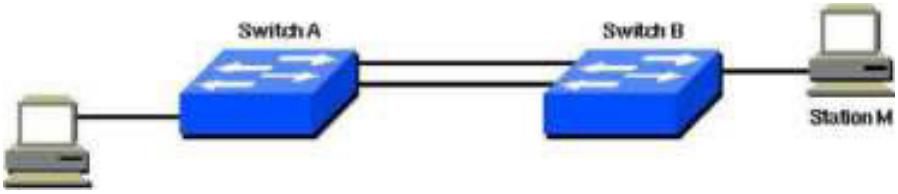
Схема сети

В данном документе используется следующая схема сети:



Основные понятия

STP выполняется на мостах и коммутаторах, совместимых с 802.1D. Существуют различные разновидности STP, но наиболее популярным и широко внедряемым стандартом является 802.1D. Внедрение протокола STP на мостах и коммутаторах предназначено для предотвращения образования петель в сети. STP нужно использовать в тех случаях, когда требуются избыточные каналы связи, а не петли. В случае отказа в сети избыточные каналы так же важны, как и резервные копии. Сбой в работе активного модуля активирует резервные каналы с тем, чтобы пользователь мог продолжать использование сети. В случае отсутствия STP на мостах и коммутаторах эта ситуация может привести к образованию петли. Рассмотрим следующую сеть:

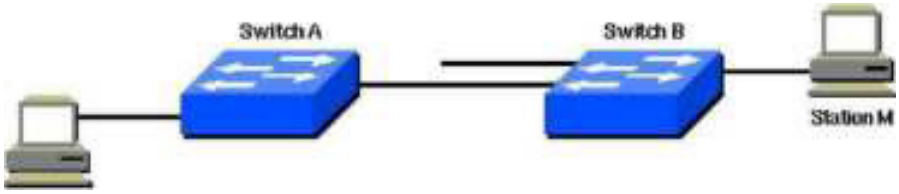


Station N

В этой сети планируется создание резервного канала между коммутатором А и коммутатором В. Однако в данной конфигурации возможно возникновение замкнутой петли. К примеру, широковещательная

или многоадресная рассылка, которая передается со станции M на станцию N, будет просто циркулировать между двумя коммутаторами.

Но при выполнении STP на обоих коммутаторах сеть логически выглядит следующим образом:



Station N

Эта информация относится к сценарию, представленному в схеме сети:

- Коммутатор 15 является магистральным коммутатором.
- Коммутаторы 12, 13, 14, 16 и 17 являются коммутаторами, прикрепленными к рабочим станциям и ПК.
- Сеть определяет следующие виртуальные локальные сети:

o 1 o 200 o 201 o 202 o 203 o 204

• Имя домена протокола магистрали VLAN (VTP) - STD-Doc.

Для обеспечения необходимой избыточности путей, а также во избежание возникновения петли STP определяет дерево, развертывающее все коммутаторы в расширенной сети. STP вводит некоторые избыточные пути данных в состояние ожидания (заблокированные), а другие пути оставляет в состоянии пересылки. Если в состоянии пересылки канал становится недоступным, STP перенастраивает сеть и перенаправляет потоки данных, используя для этого соответствующий резервный путь.

Описание технологии

Использование протокола STP предусматривает для всех коммутаторов в сети выбор корневого моста, который становится центральным узлом в сети. Все другие решения, касающиеся данной сети, в том числе какой порт заблокировать и для какого порта использовать режим пересылки, принимаются в соответствии с установками корневого моста. Среда коммутации, которая отличается от среды мостового соединения, обычно

используется с несколькими VLAN. Обычно, при внедрении корневого моста в коммутируемую сеть корневой мост считается корневым коммутатором. У каждой VLAN, поскольку они являются отдельными доменами широковещательной рассылки, должен быть свой корневой мост. Маршрут для различных VLAN может находиться в одном коммутаторе или в нескольких коммутаторах.

Примечание: Очень важен выбор корневого коммутатора для конкретной VLAN. Пользователь может сам выбрать корневой коммутатор или позволить решать коммутаторам, какой из них более уязвим. Если процесс выбора корневого коммутатора не контролируется, в сети могут возникнуть квазиоптимальные пути.

Все коммутаторы обмениваются информацией для использования при выборе корневого коммутатора, а также для последующей настройки сети. Эту информацию переносят блоки данных протокола моста (BPDU). Каждый коммутатор сравнивает параметры в BPDU, которые коммутатор отправляет соседнему устройству, с параметрами, которые коммутатор получает от этого устройства.

В процессе выбора корневого коммутатора STP чем меньше значение, тем лучше. Если коммутатор A отображает идентификатор корневого коммутатора, который меньше идентификатора, отображаемого коммутатором B, то предпочтение отдается информации от коммутатора A. Коммутатор B прекращает отображать идентификатор корневого коммутатора и принимает значение, поступившее от коммутатора A.

Дополнительная информация о некоторых вспомогательных функциях STP представлена в документе Настройка дополнительных функций STP:

- PortFast
- Root guard
- Loop guard
- BPDU guard

Работа STP

Задача

Предварительные условия

Прежде чем начать настройку STP необходимо выбрать корневой коммутатор для связующего дерева. Нужно выбрать самый централизованный коммутатор в сети, который не обязательно должен быть самым мощным. Все потоки данных в сети обрабатываются с позиции данного коммутатора. Кроме того, выберите наименее загруженный коммутатор в сети. Магистральные коммутаторы часто выступают в качестве корневого узла связующего дерева, поскольку эти коммутаторы обычно не подключены к конечным станциям. Также на них меньше влияют перемещения и изменения в сети.

После того как будет выбран корневой коммутатор, задайте соответствующие переменные для назначения этого коммутатора корневым. Единственная переменная, которую необходимо задать - это **bridge priority**. Если переменная приоритета моста коммутатора меньше, чем у всех остальных коммутаторов, другие коммутаторы автоматически выбирают этот коммутатор в качестве корневого.

Клиенты (конечные станции) портов коммутатора

Также можно выполнить команду **set spantree portfast** для каждого порта по отдельности. При выборе переменной порта **portfast**, порт немедленно переключается из режима блокировки в режим пересылки. Команда **portfast** позволяет предотвратить периоды ожидания для тех клиентов, которые используют Novell Netware или DHCP для получения IP-адреса. Однако убедитесь, что вы *не* пользуетесь этой командой в случае соединения между коммутаторами. В этом случае данная команда может привести к петле. Задержка в течение 30-60 секунд при переходе из режима блокировки в режим пересылки предотвращает образование временной петли в сети при соединении двух коммутаторов.

Для большинства других переменных STP следует оставить их значения по умолчанию.

Правила функционирования

В этом разделе представлены правила функционирования STP. При первом подключении коммутаторов они запускают процесс выбора корневого коммутатора. Каждый коммутатор передает BPDU на коммутатор, подключенный напрямую, для каждой VLAN.

При прохождении BPDU через сеть каждый коммутатор сравнивает отправленный им блок данных BPDU с BPDU, полученными от соседей. Затем коммутаторы согласовывают между собой, какой коммутатор должен стать корневым. В процессе выбора побеждает коммутатор с наименьшим идентификатором моста в сети.

Примечание: Помните о том, что на каждую виртуальную сеть определяется один корневой коммутатор. После завершения процесса идентификации корневого коммутатора, коммутаторы придерживаются следующих правил:

- **Правило STP 1**— Все порты корневого коммутатора должны находиться в режиме пересылки.

Примечание: В некоторых пограничных случаях, в которых участвуют порты с зацикливанием, для этого правила может существовать исключение.

Затем каждый коммутатор определяет лучший путь к корневому узлу. Это происходит путем сравнения информации во всех BPDU, которые коммутаторы получили на всех портах. Коммутатор использует порт с наименьшим количеством информации в BPDU в качестве пути к корневому коммутатору; порт с наименьшим количеством информации в BPDU является корневым портом. После обнаружения корневого порта коммутатор переходит к правилу 2.

- **Правило STP 2**—Корневой порт должен находиться в режиме пересылки.

Кроме того, коммутаторы в каждом сегменте ЛВС совместно определяют, какой коммутатор лучше всего использовать, чтобы переместить данные из этого сегмента в корневой мост. Этот коммутатор

называется выделенным коммутатором.

- **Правило STP 3**—В отдельном сегменте ЛВС порт выделенного коммутатора, подключенного к этому сегменту, должен быть переведен в режим пересылки.
- **Правило STP 4**—Все другие порты на всех коммутаторах (для VLAN) следует перевести в режим блокировки. Это правило относится только к тем портам, которые подключены к другим мостам или коммутаторам. STP не используется в портах, которые подключены к рабочим станциям или ПК. Эти порты остаются в состоянии пересылки.

Примечание: Добавление или удаление виртуальных локальных сетей при использовании протокола STP в режиме связующего дерева для каждого VLAN (PVST / PVST+) вызывает пересчет связующего дерева для этой VLAN, и трафик нарушается только для этой сети. Другие сегменты VLAN на магистральном канале могут пересылать трафик в обычном режиме. Добавление или удаление виртуальных локальных сетей в режиме множественных связующих деревьев (MST) вызывает пересчет связующего дерева для этой VLAN, и трафик нарушается только для этого сегмента MST.

Примечание: По умолчанию связующее дерево выполняется для каждого порта. Отключение функции связующего дерева невозможно в коммутаторах на основании отдельных портов. Возможно отключение STP для каждой VLAN или глобально для всего коммутатора, хотя это не рекомендуется. Отключение функции связующего дерева требует большой осторожности, поскольку это приводит к появлению в сети петель уровня 2.

Пошаговые инструкции

Выполните следующие шаги:

1. Чтобы получить информацию о версии ПО, используемого коммутатором, выполните команду **show version**. **Примечание:** Все коммутаторы используют одну и ту же версию ПО.

Switch-15> (enable)**show version**

WS-C5505 Software, Version McpSW: 4.2(1) NmpSW: 4.2(1) Copyright

(c) 1995-1998 by Cisco Systems NMP S/W compiled on Sep 8 1998, 10:30:21

MCP S/W compiled on Sep 08 1998, 10:26:29

System Bootstrap Version: 5.1(2)

Hardware Version: 1.0 Model: WS-C5505 Serial #: 066509927 Mod Port Model Serial # Versions

1 0 WS-X5530 008676033 Hw : 2.3

Fw 5.1(2)
Fw1
Sw 4.4(1)

4.2(1)

В этом сценарии коммутатор 15 - оптимальный выбор для корневого коммутатора сети для всех VLAN, поскольку этот коммутатор является магистральным.

2. Чтобы установить приоритет коммутатора равным 8192 для виртуальной сети или сетей, которые указывают *vlan_id*, выполните команду **set spantree root** *vlan_id.*

Примечание: Приоритет коммутаторов по умолчанию равен 32768. При установке приоритета с помощью этой команды коммутатор 15 выбирается в качестве корневого коммутатора, поскольку он использует наименьший приоритет.

Switch-15> (enable)set spantree root 1

VLAN 1 bridge priority set to 8192.

VLAN 1 bridge max aging time set to 20.

VLAN 1 bridge hello time set to 2.

VLAN 1 bridge forward delay set to 15.

Switch is now the root switch for active VLAN 1. Switch-15> (enable)

Switch-15> (enable)set spantree root 200

VLAN 200 bridge priority set to 8192.

VLAN 200 bridge max aging time set to 20.

VLAN 200 bridge hello time set to 2.

VLAN 200 bridge forward delay set to 15.

Switch is now the root switch for active VLAN 200. Switch-15> (enable)

Switch-15> (enable) set spantree root 201

VLAN 201 bridge priority set to 8192.

VLAN 201 bridge max aging time set to 20.

VLAN 201 bridge hello time set to 2.

VLAN 201 bridge forward delay set to 15.

Switch is now the root switch for active VLAN 201. Switch-15> (enable)

Switch-15> (enable) set spantree root 202

VLAN 202 bridge priority set to 8192.

VLAN 202 bridge max aging time set to 20.

VLAN 202 bridge hello time set to 2.

VLAN 202 bridge forward delay set to 15.

Switch is now the root switch for active VLAN 202. Switch-15>

Switch-15> (enable)set spantree root 203

VLAN 203 bridge priority set to 8192.

VLAN 203 bridge max aging time set to 20.

VLAN 203 bridge hello time set to 2.

VLAN 203 bridge forward delay set to 15.

Switch is now the root switch for active VLAN 203. Switch-15>

Switch-15> (enable)set spantree root 204

VLAN 204 bridge priority set to 8192.

VLAN 204 bridge max aging time set to 20.

VLAN 204 bridge hello time set to 2.

VLAN 204 bridge forward delay set to 15.

Switch is now the root switch for active VLAN 204. Switch-15> (enable)

Более краткий вариант этой команды приводит к тем же результатам, как показано на примере далее:

```
Switch-15> (enable) set spantree root 1,200-204
VLANs 1,200-204 bridge priority set to 8189.
VLANs 1,200-204 bridge max aging time set to 20.
VLANs 1,200-204 bridge hello time set to 2.
VLANs 1,200-204 bridge forward delay set to 15.
Switch is now the root switch for active VLANs 1,200-204.
Switch-15> (enable)
```

Команда **set spantree priority** предоставляет третий способ определения корневого коммутатора:

Switch-15> (enable)set spantree priority 8192 1

Spantree 1 bridge priority set to 8192.

Switch-15> (enable)

Примечание: В этом сценарии все коммутаторы начинают работу с очищенными конфигурациями. Следовательно, все коммутаторы начинают работать с приоритетом моста равным 32768. Если вы не уверены в том, что все коммутаторы в сети обладают приоритетом большим 8192, установите приоритет требуемого корневого моста равным 1.

3. Для того, чтобы настроить параметр PortFast на коммутаторах 12, 13, 14, 16 и 17, выполните команду **set spantree portfast** *mod_num/port_num.*

Примечание: Этот параметр можно настраивать только на портах, подключенных к рабочим станциям или ПК. Не включайте PortFast на портах, подключенных к другому коммутатору.

В этом примере показана настройка коммутатора 12. Другие коммутаторы можно настроить таким же образом. Коммутатор 12 поддерживает следующие подключения портов:

- Порт 2/1 подключен к коммутатору 13.
- Порт 2/2 подключен к коммутатору 15.
- Порт 2/3 подключен к коммутатору 16.
- Порты 3/1 подключены к ПК через порт 3/24.
- Порты 4/1 через порт 4/24 подключены к рабочим станциям UNIX.

4/24:

Используя эту информацию в качестве стартовой, выполните команду **set spantree portfast** на портах 3/1 - 3/24 и на портах 4/1 -

Switch-12> (enable)set spantree portfast 3/1-24 enable

Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning-tree loops. Use with caution.

Spantree ports 3/1-24 fast start enabled.

Switch-12> (enable)

Switch-12> (enable) set spantree portfast 4/1-24 enable

Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning-tree loops. Use with caution.

Spantree ports 4/1-24 fast start enabled.

Switch-12> (enable)

4. Чтобы убедиться, что коммутатор 15 является корневым коммутатором на соответствующих VLAN, выполните команду **show spantree** *vlan_id.*

Используя выходные данные этой команды, сравните MAC-адрес корневого коммутатора с MAC-адресом коммутатора, из которого поступила команда. Если адреса совпадают, коммутатор, в котором вы находитесь, является корневым коммутатором VLAN. Корневой порт 1/0 также указывает на то, что данный коммутатор является корневым. Вот пример выходных данных команды:

Switch-15> (enable)**show spantree 1** VLAN 1

spanning-tree enabled spanning-tree type

```
Designated Root              00-10-0d-b1-78-00

!    Это MAC-адрес корневого коммутатора для VLAN 1.

Designated Root Priority     8192
Designated  Root  Cost       0
Designated  Root  Port       1/0
Root Max Age 20 sec       Hello Time 2 sec Forward Delay 15 sec
```

Эти выходные данные показывают, что коммутатор 15 является выделенным корневым коммутатором связующего дерева для VLAN 1. MAC-адрес выделенного корневого коммутатора, 00-10-0d-b1-78-00, соответствует MAC-адресу идентификатора моста коммутатора Switch 15, - 00-10-0d-b1-78-00. Другим доказательством того, что это - выделенный корневой коммутатор, является использование выделенного корневого порта

```
Bridge ID Priority          8192
Bridge Max Age 20 sec     Hello Time 2 sec     Forward Delay 15 sec
```

1/0.

В этих выходных данных коммутатора 12 он признает, что коммутатор 15 является **выделенным коммутатором** для VLAN 1:

Switch-12> (enable)**show spantree 1** VLAN 1

spanning-tree enabled

spanning-tree type **IEEEDesignated Root** 00-10-0d-b1-78-00

!----- Это MAC-адрес корневого коммутатора для VLAN 1.

Designated RootPriority 8192

Designated Root Cost 19

Designated Root Port 2/3

```
Bridge ID MAC ADDR
Bridge ID Priority
Bridge Max Age 20 sec
```

Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

00-10-0d-b2-8c-00

32768

Hello Time 2 sec Forward Delay 15 sec

Примечание: Выходные данные команды **show spantree** *vlan_id* для других коммутаторов и VLAN также могут свидетельствовать, что коммутатор 15 является выделенным корневым коммутатором для всех VLAN.

Проверка

В данном разделе содержатся сведения для проверки работы текущей конфигурации.

Output Interpreter Tool (только для зарегистрированных клиентов) (OIT)

поддерживает определенные команды **show**. Используйте OIT для просмотра и анализа выходных данных команды **show**.

- **show spantree** *vlan_id*—Показывает текущее состояние связывающего дерева для данного идентификатора VLAN с точки зрения коммутатора, на котором была выполнена команда.
- **show spantree summary**—Предоставляет обзор подключенных портов связующего дерева в рамках VLAN.

Устранение неполадок

Этот раздел содержит сведения об устранении неполадок конфигурации.

Стоимость пути протокола STP автоматически изменяется при изменении скорости/дуплекса порта

STP вычисляет стоимость пути на основании скорости среды (пропускной способности) каналов между коммутаторами и стоимости портов по каждому кадру пересылки. Связующее дерево выбирает корневой порт на основании стоимости порта. Порт с наименьшей стоимостью пути к корневому мосту становится корневым портом. Корневой порт всегда находится в состоянии пересылки.

Если скорость/дуплекс порта изменяется, связующее дерево автоматически пересчитывает стоимость пути. Изменения в стоимости пути могут привести к изменениям в топологии связующего дерева.

Дополнительная информация о вычислении стоимости порта представлена в разделе *"Подсчет и присвоение стоимости порта'* документа "Настройка связующего дерева".

Команды устранения неисправностей

Средство Output Interpreter Tool (только для зарегистрированных заказчиков) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитических данных по выходным данным команды **show**.

Примечание: До использования команд **отладки** ознакомьтесь с документом Важные сведения о командах отладки.

- **show spantree** *vlan_id*—показывает текущее состояние связывающего дерева для данного идентификатора VLAN с точки зрения коммутатора, на котором была выполнена команда.
- **show spantree summary**—предоставляет обзор подключенных портов связующего дерева в рамках VLAN.
- **show spantree statistics**—отображает статистические сведения о связующем дереве.
- **show spantree backbonefast**—показывает, включена ли функция связующего дерева Backbone Fast Convergence.
- **show spantree blockedports**—показывает только заблокированные порты.
- **show spantree portstate**—определяет текущее состояние связующего дерева порта Token Ring в рамках связующего дерева.
- **show spantree portvlancost—**показывает стоимость пути для сетей VLAN на порте.
- **show spantree uplinkfast—**отображает настройки UplinkFast.

Краткие сведения о команде

Синтаксис:	**show version**
В данном документе используется:	**show version**
Синтаксис:	**set spantree root** [vlan_id]
В данном документе используется:	**set spantree root 1**
	set spantree root 1,200-204
Синтаксис:	**set spantree root** [vlan_id]
В данном документе используется:	**set spantree priority 8192 1**
Синтаксис:	**set spantree portfast** mod_num/port_num
В данном документе используется:	**set spantree portfast 3/1-24 enable**
Синтаксис:	**set spantree root** [vlan_id]
В данном документе	

Дополнительные сведения

- Ошибки протокола связующего дерева и соответствующие рекомендации по разработке
- Общая информация об изменении топологии протокола связующего дерева
- Настройка связующего дерева (коммутаторы Catalyst 4500/4000)
- Настройка связующего дерева (коммутаторы Catalyst 5500/5000)
- Настройка связующего дерева (коммутаторы Catalyst 6500/6000)
- Страницы поддержки продуктов ЛВС
- Страница поддержки коммутации ЛВС
- Техническая поддержка и документация - Cisco Systems

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92134/5.shtml

Практическая работа 5
Настройка EtherChannel

Топология

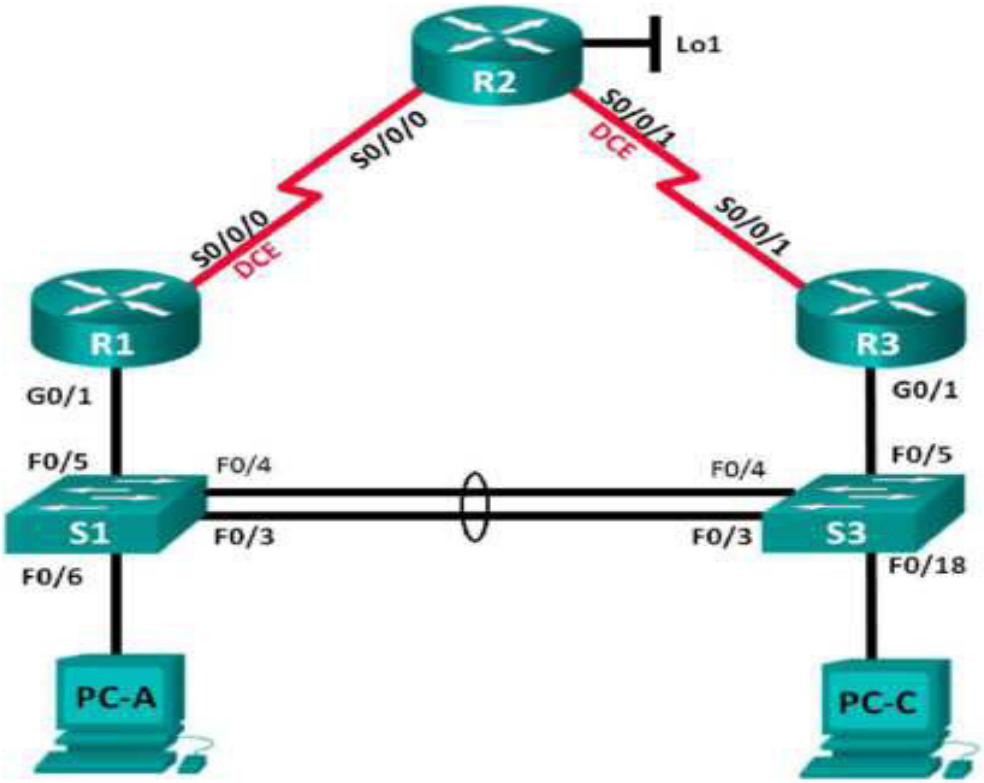


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
R2	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo1	209.165.200.225	255.255.255.224	—
R3	G0/1	192.168.1.3	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка обеспечения избыточности на первом хопе с помощью VRRP

Общие сведения/сценарий

Связующее дерево обеспечивает резервирование коммутаторами в локальной сети, не допуская возникновения петель. Но оно не позволяет организовать в сети резервирование шлюзов по умолчанию для устройств конечных пользователей на случай сбоя одного из маршрутизаторов. Протоколы обеспечения избыточности на первом хопе (First Hop Redundancy Protocols, FHRP) предоставляют избыточные шлюзы по умолчанию для конечных устройств. При этом конфигурация конечного

пользователя не требуется. В этой лабораторной работе предстоит настроить протокол VRRP, являющийся протоколом FHRP.

Агрегирование каналов позволяет создавать логические каналы, состоящие из двух или более физических каналов. Таким образом увеличивается пропускная способность, а также используется только один физический канал. Агрегирование каналов также обеспечивает избыточность в случае сбоя одного из каналов.

В этой лабораторной работе вам предстоит настроить EtherChannel — тип агрегирования каналов, который используется в коммутируемых сетях. Вы настроите EtherChannel с помощью протокола агрегирования портов (PAgP) и протокола управления агрегированием каналов (LACP).

Примечание. PAgP является проприетарным протоколом Cisco, который можно использовать только на коммутаторах Cisco и коммутаторах лицензированных поставщиков, поддерживающих PAgP. Протокол LACP является протоколом агрегирования каналов, который определен стандартом IEEE 802.3ad и не связан с конкретным поставщиком.

Протокол LACP позволяет коммутаторам Cisco осуществлять управление каналами Ethernet между коммутаторами в соответствии с протоколом 802.3ad. В создании канала могут участвовать до 16 портов. Восемь из портов находятся в активном режиме (active), а остальные восемь — в режиме ожидания (standby). В случае сбоя любого из активных портов задействуется порт, пребывающий

в режиме ожидания. Режим ожидания (standby mode) доступен только для протокола LACP, но не для протокола PAgP.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы,

коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у маршрутизаторов и коммутаторов были удалены начальные конфигурации. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 компьютера (Windows 8, 7 или Vista с программой эмуляции терминала, например Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели согласно топологии

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.

d. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора DCE.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте cisco в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 6: Проверьте подключение между PC-A и PC-C.

Отправьте ping-запрос с компьютера PC-A на компьютер PC-C. Удалось ли получить ответ? _____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг 7: Настройте маршрутизацию.

a. Настройте RIP версии 2 на всех маршрутизаторах. Добавьте в процесс RIP все сети, кроме 209.165.200.224/27.

b. Настройте маршрут по умолчанию на маршрутизаторе R2 с использованием Lo1 в качестве интерфейса выхода в сеть 209.165.200.224/27.

c. На маршрутизаторе R2 используйте следующие команды для перераспределения маршрута по умолчанию в процесс RIP.

```
R2(config)# router rip
R2(config-router)# default-information originate
```

Шаг 8: Проверьте подключение.

a. Необходимо получить ответ на ping-запросы с компьютера PC-A от каждого интерфейса на маршрутизаторах R1, R2 и R3, а также от компьютера PC-C. Удалось ли получить все ответы?

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

b. Необходимо получить ответ на ping-запросы с компьютера PC-C от каждого интерфейса на маршрутизаторах R1, R2 и R3, а также от компьютера PC-A. Удалось ли получить все ответы?

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Часть 2: Настройка обеспечения избыточности на первом хопе с помощью VRRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза.

PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет.

В части 2 вам предстоит изучить поведение сети до и после настройки протокола VRRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь 1oopЬack-адрес на R2.

Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.

a. В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

```
C:\ ping -t 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<выходные данные опущены>
```

```
C:\ tracert 209.165.200.225
Tracing route to 209.165.200.225 over a max num of 30 hops

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    13 ms    13 ms    13 ms  209.165.200.225

Trace complete.
```

Какой путь прошли пакеты от PC-A до 209.165.200.225? _____

b. В командной строке на PC-C введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

Какой путь прошли пакеты от PC-C до 209.165.200.225? _____

Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.

a. В командной строке на PC-A введите команду **ping -t** для адреса **209.165.200.225** на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

Примечание. Чтобы прервать отправку эхо-запросов, нажмите комбинацию клавиш **Ctrl+C** или закройте окно командной строки.

b. В процессе эхо-тестирования отсоедините кабель Ethernet от интерфейса F0/5 на S1. Отключение интерфейса F0/5 на S1 приведет к тому же результату.

Что произошло с трафиком эхо-запросов?

c. Какими были бы результате при повторении шагов 2a и 2b на компьютере PC-C и коммутаторе S3?

d. Повторно подсоедините кабели Ethernet к интерфейсу F0/5 или включите интерфейс F0/5 на S1 и S3, соответственно. Повторно отправьте эхо-запросы на 209.165.200.225 с компьютеров PC-A и PC-C, чтобы убедиться в том, что подключение восстановлено.

Шаг 3: Настройте VRRP на R1 и R3.

В этом шаге вам предстоит настроить VRRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для VRRP. R1 назначается активным маршрутизатором с помощью команды приоритета VRRP.

a. Настройте протокол VRRP на маршрутизаторе R1.

```
R3(config)# interface g0/1
R3(config-if)# vrrp 1 ip 192.168.1.254
```

```
R1(config)# interface g0/1
R1(config-if)# vrrp 1 ip 192.168.1.254
R1(config-if)# vrrp 1 priority 150
```

b. Настройте протокол VRRP на маршрутизаторе R3.

c. Проверьте VRRP, выполнив команду **show vrrp** на R1 и R3. R1# **show vrrp**

Используя указанные выше выходные данные, ответьте на следующие вопросы:

Какой маршрутизатор является активным? _____

Какой MAC-адрес используется для виртуального IP-адреса? _____

Какой IP-адрес и приоритет используются для резервного маршрутизатора?

d. Используйте команду **show vrrp brief** на R1 и R3, чтобы просмотреть сводку состояния VRRP. Выходные данные приведены ниже.

R1# show vrrp brief

e. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?

f. Проверьте новые настройки. Отправьте эхо-запрос с PC-A и с PC-C на loopback-адрес маршрутизатора R2. Успешно ли выполнены эхо-запросы?

Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение с коммутатором, подключенным к активному маршрутизатору VRRP (R1).

a. В командной строке на PC-A введите команду **ping -t** для адреса 209.165.200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

b. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

Что произошло с трафиком эхо-запросов?

Шаг 5: Проверьте настройки VRRP на маршрутизаторах R1 и R3.

a. Выполните команду **show vrrp brief** на маршрутизаторах R1 и R3.

Какой маршрутизатор является активным? _____

Повторно подключите кабель, соединяющий коммутатор и маршрутизатор, или включите интерфейс F0/5. Какой маршрутизатор теперь является активным? Поясните ответ.

Шаг 6: Изменение приоритетов VRRP.

Измените приоритет VRRP на 200 на маршрутизаторе R3. Какой маршрутизатор является активным?_____

Выполните команду, чтобы сделать активным маршрутизатор R3 без изменения приоритета. Какую команду вы использовали?

c. Используйте команду **show,** чтобы убедиться, что R3 является активным маршрутизатором.

Часть 1: Настройка протокола LACP

Протокол LACP является открытым протоколом агрегирования каналов, разработанным на базе стандарта IEEE. В части 3 необходимо выполнить настройку канала между S1 и S3 с помощью протокола LACP. Кроме того, отдельные каналы

необходимо настроить в качестве транковых, прежде чем они будут объединены в каналы EtherChannel.

Шаг 1: Настройте LACP между S1 и S3.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S1(config-if-range)# channel-group 2 mode active
Creating a port-channel interface Port-channel 2

S1(config if range)# no shutdown

S3(config)# interface range f0/3-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
S3(config-if-range)# channel-group 2 mode passive
Creating a port-channel interface Port-channel 2

S3(config if range)# no shutdown
```

Шаг 2: Убедитесь, что порты объединены.

Какой протокол использует Po2 для агрегирования каналов? Какие порты агрегируются для образования Po2? Запишите команду, используемую для проверки.

Шаг 3: Проверьте наличие сквозного соединения.

Убедитесь в том, что все устройства могут передавать друг другу эхо-запросы в пределах одной сети VLAN. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

Шаг 4: Проверьте конфигурации на портах.

В настоящее время интерфейсы F0/3, F0/4 и Pol (Port-channel1) на коммутаторах S1 и S3 находятся в режиме доступе, а режим управления установлен на динамический автоматический режим (dynamic auto). Проверьте конфигурацию с помощью соответствующих команд **show run interface** *идентификатор-интерфейса* и

show interfaces *идентификатор-интерфейса* **switchport.** Для интерфейса F0/3 на S1 отображаются следующие выходные данные конфигурации:

```
S1# show run interface f0/3
Building configuration...

