Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Документ подписан электронной цифровой подписью.

Сертификат: 5f619c548405aee0351d9e267d24ef84c4c1cce0
Дата действия: с 25 марта 2021 г. 11:10:18 по 25 марта 2026 г. 11:10:18

Шаталов Олег Александрович
2021.06.03 12:03:11 +03'00'

Рассмотрено
предметно-цикловой комиссией
Протокол заседания № _____
От «____»_____ 20__ г.
Председатель цикловой комиссии
_____/ Третьяк И.Ю.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

ПМ.01. Выполнение работ по проектированию сетевой инфраструктуры

МДК 01.02 «Организация, принципы построения и функционирования компьютерных сетей»

09.02.06 «Сетевое и системное администрирование»

Разработчик:
Сивокобыленко Н.В. преподаватель информационных технологий и ИКТ
ОГАПОУ БИК

Белгород 2020

Пояснительная записка

Профессиональный модуль 01 «Выполнение работ по проектированию сетевой инфраструктуры» является специальной, формирующей базовые умения для получения выпускником профессиональных умений.

Методические указания по выполнению лабораторных работ разработаны в соответствии с рабочей программой МДК 01.02 «Организация, принципы построения и функционирования компьютерных сетей», соответствуют требованиям Федерального государственного образовательного стандарта по специальностям среднего профессионального образования.

Целью методических указаний по выполнению лабораторных работ является организация и управление работой студентов на лабораторных занятиях при изучении данного модуля.

Методические указания по выполнению лабораторных работ содержат общие положения, тематику лабораторных работ, содержание лабораторных работ и требования к оформлению отчетов.

Методические указания к каждой лабораторной работе включают в себя следующие элементы: название темы, цель занятия, теоретическую часть, практическую часть (указания по выполнению) и контрольные вопросы.

Методические указания содержат лабораторные работы, которые обеспечивают формирование базовых умений и навыков владения основными методологиями процессов разработки программного обеспечения, использования методов для получения кода с заданной функциональностью и степенью качества, раскрывают принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного обеспечения.

В лабораторных работах, приведенных в данных методических рекомендациях, содержатся как задания с подробными указаниями к выполнению, так и задания без алгоритма работы.

Методические рекомендации предназначены для студентов очной формы обучения специальности 09.02.06 «Сетевое и сестемное администрирование».

Методические рекомендации направлены на повышение мотивации учащихся к изучению профессионального модуля «Выполнение работ по проектированию сетевой инфраструктуры», развитие гибкого логического и пространственного мышления учащихся, развитие профессиональных компетенций учащейся молодежи.

Тематика лабораторных работ

№	Темы	Кол-во часов
1	Лабораторная работа № 1 – 2. Развертывание коммутируемой сети с резервными каналами	4
2	Лабораторная работа № 3 – 4. Настройка Rapid PVST+, PortFast и BPDU Guard	4
3	Лабораторная работа № 5 – 6. Настройка протокола GLBP	4
4	Лабораторная работа № 7 – 8. Определение типовых ошибок конфигурации STP	4
5	Лабораторная работа № 9 – 10.Настройка EtherChannel	4
6	Лабораторная работа № 11 – 12. Поиск и устранение неполадок в работе EtherChannel	4
7	Лабораторная работа № 13 – 14. Агрегирование каналов	4
8	Лабораторная работа № 15 – 16. Настройка беспроводного маршрутизатора и клиента	4
9	Лабораторная работа №17 – 18. Настройка базового протокола OSPFv2 для одной области	4
10	Лабораторная работа № 19 – 20. Настройка OSPFv2 в сети множественного доступа	4
11	Лабораторная работа № 21 – 22. Настройка расширенных функций OSPFv2	4
12	Лабораторная работа № 23 – 24. Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области	4
13	Лабораторная работа № 25 – 26. Поиск и устранение неполадок в работе усовершенствованного протокола OSPFv2 для одной области	4
14	Лабораторная работа № 27 – 28. Владение навыками поиска и устранения неполадок в работе OSPF	4
15	Лабораторная работа № 29 – 30. Настройка OSPFv2 для нескольких областей	4
16	Лабораторная работа № 31 – 32. Настройка OSPFv3 для нескольких областей	4
17	Лабораторная работа № 33 – 34. Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей	4
18	Лабораторная работа № 35 – 36. Настройка базового PPP с аутентификацией	4
19	Лабораторная работа № 37 – 38. Отладка базового PPP с аутентификацией	4

20	Лабораторная работа № 39 – 40. Проверка PPP	4
21	Лабораторная работа № 41 – 42. Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL	4
22	Лабораторная работа № 43 – 44. Настройка туннеля VPN GRE по схеме «точка-точка»	4
23	Лабораторная работа № 45 – 46. Разработка технического обслуживания сети	4
24	Лабораторная работа № 47 – 48. Настройка Syslog и NTP	4
25	Лабораторная работа № 49 – 50. Изучение программного обеспечения для мониторинга сети	4
26	Лабораторная работа № 51. Настройка SNMP	2
27	Лабораторная работа № 52. Сбор и анализ данных NetFlow	2
28	Лабораторная работа № 53. Инструментарий сетевого администратора для наблюдения	2
29	Лабораторная работа № 54. Сбой в работе сети	2
30	Лабораторная работа № 55. Разработка документации	2
ИТОГО:		**110**

Лабораторная работа № 1

На тему: Развертывание коммутируемой сети с резервными каналами

Топология

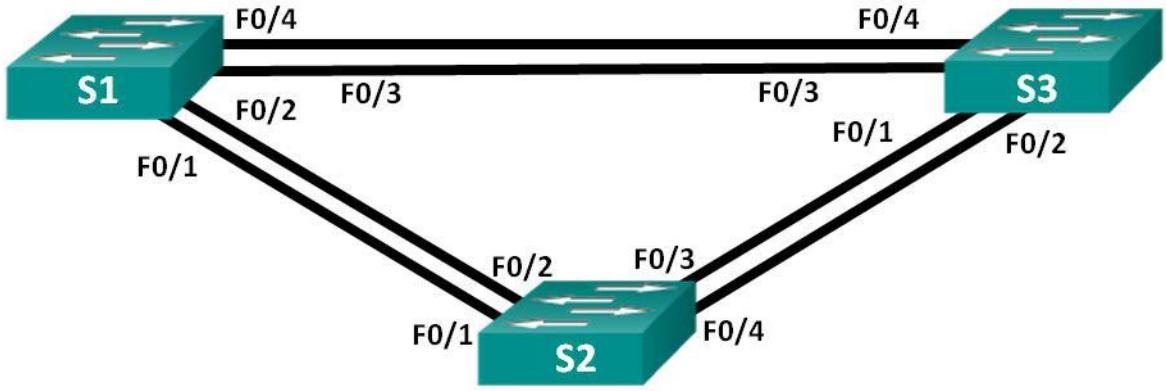


Таблица адресации

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:

1. 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

2. консольные кабели для настройки устройств Cisco IOS через порты консоли;

3. 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.

99 Отключите поиск DNS.

100 Присвойте имена устройствам в соответствии с топологией.

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

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

103 Настройте logging synchronous для консольного канала.

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

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

106 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

В 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.

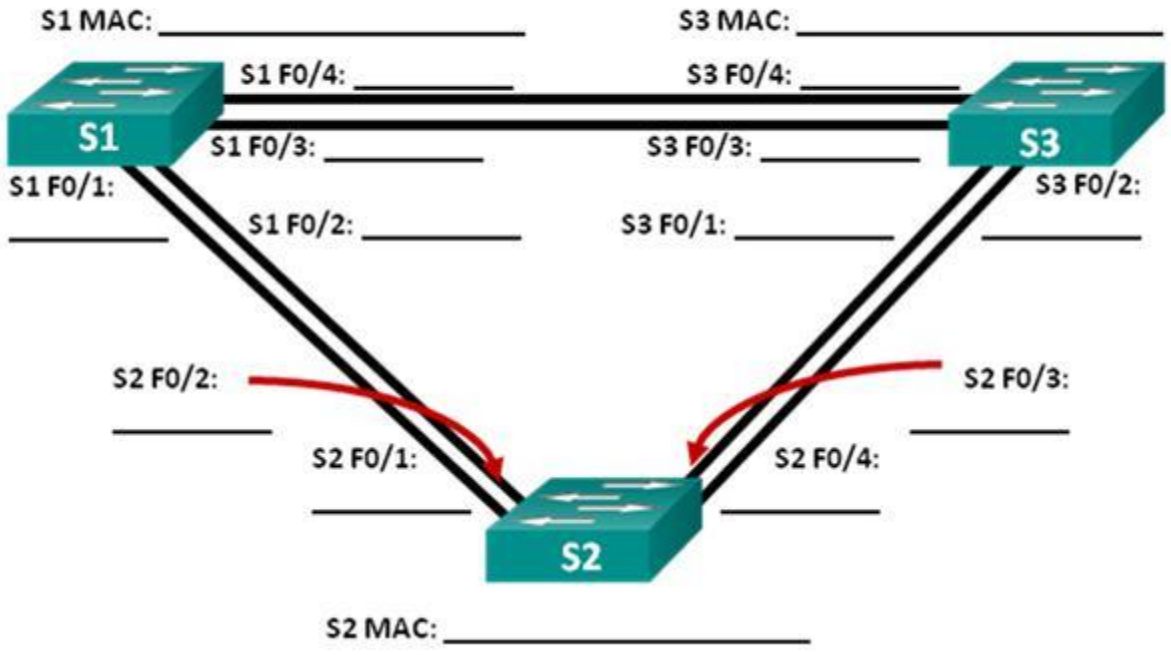
Введите команду **show spanning-tree** на всех трех коммутаторах. Приоритет идентификатора моста рассчитывается путем сложения значений приоритета и расширенного идентификатора системы. Расширенным идентификатором системы всегда является номер сети VLAN. В примере ниже все три коммутатора имеют равные 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             Forward Delay 15 sec
                    Hello Time  2 sec     Max Age 20 sec

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

      Interface    Role        Sts Cost        Prio.NbrType
```

```
------------------- ---- --- --------- --------  --------------------------------
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 secForward Delay 15 sec

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

Interface    Role        Sts Cost         Prio.NbrType
------------------- ---- --- --------- --------  --------------------------------
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.



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

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


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

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 32768sys-id-ext 1)
  Address               0cd9.96e8.7400
  Hello            Time   2 sec    Max Age 20 secForward 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
```

Почему протокол spanning-tree заменяет ранее заблокированный порт на назначенный порт 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.

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

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

```
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
      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          128.1    P2p
```

```
Fa0/2               Altn BLK 19          128.2    P2p
Fa0/3               Altn BLK 19          128.3    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        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          128.1    P2p
Fa0/2               Altn BLK 19          128.2    P2p
Fa0/3               Desg FWD 19          128.3    P2p
Fa0/4               Desg FWD 19          128.4    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

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

_____

_____

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

_____

_____

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

Лабораторная работа № 2

На тему: Настройка Rapid PVST+, PortFast и BPDU Guard

Топология

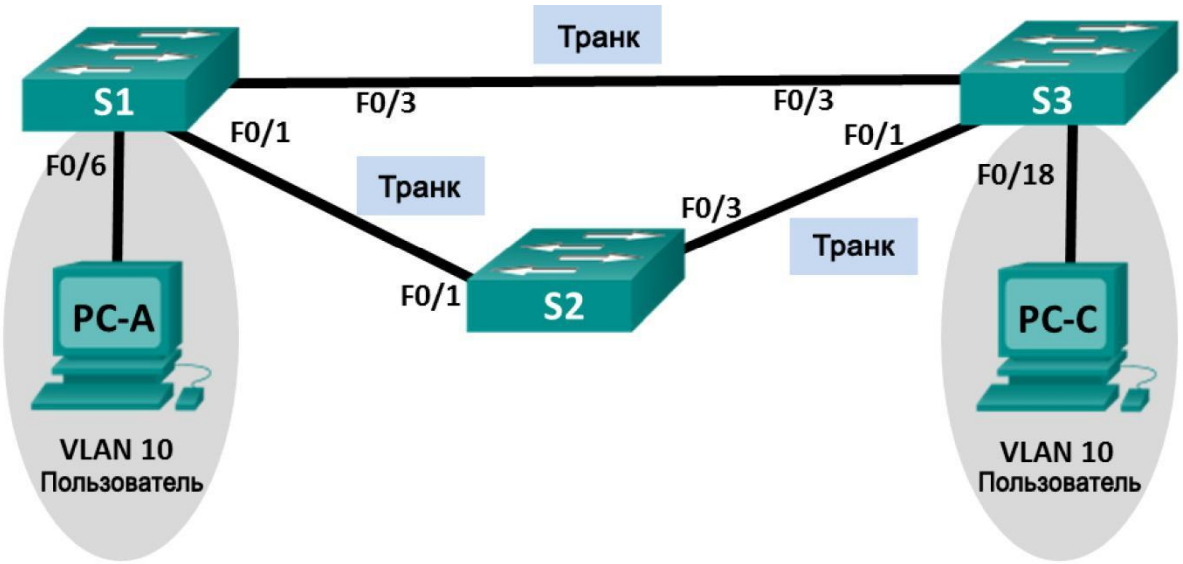


Таблица адресации

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
107	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

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.

_____
_____

d. На
стройте 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 коммутаторе S3.

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 FastEthernet0/1
*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 FastEthernet0/1
*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 FastEthernet0/1
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
*Mar 1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to 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 FastEthernet0/1, 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 FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*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 прило жении A. 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 response to a proposal
*Mar 1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed 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 mode trunk

S1(config-if)# **switchport**
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 vlan 1,10,99 root**
S1(config)# **spanning-tree 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**

Лабораторная работа № 3

На тему: Настройка протокола GLBP

Топология

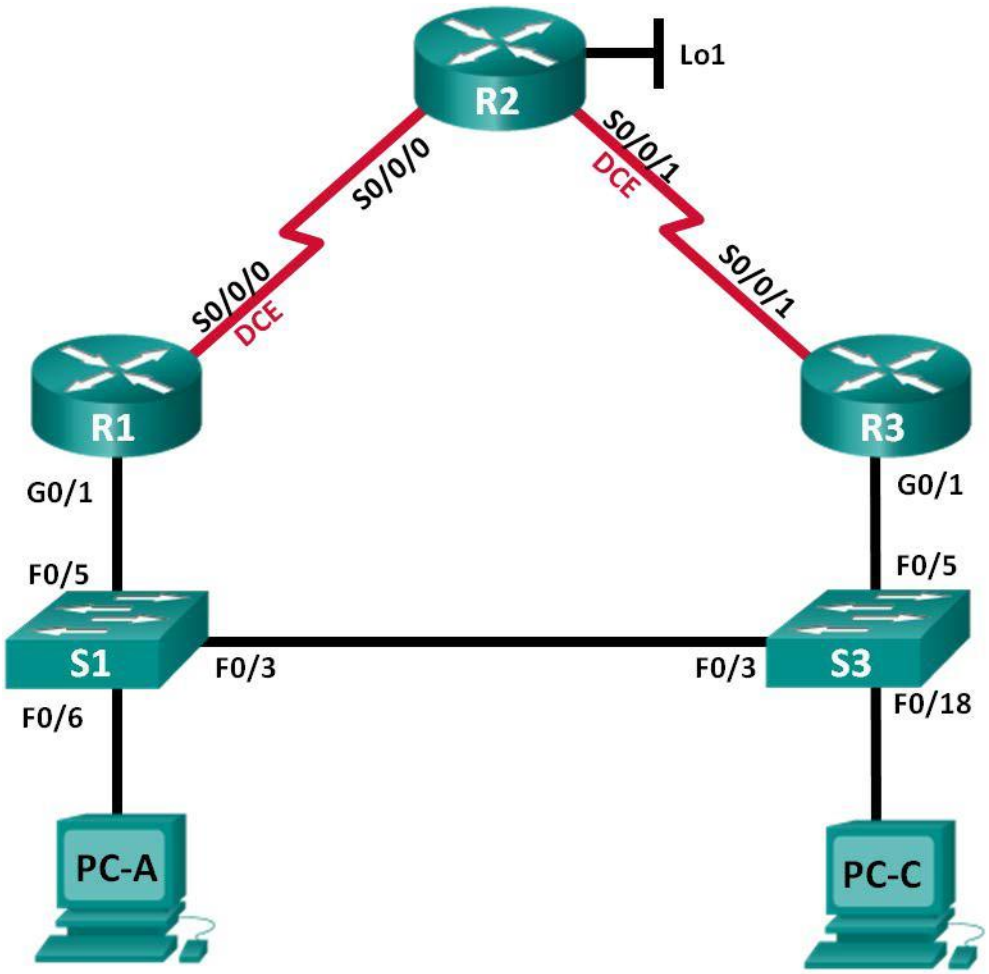


Таблица адресации

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:

a. 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

b. 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

c. 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например
Tera Term);

d. консольные кабели для настройки устройств Cisco IOS через порты консоли;

e. кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и проверка соединения

С 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.

b. Отключите поиск DNS.
c. Присвойте имена устройствам в соответствии с топологией.
d. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.
e. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора
DCE.
f. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
g. Назначьте **cisco** в качестве пароля виртуального терминала VTY и активируйте вход.
h. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
i. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 5: Настройте базовые параметры каждого коммутатора.

c. Отключите поиск DNS.
d. Присвойте имена устройствам в соответствии с топологией.
e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
f. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.
g. На каждом коммутаторе настройте шлюз по умолчанию.
h. Назначьте **cisco** в качестве пароля виртуального терминала VTY и активируйте вход.
i. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
c. 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.

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

c. 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.

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?

_____

e. 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

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

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

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

Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<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.

```
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.

```
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)
```

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?

_____

_____

_____

_____

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       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.

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

Какой маршрутизатор является активным?

_____

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

c. 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
Gi0/1       1    -   150 Active   192.168.1.254   local           192.168.1.3
Gi0/1       1    1   -   Active   0007.b400.0101  local           -
Gi0/1       1    2   -   Listen   0007.b400.0102  192.168.1.3     -

R3# show glbp brief

Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Gi0/1       1    -   100 Standby  192.168.1.254   192.168.1.1     local
Gi0/1       1    1   -   Listen   0007.b400.0101  192.168.1.1     -
Gi0/1       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

c **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**	**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. 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.

Лабораторная работа № 4

На тему: Определение типовых ошибок конфигурации STP

STP (**Spanning Tree Protocol**) — сетевой протокол (или семейство сетевых протоколов) предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях. Первоначальный протокол STP описан в стандарте 802.1D. Позже появилось несколько новых протоколов (RSTP, MSTP, PVST, PVST+), отличающихся некоторыми особенностями в алгоритме работы, в скорости, в отношении к VLANам и ряде других вопросов, но в целом решающих ту же задачу похожими способами. Все их принято обобщённо называть STP-протоколами.

Протокол STP в своё время был разработан *мамой Интернета Радией Перлман* (Radia Perlman), а позже, в начале 90х превратился в стандарт IEEE 802.1D.

В настоящее время протокол STP (или аналогичный) поддерживается почти всеми Ethernet-коммутаторами, как реальными, так и виртуальными, за исключением самых примитивных.

Алгоритм действия STP (Spanning Tree Protocol)

- После включения коммутаторов в сеть, по умолчанию каждый коммутатор считает себя корневым (root).
- Каждый коммутатор начинает посылать по всем портам конфигурационные Hello BPDU пакеты раз в 2 секунды, максимальный промежуток 20 секунд.
- Если мост получает BPDU с идентификатором моста (Bridge ID) меньшим, чем свой собственный, он прекращает генерировать свои BPDU и начинает ретранслировать BPDU с этим идентификатором. Таким образом в конце концов в этой сети Ethernet остаётся только один мост, который продолжает генерировать и передавать собственные BPDU. Он и становится *корневым мостом* (root bridge).
- Остальные мосты ретранслируют BPDU корневого моста, добавляя в них собственный идентификатор и увеличивая счетчик стоимости пути (path cost).

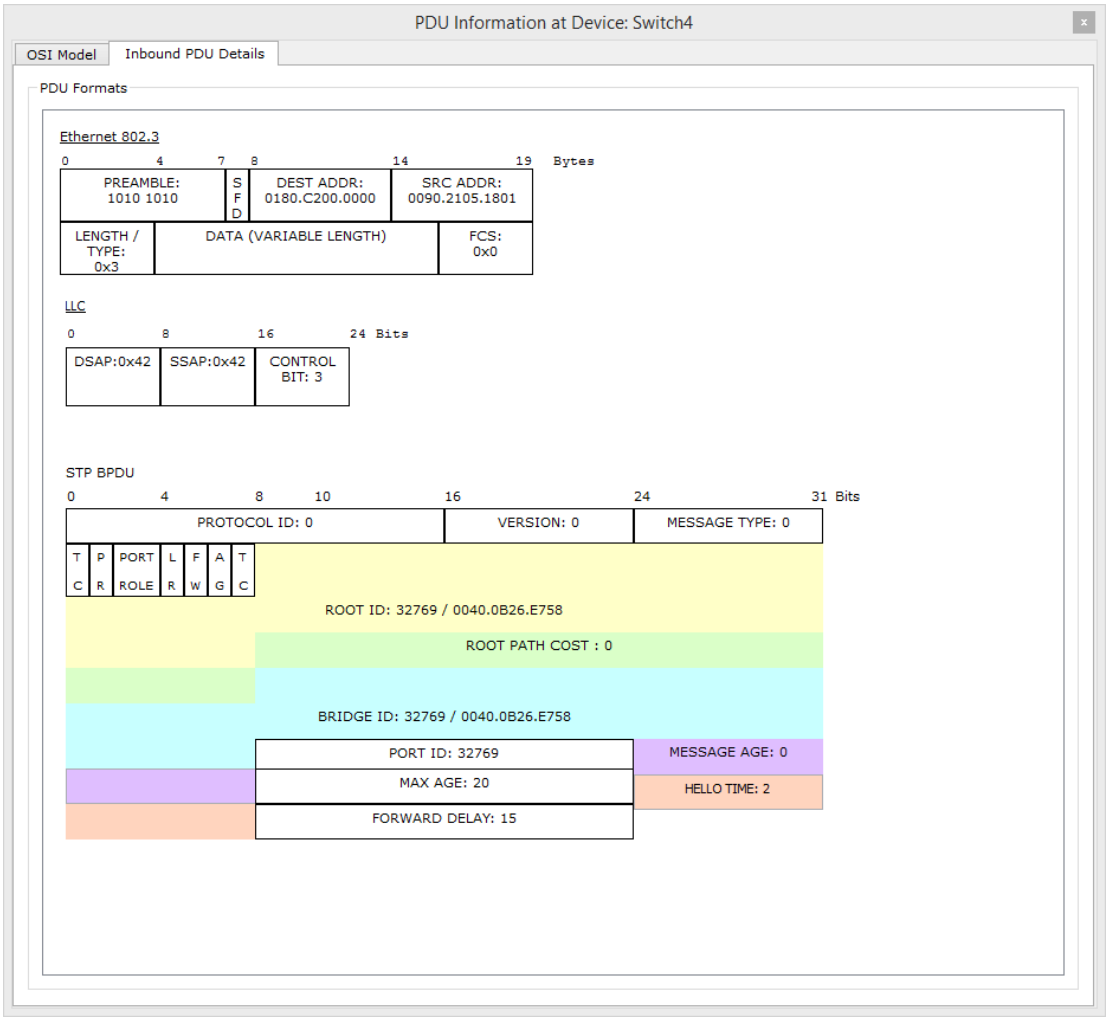
- Для каждого сегмента сети, к которому присоединены два и более портов мостов, происходит определение designated port — порта, через который BPDU, приходящие от корневого моста, попадают в этот сегмент.
- После этого все порты в сегментах, к которым присоединены 2 и более портов моста, блокируются за исключением root port и designated port.
- Корневой мост продолжает посылать свои Hello BPDU раз в 2 секунды.

BPDU кадр

Bridge Protocol Data Unit

- Protocol Identifier размер 2 байта
- Protocol Version Identifier размер 1 байт
- BPDU Type размер 1 байт
- Flags размер 1 байт
- Root Identifier размер 8 байт
- Root Path Cost размер 4 байт
- Bridge Identifier размер 8 байт
- Port Identifier размер 2 байт
- Message Age размер 2 байт
- Max Age размер 2 байт
- Hello Time размер 2 байт
- Forward Delay размер 2 байт

Вот как выглядит BPDU кадр STP



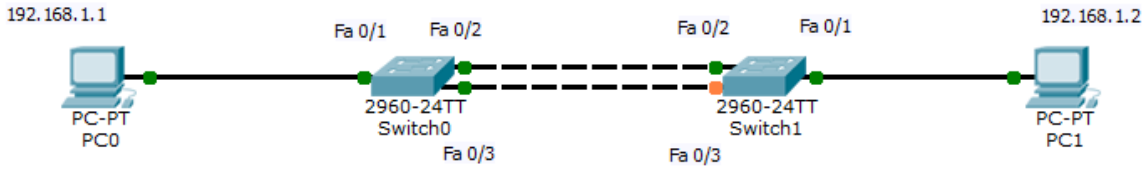
кадр BPDU

Состояния портов:

1. Блокировка (blocking)
2. Прослушивание (listening)
3. Обучение (learning)
4. Передача (forwarding)

Настройка stp

Обща схема примера работы и настройки STP. Два коммутатора соединенных двумя линками, видно то STP уже работает и один порт у второго коммутатора погашен чтобы не было петли



Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-01

Посмотрим на первом коммутаторе настройки stp. Логинимся и вводим команду

show spanning-tree

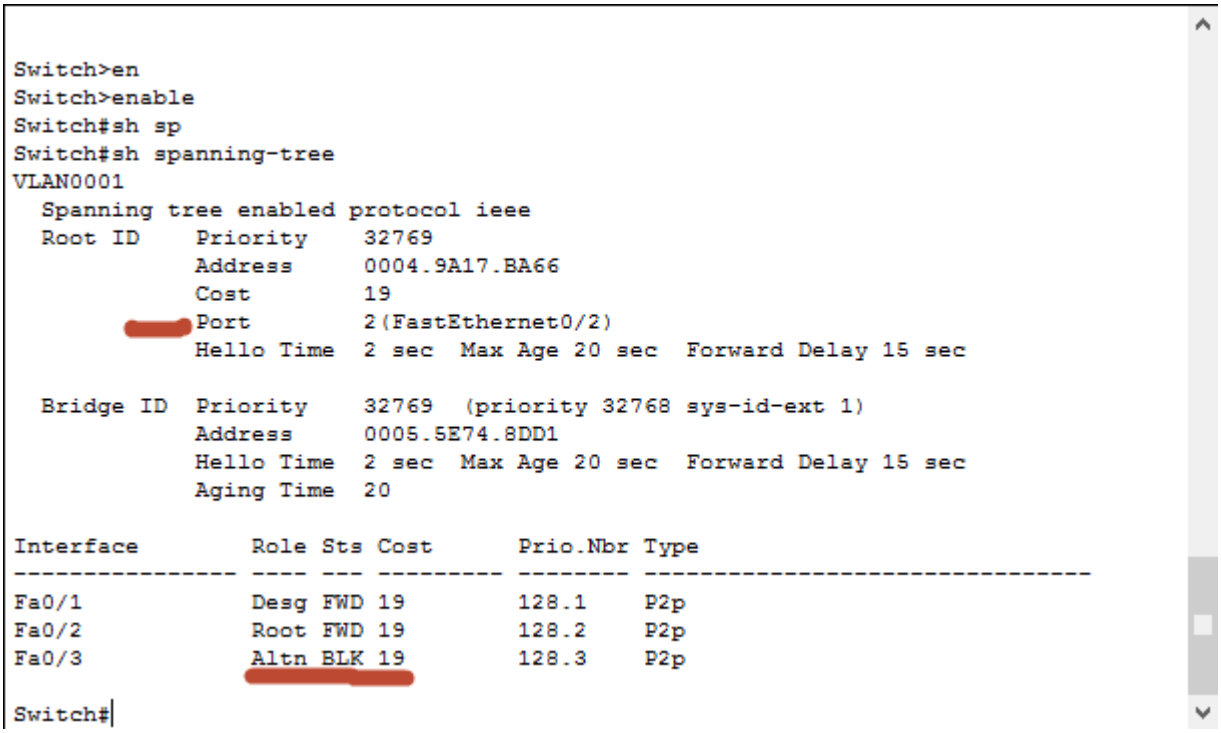
Видим, что это рутовый коммутатор и все порты в состоянии передача.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state t
o up

Switch#
Switch#sh
Switch#show sp
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0004.9A17.BA66
              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     0004.9A17.BA66
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

Switch#
```

Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-02

Смотрим, тоже на втором коммутаторе.

show spanning-tree



```
Switch>en
Switch>enable
Switch#sh sp
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0004.9A17.BA66
              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     0005.5E74.8DD1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p

Switch#
```

Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-03

Видим, что это не рутовый коммутатор. Интерфейс Fa0/2 является рутовым портом. Fa0/3 ждет в запасе.

Теперь предположим, что интерфейс Fa0/2 упал, что будет. Для примера выключим его. Заходим на 1 коммутатор.

config t

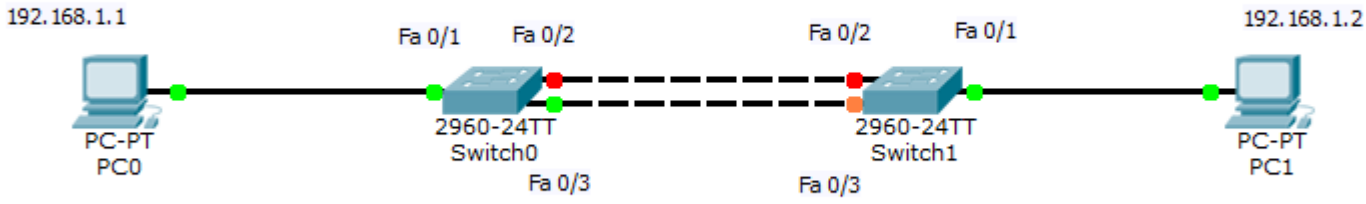
interface Fa0/2

shutdown

```
Press RETURN to get started.



Switch>en
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#in
Switch(config)#interface fa0/2
Switch(config-if)#shu
Switch(config-if)#shutdown
```

Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-04

Видим, что линк пропал



Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-05

Зайдем в этот момент на второй коммутатор и посмотрим состояние портов.

show spanning-tree

Видим, что порт Fa0/3 в состоянии обучения

```
o down


Switch>en
Switch>enable
Switch#sh sp
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0004.9A17.BA66
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0005.5E74.8DD1
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Root LRN 19        128.3    P2p

Switch#
```

Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-06

теперь в состоянии передачи, прошло около 20 секунд и линк поднялся.

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Root FWD 19        128.3    P2p

Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0004.9A17.BA66
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0005.5E74.8DD1
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Root FWD 19        128.3    P2p

Switch#
```

Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-07

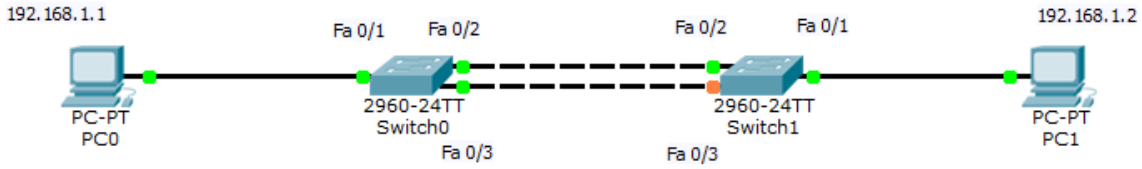
Восстановим на первом коммутаторе Fa0/2 командой

no shutdown

```
Switch>en
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#in
Switch(config)#interface fa0/2
Switch(config-if)#shu
Switch(config-if)#shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively do
wn

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state t
o down

Switch(config-if)#no s
Switch(config-if)#no sh
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state t
o up
```

Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-08

И видим, что все мгновенно восстановилось.



Что такое и как настроить протокол STP (Spanning Tree Protocol) в Cisco-09

Все же переключение в 20 секунд очень нехорошо, поэтому уже придуманы улучшенные версии протокола rstp и lacp, но о них в следующих публикациях.

Как настроить RSTP на коммутаторах Cisco

RSTP или как его еще называют в более развернутом виде **Rapid spanning tree protocol**, по сути тот же STP но более быстрый где время сходимости мгновение, вы потеряете один пакет.

Включить RSTP можно командой с режиме глобального конфигурирования, где нужно изменить режим на rapid-pvst.

spanning-tree mode rapid-pvst

Все теперь при падении одного линка, время схождения между коммутаторами будет 1 секунда, очень быстро, как видите RSTP, гораздо лучше STP и настраивается одной командой.

Лабораторная работа № 5

На тему: Настройка EtherChannel

Топология

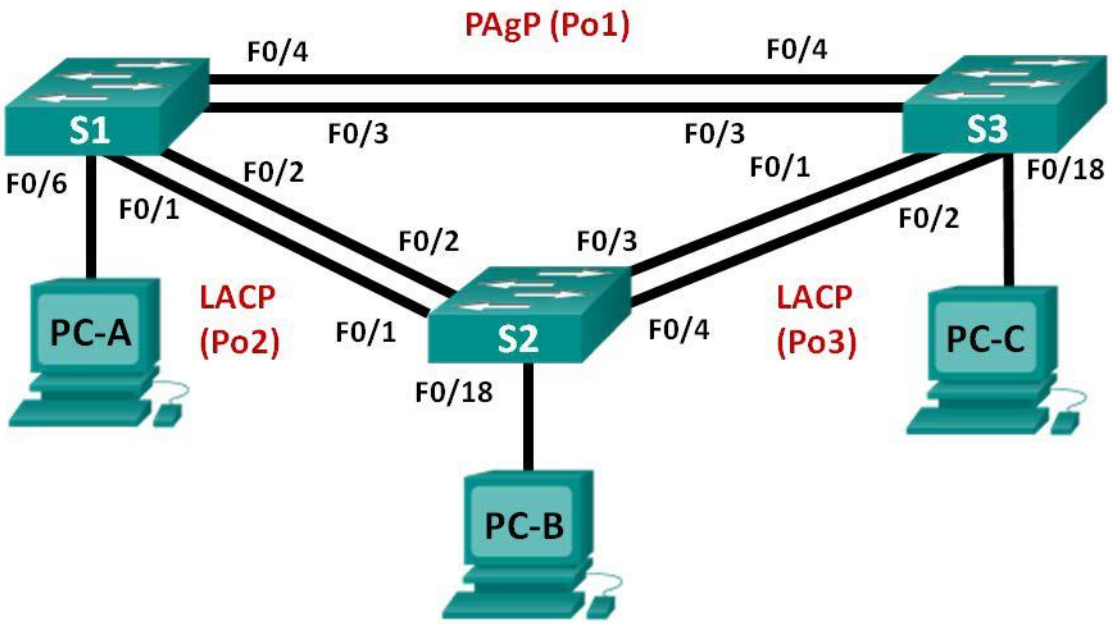


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

Задачи

Часть 1. Настройка базовых параметров коммутатора

Часть 2. Настройка PAgP

Часть 3. Настройка LACP

Исходные данные/сценарий

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 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);
- 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, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров коммутатора

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.

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. Настройте имя устройства в соответствии с топологией.

c. Зашифруйте все незашифрованные пароли.

d. Создайте баннерное сообщение дня MOTD, предупреждающее пользователей о том, что несанкционированный доступ запрещён.

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

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

g. Настройте logging synchronous, чтобы предотвратить прерывание ввода команд сообщениями консоли.

h. Отключите все порты коммутатора, кроме портов, подключенных к компьютерам.

i. Настройте сеть VLAN 99 и присвойте ей имя **Management**.

j. Настройте сеть VLAN 10 и присвойте ей имя **Staff**.

k. Настройте порты коммутатора с присоединёнными узлами в качестве портов доступа в сети VLAN

l. Назначьте IP-адреса в соответствии с таблицей адресации.

m. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте компьютеры.

Назначьте IP-адреса компьютерам в соответствии с таблицей адресации.

Часть 2: Настройка протокола PAgP

Протокол PAgP является проприетарным протоколом агрегирования каналов Cisco. В части 2 вам предстоит настроить канал между S1 и S3 с использованием протокола PAgP.

Шаг 1: Настройте PAgP на S1 и S3.

Для образования канала между S1 и S3 настройте порты на S1 с использованием рекомендуемого режима (desirable), а порты на S3 — с использованием автоматического режима (auto). Включите порты после настройки режимов PAgP.