Current configuration : 103 bytes
!
interface FastEthernet0/3
 channel-group 1 mode active

S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Шаг 5: Убедитесь, что порты объединены.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/3(P)    Fa0/4(P)

S3# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/3(P)    Fa0/4(P)
```

Что означают флаги «SU» и «P» в сводных данных по Ethernet?

Вопросы для повторения

Для чего в локальной сети может потребоваться избыточность?

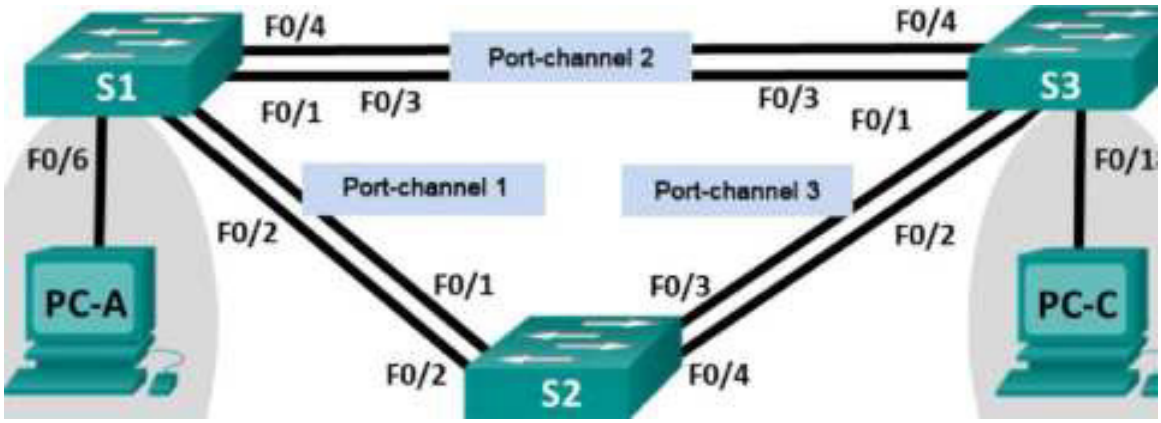
Что может препятствовать образованию каналов EtherChannel?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				

Практичекая работа 6
Поиск и устранение неполадок в работе EtherChannel

Топология



VLAN 10 VLAN 10

Пользователь Пользователь

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	Пользователь
99	Management (Руководство)

Задачи

Часть 1. Построение сети и загрузка конфигураций устройств Часть 2. Отладка EtherChannel

Исходные данные/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым администратором. В результате ошибок в конфигурации возникли проблемы со скоростью и подключением. Начальник попросил вас найти и устранить неполадки в настройке и задокументировать работу. Найдите и исправьте ошибки, используя свои знания EtherChannel и стандартные методы тестирования. Убедитесь в том, что все каналы EtherChannel используют протокол агрегирования портов (PAgP) и все узлы доступны.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.

Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и загрузка конфигураций устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры для ПК, а также загрузить конфигурации на коммутаторы.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Удалите загрузочную конфигурацию и настройки VLAN, а затем перезагрузите коммутаторы.

Шаг 4: Загрузите конфигурации коммутаторов.

Загрузите следующие конфигурации в соответствующий коммутатор. Все коммутаторы используют одинаковые пароли. Пароль привилегированного режима — **class.** Пароль для консоли и доступа vty — **cisco.** Поскольку все коммутаторы являются устройствами Cisco, сетевой администратор решил использовать протокол PAgP Cisco для всех агрегированных каналов, настроенных с использованием EtherChannel. Коммутатор S2 является корневым мостом для всех сетей VLAN в топологии.

Конфигурация коммутатора S1:

```
hostname S1
interface range f0/1-24, g0/1-2
shutdown
exit
enable secret class
no ip domain lookup
line vty 0 15
```

```
password cisco
 ogin
 ine con 0
 password cisco
 logging synchronous
 login
 exit
vlan 10
 name User
vlan 99
 Name Management
interface range f0/1-2
 switchport mode trunk
 channel-group 1 mode active
 switchport trunk native vlan 99
 no shutdown
interface range f0/3 4
 channel group 2 mode desirable
 switchport trunk native vlan 99
 no shutdown
interface f0/6
 switchport mode access
 switchport access vlan 10
 no shutdown
interface vlan 99
 ip address 192.168.1.11 255.255.25
interface port channel 1
 switchport trunk native vlan 99
 switchport mode trunk
interface port-channel 2
 switchport trunk native vlan 99
 switchport mode access
```

Конфигурация коммутатора S2:

```
hostname S2
interface range f0/1-24, g0/1-2
 shutdown
 exit
enable secret class
no ip domain lookup
line vty 0 15
 password cisco
 login
line con 0
 password cisco
 logging synchronous
```

```
 login
 exit
vlan 10
 name User
vlan 99
 name Management
spanning-tree vlan 1,10,99 root prima
interface range f0/1-2
 switchport mode trunk
 channel-group 1 mode desirable
 switchport trunk native vlan 99
 no shutdown
interface range f0/3 4
 switchport mode trunk
 channel group 3 mode desirable
 switchport trunk native vlan 99
interface vlan 99
 ip address 192.168.1.12 255.255.255.
interface port-channel 1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,99
interface port channel 3
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,9
 switchport mode trunk
```

Конфигурация коммутатора S3:

```
hostname S3
interface range f0/1 24, g0/1 2
 shutdown
 exit
enable secret class
no ip domain lookup
line vty 0 15
 password cisco
 login
line con 0
 password cisco
 logging synchronous
 login
 exit
vlan 10
 name User
vlan 99
 name Management
interface range f0/1-2
```

```
interface range f0/3 4
 switchport mode trunk
channel group 3 mode desirable
 switchport trunk native vlan 99
 no shutdown
interface f0/10
 switchport mode access
 switchport access vlan 10
 no shutdown
interface vlan 99
 ip address 192.168.1.13 255.255.255.0
interface port channel 3
 switchport trunk native vlan 99
 switchport mode trunk
```

Шаг 5: Сохраните конфигурацию.

Часть 2: Отладка EtherChannel

В части 2 необходимо проверить конфигурации на всех коммутаторах, исправить при необходимости и проверить их работоспособность.

Шаг 1: Выполните поиск и устранение неполадок в работе маршрутизатора S1.

a. Используйте команду **show interfaces trunk**, чтобы убедиться в том, что агрегированные каналы работают, как транковые порты.

Отображаются ли агрегированные каналы 1 и 2, как транковые порты?

b. Используйте команду **show etherchannel summary**, чтобы убедиться в том, что интерфейсы входят в состав соответствующего агрегированного канала, применен правильный протокол и интерфейсы задействованы.

Есть ли в выходных данных сведения о неполадках в работе EtherChannel? В случае обнаружения неполадок запишите их в отведённом ниже месте.

c. Используйте команду **show run | begin interface Port-channel** для просмотра текущей конфигурации, начиная с первого интерфейса агрегированного канала.

d. Устраните все ошибки, найденные в выходных данных из предыдущих команд **show**. Запишите команды, используемые для исправления конфигураций.

e. Используйте команду **show interfaces trunk** для проверки настроек транковой связи.

f. Используйте команду **show etherchannel summary**, чтобы убедиться в том, что агрегированные каналы работают и задействованы.

Шаг 2: Выполните поиск и устранение неполадок в работе маршрутизатора S2.

a. Выполните команду для того, чтобы убедиться, что агрегированные каналы работают в качестве транковых портов. Ниже запишите команду, которую вы использовали.

Есть ли в выходных данных сведения о неполадках в конфигурациях? В случае обнаружения неполадок запишите их в отведённом ниже месте.

b. Выполните команду, чтобы убедиться в том, что интерфейсы настроены в правильном агрегированном канале и настроен соответствующий протокол.

Есть ли в выходных данных сведения о неполадках в работе EtherChannel? В случае обнаружения неполадок запишите их в отведённом ниже месте.

c. Используйте команду **show run | begin interface Port-channel** для просмотра текущей конфигурации, начиная с первого интерфейса канала порта.

d. Устраните все ошибки, найденные в выходных данных из предыдущих команд **show**. Запишите команды, использованные для внесения изменений в конфигурацию.

e. Выполните команду для проверки параметров транковой связи.

f. Выполните команду для проверки правильного функционирования агрегированных каналов. Помните, что проблемы с агрегированным каналом могут возникнуть на любом конце канала.

Шаг 3: Выполните поиск и устранение неполадок в работе маршрутизатора S3.

a. Выполните команду для того, чтобы убедиться, что агрегированные каналы работают в качестве транковых портов.

Есть ли в выходных данных сведения о неполадках в конфигурациях? В случае обнаружения неполадок запишите их в отведённом ниже месте.

b. Выполните команду, чтобы убедиться в том, что интерфейсы настроены в правильном агрегированном канале и применен соответствующий протокол.

Есть ли в выходных данных сведения о неполадках в работе EtherChannel? В случае обнаружения неполадок запишите их в отведённом ниже месте.

c. Используйте команду **show run | begin interface Port-channel** для просмотра текущей конфигурации, начиная с первого интерфейса агрегированного канала.

d. Устраните все обнаруженные неполадки. Запишите команды, использованные для внесения изменений в конфигурацию.

e. Выполните команду для проверки параметров транковой связи. Ниже запишите команду, которую вы использовали.

f. Выполните команду для проверки правильного функционирования агрегированных каналов. Ниже запишите команду, которую вы использовали.

Шаг 4: Проверка EtherChannel и подключения

a. Используйте команду **show interfaces etherchannel** для проверки работоспособности агрегированных каналов.

b. Проверьте подключение сети VLAN Management.

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S3? Успешно ли выполняется эхо-запрос от коммутатора S2 на коммутатор S3?

c. Проверка подключения компьютеров

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C?

Если каналы EtherChannel не полностью работоспособны, отсутствует соединение между коммутаторами или между узлами. Выполните окончательную отладку.

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

Практическая работа 7

Настройка VRRP и EtherChannel

Топология

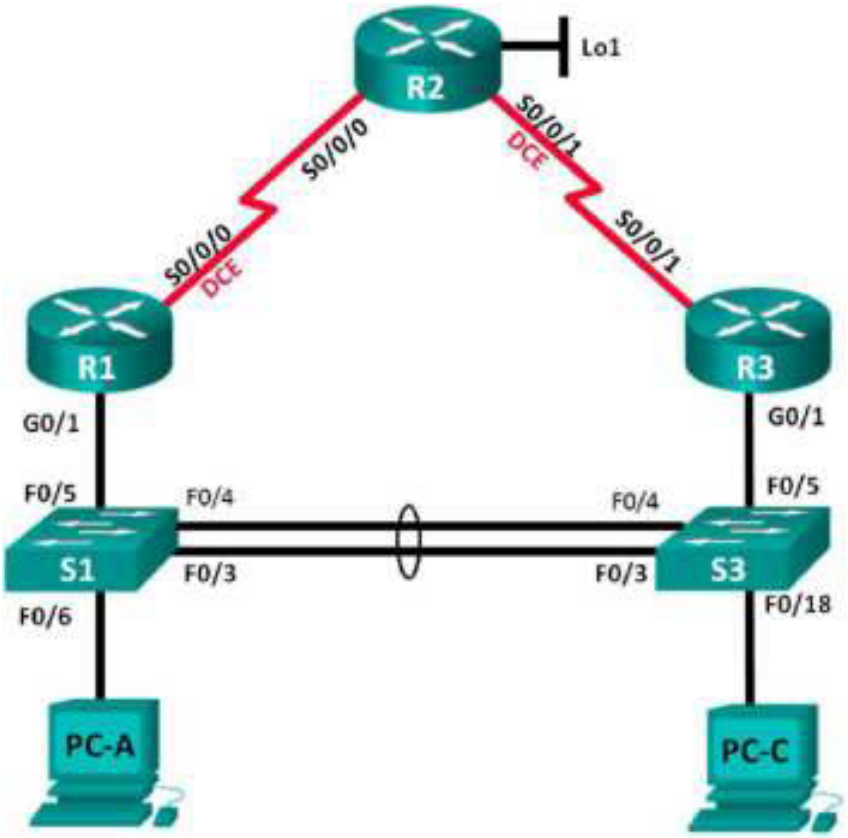


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	-
R2	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo1	209.165.200.225	255.255.255.224	—
R3	G0/1	192.168.1.3	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка обеспечения избыточности на первом хопе с помощью VRRP

Общие сведения/сценарий

Связующее дерево обеспечивает резервирование коммутаторами в локальной сети, не допуская возникновения петель. Но оно не позволяет организовать в сети резервирование шлюзов по умолчанию для устройств конечных пользователей на случай сбоя одного из маршрутизаторов. Протоколы обеспечения избыточности на первом хопе (First Hop Redundancy Protocols, FHRP) предоставляют избыточные

шлюзы по умолчанию для конечных устройств. При этом конфигурация конечного пользователя не требуется. В этой лабораторной работе предстоит настроить протокол VRRP, являющийся протоколом FHRP.

Агрегирование каналов позволяет создавать логические каналы, состоящие из двух или более физических каналов. Таким образом увеличивается пропускная способность, а также используется только один физический канал. Агрегирование каналов также обеспечивает избыточность в случае сбоя одного из каналов.

В этой лабораторной работе вам предстоит настроить EtherChannel — тип агрегирования каналов, который используется в коммутируемых сетях. Вы настроите EtherChannel с помощью протокола агрегирования портов (PAgP) и протокола управления агрегированием каналов (LACP).

Примечание. PAgP является проприетарным протоколом Cisco, который можно использовать только на коммутаторах Cisco и коммутаторах лицензированных поставщиков, поддерживающих PAgP. Протокол LACP является протоколом агрегирования каналов, который определен стандартом IEEE 802.3ad и не связан с конкретным поставщиком.

Протокол LACP позволяет коммутаторам Cisco осуществлять управление каналами Ethernet между коммутаторами в соответствии с протоколом 802.3ad. В создании канала могут участвовать до 16 портов. Восемь из портов находятся в активном режиме (active), а остальные восемь — в режиме ожидания (standby). В случае сбоя любого из активных портов задействуется порт, пребывающий

в режиме ожидания. Режим ожидания (standby mode) доступен только для протокола LACP, но не для протокола PAgP.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS

версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у маршрутизаторов и коммутаторов были удалены начальные конфигурации. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 компьютера (Windows 8, 7 или Vista с программой эмуляции терминала, например Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели согласно топологии

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.

d. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора DCE.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 6: Проверьте подключение между PC-A и PC-C.

Отправьте ping-запрос с компьютера PC-A на компьютер PC-C. Удалось ли получить ответ? _____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг 7: Настройте маршрутизацию.

a. Настройте RIP версии 2 на всех маршрутизаторах. Добавьте в процесс RIP все сети, кроме 209.165.200.224/27.

b. Настройте маршрут по умолчанию на маршрутизаторе R2 с использованием Lo1 в качестве интерфейса выхода в сеть 209.165.200.224/27.

c. На маршрутизаторе R2 используйте следующие команды для перераспределения маршрута по умолчанию в процесс RIP.

R2(config)# **router rip**

R2(config-router)# **default-information originate**

Шаг 8: Проверьте подключение.

a. Необходимо получить ответ на ping-запросы с компьютера PC-A от каждого интерфейса на маршрутизаторах R1, R2 и R3, а также от компьютера PC-C. Удалось ли получить все ответы?

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

b. Необходимо получить ответ на ping-запросы с компьютера PC-C от каждого интерфейса на маршрутизаторах R1, R2 и R3, а также от компьютера PC-A. Удалось ли получить все ответы?

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Часть 2: Настройка обеспечения избыточности на первом хопе с помощью VRRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза.

PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет.

В части 2 вам предстоит изучить поведение сети до и после настройки протокола VRRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь 1oopЬack-адрес на R2.

Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.

a. В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

```
C:\ tracert 209.165.200.225
Tracing route to 209.165.200.225 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    12 ms    13 ms    12 ms  209.165.200.225

Trace complete.
```

Какой путь прошли пакеты от PC-A до 209.165.200.225? _____

b. В командной строке на PC-C введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

Какой путь прошли пакеты от PC-C до 209.165.200.225? _____

Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.

a. В командной строке на PC-A введите команду **ping -t** для адреса **209.165.200.225** на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

Примечание. Чтобы прервать отправку эхо-запросов, нажмите комбинацию клавиш **Ctrl+C** или закройте окно командной строки.

```
C:\ ping -t 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<выходные данные опущены>
```

b. В процессе эхо-тестирования отсоедините кабель Ethernet от интерфейса F0/5 на S1. Отключение интерфейса F0/5 на S1 приведет к тому же результату.

Что произошло с трафиком эхо-запросов?

c. Какими были бы результате при повторении шагов 2a и 2b на компьютере PC-C и коммутаторе S3?

d. Повторно подсоедините кабели Ethernet к интерфейсу F0/5 или включите интерфейс F0/5 на S1 и S3, соответственно. Повторно отправьте эхо-запросы на 209.165.200.225 с компьютеров PC-A и PC-C, чтобы убедиться в том, что подключение восстановлено.

Шаг 3: Настройте VRRP на R1 и R3.

В этом шаге вам предстоит настроить VRRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для VRRP. R1 назначается активным маршрутизатором с помощью команды приоритета VRRP.

a. Настройте протокол VRRP на маршрутизаторе R1.

```
R1(config)# interface g0/1
R1(config-if)# vrrp 1 ip 192.168.1.254
R1(config-if)# vrrp 1 priority 150
```

b. Настройте протокол VRRP на маршрутизаторе R3.

```
R3(config)# interface g0/1
R3(config-if)# vrrp 1 ip 192.168.1.254
```

c. Проверьте VRRP, выполнив команду **show vrrp** на R1 и R3.

```
R1# show vrrp
```

Используя указанные выше выходные данные, ответьте на следующие вопросы: Какой маршрутизатор является активным? _____

Какой MAC-адрес используется для виртуального IP-адреса? _____

Какой IP-адрес и приоритет используются для резервного маршрутизатора?

d. Используйте команду **show vrrp brief** на R1 и R3, чтобы просмотреть сводку состояния VRRP. Выходные данные приведены ниже.

```
R1# show vrrp brief
```

e. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?

f. Проверьте новые настройки. Отправьте эхо-запрос с PC-A и с PC-C на loopback-адрес маршрутизатора R2. Успешно ли выполнены эхо-запросы?

Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение с коммутатором, подключенным к активному маршрутизатору VRRP (R1).

a. В командной строке на PC-A введите команду **ping -t** для адреса 209.165.200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

b. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

Что произошло с трафиком эхо-запросов?

Шаг 5: Проверьте настройки VRRP на маршрутизаторах R1 и R3.

a. Выполните команду **show vrrp brief** на маршрутизаторах R1 и R3.

Какой маршрутизатор является активным?_____

Повторно подключите кабель, соединяющий коммутатор и маршрутизатор, или включите интерфейс F0/5. Какой маршрутизатор теперь является активным? Поясните ответ.

Шаг 6: Изменение приоритетов VRRP.

Измените приоритет VRRP на 200 на маршрутизаторе R3. Какой маршрутизатор является активным? __

Выполните команду, чтобы сделать активным маршрутизатор R3 без изменения приоритета. Какую команду вы использовали?

c. Используйте команду **show,** чтобы убедиться, что R3 является активным маршрутизатором.

Часть 1: Настройка протокола LACP

Протокол LACP является открытым протоколом агрегирования каналов, разработанным на базе стандарта IEEE. В части 3 необходимо выполнить настройку канала между S1 и S3 с помощью протокола LACP. Кроме того, отдельные каналы необходимо настроить в качестве транковых, прежде чем они будут объединены в каналы EtherChannel.

Шаг 1: Настройте LACP между S1 и S3.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S1(config-if-range)# channel-group 2 mode active
Creating a port-channel interface Port-channel 2

S1(config-if-range)# no shutdown

S3(config)# interface range f0/3-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
S3(config-if-range)# channel-group 2 mode passive
Creating a port-channel interface Port-channel 2

S3(config-if-range)# no shutdown
```

Шаг 2: Убедитесь, что порты объединены.

Какой протокол использует Po2 для агрегирования каналов? Какие порты агрегируются для образования Po2? Запишите команду, используемую для проверки.

Шаг 3: Проверьте наличие сквозного соединения.

Убедитесь в том, что все устройства могут передавать друг другу эхо-запросы в пределах одной сети VLAN. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

Шаг 4: Проверьте конфигурации на портах.

В настоящее время интерфейсы F0/3, F0/4 и Pol (Port-channel1) на коммутаторах S1 и S3 находятся в режиме доступе, а режим управления установлен на динамический автоматический режим (dynamic auto). Проверьте конфигурацию с помощью соответствующих команд **show run interface** *идентификатор-интерфейса* и **show interfaces** *идентификатор-интерфейса* **switchport.** Для интерфейса F0/3 на S1 отображаются следующие выходные данные конфигурации:

```
S1# show run interface f0/3
Building configuration...

Current configuration : 103 bytes
!
interface FastEthernet0/3
 channel-group 1 mode active

S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Шаг 5: Убедитесь, что порты объединены.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/3(P)    Fa0/4(P)

S3# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/3(P)    Fa0/4(P)
```

Что означают флаги «SU» и «P» в сводных данных по Ethernet?

Вопросы для повторения

Для чего в локальной сети может потребоваться избыточность?

Что может препятствовать образованию каналов EtherChannel?

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				

Практическая работа 8
Настройка базового протокола OSPFv2 для одной области

Топология

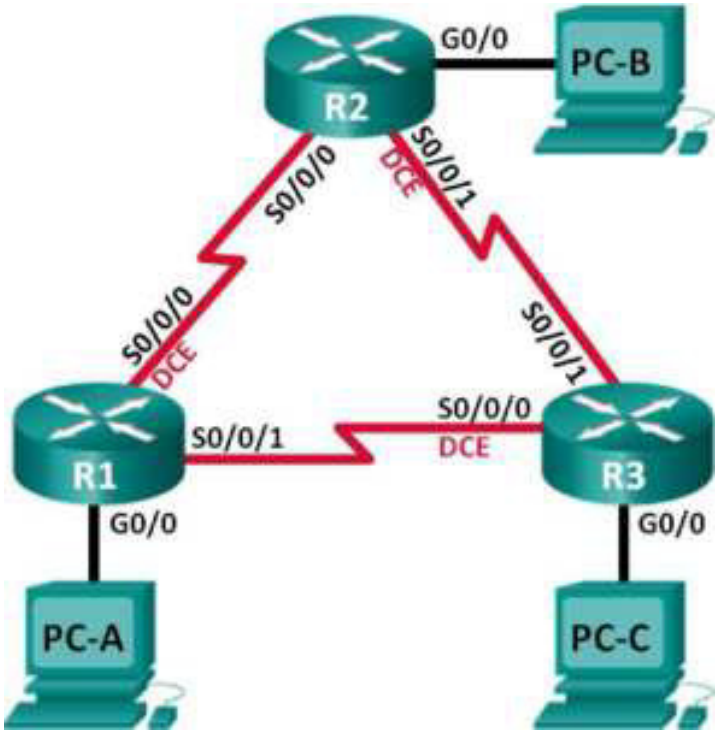


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Настройка и проверка маршрутизации OSPF

Часть 3. Изменение значения ID маршрутизатора

Часть 4. Настройка пассивных интерфейсов OSPF

Часть 5. Изменение метрик OSPF

Исходные данные/сценарий

Алгоритм кратчайшего пути (OSPF) — протокол маршрутизации для IP-сетей на базе состояния канала. Версия OSPFv2 используется для сетей протокола IPv4, а OSPFv3 - для сетей IPv6. OSPF обнаруживает изменения в топологии, например сбой канала, и быстро сходится в новой беспетлевой структуре маршрутизации. OSPF рассчитывает каждый маршрут с помощью алгоритма Дейкстры, т.е. алгоритма кратчайшего пути.

В данной работе необходимо настроить топологию сети с маршрутизацией OSPFv2, изменить значения ID маршрутизатора, настроить пассивные интерфейсы, установить метрики OSPF и использовать несколько команд интерфейса командной строки для вывода и проверки данных маршрутизации OSPF.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части вам предстоит создать топологию сети и настроить основные параметры для узлов и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве паролей консоли и VTY.

e. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

f. Настройте **logging synchronous** для консольного канала.

g. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.

h. Установите значение тактовой частоты на всех последовательных интерфейсах DCE на **128000.**

i. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте узлы ПК.

Шаг 5: Проверка соединения.

Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу, и все ПК должны иметь возможность отправлять успешные эхо-запросы на свои шлюзы по умолчанию. Компьютеры не могут отправлять успешные эхо-запросы на другие ПК, пока не настроена маршрутизация OSPF. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка и проверка маршрутизации OSPF

Во второй части вам предстоит настроить маршрутизацию OSPFv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются верным образом. После проверки OSPF, для повышения уровня безопасности необходимо настроить на каналах аутентификацию протокола OSPF.

Шаг 1: Настройте маршрутизацию OSPF на маршрутизаторе R1.

a. Используйте команду **router ospf** в режиме глобальной конфигурации, чтобы активировать OSPF на маршрутизаторе R1.

```
R1(config)# router ospf 1
```

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

b. Используйте команду **network** для сетей маршрутизатора R1. Используйте идентификатор области, равный 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

Шаг 2: Настройте OSPF на маршрутизаторах R2 и R3.

Используйте команду **router ospf** и добавьте команду **network** для сетей маршрутизаторов R2 и R3. Когда маршрутизация OSPF будет

настроена на R2 и R3, на маршрутизаторе R1 появятся сообщения об установленных отношениях смежности.

```
R1#
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R1#
00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to
FULL, Loading Done
R1#
```

Шаг 3: Проверьте информацию о соседях и маршрутизации OSPF.

a. Используйте команду **show ip ospf neighbor** для проверки списка смежных маршрутизаторов на каждом маршрутизаторе в соответствии с топологией.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2      0   FULL/  -        00:00:33    192.168.13.2    Serial0/0/1
192.168.23.1      0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
```

b. Выполните команду **show ip route,** чтобы убедиться, что в таблицах маршрутизации всех маршрутизаторов отображаются все сети.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1
```

Шаг 4: Проверьте настройки протокола OSPF.

Команда **show ip protocols** обеспечивает быструю проверку критически важных данных конфигурации OSPF. К таким данным относятся идентификатор процесса OSPF, идентификатор маршрутизатора, сети, объявляемые маршрутизатором, соседние устройства, от которых маршрутизатор принимает обновления, и значение административной дистанции по умолчанию, равное 110 для OSPF.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.23.2         110      00:19:16
    192.168.23.1         110      00:20:03
  Distance: (default is 110)
```

Шаг 5: Проверьте данные процесса OSPF.

Используйте команду **show ip ospf,** чтобы просмотреть идентификаторы процесса OSPF и маршрутизатора. Данная команда отображает данные о зоне OSPF и показывает время, когда последний раз выполнялся алгоритм поиска кратчайшего пути SPF.

```
R1# show ip ospf
 Routing Process "ospf 1" with ID 192.168.13.1
 Start time: 00:20:23.260, Time elapsed: 00:25:08.296
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 00:22:53.756 ago
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x019A61
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Шаг 6: Проверьте настройки интерфейса OSPF.

a. Выполните команду **show ip ospf interface brief,** чтобы отобразить сводку об интерфейсах, на которых активирован алгоритм OSPF.

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

```
R1# show ip ospf interface
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

```
    Adjacent with neighbor 192.168.13.1
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Шаг 7: Проверьте наличие сквозного соединения.

Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Изменение значения ID маршрутизатора

Идентификатор OSPF-маршрутизатора используется для уникальной идентификации маршрутизатора в домене маршрутизации OSPF. Маршрутизаторы компании Cisco получают ID маршрутизатора одним из трёх способов в следующем порядке:

1) IP-адрес, установленный с помощью команды OSPF **router-id** (при наличии)

2) Наивысший IP-адрес любого из loopback-адресов маршрутизатора (при наличии)

3) Наивысший активный IP-адрес любого из физических интерфейсов маршрутизатора

Поскольку ни на одном из трёх маршрутизаторов не настроены идентификаторы маршрутизатора или loopback-интерфейсы, идентификатор каждого маршрутизатора определяется наивысшим IP-адресом любого активного интерфейса.

В третьей части вам необходимо изменить значение ID идентификатора OSPF-маршрутизатора с помощью loopback-адресов. Также вам предстоит использовать команду **router-id** для изменения идентификатора маршрутизатора.

Шаг 1: Измените идентификаторы маршрутизатора, используя loopback-адреса.

a. Назначьте IP-адрес loopback 0 для маршрутизатора R1. R1(config)# **interface lo0**

```
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

b. Назначьте IP-адреса loopback 0 для маршрутизаторов R2 и R3. Используйте IP-адрес 2.2.2.2/32 для R2 и 3.3.3.3/32 для R3.

c. Сохраните текущую конфигурацию в загрузочную на всех трёх маршрутизаторах.

d. Для того чтобы идентификатор маршрутизатора получил значение loopback-адреса, необходимо перезагрузить маршрутизаторы. Выполните команду **reload** на всех трёх маршрутизаторах. Нажмите клавишу Enter, чтобы подтвердить перезагрузку.

e. После перезагрузки маршрутизатора выполните команду **show ip protocols,** чтобы просмотреть новый идентификатор маршрутизатора

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:01:00
    2.2.2.2              110      00:01:14
  Distance: (default is 110)
```

f. Выполните **show ip ospf neighbor,** чтобы отобразить изменения идентификатора маршрутизатора для соседних маршрутизаторов.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:35    192.168.13.2    Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:32    192.168.12.2    Serial0/0/0
R1#
```

Шаг 2: Измените идентификатор маршрутизатора R1 с помощью команды router-id.

Наиболее предпочтительным способом изменения ID маршрутизатора осуществляется с помощью

команды router-id.

а. Чтобы переназначить идентификатор маршрутизатора, выполните команду **router-id 11.11.11.11** на маршрутизаторе R1. Обратите внимание на уведомление, которое появляется при выполнении команды **router-id.**

```
R1(config)# router ospf 1
R1(config-router)# router-id 11.11.11.11
Reload or use "clear ip ospf process" command, for this to take effect
```

R1(config)# **end**

b. Вы получите уведомление о том, что для того, чтобы изменения вступили в силу, вам необходимо либо перезагрузить маршрутизатор, либо использовать команду **clear ip ospf process.** Выполните команду **clear ip ospf process** на всех трёх маршрутизаторах. Введите **yes,** чтобы подтвердить сброс, и нажмите клавишу Enter.

c. Для маршрутизатора R2 настройте идентификатор **22.22.22.22,** а для маршрутизатора R3 - идентификатор **33.33.33.33.** Затем используйте команду **clear ip ospf process,** чтобы сбросить процесс маршрутизации OSPF.

d. Выполните команду **show ip protocols,** чтобы проверить изменился ли идентификатор маршрутизатора R1.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    33.33.33.33          110      00:00:19
    22.22.22.22          110      00:00:31
    3.3.3.3              110      00:00:41
    2.2.2.2              110      00:00:41
  Distance: (default is 110)
```

e. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что новые идентификаторы маршрутизаторов R2 и R3 содержатся в списке.

R1# show ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:36    192.168.13.2    Serial0/0/1
22.22.22.22       0   FULL/  -        00:00:32    192.168.12.2    Serial0/0/0
```

Часть 4: Настройка пассивных интерфейсов OSPF

Команда **passive-interface** запрещает отправку обновлений маршрутизации из определённого интерфейса маршрутизатора. В большинстве случаев команда используется для уменьшения трафика в сетях LAN, поскольку им не нужно получать сообщения протокола динамической маршрутизации. В четвёртой части вам предстоит использовать команду **passive-interface** для настройки интерфейса в качестве пассивного. Также вы настроите OSPF таким образом, чтобы все интерфейсы маршрутизатора были пассивными по умолчанию, а затем включите объявления протокола маршрутизации OSPF на выбранных интерфейсах.

Шаг 1: Настройте пассивный интерфейс.

a. Выполните команду **show ip ospf interface g0/0** на маршрутизаторе R1. Обратите внимание на таймер, указывающий время получения очередного пакета приветствия. Пакеты приветствия отправляются каждые 10 секунд и используются маршрутизаторами OSPF для проверки

работоспособности соседних устройств.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

b. Выполните команду **passive-interface**, чтобы интерфейс G0/0 маршрутизатора R1 стал пассивным.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0
```

c. Повторно выполните команду **show ip ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0 стал пассивным.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
```

```
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

d. Выполните команду **show ip route** на маршрутизаторах R2 и R3, чтобы убедиться, что маршр к сети 192.168.1.0/24 по-прежнему доступен.

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
O     192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0
O     192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/30 is directly connected, Serial0/0/0
L        192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O        192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
                      [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.23.0/30 is directly connected, Serial0/0/1
L        192.168.23.1/32 is directly connected, Serial0/0/1
```

Шаг 2: Настройте маршрутизатор так, чтобы все его интерфейсы были пассивными по умолчанию.

а. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что R2 указан в качестве соседа OSPF.

R1# **show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:31    192.168.13.2    Serial0/0/1
22.22.22.22       0   FULL/  -        00:00:32    192.168.12.2    Serial0/0/0
```

b. выполните команду **passive--interface aeTauit** на R2, чтоы по умолчанию настроить все интерфейсы OSPF в качестве пассивных.

```
R2(config)# router ospf 1
R2(config-router)# passive-interface default
R2(config-router)#
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

c. Повторно выполните команду **show ip ospf neighbor** на R1. После истечения таймера простоя маршрутизатор R2 больше не будет указан, как сосед OSPF.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:34    192.168.13.2    Serial0/0/1
```

d. Выполните команду **show ip ospf interface S0/0/0** на маршрутизаторе R2, чтобы просмотреть состояние OSPF интерфейса S0/0/0.

```
R2# show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

e. В случае если все интерфейсы маршрутизатора R2 являются пассивными, маршрутизирующая информация объявляться не будет. В этом

случае маршрутизаторы R1 и R3 больше не должны иметь маршрут к сети 192.168.2.0/24. Это можно проверить с помощью команды **show ip route.**

f. На маршрутизаторе R2 выполните команду **no passive-interface,** чтобы маршрутизатор отправлял и получал обновления маршрутизации OSPF. После ввода этой команды появится уведомление

о том, что на маршрутизаторе R1 были установлены отношения смежности.

```
R2(config)# router ospf 1
R2(config-router)# no passive-interface s0/0/0
R2(config-router)#
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

g. Повторно выполните команды **show ip route** и **show ipv6 ospf neighbor** на маршрутизаторах R1 и R3 и найдите маршрут к сети 192.168.2.0/24.

Какой интерфейс использует R3 для прокладки маршрута к сети 192.168.2.0/24? Чему равна суммарная стоимость для сети 192.168.2.0/24 на R3? Отображается ли маршрутизатор R2 как сосед OSPF на маршрутизаторе R1? Отображается ли маршрутизатор R2 как сосед OSPF на маршрутизаторе R3? Что даёт вам эта информация?

h. Настройте интерфейс S0/0/1 маршрутизатора R2 таким образом, чтобы он мог объявлять маршруты OSPF. Ниже запишите используемые команды.

i. Повторно выполните команду **show ip route** на маршрутизаторе R3.

Какой интерфейс использует R3 для прокладки маршрута к сети 192.168.2.0/24?

Чему равна суммарная стоимость для сети 192.168.2.0/24 на R3? Как она была рассчитана?

Отображается ли маршрутизатор R2 как сосед OSPF для маршрутизатора R3?

Часть 5: Изменение метрик OSPF

В части 3 необходимо изменить метрики OSPF с помощью команд **auto-cost reference-bandwidth, bandwidth** и **ip ospf cost.**

Примечание. В части 1 на всех интерфейсах DCE нужно было установить значение тактовой частоты 128000.

Шаг 1: Измените заданную пропускную способность на маршрутизаторах.

Заданная пропускная способность по умолчанию для OSPF равна 100 Мб/с (скорость Fast Ethernet). Однако скорость каналов в большинстве современных устройств сетевой инфраструктуры превышает 100 Мб/с. Поскольку метрика стоимости OSPF должна быть целым числом, стоимость во всех каналах со скоростью передачи 100 Мб/с и выше равна 1. Вследствие этого интерфейсы Fast Ethernet, Gigabit Ethernet и 10G Ethernet имеют одинаковую стоимость. Поэтому, для правильного использования сетей со скоростью канала более 100 Мб/с, заданную пропускную способность необходимо установить на большее значение.

а. Выполните команду **show interface** на маршрутизаторе R1, чтобы просмотреть значение пропускной способности по умолчанию для интерфейса G0/0.

```
R1# show interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
```

```
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:17:31, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   279 packets output, 89865 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   1 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```

Примечание. Пропускная способность на интерфейсе G0/0 может отличаться от значения, приведённого выше, если интерфейс узла ПК может поддерживать только скорость Fast Ethernet. Если интерфейс узла ПК не поддерживают скорость передачи 1 Гб/с, то пропускная способность, скорее всего, будет отображена как 100000 Кб/с.

b. Выполните команду **show ip route ospf** на R1, чтобы определить маршрут к сети 192.168.3.0/24.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
                      [110/128] via 192.168.12.2, 00:01:08, Serial0/0/0
```

Примечание. Суммарная стоимость маршрута к сети 192.168.3.0/24 от маршрутизатора R1 должна быть равна 65.

c. Выполните команду **show ip ospf interface** на маршрутизаторе R3, чтобы определить стоимость маршрутизации для интерфейса G0/0.

```
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
Topology-MTID    Cost    Disabled    Shutdown      Topology Name
      0           1         no          no            Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

d. Выполните команду **show ip ospf interface s0/0/1** на маршрутизаторе R1, чтобы просмотреть стоимость маршрутизации для интерфейса S0/0/1.

```
R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
```

Как видно из выходных данных команды **show ip route,** сумма метрик стоимости этих двух интерфейсов и суммарная стоимость маршрута к сети 192.168.3.0/24 на маршрутизаторе R3 рассчитывается по формуле 1 + 64 = 65.

e. Выполните команду **auto-cost reference-bandwidth 10000** на маршрутизаторе R1, чтобы изменить параметр заданной пропускной способности по умолчанию. С подобной установкой стоимость интерфейсов 10 Гб/с будет равна 1, стоимость интерфейсов 1 Гбит/с будет равна 10, а стоимость интерфейсов 100 Мб/с будет равна 100.

```
R1(config)# router ospf 1
```

```
R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

f. Выполните команду **auto-cost reference-bandwidth 10000** на маршрутизаторах R2 и R3.

g. Повторно выполните команду **show ip ospf interface,** чтобы просмотреть новую стоимость интерфейса G0/0 на R3 и интерфейса S0/0/1 на R1.

```
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no             Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от отображаемых выходных данных. Например, для скорости Fast Ethernet (100 Мб/с) стоимость будет равна 100.

```
R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          6476      no          no             Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1

                    Adjacent with neighbor 192.168.23.2
                  Suppress hello for 0 neighbor(s)
```

h. Повторно выполните команду **show ip route ospf,** чтобы просмотреть новую суммарную стоимость для маршрута 192.168.3.0/24 (10 + 6476 = 6486).

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от того, что отображается в выходных данных. Например, если интерфейс G0/0 работает на скорости Fast Ethernet (100 Мб/с), то суммарная стоимость будет равна 6576.

```
R1(config)# router ospf 1
R1(config-router)# auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.

R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O     192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
                      [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/
```

Примечание. Изменение заданной пропускной способности по умолчанию на маршрутизаторах с 100 на 10 000 изменяет суммарные стоимости всех маршрутизаторов в 100 раз, но стоимость каждого канала и маршрута интерфейса рассчитывается точнее.

i. Для того чтобы восстановить заданную пропускную способность до значения по умолчанию, на всех трёх маршрутизаторах выполните команду **auto-cost reference-bandwidth 100.**

Для чего имеет смысл изменять заданную пропускную способность OSPF?

Шаг 2: Измените пропускную способность для интерфейса.

На большинстве последовательных каналов метрика пропускной способности имеет значение по умолчанию, равное 1544 Кбит (T1). В случае если реальная скорость последовательного канала другая, то для правильного расчёта стоимости маршрута в OSPF параметр пропускной способности нужно будет изменить, чтобы она была равна фактической скорости. Используйте команду **bandwidth,** чтобы откорректировать значение пропускной способности на интерфейсе.

Примечание. Согласно распространённому заблуждению, команда **bandwidth** может изменить физическую пропускную способность (или скорость) канала. Команда изменяет метрику пропускной способности, используемой алгоритмом OSPF для расчёта стоимости маршрутизации, но **не** изменяет фактическую пропускную способность (скорость) канала.

a. Выполните команду **show interface s0/0/0** на маршрутизаторе R1, чтобы просмотреть установленное значение пропускной способности на интерфейсе S0/0/0. Реальная скорость передачи данных на этом интерфейсе, установленная командой clock rate, составляет 128 Кб/с, при этом установленное значение пропускной способности по-прежнему равно 1544 Кб/с.

```
R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
<Output omitted>
```

b. Выполните команду **show ip route ospf** на маршрутизаторе R1, чтобы просмотреть суммарную стоимость для маршрута к сети 192.168.23.0/24 через интерфейс S0/0/0. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с равной стоимостью (128): один через интерфейс S0/0/0, другой через интерфейс S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
                      [110/128] via 192.168.12.2, 00:00:42, Serial0/0/0
```

c. Выполните команду **bandwidth 128,** чтобы установить на интерфейсе S0/0/0 пропускную способность равную 128 Кб/с.

```
R1(config)# interface s0/0/0
R1(config-if)# bandwidth 128
```

d. Повторно выполните команду **show ip route ospf.** В таблице маршрутизации больше не отображается маршрут к сети 192.168.23.0/24 через интерфейс S0/0/0. Это связано с тем, что оптимальный маршрут с наименьшей стоимостью проложен через S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1
```

e. Выполните **show ip ospf interface brief.** Стоимость для интерфейса S0/0/0 изменилась с 64 на 781, что является более точным представлением стоимости скорости канала.

```
Interface     PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1       1     0               192.168.13.1/30    64    P2P   1/1
Se0/0/0       1     0               192.168.12.1/30    781   P2P   1/1
Gi0/0         1     0               192.168.1.1/24     1     DR    0/0
```

f. Измените пропускную способность для интерфейса S0/0/1 на значение, установленное для интерфейса S0/0/0 маршрутизатора R1.

g. Повторно выполните команду **show ip route ospf,** чтобы просмотреть суммарную стоимость обоих маршрутов к сети 192.168.23.0/24. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с одинаковой стоимостью (845): один через интерфейс S0/0/0, другой через интерфейс S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
                      [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0
```

Объясните, как были рассчитаны стоимости для сетей 192.168.3.0/24 и 192.168.23.0/30 от маршрутизатора R1.

Стоимость маршрута к сети 192.168.3.0/24: R1 S0/0/1 + R3 G0/0 (781+1=782). Стоимость маршрута к сети 192.168.23.0/30: R1 S0/0/1 + R3 S0/0/1 (781+64=845).

h. Выполните команду **show ip route ospf** на R3. Суммарная стоимость сети 192.168.1.0/24 по- прежнему равна 65. В отличие от команды **clock rate,** команду **bandwidth** следует выполнить на каждом конце последовательного канала.

```
R3# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
      192.168.12.0/30 is subnetted, 1 subnets
O        192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
                      [110/128] via 192.168.13.1, 00:30:58, Serial0/0/0
```

i. Выполните команду **bandwidth 128** на всех остальных последовательных интерфейсах в топологии.

Чем равна новая суммарная стоимость для сети 192.168.23.0/24 на R1? Почему?

Шаг 3: Измените стоимость маршрута.

Для расчёта стоимости канала OSPF использует значение, установленное командой bandwidth. Рассчитанную стоимость можно изменить, настроив вручную стоимость канала с помощью команды **ip ospf cost.** Как и команда **bandwidth,** команда **ip ospf cost** действует только на той стороне канала, на которой она была применена.

a. Введите команду **show ip route ospf** на маршрутизаторе R1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O     192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
```

```
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
                      [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0
```

b. Выполните команду **ip ospf cost 1565** на интерфейсе S0/0/1 маршрутизатора R1. Стоимость 1 является выше суммарной стоимости маршрута, проходящего через R2 (1562).

```
R1(config)# int s0/0/1
R1(config-if)# ip ospf cost 1565
```

c. Повторно выполните команду **show ip route ospf** на R1, чтобы отобразить изменения в табли маршрутизации. Теперь все маршруты OSPF для маршрутизатора R1 направляются через маршрутизатор R2.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
O     192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Примечание. Изменение метрик стоимости канала с помощью команды **ip ospf cost** — это наиболее простой и предпочтительный способ изменения стоимости маршрутов OSPF. Помимо изменения стоимости в связи с реальным значением пропускной способности, у сетевого администратора могут быть другие причины для изменения стоимости маршрута, например, известная пропускная способность, предоставляемой оператором связи или фактическая стоимость канала или маршрута.

Почему маршрут к сети 192.168.3.0/24 маршрутизатора R1 теперь проходит через R2?

Вопросы на закрепление

1. Почему так важно контролировать значение ID маршрутизатора при использовании протокола OSPF?

2. Почему процесс выбора DR/BDR не рассматривается в этой лабораторной работе?

3. Почему имеет смысл устанавливать интерфейс OSPF в качестве пассивного?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	**Fast Ethernet 0/0 (F0/0)**	**Fast Ethernet 0/1 (F0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
1900	**Gigabit Ethernet 0/0 (G0/0)**	**Gigabit Ethernet 0/1 (G0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
2801	**Fast Ethernet 0/0 (F0/0)**	**Fast Ethernet 0/1 (F0/1)**	**Serial 0/1/0 (S0/1/0)**	**Serial 0/1/1 (S0/1/1)**
2811	**Fast Ethernet 0/0 (F0/0)**	**Fast Ethernet 0/1 (F0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
2900	**Gigabit Ethernet 0/0 (G0/0)**	**Gigabit Ethernet 0/1 (G0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 9
Настройка OSPFv2 в сети множественного доступа

Топология

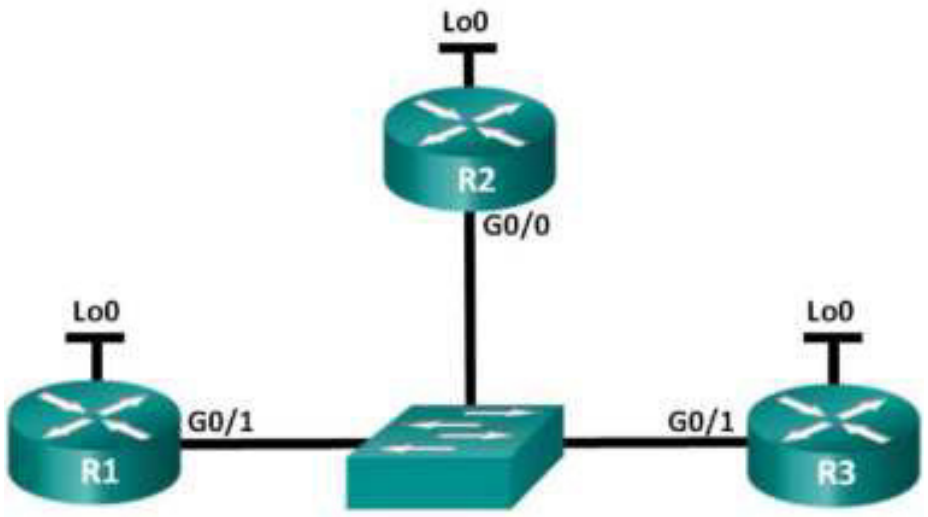


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	G0/1	192.168.1.1	255.255.255.0
	Lo0	192.168.31.11	255.255.255.255
R2	G0/0	192.168.1.2	255.255.255.0
	Lo0	192.168.31.22	255.255.255.255
R3	G0/1	192.168.1.3	255.255.255.0
	Lo0	192.168.31.33	255.255.255.255

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка и проверка OSPFv2 на DR, BDR и DROther

Часть 3. Настройка приоритета интерфейса OSPFv2 для определения DR и BDR

Исходные данные/сценарий

Сеть с множественным доступом — это сеть, содержащая более двух устройств в общей среде передачи данных. К таким сетям относятся Ethernet

и Frame Relay. В сетях с множественным доступом протокол OSPFv2 назначает выделенный маршрутизатор (DR) в качестве точки сбора и распределения отправленных и принятых объявлений о состоянии канала (LSA). На случай отказа выделенного маршрутизатора (DR) также выбирается резервный назначенный маршрутизатор (BDR). Все остальные маршрутизаторы станут маршрутизаторами DROther. Это состояние показывает, что маршрутизатор не является ни DR, ни BDR.

Поскольку DR играет роль центральной точки для сообщений протокола маршрутизации OSPF, выбранный маршрутизатор должен поддерживать больший трафик, чем другие маршрутизаторы сети. На роль DR, как правило, подходит маршрутизатор с мощным ЦП и достаточным объёмом динамической памяти.

В этой лабораторной работе вам предстоит настроить OSPFv2 на маршрутизаторах DR, BDR и DROther. Затем вам необходимо изменить приоритет маршрутизаторов, чтобы повлиять на результаты выбора DR/BDR и обеспечить назначение роли DR нужному маршрутизатору.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена и в них нет начальной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 необходимо настроить топологию сети и выполнить базовые настройки маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с диаграммой топологии и выполните разводку кабелей по необходимости.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

c. Назначьте class в качестве пароля привилегированного режима.

d. Назначьте cisco в качестве паролей консоли и VTY.

e. Зашифруйте пароли.

f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

g. Настройте logging synchronous для консольного канала.

h. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.

i. Выполните команду show ip interface brief, чтобы убедиться в правильности IP-адресации и активности интерфейсов.

j. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Часть 2: Настройка и проверка OSPFv2 на DR, BDR и DROther

В части 2 вам предстоит настроить OSPFv2 на маршрутизаторах DR, BDR и DROther. Процедура выбора DR и BDR начинается сразу после появления в сети с множественным доступом первого маршрутизатора с работающим интерфейсом. Это может случиться после включения питания маршрутизаторов или выполнения команды OSPF network на интерфейсе. Если новый маршрутизатор входит в сеть после выбора маршрутизаторов DR и BDR, он не становится маршрутизатором DR или BDR, даже если приоритет его OSPF-интерфейса или идентификатор маршрутизатора выше, чем у действующих маршрутизаторов DR и BDR. Настройте OSPF-процесс сначала на маршрутизаторе с наивысшим идентификатором, чтобы именно он стал маршрутизатором DR.

Шаг 1: Настройте протокол OSPF на маршрутизаторе R3.

Настройте OSPF-процесс сначала на маршрутизаторе R3 (с наивысшим идентификатором), чтобы именно он стал маршрутизатором DR.

a. Назначьте 1 в качестве идентификатора процесса OSPF. Настройте для маршрутизатора объявление сети 192.168.1.0/24. Для параметра OSPF *area-id* выражения network введите идентификатор области 0.

По какой причине идентификатор маршрутизатора R3 является наивысшим?

b. Убедитесь, что OSPF настроен, а маршрутизатор R3 исполняет роль DR.

Какую команду необходимо выполнить, чтобы убедиться в правильности настройки OSPF и в том, что R3 исполняет роль DR?

Шаг 2: Настройте протокол OSPF на маршрутизаторе R2.

Настройте OSPF-процесс сначала на маршрутизаторе R2 (со вторым по величине значением

идентификатора), чтобы именно он стал маршрутизатором BDR.

a. Назначьте 1 в качестве идентификатора процесса OSPF. Настройте для маршрутизатора объявление сети 192.168.1.0/24. Для

параметра OSPF *area-id* выражения network введите идентификатор области 0.

b. Убедитесь, что OSPF настроен, а маршрутизатор R2 исполняет роль BDR. Запишите команду, используемую для проверки.

c. Выполните команду show ip ospf neighbor для просмотра сведений о других маршрутизаторах в области OSPF.

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.31.33     1   FULL/DR         00:00:33    192.168.1.3     GigabitEthernet0/0
```

Обратите внимание, что R3 является маршрутизатором DR.

Шаг 3: Настройте протокол OSPF на маршрутизаторе R1.

Настройте OSPF-процесс на маршрутизаторе R1 (с самым низким идентификатором). Этот маршрутизатор станет маршрутизатором DROther, а не DR или BDR.

a. Назначьте 1 в качестве идентификатора процесса OSPF. Настройте для маршрутизатора объявление сети 192.168.1.0/24. Для параметра OSPF *area-id* выражения network введите идентификатор области 0.

b. Выполните команду show ip ospf interface brief, чтобы убедиться, что OSPF настроен, а маршрутизатору R1 назначена роль DROther.

```
R1# show ip ospf interface brief
Interface     PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Gi0/1         1     0               192.168.1.1/24     1     DROTH 2/2
```

c. Выполните команду show ip ospf neighbor для просмотра сведений о других маршрутизаторах в области OSPF.

```
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.31.22     1   FULL/BDR        00:00:35    192.168.1.2     GigabitEthern
192.168.31.33     1   FULL/DR         00:00:30    192.168.1.3     GigabitEthern
```

Каким приоритетом обладают оба маршрутизатора, DR и BDR?

Часть 3: Настройка приоритета интерфейса OSPFv2 для определения DR и BDR

В части 3 вам предстоит настроить приоритет интерфейса маршрутизатора для того, чтобы предопределить выбор DR/BDR, перезапустить процесс OSPFv2, а также убедиться в изменении маршрутизаторов DR и BDR. Приоритет интерфейса OSPF является основным параметром при определении ролей маршрутизаторов DR и BDR.

Шаг 1: Для интерфейса G0/1 маршрутизатора R1 настройте приоритет OSPF 255.

Значение 255 — это максимально возможный приоритет интерфейса.

```
R1(config)# interface g0/1
R1(config-if)# ip ospf priority 255
R1(config-if)# end
```

Шаг 2: Для интерфейса G0/1 маршрутизатора R3 настройте приоритет OSPF 100.

```
R3(config)# interface g0/1
R3(config-if)# ip ospf priority 100
R3(config-if)# end
```

Шаг 3: Для интерфейса G0/0 маршрутизатора R2 настройте приоритет OSPF 0.

Маршрутизатор с приоритетом 0 не может участвовать в процессе выбора OSPF, поэтому он не станет ни DR, ни BDR.

```
R2(config)# interface g0/0
R2(config-if)# ip ospf priority 0
R2(config-if)# end
```

Шаг 4: Перезапустите процесс OSPF

a. Используйте команду show ip ospf neighbor для определения DR и BDR.

b. Изменилось ли назначение DR?

Какой маршрутизатор исполняет роль DR? Изменилось ли назначение

BDR? Какой маршрутизатор выполняет роль BDR? Какую роль выполняет маршрутизатор R2?

Объясните немедленные изменения, вызванные командой ip ospf priority.

Примечание. Если назначения DR и BDR не изменились, выполните команду clear ip ospf 1 process на всех маршрутизаторах, чтобы сбросить процессы OSPF и инициировать новый выбор.

Если команда clear ip ospf process не привела к сбросу DR и BDR, то, сохранив текущую конфигурацию как загрузочную, выполните команду reload на всех маршрутизаторах.

c. Выполните команду show ip ospf interface на маршрутизаторах R1 и R3 для проверки заданных приоритетов и статуса DR/BDR маршрутизаторов.

```
R1# show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
  Backup Designated router (ID) 192.168.31.33, Interface address 192.168.1.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.31.22
    Adjacent with neighbor 192.168.31.33  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

R3# show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 192.168.1.3/24, Area 0
  Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 100
  Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
  Backup Designated router (ID) 192.168.31.33, Interface address 192.168.1.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
```

```
Suppress link-local Signal rq (LTS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.31.22
  Adjacent with neighbor 192.168.31.11  (Designated Router)
Suppress hello for 0 neighbor(s)
```

Какой из маршрутизаторов теперь является DR? Какой из маршрутизаторов теперь является BDR?

Важнее ли приоритет интерфейса, чем идентификатор маршрутизатора при определении DR/BDR?

Вопросы на закрепление

1. Перечислите критерии, используемые для определения DR в сети OSPF, в порядке убывания их важности.

2. Что означает приоритет интерфейса 255?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	П оследо вател ьный интерфейс №1	П оследо вател ьный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 10
Настройка расширенных функций OSPFv2

Топология

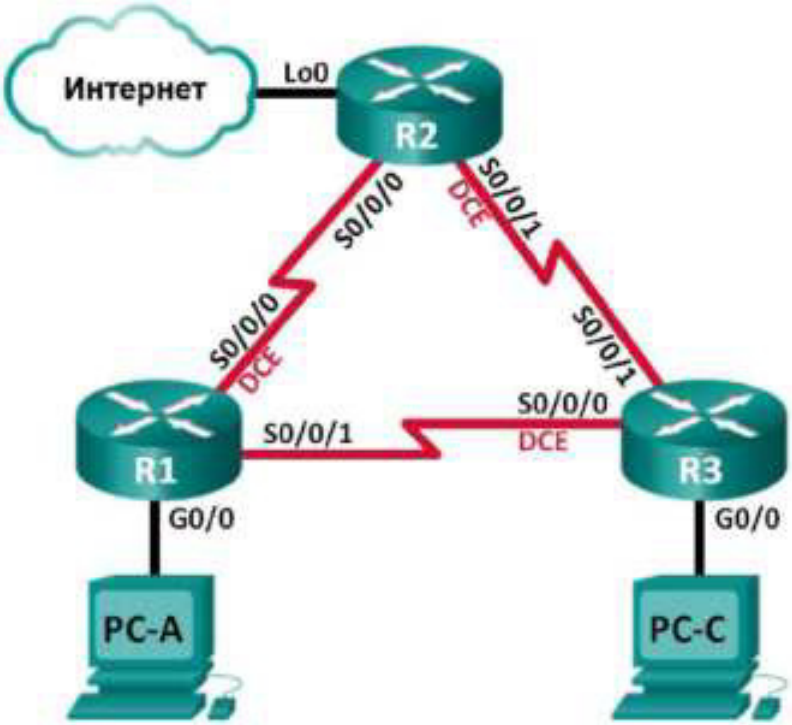


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.252	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть	**1.**	**Создание сети и настройка базовых параметров устройств**
Часть	**2.**	**Настройка и проверка маршрутизации OSPF**
Часть	**3.**	**Изменение метрик OSPF**
Часть	**4.**	**Настройка и распространение статического маршрута по умолчанию**
Часть	**5.**	**Настройка аутентификации на базе протокола OSPF**

Исходные данные/сценарий

У протокола OSPF есть расширенные функции, которые позволяют вносить изменения для управления метриками, распространения маршрута по умолчанию и обеспечения безопасности.

В этой лабораторной работе вам нужно будет настроить метрики OSPF для интерфейсов маршрутизатора, настроить распространение маршрута OSPF и использовать аутентификацию Message Digest 5 (MD5) для обеспечения безопасной маршрутизации OSPF.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.
b. Настройте имя устройств в соответствии с топологией.
c. Назначьте class в качестве пароля привилегированного режима.
d. Назначьте cisco в качестве паролей консоли и VTY.
e. Зашифруйте незашифрованные пароли.
f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
g. Настройте logging synchronous для консольного канала.
h. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.
i. Задайте для тактовой частоты на всех последовательных интерфейсах DCE значение 128000. j. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Шаг 5: Проверьте соединение.

На данный момент ПК не могут отправлять друг другу эхо-запросы. Но маршрутизаторы должны успешно отправлять эхо-запросы непосредственно

подключенным соседним интерфейсам, и все ПК должны успешно отправлять эхо-запросы на свои шлюзы по умолчанию. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка и проверка маршрутизации OSPF

В части 2 вам предстоит настроить маршрутизацию OSPFv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации правильно обновляются.

Шаг 1: Настройте идентификаторы всех маршрутизаторов.

Назначьте 1 в качестве идентификатора процесса OSPF. На каждом маршрутизаторе должны быть настроены следующие идентификаторы:

- Идентификатор маршрутизатора R1: 1.1.1.1
- Идентификатор маршрутизатора R2: 2.2.2.2
- Идентификатор маршрутизатора R3: 3.3.3.3

Шаг 2: Настройте на маршрутизаторах сведения о сети OSPF.

Шаг 3: Проверьте маршрутизацию OSPF.

a. Выполните команду show ip ospf neighbor, чтобы убедиться, что на каждом маршрутизаторе перечислены другие маршрутизаторы в сети.

b. Выполните команду show ip route ospf, чтобы убедиться, что в таблицах маршрутизации всех маршрутизаторов отображаются все сети OSPF.

Шаг 4: Проверьте сквозное подключение.

С узла PC-A отправьте эхо-запрос на узел PC-C, чтобы проверить сквозное подключение. Эхо-запросы должны проходить успешно. В противном случае устраните имеющиеся неполадки.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана ПК.

Часть 3: Изменение метрик OSPF

В части 3 необходимо изменить метрики OSPF с помощью команд auto-cost reference-bandwidth, bandwidth и ip ospf cost. Эти изменения повысят точность метрик для OSPF.

Примечание. В части 1 на всех интерфейсах DCE нужно было установить значение тактовой частоты 128000.

Шаг 1: Для всех последовательных интерфейсов настройте пропускную способность на 128 Кбит/с.

a. Выполните команду show ip ospf interface brief, чтобы просмотреть настройки стоимости по умолчанию для интерфейсов маршрутизатора.

```
R1# show ip ospf interface brief
Interface     PID   Area            IP Address/Mask
Se0/0/1       1     0               192.168.13.1/30
Se0/0/0       1     0               192.168.12.1/30
Gi0/0         1     0               192.168.1.1/24
```

b. Выполните команду bandwidth 128 на всех последовательных интерфейсах.

c. Выполните команду show ip ospf interface brief, чтобы просмотреть новые значения стоимости.

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	192.168.13.1/30	781	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

Шаг 2: Измените заданную пропускную способность для маршрутизаторов.

a. Выполните команду auto-cost reference-bandwidth 1000 на маршрутизаторах, чтобы изменить значение эталонной пропускной способности по умолчанию с целью учета интерфейсов Gigabit Ethernet.

b. Повторно выполните команду show ip ospf interface brief, чтобы просмотреть внесённые изменения значений стоимости.

```
R1# show ip ospf interface brief
Interface      PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1        1     0               192.168.13.1/30    7812  P2P   0/0
Se0/0/0        1     0               192.168.12.1/30    7812  P2P   0/0
Gi0/0          1     0               192.168.1.1/24     1     DR    0/0
```

Cost	State	Nbrs F/C
64	P2P	1/1
64	P2P	1/1
1	DR	0/0

Примечание. Если маршрутизатор оснащен интерфейсами Fast Ethernet вместо интерфейсов Gigabit Ethernet, то значение стоимости для этих интерфейсов будет равно 10.

Шаг 3: Измените стоимость маршрута.

a. Выполните команду show ip route ospf, чтобы просмотреть текущие маршруты OSPF на

маршрутизаторе R1. Обратите внимание, что в настоящее время таблица содержит два маршрута, которые используют интерфейс S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/7822] via 192.168.13.2, 00:00:12, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/15624] via 192.168.13.2, 00:00:12, Serial0/0/1
                      [110/15624] via 192.168.12.2, 00:20:03, Serial0/0/0
```

b. Выполните команду ip ospf cost 16000 на интерфейсе S0/0/1 маршрутизатора R1. Стоимость 16 000 является выше суммарной стоимости маршрута, проходящего через R2 (15 624).

c. Выполните команду show ip ospf interface brief на маршрутизаторе R1, чтобы просмотреть изменение стоимости на интерфейсе S0/0/1.

```
R1# show ip ospf interface brief
Interface     PID   Area          IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1       1     0             192.168.13.1/30    16000 P2P   1/1
Se0/0/0       1     0             192.168.12.1/30    7812  P2P   1/1
Gi0/0         1     0             192.168.1.1/24     1     DR    0/0
```

d. мовюрно выполните команду snow ip louie ospi на R1, ч1 обы просмо1ре1ь влияние этого

изменения на таблицу маршрутизации. Теперь все маршруты OSPF для маршрутизатора R1 проходят через маршрутизатор R2.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/15625] via 192.168.12.2, 00:05:31, Serial0/0/0
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/15624] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Почему маршрут к сети 192.168.3.0/24 от маршрутизатора R1 теперь проходит через R2?

Часть 4: Настройка и распространение статического маршрута по умолчанию

В части 4 вам предстоит использовать интерфейс loopback маршрутизатора R2 для моделирования подключения интернет-провайдера к Интернету. Вы создадите статический маршрут по умолчанию на маршрутизаторе R2, а затем протокол OSPF распространит этот маршрут двум другим маршрутизаторам в сети.

Шаг 1: На маршрутизаторе R2 настройте статический маршрут по умолчанию к интерфейсу loopback 0.

Настройте маршрут по умолчанию, используя интерфейс loopback, настроенный в части 1, чтобы смоделировать подключение к поставщику услуг интернета (ISP).

Шаг 2: Теперь OSPF распространит статический маршрут по умолчанию.

Выполните команду default-information originate, чтобы включить статический маршрут по умолчанию в обновления OSPF, отправляемые маршрутизатором R2.

```
R2(config)# router ospf 1
R2(config-router)# default-information originate
```

Шаг 3: Проверьте распространение статического маршрута OSPF.

a. Выполните команду show ip route static на R2.

]

```
R2# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

c

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback0
```

b. Выполните команду show ip route на маршрутизаторе R1, чтобы проверить распространение статического маршрута от маршрутизатора R2.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.12.2 to network 0.0.0.0
```

```
O*E2  0.0.0.0/0 [110/1] via 192.168.12.2, 00:02:57, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
O     192.168.3.0/24 [110/15634] via 192.168.12.2, 00:03:35, Serial0/0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/30 is directly connected, Serial0/0/0
L        192.168.12.1/32 is directly connected, Serial0/0/0
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/30 is directly connected, Serial0/0/1
L        192.168.13.1/32 is directly connected, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/15624] via 192.168.12.2, 00:05:18, Serial0/0/0
```

c. Проверьте сквозное подключение, отправив эхо-запрос от узла PC-A на адрес интерфейса ISP 209.165.200.225.

Успешно ли выполнен эхо-запрос?

Часть 5: Настройка аутентификации на базе протокола OSPF

Аутентификацию OSPF можно настроить на уровне канала или области. Существует три типа аутентификации OSPF: нулевая, с открытым паролем или по алгоритму MD5. В части 5 вам предстоит настроить аутентификацию MD5 для протокола OSPF, т.е. самый надежный тип аутентификации.

Шаг 1: Настройте аутентификацию MD5 для OSPF на одном канале.

a. Выполните команду debug ip ospf adj на маршрутизаторе R2, чтобы просмотреть сообщения отношений смежности OSPF.

```
R2# debug ip ospf adj
OSPF adjacency debugging is on
```

b. Назначьте ключ MD5 для аутентификации по протоколу OSPF на интерфейсе S0/0/0 маршрутизатора R1.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

c. Активируйте аутентификацию MD5 на интерфейсе S0/0/0 маршрутизатора R1.

```
R1(config-if)# ip ospf authentication message-digest
```

На маршрутизаторе R2 появятся сообщения отладки OSPF, уведомляющие о несовпадении типов аутентификации.

```
*Mar 19 00:03:18.187: OSPF-1 ADJ   Se0/0/0: Rcv pkt from 192.168.12.1 : Mismatched
Authentication type. Input packet specified type 2, we use type 0
```

d. На маршрутизаторе R2 выполните команду u all (самый краткий вариант команды undebug all), чтобы отключить процесс отладки.

e. Настройте аутентификацию OSPF на интерфейсе S0/0/0 маршрутизатора R2. Используйте пароль MD5, введённый для R1.

f. Выполните команду show ip ospf interface s0/0/0 на маршрутизаторе R2. В конце результатов этой команды будет выведен тип аутентификации.

```
R2# show ip ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 2.2.2.2, Network Type POINT_TO_POINT, Cost: 7812
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           7812      no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Шаг 2: Настройте аутентификацию OSPF на уровне области.

a. Выполните команду area 0 authentication, чтобы настроить аутентификацию MD5 для области OSPF 0 на маршрутизаторе R1.

```
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
```

b. Этот вариант требует назначить пароль MD5 на уровне интерфейса.