```
S1(config)# interface range f0/3-4 S1(config-if-
range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S3(config)# interface range f0/3-4
S3(config-if-range)# channel-group 1 mode auto
Creating a port-channel interface Port-channel 1
```

```
S3(config-if-range)# no shutdown
*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
S3(config-if-range)#
*Mar 1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
*Mar 1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up
S3(config-if-range)#
*Mar  1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Mar 1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
*Mar 1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

Шаг 2: Проверьте конфигурации на портах.

В настоящее время интерфейсы F0/3, F0/4 и Po1 (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 команд **show run interface** *идентификатор-интерфейса* и **show interfaces** *идентификатор-интерфейса* **switchport**, соответственно. 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 desirable
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 3: 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)          PAgP      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)          PAgP      Fa0/3(P)     Fa0/4(P)
```

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

_____

_____

_____

_____

Шаг 4: Настройте транковые порты.

После агрегирования портов команды, применённые на интерфейсе Port Channel, влияют на все объединённые в группу каналы. Вручную настройте порты Po1 на S1 и S3 в качестве транковых и назначьте их сети native VLAN 99.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk S3(config-
if)# switchport trunk native vlan 99
```

Шаг 5: Убедитесь в том, что порты настроены в качестве транковых.

a. Выполните команды **show run interface** *идентификатор-интерфейса* на S1 и S3. Какие команды включены в список для интерфейсов F0/3 и F0/4 на обоих коммутаторах? Сравните результаты с текущей конфигурацией для интерфейса Po1. Запишите наблюдения.

_____
_____
_____
_____
_____

b. Выполните команды **show interfaces trunk** и **show spanning-tree** на S1 и S3. Какой транковый порт включен в список? Какая используется сеть native VLAN? Какой вывод можно сделать на основе выходных данных?

_____
_____
_____
_____
_____

Какие значения стоимости и приоритета порта для агрегированного канала отображены в выходных данных команды **show spanning-tree**?

_____
_____
_____
_____
_____

Часть 3: 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 S2 и канала между S2 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 S2.

```
S1(config)# interface range f0/1-2
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
S2(config)# interface range f0/1-2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 2 mode passive
Creating a port-channel interface Port-channel 2
S2(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: Настройте LACP между S2 и S3.

d. Настройте канал между S2 и S3 как Po3, используя LACP как протокол агрегирования каналов.

```
S2(config)# interface range f0/3-4 S2(config-if-
range)# switchport mode trunk S2(config-if-range)#
switchport trunk native vlan 99 S2(config-if-
range)# channel-group 3 mode active Creating a
port-channel interface Port-channel 3 S2(config-if-
range)# no shutdown
S3(config)# interface range f0/1-2 S3(config-if-
range)# switchport mode trunk S3(config-if-range)#
switchport trunk native vlan 99 S3(config-if-
range)# channel-group 3 mode passive
Creating a port-channel interface Port-channel 3
S3(config-if-range)# no shutdown
```

e. Убедитесь в том, что канал EtherChannel образован.

Шаг 4: Проверьте сквозное подключение.

Убедитесь в том, что все устройства могут передавать друг другу эхо-запросы в пределах одной сети VLAN. Если нет, выполните отладку связи из конца в конец.

Примечание. Для успешной передачи эхо-запросов между ПК может потребоваться отключить межсетевые экраны на ПК.

Вопросы на закрепление

Что может препятствовать образованию каналов EtherChannel?

_____

_____

_____

Лабораторная работа № 6

На тему: Поиск и устранение неполадок в работе EtherChannel

Топология

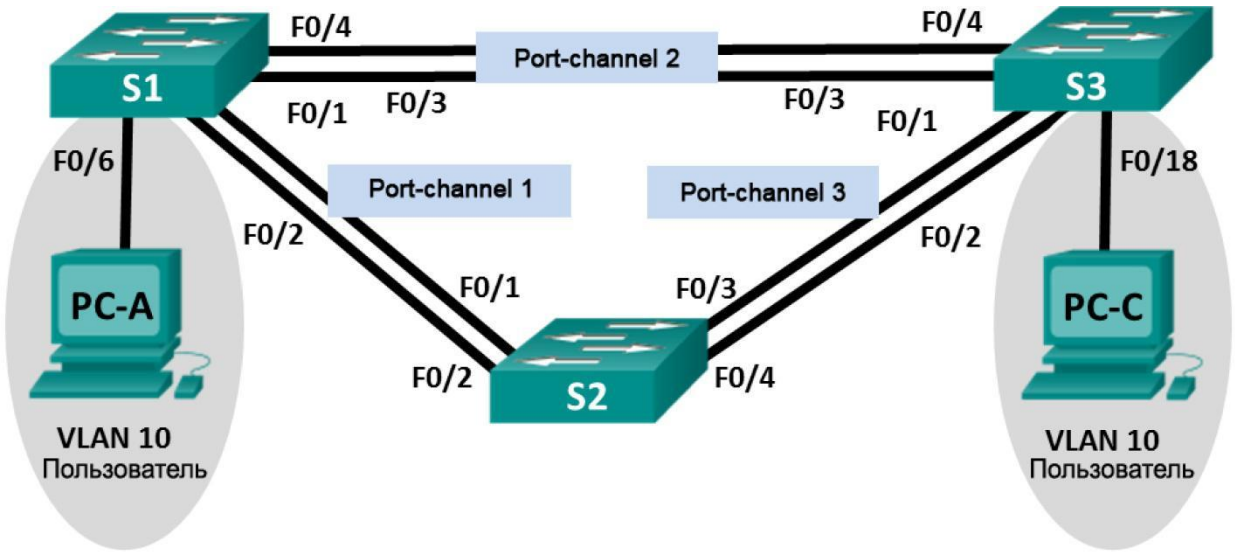


Таблица адресации

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

В 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:

f. 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

g. 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)

h. консольные кабели для настройки устройств Cisco IOS через порты консоли;

i. 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
login
line 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 192.168.1.11 255.255.255.0
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 primary
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 192.168.1.12 255.255.255.0
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 1,10,99
 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 f0/18
 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.

c. 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?

_____

d. 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.

_____

_____

_____

_____

_____

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

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

_____

_____

_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

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

В 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.

f. 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.

_____
_____
_____
_____
_____

g. 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.

_____
_____

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

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

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

j. Выполните команду для проверки параметров транковой связи.

k. 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.

_____
_____
_____
_____

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

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

_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

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

_____
_____

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

_____
_____

Шаг 4: Проверка EtherChannel и подключения

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

g. 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?

_____

h. 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.

Лабораторная работа № 7

На тему: Агрегирование каналов

Топология

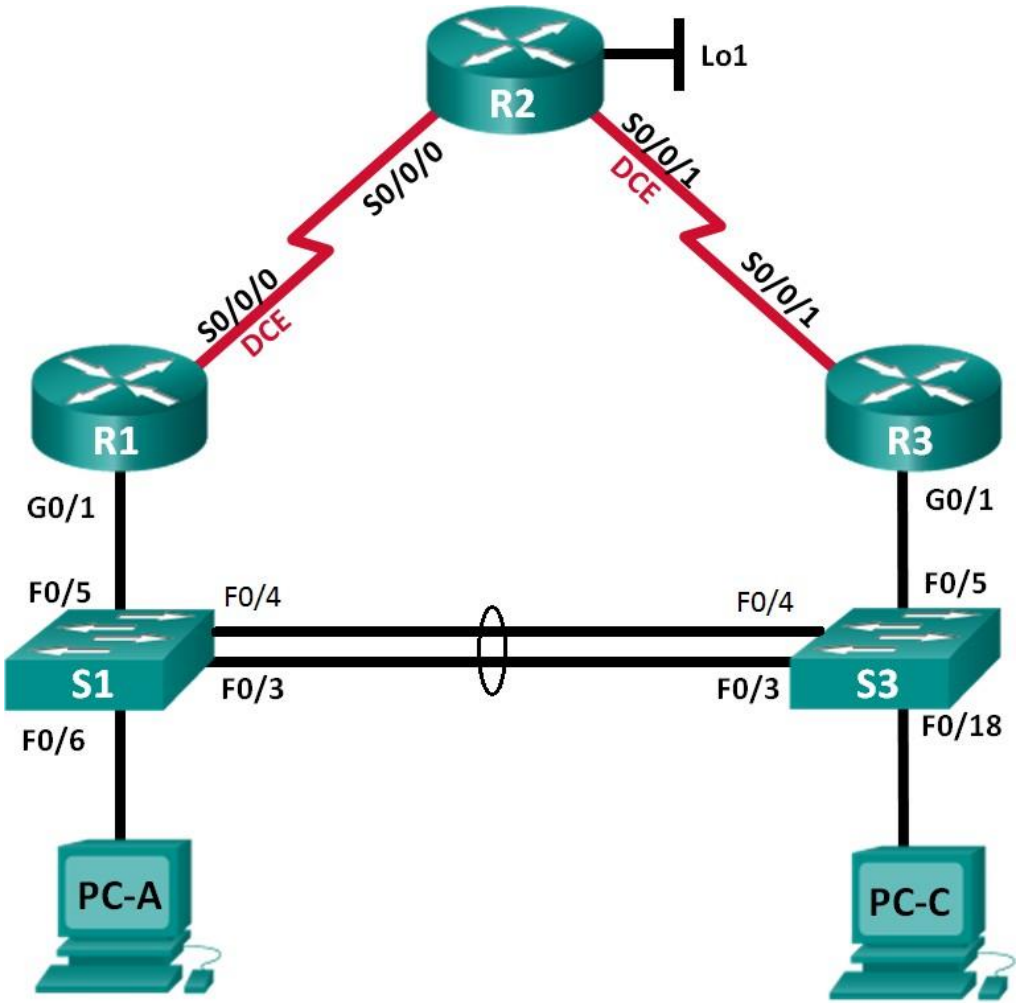


Таблица адресации

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 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 209.165.200.225 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.

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

_____

b. 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 Po1 (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.				

Лабораторная работа № 8

На тему: Настройка беспроводного маршрутизатора и клиента

Топология

Настройки маршрутизатора Linksys

Имя сети (SSID)	Сеть CCNA
Пароль сети	cisconet
Пароль маршрутизатора	cisco123

Задачи

Часть 1. Настройка основных параметров маршрутизатора Linksys серии EA

Часть 2. Настройка защиты беспроводной сети

Часть 3. Настройка дополнительных функций маршрутизатора Lynksys серии EA

Часть 4. Подключение беспроводного клиента

Исходные данные/сценарий

В наши дни доступ к сети Интернет из любого места, будь то дом или офис — широко распространенное явление. Без беспроводной связи пользователи были бы ограничены возможностью подключения только при наличии проводного соединения. Пользователи по достоинству оценили гибкость и возможности, которые предоставляют беспроводные маршрутизаторы в рамках доступа к сети и Интернету.

В этой лабораторной работе вам предстоит настроить маршрутизатор Linksys Smart Wi-Fi, применить настройки безопасности WPA2 и активировать службы DHCP. Вы рассмотрите некоторые дополнительные функции, доступные на этих маршрутизаторах, например, USB-накопители, родительский контроль и ограничения по времени. Вам также предстоит настроить беспроводной клиент для компьютера.

Необходимые ресурсы:

f. 1 маршрутизатор Linksys EA Series (EA4500 с версией микропрограммного обеспечения 2.1.39.145204 или сопоставимой версией);

g. 1 кабельный или DSL-модем (необязательно; требуется для работы интернет-службы и обычно предоставляется интернет-провайдером);

h. 1 компьютер с беспроводным сетевым адаптером (ОС Windows 7, Vista или XP);

i. кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров маршрутизатора Linksys EA Series

Самым эффективным способом настройки основных параметров маршрутизатора EA Series является запуск установочного компакт-диска Linksys EA Series, поставляемого в комплекте с маршрутизатором. Если установочный компакт-диск отсутствует, следует загрузить программу установки с веб-сайта http://Linksys.com/support.

Шаг 1: Вставьте установочный компакт-диск Linksys EA-Series в компьютер.

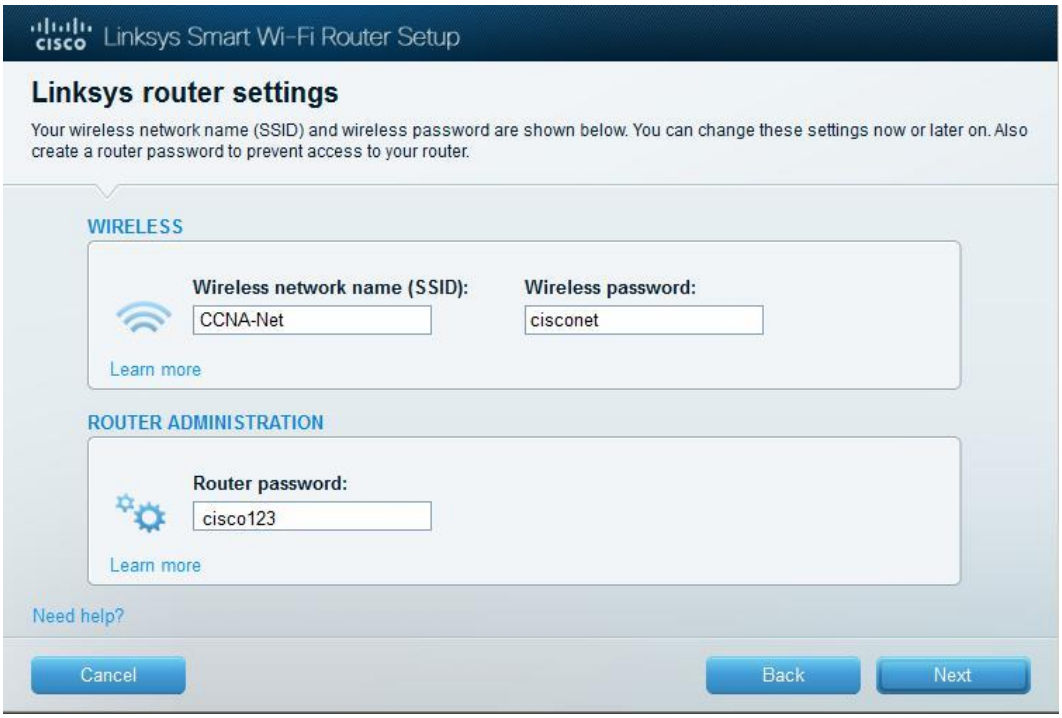
Когда отобразится соответствующий запрос, выберите **Set up your Linksys Router (Настройка маршрутизатора Linksys)**. Вам будет предложено ознакомиться с условиями лицензии на использование программного обеспечения и принять их. После того, как вы примете условия лицензии нажмите **Next > (Далее >)**.

Шаг 2: Подключите кабели в сети в соответствии с топологией.

Следуйте инструкциям по подключению кабеля питания и кабельного модема или DSL-модема с помощью Ethernet-кабеля, которые отобразятся в следующем окне. Можно подключить компьютер к одному из четырех неиспользуемых Ethernet-портов на задней стенке маршрутизатора. После подключения всех необходимых элементов нажмите **Next > (Далее >)**.

Шаг 3: Настройте параметры маршрутизатора Linksys.

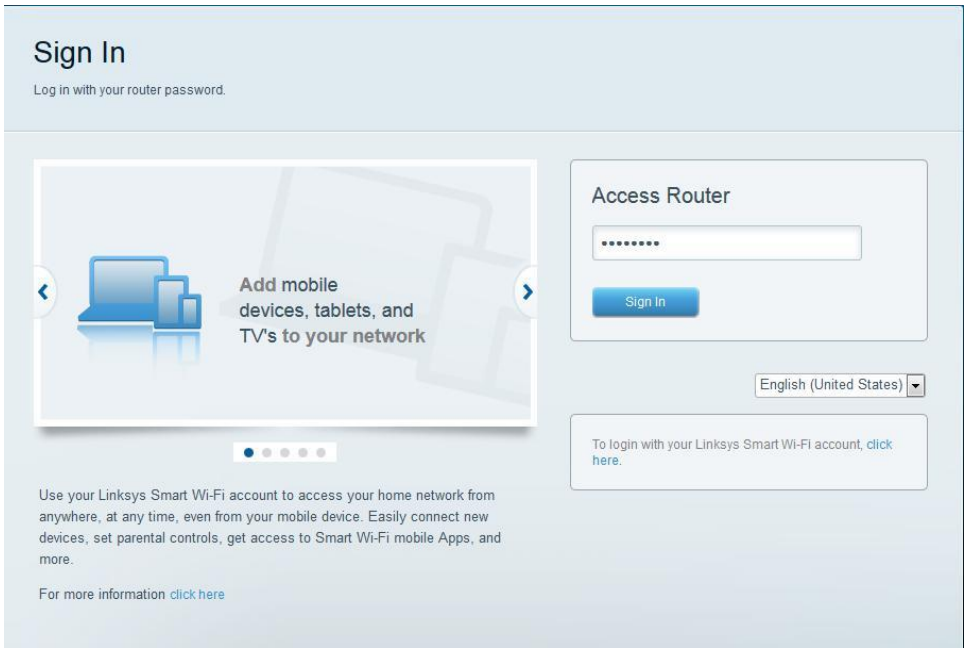
Дождитесь, когда отобразится окно **Linksys router settings (Настройки маршрутизатора Linksys)**. Для заполнения полей в этом окне используйте данные таблицы **Linksys router settings (Настройки маршрутизатора Linksys)**, приведённой в начале лабораторной работы. Нажмите **Next (Далее)**, чтобы отобразить экран со сводной информацией о настройках маршрутизатора. Нажмите **Next (Далее)**.



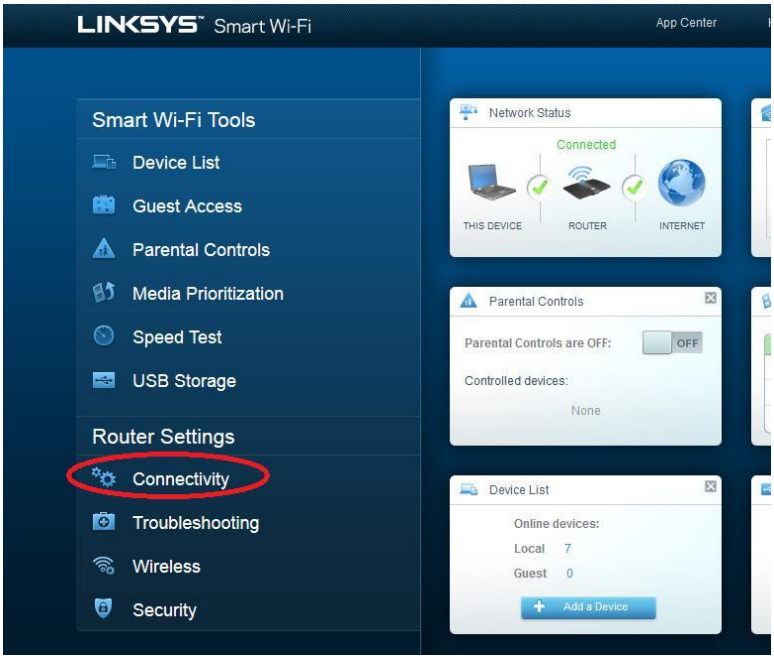
b. Отобразится окно **Create your Linksys Smart Wi-Fi account (Создание учетной записи Linksys Smart Wi-Fi)**. Учетная запись Linksys Smart Wi-Fi используется для ассоциации маршрутизатора к учетной записи, что позволяет удалённо управлять маршрутизатором с помощью браузера или мобильного устройства, на котором запущено приложение Smart Wi-Fi. В рамках этой лабораторной работы пропустите процесс настройки учетной записи. Щелкните поле **No, thanks (Нет, спасибо)** и нажмите **Continue (Продолжить)**.

Примечание. Чтобы настроить учетную запись, перейдите на веб-сайт www.linksyssmartwifi.com.

c. Отобразится окно **Sign in (Вход в систему)**. В поле **Access Router (Доступ к маршрутизатору)** введите **cisco123** и нажмите **Sign in (Войти)**.

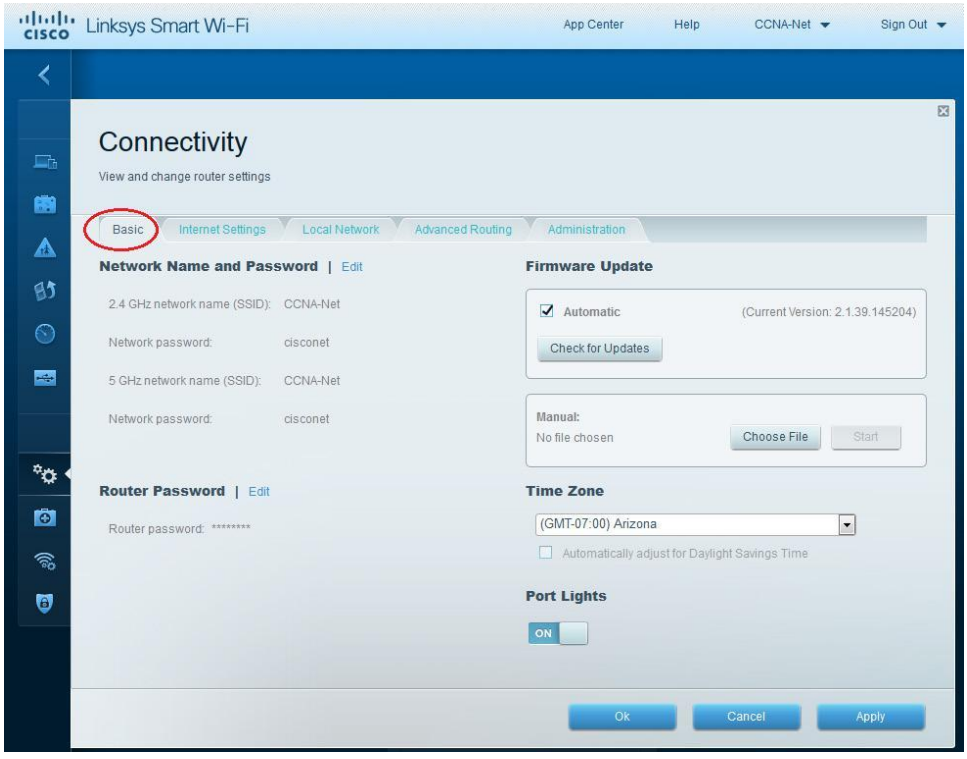


d. На домашней странице Linksys Smart Wi-Fi нажмите **Connectivity (Соединение)** чтобы просмотреть и изменить основные настройки маршрутизатора.

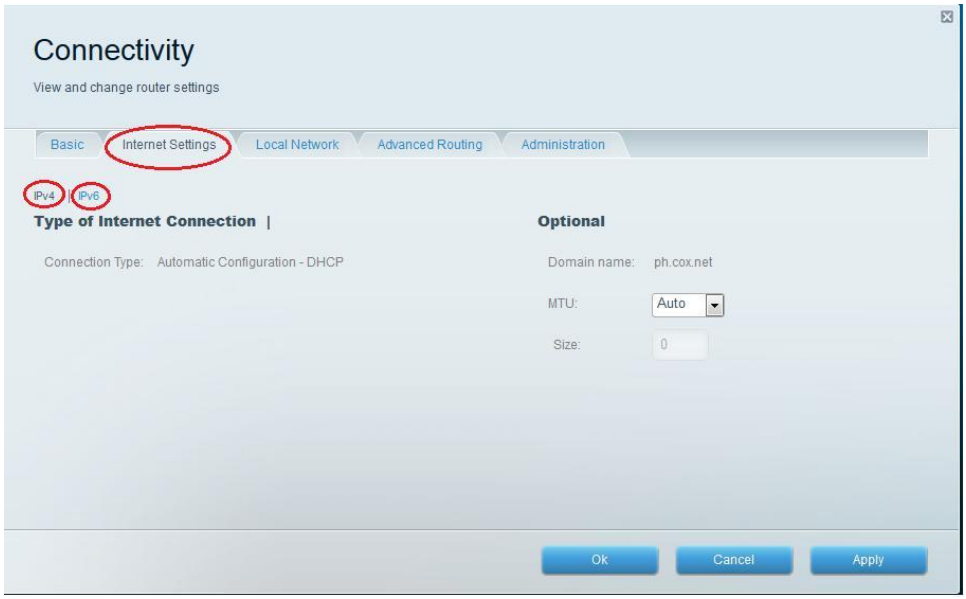


e. На вкладке **Basic (Основные настройки)** можно изменить имя и пароль сети, изменить пароль маршрутизатора, выполнить обновление микропрограммного обеспечения и задать часовой пояс для маршрутизатора. Пароль маршрутизатора и данные о сети настроены в шаге 3a.