```
R1(config)# interface s0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

c. Выполните команду show ip ospf neighbor на маршрутизаторе R3. У маршрутизатора R1 теперь отсутствуют отношения смежности с R3.

```
R3# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2         0   FULL/  -        00:00:31    192.168.23.1    Serial0/0/1
```

d. Настройте для маршрутизатора R3 аутентификацию на уровне области и назначьте тот же пароль MD5 для интерфейса S0/0/0.

```
R3(config)# router ospf 1
R3(config-router)# area 0 authentication message-digest
R3(config-router)# interface s0/0/0
R3(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

e. Выполните команду show ip ospf neighbor на маршрутизаторе R3. Обратите внимание, что теперь маршрутизатор R1 показывается в качестве соседнего устройства, а маршрутизатор R2 отсутствует.

R3# show ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:38    192.168.13.1    Serial0/0/0
```

Почему маршрутизатор R2 больше не отображается в качестве соседнего устройства OSPF?

f. На маршрутизаторе R2 настройте аутентификацию MD5 на уровне области.

```
R2(config)# router ospf 1
R2(config-router)# area 0 authentication message-digest
```

g. Назначьте **MD5KEY** в качестве пароля MD5 для канала между маршрутизаторами R2 и R3.

h. Выполните команду **show ip ospf neighbor** на всех маршрутизаторах, чтобы убедиться в восстановлении всех отношений смежности.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/           00:00:39    192.168.13.2    Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:35    192.168.12.2    Serial0/0/0

R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/           00:00:36    192.168.23.2    Serial0/0/1
1.1.1.1           0   FULL/  -        00:00:32    192.168.12.1    Serial0/0/0

R3# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:33    192.168.23.1    Serial0/0/1
1.1.1.1           0   FULL/  -        00:00:39    192.168.13.1    Serial0/0/0
```

Вопросы на закрепление

1. Какой метод управления значениями стоимости маршрута OSPF является наиболее простым и предпочтительным?

2. Каким образом команда default-information originate изменяет работу сети, использующей протокол маршрутизации OSPF?

3. Почему рекомендуется использовать аутентификацию OSPF?

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	П оследо вател ьный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Сводная таблица интерфейсов маршрутизаторов

Практическая работа 11
Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области

Топология

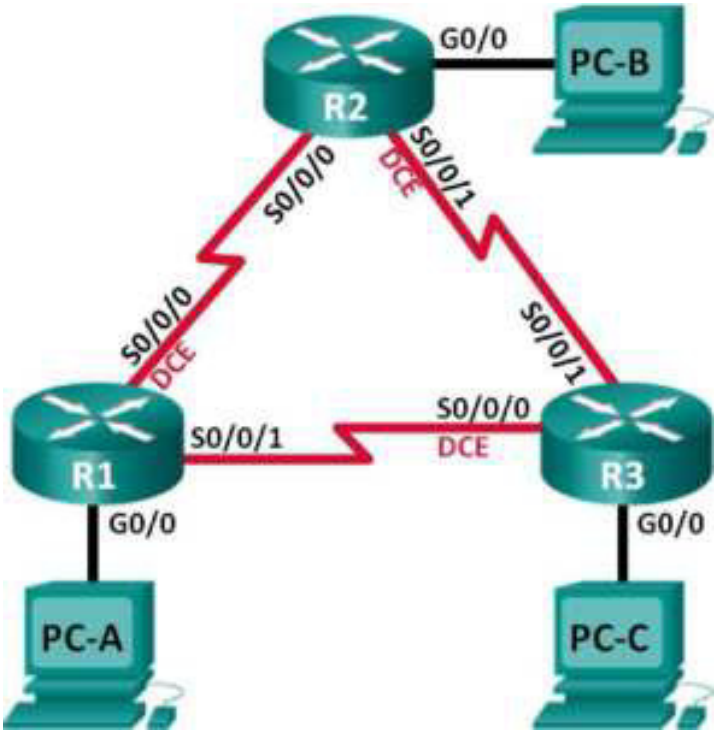


Таблица адресации

Устройство	Идентификатор маршрутизатора OSPF	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	1.1.1.1	G0/0	192.168.1.1/24 2001 :DB8:ACAD:A::1/64 FE80::1 link-local	N/A
		S0/0/0	192.168.12.1/30 2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
		S0/0/1	192.18.13.1/30 2001:DB8:ACAD:13::1/64 FE80::1 link-local	N/A
R2	2.2.2.2	G0/0	192.168.2.1/24 2001 :DB8:ACAD:B::2/64 FE80::2 link-local	N/A
		S0/0/0	192.168.12.2/30 2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
		S0/0/1	192.168.23.1/30 2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	3.3.3.3	G0/0	192.168.3.1/24 2001 :DB8:ACAD:C::3/64 FE80::3 link-local	N/A
		S0/0/0	192.168.13.2/30 2001:DB8:ACAD:13::3/64 FE80::3 link-local	N/A
		S0/0/1	192.168.23.2/30 2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A		NIC	192.168.1.3/24 2001 :DB8:ACAD:A::A/64	192.168.1.1 FE80::1
PC-B		NIC	192.168.2.3/24 2001 :DB8:ACAD:B::B/64	192.168.2.1 FE80::2
PC-C		NIC	192.168.3.3/24 2001 :DB8:ACAD:C::C/64	192.168.3.1 FE80::3

Задачи

Часть 1. Построение сети и загрузка конфигураций устройств Часть 2. Поиск и устранение неполадок подключения уровня 3 Часть 3. Поиск и устранение неполадок в работе OSPFv2 Часть 4. Поиск и устранение неполадок в работе OSPFv3

Исходные данные/сценарий

Алгоритм кратчайшего пути (OSPF) — это протокол маршрутизации для IP-сетей на основе состояния канала. OSPFv2 определен для сетей протокола IPv4, а OSPFv3 — для сетей IPv6. OSPFv2 и OSPFv3 — это полностью изолированные протоколы маршрутизации. Изменения в OSPFv2 не влияют на маршрутизацию OSPFv3, и наоборот.

В этой лабораторной работе в сети OSPF для одной области, использующей протоколы OSPFv2 и OSPFv3, возникли неполадки. Вам поручили найти неполадки в работе сети и устранить их.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и загрузка конфигураций устройств

В части 1 вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите конфигурации маршрутизаторов.

Загрузите следующие конфигурации в соответствующий маршрутизатор. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — **cisco.** Пароль для консоли и доступа vty — **class.**

Конфигурация маршрутизатора R1:

conf t

```
service password-encryption
no ip domain lookup
hostname R1
enable secret class
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 password cisco
 login
banner motd @Unauthorized Access is Prohibited!@
ipv6 unicast-routing
ipv6 router ospf 1
 router-id 1.1.1.1
 passive-interface g0/0
interface g0/0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:db8:acad:a::1/64
 ipv6 address fe80::1 link-local
interface s0/0/0
 clock rate 128000
 ip address 192.168.12.1 255.255.255.0
 ipv6 address 2001:db8:acad:12::1/64
 ipv6 address fe80::1 link-local
 ipv6 ospf 1 area 0
 no shutdown
interface s0/0/1
 ip address 192.168.13.1 255.255.255.0
 ipv6 address 2001:db8:acad:13::1/64
 ipv6 address fe80::1 link-local
 ipv6 ospf 1 area 0
 no shutdown
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
 network 129.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 0.0.0.3 area 0
 passive-interface g0/0
end
```

Конфигурация маршрутизатора R2:

```
conf t
service password-encryption
no ip domain lookup
hostname R2
enable secret class
```

```
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 password cisco
 login
banner motd @Unauthorized Access is Prohibited!@
ipv6 unicast-routing
ipv6 router ospf 1
 router id 2.2.2.2
interface g0/0
ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:db8:acad:B::2/64
 ipv6 address fe80::1 link-local
 no shutdown
interface s0/0/0
 ip address 192.168.12.2 255.255.255.252
 ipv6 address 2001:db8:acad:12::2/64
 ipv6 address fe80::2 link-local
 ipv6 ospf 1 area 0
 no shutdown
interface s0/0/1
 clock rate 128000
 ipv6 address 2001:db8:acad:23::2/64
 ipv6 address fe80::2 link-local
 no shutdown
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
end
```

Конфигурация маршрутизатора R3:

```
conf t
service password-encryption
no ip domain lookup
enable secret class
hostname R3
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 password cisco
 login
```

```
banner motd @Unauthorized Access is Prohibited!@
interface g0/0
 ipv6 address 2001:db8:acad:c::3/64
 ipv6 address fe80::3 link-local
interface s0/0/0
 clock rate 128000
 ip address 192.168.13.1 255.255.255.252
 ipv6 address 2001:db8:acad:13::3/64
 ipv6 address fe80::3 link local
 no shutdown
interface s0/0/1
 ip address 192.168.23.2 255.255.255.252
 ipv6 address 2001:db8:acad:23::3/64
 ipv6 address fe80::3 link-local
router ospf 1
 network 192.168.3.0 0.0.0.255 area 0
 passive interface g0/0
end
```

Часть 2: Поиск и устранение неполадок подключения уровня 3

В части 2 вам предстоит убедиться, что подключение уровня 3 настроено на всех интерфейсах. Для всех интерфейсов устройств понадобится протестировать подключения как для IPv4, так и для IPv6.

Шаг 1: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и что для них настроены правильные IP-адреса.

a. Введите команду show ip interface brief на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up). Запишите полученные результаты.

b. Введите команду show run interface, чтобы проверить назначения IP-адресов на всех интерфейсах маршрутизаторов. Сравните IP-адреса интерфейсов с данными из таблицы адресации и проверьте назначения маски подсети. Убедитесь, что для IPv6 был назначен адрес типа link-local. Запишите полученные результаты.

c. Устраните все обнаруженные неполадки. Запишите команды, используемые для исправления неполадок.

d. Используя команду **ping,** убедитесь, что каждый маршрутизатор сети связан с соседними

маршрутизаторами с помощью последовательных интерфейсов. Убедитесь, что компьютеры могут успешно отправлять эхо-запросы на свои шлюзы по умолчанию. Если проблемы сохраняются, продолжите поиск и устранение проблем на уровне 3.

Часть 3: Поиск и устранение неполадок в работе OSPFv2

В части 3 вам необходимо устранить неполадки OSPFv2 и выполнить изменения, необходимые для настройки маршрутов OSPFv2 и сквозного подключения IPv4.

Примечание. Интерфейсы локальной сети (G0/0) не должны объявлять данные маршрутизации OSPF, но маршруты к этим сетям должны содержаться в таблицах маршрутизации.

Шаг 1: Протестируйте сквозное подключение IPv4.

От каждого ПК отправьте эхо-запросы на другие ПК в топологии, чтобы проверить сквозное подключение.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

a. Отправьте эхо-запрос от узла PC-A на PC-B. Успешно ли выполнен эхо-запрос?

b. Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C. Успешно ли выполнен эхо-запрос?

c. Отправьте эхо-запрос с PC-B на PC-C. Успешно ли выполнен эхо-запрос?

Шаг 2: Убедитесь, что все интерфейсы на маршрутизаторе R1 назначены в область 0 протокола OSPFv2.

a. Введите команду **show ip protocols,** чтобы убедиться в том, что OSPF работает и все сети

анонсируются в области 0. Убедитесь, что идентификатор маршрутизатора настроен правильно. Запишите полученные результаты.

b. Внесите требуемые изменения в конфигурацию маршрутизатора R1, исходя из результатов команды **show ip protocols.** Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ip ospf process.**

d. Повторно введите команду **show ip protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ip ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ip ospf interface g0/0,** чтобы убедиться, что интерфейс G0/0 является пассивным.

Примечание. Эти сведения можно также получить с помощью команды **show ip protocols.**

g. Устраните все неполадки, обнаруженные на маршрутизаторе R1. Укажите все дополнительные изменения, внесённые в конфигурацию R1. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 3: Убедитесь, что все интерфейсы на маршрутизаторе R2 назначены в область 0 протокола OSPFv2.

a. Введите команду **show ip protocols,** чтобы убедиться, что OSPF работает и все сети

анонсируются в области 0. Убедитесь, что идентификатор маршрутизатора настроен правильно. Запишите полученные результаты.

b. Внесите требуемые изменения в конфигурацию маршрутизатора R2, исходя из результатов команды **show ip protocols.** Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ip ospf process.**

d. Повторно введите команду **show ip protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ip ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ip ospf interface g0/0,** чтобы убедиться, что интерфейс G0/0 является пассивным.

Примечание. Эти сведения можно также получить с помощью команды **show ip protocols.**

g. Устраните все неполадки, обнаруженные на маршрутизаторе R2. Укажите все дополнительные изменения, внесённые в конфигурацию R2. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 4: Убедитесь, что все интерфейсы на маршрутизаторе R3 назначены в область 0 протокола OSPFv2.

a. Введите команду **show ip protocols,** чтобы убедиться, что OSPF работает и все сети анонсируются в области 0. Убедитесь, что идентификатор маршрутизатора тоже настроен правильно. Запишите полученные результаты.

b. Внесите требуемые изменения в конфигурацию маршрутизатора R3, исходя из результатов команды **show ip protocols.** Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ip ospf process.**

d. Повторно введите команду **show ip protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ip ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ip ospf interface g0/0,** чтобы убедиться, что интерфейс G0/0 является пассивным.

Примечание. Эти сведения можно также получить с помощью команды **show ip protocols.**

g. Устраните все неполадки, обнаруженные на маршрутизаторе R3. Укажите все дополнительные изменения, внесённые в конфигурацию R3. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 5: Проверьте данные соседнего устройства OSPF.

a. На всех маршрутизаторах введите команду **show ip ospf neighbor,** чтобы просмотреть сведения о соседних устройствах OSPF.

Шаг 6: Проверьте информацию о маршрутах OSPFv2.

a. Введите команду **show ip route ospf,** чтобы убедиться, что каждый маршрутизатор обладает маршрутами OSPFv2 ко всем не граничащим с ним сетям.

Все ли маршруты OSPFv2 доступны?

Если какие-либо маршруты OSPFv2 пропущены, то какие?

b. Если какие-то данные маршрутизации пропущены, исправьте эти неполадки.

Шаг 7: Проверьте сквозное подключение IPv4.

На каждом ПК убедитесь в наличии сквозного подключения IPv4. Компьютеры должны успешно отправлять эхо-запросы на другие ПК в топологии. Если сквозное подключение IPv4 отсутствует, выполняйте поиск и устранение неполадок, пока не будут решены оставшиеся проблемы.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Часть 4: Поиск и устранение неполадок в работе OSPFv3

В части 4 вам необходимо устранить неполадки OSPFv3 и выполнить изменения, необходимые для настройки маршрутов OSPFv3 и сквозного подключения IPv6.

Примечание. Интерфейсы локальной сети (G0/0) не должны объявлять данные маршрутизации OSPFv3, но маршруты к этим сетям должны содержаться в таблицах маршрутизации.

Шаг 1: Протестируйте сквозное подключение IPv6.

С каждого ПК отправьте эхо-запросы на Ру6-адреса других узлов ПК в топологии, чтобы проверить сквозное подключение IPv6.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Шаг 2: Убедитесь, что одноадресная маршрутизация IPv6 включена на всех маршрутизаторах.

a. Простым способом проверки включения ^6-маршрутизации на маршрутизаторе является

использование команды **show run | section ipv6 unicast.** Если добавить вертикальную линию (|) к команде **show run,** то команда **ipv6 unicast-routing** покажет, была ли включена маршрутизация IPv6.

Примечание. Команду **show run** можно выполнить и без вертикальной линии, а затем вручную найти команду **ipv6 unicast-routing.**

Введите эту команду на каждом маршрутизаторе. Запишите полученные результаты.

b. Если одноадресная маршрутизация IPv6 не включена на одном или нескольких маршрутизаторах, включите ее. Запишите команды, используемые для исправления неполадок.

Шаг 3: Убедитесь, что все интерфейсы на маршрутизаторе R1 назначены в область 0 протокола OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь, что идентификатор маршрутизатора настроен правильно. Также убедитесь, что соответствующие интерфейсы отображаются под областью 0.

Примечание. Если у этой команды отсутствует результат, то процесс OSPFv3 не был настроен.

Запишите полученные результаты.

b. Введите необходимые изменения конфигурации для маршрутизатора R1. Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ipv6 ospf process.**

d. Повторно введите команду **show ipv6 protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ipv6 ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ipv6 ospf interface g0/0,** чтобы убедиться, что этот интерфейс не объявляет маршруты OSPFv3.

g. Устраните все неполадки, обнаруженные на маршрутизаторе R1. Укажите все дополнительные изменения, внесённые в конфигурацию R1. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 4: Убедитесь, что все интерфейсы на маршрутизаторе R2 назначены в область 0 протокола OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь, что идентификатор маршрутизатора настроен правильно. Также убедитесь, что соответствующие интерфейсы отображаются под областью 0.

Примечание. Если у этой команды отсутствует результат, то процесс OSPFv3 не был настроен.

Запишите полученные результаты.

b. Введите необходимые изменения конфигурации на маршрутизаторе R2. Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ipv6 ospf process.**

d. Повторно введите команду **show ipv6 protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ipv6 ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ipv6 ospf interface g0/0,** чтобы убедиться, что этот интерфейс не настроен для объявления маршрутов OSPFv3.

g. Укажите все дополнительные изменения, внесённые в конфигурацию R2. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 5: Убедитесь, что все интерфейсы на маршрутизаторе R3 назначены в область 0 протокола OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь, что идентификатор маршрутизатора настроен правильно. Также убедитесь, что соответствующие интерфейсы отображаются под областью 0.

Примечание. Если у этой команды отсутствует результат, то процесс OSPFv3 не был настроен.

Запишите полученные результаты.

b. Выполните необходимые изменения конфигурации на маршрутизаторе R3. Запишите команды, используемые для исправления неполадок.

При необходимости введите команду **clear ipv6 ospf process.**

d. Повторно введите команду **show ipv6 protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ipv6 ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ipv6 ospf interface g0/0,** чтобы убедиться, что этот интерфейс не объявляет маршруты OSPFv3.

g. Устраните все неполадки, обнаруженные на маршрутизаторе R3. Укажите все дополнительные изменения, внесённые в конфигурацию R3. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 6: Убедитесь, что все маршрутизаторы обладают правильной информацией об отношениях смежности с соседними маршрутизаторами.

a. Введите команду **show ipv6 ospf neighbor,** чтобы убедиться в создании отношений смежности между соседними маршрутизаторами.

b. Устраните все оставшиеся неполадки отношений смежности OSPFv3.

Шаг 7: Проверьте информацию о маршрутах OSPFv3.

a. Введите команду **show ipv6 route ospf** и убедитесь в наличии маршрутов OSPFv3 ко всем несмежным сетям.

Все ли маршруты OSPFv3 доступны?

Если какие-то маршруты OSPFv3 отсутствуют, то какие?

b. Устраните все оставшиеся ошибки маршрутизации.

Шаг 8: Проверьте сквозное подключение IPv6.

На каждом ПК убедитесь в наличии сквозного подключения IPv6. Компьютеры должны успешно отправлять эхо-запросы на каждый интерфейс в сети. Если сквозное подключение IPv6 отсутствует, выполняйте поиск и устранение неполадок, пока не будут решены оставшиеся проблемы.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Вопросы на закрепление

Почему следует устранять неполадки в работе OSPFv2 и OSPFv3 по отдельности?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 13

Поиск и устранение неполадок в работе усовершенствованного протокола OSPFv2 для одной области

Топология

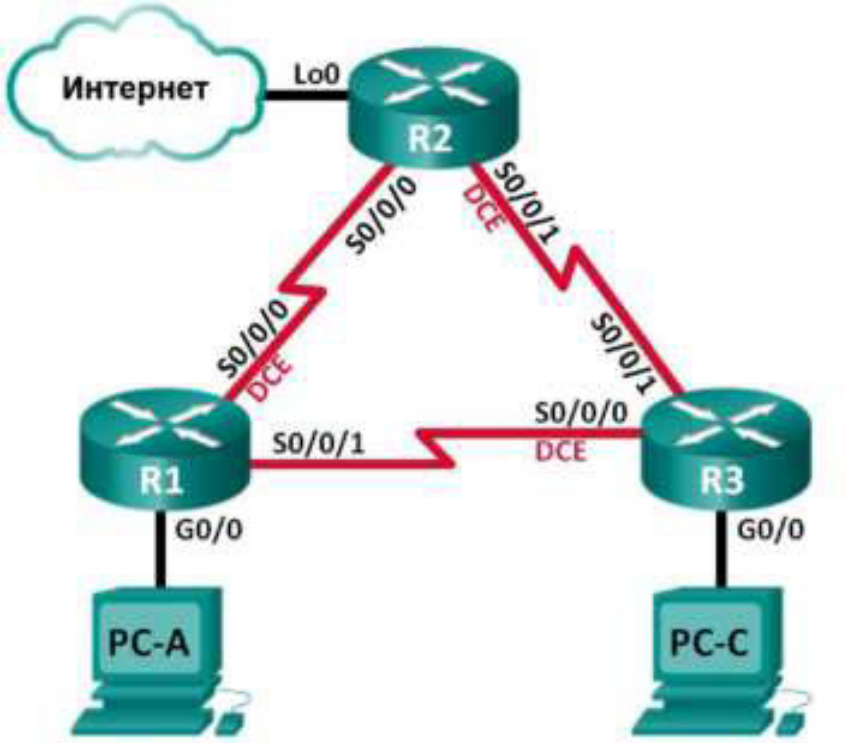


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	**G0/0**	**192.168.1.1**	**255.255.255.0**	**N/A**
	S0/0/0 (DCE)	**192.168.12.1**	**255.255.255.252**	**N/A**
	S0/0/1	**192.168.13.1**	**255.255.255.252**	**N/A**
R2	**Lo0**	**209.165.200.225**	**255.255.255.252**	**N/A**
	S0/0/0	**192.168.12.2**	**255.255.255.252**	**N/A**
	S0/0/1 (DCE)	**192.168.23.1**	**255.255.255.252**	**N/A**
R3	**G0/0**	**192.168.3.1**	**255.255.255.0**	**N/A**
	S0/0/0 (DCE)	**192.168.13.2**	**255.255.255.252**	**N/A**
	S0/0/1	**192.168.23.2**	**255.255.255.252**	**N/A**
PC-A	**NIC**	**192.168.1.3**	**255.255.255.0**	**192.168.1.1**
PC-C	**NIC**	**192.168.3.3**	**255.255.255.0**	**192.168.3.1**

Задачи

Часть 1. Построение сети и загрузка конфигураций устройств Часть 2. Поиск и устранение неполадок в работе OSPF

Исходные данные/сценарий

OSPF — это распространённый протокол маршрутизации, используемый компаниями по всему миру. Сетевой администратор должен уметь выявлять неполадки OSPF и вовремя их устранить.

В этой лабораторной работе вам предстоит найти и устранить неполадки в работе сети OSPFv2 для одной области.

Примечание. **В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.**

Примечание. **Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.**

Необходимые ресурсы:

- **3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);**
- **3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);**
- **консольные кабели для настройки устройств Cisco IOS через порты консоли;**
- **кабели Ethernet и последовательные кабели, как показано в топологии.**

Часть 1: Построение сети и загрузка конфигураций устройств

В части 1 вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите конфигурации маршрутизаторов.

Загрузите следующие конфигурации в соответствующий маршрутизатор. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — class. **Пароль для консоли и каналов vty —** cisco.

Конфигурация маршрутизатора R1:

```
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 no shut
interface Serial0/0/0
 bandwidth 20
 ip address 192.168.2.1 255.255.255.252
 ip ospf message digest key 1 md5 MD5LINK2
 clock rate 125000
 no shut
interface Serial0/0/1
 bandwidth 64
 ip ospf message-digest-key 1 md5 MD5LINK2
 ip address 192.168.3.1 255.255.255.252
 no shut
router ospf 1
 auto-cost reference-bandwidth 100
 area 0 authentication message-digest
 passive-interface g0/0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.3 area 0
banner motd ^
  Unauthorized Access is Prohibited!
```

A

```
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
 transport input all
end
```

Конфигурация маршрутизатора R2:

```
conf t
hostname R2
enable secret class
no ip domain lookup
interface Loopback0
 ip address 209.165.200.225 255.255.255.252
interface Serial0/0/0
 bandwidth 192
 ip ospf message-digest-key 1 md5 MD5LINKS
 ip address 192.168.12.2 255.255.255.252
 no shut
interface Serial0/0/1
 bandwidth 128
 ip ospf message digest key 1 md5 MD5LINKS
 ip address 192.168.23.1 255.255.255.252
 clock rate 128000
 no shut
router ospf 1
 router-id 2.2.2.2
 auto-cost reference-bandwidth 1000
 area 0 authentication message digest
 passive interface g0/0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 Loopback0
banner motd ^
  Unauthorized Access Is Prohibited!
^
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

```
 transport input all
end
```

Конфигурация маршрутизатора R3:

```
enable
configure terminal
hostname R3
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.1
 duplex auto
 speed auto
 no shut
interface Serial0/0/0
 bandwidth 128
 ip ospf message digest key 1 md5 MD5LINK
 ip address 192.168.13.2 255.255.255.252
 clock rate 128000
 no shut
interface Serial0/0/1
 bandwidth 128
 ip address 192.168.23.2 255.255.255.252
 no shut
router ospf 1
 router-id 3.3.3.3
 area 0 authentication message-digest
 passive-interface g0/0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
banner motd ^
  Unauthorized Access is Prohibited!
^
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
 transport input all
end
```

Шаг 4: Проверьте сквозное подключение.

Все интерфейсы должны быть включены, компьютеры должны успешно отправлять эхо-запросы на шлюз по умолчанию.

Часть 2: Поиск и устранение неполадок в работе OSPF

В части 2 вам нужно убедиться, что все маршрутизаторы установили между собой отношения смежности и что все сетевые маршруты доступны.

Дополнительные требования к OSPF

- **На маршрутизаторах должны быть настроены следующие идентификаторы:**
  - **Идентификатор маршрутизатора R1:** 1.1.1.1
  - **Идентификатор маршрутизатора R2:** 2.2.2.2
  - **Идентификатор маршрутизатора R3:** 3.3.3.3
- **Тактовые частоты последовательных интерфейсов должны быть установлены равными 128 Кбит/с. Для правильного расчёта метрики стоимости OSPF должны быть заданы соответствующие значения пропускной способности.**
- **Маршрутизаторы 1941 оснащены интерфейсами Gigabit, поэтому эталонная пропускная способность по умолчанию для OSPF должна быть настроена таким образом, чтобы метрики стоимости отражали соответствующие значения для всех интерфейсов.**
- **OSPF должен распространить маршрут по умолчанию для выхода в Интернет. Для моделирования этого маршрута используется интерфейс loopback 0 на маршрутизаторе R2.**
- **Для всех интерфейсов, объявляющих сведения о маршрутизации OSPF, должна быть настроена аутентификация MD5 с ключом** MD5LINKS.

Перечислите команды, используемые в процессе устранения неполадок в работе OSPF:

Перечислите изменения, выполненные для решения проблем OSPF. Если устройство работает нормально, то напишите, что «проблем не найдено».

Маршрутизатор R1:

Маршрутизатор R2:

Маршрутизатор R3:

Вопросы на закрепление

Как бы вы изменили сеть в этой лабораторной работе, чтобы весь трафик локальной сети проходил через маршрутизатор R2?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**П оследо вател ьный интерфейс №1**	**П оследо вател ьный интерфейс №2**
1800	**Fast Ethernet 0/0 (F0/0)**	**Fast Ethernet 0/1 (F0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
1900	**Gigabit Ethernet 0/0 (G0/0)**	**Gigabit Ethernet 0/1 (G0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
2801	**Fast Ethernet 0/0 (F0/0)**	**Fast Ethernet 0/1 (F0/1)**	**Serial 0/1/0 (S0/1/0)**	**Serial 0/1/1 (S0/1/1)**
2811	**Fast Ethernet 0/0 (F0/0)**	**Fast Ethernet 0/1 (F0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**
2900	**Gigabit Ethernet 0/0 (G0/0)**	**Gigabit Ethernet 0/1 (G0/1)**	**Serial 0/0/0 (S0/0/0)**	**Serial 0/0/1 (S0/0/1)**

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 13
Настройка OSPFv2 для нескольких областей

Топология

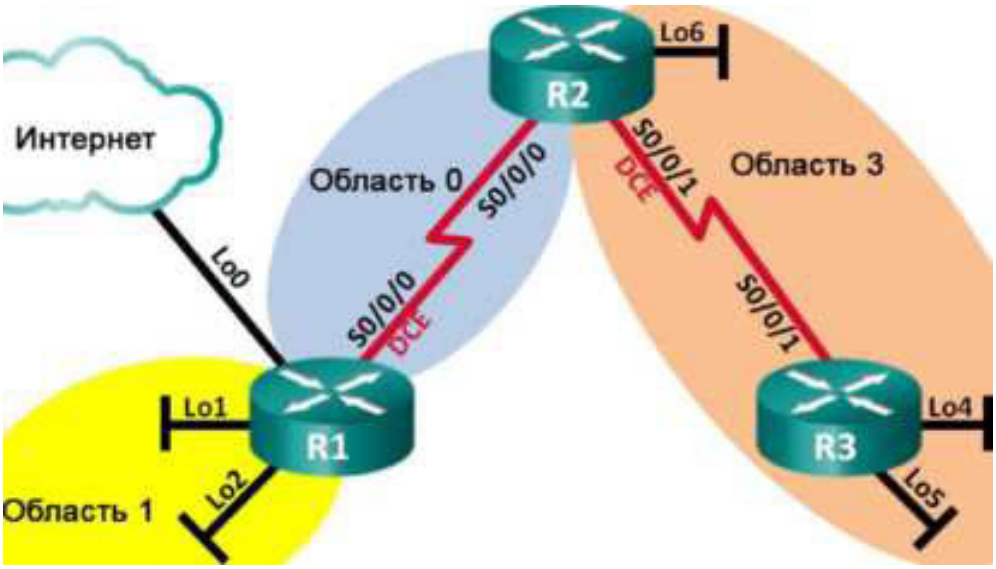


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	Lo0	209.165.200.225	255.255.255.252
	Lo1	192.168.1.1	255.255.255.0
	Lo2	192.168.2.1	255.255.255.0
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252
R2	Lo6	192.168.6.1	255.255.255.0
	S0/0/0	192.168.12.2	255.255.255.252
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252
R3	Lo4	192.168.4.1	255.255.255.0
	Lo5	192.168.5.1	255.255.255.0
	S0/0/1	192.168.23.2	255.255.255.252

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств Часть 2. Настройка сети OSPFv2 для нескольких областей Часть 3. Настройка межобластных суммарных маршрутов

Исходные данные/сценарий

Для улучшения эффективности и масштабируемости в OSPF поддерживается иерархическая маршрутизация, использующая понятие областей. Область OSPF — это группа маршрутизаторов, использующих в своих базах данных состояний каналов (LSDB) общие и одинаковые данные о состоянии каналов. Если большая область OSPF разделена на области меньшего размера, такая архитектура называется OSPF для нескольких областей. Использование OSPF для нескольких областей является целесообразным в сетях большего размера, поскольку это позволяет сократить потребление ресурсов ЦП и памяти.

В этой лабораторной работе будет выполнена настройка сети OSPFv2 для нескольких областей с межобластными суммарными маршрутами.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 необходимо настроить топологию сети и выполнить базовые настройки маршрутизаторов. Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.
b. Задайте имя устройства в соответствии с топологией.
c. Назначьте class в качестве пароля привилегированного режима.
d. Назначьте cisco в качестве паролей консоли и VTY.
e. Настройте logging synchronous для консольного канала.
f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
g. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации. Для интерфейсов оборудования передачи данных (DCE) следует задать тактовую частоту 128000. Пропускную способность для всех последовательных интерфейсов следует установить равной 128 Кбит/с.
h. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Проверьте наличие подключения на уровне 3.

Выполните команду show ip interface brief, чтобы убедиться в правильности IP-адресации и активности интерфейсов. Убедитесь, что каждый маршрутизатор может успешно отправлять эхо- запросы соседним

маршрутизаторам, подключенным с помощью последовательных интерфейсов.

Часть 2: Настройка сети OSPFv2 для нескольких областей

В части 2 необходимо настроить сеть OSPFv2 для нескольких областей, используя идентификатор процесса 1. Все интерфейсы loopback локальной сети должны быть пассивными, а для всех последовательных интерфейсов должна быть настроена аутентификация MD5 с ключом Cisco123.

Шаг 1: Определите типы маршрутизаторов OSPF в топологии.

Определите магистральный маршрутизатор (маршрутизаторы):

Определите пограничный маршрутизатор (маршрутизаторы) автономной системы (ASBR): Определите пограничный маршрутизатор (маршрутизаторы) области (ABR): Определите внутренний маршрутизатор (маршрутизаторы):

Шаг 2: Настройте протокол OSPF на маршрутизаторе R1.

a. Настройте идентификатор маршрутизатора 1.1.1.1 с идентификатором процесса OSPF 1.

b. Добавьте OSPF для сетей маршрутизатора R1.

```
R(config-router)# network 192.168.1.0 0.0.0.255 area 1
R(config-router)# network 192.168.2.0 0.0.0.255 area 1
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

c. Настройте все интерфейсы loopback локальной сети, Lo1 и Lo2, как пассивные.

d. Создайте маршрут по умолчанию к сети Интернет, используя выходной интерфейс Lo0.

Примечание. Может появиться сообщение «%Default route without gateway, if not a point-to-point interface, may impact performance» (%Маршрут по умолчанию без шлюза, если интерфейс не является интерфейсом «точка-точка», может ухудшить производительность). Это нормально, если для моделирования маршрута по умолчанию используется интерфейс loopback.

e. Настройте для протокола OSPF распространение маршрутов в областях OSPF.

Шаг 3: Настройте протокол OSPF на маршрутизаторе R2.

a. Настройте идентификатор маршрутизатора 2.2.2.2 с идентификатором процесса OSPF 1.

b. Добавьте OSPF для сетей маршрутизатора R2. Добавьте сети в соответствующую область. Запишите использованные команды в поле ниже.

c. Настройте все интерфейсы loopback локальных сетей как пассивные.

Шаг 4: Настройте протокол OSPF на маршрутизаторе R3.

a. Настройте идентификатор маршрутизатора 3.3.3.3 с идентификатором процесса OSPF 1.

b. Добавьте OSPF для сетей маршрутизатора R3. Запишите использованные команды в поле ниже.

c. Настройте все интерфейсы loopback локальных сетей как пассивные.

Шаг 5: Убедитесь в правильности настройки протокола OSPF и в установлении отношений смежности между маршрутизаторами.

a. Введите команду **show ip protocols,** чтобы проверить параметры OSPF на каждом

маршрутизаторе. Используйте эту команду, чтобы определить типы маршрутизаторов OSPF и сети, назначенные каждой области.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an area border and autonomous system boundary router
 Redistributing External Routes from,
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 1
    192.168.2.0 0.0.0.255 area 1
    192.168.12.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback1
    Loopback2
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2              110      00:01:45
  Distance: (default is 110)
R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.6.0 0.0.0.255 area 3
    192.168.12.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 3
```

```
  Passive Interface(s):
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:01:20
    1.1.1.1              110      00:10:12
  Distance: (default is 110)
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.4.0 0.0.0.255 area 3
    192.168.5.0 0.0.0.255 area 3
    192.168.23.0 0.0.0.3 area 3
  Passive Interface(s):
    Loopback4
    Loopback5
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:07:46
    2.2.2.2              110      00:07:46
  Distance: (default is 110)
```

К какому типу маршрутизаторов OSPF относится каждый маршрутизатор?

R1:

R2:

R3:

b. Введите команду **show ip ospf neighbor,** чтобы убедиться в

]

```
Neighbor ID     Pri   State           Dead Time   Address         Interfac
2.2.2.2           0   FULL/  -        00:00:38    192.168.23.1    Serial0/
```

интерс

c. Для отображения суммарной стоимости маршрута используйте сокращенную команд ospf interface.

```
R1# show ip ospf interface brief
Interface     PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/0       1     0               192.168.12.1/30    781   P2P   1/1
Lo1           1     1               192.168.1.1/24     1     LOOP  0/0
Lo2           1     1               192.168.2.1/24     1     LOOP  0/0

R2# show ip ospf interface brief
Interface     PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/0       1     0               192.168.12.2/30    781   P2P   1/1
Lo6           1     3               192.168.6.1/24     1     LOOP  0/0
Se0/0/1       1     3               192.168.23.1/30    781   P2P   1/1

R3# show ip ospf interface brief
Interface     PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo4           1     3               192.168.4.1/24     1     LOOP  0/0
Lo5           1     3               192.168.5.1/24     1     LOOP  0/0
Se0/0/1       1     3               192.168.23.2/30    781   P2P   1/1
```

Шаг 6: Настройте аутентификацию MD5 для всех последовательных интерфей

установлении отношений смежности OSPF между маршрутизаторами.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:34    192.168.12.2    Serial0/0

R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:36    192.168.12.1    Serial0/0
3.3.3.3           0   FULL/  -        00:00:36    192.168.23.2    Serial0/0

R3# show ip ospf neighbor
```

Настройте аутентификацию MD5 для OSPF на уровне интерфейса с ключом аутентификации Cisco123. Почему перед настройкой аутентификации OSPF полезно проверить правильность работы OSPF?

Шаг 7: Проверьте восстановление отношений смежности OSPF.

Снова введите команду show ip ospf neighbor, чтобы убедиться в восстановлении отношений смежности OSPF между маршрутизаторами

после реализации аутентификации MD5. Прежде чем перейти к части 3, устраните все найденные ошибки.

Часть 3: Настройка межобластных суммарных маршрутов

OSPF не выполняет автоматическое суммирование. Суммирование межобластных маршрутов необходимо вручную настроить на маршрутизаторах ABR. В части 3 необходимо настроить на маршрутизаторах ABR суммарные межобластные маршруты. С помощью команд show можно будет наблюдать, каким образом суммирование влияет на таблицу маршрутизации и базы данных LSDB.

Шаг 1: Просмотрите таблицы маршрутизации OSPF для всех маршрутизаторов.

a. Введите команду show ip route ospf на маршрутизаторе R1. Для маршрутов OSPF, начинающихся в другой области, используется дескриптор (O IA), обозначающий межобластные маршруты.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

      192.168.4.0/32 is subnetted, 1 subnets
O IA     192.168.4.1 [110/1563] via 192.168.12.2, 00:23:49, Serial0/0/0
      192.168.5.0/32 is subnetted, 1 subnets
O IA     192.168.5.1 [110/1563] via 192.168.12.2, 00:23:49, Serial0/0/0
      192.168.23.0/30 is subnetted, 1 subnets
O IA     192.168.6.1 [110/782] via 192.168.12.2, 00:02:01, Serial0/0/0
      192.168.23.0/30 is subnetted, 1 subnets
O IA     192.168.23.0 [110/1562] via 192.168.12.2, 00:23:49, Serial0/0/0
```

b. Повторите команду show ip route ospf для маршрутизаторов R2 и R3. Запишите межобластные маршруты OSPF для каждого маршрутизатора.

R2:

R3:

Шаг 2: Просмотрите базы данных LSDB на всех маршрутизаторах.

a. Введите команду show ip ospf database на маршрутизаторе R1. Маршрутизатор ведет отдельную базу данных LSDB для каждой области, участником которой является этот маршрутизатор.

```
R1# show ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1295        0x80000003 0x0039CD 2
2.2.2.2         2.2.2.2         1282        0x80000002 0x00D430 2

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.1     1.1.1.1         1387        0x80000002 0x00AC1F
```

```
192.168.2.1     1.1.1.1         1387        0x80000002 0x00A129
192.168.4.1     2.2.2.2         761         0x80000001 0x000DA8
192.168.5.1     2.2.2.2         751         0x80000001 0x0002B2
192.168.6.1     2.2.2.2         1263        0x80000001 0x00596A
192.168.23.0    2.2.2.2         1273        0x80000001 0x00297E

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1342        0x80000006 0x0094A4 2

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.4.1     1.1.1.1         760         0x80000001 0x00C8E0
192.168.5.1     1.1.1.1         750         0x80000001 0x00BDEA
192.168.6.1     1.1.1.1         1262        0x80000001 0x0015A2
192.168.12.0    1.1.1.1         1387        0x80000001 0x00C0F5
192.168.23.0    1.1.1.1         1272        0x80000001 0x00E4B6

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         1343        0x80000001 0x001D91 1
```

b. Повторите команду **show ip route database** для маршрутизаторов R2 и R3. Запишите

идентификаторы каналов (Link ID) для состояний суммарных сетевых каналов (Summary Net Link State) каждой области.

R2:

R3:

Шаг 3: Настройте межобластные суммарные маршруты.

a. Рассчитайте суммарный маршрут для сетей в области 1.

b. Настройте суммарный маршрут для области 1 на маршрутизаторе R1.

```
R1(config)# router ospf 1
R1(config-router)# area 1 range 192.168.0.0 255.255.252.0
```

c. Рассчитайте суммарный маршрут для сетей в области 3. Запишите результаты.

d. Настройте суммарный маршрут для области 3 на маршрутизаторе R2. Запишите использованные команды в отведённой ниже области.

Шаг 4: Повторно отобразите таблицы маршрутизации OSPF для всех маршрутизаторов.

Выполните команду show ip route ospf на каждом маршрутизаторе. Запишите результаты для суммарных и межобластных маршрутов.

R1: R2: R3:

Шаг 5: Просмотрите базы данных LSDB на всех маршрутизаторах.

Выполните команду show ip route database на каждом маршрутизаторе. Запишите идентификаторы каналов (Link ID) для состояний суммарных сетевых каналов (Summary Net Link State) каждой области.

R1: R2: R3:

Пакет LSA какого типа передается в магистраль маршрутизатором ABR, когда включено суммирование межобластных маршрутов?

Шаг 6: Проверьте сквозное подключение.

Убедитесь в доступности всех сетей с каждого маршрутизатора. При необходимости выполните поиск и устранение неполадок.

Вопросы на закрепление

Какие три преимущества при проектировании сети предоставляет OSPF для нескольких областей?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	П оследо вател ьный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 14
Настройка OSPFv3 для нескольких областей

Топология

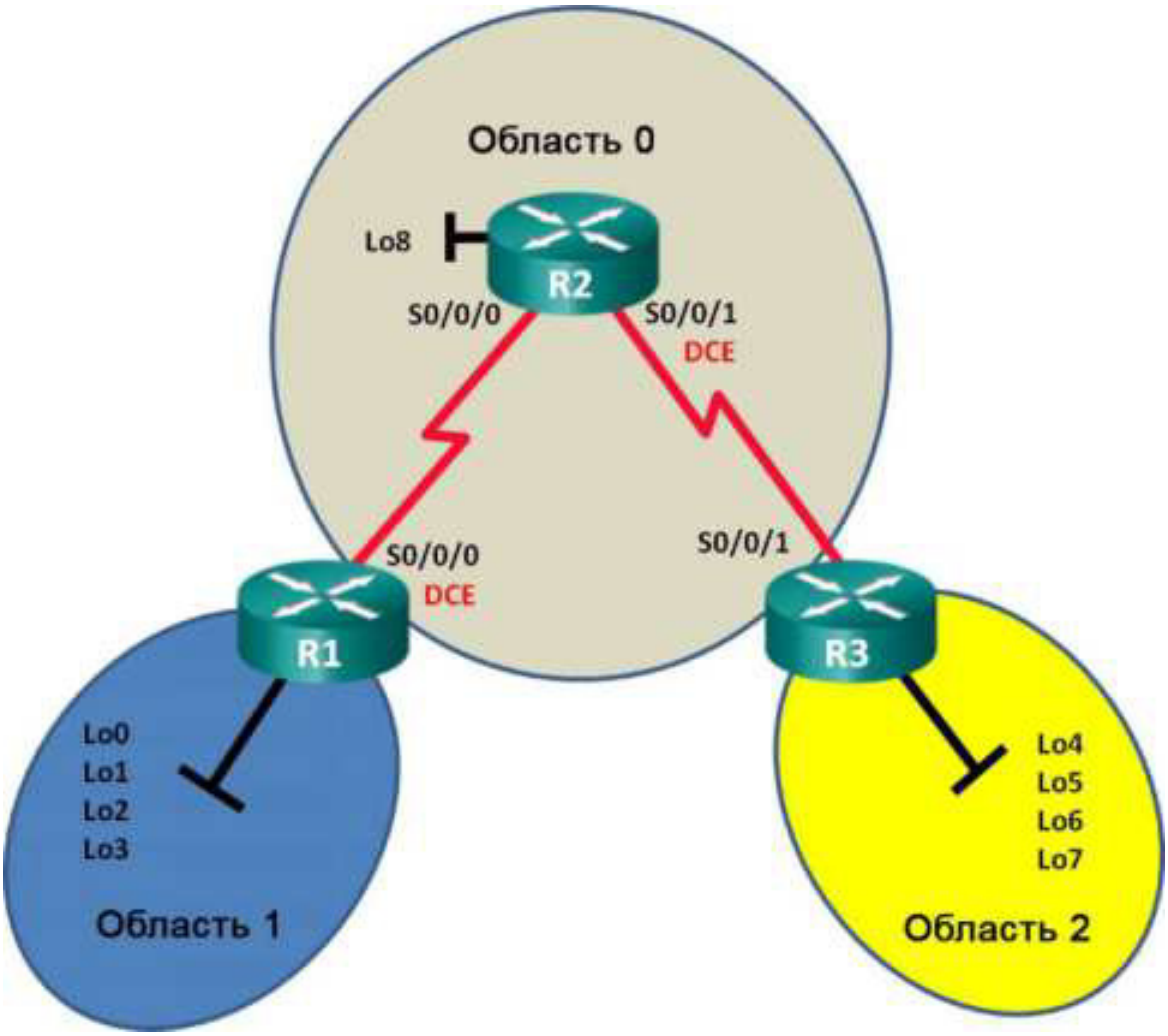


Таблица адресации

Устройство	Интерфейс	^6-адрес	Шлюз по умолчанию
R1	S0/0/0 (DCE)	2001 :DB8:ACAD:12::1/64 FE80::1 link-local	N/A
	Lo0	2001 :DB8:ACAD::1/64	N/A
	Lo1	2001 :DB8:ACAD:1::1/64	N/A
	Lo2	2001 :DB8:ACAD:2::1/64	N/A
	Lo3	2001 :DB8:ACAD:3::1/64	N/A
R2	S0/0/0	2001 :DB8:ACAD:12::2/64 FE80::2 link-local	N/A
	S0/0/1 (DCE)	2001 :DB8:ACAD:23::2/64 FE80::2 link-local	N/A
	Lo8	2001 :DB8:ACAD:8::1/64	N/A
R3	S0/0/1	2001 :DB8:ACAD:23::3/64 FE80::3 link-local	N/A
	Lo4	2001 :DB8:ACAD:4::1/64	N/A
	Lo5	2001 :DB8:ACAD:5::1/64	N/A
	Lo6	2001 :DB8:ACAD:6::1/64	N/A
	Lo7	2001 :DB8:ACAD:7::1/64	N/A

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка маршрутизации с использованием протокола OSPFv3 для нескольких областей

Часть 3. Настройка суммирования межобластных маршрутов

Исходные данные/сценарий

Использование OSPFv3 для нескольких областей в крупных сетях на основе протокола IPv6 может снизить нагрузку на маршрутизатор благодаря уменьшению размера таблиц маршрутизации и снижению требований к

памяти. В OSPFv3 для нескольких областей все области подключены к магистральной области (область 0) с помощью пограничных маршрутизаторов области (ABR).

В этой лабораторной работе необходимо реализовать маршрутизацию OSPFv3 для нескольких областей и настроить на пограничных маршрутизаторах области (ABR) суммирование межобластных маршрутов. Также понадобится использовать ряд команд **show** для вывода на экран и проверки данных маршрутизации OSPFv3. В этой лабораторной работе для моделирования сети в нескольких областях OSPFv3 используются loopback-адреса.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS

доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов см. в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 необходимо настроить топологию сети и выполнить базовые настройки маршрутизаторов. Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Настройте имя устройств в соответствии с топологией.

c. Назначьте **class** в качестве пароля привилегированного режима.

d. Установите **cisco** в качестве пароля vty.

e. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

f. Настройте **logging synchronous** для консольного канала.

g. Зашифруйте все незашифрованные пароли.

h. Настройте для всех интерфейсов индивидуальные адреса и link-local адреса IPv6 каналов, приведённые в таблице адресации.

i. Включите маршрутизацию для индивидуальной адресации IPv6 на каждом маршрутизаторе. j. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Проверьте соединение.

Маршрутизаторы должны успешно отправлять эхо-запросы друг другу. Пока маршрутизация OSPFv3 не настроена, маршрутизаторы не смогут отправлять эхо-запросы к удалённым интерфейсам loopback. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка маршрутизации OSPFv3 для нескольких областей

В части 2 необходимо настроить маршрутизацию OSPFv3 на всех маршрутизаторах, чтобы разделить

домен сети на три отдельных области, а затем проверить правильность обновления таблицы

маршрутизации.

Шаг 1: Назначьте идентификаторы маршрутизаторов.

a. На маршрутизаторе R1 введите команду **ipv6 router ospf**, чтобы запустить на маршрутизаторе процесс OSPFv3.

```
R1(config)# ipv6 router ospf 1
```

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

b. Назначьте маршрутизатору R1 идентификатор маршрутизатора OSPFv3 **1.1.1.1.**

```
R1(config-rtr)# router-id 1.1.1.1
```

c. Задайте для маршрутизатора R2 идентификатор **2.2.2.2**, а для маршрутизатора R3 — идентификатор **3.3.3.3.**

d. Выполните команду **show ipv6 ospf**, чтобы проверить для всех маршрутизаторов идентификаторы OSPF.

```
R2# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 2.2.2.2
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 <Данные опущены>
```

Шаг 2: Настройте OSPFv3 для нескольких областей.

a. Выполните команду **ipv6 ospf 1 area** *идентификатор-области* для каждого интерфейса

маршрутизатора R1, участвующего в маршрутизации OSPFv3. Интерфейсы loopback назначены области 1, а последовательный интерфейс

назначен области 0. Чтобы обеспечить объявление правильной подсети, нужно будет изменить тип сети для интерфейсов loopback.

```
R1(config)# interface lo0
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface lo1
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface lo2
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface lo3
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# ipv6 ospf network point-to-point
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 ospf 1 area 0
```

b. Чтобы проверить состояние OSPFv3 для нескольких областей, используйте команду **show ipv6 protocols.**

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Router ID 1.1.1.1
  Area border router
  Number of areas: 2 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/0
  Interfaces (Area 1):
    Loopback0
    Loopback1
    Loopback2
    Loopback3
  Redistribution:
    None
```

c. Назначьте все интерфейсы маршрутизатора R2 для участия в области 0 OSPFv3. Для интерфейса loopback измените тип сети на «точка-точка». Запишите использованные команды в поле ниже.

d. Используйте команду **show ipv6 ospf interface brief**, чтобы просмотреть, для каких интерфейсов включена поддержка OSPFv3.

Interface	PID	Area	Intf ID	Cost	State	Nbrs F/C
Lo8	1	0	13	1	P2P	0/0
Se0/0/1	1	0	7	64	P2P	1/1
Se0/0/0	1	0	6	64	P2P	1/1

e. Назначьте интерфейсы loopback маршрутизатора R3 для участия в области 2 OSPFv3 и измените тип сети на «точка-точка». Назначьте последовательный интерфейс для участия в области 0 OSPFv3. Запишите использованные команды в поле ниже.

f. Используйте команду **show ipv6 ospf** для проверки конфигураций.

```
R3# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 3.3.3.3
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an area border router
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 RFC1583 compatibility enabled
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        SPF algorithm executed 2 times
        Number of LSA 16. Checksum Sum 0x0929F8
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 2
        Number of interfaces in this area is 4
        SPF algorithm executed 2 times
        Number of LSA 13. Checksum Sum 0x048E3C
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Шаг 3: Проверьте соседние маршрутизаторы OSPFv3 и данные маршрутизации.

a. Введите команду **show ipv6 ospf neighbor** на всех маршрутизаторах, чтобы убедиться в том, что для каждого маршрутизатора в качестве соседей перечислены соответствующие маршрутизаторы.

```
R1# show ipv6 ospf neighbor

            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:39    6               Serial0/0/0
```

D. Введите команду **show ipv6 route ospT** на всех маршрутизаторах, чтобы убедиться в том, что каждому маршрутизатору известны маршруты ко всем сетям таблицы адресации.

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 16 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, M - MNRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCR - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:DB8:ACAD:4::/64 [110/129]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:5::/64 [110/129]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:6::/64 [110/129]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:7::/64 [110/129]
     via FE80::2, Serial0/0/0
O   2001:DB8:ACAD:8::/64 [110/65]
     via FE80::2, Serial0/0/0
O   2001:DB8:ACAD:23::/64 [110/128]
     via FE80::2, Serial0/0/0
```

Что означает метка OI для маршрута?

c. Введите на всех маршрутизаторах команду **show ipv6 ospf database**.

```
R1# show ipv6 ospf database

            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

ADV Router       Age         Seq#        Fragment ID  Link count  Bits
 1.1.1.1         908         0x80000001  0            1           B
 2.2.2.2         898         0x80000003  0            2           None
 3.3.3.3         899         0x80000001  0            1           B

                Inter Area Prefix Link States (Area 0)

ADV Router       Age         Seq#        Prefix
 1.1.1.1         907         0x80000001  2001:DB8:ACAD::/62
 3.3.3.3         898         0x80000001  2001:DB8:ACAD:4::/62

                Link (Type-8) Link States (Area 0)

ADV Router       Age         Seq#        Link ID     Interface
 1.1.1.1         908         0x80000001  6           Se0/0/0
 2.2.2.2         909         0x80000002  6           Se0/0/0
```

```
                Intra Area Prefix Link States (Area 0)

ADV Router      Age         Seq#        Link ID    Ref-lstype  Ref-LSID
 1.1.1.1        908         0x80000001  0          0x2001      0
 2.2.2.2        898         0x80000003  0          0x2001      0
 3.3.3.3        899         0x80000001  0          0x2001      0

                Router Link States (Area 1)

ADV Router      Age         Seq#        Fragment ID  Link count  Bits
 1.1.1.1        908         0x80000001  0            0           B

                Inter Area Prefix Link States (Area 1)

ADV Router      Age         Seq#        Prefix
 1.1.1.1        907         0x80000001  2001:DB8:ACAD:12::/64
 1.1.1.1        907         0x80000001  2001:DB8:ACAD:8::/64
 1.1.1.1        888         0x80000001  2001:DB8:ACAD:23::/64
 1.1.1.1        888         0x80000001  2001:DB8:ACAD:4::/62

                Link (Type-8) Link States (Area 1)

ADV Router      Age         Seq#        Link ID    Interface
 1.1.1.1        908         0x80000001  13         Lo0
 1.1.1.1        908         0x80000001  14         Lo1
 1.1.1.1        908         0x80000001  15         Lo2
 1.1.1.1        908         0x80000001  16         Lo3


               Intra Area Prefix Link States (Area 1)

ADV Router      Age         Seq#        Link ID    Ref-lstype  Ref-LSID
 1.1.1.1        908         0x80000001  0          0x2001      0
```

Сколько баз данных состояния каналов содержит маршрутизатор R1? Сколько баз данных состояния каналов содержит маршрутизатор R2? Сколько баз данных состояния каналов содержит маршрутизатор R3?

Часть 3: Настройка суммирования межобластных маршрутов

В части 3 необходимо вручную настроить суммирование межобластных маршрутов на маршрутизаторах ABR.

Шаг 1: Выполните объединение сетей на маршрутизаторе R1.

а. Выведите список сетевых адресов интерфейсов loopback и определите раздел гекстета, в котором адреса различаются.

2001 :DB8:ACAD:0000::1/64

2001 :DB8:ACAD:0001 ::1/64

2001 :DB8:ACAD:0002::1/64

2001:DB8:ACAD:0003::1/64

b. Перекодируйте различающиеся части из шестнадцатеричного в двоичный код.

2001:DB8:ACAD: 0000 0000 0000 0000::1/64

2001:DB8:ACAD: 0000 0000 0000 0001::1/64

2001:DB8:ACAD: 0000 0000 0000 0010::1/64

2001:DB8:ACAD: 0000 0000 0000 0011::1/64

c. Подсчитайте число крайних слева совпадающих битов для определения префикса объединённого маршрута.

2001:DB8:ACAD: 0000 0000 0000 0000::1/64

2001:DB8:ACAD: 0000 0000 0000 0001::1/64

2001:DB8:ACAD: 0000 0000 0000 0010::1/64

2001:DB8:ACAD: 0000 0000 0000 0011::1/64

Сколько битов совпадает?

d. Скопируйте совпадающие биты и добавьте нулевые биты, чтобы определить объединённый сетевой адрес (префикс).

2001:DB8:ACAD: 0000 0000 0000 0000::0

e. Перекодируйте двоичную часть обратно в шестнадцатеричный код.

2001:DB8:ACAD::

f. Добавьте префикс объединённого маршрута (результат шага 1c).

2001:DB8:ACAD::/62

Шаг 2: Настройте суммирование межобластных маршрутов на маршрутизаторе R1.

a. Чтобы вручную настроить суммирование межобластной маршрутизации на R1, используйте команду **area** *area-id* **range** *address mask*.

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# area 1 range 2001:DB8:ACAD::/62
```

b. Просмотрите маршруты OSPFv3 на маршрутизаторе R3.

```
R3# show ipv6 route ospf
IPv6 Routing Table - default - 14 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:DB8:ACAD::/62 [110/129]
     via FE80::2, Serial0/0/1
O   2001:DB8:ACAD:8::/64 [110/65]
     via FE80::2, Serial0/0/1
O   2001:DB8:ACAD:12::/64 [110/128]
     via FE80::2, Serial0/0/1
```

Сравните эти результаты с результатами из части 2, шаг 3b. Каким образом сети в области 1 теперь представлены в таблице маршрутизации на маршрутизаторе R3?

c. Просмотрите маршруты OSPFv3 на маршрутизаторе R1.

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:ACAD::/62 [110/1]
     via Null0, directly connected
OI  2001:DB8:ACAD:4::/64 [110/129]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:5::/64 [110/129]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:6::/64 [110/129]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:7::/64 [110/129]
     via FE80::2, Serial0/0/0
O   2001:DB8:ACAD:8::/64 [110/65]
     via FE80::2, Serial0/0/0
O   2001:DB8:ACAD:23::/64 [110/128]
     via FE80::2, Serial0/0/0
```

Сравните эти результаты с результатами из части 2, шаг 3b. Как объединённые сети представлены в таблице маршрутизации на маршрутизаторе R1?

Шаг 3: Объедините сети и настройте суммирование межобластных маршрутов на маршрутизаторе R3.

a. Объедините интерфейсы loopback на маршрутизаторе R3.

1) Выведите список сетевых адресов и определите гекстет, в котором адреса различаются.

2) Перекодируйте различающиеся части из шестнадцатеричного в двоичный код.

3) Подсчитайте число крайних слева совпадающих битов для определения префикса объединённого маршрута.

4) Скопируйте совпадающие биты и добавьте нулевые биты, чтобы определить объединённый сетевой адрес (префикс).

5) Перекодируйте двоичную часть обратно в шестнадцатеричный код.

6) Добавьте префикс суммарного маршрута.

Запишите объединённый адрес в отведённом для этого поле.

b. Вручную настройте суммирование межобластных маршрутов на маршрутизаторе R3. Запишите команды в предусмотренной для этого области.

c. Убедитесь, что маршруты области 2 объединены на маршрутизаторе R1. Какая команда была использована?

d. Запишите элемент таблицы маршрутизации на маршрутизаторе R1 для суммарного маршрута, объявленного маршрутизатором R3.

Вопросы на закрепление

1. Почему нужно использовать OSPFv3 для нескольких областей?

2. Каковы преимущества настройки суммирования межобластных маршрутов?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	П оследо вател ьный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 15
Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей

Топология

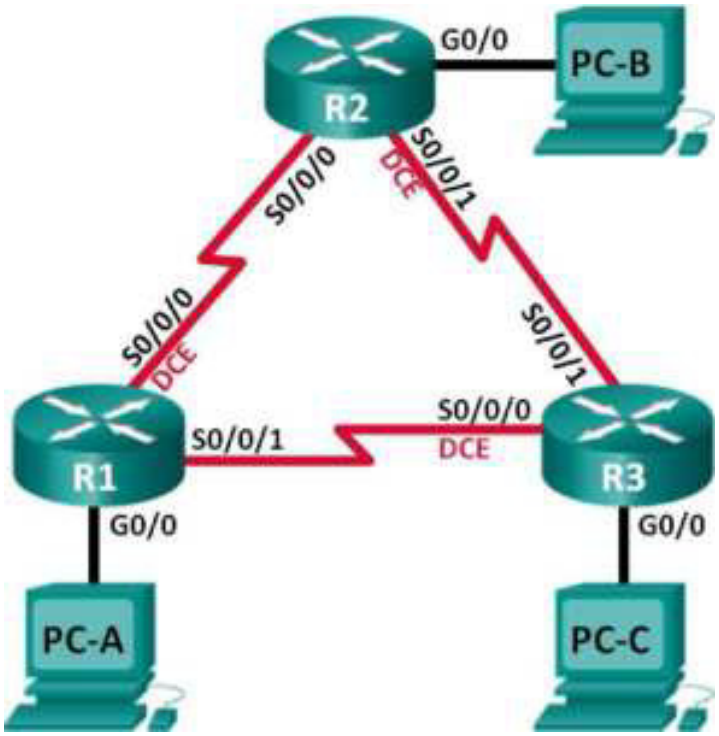


Таблица адресации

Устройство	Идентификатор маршрутизатора	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	1.1.1.1	G0/0	192.168.1.1/24 2001 :DB8:ACAD:A::1/64 FE80::1 link-local	N/A
		S0/0/0	192.168.12.1/30 2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
		S0/0/1	192.18.13.1/30 2001:DB8:ACAD:13::1/64 FE80::1 link-local	N/A
R2	2.2.2.2	G0/0	192.168.2.1/24 2001 :DB8:ACAD:B::2/64 FE80::2 link-local	N/A
		S0/0/0	192.168.12.2/30 2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
		S0/0/1	192.168.23.1/30 2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	3.3.3.3	G0/0	192.168.3.1/24 2001 :DB8:ACAD:C::3/64 FE80::3 link-local	N/A
		S0/0/0	192.168.13.2/30 2001:DB8:ACAD:13::3/64 FE80::3 link-local	N/A
		S0/0/1	192.168.23.2/30 2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A		NIC	192.168.1.3/24 2001 :DB8:ACAD:A::A/64	192.168.1.1 FE80::1
PC-B		NIC	192.168.2.3/24 2001 :DB8:ACAD:B::B/64	192.168.2.1 FE80::2
PC-C		NIC	192.168.3.3/24 2001 :DB8:ACAD:C::C/64	192.168.3.1 FE80::3

Задачи

Часть 1. Построение сети и загрузка конфигураций устройств Часть 2. Поиск и устранение неполадок подключения уровня 3 Часть 3. Поиск и устранение неполадок в работе OSPFv2 Часть 4. Поиск и устранение неполадок в работе OSPFv3

Исходные данные/сценарий

Алгоритм кратчайшего пути (OSPF) — это протокол маршрутизации для IP-сетей на основе состояния канала. OSPFv2 определен для сетей протокола IPv4, а OSPFv3 — для сетей IPv6. OSPFv2 и OSPFv3 — это полностью изолированные протоколы маршрутизации. Изменения в OSPFv2 не влияют на маршрутизацию OSPFv3, и наоборот.

В этой лабораторной работе в сети OSPF для одной области, использующей протоколы OSPFv2 и OSPFv3, возникли неполадки. Вам поручили найти неполадки в работе сети и устранить их.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и на этих устройствах отсутствуют файлы загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и загрузка конфигураций устройств

В части 1 вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите конфигурации маршрутизаторов.

Загрузите следующие конфигурации в соответствующий маршрутизатор. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — **cisco.** Пароль для консоли и доступа vty — **class.**

Конфигурация маршрутизатора R1:

conf t

```
service password-encryption
no ip domain lookup
hostname R1
enable secret class
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 password cisco
 login
banner motd @Unauthorized Access is Prohibited
ipv6 unicast-routing
ipv6 router ospf 1
 router-id 1.1.1.1
 passive-interface g0/0
interface g0/0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:db8:acad:a::1/64
 ipv6 address fe80::1 link-local
interface s0/0/0
 clock rate 125000
 ip address 192.168.12.1 255.255.255.0
 ipv6 address 2001:db8:acad:12::1/64
 ipv6 address fe80::1 link-local
 ipv6 ospf 1 area 0
 no shutdown
interface s0/0/1
 ip address 192.168.13.1 255.255.255.0
 ipv6 address 2001:db8:acad:13::1/64
 ipv6 address fe80::1 link-local
 ipv6 ospf 1 area 0
 no shutdown
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
 network 129.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 0.0.0.3 area 0
 passive-interface g0/0
end
```

Конфигурация маршрутизатора R2:

```
conf t
service password-encryption
no ip domain lookup
hostname R2
enable secret class
```

```
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 password cisco
 login
banner motd ©Unauthorized Access is Prohibited!
ipv6 unicast-routing
ipv6 router ospf 1
 router-id 2.2.2.2
interface g0/0
 ip address 192.168.12.2 255.255.255.0
 ipv6 address 2001:db8:acad:12::2/64
 ipv6 address fe80::1 link-local
 ipv6 ospf 1 area 0
 no shutdown
interface s0/0/0
 ip address 192.168.23.2 255.255.255.252
 ipv6 address 2001:db8:acad:23::2/64
 ipv6 address fe80::2 link-local
 ipv6 ospf 1 area 0
 no shutdown
interface s0/0/1
 clock rate 128000
 ipv6 address 2001:db8:acad:13::2/64
 ipv6 address fe80::2 link-local
 no shutdown
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.23.2 0.0.0.3 area 0
 network 192.168.23.2 0.0.0.3 area 0
end
```

Конфигурация маршрутизатора R3:

```
enable
configure terminal
no ip domain lookup
enable secret class
hostname R3
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 password cisco
 login
```