В раскрывающемся списке выберите соответствующий часовой пояс для маршрутизатора и нажмите **Apply (Применить)**.



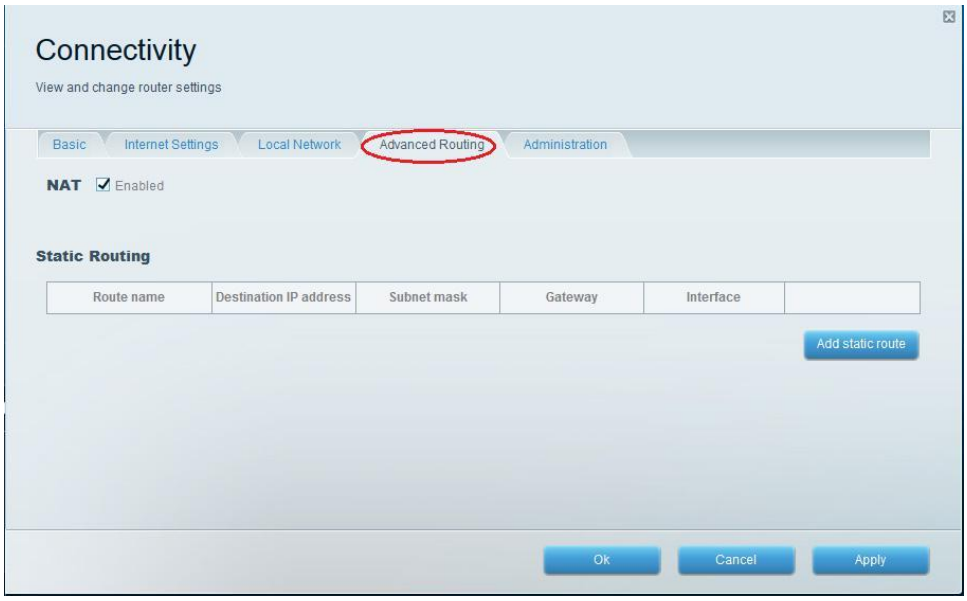
d. На вкладке **Internet Settings (Настройки Интернета)** отображены сведения об интернет-подключении. В этом примере маршрутизатор автоматически настраивает подключение для DHCP. На этом экране можно отобразить сведения как об IPv4, так и об IPv6.



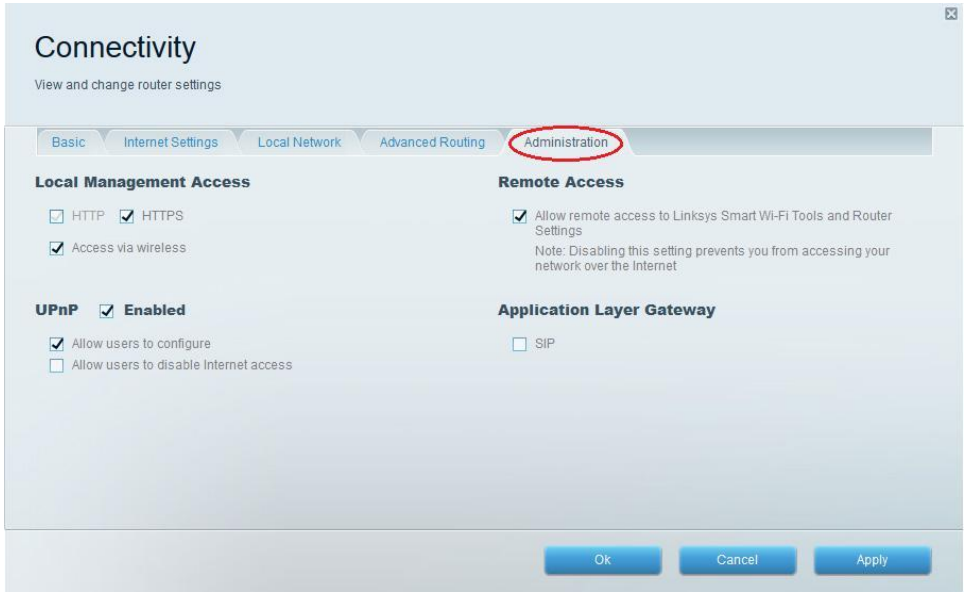
g. На вкладке **Local Network (Локальная сеть)** доступны параметры настройки локального DHCP-сервера. В настройках локальной сети по умолчанию задана сеть 192.168.1.0/24 и локальный IP-адрес маршрутизатора по умолчанию 192.168.1.1. Эти настройки можно изменить, нажав **Edit (Изменить)** рядом с разделом **Router Details (Сведения о маршрутизаторе)**. На этом экране можно изменить настройки DHCP-сервера. Можно задать начальный адрес DHCP, максимальное число пользователей DHCP, срок аренды клиента и статические DNS-серверы. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые на этом экране.

Примечание. Если DHCP используется для получения данных о подключении к сети интернет-провайдера, эти DNS-адреса, наиболее вероятно, будут заполняться данными DNS-сервера интернет-провайдера.

c. На вкладке **Advanced Routing (Дополнительная маршрутизация)** можно отключить функцию преобразования сетевых адресов (NAT), которая по умолчанию включена. На этом экране также можно добавить статические маршруты. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.



d. На вкладке **Administration (Администрирование)** доступны элементы управления, с помощью которых осуществляется управление программным обеспечением Smart Wi-Fi. Щелкнув соответствующее поле, можно активировать доступ к удалённому управлению маршрутизатором. Также можно активировать доступ по HTTPS и ограничить возможности управления беспроводной сетью. На этом экране также доступны элементы управления Universal Plug and Play (UPnP) и шлюза уровня приложения. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.

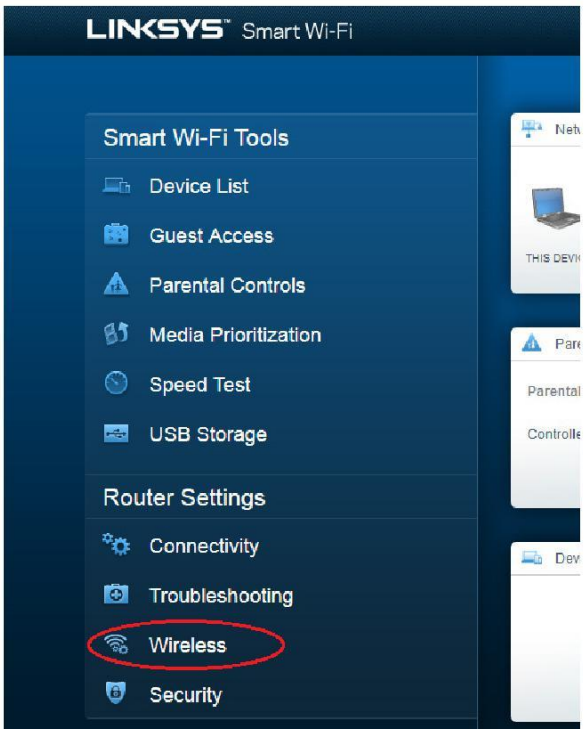


Часть 2: Защита беспроводной сети

В части 2 вам предстоит настроить функции защиты маршрутизатора Linksys EA Series и рассмотреть параметры межсетевого экрана и переадресации портов на маршрутизаторе Linksys Smart Wi-Fi.

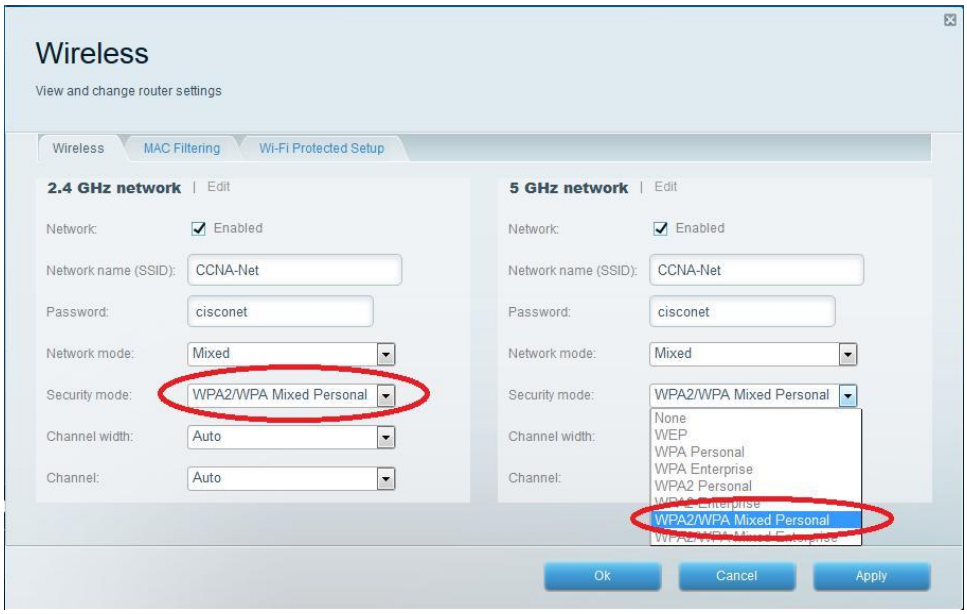
Шаг 1: Добавьте функции безопасности WPA на беспроводные маршрутизаторы.

a. На главной странице Linksys Smart Wi-Fi нажмите **Wireless (Беспроводная связь)**.



b. В окне **Беспроводная связь (Wireless)** отображаются настройки для полос 2,4 и 5 ГГц. Используйте кнопку **Edit (Изменить)** рядом с каждым из столбцов, чтобы изменить настройки безопасности для каждого частотного диапазона беспроводной сети. Имя и пароль сети ранее настроены в части 1. Нажмите раскрывающийся список **Security mode (Режим безопасности)**, чтобы выбрать параметр **WPA2/WPA Mixed Personal** для каждого из диапазонов. Нажмите **Apply (Применить)**, чтобы сохранить свои настройки, после чего нажмите **ОК**.

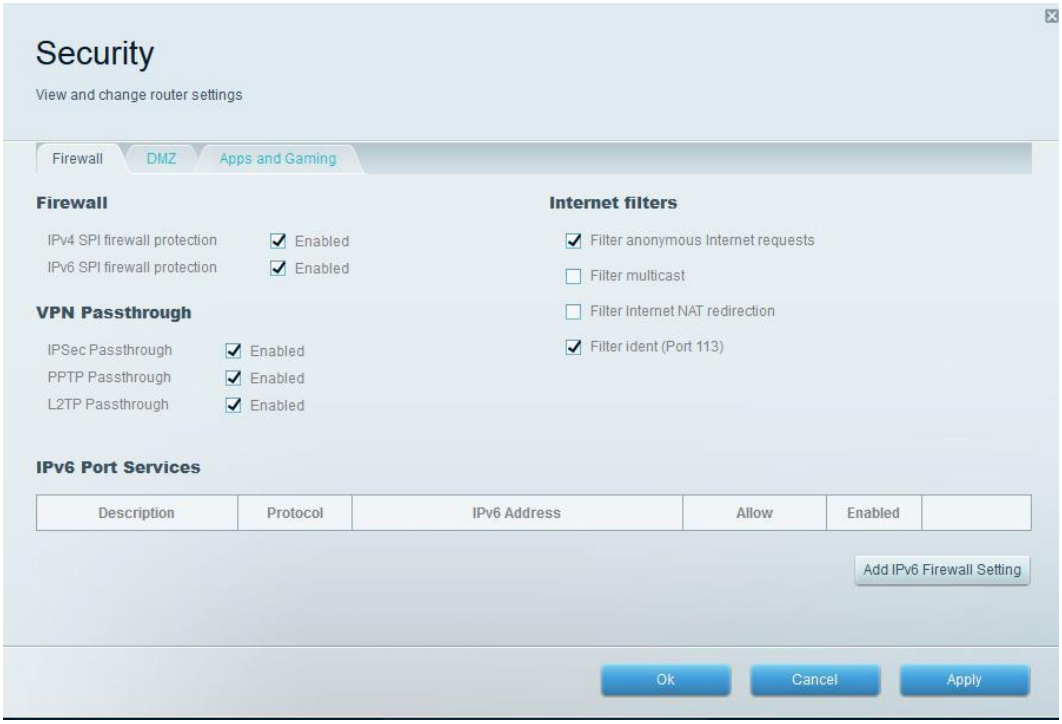
c.



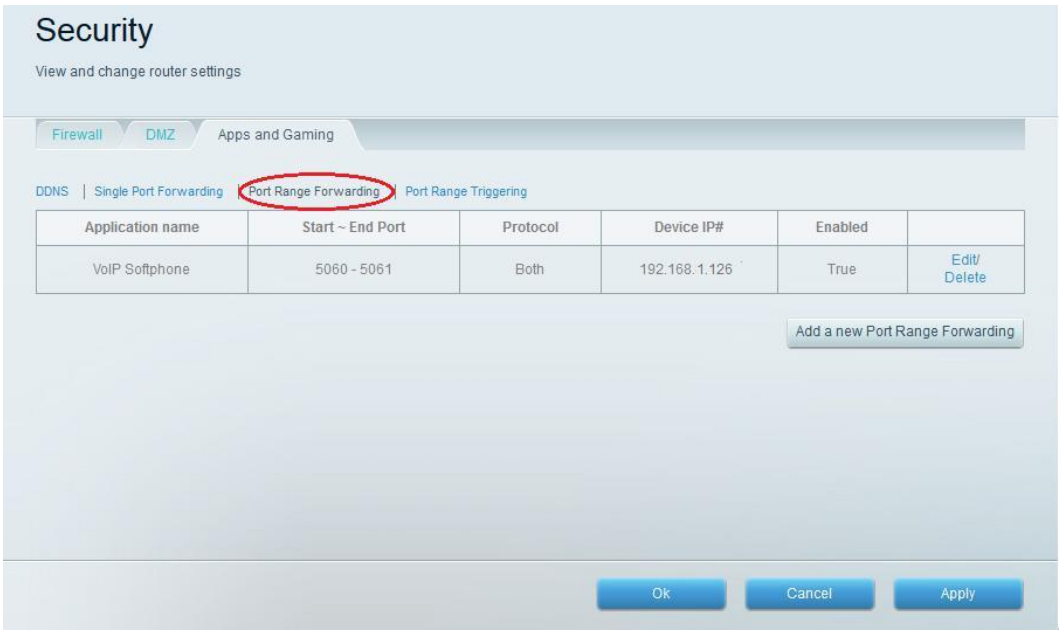
Шаг 2: Примените настройки межсетевого экрана и переадресации портов.

a. На главной странице Linksys Smart Wi-Fi нажмите **Security (Безопасность)**. В окнах **Безопасность (Security)** доступны вкладки **Firewall (Межсетевой экран)**, **DMZ** и **Apps and Gamig (Приложения и игры)**, на которых можно просмотреть и изменить настройки безопасности маршрутизатора.

b. На вкладке **Firewall (Межсетевой экран)** отображается раздел настроек межсетевого экрана, где можно включить или отключить защиту межсетевого экрана с анализом пакетов с учетом состояния соединений (SPI) для IPv4 и IPv6, параметры транзитной пересылки по виртуальной частной сети (VPN) и интернет-фильтры. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.



c. На вкладке **Apps and Gamig (Приложения и игры)** доступны функции переадресации портов. В этом примере порты 5060 и 5061 открыты для программного телефона VoIP, запущенного на локальном устройстве с IP-адресом 192.168.1.126. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.

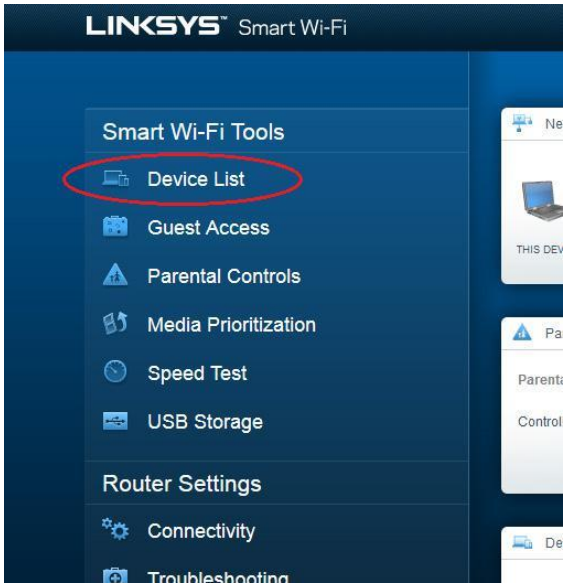


Часть 3: Изучение дополнительных функций на маршрутизаторе Lynksys серии EA

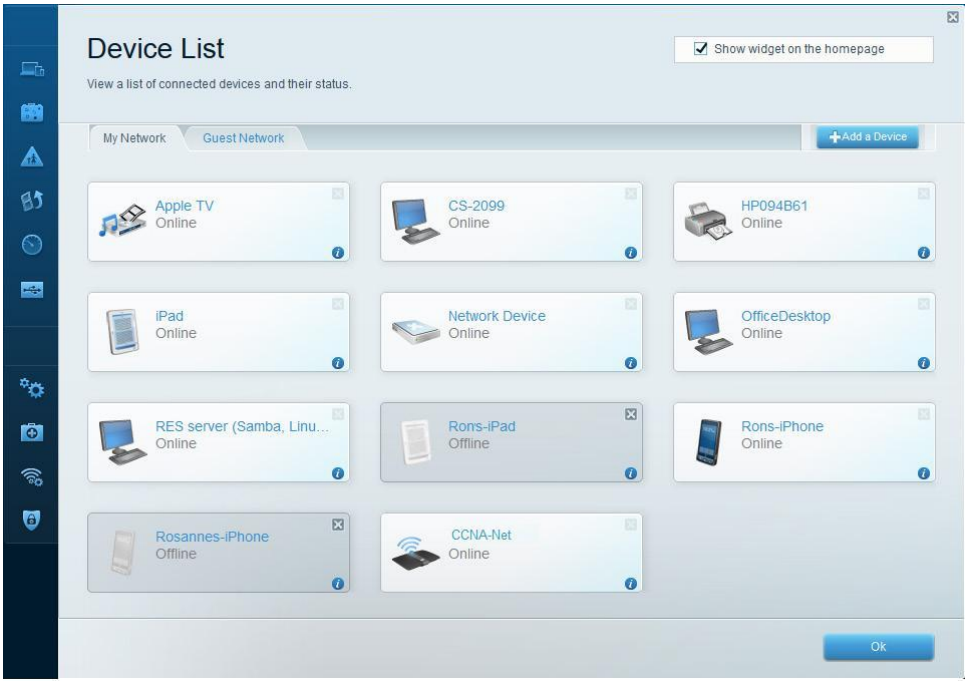
В части 3 вам предстоит рассмотреть ряд дополнительных функций, доступных на маршрутизаторе Linksys EA Series.

Шаг 1: Изучите инструменты Smart Wi-Fi.

a. На главной странице Linksys Smart Wi-Fi нажмите **Device List (Список устройств)**.

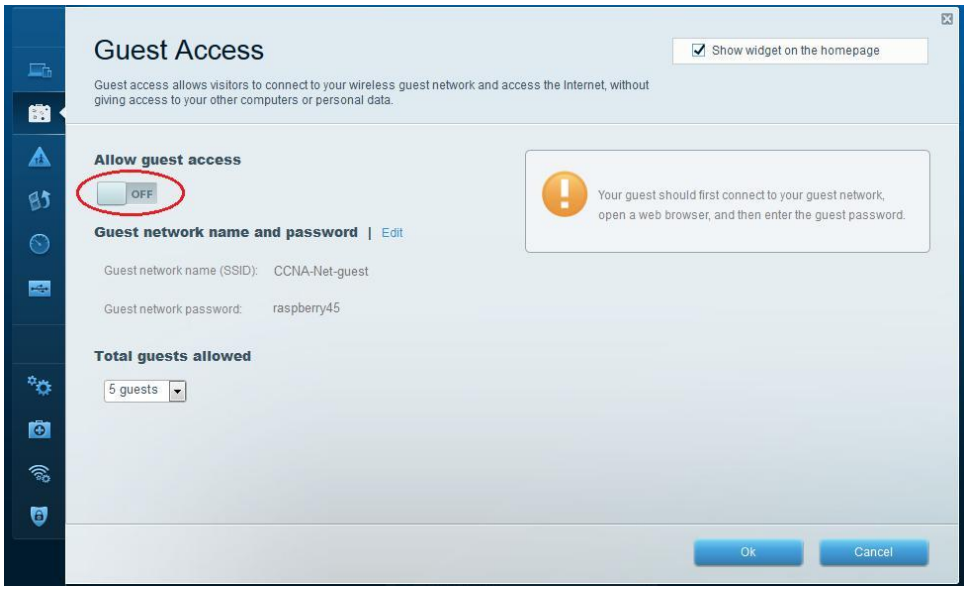


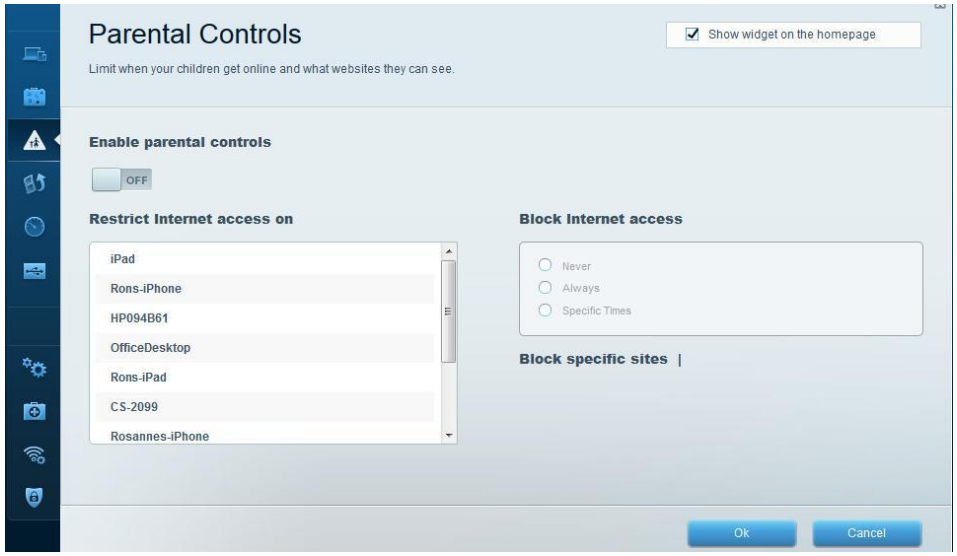
В окне **Список устройств (Device List)** отображается список клиентов в локальной сети. Обратите внимание на вкладку **Guest Network (Гостевая сеть)**. Если гостевая сеть активирована, клиенты этой сети отображаются на вкладке **Guest Network (Гостевая сеть)**.



b. На главной странице Linksys Smart Wi-Fi нажмите **Guest Access (Гостевой доступ)**. Клиенты гостевой сети имеют доступ только к сети Интернет и не имеют доступа к другим клиентам локальной сети. Чтобы разрешить гостевой доступ, нажмите на кнопку **Allow guest access (Разрешить гостевой доступ)**. Щелкните ссылку **Edit (Изменить)** (рядом с именем и паролем гостевой сети), чтобы изменить пароль гостевой сети, и нажмите **OK**, чтобы принять и сохранить изменения.

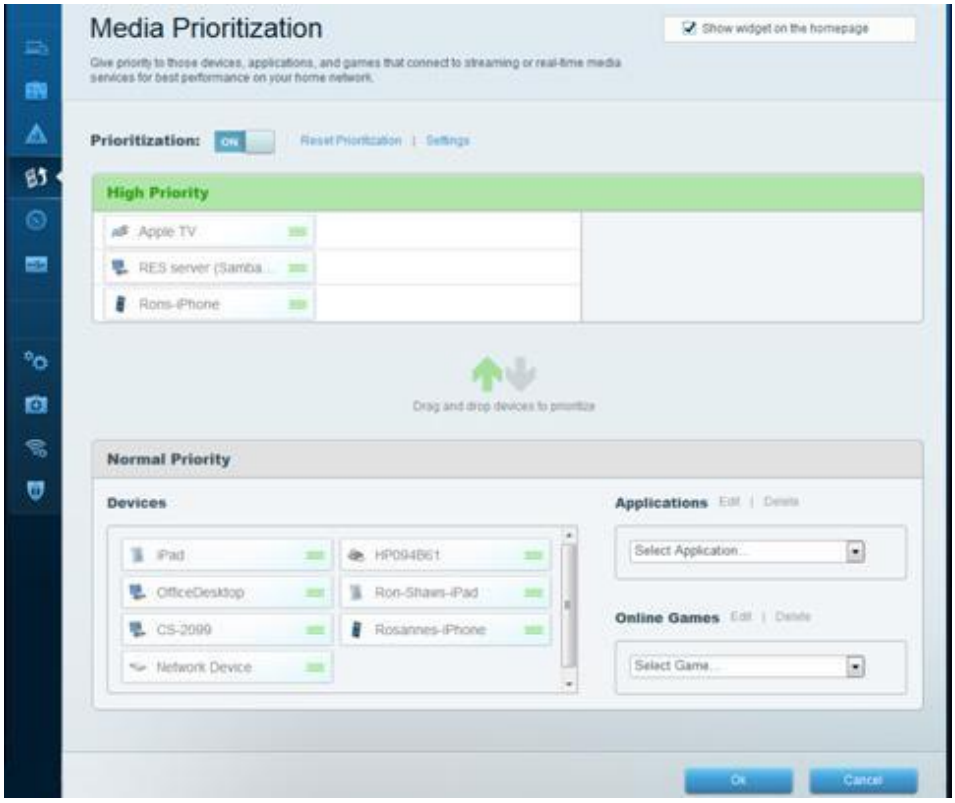
c. На главной странице Linksys Smart Wi-Fi нажмите **Parental Control (Родительский контроль)**. Эти параметры можно использовать для ограничения доступа к Интернету на отдельных устройствах, а также чтобы ограничить доступ по времени и доступ к веб-сайтам. Нажмите **OK**, чтобы сохранить настройки.





d. На главной странице Linksys Smart Wi-Fi выберите **Media Prioritization (Приоритизация мультимедиа)**. С помощью этих параметров можно назначить приоритет пропускной способности сети для выбранных устройств в локальной сети. В этом примере устройству, помеченному как «Apple TV», назначается самый

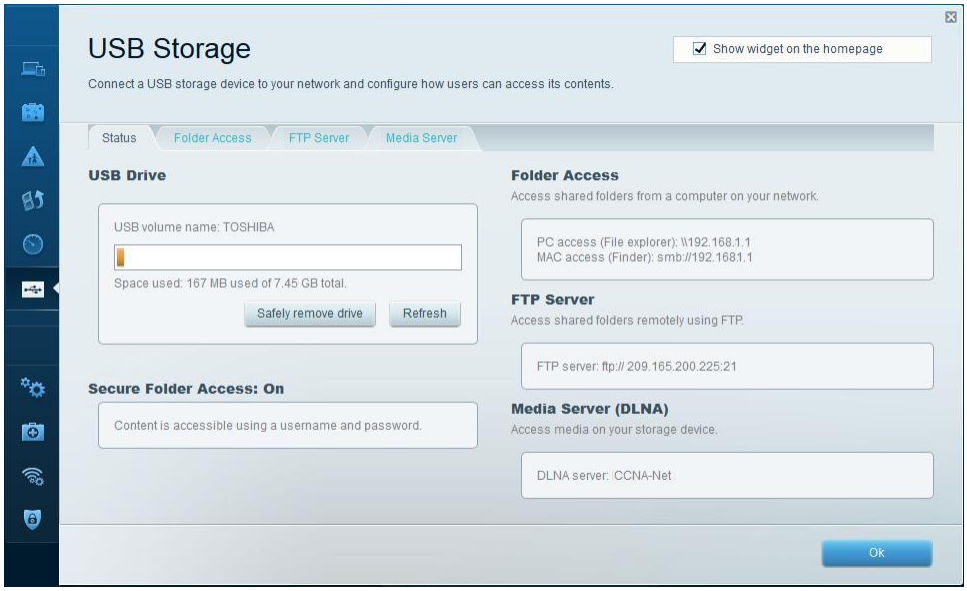
высокий приоритет для ресурсов сети. Чтобы изменить настройки приоритетов, просто перетащите устройства в списке и нажмите **OK**, чтобы сохранить настройки.



e. На главной странице Linksys Smart Wi-Fi нажмите **Speed Test (Проверка скорости)**. Эта утилита используется для проверки скорости доступа к Интернету. В этом примере показаны результаты проверки скорости. Маршрутизатор сохраняет результаты всех проверок скорости и предоставляет возможность вывода этих журналов на экран.

f. На главной странице Linksys Smart Wi-Fi нажмите **USB Storage (Устройство хранения USB)**. Этот экран используется для просмотра настроек USB-накопителя. Отсюда можно перейти на соответствующую

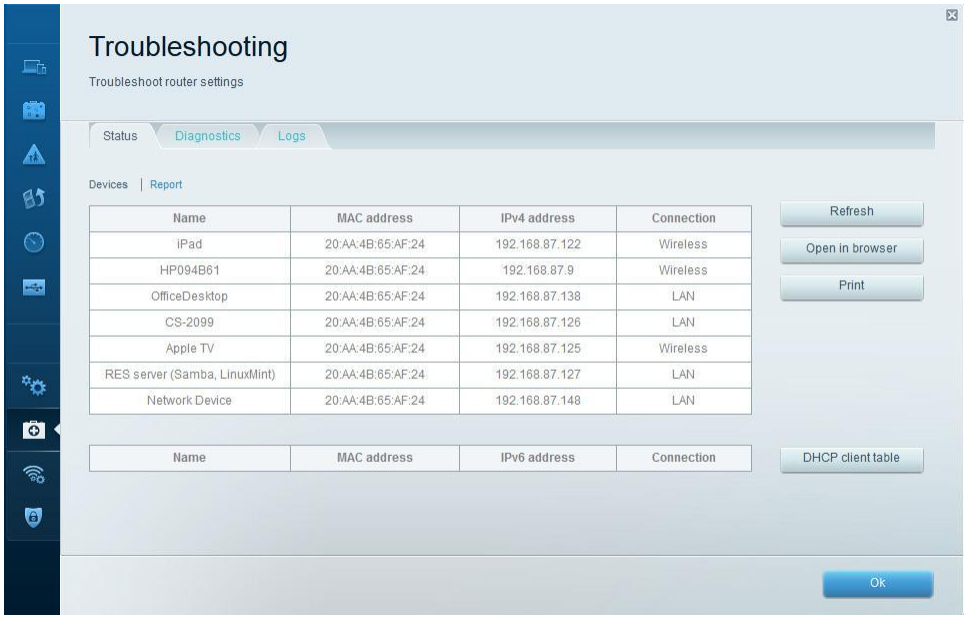
вкладку для настройки FTP-серверов и серверов мультимедиа. Также можно настроить отдельные учетные записи пользователей для доступа к этим серверам. Для этого нажмите вкладки в верхней части данного экрана. Чтобы использовать этот параметр, необходимо подсоединить USB-накопитель к задней стенке маршрутизатора. Нажмите **OK**, чтобы сохранить все внесённые изменения.



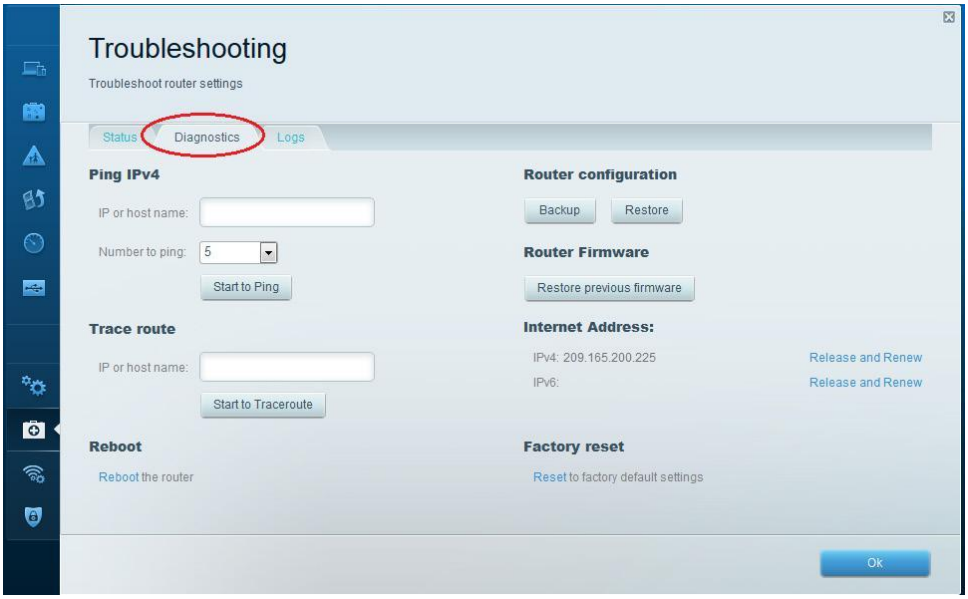
Шаг 2: Поиск и устранение неполадок в работе маршрутизатора.

На главной странице Linksys Smart Wi-Fi нажмите **Troubleshooting (Поиск и устранение неполадок)**.

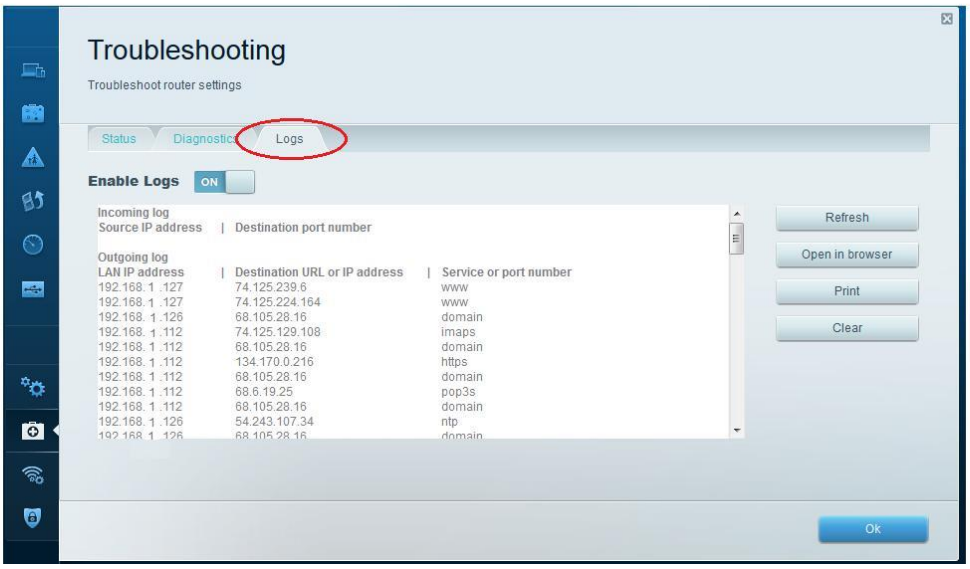
a. На вкладке **Status (Состояние)** представлен список клиентов локальной сети, а также MAC-адреса и IP-адреса их сетевых адаптеров. На этой вкладке также отображается способ их подключения к сети. Нажмите **OK**, чтобы сохранить все внесённые изменения.



На вкладке **Diagnostics (Диагностика)** представлены утилиты ping и traceroute. С помощью этой вкладки также можно перезагрузить маршрутизатор, выполнить резервное копирование или восстановление конфигурации маршрутизатора, восстановить предыдущую версию микропрограммного обеспечения, опубликовать и обновить интернет-адреса на своем маршрутизаторе и выполнить сброс до заводских настроек по умолчанию. Нажмите **OK**, чтобы сохранить все внесённые изменения.



с. На вкладке **Logs (Журналы)** доступны журналы «Входящие», «Исходящие», «Безопасность» и «DHCP». С этого экрана можно отправить журналы на печать или удалить их. Нажмите **OK**, чтобы сохранить все внесённые изменения.

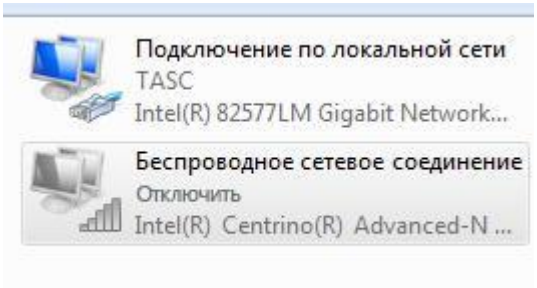


Часть 4: Подключение клиента беспроводной сети

В части 4 вам предстоит настроить адаптер беспроводной сети на компьютере для подключения к маршрутизатору Linksys EA Series.

Примечание. Данная лабораторная работа была выполнена на ПК под управлением ОС Windows 7. Ее можно выполнить и с любой другой из указанных версий операционной системы Windows, однако параметры меню и окна в этом случае могут отличаться.

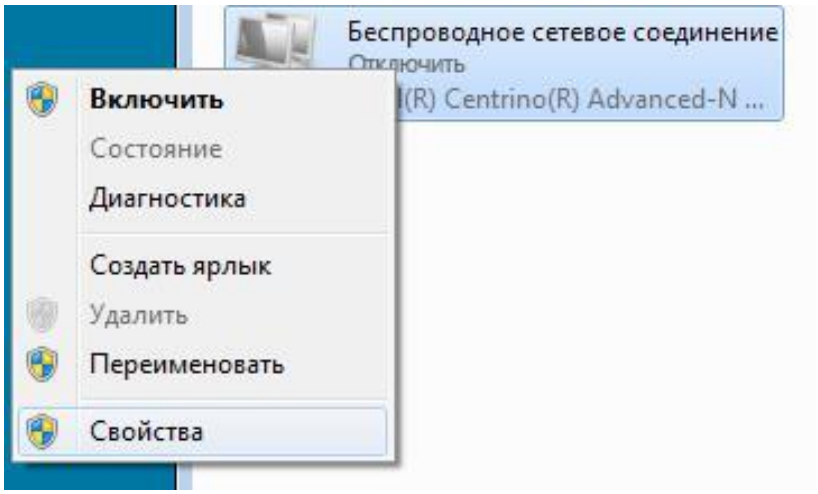
Шаг 3: Используйте «Центр управления сетями и общим доступом». Откройте **Центр управления сетями и общим доступом**, нажав кнопку **Пуск > Панель управления > Просмотр состояния сети и задач** под заголовком «Сеть и Интернет» в представлении по категориям. В левой части экрана нажмите на ссылку **Изменение параметров адаптера**. Откроется окно **Сетевые подключения** со списком доступных сетевых адаптеров на этом компьютере. В данном окне найдите адаптеры **Подключение по локальной сети** и **беспроводное сетевое соединение**.



Примечание. В этом окне могут отображаться также адаптеры виртуальной частной сети (VPN) и другие типы сетевых подключений.

Шаг 4: Поработайте с беспроводным сетевым адаптером.

Выберите и щелкните правой кнопкой мыши параметр **беспроводное сетевое соединение**, чтобы отобразить раскрывающийся список. Если сетевой адаптер отключен, необходимо **Включить** его.



b. Нажмите правой кнопкой мыши на **Wireless Network Connection (беспроводное сетевое соединение)**, и выберите **Connect/Disconnect (Подключить/Отключить)**. Здесь показан список идентификаторов SSID в

диапазоне действия сетевого адаптера. Выберите **CCNA-Net**, затем нажмите **Connect (Подключить)**.

- Когда отобразится соответствующий запрос, введите **cisconet**, чтобы указать ключ безопасности сети, после чего нажмите **OK**.

Если доступно подключение к беспроводной сети, на панели задач должен отображаться значок беспроводной сети. Нажмите на этот значок, чтобы отобразить список идентификаторов SSID в диапазоне действия сетевого адаптера.

Идентификатор SSID **CCNA-Net** теперь должен показывать подключение к беспроводной сети CCNA.

Вопросы на закрепление

Почему вам не стоит использовать инструменты безопасности WEP для своей беспроводной сети?

_____

_____

_____

Лабораторная работа № 9

На тему: Настройка базового протокола OSPFv2 для одной области

Топология

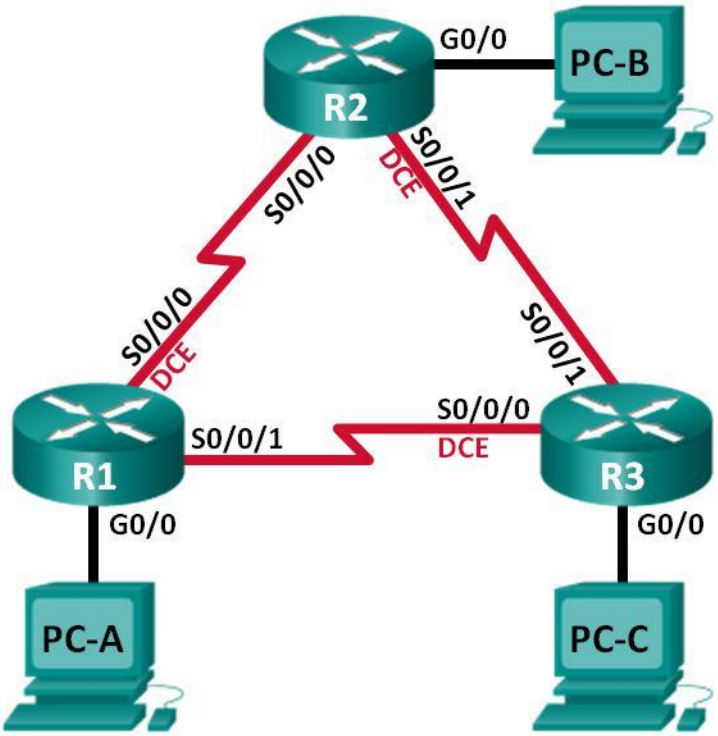


Таблица адресации

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 лабораторной 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, 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
L192.168.1.1/32 is directly connected, GigabitEthernet0/0
O192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O192.168.3.0/24 [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
C192.168.12.0/30 is directly connected, Serial0/0/0
L192.168.12.1/32 is directly connected, Serial0/0/0 192.168.13.0/24 is
variably subnetted, 2 subnets, 2 masks
C192.168.13.0/30 is directly connected, Serial0/0/1
L192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
```

```
O192.168.23.0/30 [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
```

Какую команду вы бы применили, чтобы просмотреть только маршруты OSPF в таблице маршрутизации?

_____

_____

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.

```
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	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

b. Для того чтобы увидеть более подробные данные об интерфейсах, на которых активирован OSPF, выполните команду **show ip ospf interface**.

```
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 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)
        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 00:00:03
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

Adjacent with neighbor 192.168.23.1
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**.

a. 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 маршрут 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
L192.168.2.1/32 is directly connected, GigabitEthernet0/0
```

```
O192.168.3.0/24 [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
C192.168.12.0/30 is directly connected, Serial0/0/0
L192.168.12.2/32 is directly connected, Serial0/0/0 192.168.13.0/30
is subnetted, 1 subnets
O192.168.13.0 [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
L192.168.23.1/32 is directly connected, Serial0/0/1
```

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

a. 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 default** на R2, чтобы 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)
```

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**.

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.

a. 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# 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
O192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O192.168.23.0 [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**.

```
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.
```

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.

```
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          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
O192.168.3.0/24 [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 1565 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 таблице 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-ISinter 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
O192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
192.168.23.0/30 is subnetted, 1 subnets
O192.168.23.0 [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.

Лабораторная работа № 10

На тему: Настройка OSPFv2 в сети множественного доступа

Топология

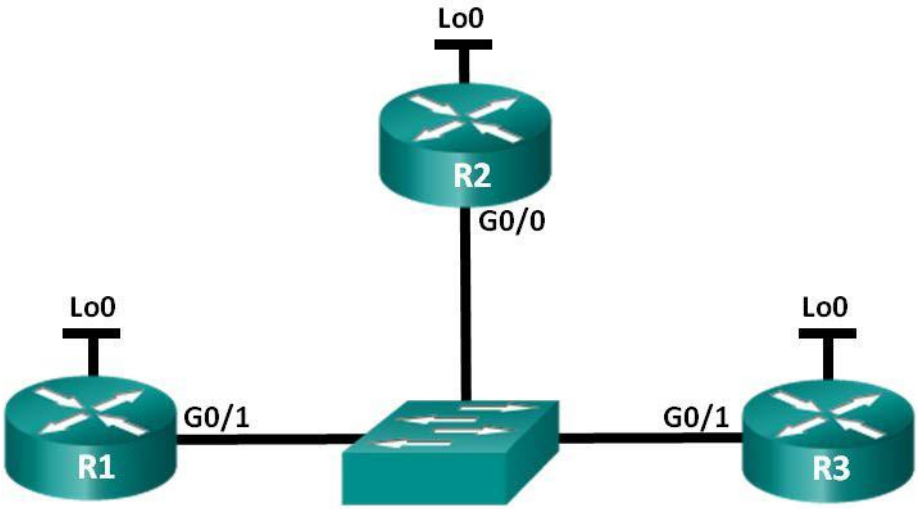


Таблица адресации

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:

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

n. Отключите поиск DNS.

o. Настройте имена устройств в соответствии с топологией.

p. Назначьте **class** в качестве пароля привилегированного режима.

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

r. Зашифруйте пароли.

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

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

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

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

В Сохраните текущую конфигурацию в загрузочную конфигурацию.

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

4. 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.

108 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?

_____

_____

109 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.

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.

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

_____

_____

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.

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.

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
```

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    GigabitEthernet0/1
192.168.31.33      1   FULL/DR         00:00:30    192.168.1.3    GigabitEthernet0/1
```

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

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

i. Изменилось ли назначение DR?

_____

j. 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.

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
  Supports Link-local Signaling (LLS)
  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

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

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

i. Что означает приоритет интерфейса 255?

_____

_____

_____

_____

_____

_____

_____

_____

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

j. 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.

Лабораторная работа № 11

На тему: Настройка расширенных функций OSPFv2

Топология

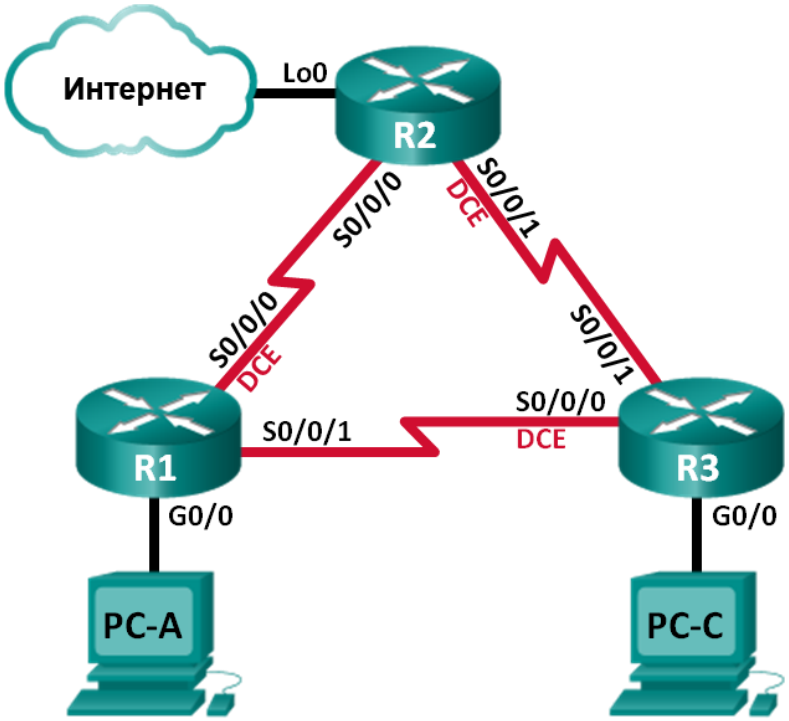


Таблица адресации

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    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
```

b. Выполните команду **bandwidth 128** на всех последовательных интерфейсах.

c. Выполните команду **show ip ospf interface brief**, чтобы просмотреть новые

значения 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    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
```

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. Повторно выполните команду **show ip route ospf** на R1, чтобы просмотреть 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


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 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.

Лабораторная работа № 12

На тему: Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области

Топология

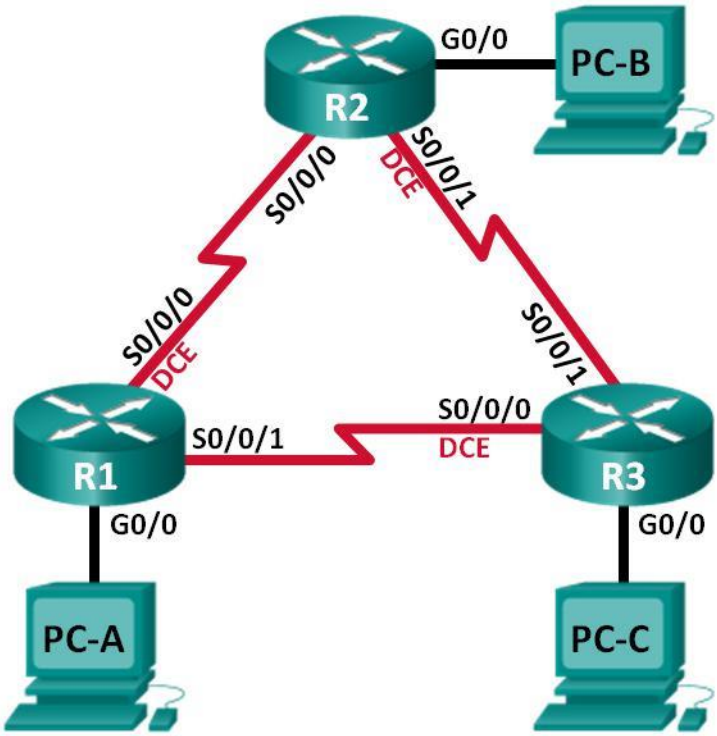


Таблица адресации

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	N/A

			FE80::1 link-local	
		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	192.168.1.1

			2001:DB8:ACAD:A::A/64	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:

b. 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

c. 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

d. консольные кабели для настройки устройств Cisco IOS через порты консоли;

e. 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 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.

Введите команду **show ip interface brief** на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up). Запишите полученные результаты.

_____
_____
_____
_____
_____
_____
_____
_____

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.

_____
_____
_____
_____
_____
_____
_____
_____

Устраните все обнаруженные неполадки. Запишите команды, используемые для исправления неполадок.

_____
_____
_____
_____
_____
_____
_____
_____

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?

_____

f. 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.

_____
_____
_____
_____
_____
_____
_____
_____

c. Внесите требуемые изменения в конфигурацию маршрутизатора R1, исходя из результатов команды **show ip protocols**. Запишите команды, используемые для исправления неполадок.

_____
_____
_____
_____
_____
_____
_____
_____

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.

e. 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**.

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.

_____

_____

_____

_____

_____

_____

_____

_____

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.

e. 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**.

f. 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 всесети 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.

c. 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**.

d. 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?

_____
_____

3. 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

с. 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 IPv6-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 IPv6-маршрутизации на маршрутизаторе является использование команды **show run | section ipv6 unicast**. Если добавить вертикальную линию (|)

В 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.

_____

_____

_____

_____

_____

_____

c. 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.

B Введите команду **show ipv6 ospf interface g0/0**, чтобы убедиться, что этот интерфейс не объявляет маршруты OSPFv3.

d. 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.

_____
_____
_____
_____
_____
_____
_____
_____

e. Введите необходимые изменения конфигурации на маршрутизаторе R2. 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 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.

_____
_____
_____

_____
_____
_____
_____
_____

g. Выполните необходимые изменения конфигурации на маршрутизаторе R3. 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 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.

Лабораторная работа № 13

На тему: Поиск и устранение неполадок в работе усовершенствованного протокола OSPFv2 для одной области

Топология

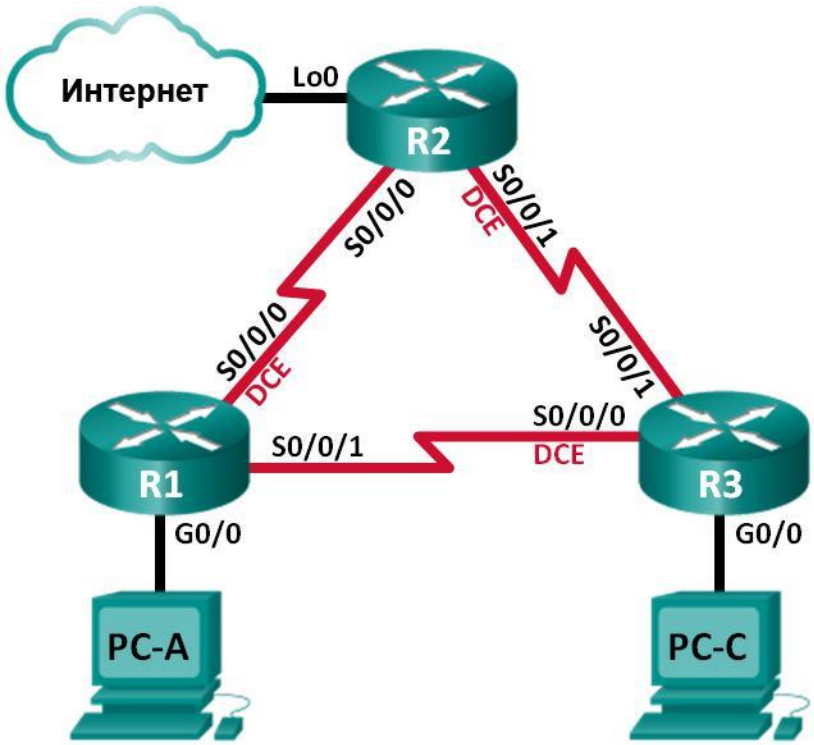


Таблица адресации

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;
- В 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

- каналов vty — **cisco**.

Конфигурация маршрутизатора R1:

```
conf t
hostname 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 128
 ip address 192.168.12.1 255.255.255.252
 ip ospf message-digest-key 1 md5 MD5LINKS
 clock rate 128000
 no shut
interface Serial0/0/1
 bandwidth 64
 ip ospf message-digest-key 1 md5 MD5LINKS
 ip address 192.168.13.1 255.255.255.252
 no shut
router ospf 1
 auto-cost reference-bandwidth 1000
 area 0 authentication message-digest
 passive-interface g0/0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 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
```

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 182
 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:

```
conf t
hostname R3
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 no shut
interface Serial0/0/0
 bandwidth 128
 ip ospf message-digest-key 1 md5 MD5LINKS
 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**	**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

5. 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.

Лабораторная работа № 14

На тему: Владение навыками поиска и устранения неполадок в работе OSPF

Задача

Описание процесса и инструментов, применяемых для поиска и устранения неполадок в сетях OSPF для одной области.

Сценарий

Вы решили изменить протокол маршрутизации с RIPv2 на OSPFv2. Исходные физические параметры топологии сети вашего предприятия малого или среднего бизнеса останутся неизменными. Используйте для сети вашего предприятия малого или среднего бизнеса схему из PDF-файла к этому упражнению.

Схема адресации готова, после этого вы настраиваете IPv4 и VLSM на своих маршрутизаторах.

В качестве протокола маршрутизации используется OSPF. Однако не все маршрутизаторы делятся информацией о маршрутах друг с другом.

Для выполнения упражнения обратитесь к инструкциям из файла PDF, прилагающегося к этому упражнению.

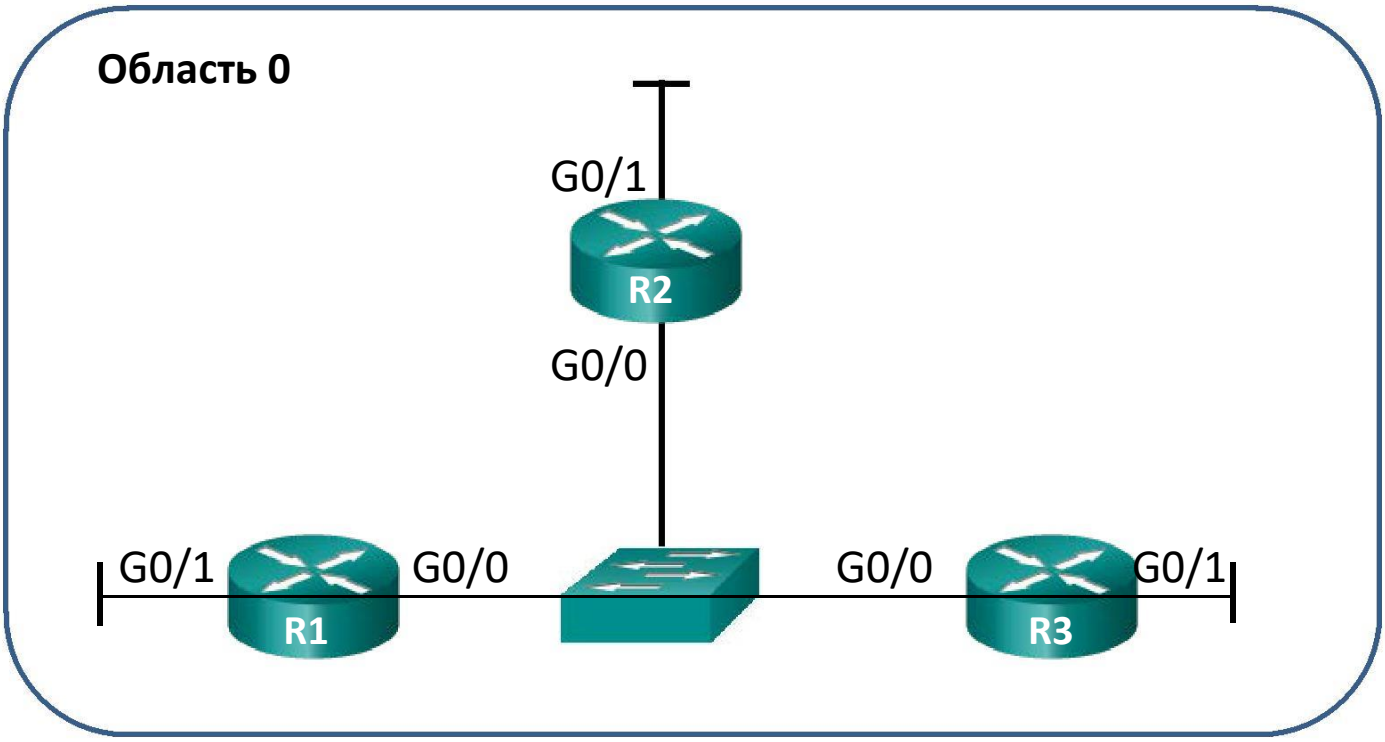
По завершении необходимых действий класс должен снова объединиться и сравнить зарегистрированное время исправления настроек. Группа, которая быстрее остальных нашла и исправила ошибку

в конфигурации, признается победителем только в том случае, если она также объяснила процесс поиска и устранения неполадок и доказала работоспособность топологии.

Необходимые ресурсы:

- Схема топологии
- Симулятор Packet Tracer
- Таймер

Схема топологии



Инструкции

Выберите в классе партнера для выполнения задания. Для создания схемы топологии этого упражнения используйте Packet Tracer.

Шаг 1: Создайте топологию для этого сценария, используя данные для моделирования на странице упражнения.

Шаг 2: Настройте маршрутизаторы.

a. Используйте IPv4 для всех интерфейсов.

b. Включите VLSM в схему адресации.

c. В конфигурации допустите одну преднамеренную ошибку.

d. Убедитесь, что сеть не работает из-за этой ошибки.

e. Сохраните файл, который будет использоваться на шаге 3.

Шаг 3: Обменяйтесь своими файлами Packet Tracer с другой группой.

a. Найдите ошибку конфигурации в сетевом файле Packet Tracer, полученном от другой группы.

b. Исправьте ошибку конфигурации OSPF, чтобы восстановить работу сети.

_____
_____
_____
_____
_____

В Запишите, сколько времени вам понадобилось на поиск и устранение сетевой ошибки OSPF.

_____
_____
_____
_____

В После этого соберитесь всем классом, чтобы выбрать лучшего специалиста по устранению неполадок.

Лабораторная работа № 15

На тему: Настройка OSPFv2 для нескольких областей

Топология

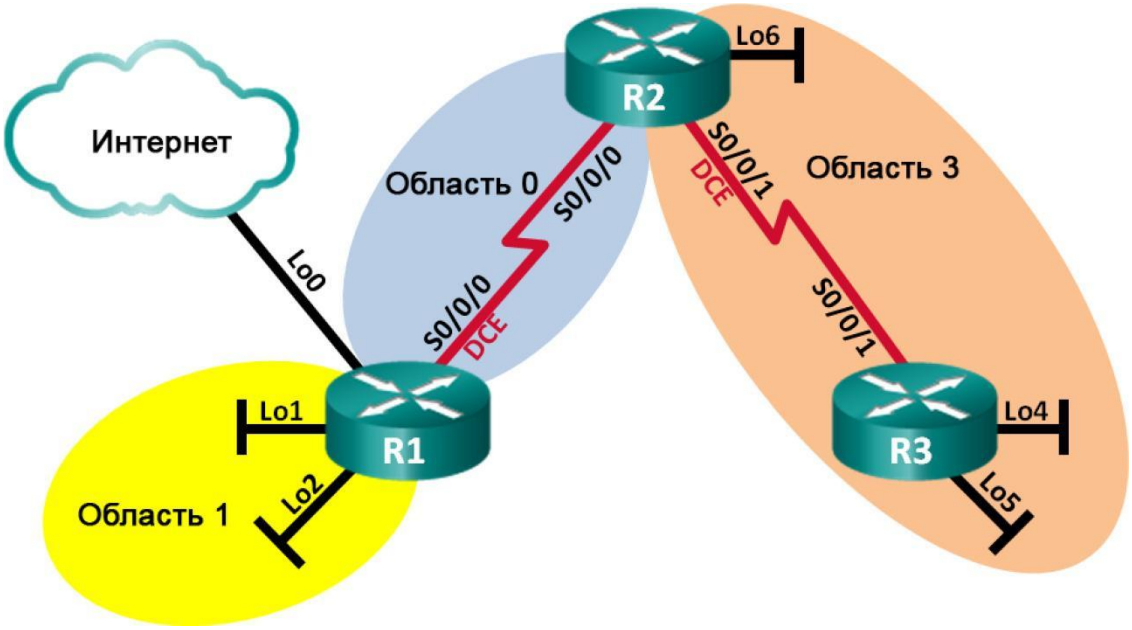


Таблица адресации

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.

1. Отключите поиск DNS.

m. Задайте имя устройства в соответствии с топологией.

n. Назначьте **class** в качестве пароля привилегированного режима.

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

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

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

r. 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.

s. 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 в 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.

j. Настройте идентификатор маршрутизатора 1.1.1.1 с идентификатором процесса OSPF 1.

k. Добавьте OSPF для сетей маршрутизатора R1.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 1 R1(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
```

l. Настройте все интерфейсы loopback локальной сети, Lo1 и Lo2, как пассивные.

m. 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.

n. Настройте для протокола OSPF распространение маршрутов в областях OSPF.

Шаг 3: Настройте протокол OSPF на маршрутизаторе R2.

C Настройте идентификатор маршрутизатора 2.2.2.2 с идентификатором процесса OSPF 1.

C 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.

k. Настройте идентификатор маршрутизатора 3.3.3.3 с идентификатором процесса OSPF 1.

e. Добавьте OSPF для сетей маршрутизатора R3. Запишите использованные команды в поле ниже.

_____
_____
_____
_____
_____
_____

f. Настройте все интерфейсы loopback локальных сетей как пассивные.

Шаг 5: Убедитесь в правильности настройки протокола OSPF и в установлении отношений смежности между маршрутизаторами.

d. 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 allinterfaces is not set
          Incoming update filter list for allinterfaces is not set
          Router ID 1.1.1.1
          It is an area border and autonomoussystem 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:

_____

_____

В Введите команду **show ip ospf neighbor**, чтобы убедиться в 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    Serial0/0/0

    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    Serial0/0/0
    3.3.3.3            0 FULL/     -     00:00:36      192.168.23.2    Serial0/0/1

R3# show ip ospf neighbor

    Neighbor ID      Pri State           Dead Time      Address         Interface
    2.2.2.2            0 FULL/     -     00:00:38      192.168.23.1    Serial0/0/1
```

d. Для отображения суммарной стоимости маршрута используйте сокращенную команду **show ip 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 интерфейсов.

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.

f. Введите команду **show ip route ospf** на маршрутизаторе R1. Для маршрутов OSPF, начинающихся в другой области, используется дескриптор (O IA), обозначающий межобластные маршруты.

g.

```
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 NSSAexternal   type2
              E1  -OSPF external type 1, E2 - OSPF   external type2
              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
              c.    - replicated route, % - next hop

       override Gateway of last resort is 0.0.0.0 to network

       0.0.0.0


             192.168.4.0/32is subnetted, 1 subnets
       O IA     192.168.4.1[110/1563] via 192.168.12.2, 00:23:49, Serial0/0/0
             192.168.5.0/32is 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
```

e. 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.

4. Введите команду **show ip ospf database** на маршрутизаторе R1. Маршрутизатор ведет отдельную базу данных LSDB для каждой области, участником которой является этот маршрутизатор.

5.

```
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
       192.168.23.02.2.2.2          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
       192.168.12.01.1.1.1          1387           0x80000001 0x00C0F5
       192.168.23.01.1.1.1          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
```

d. 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.

d. Рассчитайте суммарный маршрут для сетей в области 1.

e. 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
```

f. Рассчитайте суммарный маршрут для сетей в области 3. Запишите результаты.

_____
_____

g. 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**	**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

g.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.

Лабораторная работа № 16

На тему: Настройка OSPFv3 для нескольких областей

Топология

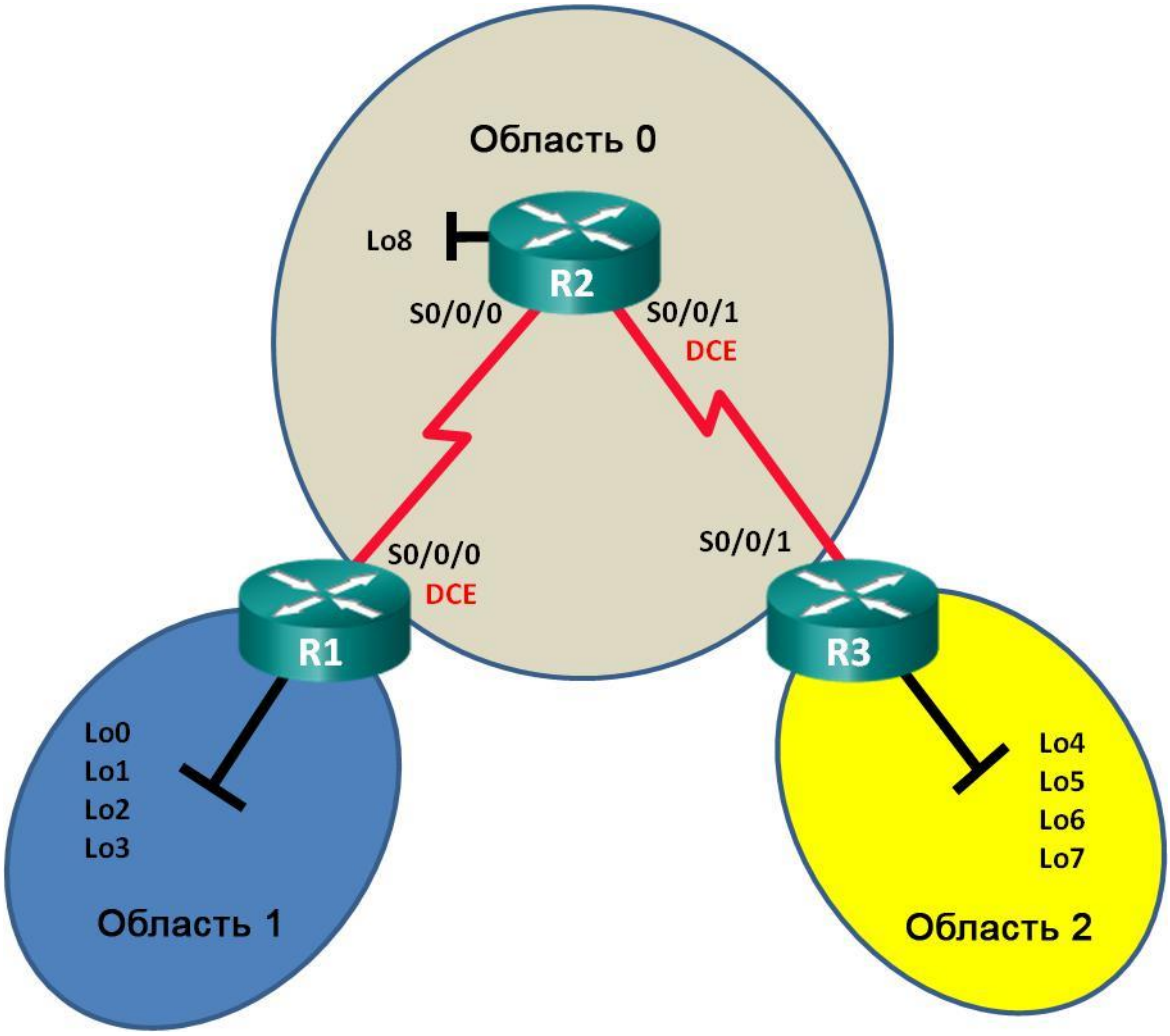


Таблица адресации

Устройство	Интерфейс	IPv6-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 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:

j. 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

k. 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала,
например Tera Term);

l. консольные кабели для настройки устройств Cisco IOS через порты консоли;

m. 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.

g. Отключите поиск DNS.

h. Настройте имя устройств в соответствии с топологией.

i. Назначьте **class** в качестве пароля привилегированного режима.

j. Установите **cisco** в качестве пароля vty.

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

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

m. Зашифруйте все незашифрованные пароли.

n. Настройте для всех интерфейсов индивидуальные адреса и link-local адреса IPv6 каналов, приведённые в таблице адресации.

o. Включите маршрутизацию для индивидуальной адресации IPv6 на каждом маршрутизаторе.

p. 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

d. 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.

В 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.

В Назначьте маршрутизатору R1 идентификатор маршрутизатора OSPFv3 **1.1.1.1**.

```
R1(config-rtr)# router-id 1.1.1.1
```

В Задайте для маршрутизатора R2 идентификатор **2.2.2.2**, а для маршрутизатора R3 — идентификатор **3.3.3.3**.

В 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.

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
```

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
```

h. 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.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

i. Используйте команду **show ipv6 ospf interface brief**, чтобы просмотреть, для каких интерфейсов включена поддержка OSPFv3.

```
R2# show ipv6 ospf interface brief
```

```
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
```

j. 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.

6. 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
```

b. Введите команду **show ipv6 route ospf** 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, 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: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
      h.  2001:DB8:ACAD:8::/64 [110/65]
            via FE80::2, Serial0/0/0
      e.  2001:DB8:ACAD:23::/64 [110/128]
            via FE80::2, Serial0/0/0
```

Что означает метка OI для маршрута?

_____

_____

f. 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

d. части 3 необходимо вручную настроить суммирование межобластных маршрутов на маршрутизаторах ABR.

Шаг 1: Выполните объединение сетей на маршрутизаторе R1.

f. 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

d. 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

e. 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? _____

f. Скопируйте совпадающие биты и добавьте нулевые биты, чтобы определить объединённый сетевой адрес (префикс).

2001:DB8:ACAD: 0000 0000 0000 0000::0

g. Перекодируйте двоичную часть обратно в шестнадцатеричный код.

2001:DB8:ACAD::

h. Добавьте префикс объединённого маршрута (результат шага 1c).

2001:DB8:ACAD::/62

Шаг 2: Настройте суммирование межобластных маршрутов на маршрутизаторе R1.

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
```

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.

e. Объедините интерфейсы loopback на маршрутизаторе R3.

Выведите список сетевых адресов и определите гекстет, в котором адреса различаются.

Перекодируйте различающиеся части из шестнадцатеричного в двоичный код.

Подсчитайте число крайних слева совпадающих битов для определения префикса объединённого маршрута.

Скопируйте совпадающие биты и добавьте нулевые биты, чтобы определить объединённый сетевой адрес (префикс).

Перекодируйте двоичную часть обратно в шестнадцатеричный код.

Добавьте префикс суммарного маршрута.

Запишите объединённый адрес в отведённом для этого поле.

_____
_____
_____
_____
_____
_____
_____

d. Вручную настройте суммирование межобластных маршрутов на маршрутизаторе R3. Запишите команды в предусмотренной для этого области.

_____
_____
_____
_____

e. Убедитесь, что маршруты области 2 объединены на маршрутизаторе R1. Какая команда была использована?

f. Запишите элемент таблицы маршрутизации на маршрутизаторе R1 для суммарного маршрута, объявленного маршрутизатором R3.

Вопросы на закрепление

С Почему нужно использовать OSPFv3 для нескольких областей?

С 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**	**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.

Лабораторная работа № 17

На тему: Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей

Топология

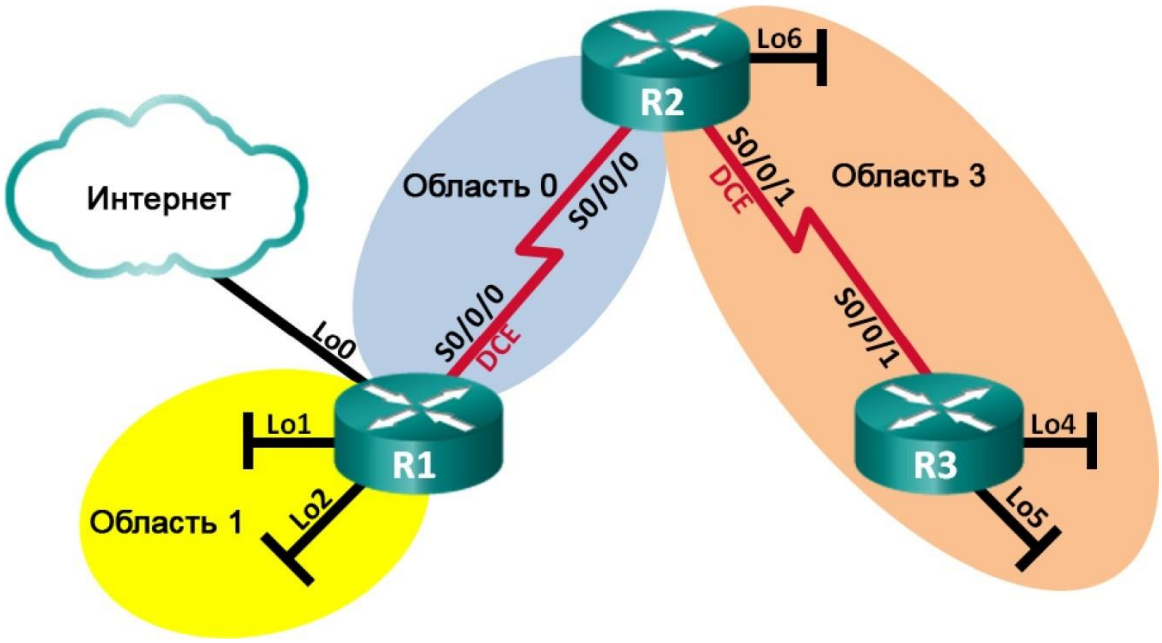


Таблица адресации

Устройство	Интерфейс	IP-адрес
R1	Lo0	209.165.200.225/30
	Lo1	192.168.1.1/24 2001:DB8:ACAD:1::1/64 FE80::1 link-local
	Lo2	192.168.2.1/24 2001:DB8:ACAD:2::1/64 FE80::1 link-local
	S0/0/0 (DCE)	192.168.12.1/30 2001:DB8:ACAD:12::1/64 FE80::1 link-local
R2	S0/0/0	192.168.12.2/30 2001:DB8:ACAD:12::2/64 FE80::2 link-local
	S0/0/1 (DCE)	192.168.23.2/30 2001:DB8:ACAD:23::2/64 FE80::2 link-local

	Lo6	192.168.6.1/24 2001:DB8:ACAD:6::1/64 FE80::2 link-local
R3	Lo4	192.168.4.1/24 2001:DB8:ACAD:4::1/64 FE80::3 link-local
	Lo5	192.168.5.1/24 2001:DB8:ACAD:5::1/64 FE80::3 link-local
	S0/0/1	192.168.23.1/30 2001:DB8:ACAD:23::1/64 FE80::3 link-local

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 выбора кратчайшего пути (OSPF) — это протокол маршрутизации (с открытым стандартом) на базе состояния каналов для IP-сетей. OSPFv2 определен для сетей на основе протокола IPv4, а OSPFv3 определен для сетей на основе протокола IPv6. Протоколы маршрутизации OSPFv2 и OSPFv3 полностью изолированы друг от друга, т. е. изменения OSPFv2 не влияют на маршрутизацию OSPFv3.

В этой лабораторной работе в сети OSPF для нескольких областей, использующей OSPFv2 и OSPFv3, возникают 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);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и загрузка конфигураций устройств

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Загрузите файлы конфигурации маршрутизатора.

Загрузите следующие конфигурации в соответствующий маршрутизатор. На всех маршрутизаторах настроены одинаковые пароли. Паролем привилегированного режима является **class**, а паролем канала **— cisco**.

Конфигурация маршрутизатора R1:

```
ena
ble
con
f t
hos
tna
me
R1
enable
secret class
ipv6
unicast-
routing no
ip domain
lookup
interface
Loopback0
 ip address 209.165.200.225 255.255.255.252
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
 ipv6 address
 2001:DB80:ACAD:1::1/64 ipv6
 ospf network point-to-point
interface Loopback2
 ip address 192.168.2.1 255.255.255.0
 ipv6 address
 2001:DB8:ACAD:2::1/64 ipv6
 ospf 1 area 1
 ipv6 ospf network point-
to-point interface
Serial0/0/0
 ip address 192.168.21.1 255.255.255.252
 ipv6 address FE80::1 link-
```

```
 local ipv6 address
 2001:DB8:ACAD:12::1/64 ipv6
 ospf 1 area 0
 clock
 rate
 128000
 shutdown
router ospf 1
 router-id 1.1.1.1
 passive-interface
 Loopback1 passive-
 interface Loopback2
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.12.0
 0.0.0.3 area 0 default-
 information originate
ipv6 router ospf 1
 area 1 range
2001:DB8:ACAD::/61 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
 logging
 synchronous
 login
 transport
input all
end
```

Конфигурация маршрутизатора R2:

```
ena
ble
con
f t
hos
tna
me
R2
ipv6
unicast-
routing no
```

```
ip domain
lookup
enable
secret class
interface
Loopback6
 ip address 192.168.6.1 255.255.255.0
 ipv6 address
2001:DB8:CAD:6::1/64
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.252
 ipv6 address FE80::2 link-
 local ipv6 address
 2001:DB8:ACAD:12::2/64 ipv6
 ospf 1 area 0
 no shutdown
interface
Serial0/0/1
 ip address 192.168.23.2 255.255.255.252
 ipv6 address FE80::2 link-
 local ipv6 address
 2001:DB8:ACAD:23::2/64 ipv6
 ospf 1 area 3
 clock
 rate
 128000 no
 shutdown
router ospf 1
 router-id 2.2.2.2
 passive-interface Loopback6
 network 192.168.6.0 0.0.0.255 area 3
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0
0.0.0.3 area 3 ipv6 router
ospf 1
 router-id
2.2.2.2
banner
motd @
  Unauthorized Access is
Prohibited! @ line con 0
 password
 cisco
 logging
 synchronous
 login
line vty 0 4
 password
 cisco
```

```
 logging
 synchronous
 login
 transport
input all
end
```

Конфигурация маршрутизатора R3:

```
ena
ble
con
f t
hos
tna
me
R3
no ip domain
lookup ipv6
unicast-
routing
enable
secret class
interface
Loopback4
 ip address 192.168.4.1 255.255.255.0
 ipv6 address
 2001:DB8:ACAD:4::1/64 ipv6
 ospf 1 area 3
interface Loopback5
 ip address 192.168.5.1 255.255.255.0
 ipv6 address 2001:DB8:ACAD:5::1/64
 ipv6 ospf 1
area 3
interface
Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
 ipv6 address FE80::3 link-
 local ipv6 address
 2001:DB8:ACAD:23::1/64 ipv6
 ospf 1 area 3
 no
shutd
own
route
r
ospf
1
 router-id 3.3.3.3
 passive-interface
 Loopback4 passive-
```

```
 interface Loopback5
 network 192.168.4.0 0.0.0.255 area 3
 network 192.168.5.0
0.0.0.255 area 3 ipv6 router
ospf 1
 router-id
3.3.3.3
banner
motd @
  Unauthorized Access is
Prohibited! @ line con 0
 password
 cisco
 logging
 synchronous
 login
line vty 0 4
 password
 cisco
 logging
 synchronous
 login
 transport
input all
end
```

Шаг 3: Сохраните конфигурацию.

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 в том, что интерфейсы, перечисленные в таблице адресации, включены и что для них настроены правильные параметры IP-адресации.

a. Введите команду **show ip interface brief** на всех трех маршрутизаторах, чтобы убедиться, что интерфейсы находятся в активном состоянии (up/up).

b. Введите команду **show run | section interface** для просмотра всех команд, связанных с интерфейсами.

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

_____

_____

_____

_____

d. С помощью команды **ping** убедитесь, что подключения IPv4 и IPv6 настроены на всех напрямую подключенных интерфейсах маршрутизатора. Если проблемы сохраняются, продолжите поиск и устранение проблем на уровне 3.

Часть 3: Поиск и устранение неполадок в работе OSPFv2

Примечание. Интерфейсы локальной сети (loopback) не должны объявлять данные маршрутизации OSPF, но маршруты к этим сетям должны содержаться в таблицах маршрутизации.

Шаг 1: Протестируйте сквозное подключение IPv4.

С каждого маршрутизатора отправьте эхо-запрос на все интерфейсы других маршрутизаторов. Запишите результаты в области ниже, поскольку проблемы подключения IPv4 OSPFv2 действительно существуют.

_____

_____

_____

_____

Шаг 2: Убедитесь, что все интерфейсы маршрутизатора R1 назначены в соответствующие области OSPFv2.

a. Введите команду **show ip protocols**, чтобы убедиться, что OSPF работает и все сети объявлены

в соответствующих областях. Убедитесь, что идентификатор маршрутизатора настроен правильно, в том числе и для OSPF.

b. При необходимости внесите изменения в конфигурацию маршрутизатора R1, используя результаты команды **show ip protocols**. Запишите команды, использованные для внесения изменений в конфигурацию.

_____

_____

_____

_____

c. При необходимости повторно введите команду **show ip protocols**, чтобы убедиться в том, что внесённые изменения привели к желаемому результату.

d. Введите команду **show ip ospf interface brief**, чтобы убедиться в том, что последовательный интерфейс и интерфейсы loopback 1 и 2 указываются как сети OSPF, назначенные
в соответствующие области.

e. Устраните все проблемы OSPFv2, обнаруженные на маршрутизаторе R1.

Шаг 3: Убедитесь, что все интерфейсы маршрутизатора R2 назначены в соответствующие области OSPFv2.

a. Введите команду **show ip protocols**, чтобы убедиться, что OSPF работает и все сети объявлены в соответствующих областях. Убедитесь, что идентификатор маршрутизатора также задан правильно.

b. При необходимости внесите изменения в конфигурацию маршрутизатора R2, используя результаты команды **show ip protocols**. Запишите команды, использованные для внесения изменений в конфигурацию.

_____

_____

_____

_____

c. При необходимости повторно введите команду **show ip protocols**, чтобы убедиться в том, что внесённые изменения привели к желаемому результату.

d. Введите команду **show ip ospf interface brief**, чтобы убедиться, что все интерфейсы указаны как сети OSPF, назначенные в соответствующие области.

e. Устраните все проблемы OSPFv2, обнаруженные на маршрутизаторе R2.

Шаг 4: Убедитесь, что все интерфейсы маршрутизатора R3 назначены в соответствующие области OSPFv2.

a. Введите команду **show ip protocols**, чтобы убедиться, что OSPF работает и все сети объявлены в соответствующих областях. Убедитесь, что идентификатор маршрутизатора также задан правильно.

b. При необходимости внесите необходимые изменения в конфигурацию маршрутизатора R3, используя результаты команды **show ip protocols**. Запишите команды, использованные для внесения изменений в конфигурацию.