```
banner motd #Unauthorized Access is Prohibited!#
interface g1/1
 ipv6 address 2001:db8:acad:c1::1/64
 ipv6 address fe80::1 link-local
interface s1/1/0
 no ip address
 clock rate 128000
 ip address 192.168.13.1 255.255.255.252
 ipv6 address 2001:db8:acad:13::1/64
 ipv6 address fe80::1 link-local
 no shutdown
interface s1/1/1
 ip address 192.168.13.2 255.255.255.252
 ipv6 address 2001:db8:acad:23::1/64
 ipv6 address fe80::1 link-local
router ospf 1
 network 192.168.3.0 0.0.0.255 area 0
 passive-interface g1/1
end
```

Часть 2: Поиск и устранение неполадок подключения уровня 3

В части 2 вам предстоит убедиться, что подключение уровня 3 настроено на всех интерфейсах. Для всех интерфейсов устройств понадобится протестировать подключения как для IPv4, так и для IPv6.

Шаг 1: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и что для них настроены правильные IP-адреса.

a. Введите команду **show ip interface brief** на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up). Запишите полученные результаты.

b. Введите команду **show run interface,** чтобы проверить назначения IP-адресов на всех интерфейсах маршрутизаторов. Сравните IP-адреса интерфейсов с данными из таблицы адресации и проверьте назначения маски подсети. Убедитесь, что для IPv6 был назначен адрес типа link-local. Запишите полученные результаты.

c. Устраните все обнаруженные неполадки. Запишите команды, используемые для исправления неполадок.

d. Используя команду **ping**, убедитесь, что каждый маршрутизатор сети связан с соседними

маршрутизаторами с помощью последовательных интерфейсов. Убедитесь, что компьютеры могут успешно отправлять эхо-запросы на свои шлюзы по умолчанию. Если проблемы сохраняются, продолжите поиск и устранение проблем на уровне 3.

Часть 3: Поиск и устранение неполадок в работе OSPFv2

В части 3 вам необходимо устранить неполадки OSPFv2 и выполнить изменения, необходимые для настройки маршрутов OSPFv2 и сквозного подключения IPv4.

Примечание. Интерфейсы локальной сети (G0/0) не должны объявлять данные маршрутизации OSPF, но маршруты к этим сетям должны содержаться в таблицах маршрутизации.

Шаг 1: Протестируйте сквозное подключение IPv4.

От каждого ПК отправьте эхо-запросы на другие ПК в топологии, чтобы проверить сквозное подключение.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

a. Отправьте эхо-запрос от узла PC-A на PC-B. Успешно ли выполнен эхо-запрос?

b. Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C. Успешно ли выполнен эхо-запрос?

c. Отправьте эхо-запрос с PC-B на PC-C. Успешно ли выполнен эхо-запрос?

Шаг 2: Убедитесь, что все интерфейсы на маршрутизаторе R1 назначены в область 0 протокола OSPFv2.

a. Введите команду **show ip protocols**, чтобы убедиться в том, что OSPF работает и все сети

анонсируются в области 0. Убедитесь, что идентификатор маршрутизатора настроен правильно. Запишите полученные результаты.

b. Внесите требуемые изменения в конфигурацию маршрутизатора R1, исходя из результатов команды **show ip protocols.** Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ip ospf process.**

d. Повторно введите команду **show ip protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ip ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ip ospf interface g0/0,** чтобы убедиться, что интерфейс G0/0 является пассивным.

Примечание. Эти сведения можно также получить с помощью команды **show ip protocols.**

g. Устраните все неполадки, обнаруженные на маршрутизаторе R1. Укажите все дополнительные изменения, внесённые в конфигурацию R1. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 3: Убедитесь, что все интерфейсы на маршрутизаторе R2 назначены в область 0 протокола OSPFv2.

a. Введите команду **show ip protocols,** чтобы убедиться, что OSPF работает и все сети

анонсируются в области 0. Убедитесь, что идентификатор маршрутизатора настроен правильно. Запишите полученные результаты.

b. Внесите требуемые изменения в конфигурацию маршрутизатора R2, исходя из результатов команды **show ip protocols.** Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ip ospf process.**

d. Повторно введите команду **show ip protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ip ospf interface brief**, чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ip ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0 является пассивным.

Примечание. Эти сведения можно также получить с помощью команды **show ip protocols.**

g. Устраните все неполадки, обнаруженные на маршрутизаторе R2. Укажите все дополнительные изменения, внесённые в конфигурацию R2. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 4: Убедитесь, что все интерфейсы на маршрутизаторе R3 назначены в область 0 протокола OSPFv2.

a. Введите команду **show ip protocols**, чтобы убедиться, что OSPF работает и все сети анонсируются в области 0. Убедитесь, что идентификатор маршрутизатора тоже настроен правильно. Запишите полученные результаты.

b. Внесите требуемые изменения в конфигурацию маршрутизатора R3, исходя из результатов команды **show ip protocols.** Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ip ospf process.**

d. Повторно введите команду **show ip protocols**, чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ip ospf interface brief**, чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ip ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0 является пассивным.

Примечание. Эти сведения можно также получить с помощью команды **show ip protocols.**

g. Устраните все неполадки, обнаруженные на маршрутизаторе R3. Укажите все дополнительные изменения, внесённые в конфигурацию R3.

Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 5: Проверьте данные соседнего устройства OSPF.

a. На всех маршрутизаторах введите команду **show ip ospf neighbor**, чтобы просмотреть сведения о соседних устройствах OSPF.

Шаг 6: Проверьте информацию о маршрутах OSPFv2.

a. Введите команду **show ip route ospf**, чтобы убедиться, что каждый маршрутизатор обладает маршрутами OSPFv2 ко всем не граничащим с ним сетям.

Все ли маршруты OSPFv2 доступны?

Если какие-либо маршруты OSPFv2 пропущены, то какие?

b. Если какие-то данные маршрутизации пропущены, исправьте эти неполадки.

Шаг 7: Проверьте сквозное подключение IPv4.

На каждом ПК убедитесь в наличии сквозного подключения IPv4. Компьютеры должны успешно отправлять эхо-запросы на другие ПК в топологии. Если сквозное подключение IPv4 отсутствует, выполняйте поиск и устранение неполадок, пока не будут решены оставшиеся проблемы.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Часть 4: Поиск и устранение неполадок в работе OSPFv3

В части 4 вам необходимо устранить неполадки OSPFv3 и выполнить изменения, необходимые для настройки маршрутов OSPFv3 и сквозного подключения IPv6.

Примечание. Интерфейсы локальной сети (G0/0) не должны объявлять данные маршрутизации OSPFv3, но маршруты к этим сетям должны содержаться в таблицах маршрутизации.

Шаг 1: Протестируйте сквозное подключение IPv6.

С каждого ПК отправьте эхо-запросы на Ру6-адреса других узлов ПК в топологии, чтобы проверить сквозное подключение IPv6.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Шаг 2: Убедитесь, что одноадресная маршрутизация IPv6 включена на всех маршрутизаторах.

a. Простым способом проверки включения ^6-маршрутизации на маршрутизаторе является

использование команды **show run | section ipv6 unicast.** Если добавить вертикальную линию (|) к команде **show run**, то команда **ipv6 unicast-routing** покажет, была ли включена маршрутизация IPv6.

Примечание. Команду **show run** можно выполнить и без вертикальной линии, а затем вручную найти команду **ipv6 unicast-routing.**

Введите эту команду на каждом маршрутизаторе. Запишите полученные результаты.

b. Если одноадресная маршрутизация IPv6 не включена на одном или нескольких маршрутизаторах, включите ее. Запишите команды, используемые для исправления неполадок.

Шаг 3: Убедитесь, что все интерфейсы на маршрутизаторе R1 назначены в область 0 протокола OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь, что идентификатор маршрутизатора настроен правильно. Также убедитесь, что соответствующие интерфейсы отображаются под областью 0.

Примечание. Если у этой команды отсутствует результат, то процесс OSPFv3 не был настроен.

Запишите полученные результаты.

b. Введите необходимые изменения конфигурации для маршрутизатора R1. Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ipv6 ospf process.**

d. Повторно введите команду **show ipv6 protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ipv6 ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ipv6 ospf interface g0/0,** чтобы убедиться, что этот интерфейс не объявляет маршруты OSPFv3.

g. Устраните все неполадки, обнаруженные на маршрутизаторе R1. Укажите все дополнительные изменения, внесённые в конфигурацию R1. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 4: Убедитесь, что все интерфейсы на маршрутизаторе R2 назначены в область 0 протокола OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь, что идентификатор маршрутизатора настроен правильно. Также убедитесь, что соответствующие интерфейсы отображаются под областью 0.

Примечание. Если у этой команды отсутствует результат, то процесс OSPFv3 не был настроен.

Запишите полученные результаты.

b. Введите необходимые изменения конфигурации на маршрутизаторе R2. Запишите команды, используемые для исправления неполадок.

c. При необходимости введите команду **clear ipv6 ospf process.**

d. Повторно введите команду **show ipv6 protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ipv6 ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ipv6 ospf interface g0/0**, чтобы убедиться, что этот интерфейс не настроен для объявления маршрутов OSPFv3.

g. Укажите все дополнительные изменения, внесённые в конфигурацию R2. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 5: Убедитесь, что все интерфейсы на маршрутизаторе R3 назначены в область 0 протокола OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь, что идентификатор маршрутизатора настроен правильно. Также убедитесь, что соответствующие интерфейсы отображаются под областью 0.

Примечание. Если у этой команды отсутствует результат, то процесс OSPFv3 не был настроен.

Запишите полученные результаты.

b. Выполните необходимые изменения конфигурации на маршрутизаторе R3. Запишите команды, используемые для исправления неполадок.

При необходимости введите команду **clear ipv6 ospf process.**

d. Повторно введите команду **show ipv6 protocols,** чтобы убедиться в эффективности выполненных изменений.

e. Введите команду **show ipv6 ospf interface brief,** чтобы убедиться, что все интерфейсы перечислены как сети OSPF, назначенные в область 0.

f. Введите команду **show ipv6 ospf interface g0/0,** чтобы убедиться, что этот интерфейс не объявляет маршруты OSPFv3.

g. Устраните все неполадки, обнаруженные на маршрутизаторе R3. Укажите все дополнительные изменения, внесённые в конфигурацию R3. Если устройство работает нормально, то напишите, что «проблем не найдено».

Шаг 6: Убедитесь, что все маршрутизаторы обладают правильной информацией об отношениях смежности с соседними маршрутизаторами.

a. Введите команду **show ipv6 ospf neighbor,** чтобы убедиться в создании отношений смежности между соседними маршрутизаторами.

b. Устраните все оставшиеся неполадки отношений смежности OSPFv3.

Шаг 7: Проверьте информацию о маршрутах OSPFv3.

a. Введите команду **show ipv6 route ospf** и убедитесь в наличии маршрутов OSPFv3 ко всем несмежным сетям.

Все ли маршруты OSPFv3 доступны?

Если какие-то маршруты OSPFv3 отсутствуют, то какие?

b. Устраните все оставшиеся ошибки маршрутизации.

Шаг 8: Проверьте сквозное подключение IPv6.

На каждом ПК убедитесь в наличии сквозного подключения IPv6. Компьютеры должны успешно отправлять эхо-запросы на каждый интерфейс в сети. Если сквозное подключение IPv6 отсутствует, выполняйте поиск и устранение неполадок, пока не будут решены оставшиеся проблемы.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Вопросы на закрепление

Почему следует устранять неполадки в работе OSPFv2 и OSPFv3 по отдельности?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа № 16

Настройка базового PPP с аутентификацией

Топология

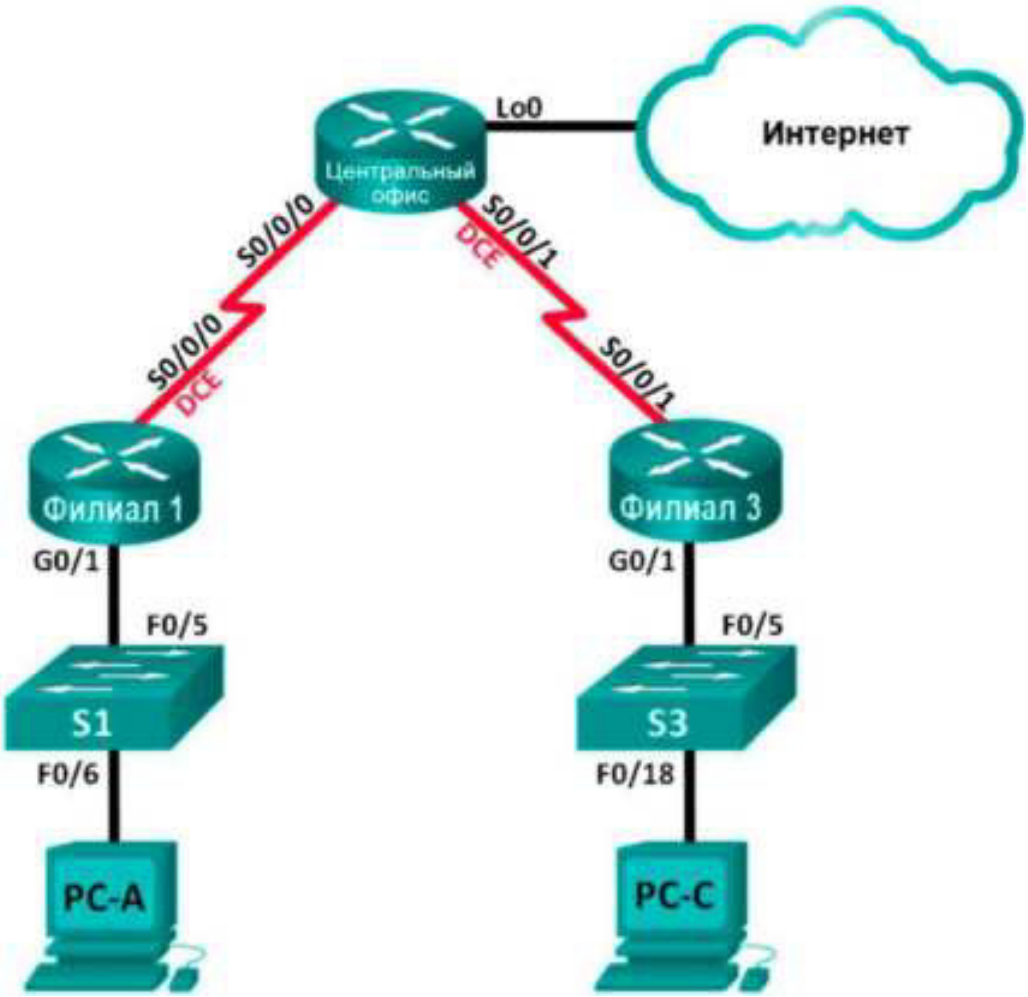


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Филиал 1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
Central	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
Филиал 3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка инкапсуляции PPP

Часть 3. Настройка аутентификации CHAP PPP

Исходные данные/сценарий

PPP — очень распространенный протокол WAN уровня 2. PPP можно использовать для подключения из локальной сети к WAN-провайдеру и для подключения сегментов LAN в рамках корпоративной сети.

В этой лабораторной работе требуется настроить инкапсуляцию PPP на выделенных последовательных каналах между маршрутизаторами филиалов и центральным маршрутизатором. Требуется настроить протокол аутентификации по квитированию вызова (CHAP) PPP на последовательных каналах PPP. Вы также изучите влияние, оказываемое

изменениями инкапсуляции и аутентификации на состояние последовательного канала.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

1) 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

2) 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

3) 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

4) консольные кабели для настройки устройств Cisco IOS через порты консоли;

5) кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например,

IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имя устройства.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

g. Настройте ведение журнала состояния консоли на синхронный режим.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

i. Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

j. На маршрутизаторе «Главный» создайте **Loopback 0** для имитации доступа в Интернет и назначьте IP-адрес согласно таблице адресации.

Шаг 4: Настройте маршрутизацию.

a. Включите на маршрутизаторах использование протокола OSPF для одной области и используйте в качестве идентификатора процесса значение 1. Добавьте в процесс OSPF все сети, за исключением 209.165.200.224/27.

b. На маршрутизаторе «Главный» настройте маршрут по умолчанию к симулируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите маршрут в процесс OSPF.

c. **На всех маршрутизаторах выполните команды** show ip route ospf, show ip ospf interface brief

и **show ip ospf neighbor,** чтобы проверить правильность настройки OSPF. Обратите внимание на идентификатор каждого маршрутизатора.

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Все устройства должны успешно выполнять эхо-запросы ко всем остальным устройствам, указанным в топологии. Если это не так, выполняйте поиск и устранение неполадок то до тех пор, пока не удастся установить сквозное соединение.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

Шаг 7: Сохраните настройки.

Часть 2: Настройка инкапсуляции PPP

Шаг 1: Отобразите инкапсуляцию, используемую в последовательном интерфейсе по умолчанию.

На маршрутизаторах выполните команду **show interfaces serial** *идентификатор_интерфейса* для отображения текущей инкапсуляции, используемой в последовательном интерфейсе.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1003 packets input, 78348 bytes, 0 no buffer
     Received 527 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1090 packets output, 80262 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Укажите тип инкапсуляции, используемой в последовательном интерфейсе по умолчанию, для маршрутизатора Cisco.
шаг 2: Измените инкапсуляцию на PPP.
a. Для изменения инкапсуляции HDLC на PPP введите команду encapsulation ppp на интерфейсе SO/O/O маршрутизатора «Филиал 1»

```
Branch1(config)# interface s0/0/0
```

.

```
Branch1(config-if)# encapsulation ppp
Branch1(config-if)#
Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Branch1(config-if)#
Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
```

b. Введите команду для отображения состояния канала и протокола канала

для интерфейса S0/0/0 маршрутизатора «Филиал 1». Задокументируйте выполненную команду. Укажите текущее состояние интерфейса S0/0/0.

c. Для исправления разночтений в настройках инкапсуляции для последовательного интерфейса ведите команду encapsulation ppp на интерфейсе S0/0/0 для маршрутизатора Central.

```
Central(config)# interface s0/0/0
Central(config-if)# encapsulation ppp
Central(config-if)#
.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

d. Убедитесь, что интерфейс SO/O/O как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» находится в активном состоянии и настроен с инкапсуляцией PPP.

Укажите состояние протокола PPP (LCP).укажите, согласование каких протоколов NCP было выполнено.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:03:58
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     77 packets input, 4636 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     117 packets output, 5800 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 8 interface resets
     22 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     18 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Central# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:01:20
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     41 packets input, 2811 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     40 packets output, 2739 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Шаг 3: Намеренно разорвите последовательное подключение.

a. Выполните команды debug ppp, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы «Филиал 1» и «Главный».

```
Branch1# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch1# debug ppp packet
PPP packet display debugging is on

Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central# debug ppp packet
PPP packet display debugging is on
```

b. Наблюдайте за сообщениями команды debug PPP при проходе трафика по последовательному каналу между маршрутизаторами «Филиал 1» и «Главный».

```
Branch1#
Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#
Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
```

c. Разорвите последовательное подключение путем возвращения HDLC в качестве инкапсуляции для последовательного интерфейса S0/0/0 маршрутизатора «Филиал 1». Запишите команду, использованную для изменения инкапсуляции на HDLC.

d. Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Филиал 1». Последовательное подключение завершено, и протокол линии связи не функционирует. Маршрут к 10.1.1.2 («Главный») удалён из

таблицы маршрутизации.

```
Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.295: PPP: NET STOP send to AAA.
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.29
Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN
Branch1(config-if)#
Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
```

e. Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Главный». Маршрутизатор «Главный» продолжает попытки установить подключение к маршрутизатору «Филиал 1», как видно из сообщений команды debug. Если интерфейсы не могут установить подключение, интерфейсы снова прекращают работу. Кроме того, OSPF не может сформировать отношения смежности с соседним с ним устройством

вследствие несоответствия инкапсуляции для последовательного канала.

```
Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification
Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message
Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.296: PPP: NET STOP send to AAA.
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.1
Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN
Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification
.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message
.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]
.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING
.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction
.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]
.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:29:52.296: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]
.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
.Jun 20 02:29:54.308: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<Данные опущены>
.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:10.436: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING
```

```
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:30:14.452: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<Данные опущены>
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:32.580: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not running
.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING
.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]
.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
```

Что происходит в случае, если на одном конце последовательного канала используется инкапсуляция PPP, а на другом — HDLC?

f. Введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1», чтобы исправить несоответствующую инкапсуляцию.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
```

g. Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Филиал 1» при установке подключения между маршрутизаторам «Филиал1» и «Главный».

```
Branch1(config-if)#
Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification
Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message
Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]
Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING
Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction
Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line

Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.399: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP:    Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
<Данные опущены>
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on Serial0/0/0 from
LOADING to FULL, Loading Done
Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]
```

h.наблюдайте за сообщениями команды debug PPP от маршрутизатора «Главный» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

```
Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10
Jun 20 03:01:59.393: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating
Jun 20 03:01:59.393: PPP: NET STOP send to AAA.
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negotiated
.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN
.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.1
.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1
.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]
.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING
.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction
.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line
<Данные опущены>
.Jun 20 03:01:59.401: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 03:01:59.433: Se0/0/0 IPCP:    Address 10.1.1.2 (0x03060A010102)
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]
```

```
<Данные опущены>
.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open
.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60
.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]
.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]
Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open
Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]
Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
```

Основываясь на сообщении команды debug, укажите, через какие этапы проходит PPP, если другой конец последовательного канала на маршрутизаторе Central настроен с инкапсуляцией PPP.

Что произойдет, если инкапсуляция PPP настроена на обоих концах последовательного канала?

i. Введите команду **undebug all** (или **u all**) на маршрутизаторах «Филиал 1» и «Главный» и отключите всю отладку на обоих маршрутизаторах.

j. После стабилизации сети выполните команду **show ip interface brief** на маршрутизаторах «Филиал 1» и «Главный». Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

k. Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» настроен на инкапсуляцию PPP.

Ниже запишите команду для проверки инкапсуляции PPP.

l .Инкапсуляцию в последовательном интерфейсе для связи между маршрутизаторами «Главный» и «Филиал 3» измените на инкапсуляцию PPP.

```
Central(config)# interface s0/0/1
Central(config-if)# encapsulation ppp

Central(config-if)#
Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
LOADING to FULL, Loading Done

Branch3(config)# interface s0/0/1
Branch3(config-if)# encapsulation ppp
Branch3(config-if)#
Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from LOADING to FULL, Loading Done
```

m. Перед переходом к части 3 убедитесь в том, что сквозное соединение восстановлено.

Часть 3: Настройка аутентификации CHAP PPP

Шаг 1: Убедитесь, что инкапсуляция PPP настроена на всех последовательных интерфейсах.

Запишите команды, используемые для подтверждения того, что настроена инкапсуляция PPP.

Шаг 2: Настройте аутентификацию CHAP PPP для канала между маршрутизатором «Главный» и маршрутизатором «Филиал 3».

a. Настройте имя пользователя для аутентификации CHAP.

```
Central(config)# username Branch3 password cisco
Branch3(config)# username Central password cisco
```

b. Выполните команды **debug ppp** на маршрутизаторе «Филиал 3» для наблюдения за процессом, который связан с аутентификацией.

```
Branch3# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch3# debug ppp packet
PPP packet display debugging is on
```

c. Настройте интерфейс S0/0/1 на маршрутизаторе «Филиал 3» для аутентификации CHAP.

```
Branch3(config)# interface s0/0/1
Branch3(config-if)# ppp authentication chap
```

d. Изучите сообщения команды debug PPP на маршрутизаторе «Филиал 3», выдаваемые во время согласования с маршрутизатором.«Главный».

```
Branch3(config-if)#
Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed
Jun 20 04:25:02.079: PPP: NET STOP send to AAA.
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated
.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN
.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, addres
10.2.2.2
.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2
.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA6C]
.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING
.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction
.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]
<Данные опущены>
.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]
.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 04:25:02.091: Se0/0/1 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 04:25:02.091: Se0/0/1 LCP:    MagicNumber 0xF7B20F10 (0x0506F7B20F10)
.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 26 from "Branch3"
.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open
.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]
.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated User
.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User
.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol not up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP. state[Initial]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10
```

```
<Данные опущены>
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0, address
10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from LOADING to FULL, Loading Done
.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333 link[cdp]
.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
```

Основываясь на сообщениях команды debug для PPP, укажите, какие этапы проходит маршрутизатор «Филиал 3», прежде чем будет установлена связь с маршрутизатором «Главный».

e. Введите команду **debug ppp authentication** для наблюдения за сообщениями аутентификации CHAP на маршрутизаторе Central.

```
Central# debug ppp authentication
PPP authentication debugging is on
```

f. Настройте аутентификацию CHAP на интерфейсе S0/0/1 на маршрутизаторе «Главный».

g. Наблюдайте за сообщениями команд debug PPP, относящихся к аутентификации CHAP на маршрутизаторе «Главный».

```
Central(config-if)#
.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction
.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]
.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA
```

h. Введите команду **undebug all** (или **u all**) на маршрутизаторах «Главный» и «Филиал 3» и отключите всю отладку.

```
Central# undebug all
All possible debugging has been turned off
```

Шаг 3: Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.

a. На маршрутизаторе «Главный» настройте имя пользователя для использования с «Филиал 1». Назначьте **cisco** в качестве пароля.

```
Central(config)# username Branch1 password cisco
```

b. На маршрутизаторах «Главный» и «Филиал 1» настройте аутентификацию CHAP на интерфейсе S0/0/0. Что происходит с интерфейсом?

Примечание. Для ускорения процесса выключите интерфейс и снова его включите.

c. Для исследования возникшего процесса используйте команду

debug ppp negotiation.

```
Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central(config-if)#
.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP
.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message
.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]
.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING
.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction
.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15
.Jun 20 05:25:26.229: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 05:25:26.233: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
```

```
.Jun 20 05:25:26.233: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open
.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer
.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING
.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to Stopping]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification
.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN
```

Объясните, что приводит к окончательному завершению канала. Запишите ниже команду, выполненную для устранения неполадки.

d. Введите команду **undebug all** на всех маршрутизаторах, чтобы отключить отладку.

e. Проверьте связь между конечными устройствами.

Вопросы на закрепление

1. Каковы признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция?

2. Каковы признаки того, что на канале последовательной связи настроена несоответствующая аутентификация?Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial0/0/0(S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial0/0/0(S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial0/1/0(S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial0/0/0(S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial0/0/0(S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 17

Отладка базового PPP с аутентификацией

Топология

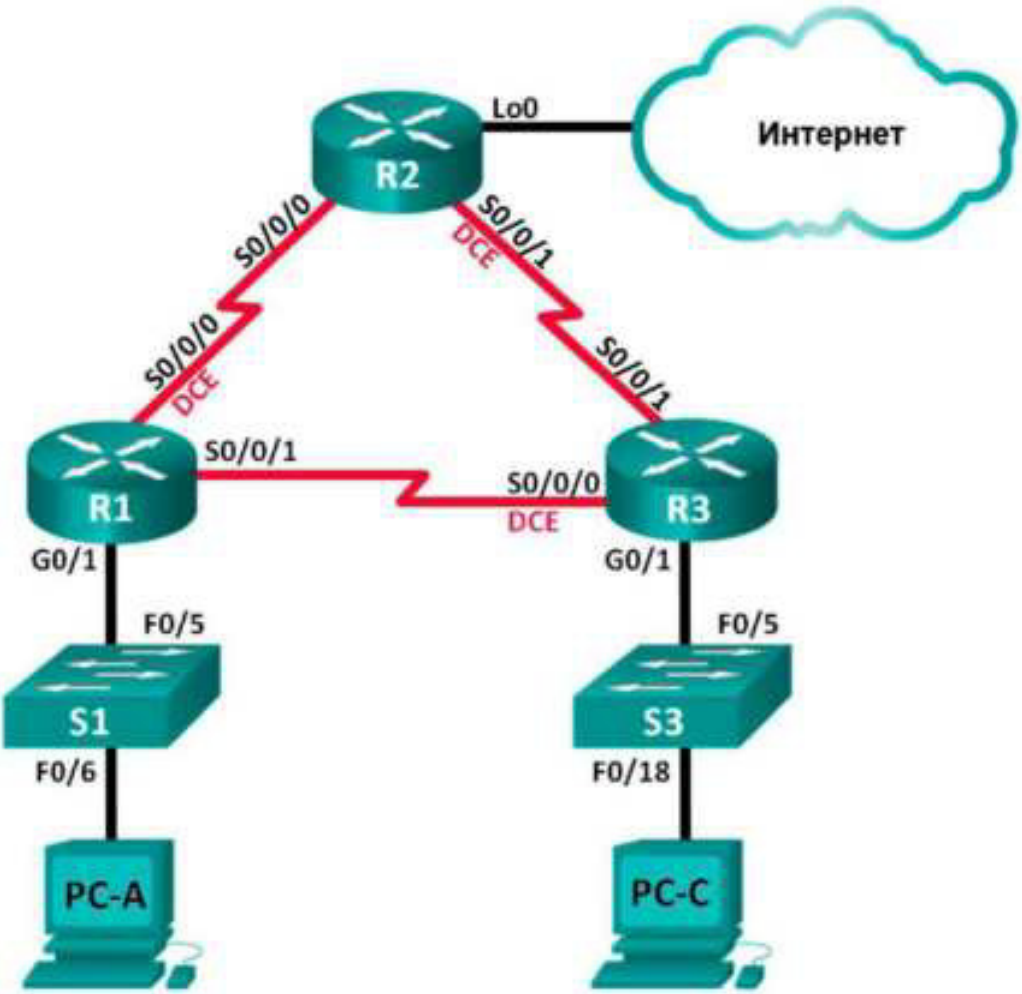


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	Недоступно
	S0/0/1	192.168.13.1	255.255.255.252	Недоступно
R2	Lo0	209.165.200.225	255.255.255.252	Недоступно
	S0/0/0	192.168.12.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	Недоступно
R3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	Недоступно
	S0/0/1	192.168.23.2	255.255.255.252	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Построение сети и загрузка настроек устройств

Часть 2. Поиск и устранение неполадок канального уровня

Часть 3. Поиск и устранение неполадок сетевого уровня

Исходные данные/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым инженером. В результате нескольких ошибок в настройках возникли проблемы со связью. Начальник попросил вас найти и устранить неполадки в настройке и задокументировать работу. Найдите и исправьте ошибки, используя свои знания PPP и стандартные методы тестирования. Убедитесь, что на всех последовательных каналах используется аутентификация CHAP PPP и что все сети доступны.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

• 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

• 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

• 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например, Tera Term)

• консольные кабели для настройки устройств Cisco IOS через порты консоли;

• кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и загрузка настроек устройств

В части 1 вам предстоит создать топологию сети, настроить базовые параметры для узлов ПК и загрузить настройки маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите настройки маршрутизатора.

Загрузите в соответствующий маршрутизатор следующие настройки. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — **class.** Пароль для консоли и доступа vty — **cisco.** Все последовательные интерфейсы должны быть настроены с инкапсуляцией PPP и аутентификацией по протоколу CHAP с паролем **chap123.**

Настройка маршрутизатора R1

```
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Настройка маршрутизатора R2:

```
hostname R2
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R1 password chap123
username r3 password chap123
interface lo0
 ip address 209.165.200.225 255.255.255.252
interface s0/0/0
 ip address 192.168.12.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.1 255.255.255.252
 clock rate 128000
 no shutdown
 exit
router ospf 1
 router-id 2.2.2.2
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 default-information originate
 exit
ip route 0.0.0.0 0.0.0.0 loopback0
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

```
hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
```

Настройка маршрутизатора R3:

```
interface g0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.13.2 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
 exit
router ospf 1
 router-id 3.3.3.3
 network 192.168.13.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 passive-interface g0/1
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Шаг 4: Сохраните текущую конфигурацию.

Часть 2: Поиск и устранение неполадок канального уровня

В части 2 следует использовать команды **show** для устранения неполадок канального уровня. Не забудьте проверить такие параметры, как тактовая частота, инкапсуляция, CHAP и имена и пароли пользователей.

Шаг 1: Изучите настройку маршрутизатора R1.

a. Используйте команду **show interfaces,** чтобы определить, установлен ли PPP на обоих последовательных каналах.

Основываясь на результатах работы команды **show interfaces** для S0/0/0 и S0/0/1, укажите возможные неполадки в каналах PPP.

b. В процессе поиска и устранения неполадок используйте команду **debug ppp authentication** для просмотра результатов аутентификации PPP в реальном времени.

```
R1# debug ppp authentication
PPP authentication debugging is on
```

c. Для исследования настроек на S0/0/0 используйте команду **show run interface s0/0/0 .**

Устраните все неполадки, связанные с S0/0/0. Запишите команды, использованные для исправления настройки.

Укажите выходные данные команды debug, выполненной после устранения неполадки.

d. Для исследования параметров на S0/0/1 используйте команду **show run interface s0/0/1 .**

Устраните все неполадки, связанные с S0/0/1. Запишите команды, использованные для исправления настройки.

Укажите выходные данные команды debug, выполненной после устранения неполадки.

e. Для отключения вывода данных команды debug PPP используйте команду **no debug ppp authentication** или **undebug all.**

f. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username** .

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

Шаг 2: Исследуйте настройку маршрутизатора R2.

a. Используйте команду **show interfaces,** чтобы определить, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены?

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

b. Для исследования связей, которые не были установлены, используйте команду **show run interface.**

Устраните все обнаруженные неполадки, относящиеся к интерфейсам. Запишите команды, использованные для исправления настройки.

c. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username .**

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

d. Используйте команду **show ppp interface serial** для того последовательного интерфейса, который вы отлаживаете.

Связь установлена?

Шаг 3: Исследуйте настройку маршрутизатора R3.

a. Используйте команду **show interfaces,** чтобы определить, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены?

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

b. Для исследования всех последовательных связей, которые не были установлены, используйте команду **show run interface.**

Устраните все неполадки, обнаруженные на интерфейсах. Запишите команды, использованные для исправления настройки.

c. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username .**

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

d. Используйте **команду** show, чтобы убедиться, что последовательные связи установлены.

e. Связь по протоколу PPP установлена во всех каналах?

f. Эхо-запрос от узла ПК A к Lo0 выполняется успешно?

g. Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C?

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

Часть 3: Поиск и устранение неполадок сетевого уровня

В части 3 вам предстоит убедиться, что подключения уровня 3 установлены на всех интерфейсах, исследуя для этого настройки IPv4 и OSPF.

Шаг 1: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и настроены с правильными IP-адресами.

Выполните команду **show ip interface brief** на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up).

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

Шаг 2: Проверка маршрутизации OSPF

Введите **команду show ip protocols,** чтобы убедиться, что OSPF запущен и что все сети объявляются.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

Успешно ли выполняется эхо-запрос от узла ПК А на узел ПК С?

Если между некоторыми узлами нет связи, продолжите поиск и устранение неполадок, чтобы устранить все имеющиеся неполадки.

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 18

Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL

Топология

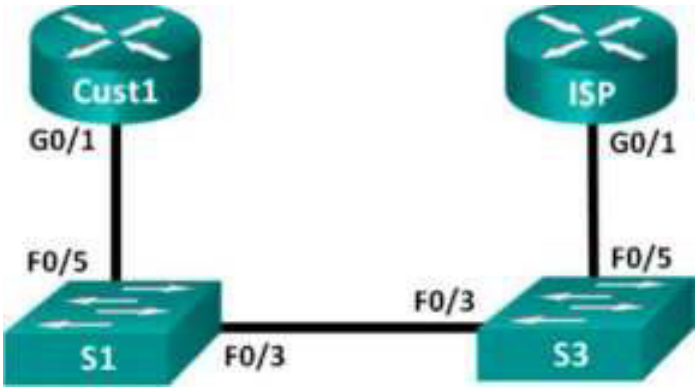


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cust1	G0/1	Получен с помощью PPP	Получен с помощью PPP	Получен с помощью PPP
ISP	G0/1	Недоступно	Недоступно	Недоступно

Задачи

Часть 1. Развёртывание сети

Часть 2. Настройка маршрутизатора ISP

Часть 3. Настройка маршрутизатора Cust1

Исходные данные/сценарий

Интернет-провайдеры часто используют протокол PPPoE для передачи данных по каналам DSL своим заказчикам. PPP поддерживает назначение IP-адреса устройству на удаленном конце канала PPP. Что ещё более важно, PPP поддерживает аутентификацию CHAP. Интернет-

провайдеры могут проверять учётные записи, чтобы определить, оплатил ли заказчик свой счёт, прежде чем позволить ему подключиться к Интернету

В этой лабораторной работе выполняется настройка подключения на стороне клиента и интернет- провайдера для настройки PPPoE. В большинстве случаев достаточно выполнить настройку на стороне клиента.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от

данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь в том, что маршрутизаторы и коммутаторы очищены от данных и на них нет стартовых конфигураций. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;

- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имя устройств в соответствии с топологией.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

g. Настройте ведение журнала состояния консоли на синхронный режим.

h. Сохраните настройку.