_____

_____

_____

_____

c. При необходимости повторно введите команду **show ip protocols**, чтобы

убедиться в том, что внесённые изменения привели к желаемому результату.

d. Введите команду **show ip ospf interface brief**, чтобы убедиться, что все интерфейсы указаны как сети OSPF, назначенные в соответствующие области.

e. Устраните все проблемы OSPFv2, обнаруженные на маршрутизаторе R3.

Шаг 5: Проверьте сведения о соседних маршрутизаторах OSPFv2.

Введите команду **show ip ospf neighbor**, чтобы убедиться, что для каждого маршрутизатора перечислены все соседние маршрутизаторы OSPFv2.

Шаг 6: Проверьте информацию о маршрутах OSPFv2.

a. Введите команду **show ip route ospf**, чтобы убедиться, что каждый маршрутизатор содержит все маршруты OSPFv2 в своих таблицах маршрутизации.

b. Если какие-либо маршруты OSPFv2 отсутствуют в таблицах, найдите и устраните неполадки.

Шаг 7: Проверьте сквозное подключение IPv4.

С каждого маршрутизатора отправьте эхо-запрос на все интерфейсы других маршрутизаторов. Если сквозное подключение IPv4 отсутствует, выполняйте поиск и устранение неполадок, пока не будут решены оставшиеся проблемы.

Часть 4: Поиск и устранение неполадок в работе OSPFv3

Примечание. Интерфейсы локальной сети (loopback) не должны объявлять данные маршрутизации OSPFv3, но маршруты к этим сетям должны содержаться в таблицах маршрутизации.

Шаг 1: Протестируйте сквозное подключение IPv6.

С каждого маршрутизатора отправьте эхо-запрос на все интерфейсы других маршрутизаторов. Запишите результаты в области ниже, поскольку проблемы подключения IPv6 действительно существуют.

_____

_____

_____

_____

Шаг 2: Убедитесь, что одноадресная маршрутизация IPv6 включена на всех маршрутизаторах.

a. Простым способом проверки включения IPv6-маршрутизации на маршрутизаторе является использование команды **show run | section ipv6 unicast**.

Если маршрутизация IPv6 была включена, при добавлении в команду **show run** раздела конвейера отображается команда **ipv6 unicast- routing**.

b. Если одноадресная маршрутизация IPv6 не включена на одном или нескольких маршрутизаторах, включите ее. При необходимости запишите команды, использованные для исправления конфигурации.

_____

_____

_____

_____

Шаг 3: Убедитесь, что все интерфейсы маршрутизатора R1 назначены в соответствующие области OSPFv3.

a. Введите команду **show ipv6 protocols**, чтобы проверить правильность идентификатора маршрутизатора и убедиться, что используемые интерфейсы отображаются в соответствующих областях.

b. При необходимости внесите необходимые изменения в конфигурацию маршрутизатора R1, используя результаты команды **show ipv6 protocols**. Запишите команды, использованные для внесения изменений в конфигурацию. Может потребоваться перезапуск процесса OSPF путем применения команды **clear ipv6 ospf process**.

_____

_____

_____

_____

c. Повторно введите на маршрутизаторе R1 команду **show ipv6 protocols**, чтобы убедиться в том, что внесённые изменения вступили в силу.

d. Введите на маршрутизаторе R1 команду **show ipv6 route ospf**, чтобы убедиться в правильности настройки суммирования межобластных маршрутов.

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 12 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user
       Static route B - BGP, R - RIP, 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::/61 [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:23::/64 [110/128]
     via FE80::2, Serial0/0/0
```

e. Какие сети IPv6 включены в суммирование межобластных маршрутов, показанное в таблице маршрутизации?

_____

_____

_____

_____

f. При необходимости внесите необходимые изменения в конфигурацию маршрутизатора R1. Запишите команды, использованные для внесения изменений в конфигурацию.

_____

_____

_____

_____

g. При необходимости повторно введите команду **show ipv6 route ospf** на маршрутизаторе R1 для проверки внесённых изменений.

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 11 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user
       Static route B - BGP, R - RIP, 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::1/128
[110/128]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:5::1/128 [110/128]
     via FE80::2, Serial0/0/0
OI  2001:DB8:ACAD:23::/64 [110/128]
     via FE80::2, Serial0/0/0
```

Шаг 4: Убедитесь, что все интерфейсы маршрутизатора R2 назначены в соответствующие области OSPFv3.

a. Введите команду **show ipv6 protocols** и убедитесь в правильности идентификатора маршрутизатора и в том, что используемые интерфейсы появляются в соответствующих областях.

b. При необходимости внесите необходимые изменения в конфигурацию маршрутизатора R2, используя результаты команды **show ipv6 protocols**. Запишите команды, использованные для внесения изменений в конфигурацию. Может потребоваться перезапуск процесса OSPF путем применения команды **clear ipv6 ospf process**.

_____

_____

_____

_____

c. Убедитесь, что изменение конфигурации привело к нужному результату.

Шаг 5: Убедитесь, что все интерфейсы маршрутизатора R3 назначены в соответствующие области OSPFv3.

a. Введите команду **show ipv6 protocols**, чтобы проверить правильность идентификатора маршрутизатора и убедиться, что используемые интерфейсы отображаются в соответствующих областях.

b. При необходимости внесите необходимые изменения в конфигурацию маршрутизатора R3, используя результаты команды **show ipv6 protocols**. Запишите команды, использованные для внесения изменений в конфигурацию. Может потребоваться перезапуск процесса OSPF путем применения команды **clear ipv6 ospf process**.

_____

_____

_____

_____

c. Убедитесь, что изменения конфигурации привели к нужному результату.

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.

Шаг 7: Проверьте информацию о маршрутах OSPFv3.

a. Введите команду **show ipv6 route ospf** и убедитесь, что существуют маршруты OSPFv3 ко всем сетям.

b. Устраните все оставшиеся ошибки маршрутизации.

Шаг 8: Проверьте сквозное подключение IPv6.

С каждого маршрутизатора отправьте эхо-запросы на все интерфейсы IPv6 других маршрутизаторов. Если проблемы сквозного подключения IPv6 сохраняются, продолжите поиск и устранение неисправностей, чтобы устранить их.

Вопросы на закрепление

Почему для устранения всех проблем нельзя просто использовать одну команду **show running- configuration**?

_____
_____
_____
_____

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.				

Лабораторная работа № 18

На тему: Настройка базового PPP с аутентификацией

Топология

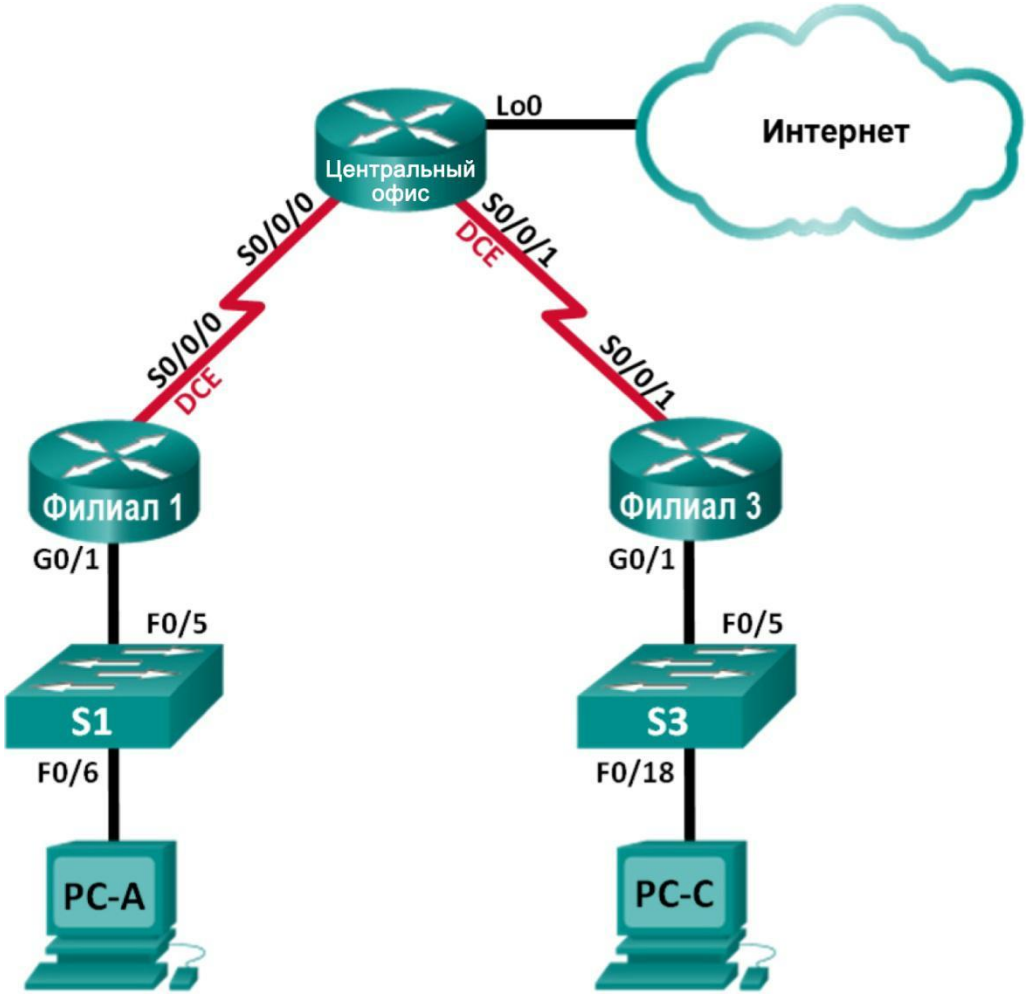


Таблица адресации

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

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:

k. 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

l. 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель)

g. 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например
Tera Term);

h. консольные кабели для настройки устройств Cisco IOS через порты консоли;

i. кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

7. 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.

c. Отключите поиск DNS.

d. Настройте имя устройства.

e. Зашифруйте незашифрованные пароли.

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

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

h. Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

i. Настройте ведение журнала состояния консоли на синхронный режим.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации
включите физические интерфейсы.

e. Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

f. На маршрутизаторе «Главный» создайте **Loopback 0** для имитации доступа в Интернет

назначьте IP-адрес согласно таблице адресации.

Шаг 4: Настройте маршрутизацию.

i. 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.

j. На маршрутизаторе «Главный» настройте маршрут по умолчанию к симулируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите маршрут в процесс OSPF.

k. 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.

h. Для изменения инкапсуляции HDLC на PPP введите команду **encapsulation ppp** на интерфейсе S0/0/0 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
```

g. 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.

_____
_____
_____
_____

h. 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
```

i. Убедитесь, что интерфейс S0/0/0 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.

Выполните команды **debug ppp**, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы «Филиал 1» и «Главный».

```
Branch1# debug ppp negotiation
```

c. 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
```

g. 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]
```

d. 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.

_____

_____

_____

_____

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
```

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?

_____

_____

_____

_____

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
```

C Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Филиал 1» при установке подключения между маршрутизаторами «Филиал 1» 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?

_____

_____

c. Введите команду **undebug all** (или **u all**) на маршрутизаторах «Филиал 1» и «Главный» и отключите всю отладку на обоих маршрутизаторах.

d. После стабилизации сети выполните команду **show ip interface brief** на маршрутизаторах «Филиал 1» и «Главный». Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

_____

_____

e. 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.

_____

_____

_____

_____

f. 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».

e. Настройте имя пользователя для аутентификации CHAP.

```
Central(config)# username Branch3 password cisco
Branch3(config)# username Central password cisco
```

f. 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
```

f. Настройте интерфейс S0/0/1 на маршрутизаторе «Филиал 3» для аутентификации CHAP.

```
Branch3(config)# interface s0/0/1 Branch3(config-if)#
ppp authentication chap
```

g. 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, address
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 [29F4DA8C]
.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 28 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».

_____

_____

_____

_____

h. Введите команду **debug ppp authentication** для наблюдения за сообщениями аутентификации CHAP на маршрутизаторе Central.

```
Central# debug ppp authentication
PPP authentication debugging is on
```

i. Настройте аутентификацию CHAP на интерфейсе S0/0/1 на маршрутизаторе «Главный».

j. 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
.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"
.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4
.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up
.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

h. Введите команду **undebug all** (или **u all**) на маршрутизаторах «Главный» и «Филиал 3» отключите всю отладку.

```
Central# undebug all
All possible debugging has been turned off
```

Шаг 3: Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.

c. На маршрутизаторе «Главный» настройте имя пользователя для использования с «Филиал 1». Назначьте **cisco** в качестве пароля.

Central(config)# **username Branch1 password cisco**

d. 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.

e. Для исследования возникшего процесса используйте команду **debug ppp negotiation**.

Central# **debug ppp negotiation**

```
d.  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.

_____

_____

_____

_____

_____

_____

_____

В Введите команду **undebug all** на всех маршрутизаторах, чтобы отключить отладку.

В 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 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.

Лабораторная работа № 19

На тему: Отладка базового PPP с аутентификацией

Топология

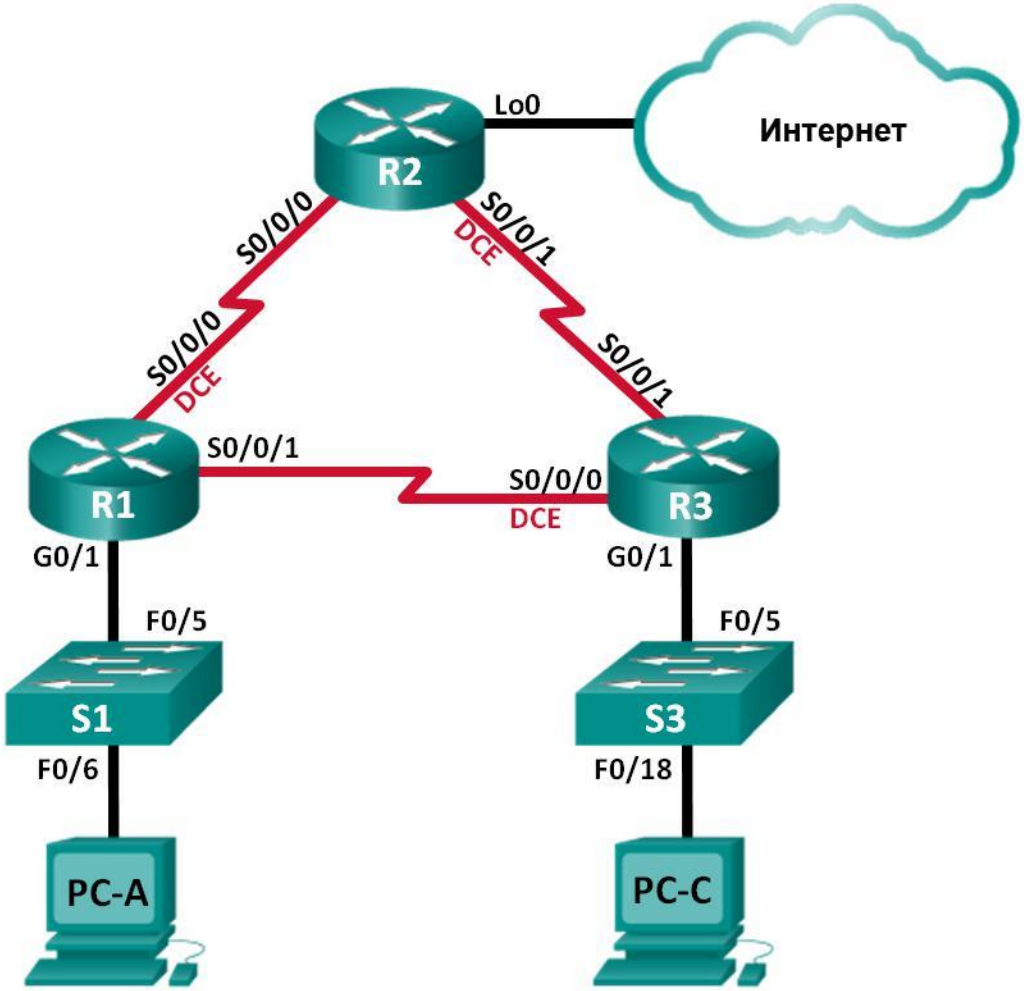


Таблица адресации

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.

v. 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

- 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:

B 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

110 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

111 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например, Tera Term)

112 консольные кабели для настройки устройств Cisco IOS через порты консоли;

113 кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и загрузка настроек устройств

h. 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

i. доступа vty — **cisco**. Все последовательные интерфейсы должны быть настроены с инкапсуляцией PPP и аутентификацией по протоколу CHAP с паролем **chap123**.

Настройка маршрутизатора R1:

```
hostname R1
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
```

```
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
 encapsulation ppp
•     authentication chap
interface s0/0/1
 ip address 192.168.31.1 255.255.255.252
 encapsulation ppp
 ppp authentication pap
exit
router ospf 1
 router-id 1.1.1.1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 0.0.0.3 area 0
 passive-interface g0/1
 exit

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
t.     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
```

Настройка маршрутизатора R3:

```
hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123 username R3 password
chap123
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
k.          authentication chap
no shutdown
interface s0/0/1
 ip address 192.168.23.2 255.255.255.252
 encapsulation ppp
B           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**.

l. 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?

_____
_____
_____
_____
_____
_____
_____

Эхо-запрос от узла ПК A к Lo0 выполняется успешно?

_____
_____
_____
_____

_____
_____
_____

q.

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

e. 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)	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.

Лабораторная работа № 20

На тему: Проверка PPP

PPP это Internet'овскиий стандарт по передаче IP пакетов по последовательным линиям. PPP поддерживает синхронными и асинхронными линиями. По некоторым моментам дискуссии о PPP, а также PPP против SLIP советую посмотреть документ на ftp.uu.net:vendor/MorningStar/papers/sug91-cheapIP.ps.Z (paper) и sug91-cheapIP.shar.Z (overhead projector slides)

2.2 PPP features which may or may not be present

По ту и по эту сторону совместимости с базовым PPP фрамингом надо знать, что многие программы добавляют свои дополнительные возможности. Желательно запомнить, что не все свободно распространяемые программы, а также коммерческие программы имеют в себе полный набор всех возможностей.

Demand dial (дозвон по запросу)	Подключение PPP интерфейса и набор тел. номера по приходу пакета. отключение интерфейса PPP после некоторого периода отсутствия активности.
Redial	Подключение PPP интерфейса, который потом не будет отключен и будет всегда сохранять в своем распоряжении подключенный канал.
Campling	(см. Redial)
Scripting	Установка через серию сообщений или промежуточных соединений для установления PPP соединения, больше похоже на последовательности используемые для установления связи по UUCP.
Parallel	Конфигурирование нескольких PPP линий для одного и того-же подключения к хосту, для равномерного разделения трафика между ними. (В процессе стандартизации)
Filtering	Выборка, при каких пакетах имеет смысл начинать прозвон по линии, а при каких нет. Отталкиваясь в принятии решения от IP или TCP типа пакета или TOS (Type of Service). К примеру, игнорировать все ICMP пакеты.
Header Compression (сжатие заговка)	Сжатие TCP заголовка в соответствии с RFC1144 Не обязательно при использовании на высокоскоростных линиях, но оченьполезен на низкоскоростных.
Server	Принятие входящих PPP соединений, которые могут также требовать дополнительной маршрутизации.
Tunneling	Построение виртуальных сетей по PPP соединению, через TCP поток, через существующую IP сеть. (Build a virtual network over a PPP link across a TCP stream through an existing IP network.)
Extra escaping	Байт ориентированные символы, не входящие в стандартный набор символов, используемый при установлении связи, они могут быть сконфигурированы отдельно, но также не пересекаться с теми, что используются при установлении связи. (Byte-stuffing characters outside the negotiated asyncmap, configurable in advance but not negotiable.)

2.3 PPP glossary

Каждая технология со временем обрастает акронимами... PPP не исключение. т.к почти все термины употребляются в своей английской/американской транскрипции, то мне кажется, что перевод этих сокращений не имеет смысла.

ack	Acknowlegement
AO	Active Open [state diagram] (недавно стала частью FSM в RFC1331)
C	Close [state diagram]
CHAP	Challenge-Handshake Authentication Protocol (RFC1334)
D	Lower layer down [state diagram]
DES	Data Enryption Protocol
DNA	Digital Network Architecture
IETF	Internet Engineering Task Force.
IP	Internet Protocol
IPCP	IP Control Protocol.
IPX	Internetwork Packet Exchange (Novell's networking stack)
FCS	Frame Check Sequence [X.25]
FSA	Finite State Automation
FSM	Finite State Maschine
LCP	Link Control Protocol.
LQR	Link Quality Report.
MD4	MD4 digital signature algorithm
MD5	MD5 digital signature algorithm
MRU	Maximum Receive Unit
MTU	Maximum Transmission Unit
nak	Negative Acknowledgement
NCP	Network Control Protocol.
NRZ	Non-Return to Zero bit encoding. (SYNC ppp default because of availability)
NRZI	Non-Return to Zero Inverted bit encoding. (SYNC ppp preferred alternative to NRZ)
OSI	Open Systems Interconnect
PAP	Password Authentication Protocol (RFC1334)
PDU	Protocol Data Unit (тоже что packet)
PO	Passive open [no longer part of state diagram]

PPP	Point to Point Protocol (RFC1548 /RFC1549,1332,1333,1334,1551,1376,1377,1378)
RCA	Receive Configure-Ack [state diagram]
RCJ	Receive Code-Reject [state diagram]
RCN	Receive Configure-Nak or -Reject [state diagram]
RCR+	Receive good Configure-Request [state diagram]
RER	Receive Echo-Request [no longer part of state diagram]
RFC	Request for Comments (internet standard)
RTA	Receive Terminate-Ack [state diagram]
RTR	Receive Terminate-Request [state diagram]
RUC	Receive unknown code [state diagram]
sca	Send Configure-Ack [state diagram]
scj	Send Code-Reject [state diagram]
scn	Send Configure-Nak or -Reject [state diagram]
scr	Send Configure-Request [state diagram]
ser	Send Echo-Reply [no longer part of state diagram]
sta	Send Terminate-Ack [state diagram]
str	Send Terminate-Request [state diagram]
ST-II	Stream Protocol
TO+	Timeout with counter > 0 [state diagram]
TO-	Timeout with counter expired [state diagram]
VJ	Van Jacobson (RFC1144 header compression algorithm)
XNS	Xerox Network Services

Общая информация

Point-to-Point Protocol (PPP) разработан для разрешения проблем связанных с недостаточным количеством стандартных средств инкапсуляции протоколов вида "point-to-point IP". Ко всему прочему PPP был также разработан для упрощения выдачи и управления IP адресами, асинхронной и bit-oriented синхронной инкапсуляцией, смешивания сетевых протоколов(network protocol multiplexing), конфигурирования и тестирования качества связи, обнаружения ошибок и опциями для установления таких особеностей сетевого уровня как настройка адресов и установка сжатия данных. Для поддержки выше перечисленных качеств, PPP должен

предоставлять управление по расширенному Link Control Protocol (LCP) и семейству протоколов Network Control Protocols (NCPs) которые используются для установления параметров связи. На сегодняшний день PPP поддерживает не только IP, но и другие протоколы, включая IPX и DECNet.

PPP Components

PPP предоставляет возможность передачи датаграмм по последовательным point-to-point линиям. Он имеет 3 компоненты:

- Метод предоставления инкапсуляции датаграмм по последовательным PPP линиям используя HDLC (High-Level Data Link Control) протокол для упаковки датаграмм по PPP средствам связи.
- Расширенный LCP(Link Control Protocol) для установления, конфигурирования и тестирования физического соединения (test the data-link connection)
- Семейство протоколов (NCPs) для установления и управления иными сетевыми протоколами, иными словами: PPP разработан для поддержки одновременно нескольких сетевых протоколов.

General Operation

В момент установления связи через PPP соединение, PPP драйвер вначале шлет пакеты LCP для конфигурирования и (возможно) тестирования линии связи. После того как связь и дополнительные возможности будут установлены как надо посредством LCP, PPP драйвер посылает NCP фреймы для изменения и/или настройки одного или более сетевых протоколов. Когда этот процесс закончиться, то сетевые пакеты получают возможность быть переданными через установленное соединение. Оно будет оставаться настроенным и активным до тех пор, пока определенные LCP или NCP пакеты не закроют соединение, или до тех пор пока не произойдет какое-нибудь внешнее событие, которое приведет к потере соединения (к примеру: таймер отсутствия активности или вмешательство пользователя)

Physical-Layer Requirements

PPP адаптирован для работы с любым DTE/DCE интерфейсом, включая EIA/TIA-232-C (RS-232), EIA/TIA-422-C(RS-422), EIA/TIA-423-C(RS-423), ITU-T (CCITT) V.35. Единственное требование к оборудованию, налагаемое PPP - это

наличие дуплексного оборудования, не важно выделенное оно или переключаемое (either dedicated or switched), которое может работать на асинхронных или bit-oriented синхронных, прозрачных для PPP пакетах.

PPP Link Layer

PPP использует принципы, терминологию и структуру пакетов в описанных ISO документах касающихся HDLC (ISO 3309-1979) и его дополненной версии:

- ISO 3309:1984/PDAD1 "Addendum 1: Start/stop transmission."
- ISO 3309-1979: описывает структуру пакетов HDLC для использования в синхронных системах.
- ISO 3309:1984/PDAD1: описывает предложения по изменениям в ISO 3309-1979, которые позаоляют использовать асинхронные системы.

Процедуры управления PPP используют определения и управляющие поля стандартизированные в документах: ISO 4335-1979 и ISO 4335-1979/Addendum 1-1979.

Формат пакета PPP:

1	**1**	**1**	**2**	**Variable**	**2 или 4**
Flag	Address	Control	Protocol	DATA	FCS

Flag:	Один байт обозначающий начало или конец пакета Поле флага содержит двоичную последовательность: 01111110.
Address:	Один байт содержащий двоичную последовательность: 11111111, Стандартный широковещательный адрес. PPP не поддерживает индивидуальную адресацию станций.
Control:	Один байт содержащий двоичную последовательность: 00000011, который посылается для передачи пользовательских данных в неразделенных пакетах. (for transmission of user data in an unsequenced frame.
Protocol:	2 байта кодируют протокол упакованный во врейм протокола PPP. Значения протоколов можно узнать документе Assigned Numbers Request for Comments (RFC).
Data:	0 или больше байт составляющих датаграмму протокола указанного в поле "Protocol". Конец информационного поля определяется нахождением заканчивающей последовательности и 2байтной последовательности в поле FCS. По умолчанию максимальная длина инфрмационоого поля 1500байт.Однако, по взаимной "договоренности", учитывая использование PPP могут использоваться иные значения длины поля
Frame Check Sequence (FCS):	Обычно 16bit (2байта). Однако, по взаимной "договоренности" может использоваться и 32bit (4байта) котроль целостности пакетов.

PPP Link Control Protocol

PPP LCP предоставляет методы для для установления, конфигурирования, поддержания и тестирования point-to-point соединения. LCP распадается на 4 фазы:

- Конфигурирование и установление связи - Перед передачей какой-либо датаграммы (к примеру IP) LCP должен в начале открыть соединение и произвести начальный обмен параметрами настройки. Этот этап заканчивается, когда пакет о подтверждении произведенной настройки будет послан и принят обратно.
- Определение качества связи - LCP позволяет (но не требует) добавить фазу тестирования канала связи, эта фаза будет следовать сразу-же за первой. В течении этой фазы опрределяется способно-ли соединение с достаточным качеством транспортировать какой-либо сетевой протокол. Эта фаза не является обязательной. LCP должен затянуть передачу какого-либо сетевого протокола до тех пор пока эта фаза не будет выполнена.
- Установление настроек сетевого протокола - После того как LCP закончит определение параметров связи, сетевые протоколы должны быть независимо друг от друга настроены соответствующими NCP, которыми могут в любой момент времени начать или прекратить пользоваться.
- Окончание связи - LCP может в любое время прервать установленную связь. Это может произойти по требованию пользователя или из-за какого-нибудь физического события, к примеру потери несущей или истечению допустимого периода времени неиспользования канала.

Существует три типа LCP пекетов:

- Пакеты установления- Используются для установления и настройки связи
- Пакеты прерывания - Используются для прерывания установленной связи
- Пакеты сохранения связи - Используются для управления и диагностики связи

Что умеет PPP в сравнении с HDLC?

1. Управление качеством линии (PPP отключает линк, если количество ошибок превысит заданное значение).
2. Аутентификация с помощью PAP или CHAP.

3. Multilink – технология напоминающая Etherchannel в Ethernet-е: несколько разных линков объединяются в один логический, со скоростью, равной сумме входящих в него линков.

4. PPP Callback – технология, использующаяся для повышения безопасности: клиент устанавливает соединение с сервером, сервер разрывает соединение и устанавливает со своей стороны новое – к клиенту.

На самом деле, при передачи данных с маршрутизатора на маршрутизатор, PPP инкапсулируется в HDLC, который выполняет «транспортные» функции для PPP фреймов. Подробнее про HDLC можно почитать в статье «Протокол HDLC – пример настройки и описание». PPP – обладает уровневой структурой, когда фрейм PPP приходит из сети он поднимается по внутренним подуровням PPP снизу вверх:

1. Первый подуровень HDLC – получает фрейм, проверяет адрес получателя, контрольную сумму и передаёт полезнуюинформацию дальше.

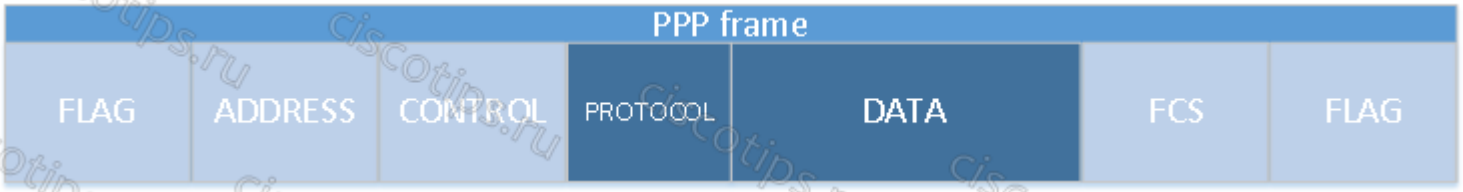
2. Подуровень LCP (Link Control Protocol), как видно из названия, занимается управлением соединением, отправляет и получает разные служебные флаги, следит за состоянием соединения (подключено/выключено), следит за качеством линии, следит за согласованностью параметров конфигурации между точками.

3. Подуровень NCP (Network Control Protocol) состоит из большого количества модулей, каждый из которых занимается связью с каким-то конкретным протоколом третьего уровня (IPv4, IPv6, IPX, AppleTalk, …). Благодаря этому, в рамках одного установленного PPP соединения с одним логином и паролем, можно передавать траффик разных протоколов сетевого уровня.

Установка связи между двумя маршрутизаторами по протоколу PPP происходит по уровням снизу вверх, разрыв связи – сверху вниз.

То есть устанавливается связь в таком порядке: LCP,NCP, полезные данные третьего уровня. А разрывается: конец передачи полезных данных, NCP, LCP. Как видно, HDLC не устанавливает и не разрывает соединения, так как в PPP используются HDLC фреймы без подтверждения доставки.

Структура PPP фрейма имеет следующий вид:



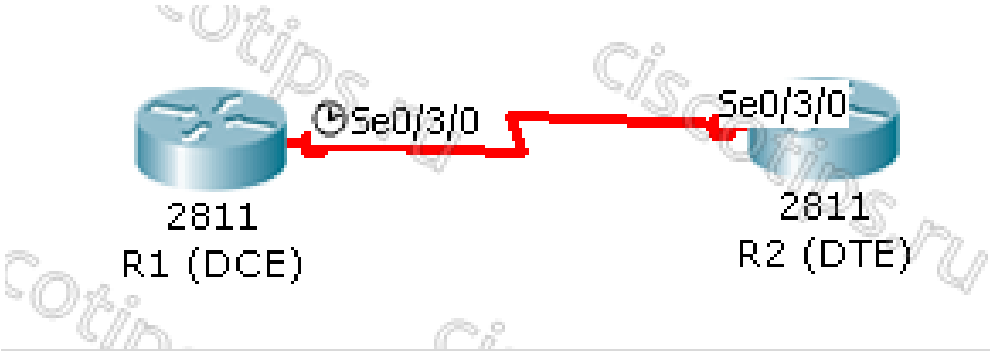
1. FLAG – признак начала фрейма, специальная последовательность нулей и единиц («01111110»), которая говорит получателю, что далее будет следовать тело фрэйма.
2. ADDRESS – адрес получателя, в протоколе PPP всегда используется широковещательный «11111111».
3. CONTROL – поле содержит значение «00000011»
4. PROTOCOL – поле, содержащее номер протокола третьего уровня, пакет которого «завёрнут» в данный фрейм.
5. DATA – поле с полезными данными вышестоящих протоколов.
6. FCS – контрольная сумма, которая считается при отправке фрейма и сравнивается с полученным пересчётом, который делается при получении фрейма. В результате, если суммы не совпадают, кадр считается «битым» и отбрасывается.
7. FLAG – признак окончания фрейма, содержит то же значение что и признак начала фрейма.

Настройка PPP на оборудовании cisco, как уже было сказано, в курсе CCNA не сложная. Выполняется она на интерфесе:

1. Выбираем алгоритм сжатия командой compress
2. Устанавливаем качество линии, которое будет считаться приемлемым (при количестве ошибок, больше заданного связь будет разрываться). Для этого служит команда **ppp quality**.
3. Выбираем способ аутентификации PAP или CHAP (подробнее об этом можно узнать из статьи «В чём разница между PAP и CHAP». Способ аутентификации задаётся командной **ppp authentication**.
4. Необходимо настроить пользователя под которым наш маршрутизатор будет подключаться к другому. Здесь команды разнятся для CHAP и PAP. Сам пользователь добавляется командой **username** <имя> **password** <пароль>, причём делать это надо не на интерфейсе, а в режиме глобальной конфигурации, но в случае

использования PAP, надо ещё использовать на интерфейсе команду **ppp pap sent-username** <имя> **password** <пароль>.

Использование PAP в реальных конфигурациях не желательно, поэтому мы ограничимся примером настройки CHAP. Итак, предположим, что топология следующая, необходимо настроить PPP с аутентификацией CHAP. Настройка на первом маршрутизаторе:




```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#username R2 password 123456789
R1(config)#interface serial 0/3/0
R1(config-if)#en
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down
```

Настройка на втором маршрутизаторе:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#username R1 password 123456789
R2(config)#interface serial0/3/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#ip address 192.168.0.2 255.255.255.0
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up
```

Обратите внимание, что пользователь, которого мы заводим на маршрутизаторе R1 имеет имя R2, а на R2 – R1. Это необходимо, так как когда один роутер подключается к другому, он указывает своё имя, соответственно, другой должен знать это имя (видеть его в своём списке локальных пользователей). Ещё одна немаловажная деталь: пароли к пользователям R1 и R2 обязательно должны совпадать.

Для проверки можем выполнить команду:

```
R2#sh ip inter brief
Interface              IP-Address      OK? Method Status                Protocol
 …
Serial0/3/0            192.168.0.2     YES manual up                    up
 …
```

Если status будет «up», а протокол – «down», то это, как правило означает, что какие-то проблемы с PPP – не та аутентификация, не совпали пароли, качество линии ниже того, что мы заказывали и т.п.

Лабораторная работа № 21

На тему: Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL

Топология

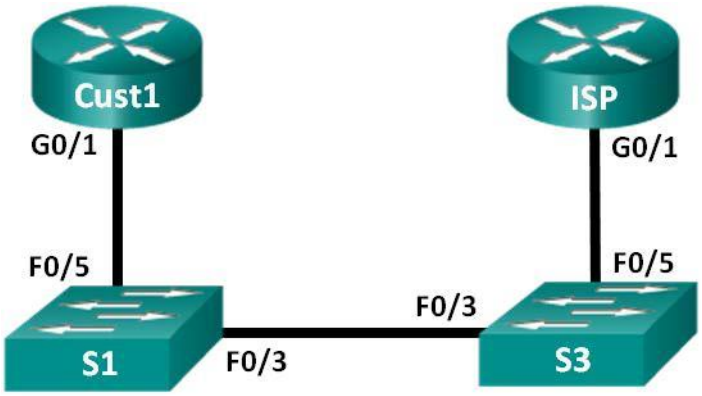


Таблица адресации

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

- 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:

j. 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

k. 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

l. консольные кабели для настройки устройств Cisco IOS через порты консоли;

m. 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.