Часть 2: Настройка маршрутизатора интернет-провайдера ISP

В части 2 необходимо настроить маршрутизатор ISP с использованием параметров PPPoE для приёма подключений от маршрутизатора Cust1.

Примечание. Многие из команд настройки PPPoE для маршрутизатора интернет-провайдера выходят за рамки курса; однако они необходимы для выполнения лабораторной работы. Их можно скопировать

и вставить в Маршрутизатор ISP в командной строке режима глобальной конфигурации.

a. Создайте в локальной базе учётных записей имя пользователя **Custl** с паролем **ciscopppoe.**

```
ISP(config)# username Cust1 password ciscopppoe
```

b. Создайте пул адресов, которые будут назначены пользователям.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

c. Создайте виртуальный шаблон Virtual Template и свяжите с ним IP-адрес G0/1. Свяжите виртуальный шаблон с пулом адресов. Настройте CHAP для аутентификации пользователей

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

Назначьте шаблон группе PPPoE.

.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

e.Свяжите группу bba-group с физическим интерфейсом G0/1

```
ISP(config)# interface g0/1
ISP(config-if# pppoe enable group global
ISP(config-if)# no shutdown
```

Часть 3: Настройка маршрутизатора Custl

В части 3 необходимо настроить маршрутизатор Cust1 с использованием параметров PPPoE.

a. Настройте интерфейс G0/1 для подключения PPPoE.

```
Cust1(config)# interface g0/1
Cust1(config-if)# pppoe enable
Cust1(config-if)# pppoe-client dial-pool-number 1
Cust1(config-if)# exit
```

d. Свяжите интерфейс G0/1 с интерфейсом номеронабирателя Dialer. Используйте имя пользователя **Custl** и пароль **ciscopppoe,** настроенные в части 2.

```
Cust1(config)# interface dialer 1
Cust1(config-if)# mtu 1492
Cust1(config-if)# ip address negotiated
Cust1(config-if)# encapsulation ppp
Cust1(config-if)# dialer pool 1
Cust1(config-if)# ppp authentication chap callin
Cust1(config-if)# ppp chap hostname Cust1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# exit
```

c. Настройте статический маршрут по умолчанию через интерфейс номеронабирателя.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

d.Настройте отладку на маршрутизаторе Cust1 для отображения согласования PPP и PPPoE.

```
Cust1# debug ppp authentication
Cust1# debug pppoe events
```

e. Включите интерфейс G0/1 на маршрутизаторе Cust1 и проверьте выходные данные отладки при установлении сеанса номеронабирателя PPPoE и во время аутентификации CHAP.

```
*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
```

```
*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
*Jul 30 19:29:03.839:  padi timer expired
*Jul 30 19:29:03.839:  Sending PADI: Interface = GigabitEthernet0/1
*Jul 30 19:29:03.839: PPPoE 0: I PADO  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.887:  PPPOE: we've got our pado and the pado timer went off
*Jul 30 19:29:05.887: OUT PADR from PPPoE Session
*Jul 30 19:29:05.895: PPPoE 1: I PADS  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.895: IN PADS from PPPoE Session
*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.
*Jul 30 19:29:05.899: PPPoE : encap string prepared
*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client
*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction
*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout
*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]
*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication
*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request
*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL
*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4
*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
```

f. Введите команду **show ip interface brief** на маршрутизаторе Cust1, чтобы отобразить IP-адрес, назначенный маршрутизатором ISP. Выходные данные приведены ниже. Каким способом был получен этот IP-адрес?

g.Введите команду **show pppoe session** на маршрутизаторе Custl. Выходные данные приведены

ниже. :: show pppoe session

```
Cust1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer1                    10.0.0.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
```

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area


          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
          ia - IS-IS inter area, * - candidate default, U - per-user static route
          o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
          + - replicated route, % - next hop override

   Gateway of last resort is 0.0.0.0 to network 0.0.0.0

   S*    0.0.0.0/0 is directly connected, Dialer1
         10.0.0.0/32 is subnetted, 2 subnets
   C        10.0.0.1 is directly connected, Dialer1
   C        10.0.0.254 is directly connected, Dialer1
```

h.Введите команду **show ip route** на маршрутизаторе Cust1. Выходные

```
Cust1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
          SID   LocMAC                                      VA-st      Type
    N/A     1   30f7.0da3.0b01  Gi0/1                   Di1 Vi2        UP
                30f7.0da3.0bc1                              UP
```

i. Отправьте эхо-запрос на адрес 10.0.0.254 с маршрутизатора Cust1. Эхо-запрос должен быть успешным. В противном случае устраните неполадки, пока не будет установлено подключение.

```
Cust1# ping 10.0.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Вопросы на закрепление

Почему интернет-провайдеры, использующие технологию DSL, главным образом используют протокол PPPoE?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа19

. Настройка туннеля VPN GRE по схеме «точка-точка»

Топология

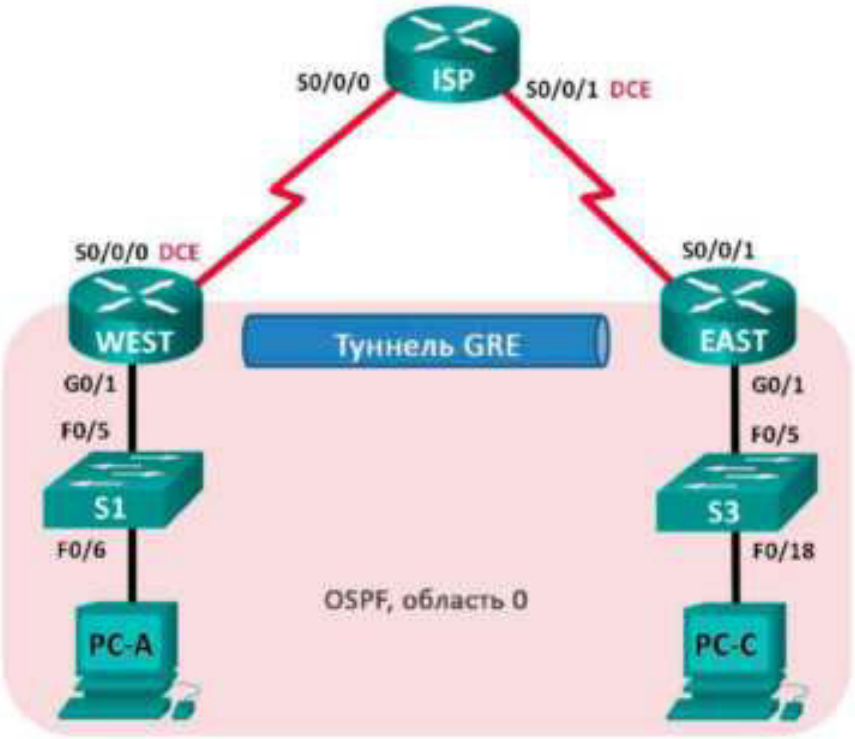


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
EAST	G0/1	172.16.2.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.2	255.255.255.252	Недоступно
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка туннеля GRE

Часть 3. Включение маршрутизации через туннель GRE

Исходные данные/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4

- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точка- точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Назначьте имена устройств.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

g. Настройте ведение журнала состояния консоли на синхронный режим.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

i. **Настройте тактовую частоту на** 128000 **для всех последовательных интерфейсов DCE.**

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте соединение.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхо- запросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

Шаг 7: Сохраните текущую конфигурацию.

Часть 2: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

a.

астройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

b. Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
EAST(config-if)# tunnel source 10.2.2.1
EAST(config-if)# tunnel destination 10.1.1.1
```

Примечание. Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

Шаг 2: Убедитесь, что туннель GRE работает.

a. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

```
WEST# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Tunnel0                    172.16.12.1     YES manual up                    up

EAST# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.2.1      YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Tunnel0                    172.16.12.2     YES manual up                    up
```

b.С помощью команды **show interfaces tunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

c.Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

```
WEST# ping 172.16.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms
```

d. С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

e. Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST?

С какими интерфейсами связаны эти IP-адреса? Почему?

f. Команды **ping** и **traceroute** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 3: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда network будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

a.

астройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

b. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Шаг 2: Проверка маршрутизации OSPF.

a.

тправьте с маршрутизатора WEST команду **show ip route** для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.1.1.2


      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

b.

акой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

b. Отравьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

Шаг 3: Проверьте связь между конечными устройствами.

a. Отправьте эхо-запрос с ПК A на ПК C. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

b. Запустите трассировку от ПК A к ПК C. Каков путь от ПК A до ПК C?

Вопросы на закрепление

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?

2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 20

Настройка Syslog и NTP

Топология

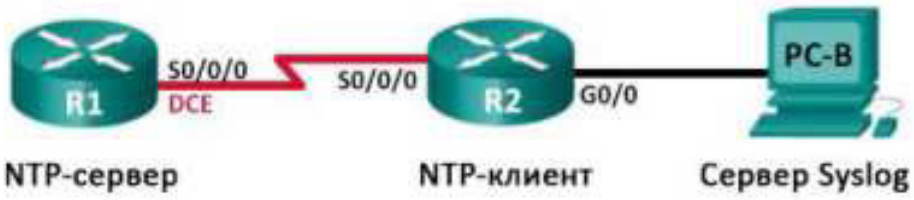


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
R2	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	G0/0	172.16.2.1	255.255.255.0	Недоступно
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка NTP Таблица

Часть 3. Настройка Syslog

Исходные данные/сценарий

Сообщения Syslog, создаваемые сетевыми устройствами, могут собираться и архивироваться на сервере Syslog. Эту информацию можно использовать для наблюдения, отладки и поиска и устранения неполадок. Администратор может настраивать место сохранения и отображения сообщений. Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP.

В этой лабораторной работе необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента Syslog и NTP. Приложение сервера Syslog, например Tftp32d или другая аналогичная программа, будет выполняться на ПК B. Кроме того, необходимо настроить уровень важности сообщений журнала, которые будут собираются и архивироваться на сервере Syslog.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 компьютер (с ОС Windows 7, Vista или XP или с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 необходимо настроить топологию сети и базовые параметры, например IP-адреса интерфейса, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имя устройства.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

g. Настройте ведение журнала состояния консоли на синхронный режим.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

i. Установите тактовую частоту **128000** для последовательного интерфейса DCE.

Шаг 4: Настройте маршрутизацию.

Включите на маршрутизаторах протокол OSPF с одной областью с идентификатором процесса 1. Добавьте все сети в процесс OSPF для области 0.

Шаг 5: Настройте ПК B.

Настройте IP-адрес и шлюз по умолчанию для ПК B согласно таблице адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Убедитесь, что все устройства могут отправлять эхо-запросы на каждое другое устройство в сети. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Шаг 7: Сохраните текущую конфигурацию в загрузочную.

Часть 2: Настройка NTP

В части 2 необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента NTP маршрутизатора R1. Необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

Шаг 1: Выведите на экран текущее время.

Введите команду **show clock** для отображения текущего времени на R1.

```
R1# show clock
*12:30:06.147 UTC Tue May 14 2013
```

Запишите отображаемые сведения о текущем времени в следующей таблице.

Дата	
Время	
Часовой пояс	

Шаг 2: Установите время.

С помощью команды **clock set** установите время на маршрутизаторе R1. Ниже приводится пример настройки даты и времени.

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul  5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54
UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by
console.
```

Примечание. Время можно также настроить с помощью команды **clock timezone** в режиме глобальной конфигурации. Для получения дополнительной информации о команде **clock timezone** посетите веб-сайт www.cisco.com и определите часовой пояс для вашего региона.

Шаг 3: Настройте главный сервер NTP.

Настройте маршрутизатор R1 в качестве главного сервера NTP с помощью команды **ntp master** *stratum-number* в режиме глобальной конфигурации. Значение stratum показывает в каком количестве переходов NTP от доверенного источника времени находится сервер. В этой лабораторной работе в качестве stratum данного сервера NTP используется число 5.

```
R1(config)# ntp master 5
```

Шаг 4: Настройте клиент NTP.

a. Введите команду **show clock** на маршрутизаторе R2. Запишите текущее время, отображаемое на маршрутизаторе R2, в следующей таблице.

Дата	
Время	
Часовой пояс	

b. Настройте R2 в качестве клиента NTP. Используйте команду **ntp server,** чтобы указать на IP-адрес или имя компьютера сервера NTP. Команда **ntp update-calendar** периодически обновляет календарь на основе времени NTP.

```
R2(config)# ntp server 10.1.1.1
R2(config)# ntp update-calendar
```

Шаг 5: Проверьте настройку NTP.

a. Используйте команду **show ntp associations,** чтобы проверить, что маршрутизатор R2 связан через NTP с маршрутизатором R1.

```
R2# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.1.1.1        127.127.1.1      5     11     64   177 11.312  -0.018  4.298
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

b. Введите команду **show clock** на маршрутизаторах R1 и R2 и сравните метку времени.

Примечание. Синхронизация метки времени на маршрутизаторе R2 с меткой времени на маршрутизаторе R1 может занять несколько минут.

```
R1# show clock
09:43:32.799 UTC Fri Jul 5 2013
R2# show clock
09:43:37.122 UTC Fri Jul 5 2013
```

Часть 3: Настройте Syslog

Сообщения Syslog от сетевых устройств могут собираться и архивироваться на сервере Syslog. В этой лабораторной работе в качестве программного обеспечения сервера Syslog используется Tftpd32. Администратор может настраивать типы сообщений, которые можно отправлять на сервер Syslog.

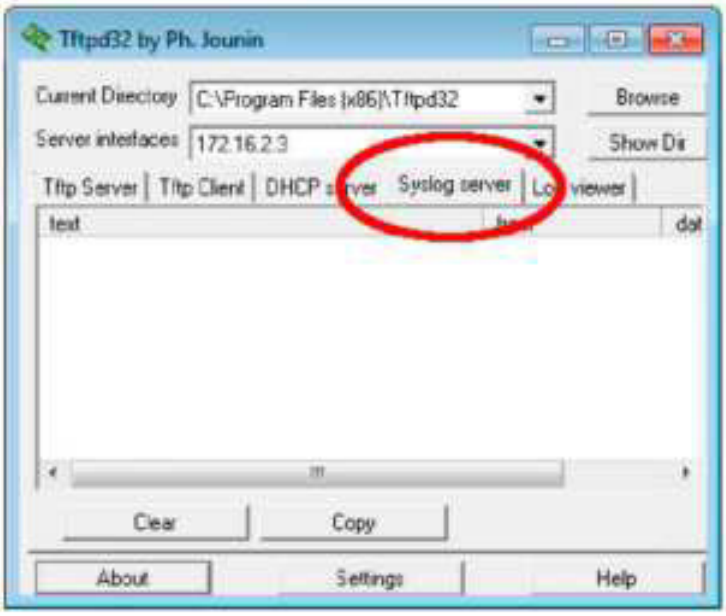
Шаг 1: (Дополнительно) Установите сервер Syslog.

Если сервер Syslog еще не установлен на компьютере, загрузите и установите последнюю версию сервера Syslog, например Tftpd32. Последнюю версию Tftpd32 можно найти по следующей ссылке:

http://tftpd32.jounin.net/

Шаг 2: Запустите сервер Syslog на компьютере ПК B.

После запуска приложения Tftpd32 перейдите на вкладку **Syslog server.**



Шаг 3: Убедитесь, что на маршрутизаторе R2 включена служба меток времени.

С помощью команды **show run** проверьте, что служба меток времени включена для журналирования на маршрутизаторе R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

Если служба меток времени не включена, используйте следующую команду, чтобы включить её.

```
R2(config)# service timestamps log datetime msec
```

Шаг 4: Настройте R2 для сохранения сообщений журнала на сервере Syslog.

Настройте R2 для отправки сообщений Syslog на сервер Syslog — ПК B. IP-адрес сервера Syslog ПК B — 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

Шаг 5: Выведите на экран параметры по умолчанию для журналирования.

Используйте команду **show logging,** чтобы вывести на экран параметры журналирования по умолчанию.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


        Console logging: level debugging, 47 messages logged, xml disabled,
                         filtering disabled
        Monitor logging: level debugging, 0 messages logged, xml disabled,
                         filtering disabled
        Buffer logging:  level debugging, 47 messages logged, xml disabled,
                        filtering disabled
        Exception Logging: size (4096 bytes)
        Count and timestamp logging messages: disabled
        Persistent logging: disabled

    No active filter modules.

        Trap logging: level informational, 49 message lines logged
            Logging to 172.16.2.3  (udp port 514, audit disabled,
                  link up),
                  6 message lines logged,
                  0 message lines rate-limited,
                  0 message lines dropped-by-MD,
                  xml disabled, sequence number disabled
                  filtering disabled
            Logging Source-Interface:       VRF Name:
```

Назовите IP-адрес сервера Syslog.

Какие протокол и порт использует сервер Syslog?

Какой уровень сообщений настроен?

Шаг 6: Настройте и проверьте результат настройки уровней важности для журналирования на маршрутизаторе R2.

a. Используйте команду **logging trap ?** для определения доступности различных уровней ловушек. При настройке уровня

сообщений, отправляемые на сервер Syslog, будут включать сообщения настроенного уровня и сообщение более низких уровней.

```
R2(config)# logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
```

Если введена команда **logging trap warnings,** сообщения с какими уровнями важности будут регистрироваться?

b. Укажите уровень важности для журналирования равный 4.

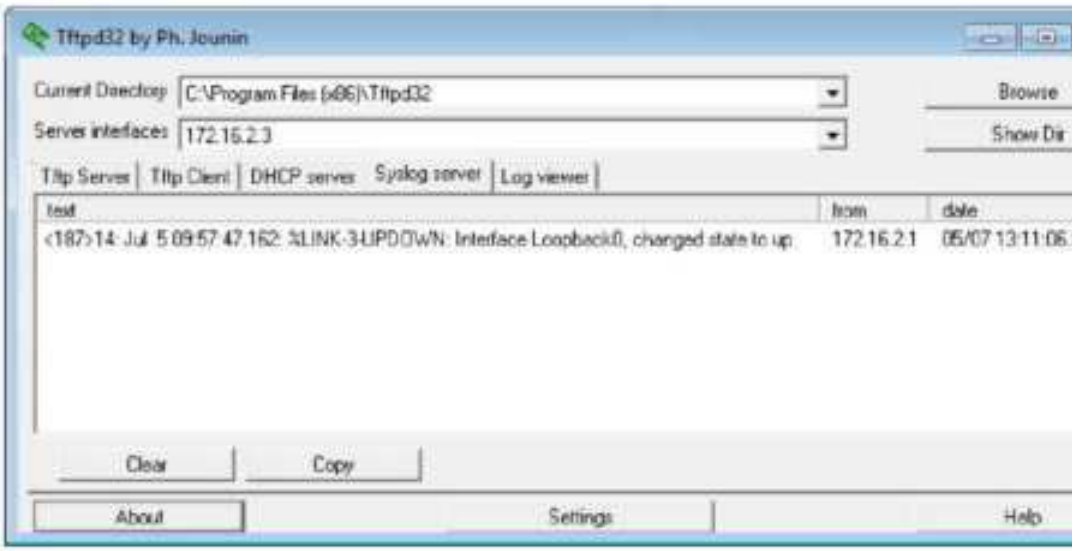
```
R2(config)# logging trap warnings
```

или

```
R2(config)# logging trap 4
```

c. Создайте интерфейс LoopbackO на маршрутизаторе R2 и просмотрите сообщения журнала как в окне терминала, так и в окне сервера Syslog на ПК B.

```
R2(config)# interface lo 0
R2(config-if)#
Jul  5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to
Jul  5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopb
changed state to up
```



d. Удалите интерфейс Loopback 0 на маршрутизаторе R2 и просмотрите сообщения журнала.

```
R2(config-if)# no interface lo 0
R2(config)#
Jul  5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
Jul  5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
```

Отображаются ли какие-либо сообщения на сервере Syslog при выборе уровня серьёзности 4? Если какие-либо сообщения журнала отображаются, объясните, какие сообщения отображаются и почему.

e. Укажите уровень важности для журналирования равный 6. или

```
R2(config)# logging trap informational
```

или

```
R2(config)# logging trap 6
```

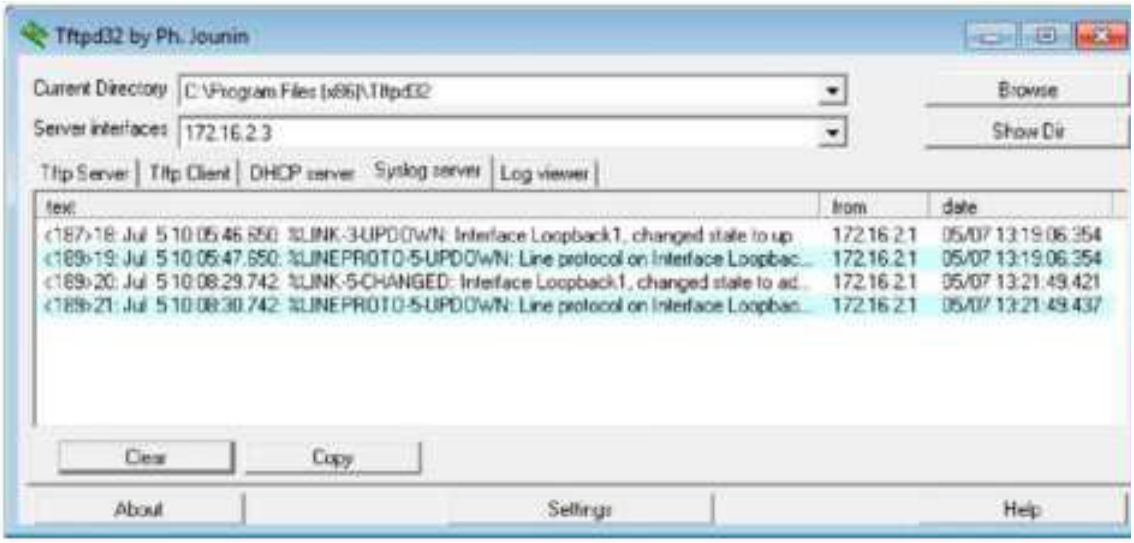
f. Удалите записи Syslog на ПК B. Нажмите кнопку **Clear** (Очистить) в диалоговом окне Tftpd32.

g. Создайте интерфейс Loopback 1 на маршрутизаторе R2.

```
R2(config)# interface lo 1
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

h. Удалите интерфейс Loopback 1 с маршрутизатора R2.

```
R2(config-if)# no interface lo 1
R2(config-if)#
Jul  5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to
administratively down
Jul  5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to down
```



i. Проанализируйте выходные данные сервера Syslog. Сравните эти результаты с результатами на уровне важности 4. Каковы ваши наблюдения?

Вопросы на закрепление

Какая проблема возникает при настройке слишком высокого (самый маленький номер) или слишком низкого (самый большой номер) уровня важности для Syslog?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 21

Настройка SNMP

Топология

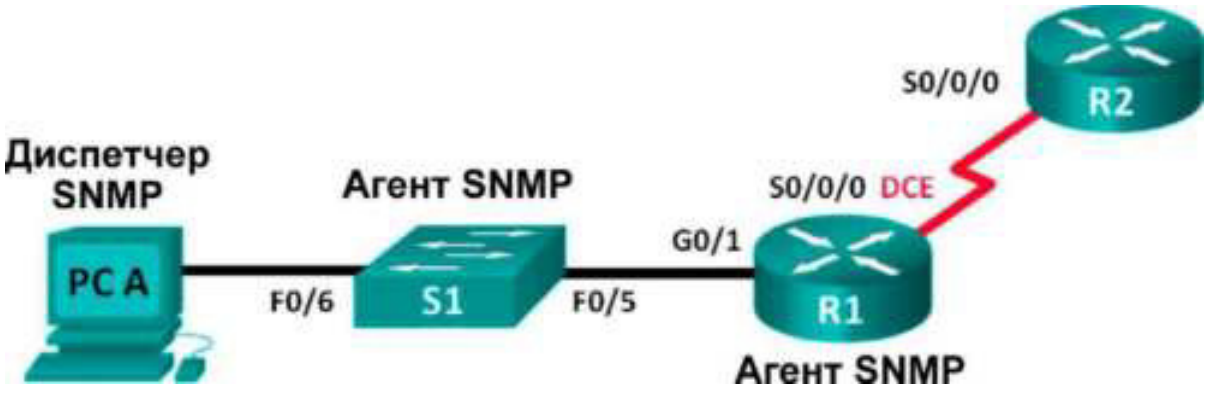


Таблица адресации

Устройство	Интерфейс	Р-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0	192.168.2.1	255.255.255.252	Недоступно
R2	S0/0/0	192.168.2.2	255.255.255.252	Недоступно
S1	VLAN 1	192.168.1.2	255.255.255.0	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств Часть 2. Настройка диспетчера и агентов SNMP

Часть 3. Преобразование кодов OID с использованием Cisco SNMP Object Navigator

Исходные данные/сценарий

Протокол SNMP (Simple Network Management Protocol — простой протокол управления сетями) — это протокол управления сетью и

стандарт IETF, который может использоваться как для мониторинга сети, так и для контроля клиентов в ней. SNMP может использоваться для получения и настройки переменных, связанных с состоянием и настройкой сетевых машин, таких как маршрутизаторы и коммутаторы, а также клиентские компьютеры сети. Диспетчер SNMP может опрашивать агенты SNMP для получения данных, либо данные могут автоматически отправляться на диспетчер SNMP путём настройки ловушек на агентах SNMP.

В этой лабораторной работе вы будете должны загрузить, установить и настроить программное обеспечение для управления SNMP с на компьютере ПК А. Вы также настроите маршрутизатор Cisco и коммутатор Cisco в качестве агентов SNMP. После получения сообщений с уведомлением SNMP от агента SNMP вы должны будете преобразовать коды MIB/ID объекта (OID), чтобы получить подробную информацию данных сообщений с помощью Cisco SNMP Object Navigator.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Примечание. Применение команд **snmp-server** в этой лабораторной работе приведёт к тому, что коммутатор Cisco 2960 сгенерирует сообщение с предупреждением при сохранении файла настройки в NVRAM. Чтобы избежать этого сообщения с предупреждением, убедитесь, что коммутатор использует шаблон **lanbase-routing.** Шаблон IOS контролируется диспетчером базы данных коммутатора (SDM). При изменении предпочтительного шаблона новый шаблон будет использоваться после перезагрузки, даже если настройка не сохраняется.

```
S1# show sdm prefer
```

Используйте следующие команды для назначения шаблона

```
S1# configure terminal
S1(config)# sdm prefer lanbase-routing
S1(config)# end
S1# reload
```

lanbase-routing в качестве шаблона SDM по умолчанию.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный);
- 1 ПК (с Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- 1 ПК (с Windows 7, Vista или XP с доступом к Интернету);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

- ПО для управления протоколом SNMP (PowerSNMP Free Manager компании Dart Communications или сервер Syslog SolarWinds Kiwi, ознакомительная версия с испытательным периодом 30 дней)

Часть 1: Построение сети и базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и сделать базовую настройку устройств.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте компьютер.

Шаг 3: Инициализируйте и перезагрузите коммутатор и маршрутизаторы при необходимости.Шаг 4: Произведите базовую настройку маршрутизаторов и коммутатора.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

c. Настройте IP-адреса в соответствии с таблицей адресации. (В этот раз не настраивайте интерфейс S0/0/0 маршрутизатора R1.)

d. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Настройте **logging synchronous,** чтобы сообщения от консоли не могли прерывать ввод команд.

g. Проверьте подключения между устройствами локальной сети с помощью команды ping.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Настройка диспетчера и агентов SNMP

В части 2 вы должны будете установить ПО для управления SNMP и настроить его на ПК A, а также

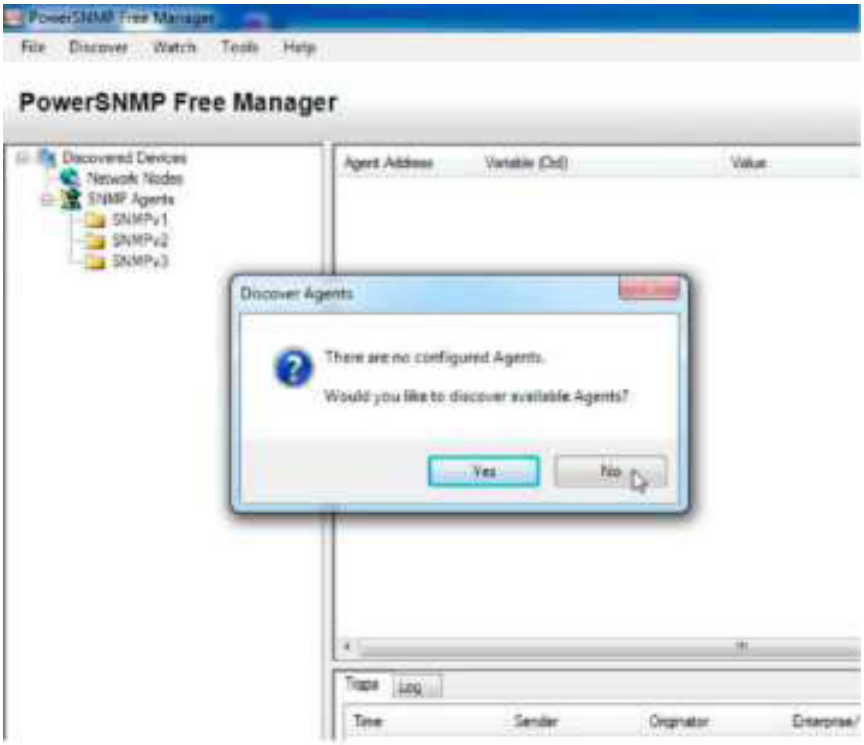
настроить R1 и S1 в качестве агентов SNMP.

Шаг 1: Установите программу управления SNMP.

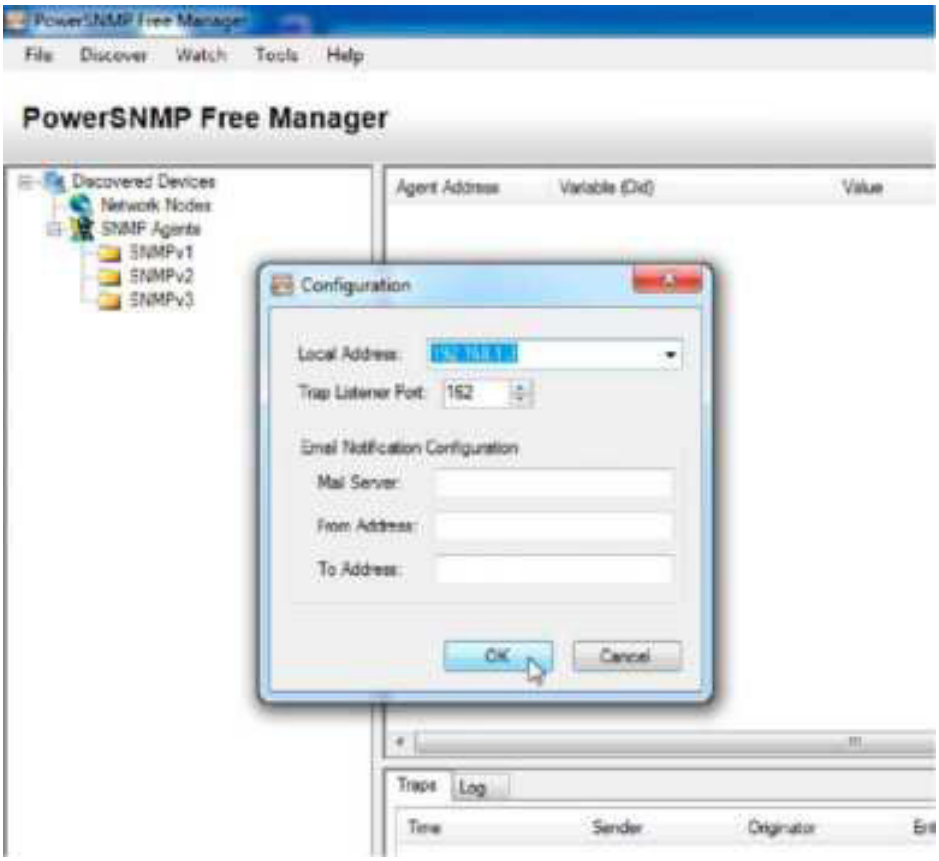
a. Загрузите и установите бесплатное приложение PowerSNMP Free Manager от компании Dart Communications, перейдя по следующему URL-адресу: http://www.dart.com/snmp-free-manager.aspx.

b. Запустите программу PowerSNMP Free Manager.

c. При отображении запроса на поиск доступных агентов SNMP нажмите кнопку **No** (Нет). Поиск агентов SNMP осуществляется после настройки SNMP на маршрутизаторе R1. PowerSNMP Free Manager поддерживает SNMP версии 1, 2, и 3. В данной лабораторной работе используется SNMPv2.



d. Во всплывающем окне настройки (если всплывающее окно не отображается, перейдите во вкладку Tools > Configuration (Инструменты > Настройка)) назначьте локальный IP-адрес для прослушивания на 192.168.1.3 и нажмите OK.



Примечание. При отображении запроса на поиск доступных агентов SNMP нажмите кнопку **No** и перейдите к следующему части данной лабораторной работы.

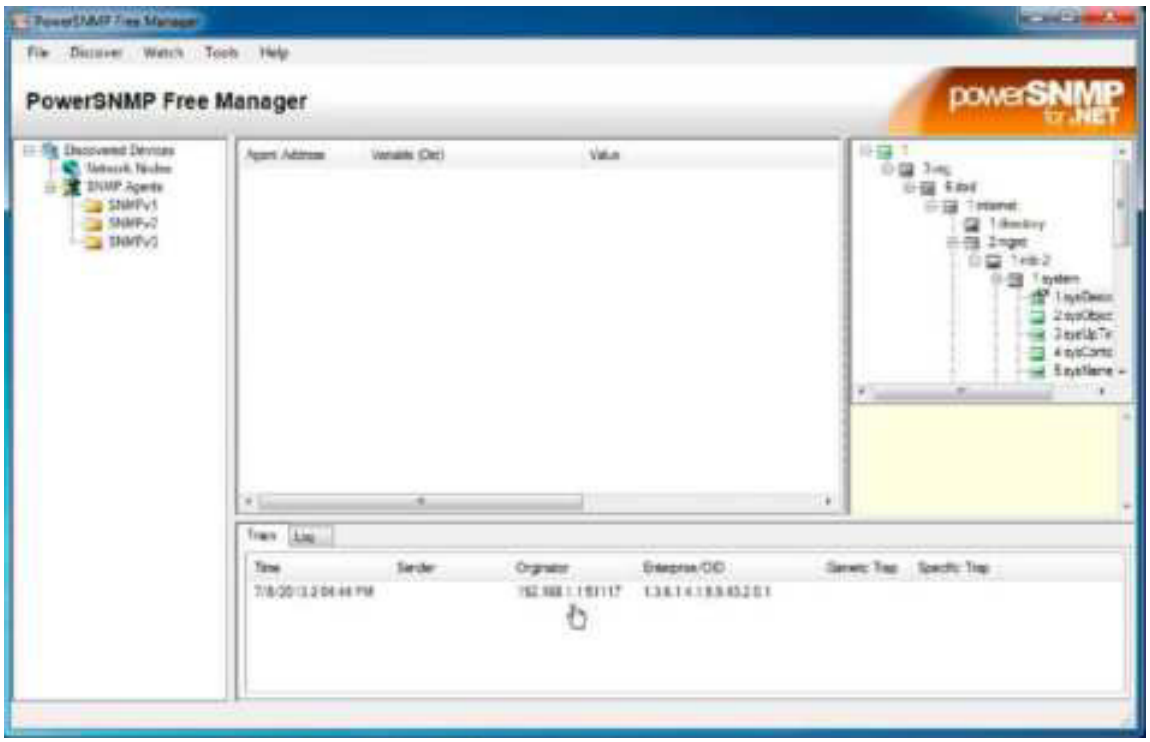
Шаг 2: Настройте агент SNMP.

a. На маршрутизаторе R1 введите следующие команды в режиме глобальной конфигурации, чтобы настроить его в качестве агента SNMP. В строке 1 ниже строкой сообщества SNMP является **ciscolab** с правами только для чтения, а именованный список доступа SNMP_ACL определяет, какие узлы могут получать данные SNMP от маршрутизатора R1. В строках 2 и 3 команды местоположения и контактной информации агента SNMP предоставляют описательную

контактную информацию. В строке 4 указаны IP-адрес узла, который будет получать уведомления SNMP, версия SNMP и строка сообщества. Строка 5 включает все ловушки SNMP по умолчанию; строки 6 и 7 создают именованный список контроля доступа, определяющий, каким узлам разрешено получение информации SNMP от маршрутизатора.

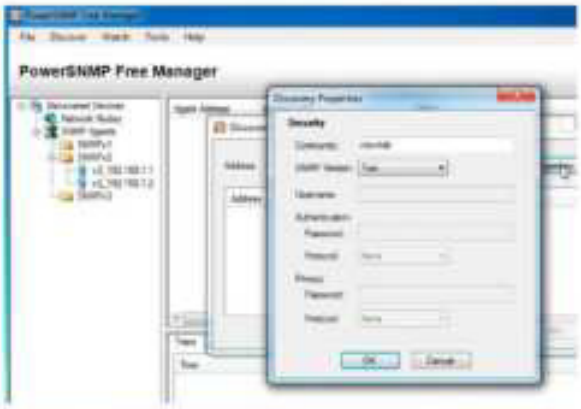
```
R1(config)# snmp-server community ciscolab ro SNMP_ACL
R1(config)# snmp-server location snmp_manager
R1(config)# snmp-server contact ciscolab_admin
R1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

b.На этом этапе можно заметить, что PowerSNMP Free Manager получает уведомления от маршрутизатора R1. Если уведомления не приходят, вы можете попытаться принудительно установить отправку уведомления SNMP, введя команду **copy run start** на маршрутизаторе R1. Если вам не удаётся это сделать, перейдите к следующему шагу.

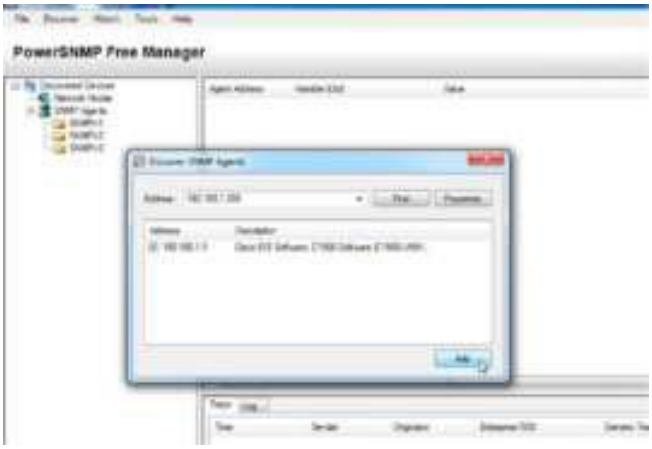


Шаг 3: Выполните обнаружение агентов SNMP.

а. В программе PowerSNMP Free Manager на компьютере ПК А откройте окно **Discover > SNMP Agents** (Обнаружение > Агенты SNMP). Введите IP-адрес **192.168.1.255.** В том же окне щёлкните **Properties** (Свойства) и выберите в поле «Community» (Сообщество) параметр **ciscolab,** а в поле «SNMP Version» параметр **Two** (2), затем щёлкните **OK.** Теперь можете нажать **Find** (Найти) для обнаружения всех агентов SNMP в сети 192.168.1.0. Программа PowerSNMP Free Manager должна обнаружить маршрутизатор R1 по адресу 192.168.1.1. Установите флажок и щёлкните **Add** (Добавить), чтобы добавить маршрутизатор R1 в качестве агента SNMP


PowerSNMP Free Manager


PowerSNMP Free Manager


PowerSNMP Free Manager

b. В программе PowerSNMP Free Manager маршрутизатор R1 добавляется в список доступных агентов SNMPv2.

c. Настройте коммутатор S1 в качестве агента SNMP. Вы можете использовать те же команды **snmp server,** которые вы использовали для настройки R1.

d. После завершения настройки коммутатора S1 уведомления SNMP с адреса 192.168.1.2 отображаются в окне «Traps» (Прерывания) программы PowerSNMP Free Manager. В программе PowerSNMP Free Manager добавьте коммутатор S1 в качестве агента SNMP с помощью тех же действий, которые вы выполнили для обнаружения R1.

Часть 3: Преобразование кодов OID с использованием Cisco SNMP Object Navigator

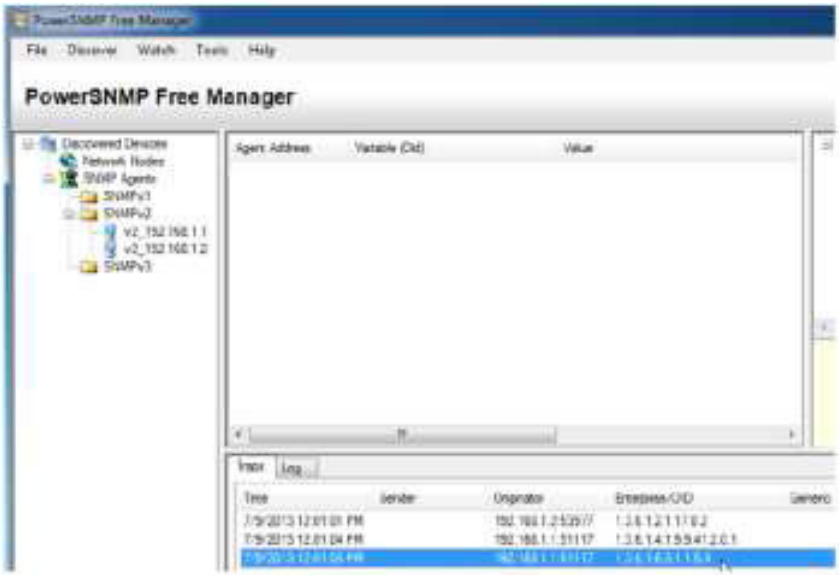
В части 3 принудительно установите отправку уведомлений SNMP на диспетчер SNMP, размещенный на компьютере ПК A. После этого вы должны будете преобразовать полученные коды OID в имена, чтобы прочитать сообщения. Коды MIB/OID можно легко преобразовать с помощью средства Cisco SNMP Object Navigator на веб-сайте http://www.cisco.com.

Шаг 1: Удалите текущие сообщения SNMP.

В программе PowerSNMP Free Manager щёлкните правой кнопкой мыши окно **Traps** (Ловушки) и выберите **Clear** (Очистить) для удаления сообщений SNMP.

Шаг 2: Создайте ловушку и уведомление SNMP.

На маршрутизаторе R1 настройте интерфейс S0/0/0 согласно таблице адресации в начале данной лабораторной работы. Перейдите в режим глобальной конфигурации и разрешите интерфейсу отправлять уведомления, создаваемые в случае ловушки SNMP, на диспетчер SNMP на компьютере ПК A. Запомните коды организации/OID, отображаемые в окне ловушек.



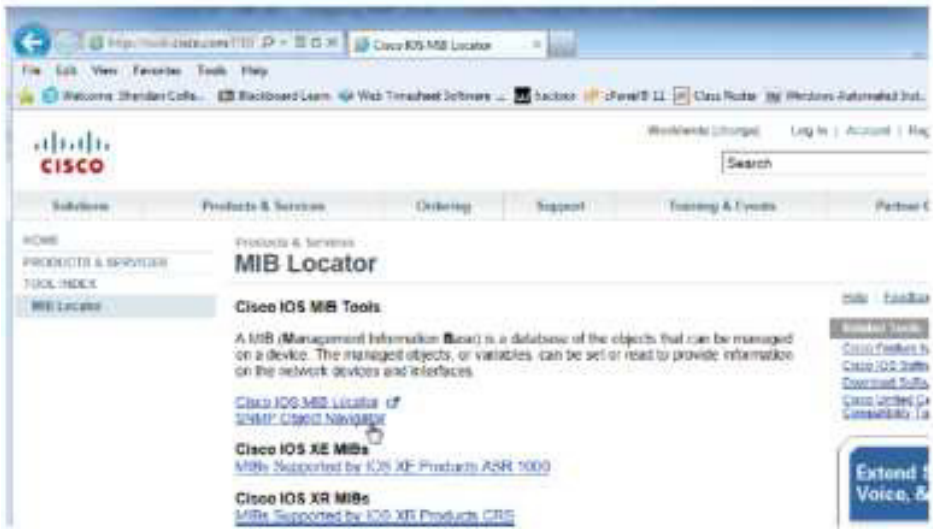
Шаг 3: Декодируйте сообщения MIB/OID SNMP.

На компьютере с доступом к Интернету откройте веб-браузер и перейдите на веб-сайт http://www. cisco. com.

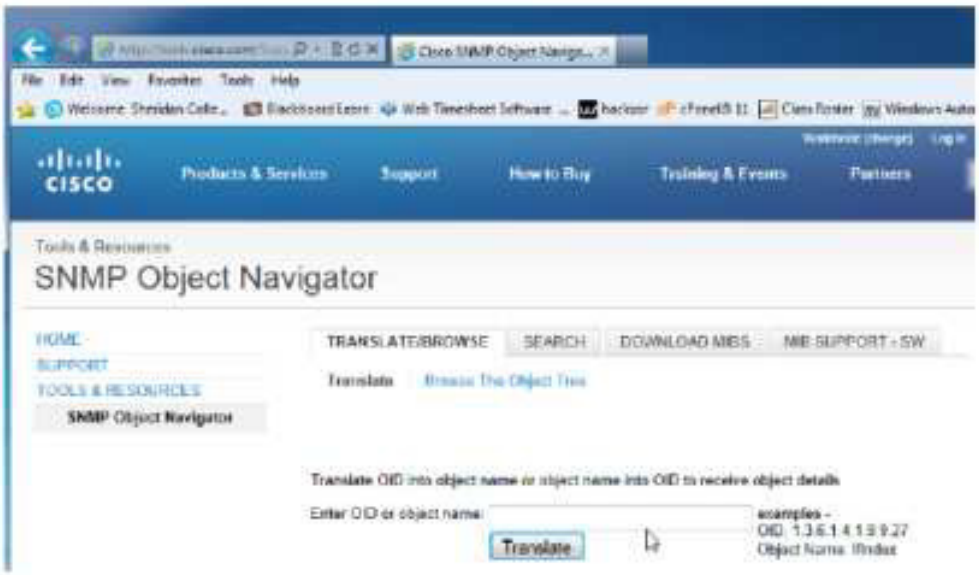
a. С помощью средства поиска в верхней части окна выполните поиск **SNMP Object Navigator.**

b. **Выберите в результатах** SNMP Object Navigator MIB Download MIBs OID OIDs.

c. **Перейдите на страницу** MIB Locator. **Выберите** SNMP Object Navigator.



d.На странице **SNMP Object Navigator** выполните декодирование кода OID из программы PowerSNMP Free Manager, который был создан в действии 2 части 3 данной лабораторной работы. Введите код OID и выберите **Translate** (Преобразовать).



e. Запишите коды OID и соответствующие им сообщения, полученные в результате преобразования, ниже.

Вопросы на закрепление

1. Перечислите несколько потенциальных преимуществ наблюдения за сетью с помощью протокола SNMP.

2. Почему при работе с SNMPv2 предпочтительно использовать исключительно доступ с правами только для чтения?Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательн ый интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	=Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 22

Сбор и анализ данных NetFlow. Программное обеспечение системы сбора данных и анализатора NetFlow

Топология

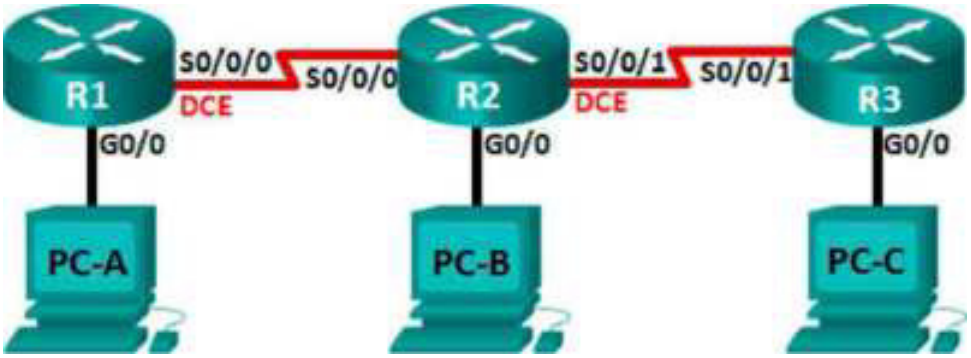


Таблица адресации

Устройства	**Интерфейс**	**IP-адрес**	**Шлюз по умолчанию**
R1	G0/0	192.168.1.1/24	Недоступно
	S0/0/0 (DCE)	192.168.12.1/30	Недоступно
R2	G0/0	192.168.2.1/24	Недоступно
	S0/0/0	192.168.12.2/30	Недоступно
	S0/0/1 (DCE)	192.168.23.1/30	Недоступно
R3	G0/0	192.168.3.1/24	Недоступно
	S0/0/1	192.168.23.2/30	Недоступно
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка NetFlow на маршрутизаторе

Часть 3. Анализ NetFlow с помощью интерфейса командной строки

Часть 4. Изучение ПО сбора данных и анализатора NetFlow

Исходные данные/сценарий

NetFlow — это технология Cisco IOS, предоставляющая статистические данные о пакетах, проходящих через маршрутизатор или многоуровневый коммутатор Cisco. NetFlow обеспечивает контроль сети и безопасности, планирование сетевых ресурсов, анализ трафика и учёт IP. Важно не путать назначение и результаты NetFlow с назначением и результатами оборудования и программного обеспечения для сбора пакетов. Средства сбора пакетов записывают всю входящую и исходящую информацию сетевого устройства для последующего анализа, в то время как NetFlow собирает только определённую статистическую информацию.

Flexible NetFlow — это новейшая версия технологии NetFlow, которая расширяет возможности первоначального протокола NetFlow, позволяя настраивать параметры анализа трафика. Flexible NetFlow использует формат экспорта версии 9. Начиная с Cisco IOS версии 15.1, поддерживаются многие полезные команды Flexible NetFlow.

В этой лабораторной работе вам потребуется настроить NetFlow для сбора данных входящих и исходящих пакетов. С помощью команды **show** вы сможете проверить, что NetFlow находится в рабочем состоянии и осуществляет сбор статистических данных. Вы также рассмотрите доступные варианты ПО сборщика данных и анализатора NetFlow.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в

сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и сделать базовую настройку устройств. **Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.**

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

d. Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и включите запрос пароля при подключении.

e. Зашифруйте пароли.

f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

g. Настройте **logging synchronous** на линии консоли.

h. Настройте тактовую частоту на всех последовательных интерфейсах DCE на **128000.**

i. Настройте IP-адреса, как указано в таблице адресации.

j. Настройте OSPF с использованием идентификатора процесса 1 и объявите все сети. Интерфейсы Ethernet должны быть пассивными.

k. Создайте учётную запись в локальной базе данных на маршрутизаторе R3 с именем пользователя **admin** и паролем **cisco** и с уровнем привилегий **15.**

I. На маршрутизаторе R3 включите службу HTTP и настройте проверку подлинности пользователей HTTP с помощью локальной базы данных.

m. Скопируйте текущую конфигурацию в файл загрузочной конфигурации. **Шаг 4: Настройте узлы.**

Шаг 5: Проверьте связь между конечными устройствами.

Все устройства должны иметь возможность отправлять эхо-запросы другим устройствам в топологии. При необходимости устраните неисправности, пока связь между конечными устройствами не будет установлена.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра на ПК.

Часть 2: Настройка NetFlow на маршрутизаторе

В части 2 вы должны будете настроить NetFlow на маршрутизаторе R2. NetFlow собирает весь входящий и исходящий трафик на последовательных интерфейсах R2 и экспортирует данные на сборщик данных NetFlow — ПК B. Для экспорта данных на сборщик NetFlow будет использоваться Flexible NetFlow версии 9.

Шаг 1: Настройте сбор данных NetFlow.

Настройте сбор данных NetFlow на обоих последовательных интерфейсах. Выполните сбор данных из входящих и исходящих пакетов.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Шаг 2: Настройте экспорт данных NetFlow.

С помощью команды **ip flow-export destination** определите IP-адрес и порт UDP сборщика данных NetFlow, на который маршрутизатор должен экспортировать данные NetFlow. Для данной настройки будет использоваться номер порта UDP 9996

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Шаг 3: Настройте версию экспорта NetFlow.

Маршрутизаторы Cisco под управлением IOS 15.1 поддерживают NetFlow версии 1, 5 и 9. Версия 9 — это наиболее универсальный формат экспорта данных, однако он не совместим с более ранними версиями. Для установки версии NetFlow используйте команду **ip flow-export version.**

```
R2(config)# ip flow-export version 9
```

Шаг 4: Выполните проверку конфигурации NetFlow.

a. Введите команду **show ip flow interface** для просмотра сведений об интерфейсе сбора данных NetFlow.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

b. Введите команду **show ip flow export** для просмотра сведений об экспорте данных NetFlow.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.3 (9996)
  Version 9 flow records
  388 flows exported in 63 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Часть 3: Анализ NetFlow с помощью интерфейса командной строки

В части 3 вы должны будете генерировать трафик данных между маршрутизаторами R1 и R3 для

наблюдения за работой технологии NetFlow.

Шаг 1: Создайте трафик данных между маршрутизаторами R1 и R3.

c. Подключитесь по Telnet от маршрутизатора R1 к маршрутизатору R3 с использованием IP-адреса 192.168.3.1. Введите пароль **cisco** для перехода в пользовательский режим. Введите пароль **class** для включения глобального режима ввода. Введите команду **show run,** чтобы создать трафик Telnet. Не закрывайте текущий сеанс Telnet.

d. На маршрутизаторе R3 введите команду **ping 192.168.1.1 repeat 1000,** чтобы отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. Будет создан трафик ICMP через маршрутизатор R2.

c. На компьютере ПК A перейдите к маршрутизатору R3, используя IP-адрес 192.168.3.1. Войдите в систему с именем пользователя **admin** и паролем **cisco.** После входа в маршрутизатор R3 оставьте браузер открытым.

Примечание. Убедитесь, что в браузере отключено блокирование всплывающих окон.

Шаг 2: Выведите на экран сводную статистику NetFlow.

На маршрутизаторе R2 введите команду **show ip cache flow,** чтобы отобразить изменения в сводных данных NetFlow, включая распределение размеров пакета, информацию о потоках IP, записанные протоколы и активность интерфейса. Теперь протоколы отображают сводные данные.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
  1546 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           4       0.0        27    43      0.2       5.0      15.7
TCP-WWW            104       0.2        14   275      3.4       2.1       1.5
ICMP                 4       0.0      1000   100      8.8      27.9      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Total:             112       0.2        50   146     12.5       3.1       2.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    43
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    40
```

Шаг 3: Завершите сеансы Telnet и закройте браузер.

a. Введите команду **exit** на маршрутизаторе R1, чтобы отключить сеанс связи по Telnet с маршрутизатором R3.

b. Закройте сеанс браузера на компьютере ПК A.

Шаг 4: Удалите статистику NetFlow.

a. На маршрутизаторе R2 введите команду **clear ip flow stats,** чтобы удалить статистику NetFlow.

```
R2# clear ip flow stats
```

b.Повторно введите команду **show ip cache flow,** чтобы убедиться, что статистика NetFlow сброшена. Обратите внимание: даже несмотря на то, что вы больше не создаёте данные с помощью маршрутизатора R2, они по-прежнему принимаются NetFlow. В приведенном ниже примере адрес назначения для данного трафика — групповой адрес 224.0.0.5, это данные LSA OSPF.

```
R2# show ip cache flow
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 2 added
  1172 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:09:48
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IP-other             2       0.0       193    79      0.6    1794.8       5.7
Total:               2       0.0       193    79      0.6    1794.8       5.7


SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    33
```

Часть 4: Изучение ПО сборщика данных и анализатора NetFlow

Программное обеспечение сборщика данных и анализатора NetFlow предоставляют многие производители. Некоторые программы распространяются бесплатно, другие — нет. По следующему URL-адресу размещена веб-страница с обзором некоторых бесплатных программ NetFlow:

http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking solutions products genericco ntent0900aecd805ff72b.html

Просмотрите эту веб-страницу, чтобы ознакомиться с некоторыми из доступных программных продуктов сборщика данных и анализатора NetFlow.

Вопросы на закрепление

1. В чём заключается назначение ПО сборщика данных NetFlow?

2. В чём заключается назначение программного анализатора NetFlow?

3. Перечислите семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 23

Инструментарий сетевого администратора для наблюдения

Итак, что в принципе, должен делать (уметь делать) системный администратор:

Устанавливать/обновлять/удалять ПО

Настройку ПО

Планировать работы

Документировать

Мониторить состояние ИТ-систем

Диагностировать и поддерживать ИТ-системы

Резервное копирование/архивацию ПО и данных

Для всего этого есть немало различного ПО, постараемся описать все самое необходимое.

1 Окружение (среда)

С чего начинается работа системного администратора — с выбора удобного окружения. Это не просторный светлый офис и удобный стул, хотя это немаловажно, а выбор операционной системы. Мои коллеги работают на Mac OS X, Windows и Ubuntu. После многих проб и экспериментов с дистрибутивами и разными оболочками рабочего стола (Debian, Kubuntu, Fedora Gnome/Cinnamon) я остановился на Ubuntu 12.04 (Unity). Я просто освоился и привык к Unity, сейчас она мне кажется логичной и достаточно удобной оболочкой PC. Основное требование для админа это стабильность и простота. Не хочу ни с кем спорить, но именно так себя зарекомендовал Ubuntu.

Подробно описывать средства для планирования документирования я,пожалуй, не буду. Отмечу, что для документирования мне хватает блокнота (Gedit) и Libre Office ну и Google Docs для совместного использования доков. Все самые полезные заметки и документы мы храним в wiki. Для учета рабочего времени и контроля выполнения задач мы используем Redmine.

Конечно же, необходимы средства для коммуникации с коллегами и клиентами. Обычно это e-mail и Skype ну и телефон. Для планирования я использую Google Calendar, любое другое средство будет одинаково хорошим, если Вы будете на самом деле им пользоваться, например ежедневник.

Так или иначе очень много приходится работать в консоли, локально или на удаленных серверах. Поэтому, наиболее важные вещи в повседневной работе администратора *nix это утилиты командной строки.

2 Утилиты командной строки

Чаще всего приходится работать с текстом (конфиги, логи, руководства и т.п.), поэтому начнем с текстовых редакторов и прочих средств для манипуляций с текстом и строками:

vi/vim — этот редактор незаменимый инструмент любого администратора,

поскольку его можно найти практически на любом сервере (на любом

юниксе) и если вы до сих пор первым делом когда он открывается тут же

выходите из него по ctrl+z, то я настоятельно рекомендую вам хотя бы

прочитать в man vim как правильно нужно это делать.

nano — самый простенький редактор, поставляется по-умолчанию в

Debian/Ubuntu.

mcedit — для любителей mc и синих экранов, не самых плохой вариант, достаточно прост и удобен.

cat — concatinate — изначально инструмент для объединения файлов, но чаще используется для вывода содержимого файла, а также для вставки строк в файл.

tail — по-умолчанию выводит последние 10 строк файла, можно

использовать для слежения за логом (с ключом -f)

wc — считает строки слова и количество байт в файле

head — как и tail выводит 10 строк файла, но как наверное понятно из

названия, с начала файла.

grep — самый незаменимый инструмент для фильтрации текстового вывода или просто для поиска нужной строки в файлах.

sed — stream editor — очень полезен для автоматизации рутинных задач, замена строк в файлах (правка конфигов), удаление строк, вывод содержимого по маске и т.д.

awk/gawk — очень мощная утилита (на самом деле AWK — целый язык программирования), которая помогает парсить файлы и манипулировать выводом строк и еще много чего.

Информацию о всех перечисленный утилитах можно почерпнуть в man. Кстати, о man:

man — доступ к справочным страницам — это то, без чего наверное не обходится ни один рабочий день юникс-администратора. Если вы начинающий специалист, то обязательно начните с ввода man man в командной строке.

Список можно продолжать, долго продолжать, утилит на самом деле очень много. Но пока остановимся на этом и посмотрим, что можно сделать полезного с помощью awk, wc, cat и grep, почитав немного man.3

Немного практики

Чем же все таки полезны на практике перечисленные утилиты, попробую показать на примере парсинга логов.

Есть лог-файл apache (access.log) в следующем формате: 1.2.3.4 - - [12/May/2014:03:08:55 +0400] "GET /shop/goods-list HTTP/1.1" 200 1691 "http://example.ru/shop/goods-list" "Mozilla/5.0 (Windows NT 6.2; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0"

Напишем простой скрипт для подсчета процента успешно обработанных запросов.

```
#!/bin/bash

SUM=`wc -l access.log` # Подсчитаем количество строк в файле

OK=`cat access.log | awk '{print $9}' | grep 200 | wc -l` # Подсчитаем сколько
строк с кодом "200"

awk -v SUM="$SUM" -v OK="$OK" '
BEGIN {
printf "Passed: %3.2f%%\n", OK / SUM * 100
exit
}'
```

Получим примерно такой вывод: Passed: 93.62%

И еще несколько полезных примеров:

Подсчитаем объем переданных данных за час, предшествующий текущему

```
cat access.log | grep `date +%H:%M -d "-1 hour"` | awk '{ total += $10
```

```
END { print total/1024/1024 FS"MB" }'
```

Вычислим общий объем переданных данных

```
awk '{ total += $10 } END { print total/1024/1024 FS"MB" }'
```

```
access.log
```

Вычислим среднее время обработки запроса

```
#!/bin/bash

COUNT=`wc -l access.log`

SUM=`cat access.log | awk '{ total += $16 } END { print total }' `

awk -v COUNT="$COUNT" -v SUM="$SUM" '

BEGIN {

printf "Average req-time %3.2fs\n", SUM / COUNT

exit

}'
```

4 Диагностика загрузки системы

Чтобы понять насколько загружен сервер есть несколько утилит, прежде всего можно оценить загрузку по показателю load average, на Хабре уже писали что это показатель средней загруженности системы выражающийся в числе блокирующих процессов ожидающих получения ресурсов, за 1 минуту, 5 минут и 15 минут соответственно.

Первое, что поможет оценить текущую загруженность сервера и увидеть какие же процессы в данный больше нагружают сервер — top или htop

top — отображение процессов linux — кроме этого отображает uptime, load average, число выполняющихся задач и тредов. Показатели процессора (в процентном соотношении):

— **us** — время потраченное на выполнение пользовательских без изменения приоритета обработки (un-nice),

— **sy** — время потраченное на выполнение системных (kernel) процессов,

— **ni** — время потраченное на выполнение пользовательских с изменением приоритета обработки (nice),

— **wa** — время ожидания ввода/вывода (дисковой подсистемы),

— **hi** — время на обработку аппаратных прерываний,

— **si** — время на обработку софтварных прерываний,

— **st** — время «украденное» гипервизором для обработки задач на другой виртуальной машине — актуально для виртуальных машин (VPS/VDS) и полезно для оценки честности хостера, если этот показатель велик, то ваш провайдер нагло оверселлит.

Также top покажет вам сколько в целом потребляется памяти и для чего (процессы, кеши, буфферы), а также покажет сколько потребляет каждый процесс:

— **VIRT** — отображает сколько в целом памяти использует процесс включая код, данные, общие библиотеки, а также страницы памяти сброшенные в своп и страницы памяти которые были зарезервированы но не использованы,

— **RES** — размер резидентной памяти — текущее количество оперативной памяти (без свопа) используемой процессом,

— **SHR** — размер разделяемой памяти — текущее количество оперативной памяти доступной для процесса, как правило, не вся эта память резидентная. Это число просто отображает, сколько памяти может быть разделено с другими процессами.

Кроме отображения показателей использования ресурсов системы top также используется для манипуляций над процессами, можно послать сигнал завершения процессу либо изменить его приоритет (nice).

htop — более цветастая версия top — обладает всеми теми же возможностями, что и top, но имеет более дружественный интерфейс (позволяет прокручивать список процессов как вертикально так и горизонтально), а также умеет вызывать lsof, strace и ltrace для выбранного процесса (о них позже расскажем подробней).

Чтобы оценить нагрузку на дисковую подсистему ввода/вывода можно воспользоваться утилитой iotop:

iotop — top-подобная утилита для мониторинга нагрузки на диск, выводит таблицу процессов с текущими показателями использования дискового ввода/вывода, такими как:

— PRIO — приоритет процесса,

— DISK READ — чтение с диска Байт/сек,

— DISK WRITE — запись на диск Байт/сек,

— SWAPIN — время (в процентном соотношении) потраченное процессом на свопинг,

— IO — время (в процентном соотношении) потраченное процессом на ожидание ввода/вывода.

Дополнительно выводится информация о суммарном битрейте чтения/записи дисковой подсистемы.

vmstat — выводит суммарную информацию о процессах, памяти, вводе/выводе, активности процессора и дисков. В отличии от iotop не требует привилегий суперпользователя.

5 Диагностика сбоев программ, troubleshooting

Бывают ситуации когда программа или демон работают не так как вы ожидаете, либо по непонятным причинам сбоят. Когда все логи просмотрены (или когда нет логов), все конфиги проверены и документация перечитана (если есть конечно), на помощь придут утилиты трассировки системных вызовов stace, ltrace, а также lsof покажет список открытых файлов: **strace** — утилита позволяет перехватывать системные вызовы и сигналызапускаемого процесса либо уже запущенного процесса по его PID. Вывод можно фильтровать, например выводить только вызовы open() или select(). Если вызов возвращает не отрицательное значение, то все хорошо, если выдается например:

open("/foo/bar", O_RDONLY) = -1 ENOENT (No such file or directory), то из этого можно понять что приложение пытается открыть несуществующий файл. Также иногда случается, что некорректно выставлены права на файл. Еще например не запускается виртуальная машина, потому, что гипервизор не может выделить ей нужное количество оперативной памяти. Strace в таких ситуациях здорово помогает.

Если вам просто интересно посмотреть, как работает тот или иной сервис, какие он использует системный вызовы, то stace — ваш друг. Например хотите узнать чем принципиально отличается Apache от Nginx, просто возьмите и посмотрите.

ltrace — утилита для трассировки библиотечных вызовов — очень похожа на strace, но перехватывает только вызовы к динамическим библиотекам.

ldd — если натравить ее на программку покажет какие программа использует библиотеки. Полезно если нужно перенести программу в chroot. **lsof** — выводит список открытых файлов с указанием, по умолчанию выводит все подряд. Может выводить список для конкретного процесса по PID (достаточно удобный вывод в htop), для пользователя по UID, или например какие процессы используют тот или иной файл.

Основная литература:

Кузин, А. В. Компьютерные сети : учебное пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2023. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2047215 (дата обращения: 20.06.2023). – Режим доступа: по подписке.

Дополнительная литература:

Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2023. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1921406 (дата обращения: 20.06.2023). – Режим доступа: по подписке.