В Отключите поиск DNS.

В Настройте имя устройств в соответствии с топологией.

В Зашифруйте незашифрованные пароли.

В Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

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

В Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

В Настройте ведение журнала состояния консоли на синхронный режим.

В Сохраните настройку.

Часть 2: Настройка маршрутизатора интернет-провайдера ISP

w. 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.

- Создайте в локальной базе учётных записей имя пользователя **Cust1** с паролем **ciscopppoe**.

```
ISP(config)# username Cust1 password ciscopppoe
```

- Создайте пул адресов, которые будут назначены пользователям.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

- 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
```

6. Назначьте шаблон группе PPPoE.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

7. 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 Cust1

В части 3 необходимо настроить маршрутизатор Cust1 с использованием параметров PPPoE.

114 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
```

115 Свяжите интерфейс G0/1 с интерфейсом номеронабирателя Dialer. Используйте имя пользователя **Cust1** 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
```

116 Настройте статический маршрут по умолчанию через интерфейс номеронабирателя.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

117 Настройте отладку на маршрутизаторе Cust1 для отображения согласования PPP и PPPoE.

```
Cust1# debug ppp authentication
Cust1# debug pppoe events
```

118 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
```

j. 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?

```
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
```

- Введите команду **show ip route** на маршрутизаторе Cust1. Выходные данные приведены ниже.

```
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
u.       - 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
C10.0.0.1 is directly connected, Dialer1
C10.0.0.254 is directly connected, Dialer1
```

c. Введите команду **show pppoe session** на маршрутизаторе Cust1. Выходные данные приведены ниже.

```
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
```

l. 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.

o. 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.

Лабораторная работа № 22

На тему: Настройка туннеля VPN GRE по схеме «точка-точка»

Топология

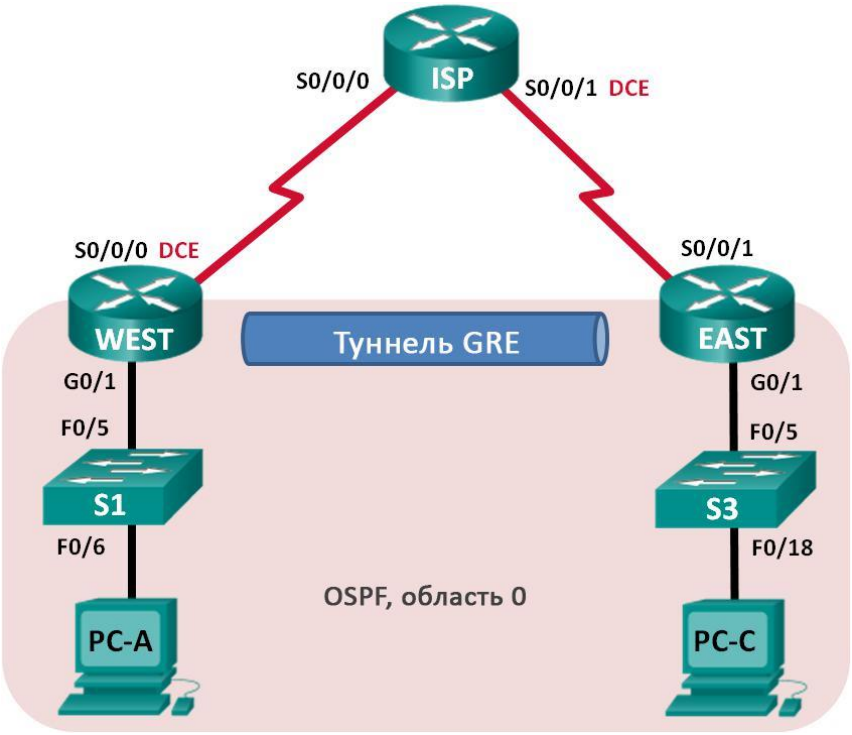


Таблица адресации

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

8. 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:

119 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

120 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

121 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например

Tera Term);

122 консольные кабели для настройки устройств Cisco IOS через порты консоли;

123 кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

k. 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.

- Отключите поиск DNS.
- Назначьте имена устройств.
- Зашифруйте незашифрованные пароли.
- Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.
- Настройте ведение журнала состояния консоли на синхронный режим.
- 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.
- 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.

В Настройте 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
```

d. 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.

m. 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
```

В 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?

_____

_____

_____

_____

_____

_____

В 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
```

p. С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

_____

_____

m. 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?

_____

_____

n. 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

r. 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.

e. Настройте 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
```

f. 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.

f. Отправьте 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
B        - 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
e.             10.1.1.0/30 is directly connected, Serial0/0/0
      L10.1.1.1/32 is directly connected, Serial0/0/0 172.16.0.0/16 is
            variably subnetted, 5 subnets, 3 masks
      C172.16.1.0/24 is directly connected, GigabitEthernet0/1
      L172.16.1.1/32 is directly connected, GigabitEthernet0/1
      O172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
      C172.16.12.0/30 is directly connected, Tunnel0
      L172.16.12.1/32 is directly connected, Tunnel0
```

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

_____

_____

j. Отправьте 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.

m. 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.

n. 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.

Лабораторная работа № 23

На тему: Разработка технического обслуживания сети

Техническое обслуживание (**ТО**) – комплекс операций по поддержанию работоспособности или исправности объектов технической эксплуатации первичных сетей при его использовании по назначению в течении срока службы.

ТО первичных сетей может осуществляться с использованием следующих методов:

1) **профилактическое ТО (ПТО)**, выполняемое через определенные временные интервалы и направленное на временное предупреждение возможности появления отказа или ухудшения функционирования ОТЭ.

ПТО включает:

- периодический эксплуатационный контроль,
- плановые измерения эксплуатационных характеристик и ремонтно-настроечные работы (РНР),
- плановую замену компонентов аппаратуры,
- текущее обслуживание оборудования и аппаратуры.

2) **корректирующее ТО (КТО)**, выполняемое после обнаружения состояния неработоспособности ОТЭ и направленное на его восстановление в состояние, когда параметры качества ОТЭ находятся в пределах установленных допусков.

КТО включает:

- непрерывный эксплуатационный контроль,
- эпизодический эксплуатационный контроль,
- оперативно-технический контроль,
- ремонтно-восстановительные и ремонтно-настроечные работы (РВР и РНР),
- измерение эксплуатационных характеристик.

3) **управляемое ТО (УТО)**, выполняемое путем систематического применения методов анализа состояния ОТЭ с использованием средств контроля рабочих характеристик ОТЭ, средств управления качеством передачи и устранением неисправностей, и направленное на сведение к минимуму ПТО и сокращение КТО.

УТО включает:

- непрерывный эксплуатационный контроль,
- оперативно-технический контроль,
- операции управления и переключения на резерв.

Для современных средств электросвязи основным является применение УТО.

Система оперативно-технического управления первичными сетями СОТУ:

1 Общие принципы организации СОТУ распространяются в одинаковой степени, как на магистральную, так и на внутризоновую и местную первичные сети.

СОТУ первичными сетями должна быть централизованной, интегрированной и состоящей из комплекса взаимоувязанных систем управления. Управление и общая координация функционирования в повседневных условиях, должны обеспечиваться центральными органами управления с вертикально-интегрированным принципом построения, который отражает территориально-иерархическую структуру и включает три уровня управления: местный, зоновый и национальный.

2 СОТУ обеспечивает оперативно-техническое управление как первичными, так и вторичными сетями электросвязи и в том числе каналами междугородного телевизионного, звукового вещания и фотогазетными трактами на территории Республики Беларусь.

СОТУ построена по территориально-иерархическому принципу и осуществляет управление через структурные подразделения организации (филиала) связи.

Каждое подразделение СОТУ выполняет свои функции под руководством вышестоящего подразделения, а также самостоятельно – в пределах задач и прав, определяемых его уровнем. Подразделения СОТУ имеют соответствующий административный статус (соответствующие административные права) для реализации вырабатываемых управляющих воздействий.

3 Организационно СОТУ представляет собой территориально разнесенную многоуровневую иерархическую структуру и включает в себя комплекс технических средств, а также технический персонал, обеспечивающий выполнение задач оперативно-технического управления.

В СОТУ входят подсистемы управления:

– первичной сетью (с разделением по методу управления: имеющие возможность дистанционного управления и не имеющие такой возможности):

– сетью ТСС;

– вторичными сетями электросвязи.

Каждая из этих подсистем управления имеет соответствующее количество уровней иерархии (магистральный, внутризоновый и местный), соответствующее количество и размещение центров управления в зависимости от назначения, размеров и разветвленности управляемых сетей.

На верхнем иерархическом уровне СОТУ функционирует НЦУ. Функции НЦУ возложены на Национальный центр управления национального оператора электросвязи в обязанности которого входит:

– ежегодный сбор и обобщение информации о состоянии сетей и средств электросвязи;

– контроль за ходом аварийно-восстановительных и других неотложных работ на сетях электросвязи по восстановлению связи и ликвидации аварийных ситуаций;

– круглосуточный оперативный контроль и мониторинг состояния первичной и вторичных сетей электросвязи, сети ТСС;

– организацию связи для обеспечения нужд государственного управления, национальной безопасности, обороны, охраны правопорядка. Предупреждения и ликвидации чрезвычайных ситуаций;

– приостановку или ограничение использования сети электросвязи общего пользования;

– управление маршрутизацией на сетях электросвязи и пропуск необходимого трафика в интересах приоритетных пользователей;

– использование сетей и средств электросвязи взаимодействующих сетей электросвязи по взаимосогласованным планам.

4 В рамках СОТУ оперативно-техническое управление СМП осуществляется с помощью подсистемы управления первичной сетью, включающей следующие уровни управления:

– Национальный уровень управления;

– узловой пункт управления (далее – УПУ);

– информационно-исполнительный пункт (далее – ИП).

Оперативно-техническое управление первичной сетью осуществляют структурные подразделения организаций (филиалов) связи.

4.1 На национальном уровне оперативно-технического управления первичной сетью действуют:

– Национальный центр управления НЦУ;

– Оперативно-диспетчерская служба Республики (далее – ОДС-Р), которая оперативно подчиняется НЦУ;

– Оперативный пункт управления первичной сетью (далее – ОПУ-ПС), который оперативно подчиняется НЦУ.

4.2 УПУ осуществляет оперативно-техническое управление СМП на закрепленной территории и оперативно подчиняется ОПУ-ПС. Функции УПУ выполняют подразделения оперативного управления.

4.3 ИП осуществляет функции по оперативно-техническому управлению участком СМП в организациях (филиалах) связи, в которых он организован, и оперативно подчиняется УПУ. Функции ИП выполняют цеха, административно подчиненные оператору электросвязи.

5 В рамках СОТУ подразделения организаций (филиалов) связи должны участвовать в едином технологическом процессе управления СМП.

6 Обмен информацией и подача команд между подразделениями СОТУ должны осуществляться в соответствии с установленными алгоритмами оперативно-технического управления сетями электросвязи.

7 Формирование обобщенных сигналов состояния КО и критерии оценки состояния КО определяются типом систем передачи, используемых на первичных сетях.

8 Информация о состоянии КО в СОТУ первичными сетями может передаваться формализовано, в виде кодограмм. Перечень кодовых обозначений, правила обработки, передачи и оформления кодовой информации определяются документами, регламентирующими технологический процесс (алгоритмы) оперативно-технического управления первичными сетями.

Взаимодействие и обмен оперативной информацией между подразделениями СОТУ должны осуществляться с использованием каналов ССУ, а также путем использования служебной телеграфной сети и служебной сети передачи данных.

9 СОТУ СМП и СОТУ ВзПС при выполнении плановых задач должны обеспечивать:

– формирование первичных сетей, включая разработку планов формирования сетей электросвязи, распоряжений го формированию сетей электросвязи, доведение их до заинтересованных подразделений СОТУ, вторичных сетей электросвязи и других пользователей, контроль за их выполнением;

– разработку предложений и план-графиков го организации и проведению реконструкций сетей электросвязи, доведение этой информации до заинтересованных подразделений СОТУ, вторичных сетей электросвязи и других пользователей услуг электросвязи, контроль за проведением реконструкций:

– разработку и коррекцию графиков обходов и замен в интересах пользователей и вторичных сетей электросвязи, доведение их до заинтересованных подразделений СОТУ, вторичных сетей электросвязи и других пользователей;

– составление технологических карт на введение графиков обходов и замен;

– разработку и коррекцию планов РНР и измерений, оформление заявок на проведение РНР. выдача разрешений на их проведение, оповещение заинтересованных подразделений СОТУ. вторичных сетей электросвязи и других пользователей;

– контроль за проведением РНР и РВР;

– разработку алгоритмов по оперативно-техническому управлению первичными сетями и ведение эксплуатационно-технической документации;

– ведение базы данных го оперативно-техническому управлению первичными сетями.

10 СОТУ СМП и СОТУ ВзПС при выполнении оперативных задач должны обеспечивать:

– определение состояния КО;

– сбор и анализ сообщений об изменении состояния КО;

– определение неисправного участка КО СОТУ;

– принятие решений и выдача команд подразделениям СТЭ на проведение РВР для устранения неисправностей;

– контроль за ходом работ по ликвидации неисправностей;

– управление перестройками на первичных сетях по заранее разработанным графикам обходов и замен, контроль за вводом и снятием обходов и замен;

– проведение тренировок по заранее разработанным перечням связей с целью подготовки функционирования сетей в нетиповых ситуациях;

– составление в оперативной обстановке обходных трасс для трактов и каналов передачи при невозможности резервирования по заранее разработанным графикам обходов и замен, выдача команд на их организацию и контроль за их выполнением;

– оповещение заинтересованных подразделений СТЭ, вторичных сетей электросвязи и других пользователей при изменении состояния КО;

– контроль за проведением контрольных измерений и РНР и их результатами;

– оформление оперативных и аварийных работ, а также оповещение о запрете РНР.

11 СОТУ при выполнении задач по управлению качеством должна обеспечивать:

– составление суточных сводок о работе КО первичных сетей;

– сбор данных о повреждаемости КО первичных сетей;

– составление статистических отчетов о работе КО первичных сетей;

– анализ качества и эффективности работы подразделений СОТУ первичных сетей;

– разработку предложений по повышению качества и надежности работы первичных сетей и работы СОТУ.

Задачние:

Изучить теорию предоставить отчет в виде презентации и ответить на контрольные вопросы.

Лабораторная работа № 24

На тему: Настройка Syslog и NTP

Топология

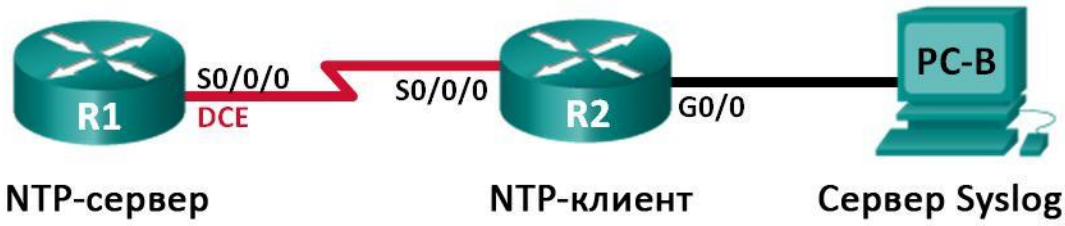


Таблица адресации

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

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

- 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,

В 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

9. 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,

l. они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

m. 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

n. 1 компьютер (с ОС Windows 7, Vista или XP или с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32);

o. консольные кабели для настройки устройств Cisco IOS через порты консоли;

p. кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

• 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

e. 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.

n. 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	

c 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
```

n. 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.

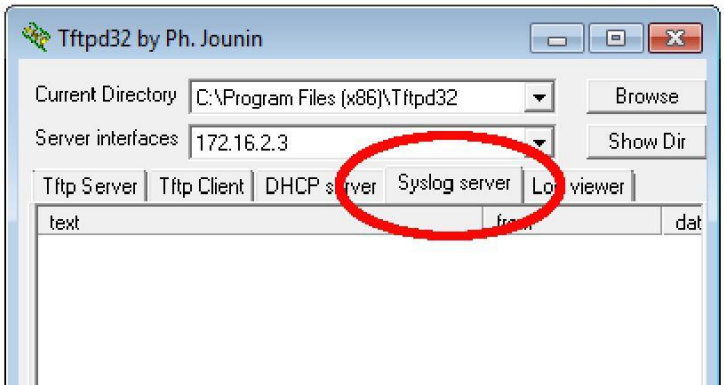
Шаг 1: (Дополнительно) Установите сервер Syslog.

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.

s. 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.

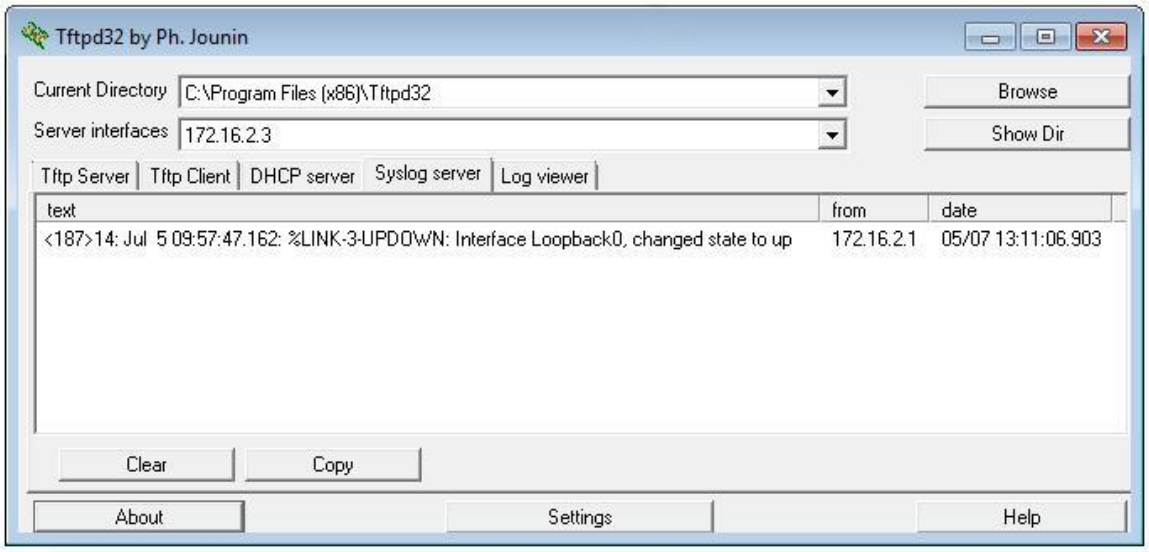
```
R2(config)# logging trap warnings
```

или

```
R2(config)# logging trap 4
```

c. Создайте интерфейс Loopback0 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 up
Jul 5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
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.

```
R2(config)# logging trap informational
```

или

```
R2(config)# logging trap 6
```

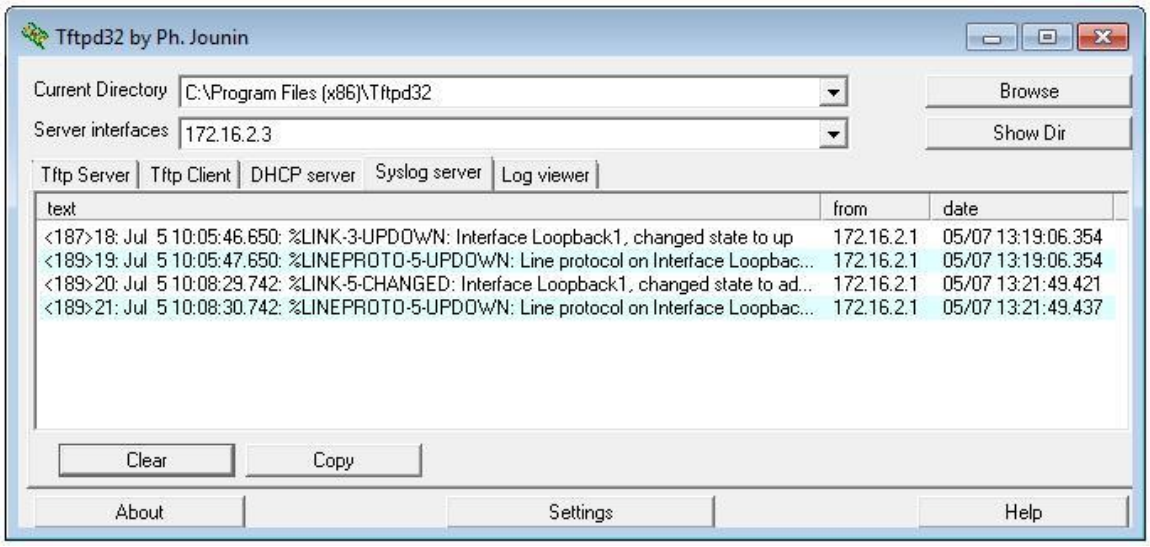
f. Удалите записи Syslog на ПК B. Нажмите кнопку **Clear** (Очистить) в диалоговом окне Tftpd32.

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.

d. 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.

Лабораторная работа № 25

На тему: Изучение программного обеспечения для мониторинга сети

Теоретическая часть. Разработка технического задания

Техническое задание представляет собой документ, в котором сформулированы основные цели разработки, требования к программному продукту, определены сроки и этапы разработки и регламентирован процесс приемо-сдаточных испытаний. В разработке технического задания участвуют как представители заказчика, так и представители исполнителя. В основе этого документа лежат исходные требования заказчика, анализ передовых достижений техники, результаты выполнения научно-исследовательских работ, предпроектных исследований, научного прогнозирования и т. п.

Порядок разработки технического задания

Разработка технического задания выполняется в следующей последовательности. Прежде всего, устанавливают набор выполняемых функций, а также перечень и характеристики исходных данных. Затем определяют перечень результатов, их характеристики и способы представления.

Далее уточняют среду функционирования программного обеспечения: конкретную комплектацию и параметры технических средств, версию используемой операционной системы и, возможно, версии и параметры другого установленного программного обеспечения, с которым предстоит взаимодействовать будущему программному продукту.

В случаях, когда разрабатываемое программное обеспечение собирает и хранит некоторую информацию или включается в управление каким-либо техническим процессом, необходимо также четко регламентировать действия программы в случае сбоев оборудования и энергоснабжения.

1. Общие положения

1.1. Техническое задание оформляют в соответствии с ГОСТ 19.106—78 на листах формата А4 и А3 по ГОСТ 2.301—68, как правило, без заполнения полей листа. Номера листов (страниц) проставляют в верхней части листа над текстом.

1.2. Лист утверждения и титульный лист оформляют в соответствии с ГОСТ 19.104—78. Информационную часть (аннотацию и содержание), лист регистрации изменений допускается в документ не включать.

1.3. Для внесения изменений и дополнений в техническое задние на последующих стадиях разработки программы или программного изделия выпускают дополнение к нему. Согласование и утверждение дополнения к техническому заданию проводят в том же порядке, который установлен для технического задания.

1.4. Техническое задание должно содержать следующие разделы:

•введение;

•наименование и область применения;

•основание для разработки;

•назначение разработки;

•технические требования к программе или программному изделию;
•технико-экономические показатели;
•стадии и этапы разработки;
•порядок контроля и приемки;
•приложения.

В зависимости от особенностей программы или программного изделия допускается уточнять содержание разделов, вводить новые разделы или объединять отдельные из них. При необходимости допускается в техническое задание включать приложения.

2. Содержание разделов

2.1.Введение должно включать краткую характеристику области применения программы или программного продукта, а также объекта (например, системы), в котором предполагается их использовать. Основное назначение введения — продемонстрировать актуальность данной разработки и показать, какое место эта разработка занимает в ряду подобных.

2.2.В разделе «Наименование и область применения» указывают наименование, краткую характеристику области применения программы или программного изделия и объекта, в котором используют программу или программное изделие.

2.3.В разделе «Основание для разработки» должны быть указаны:

• документ (документы), на основании которых ведется разработка. Таким документом может служить план, приказ, договор и т. п.;

• организация, утвердившая этот документ, и дата его утверждения;

• наименование и (или) условное обозначение темы разработки.

2.4. В разделе «Назначение разработки» должно быть указано функциональное и эксплуатационное назначение программы или программного изделия.

2.5. Раздел «Технические требования к программе или программному изделию» должен содержать следующие подразделы:

•требования к функциональным характеристикам;
•требования к надежности;
•условия эксплуатации;
•требования к составу и параметрам технических средств;
•требования к информационной и программной совместимости;
•требования к маркировке и упаковке;
•требования к транспортированию и хранению;
•специальные требования.

2.5.1.В подразделе «Требования к функциональным характеристикам» должны быть указаны требования к составу выполняемых функций, организации входных и выходных данных, временным характеристикам и т. п.

2.5.2.В подразделе «Требования к надежности» должны быть указаны требования к обеспечению надежного функционирования (обеспечение устойчивого функционирования, контроль входной и выходной информации, время восстановления после отказа и т. п.).

2.5.3.В подразделе «Условия эксплуатации» должны быть указаны условия эксплуатации (температура окружающего воздуха, относительная влажность и т. п. для выбранных типов носителей данных), при которых должны обеспечиваться заданные характеристики, а также вид обслуживания, необходимое количество и квалификация персонала.

2.5.4.В подразделе «Требования к составу и параметрам технических средств» указывают необходимый состав технических средств с указанием их технических характеристик.

2.5.5.В подразделе «Требования к информационной и программной совместимости должны быть указаны требования к информационным структурам на входе и выходе и методам решения, исходным кодам, языкам программирования. При необходимости должна обеспечиваться защита информации и программ.

2.5.6.В подразделе «Требования к маркировке и упаковке» в общем случае указывают требования к маркировке программного изделия, варианты и способы упаковки.

2.5.7.В подразделе «Требования к транспортированию и хранению» должны быть указаны для программного изделия условия транспортирования, места хранения, условия хранения, условия складирования, сроки хранения в различных условиях.

2.5.8. В разделе «Технико-экономические показатели» должны быть указаны: ориентировочная экономическая эффективность, предполагаемая годовая потребность, экономические преимущества разработки по сравнению с лучшими отечественными и зарубежными образцами или аналогами.

2.6.В разделе «Стадии и этапы разработки» устанавливают необходимые стадии разработки, этапы и содержание работ (перечень программных документов, которые должны быть разработаны, согласованы и утверждены), а также как правило, сроки разработки и определяют исполнителей.

2.7.В разделе «Порядок контроля и приемки» должны быть указаны виды испытаний и общие требования к приемке работы.

2.8.В приложениях к техническому заданию при необходимости приводят:

•перечень научно-исследовательских и других работ, обосновывающих разработку;

•схемы алгоритмов, таблицы, описания, обоснования, расчеты и другие документы, которые могут быть использованы при разработке;

•другие источники разработки.

В случаях, если какие-либо требования, предусмотренные техническим заданием, заказчик не предъявляет, следует в соответствующем месте указать «Требования не предъявляются».

Примеры разработки технического задания приведены в приложениях Б и В.

Порядок выполнения работы

1. Разработать техническое задание на программный продукт согласно своему варианту (см. варианты в приложении А) в соответствии с ГОСТ 19.106-78. При разработке технического задания не ограничиваться требованиями,

приведенными условии задачи приложения А, добавить своих требования , выработанные на предыдущем этапе после анализа бизнес-модели.

2. Оформить отчет по лабораторной работе.
3. Представить отчет по лабораторной работе для защиты.

Требования к результатам выполнения лабораторной работы

При формировании технического задания обратить внимание на

- Требования для пункта 2.5.1 –это набор пользовательских требований четко описывающий функционал разрабатываемого программного средства (не мене 20) (п 2.5.1)
- Требования для пунктов 2.5.2-2.5.5 –это нефункциональные требования к структуре и эксплуатации программного средства.
- Требования для пунктов 2.5.6-2.5.8. технического задания не формируются
- Требования для пункта 2.6 представляются в виде диаграммы Ганта.
- Требования для пункта 2.7 формируются обобщенно и будут уточнены в процессе разработки.

Защита отчета по лабораторной работе

Отчет по лабораторной работе должен быть оформлен согласно требований СТО ВГУЭС и состоять из следующих структурных элементов:

- титульный лист;
- текстовая часть;
- приложение: разработанное технического задания на программное средство.

Текстовая часть отчета должна включать пункты:

- условие задачи;
- порядок выполнения.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Что такое жизненный цикл программного продукта?
2. Дайте определение модели жизненного цикла ПО.
3. Приведите этапы разработки программного средства.
4. Какие этапы включает в себя модель ЖЦ ПС согласно ГОСТ 19.102-77?
5. Что включает в себя этап предпроектного исследования?
6. Перечислите функциональные требования к программному продукту.
7. Перечислите эксплуатационные требования к программному продукту.
8. Перечислите правила разработки технического задания.
9. Назовите основные разделы технического задания.

10. В каких отношениях находятся заказчик и разработчик при выработке требований к программному средству?

Лабораторная работа № 26

На тему: Настройка SNMP

Топология

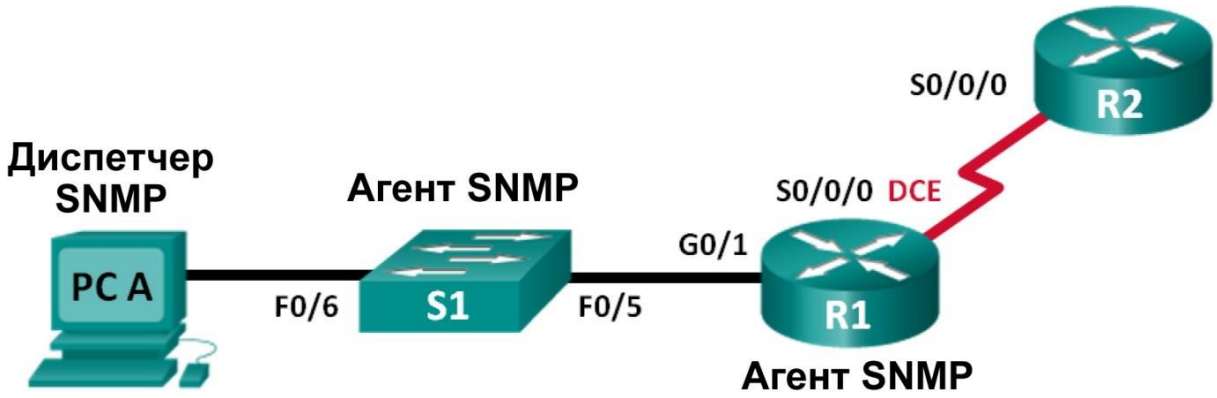


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0	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 A. 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 **lanbase-routing** в качестве шаблона SDM
по умолчанию.

```
S1# configure terminal
S1(config)# sdm prefer lanbase-routing

S1(config)# end
S1# reload
```

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

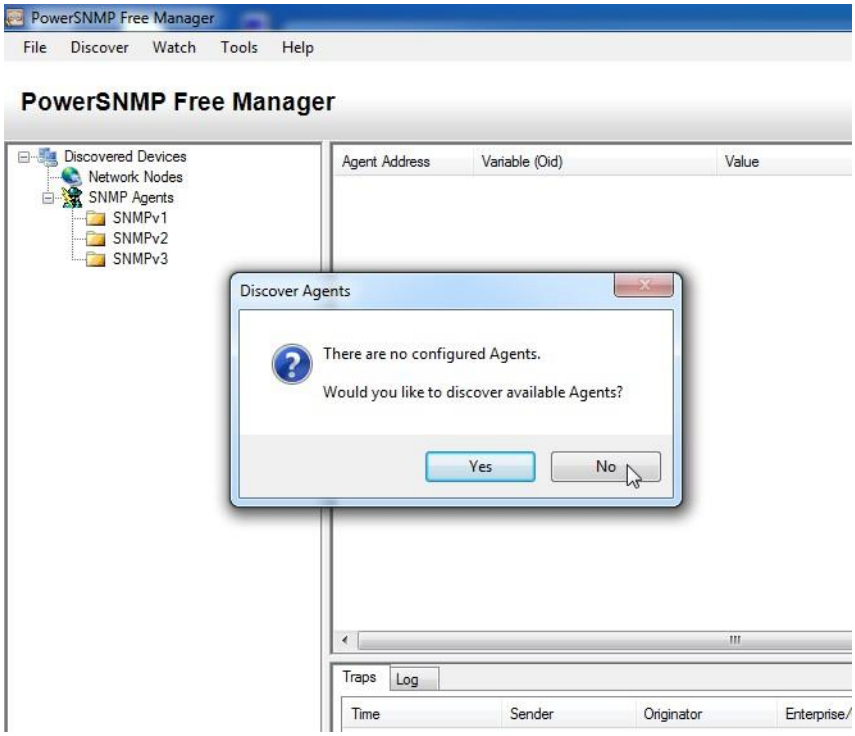
В части 2 вы должны будете установить ПО для управления SNMP и настроить его на ПК A, а также настроить R1 и S1 в качестве агентов SNMP.

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.

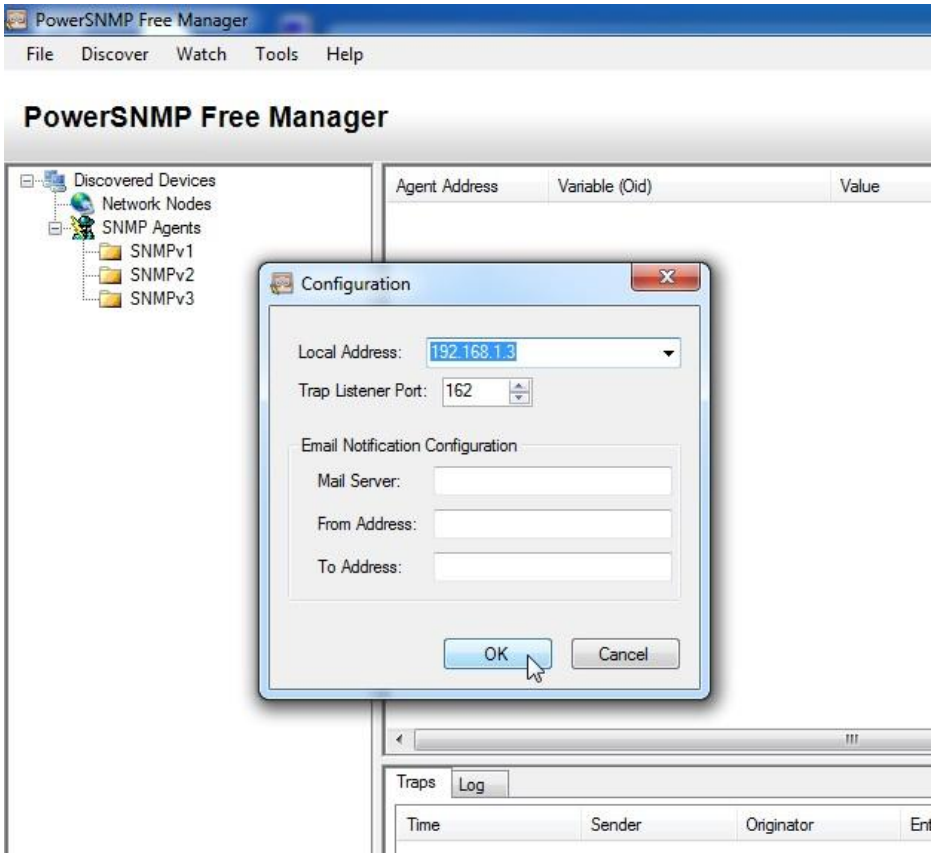
b. Запустите программу PowerSNMP Free Manager.

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.

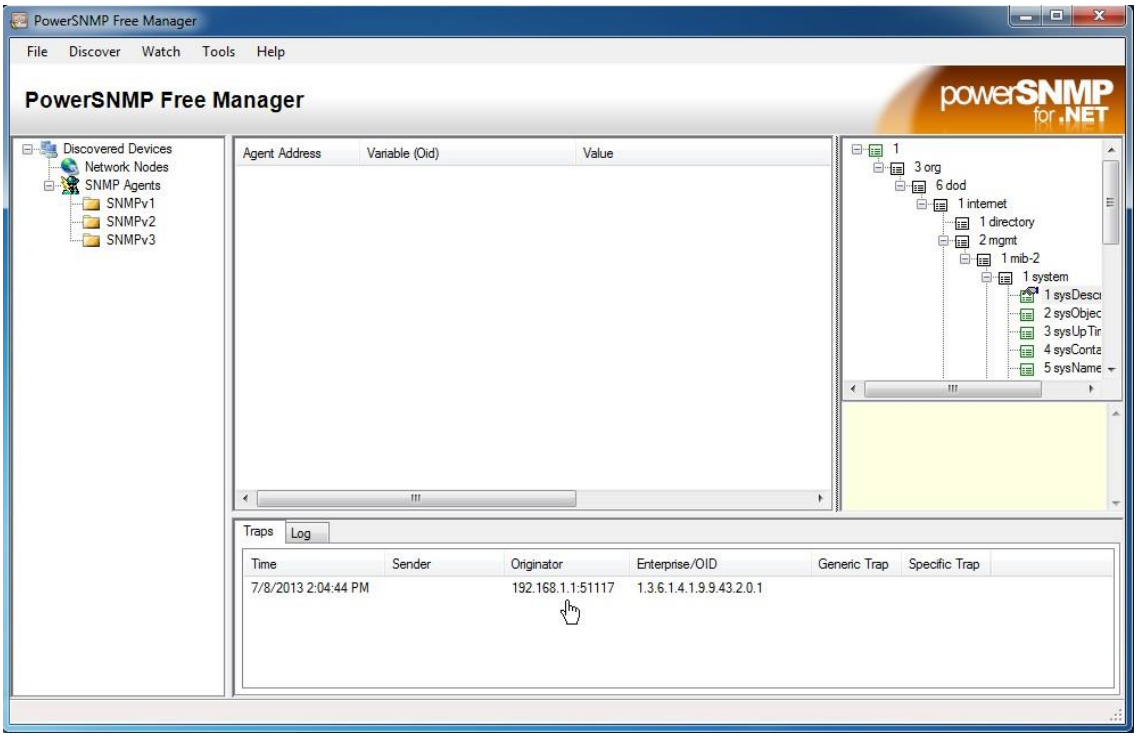
Шаг 2: Настройте агент SNMP.

а. 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
```

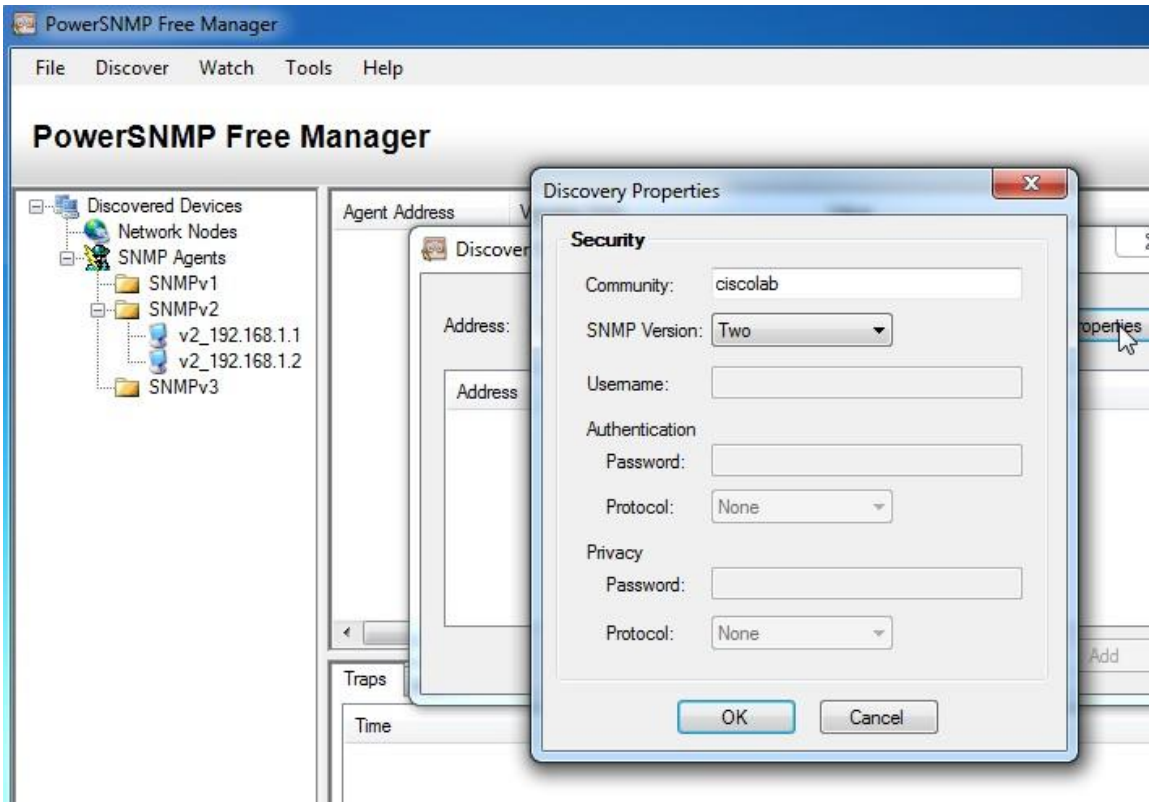
```
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard
SNMP_ACL R1(config-std-nacl)# permit
192.168.1.3
```

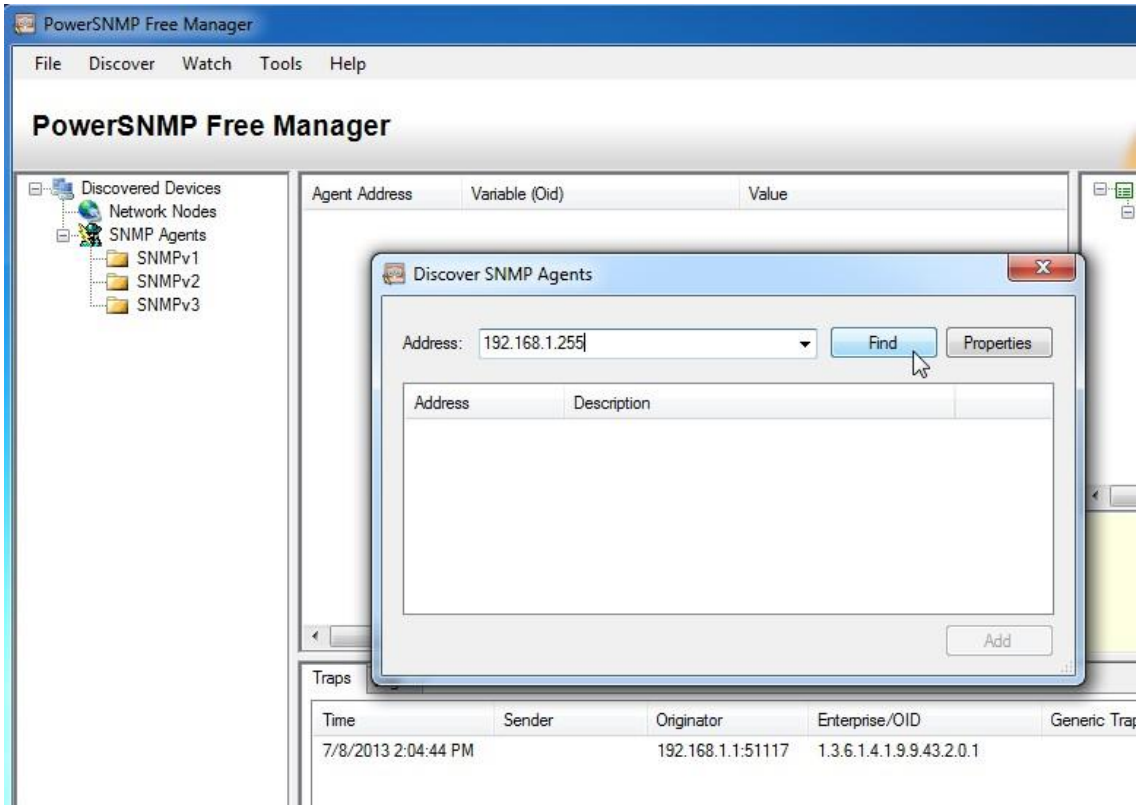
b. На этом этапе можно заметить, что PowerSNMP Free Manager получает уведомления от маршрутизатора R1. Если уведомления не приходят, вы можете попытаться принудительно установить отправку уведомления SNMP, введя команду **copy run start** на маршрутизаторе R1. Если вам не удаётся это сделать, перейдите к следующему шагу.

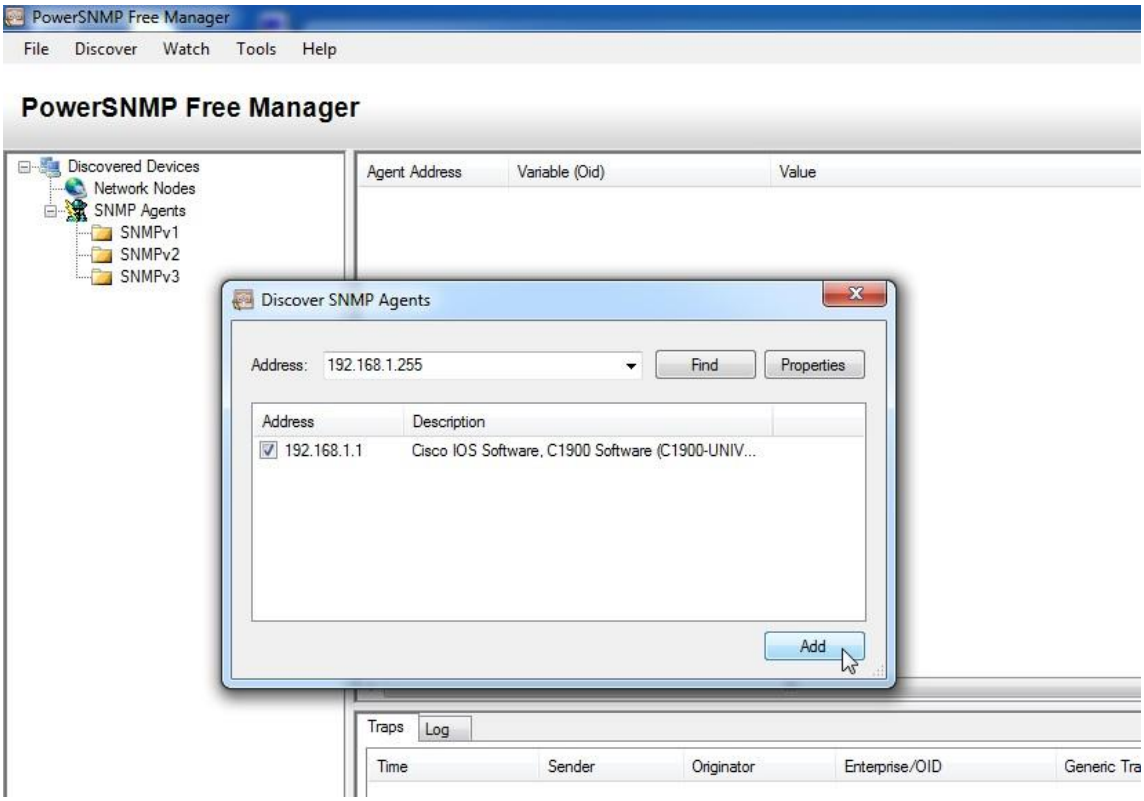


Шаг 3: Выполните обнаружение агентов SNMP.

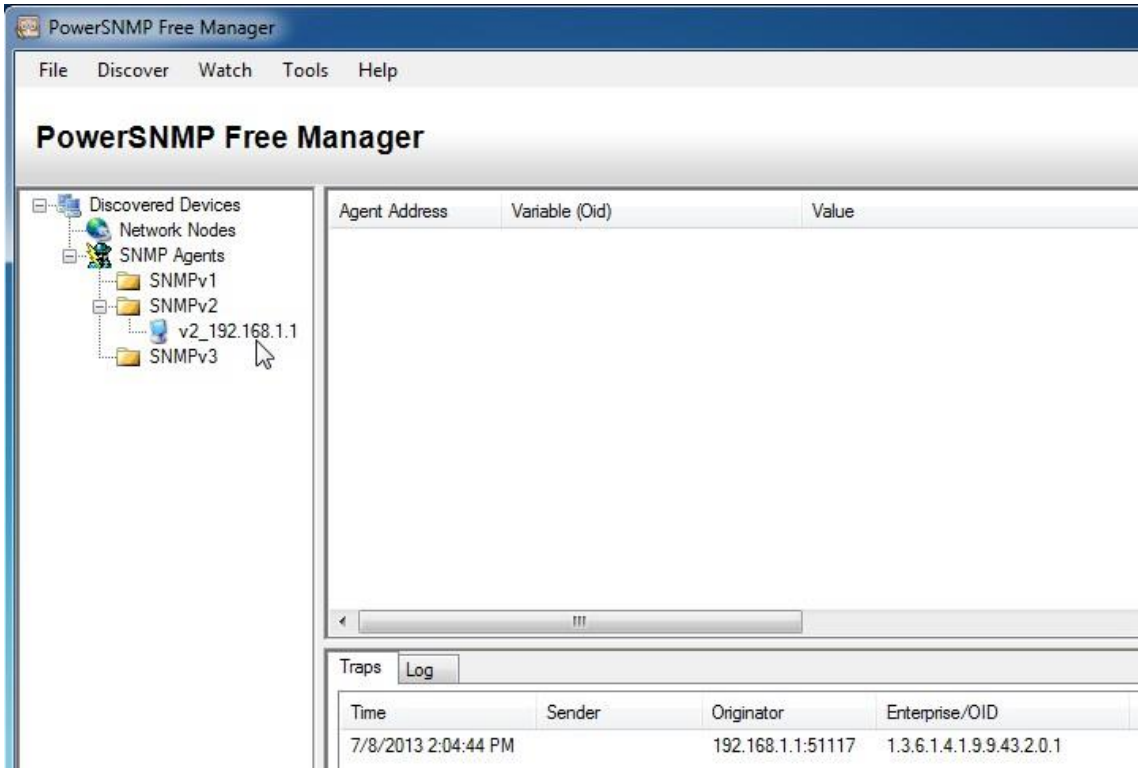
a. В программе PowerSNMP Free Manager на компьютере ПК A откройте окно **Discover > SNMP Agents** (Обнаружение > Агенты SNMP). Введите IP-адрес **192.168.1.255**. В том же окне щёлкните **Properties** (Свойства) и выберите в поле «Community» (Сообщество) параметр **ciscolab**, а в поле «SNMP Version» 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
File
Discover
Watch
Tools
Help
PowerSNMP Free Manager
Discovered Devices
Network Nodes
SNMP Agents
SNMPv1
SNMPv2
v2_192.168.1.1
v2_192.168.1.2
SNMPv3
Agent Address
Address:
Address
Traps
Time
Discovery Properties
Security
Community:
ciscolab
SNMP Version:
Two
Username:
Authentication
Password:
Protocol:
None
Privacy
Password:
Protocol:
None
OK
Cancel
Add


PowerSNMP Free Manager
File
Discover
Watch
Tools
Help
PowerSNMP Free Manager
Discovered Devices
Network Nodes
SNMP Agents
SNMPv1
SNMPv2
SNMPv3
Agent Address
Variable (Oid)
Value
Discover SNMP Agents
Address:
192.168.1.255
Find
Properties
Address
Description
Add
Traps
Time
Sender
Originator
Enterprise/OID
7/8/2013 2:04:44 PM
192.168.1.1:51117
1.3.6.1.4.1.9.9.43.2.0.1



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

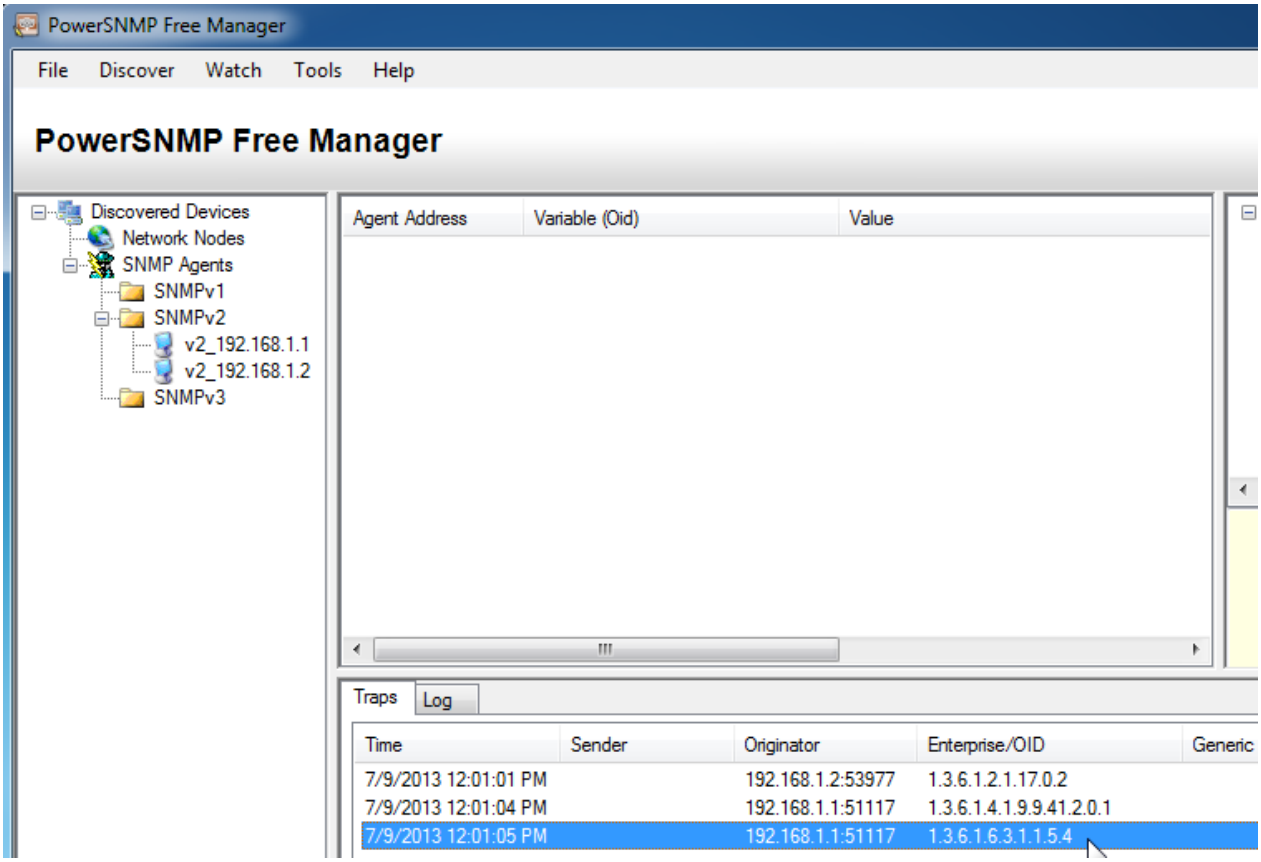
В части 3 принудительно установите отправку уведомлений SNMP на диспетчер SNMP, размещенный на компьютере ПК A. После этого вы должны будете преобразовать полученные коды OID в имена, чтобы прочитать сообщения. Коды MIB/OID можно легко преобразовать с помощью средства Cisco SNMP Object Navigator на веб-сайте 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.

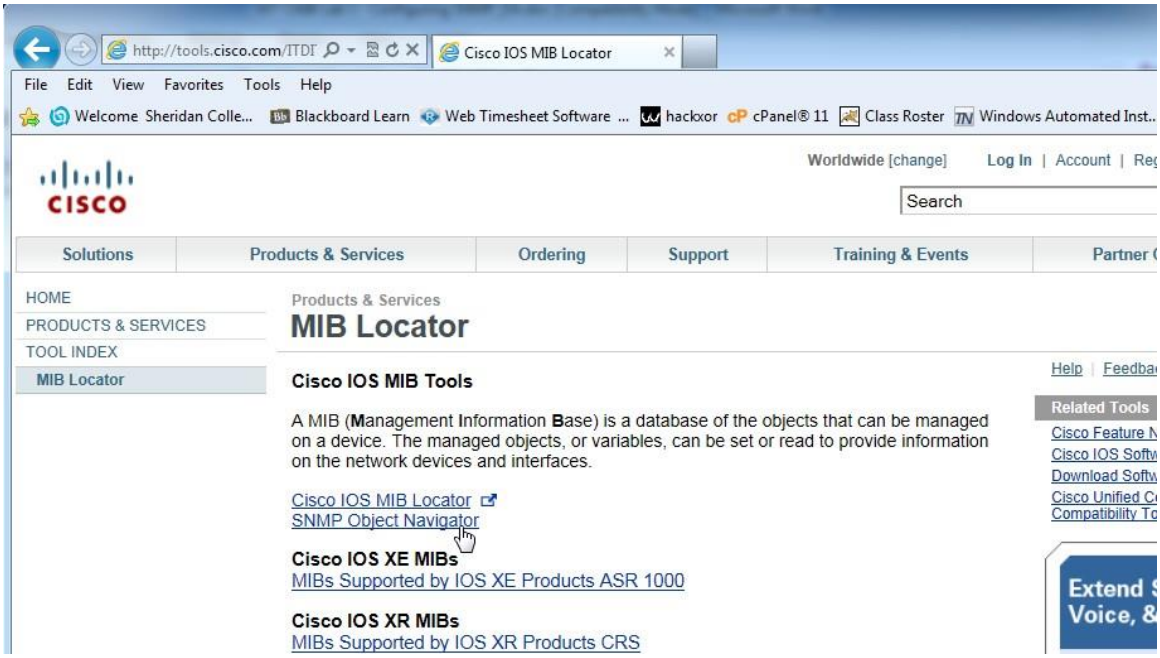
На компьютере с доступом к Интернету откройте веб-браузер и перейдите на веб-сайт

http://www.cisco.com.

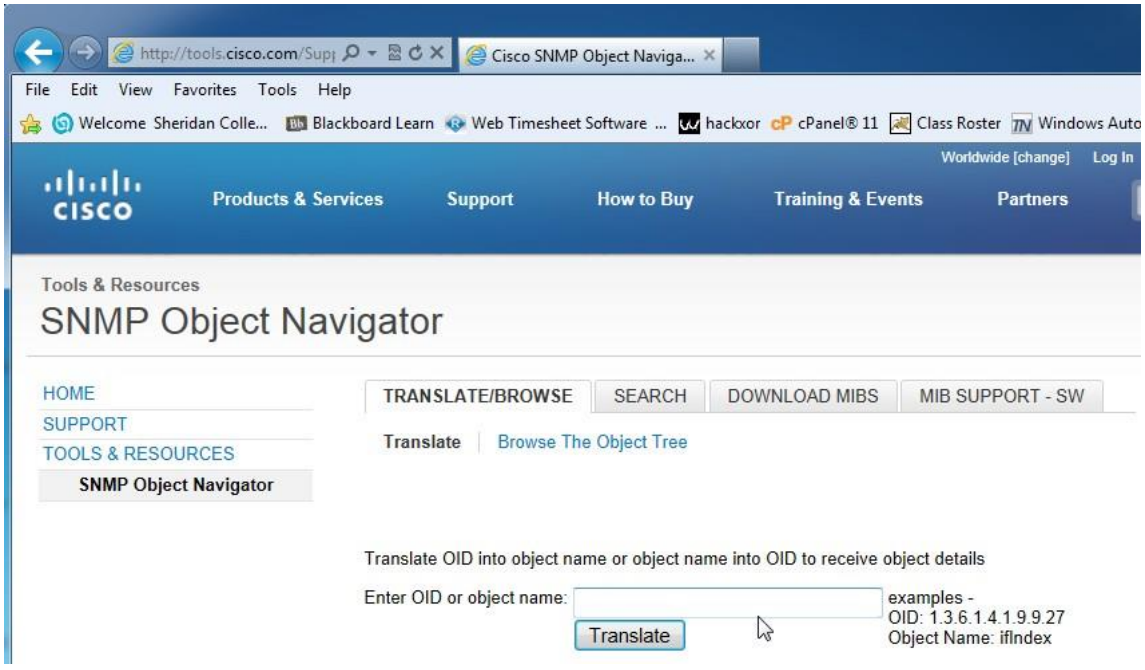
a. С помощью средства поиска в верхней части окна выполните поиск **SNMP Object Navigator**.

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**	**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.

Лабораторная работа № 27

На тему: Сбор и анализ данных NetFlow

Топология

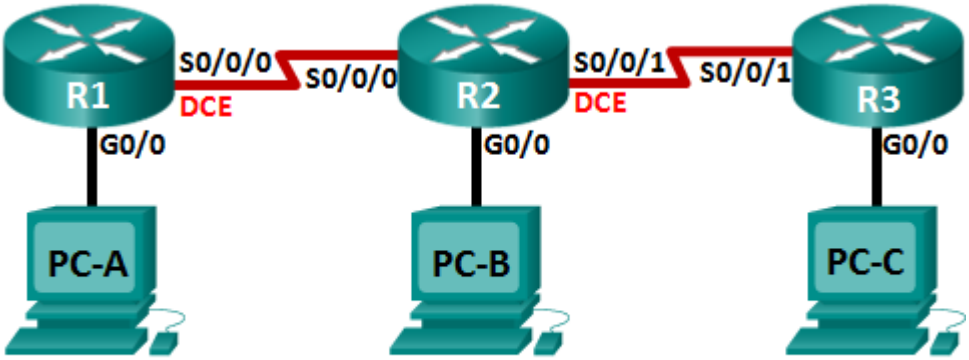


Таблица адресации

Устройство	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**.
l. 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
  ingres
  s ip
  flow
  egress

Serial0/0/1
```

```
ip
flow
ingres
s 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.

a. 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.

b. 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  .14  .01  .70 .000  .00 .001  .00 .001  .01 .009 .001 .002 .000 .001
          7    8    0         1         1         1

    512  544  576  102 1536  204 2560  307 3584  409 4608
                   4         8         2         6
   .001  .00  .09  .00 .000  .00 .000  .00 .000  .00 .000
          1    7    0         0         0         0

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  .00  1.0  .00 .000  .00 .000  .00 .000  .00 .000 .000 .000 .000 .000
           0    0    0         0         0         0

    512  544  576  102 1536  204 2560  307 3584  409 4608
                   4         8         2         6
   .000  .00  .00  .00 .000  .00 .000  .00 .000  .00 .000
           0    0    0         0         0         0

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  Byte    Packet Active(Sec) Idle(Sec)
                                           s        s
--------           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   Pkt
                                                                            s
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP   Pkt
                                                                            s
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.				

Лабораторная работа № 28

На тему: Инструментарий сетевого администратора для наблюдения

Цель работы

Требуется научиться:

- определять сетевые настройки машины;
- проверять доступность удаленных узлов и маршруты до них;
- захватывать, анализировать и сохранять сетевой трафик.

Предполагается, что вы знаете:

- об уровнях и протоколах сетевого взаимодействия, модель OSI (лекция 1);
- что такое IP-адрес и маска подсети, как их вычислять (СПО, ЛР по Linux);
- что такое DNS (там же).

Изученное в ходе ЛР пригодится:

- в учебе — для отладки программ на последующих ЛР;
- на практике — для поиска причин и источников неполадок (troubleshooting).

Задание

Примечание. В задании встречаются протоколы и инструменты, которые еще не изучались (traceroute, ICMP, UDP, TCP, DNS) — в таких местах даны краткие пояснения, а подробности будут рассмотрены на последующих занятиях.

Определение сетевых настроек

1. Просмотрите параметры сетевого подключения через GUI (графический интерфейс).

Для этого дважды щелкните на значке сетевого подключения (на панели уведомлений в правом нижнем углу) и на вкладке «Поддержка» нажмите кнопку «Подробности…».

Выделите все строки таблицы и занесите в отчет.

Можно наблюдать:

- физический адрес — адрес канального уровня (L2), он же MAC-адрес;
- IP-адрес — адрес сетевого уровня (L3);
- маску подсети, с помощью которой IP-адрес делится на адрес сети (префикс) и номер узла в ней;
- основной шлюз — IP-адрес машины, через которую направляются пакеты во внешнюю сеть;
- DHCP-сервер — IP-адрес машины, с помощью которой был получен IP-адрес данной, то есть выполнена динамическая конфигурация IP;
- время, когда аренда получена — то есть выдан динамический IP — и когда аренда истекает — то есть понадобится снова обратиться к DHCP-серверу за новым адресом;
- DNS-сервер — IP-адрес машины, к которой данная будет обращаться при необходимости разрешить (преобразовать) символьное имя (например, `mpei.ru`) в IP-адрес.

2. Просмотрите параметры сетевого подключения через командную строку.

Для этого откройте командную строку (Пуск → Выполнить, ввести `cmd`), в ней выполните команду:

```
ipconfig /all
```

Саму команду и ее вывод скопируйте и занесите в отчет.

Раздел «Настройка протокола IP для Windows» относится ко всей машине, а не к отдельным сетевым подключениям. В частности:

- по имени компьютера можно обратиться к нему *в локальной сети*, однако эта возможность специфична для Windows и может быть выключена;
- IP-маршрутизация (обычно выключена) определяет, будет ли данный узел пересылать пакеты, которые предназначены не ему.

Далее следуют разделы, описывающие сетевые подключения (обычно одно). Убедитесь, что показания в таком разделе соответствуют полученным из GUI. Присутствует и настройка, через GUI невидимая: «автонастройка включена» — она означает, что в случае, когда адрес не задан статически, а DHCP-сервер недоступен, интерфейс получит специальный адрес автоматической конфигурации.

3. Проанализируйте полученные настройки.

- Из IP-адреса и маски подсети определите и запишите адрес сети (префикс).
- Находится ли шлюз по умолчанию в той же сети? Если нет, то в какой?
- Находится ли сервер DHCP в той же сети?
- Находится ли сервер DNS в той же сети?

Ping: проверка доступности узлов

Команда `ping` позволяет направить узло специальные запросы, на которые тот должен ответить, чтобы подтвердить свою доступность.

4. В командной строке выполните:

```
ping mpei.ru
```

Сделайте то же самое для других адресов:

- собственного IP-адреса машины (полученного в предыдущем разделе);
- основного шлюза;
- сервера DNS;
- `mos.ru`;
- `lab.facelessmen.org`;

Из показаний `ping` сведите в таблицу: символьный адрес узла, его IP-адрес и среднее время отклика.

5. Выполните команду:

```
ping mpei.ru
```

Как можно видеть, на запросы `ping` не получено ответов, потери 100 %. Это не означает, что узел недоступен (попробуйте зайти на сайт) — просто сервер или промежуточное устройство настроены не давать ответов на запросы, которые шлет `ping`. Это делается для безопасности: `ping` позволяет сканировать доступность узлов и сервисов на них, способен создать нагрузку на сервер.

Трассировка маршрутов прохождения трафика

Полезно бывает отследить маршрут (trace route) прохождения пакета до заданного узла. В Linux соответствующая программа называется `traceroute`, в Windows — `tracert`.

6. Выполните команду:

```
tracert lab.facelessmen.org
```

Занесите команду и ее вывод в отчет.

Можно наблюдать два факта:

- Не для всех узлов можно получить символьное имя по IP. Если символьное имя и не нужно, у `tracert` есть ключ `-d`.
- Не все пункты маршрута удается установить — как минимум, это узлы, настроенные не слать ответы на запросы `tracert`, а некоторые узлы блокируют и чужие ответы (как правило, на границах защищенных сетей).

Разрешение символьных (доменных) имен в IP-адреса

Как известно, пакеты направляются на адреса сетевого уровня, в типичном случае — на IP-адреса, а люди пользуются символьными именами, например, `mpei.ru`. Разрешением (resolution, т. е. преобразованием) символьных имен в адреса занимается система доменных имен (Domain Name System — DNS). Сервер DNS содержит базу соответствия имен адресам; клиент запрашивает по протоколу DNS адрес для имени, сервер отвечает ему.

7. Выполните команду:

```
nslookup mpei.ru
```

Занесите команду и ее вывод в отчет.

«Non-authoritative answer» означает, что ответ дан не официальным сервером DNS, обслуживающим вышестоящую зону — в случае `mpei.ru`, зону `ru.` — а промежуточным сервером DNS. Это нормально. Промежуточные сервера кэшируют (запоминают) ответы вышестоящих, чтобы снизить на них нагрузку и отвечать быстрее.

Кэшируют ответы DNS не только сервера, но и клиенты, в том числе локальная машина. Обычно это ускоряет работу и потому удобно, но для лабораторной работы или при проблемах с DNS кэшированный ответ мешает понять, что происходит. Можно сбросить кэш специальной командой:

```
ipconfig /flushdns
```

Wireshark: захват и анализ сетевого трафика

Все проходящие через машину сетевые пакеты можно захватить (capture) и пристально изучить. Это радикальный способ отладки программ, исследования протоколов и отслеживания проблем.

Программа Wireshark позволяет как захватить сетевой трафик, так и с удобством просмотреть его, исследовать в разных разрезах, собрать статистику.

Примечание. В лаборатории установлена Wireshark 1.10 — последняя версия, поддерживающая Windows XP; новейшая версия Wireshark — 2.4 (на февраль 2018).

Исследуем, что происходит в сети при заходе на web-страницу.

Захват пакетов

8. Запустите Wireshark из меню «Пуск».

На главной странице доступны ссылки на справку («Online» справа), список недавних файлов («Files» по центру) и главный интересующий нас раздел «Capture». По существу, в нем можно выбрать, с каких сетевых интерфейсов (например: кабельного подключения, Wi-Fi) и какие именно данные захватывать.

9. Откройте диалог «Capture options» и настройте захват пакетов, который относятся к заходу на web-страницу по основному сетевому интерфейсу.

- В списке интерфейсов (вверху) отметьте тот, который исследовали в начале лабораторной работы.
- В поле «Capture filter» введите выражение:

```
(tcp port 80) or (udp port 53) or icmp
```

- Не закрывайте диалог.

Смысл фильтра захвата — отобрать только запрос страницы и ответ на него с собственно страницей (`tcp port 80`), запросы и ответы DNS (`udp port 53`), а также служебные сообщения ICMP (`icmp`), появляющиеся при некоторых ошибках.

10. Откройте браузер. Если он уже открыт, закройте в нем все окна и вкладки, оставив единственную пустую.

В противном случае будут захвачены не только те пакеты, которые требуется исследовать, и придется дополнительно их фильтровать.

11. Очистите кэш браузера.

В лаборатории установлен Internet Explorer 8, где это делается из меню *Сервис → Удалить журнал обозревателя…* с обязательно установленной галочкой *Временные файлы интернета*.

12. Очистите кэш DNS.

13. В Wireshark запустите захват пакетов кнопкой «Start» диалога настройки захвата. Вне диалога это делалось бы кнопкой «Start capture».

14. В адресной строке браузера введите адрес:

```
lab.facelessmen.org
```

и нажмите выполните переход (нажмите *Enter* или кнопку).

В Wireshark должны появится два пакета DNS (выделяются голубым) и несколько пакетов HTTP (выделяются салатовым).

15. Остановите захват пакетов красной кнопкой «Stop capture» слева вверху.

Просмотр пакетов

Рабочее окно Wireshark разделено на три области (сверху-вниз):

- Список пакетов со столбцами их свойств и подсветкой в зависимости от типа.
- Результат разбора пакета (dissection — термин Wireshark), то есть структурированное представление пакета, разобранного в соответствии с протоколами.
- Содержимое пакета в виде байт в шестнадцатеричном виде (hex) и соответствующего им текста. Числа `0000`, `0010` и т. д. по левому краю — смещения от начала пакета в hex, то есть 0, 16 и т. д.

Области диссекции и содержимого пакета связаны. При выборе поля или уровня диссекции подсвечиваются соответствующие байты в содержимом. И

наоборот — при щелчке на байте содержимого подсвечивается элемент диссекции, к которому этот байт относится.

Над списком пакетов есть поле фильтра, позволяющее дополнительно отобрать захваченные пакеты. В строке состояния внизу окна отображается общее число пакетов *(packets)* и количество отображаемых из них *(displayed)*. Фильтр — логическое выражение, включающее свойства пакета. Список свойств можно увидеть в диалоге «Expression…» рядом с фильтром. Обратите внимание, что [синтаксис][wireshark/filter] этого фильтра (отображения) отличается от фильтра захвата: например, вместо `tcp port 80` пишется `tcp.port == 80`.

Настройка отображения списка пакетов

В списке пакетов отображаются их основные свойства:

- номер пакета;
- время прохождения (по умолчанию — в секундах от начала захвата);
- IP-адреса источника (source) и получателя (destination);
- протокол верхнего уровня;
- полная длина;
- краткая сводка (info), отражающая суть пакета.

В зависимости от задачи бывает полезно видеть и другие поля. Добавим столбцы с портами и будем отображать порты в числовом виде в сводке.

16. В диалоге *Edit → Preferences…* выберите раздел *Columns*.
17. Добавьте столбец с портом отправителя: внизу в выпадающем списке выберите *Src port (unresolved)* и нажмите *Add*, переименуйте столбец, щелкнув по его мени в таблице. Перетащите его мышью перед столбцом *Protocol*.
18. Сделайте то же самое для порта получателя *Dest port (uresolved)*.
19. Перейдите в раздел *Name resolution* и снимите галочку *Resolve transport names*.
20. Закройте диалог кнопкой OK и убедитесь, что новые столбцы появились.

Вид времени прохождения можно менять в меню *View → Time display format*. Нужно понимать, что у Wireshark не всегда есть информация о том, в каком часовом поясе захвачен трафик (при анализе файлов — см. ниже), поэтому отображение абсолютного времени может быть со смещением.

Исследование пакетов

Результаты разбора сгруппированы по протоколам и упорядочены по уровням от нижнего (L2, канального) к верхнему (L7, прикладному). Внутри уровней выделены поля данных. В квадратных скобках показываются косвенные показатели, которые в пакет непосредственно не записаны.

Исследование отдельных пакетов (DNS)

Рассмотрим пакет с ответом DNS («standard query response» в сводке). Уровни:

- Frame — условный уровень, на котором Wireshark отображает сведения об интерфейсе, с которого был захвачен пакет, с времени захвата.
- Ethernet II — канальный уровень (L2). Его свойств немного:
  - MAC-адреса отправителя *(Src)* и получателя *(Dst)*. Они показаны как 6 байт в hex (так они записаны в пакете), а также с префиксом-названием производителя оборужования, потому что диапазоны адресов приписаны к ним.

- Протокол следующего уровня (L3) в виде кода (так записано в пакете) и по названию (из справочника).

- Internet Protocol Version 4 — сетевой уровень (L3), пакет IPv4. Среди его свойств есть IP-адрес отправителя *(Src)* и получателя *(Dst)*. Можно убедиться, что они совпадают с собственным адресом машины и адресом сервера DNS, установленного в начале ЛР.
- User Datagram Protocol — транспортный уровень (L4). На этом уровне определяется, какому приложению предназначен пакет, по номерам портов: отправителя *(Src port)* по получателя *(Dst port)*. В данном случае пакет отправлен сервером DNS, который работает на порту 53, а получен клиентом DNS на порту со случайным большим номером.
- Domain Name System (response) — прикладной уровень (L7). Собственно сообщение-ответ на запрос, какой IP у `lab.facelessmen.org`. Стоит отметить:
  - поле *[Request In: ...]* — ссылку на пакет с запросом, к которому относится рассматриваемый ответ;
  - поле *Transaction ID*, одинаковое в запросе и ответе, чтобы клиент мог отправить несколько запросов, а затем связать ответы с ними — фактически это поле играет роль сеансового (L5) уровня, хотя отдельного протокола под это не выделено.

21. В области разбора пакета выделите последовательно L2, L3, L4, L7 и проследите в области содержимого пакета, что они расположены последовательно — это и есть инкапсуляция уровней.

22. В области содержимого пакета выберите несколько байт, чтобы увидеть, каким полям и каких уровней они соответствуют.

При исследованиях трафика, особенно сообща с другими специалистами, бывает полезно добавить к пакетам текстовые комментарии. Для этого нужно использовать пункт *Packet comment…* контекстного меню пакета в списке.

23. Добавьте к рассматриваемому пакету комментарий «`look at me`».

По комментариям можно пакеты искать (фильтровать):

- фильтр `pkt_comment` или `frame.comment` выбирает все пакеты с комментариями;
- фильтр `frame.comment contains "look"` выбирает пакеты, комментарий к которым содержит подстроку `look`.

Исследование сеансов (HTTP)

24. Введите фильтр отображения: `http || dns || icmp`.

Хотя он одинаков по сути с фильтром захвата, но сообщает Wireshark, что нас интересуют не просто пакеты через порт 80 по протоколу TCP, а именно сообщения HTTP (они же, но на уровне L7). В результате количество пакетов в списке сократилось: остались только несущие сообщения, а служебные скрыты.

25. Щелкнув по любому пакету HTTP (салатовому) правой кнопкой мыши, выберите в контекстном меню *Follow TCP stream* (проследить сеанс).

В открывшемся окне показаны данные, переданные клиентом серверу (подсвечены красным) и от сервера клиенту (подсвечены синим). Как можно наблюдать:

- Протокол имеет текстовый формат. Для случаев, когда это не так, имеется возможность переключить просмотр в режим отображения байт *(Hex Dump)*.
- Помимо непосредственно текста страницы передается немало служебных данных.

26. Закройте окно слежения за сеансом.

Обратите внимание, что фильтр отображения изменился на `tcp.stream eq 0`: число в конце (`0` в примере) — порядковый номер сеанса из всех захваченных. Соответственно, пропала фильтрация только пакетов с сообщениями HTTP. Если просмотреть пакеты, в большинстве нет данных выше *Transmission Control Protocol* (TCP) — это служебные пакеты L4+L5, нужные для установления, поддержки и завершения сеанса. Они будут рассмотрены на последующих ЛР.

27. Верните предыдущий фильтр отображения.

Они сохраняются в выпадающем списке поля фильтра. После выбора нужно применить фильтр, нажав *Enter* или кнопку *Apply*.

Анализ трафика

Иногда отдельные пакеты не представляют большого интереса, зато можно сделать выводы по статистике трафика. Опробуем важнейшие средства из меню *Statistics*. В каждом пункте нужно открыть соответствующий диалог и ознакомиться с его содержимым и возможностями.

28. *Protocol Hierarchy* — сводка, какие протоколы и насколько часто встречаются в захваченном трафике. Позволяет сразу обнаружить сетевую активность, которой быть не должно, или наоборот.
29. *Conversations* — сеансы в широком смысле, то есть не только L5, но и обмены данными, например, по протоколу DNS.
30. *Endpoints* — уникальные адреса и порты участников.
31. *Packet Lengths* — гистограмма распределения длин пакетов. Полезна для выявления аномальной активности или для оптимизации настроек сетевого ПО и аппаратуры.
32. *IO Graph* — график пакетов или байт в секунду. Полезен для анализа нагрузки и обнаружения времени атак. Сохраните его как рисунок `lab01-tools-iograph.png`.
33. *Flow Graph…* — диаграмма последовательности переданных пакетов. Постройте ее для отображаемых пакетов *(Displayed packets)* всех видов *(General flow)* с отображением сетевых адресов *(Network source/destination addresses)*. Сохраните результат в текстовый файл `lab01-tools-flowgraph.txt`.

Сохранение данных

Далеко не всегда пакеты захватываются в Wireshark, сразу же анализируются и забываются. Гораздо чаще захват происходит:

- в то время, когда наблюдается интересующий трафик;
- на той машине (устройстве), где это возможно;
- не обязательно Wireshark (`tcpdump`, встроенными средствами оборудования).

Анализ же выполняется отдельно, иногда не одним человеком и по несколько раз. Очевидно, для этого нужно сохранять захваченные пакеты в файл, чтобы передавать его и анализировать трафик offline.

34. Выберите пункт меню *File → Save* и сохраните запись трафика в файл `lab01-tools.pcapng`.

Здесь необходимо обратить внимание на формат файла:

- *Wireshark/... `*.pcapng`* — современный формат Wireshark: позволяет сохранять комментарии к пакетам, расширяем в будущем, однако не поддерживается многими небольшими утилитами для обработки записей трафика.
- *Wireshark/tcpdump/... `*.pcap`* — классический формат. Не вполне универсален и не расширяем, зато поддерживается всеми средствами обработки записей.
- То же с «nanosecond precision» — времена прохождения пакетов записываются с точностью до наносекунд, что бывает нужно на быстрых интерфейсах.

Wireshark позволяет открыть файл в одном формате и сохранить в другом.

В аналогичном диалоге *File → Export specified packets...* можно выбрать, какие пакеты сохранять: все, отображаемые или с выбранными номерами.

35. Убедитесь, что файл сохранился, и закройте Wireshark. Выберите файл в «Проводнике» и откройте его в Wireshark.

Иногда нужно экспортировать не пакеты, а результаты их разбора, то есть, по сути, область списка пакетов, область разбора пакета или обе сразу. Для этого применяется пункты меню из группы *File → Export packet dissections*: можно экспортировать данные как в текстовом виде для чтения *(...as "Plain Text" file)*, так и в структурированных видах.

В открывшемся диалоге можно выбрать, что сохранять:

- *packet summary* — строку из списка пакетов;
- *packet details* — результат разбора в текстовом виде;
- *packet bytes* — содержимое пакета как байты в шестнадцатеричном виде.

36. Сохраните только список пакетов как текстовый файл `lab01-tools-export.txt`.

На сайте Wireshark есть познавательный сборник записей трафика разных протоколов.

Контрольные вопросы

Примечание. Во всех вопросах «привести пример» означат открыть запись трафика в Wireshark и продемонстрировать требуемое.

1. Может ли быть настроен IP-адрес, но не настроен шлюз по умолчанию? Если да, к чему это приведет; если нет, почему?
2. Может ли быть настроен IP-адрес, но не выбран сервер DHCP? Если да, в каком случае и на что это повлияет; если нет, почему?
3. Может ли быть настроен IP-адрес, но не настроен сервер DNS? Если да, к чему это приведет; если нет, почему?

4. Если не настроено статического адреса и не работает DHCP, получит ли интерфейс адрес (при настройках, наблюдавшихся в ЛР), и если да, какой?

5. Можно ли с компьютера под управлением Windows с помощью `ping` проверить доступность компьютера под управленим Linux? А наоборот?

6. Верно ли, что если не приходят ответы на `ping`, сервер недоступен по сети? Если да, приведите пример из ЛР; если нет, в каком случае?

7. Может ли IP-адрес не иметь доменных имен? А наоборот?

8. Можно ли настройкой машины с IP-адресом добиться, чтобы этот адрес нельзя было найти по доменному имени? Если да, в каком случае; если нет, почему?

9. Возможно ли по IP-адресу узнать его доменные имена?

10. Можно ли с помощью Wireshark перехватить трафик, идущий непосредственно между двумя другими машинами (без удаленного доступа к этим машинам)?

11. Как с помощью Wireshark захватить трафик и через кабель, и через Wi-Fi?

12. Как в Wireshark ограничить перечень захватываемых пакетов? Приведите пример *не* из ЛР.

13. Как в Wireshark отфильтровать захваченные пакеты? Приведите пример *не* из ЛР.

14. Исследователю нужно проанализировать задержки между пакетами, то есть время, прошедшее между появлением соседних захваченных пакетов. Как быстро получить в Wireshark эти сведения?

15. Как в Wireshark просмотреть, представление интересующего поля протокола в содержимом пакета (в виде байт)? Продемонстрируйте на примере.

16. Как в Wireshark определить, к какому полю и какого протокола относится произвольбый байт в содержимом пакета? Продемонстрируйте на примере.

17. Как в Wireshark, имея захваченный трафик, найти IP-адреса всех участников и отфильтровать только пакеты, связанные с определенным адресом?

18. Как в Wireshark, имея захваченный трафик, найти все сеансы TCP в нем и отфильтровать только пакеты, участвующие в одном из них?

19. Администратору известно, что в трафике его сервера в основном HTTP, некоторый объем DNS и на порядок меньше ICMP, чем DNS. Как в Wireshark, захватив этот трафик, быстро проверить, что соотношения протоколов в норме?

20. Требуется проанализировать запись трафика, содержащую начало DDoS-атаки, при которой трафика внезапно стало на порядок больше нормы. Как в Wireshark быстро найти момент начала атаки? (Запись начинается раньше.)

21. Администратору известно, что в нормальном трафике размеры пакетов в основном менее 400 байт, хотя иногда встречаются и больше (до 1500 байт). При конкретной атаке направляется много пакетов длиной около 1000 байт. Как в Wireshark быстро проверить, была ли атака за время записи?

22. В каких случаях имеет смысл сохранять захваченные пакеты в `*.pcap`, а в каких — в `.pcapng`? Что делать, если нужен файл `*.pcap`, а имеется `*.pcapng`?

Лабораторная работа № 29

На тему: Сбой в работе сети

Топология

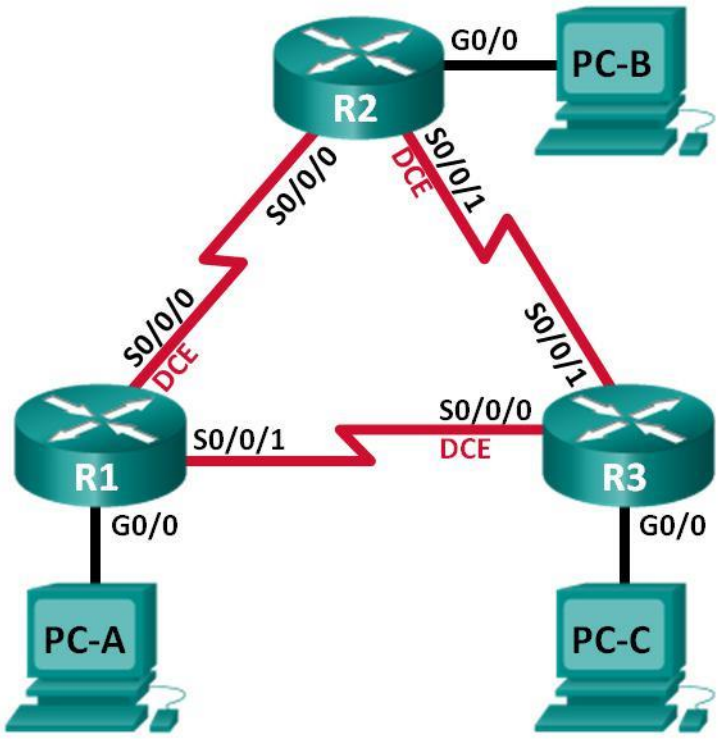


Таблица адресации

Устройство	Интерфейс	IPv6-адрес	Шлюз по умолчанию
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 локальный канал	Недоступно
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:13::1/64 FE80::1 локальный канал	Недоступно
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 локальный канал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 локальный канал	Недоступно
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 локальный канал	Недоступно
R3	G0/0	2001:DB8:ACAD:C::3/64 FE80::3 локальный канал	Недоступно
	S0/0/0 (DCE)	2001:DB8:ACAD:13::3/64 FE80::3 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 локальный канал	Недоступно
PC-A	Сетевой адаптер	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	Сетевой адаптер	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	Сетевой адаптер	2001:DB8:ACAD:C::C/64	FE80::3

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Настройка и проверка маршрутизации

Часть 3. Настройка пассивных интерфейсов

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.

В данной лабораторной работе необходимо настроить топологию сети с маршрутизацией OSPFv3, назначить идентификаторы маршрутизаторов, настроить пассивные интерфейсы и использовать несколько команд интерфейса командной строки для вывода и проверки данных маршрутизации

OSPFv3.

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:

q. 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

r. 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала,
например Tera Term);

s. консольные кабели для настройки устройств Cisco IOS через консольные порты;

t. кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

С первой части лабораторной работы 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.

o. Отключите поиск DNS.

p. Присвойте имена устройствам в соответствии с топологией.

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

r. Установите **cisco** в качестве пароля vty.

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

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

u. Зашифруйте все незашифрованные пароли.

v. Настройте индивидуальные и локальные IPv6-адреса канала, которые указаны в таблице адресации для всех интерфейсов.

w. Включите IPv6-маршрутизацию на каждом маршрутизаторе.

x. 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 к другим ПК, пока не настроена маршрутизация OSPFv3. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка маршрутизации OSPFv3

Во второй части вам предстоит настроить маршрутизацию OSPFv3 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются верным образом.

Шаг 1: Назначьте идентификаторы маршрутизаторов.

Для идентификатора маршрутизатора протокол OSPFv3 использует 32 -битный адрес. Поскольку на маршрутизаторах не настроены IPv4-адреса, вам необходимо вручную назначить идентификатор маршрутизатора с помощью команды **router-id**.

t. Выполните команду **ipv6 router ospf**, чтобы активировать OSPFv3 в маршрутизаторе.

```
R1(config)# ipv6 router ospf 1
```

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

u. Назначьте маршрутизатору R1 идентификатор OSPFv3 **1.1.1.1**.

```
R1(config-rtr)# router-id 1.1.1.1
```

v. Начните процесс маршрутизации OSPFv3 и назначьте идентификатор маршрутизатора **2.2.2.2** маршрутизатору R2, а идентификатор **3.3.3.3** маршрутизатору R3.

w. Выполните команду **show ipv6 ospf**, чтобы проверить идентификаторы на всех маршрутизаторах.

```
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 <output omitted>
```

Шаг 2: Настройте протокол OSPFv6 на маршрутизаторе R1.

При использовании IPv6 на каждом интерфейсе обычно настроено несколько IPv6-адресов. В OSPFv3 не используется команда network. Вместо этого, маршрутизация OSPFv3 активируется не на сетевом, а на интерфейсном уровне.

g. Выполните команду **ipv6 ospf 1 area 0** для каждого интерфейса маршрутизатора R1, который должен участвовать в маршрутизации OSPFv3.

```
R1(config)# interface g0/0 R1(config-if)#
ipv6 ospf 1 area 0 R1(config-if)#
interface s0/0/0 R1(config-if)# ipv6 ospf
1 area 0 R1(config-if)# interface s0/0/1
R1(config-if)# ipv6 ospf 1 area 0
```

Примечание. Идентификатор процесса должен совпадать с идентификатором процесса, использованным на шаге 1a.

В Добавьте интерфейсы маршрутизаторов R2 и R3 в OSPFv3-область 0. Добавляя интерфейсы в область 0, вы увидите сообщения об установленных отношениях смежности с соседними маршрутизаторами.

```
R1#
*Mar 19 22:14:43.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING
to FULL, Loading Done
R1#
*Mar 19 22:14:46.763: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

Шаг 3: Проверьте соседей OSPFv3.

Выполните команду **show ipv6 ospf neighbor**, чтобы убедиться, что маршрутизатор установил отношения смежности с соседними маршрутизаторами. Если идентификатор соседнего маршрутизатора не отображается или если не отображает состояние FULL, то отношения смежности OSPF не были установлены.

```
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
       3.3.3.3            0 FULL/     -   00:00:39       6               Serial0/0/1
       2.2.2.2            0 FULL/     -   00:00:36       6               Serial0/0/0
```

Шаг 4: Проверьте настройки протокола OSPFv3.

Команда **show ipv6 protocols** позволяет быстро проверить критически важные данные конфигурации OSPFv3, включая идентификатор процесса OSPF, идентификатор маршрутизатора и интерфейсы, включённые для OSPFv3.

```
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
Number of areas: 1 normal, 0 stub, 0 nssa
Interfaces (Area 0):
Serial0/0/1
```

```
Serial0/0/0
GigabitEthernet0/0
Redistribution:
None
```

Шаг 5: Проверьте интерфейсы OSPFv3.

в Выполните команду **show ipv6 ospf interface**, чтобы отобразить подробный список для каждого интерфейса с активированным OSPF.

```
R1# show ipv6 ospf interface
Serial0/0/1 is up, line protocol is up Link Local
Address FE80::1, Interface ID 7
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1 Network
Type POINT_TO_POINT, Cost: 64


Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due
in 00:00:05
Graceful restart helper support enabled
Index 1/3/3, flood queue length 0
Next 0x0(0)/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 3.3.3.3
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1 Network
Type POINT_TO_POINT, Cost: 64 Transmit Delay is 1 sec, State
POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due
in 00:00:00
Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/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 1, Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1 Network
Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1 Designated Router
(ID) 1.1.1.1, local address FE80::1 No backup designated router
on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due
in 00:00:03
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/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)
```

k. Для отображения сводки об интерфейсах с активированным OSPFv3, выполните команду **show ipv6 ospf interface brief**.

```
R1# show ipv6 ospf interface brief

       Interface  PID    Area        Intf ID        Cost   State  Nbrs F/C
       Se0/0/1    1      0           7              64     P2P    1/1
       Se0/0/0    1      0           6              64     P2P    1/1

Gi0/0               1      0               3           1      DR     0/0
```

Шаг 6: Проверьте таблицу маршрутизации IPv6.

Выполните команду **show ipv6 route**, чтобы убедиться, что в таблице маршрутизации отображаются все сети.

```
R2# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes:        C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, 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
       e.  2001:DB8:ACAD:A::/64 [110/65]
            via FE80::1, Serial0/0/0
C          2001:DB8:ACAD:B::/64 [0/0]
via GigabitEthernet0/0, directly connected L
2001:DB8:ACAD:B::2/128 [0/0]
via GigabitEthernet0/0, receive
       j.  2001:DB8:ACAD:C::/64 [110/65]
            via FE80::3, Serial0/0/1
C          2001:DB8:ACAD:12::/64 [0/0]
via Serial0/0/0, directly connected
L          2001:DB8:ACAD:12::2/128 [0/0]
via Serial0/0/0, receive
       8.  2001:DB8:ACAD:13::/64 [110/128]
            via FE80::3, Serial0/0/1
via FE80::1, Serial0/0/0
C          2001:DB8:ACAD:23::/64 [0/0]
via Serial0/0/1, directly connected
L          2001:DB8:ACAD:23::2/128 [0/0]
via Serial0/0/1, receive
L          FF00::/8 [0/0]
via Null0, receive
```

Какую команду вы бы применили, чтобы просмотреть только маршруты OSPF в таблице маршрутизации?

_____

_____

_____

_____

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: Настройка пассивных интерфейсов OSPFv3

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 третьей части лабораторной работы вам предстоит использовать команду **passive-interface** для настройки интерфейса в качестве пассивного. Также вы настроите OSPFv3 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.

l. Выполните команду **show ipv6 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 ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up Link Local
Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1 Network
Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1 Designated Router
(ID) 1.1.1.1, local address FE80::1 No backup designated router
on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due
in 00:00:05
Graceful restart helper support enabled Index
1/1/1, flood queue length 0 Next
0x0(0)/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)
```

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

```
R1(config)# ipv6 router ospf 1 R1(config-rtr)#
passive-interface g0/0
```

n. Повторно выполните команду **show ipv6 ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0 стал пассивным.

```
R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up Link Local
Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1 Network
Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1 No
designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 No Hellos
(Passive interface)
Wait time before Designated router selection 00:00:34 Graceful
restart helper support enabled
Index 1/1/1, flood queue length 0 Next
0x0(0)/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)
```

g. Выполните команду **show ipv6 route ospf** на маршрутизаторах R2 и R3, чтобы убедиться, что маршрут к сети 2001:DB8:ACAD:A::/64 по-прежнему доступен.

```
R2# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route B -
BGP, R - RIP, 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:A::/64 [110/65] via
FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65] via
FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128] via
FE80::3, Serial0/0/1
via FE80::1, Serial0/0/0
```

Шаг 2: Настройте маршрутизатор таким образом, чтобы все интерфейсы были пассивными по умолчанию.

i. Выполните команду **passive-interface default** на R2, чтобы все интерфейсы OSPFv3 были пассивными по умолчанию.

```
R2(config)# ipv6 router ospf 1 R2(config-rtr)#
passive-interface default
```

j. Выполните команду **show ipv6 ospf neighbor** на R1. После истечения таймера простоя маршрутизатор R2 больше не будет указываться, как сосед OSPF.

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
3.3.3.3                 0   FULL/  -        00:00:37    6               Serial0/0/1
```

e. Выполните команду **show ipv6 ospf interface S0/0/0** на маршрутизаторе R2, чтобы просмотреть состояние OSPF интерфейса S0/0/0.

```
R2# show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up Link Local
Address FE80::2, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2 Network
Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 No Hellos
(Passive interface)
Graceful restart helper support enabled Index 1/2/2,

flood queue length 0

Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 3
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. Если все OSPFv3-интерфейсы маршрутизатора R2 являются пассивными, то информация о маршрутизации не будет объявляться. В этом случае маршрутизаторы R1 и R3 больше не должны иметь маршрут к сети 2001:DB8:ACAD:B::/64. Это можно проверить с помощью команды **show ipv6 route**.

e. Для того чтобы интерфейс S0/0/1 маршрутизатора R2 мог отправлять и получать обновления маршрутизации OSPFv3, выполните команду **no passive-interface**. После ввода команды появится уведомление о том, что на маршрутизаторе R3 были установлены отношения смежности
с соседним устройством.

```
R2(config)# ipv6 router ospf 1 R2(config-rtr)# no
passive-interface s0/0/1
*Apr 8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from
LOADING to FULL, Loading Done
```

i. Повторно выполните команды **show ipv6 route** и **show ipv6 ospf neighbor** на маршрутизаторах R1

и R3 и найдите маршрут к сети 2001:DB8:ACAD:B::/64.

Какой интерфейс использует R1 для маршрутизации в сеть 2001:DB8:ACAD:B::/64?

_____

_____

_____

_____

Чем равна суммарная метрика стоимости для сети 2001:DB8:ACAD:B::/64 на R1?

_____
_____
_____
_____

Отображается ли маршрутизатор R2 как сосед OSPFv3 на маршрутизаторе R1?

_____
_____
_____
_____

Отображается ли маршрутизатор R2 как сосед OSPFv3 на маршрутизаторе R3?

_____
_____
_____
_____

Что даёт вам эта информация?

_____
_____
_____
_____

d. На маршрутизаторе R2 выполните команду **no passive-interface S0/0/0**, чтобы обновления маршрутизации OSPFv3 объявлялись на этом интерфейсе.

e. Убедитесь, что теперь маршрутизаторы R1 и R2 являются OSPFv3-соседями.

Вопросы на закрепление

h. Если бы идентификатор процесса OSPFv6 для R1 был равен 1, а идентификатор процесса OSPFv3 для R2 был равен 2, был бы возможен обмен информации о маршрутизации между этими двумя маршрутизаторами? Почему?

_____
_____
_____
_____

i. По какой причине отказались от использования команды **network** в OSPFv3?

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.

е. 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.

Лабораторная работа № 30

На тему: Разработка документации

Теоретические сведения

Технические документы – обобщающее название документов (графических и текстовых), в которых зафиксирована техническая мысль.

Техническая документация возникает в процессе проектирования зданий и инженерных сооружений, конструирования машин, проведения научно-технических и экспериментальных исследований, организации промышленного производства, во время осуществления геодезических работ, геологических изысканий. С техническими документами все больше стали иметь дело работники делопроизводства, органов научно-технической информации, ведомственных архивов.

Наиболее широко известна конструкторская, проектная, технологическая, научно-исследовательская документация. Основным видом технических документов является чертеж – изображение предмета на плоскости, выполненное особыми графическими приемами. Чертеж, на котором имеются некоторые текстовые указания, дает возможность представить внешний вид предмета в пространстве, понять его устройство, а также установить, из каких материалов и каким способом предмет следует изготовлять.

Техническая документация служит для решения научно-технических проблем, возведения новых зданий и сооружений, изготовления предметов промышленного производства и т.п. Технические документы сохраняют свое практическое значение и после окончания строительства или снятия изделия с серийного производства и выполнения других работ. Так, технические документы по строительству необходимы для эксплуатации построенных по этим проектам объектов, различного рода перестроек и т.д. Старые технические документы используются при утверждении новых проектов в качестве сравнения и для различного рода справок. Для эксплуатации машин и агрегатов также оказывается необходимым наличие технической документации.

Технические документы широко используются в качестве источников для исследований в области истории науки и техники, установления научного приоритета. Историко-научные и историко-технические выводы являются базой для прогнозирования развития науки и техники, что имеет исключительно большое практическое значение.

2.1. Конструкторская документация

Для изготовления изделия промышленного производства разрабатывается конструкторская документация. Стандарты определяют виды и комплектность конструкторских документов на изделия всех отраслей промышленности.

Устанавливает следующие виды конструкторских документов:

- чертеж – детали, сборочный, общего вида, теоретический, габаритный, монтажный;

- чертеж-схема;

- спецификация, техническое описание, ведомости, пояснительная записка и др.

Текстовые конструкторские документы могут содержать сплошной текст (технические описания, паспорта, расчеты, пояснительные записки, инструкции и т.п.) и текст, разбитый на графы (спецификации, ведомости, таблицы и др.). Рассмотрим каждый из видов конструкторских документов.

На **чертеже детали** содержится ее изображение и другие данные, необходимые для изготовления: размеры, материал, термообработка до заданной прочности (в кг/мм^2), чистота обработки поверхности, класс точности и допуски.

На **сборочном чертеже** – изображение сборочной единицы, которое дает представление о расположении и взаимной связи ее составных частей и обеспечивает возможность осуществления сборки и контроля. На сборочном чертеже иногда помещаются схемы соединения или расположения составных частей изделия, если они не оформлены в виде специальных документов, а также показываются крайние положения перемещающихся частей конструкций.

На **чертеже общего вида** содержится изображение изделия с разрезами и сечениями, текстовая часть и надписи, необходимые для понимания конструктивного устройства этого изделия, а также взаимодействия его основных составных частей и принципа работы, данные о его составе. На чертежах общих видов помещаются технические характеристики.

Теоретический чертеж – документ, определяющий геометрическую форму (обводы) изделия и координаты расположения его составных частей.

Габаритный чертеж – технический документ, содержащий контурное (упрощенное) изображение изделия с указанием габаритных, установочных и присоединительных размеров.

На **монтажном чертеже** также приводится контурное изображение изделия и данные, необходимые для его установки (монтажа).

Чертеж-схема – это упрощенное изображение машин, механизмов, установок и пр., дающее лишь в общих чертах представление об их устройстве и принципах действия. На схемах показаны в виде условных изображений или обозначений части изделий и связи между ними. **Электротехнические схемы** являются основным видом чертежной документации, составляемой при разработке электротехнических изделий, проектов механизации и автоматизации производственных циклов и процессов. Схемы не дают представления о внешнем виде конструкции и размерах предмета.

В **техническом описании** содержатся сведения о наиболее характерных особенностях данного изделия, приводятся его основные показатели, описывается назначение конструкции, устройство и работа его отдельных частей.

Спецификация – документ, определяющий состав изделия, сборочной единицы, комплекса или комплекта.

Пояснительная записка – текстовой технический документ, содержащий описание устройства и принципа действия разрабатываемого изделия, а также обоснование принятых технических и технико-экономических решений.

Ведомости – это списки различных документов, сгруппированных по определенным признакам. Составляются ведомости спецификаций, ссылочных документов, покупных изделий, ведомости технических документов, вошедших в состав технического предложения, эскизного и технического проектов, ведомости держателей подлинников, т.е. перечень предприятий, которые хранят подлинные документы, разработанные для данного изделия, ведомости согласования применения изделий и др.

Конструкторские документы в зависимости от способа их выполнения и характера использования подразделяются на оригиналы, подлинники, дубликаты, копии.

Оригиналом считается документ, выполненный конструктором на бумаге и предназначенный для изготовления по нему подлинника (кальки и др.). **Подлинник** – это технический документ, подписанный ответственными лицами и выполненный на материале, позволяющем многократное снятие с него копий. **Дубликаты** – копии подлинников. Они также выполняются на материале, который дает возможность снимать с него многократные копии, и подписываются ответственными лицами. **Копии** – документы, выполненные способом, обеспечивающим их идентичность с подлинником и предназначенные для непосредственного использования при разработке, в производстве, эксплуатации, ремонте изделия.

2.2. Проектно-сметная документация

Проектно-сметная документация создается при решении вопроса о возведении, реконструкции и ремонте объектов капитального строительства. Проектная документация для строительства характеризует вид строительства, внешний вид и технико-экономические показатели объекта, архитектурные и технологические решения, стоимость работ. Проектная документация для строительства подразделяется на проектную документацию по планировке и застройке городов, поселков, промышленных комплексов, сельских и других населенных пунктов; по жилищно-гражданскому, промышленному и сельскохозяйственному, энергетическому и гидротехническому, транспортному строительству.

В процессе проектирования объектов капитального строительства создаются **индивидуальные, экспериментальные, типовые проекты, проекты-эталоны, проекты-привязки и проекты малых архитектурных форм.**

Основные виды проектной документации – генеральный план, чертежи фасадов, планов, разрезов здания, паспорта проектов, рисунки, пояснительные записки, эскизы, расчеты, схемы, картографические документы, сметы.

На **генеральном плане** дается изображение всего участка строительства, на котором в контурах вида сверху представлено размещение существующих и проектируемых объектов, отражено благоустройство, озеленение, а иногда и топографическое состояние места строительства.

Для строительства какого-либо объекта промышленного или гражданского назначения разрабатываются **общие чертежи** и **чертежи деталей**. К общим относятся чертежи фасадов, планов по этажам, а также поперечные и продольные разрезы здания. **Фасад** – это внешний вид здания с фрагментами его архитектурного оформления. На общих чертежах (планах и разрезах) указывается расположение оборудования, инженерных коммуникаций, взаимная их увязка, маркировка, а также габаритные размеры. Для проведения особых видов строительно-монтажных работ (отопление и вентиляция, водопровод и канализация, электроосвещение, телефон, и др.) выполняются чертежи специального оснащения зданий и сооружений с деталировкой сложных узлов и со спецификациями на оборудование и материалы. На деталировочных чертежах указываются размеры деталей и элементов здания или сооружения, их сопряжения, сечения конструктивных элементов и спецификации.

Для оценки архитектурной стороны проекта создаются в красках **рисунки фасадов** проектируемых зданий. Рисунки, так же как и чертежи, представляют собой изображение предмета на плоскости, но в отличие от чертежа, выполненного в ортогональной проекции, рисунки дают рельефное изображение предметов. Различаются рисунки художественные и технические. **Художественные рисунки** изображают предмет в перспективе, **технические** выполняются в аксонометрии: фронтальной, изометрической и диметрической проекциях.

Эскизами называются чертежи, выполненные от руки, обычно на миллиметровой бумаге. Они являются черновиками, содержание которых потом переносится на ватман с помощью чертежных инструментов.

Паспорт проекта – документ, в котором дается схематическое изображение объекта, краткое описание и сообщаются основные технические показатели.

В **пояснительной записке** содержится справка о проектировании объекта, сведения о его назначении, внешнем виде, внутреннем устройстве; сообщаются наиболее характерные особенности данного объекта, приводятся его основные технические показатели, указывается назначение, описывается внутреннее устройство и работа отдельных частей, особенности конструкции. Кроме того, в пояснительной записке дается объяснение экономических, общественных и других условий и предпосылок создания объекта, аргументация выбора данного варианта.

Расчеты (гидравлические, тепловые, аэродинамические, на сейсмичность и др.) указывают параметры здания или сооружения и его

составных частей в зависимости от установленных расчетных данных. Расчеты производятся на основании использования достижений физико-химических, биологических и других отраслей науки.

В состав проектов многих сооружений (дорог, электростанций, гидротехнических и др.) входят **картографические документы**: топографические, специальные и иные карты, планы городов, населенных пунктов, местности.

К проектной документации всегда прикладываются сметы, которые хотя и не являются техническими документами в собственном смысле слова, но необходимы, так как ни одна стройка невозможна без предварительного установления финансовых затрат. Сметная документация (генеральная, рабочая смета, калькуляция) составляется на основе единичных расценок строительных работ и других нормативных материалов, установленных соответствующими ведомствами.

2.3. Технологическая документация

Технологическая документация – совокупность графических и текстовых технических документов, которые отдельно или в комплексе определяют процесс изготовления изделий промышленного производства или процесс сооружения объектов капитального строительства.

В технологической документации отражены способы изготовления деталей, сборки промышленных изделий, строительства, эксплуатации и ремонта сооружений, способы организации производственного процесса. К этой документации относятся технологические карты, заводские регламенты, чертежи приспособлений, оборудования и инструмента, графики работы цехов и бригад, технические условия, схемы технологического процесса и другие нормативные материалы по составлению технологии.

Основным технологическим документом является **технологическая карта**, на которой дается подробное описание и приводятся расчеты всех производственных операций, необходимых для изготовления изделия.

Технологические карты бывают следующих видов:

1) операционная, на которой зафиксирована отдельная производственная операция (просверлить отверстие, отшлифовать поверхность и т.п.);

2) общая, или маршрутная, на которой показаны в определенной последовательности все операции по изготовлению изделия или детали;

3) цикловая, на которой перечисляются группы операций, выполняемых одним рабочим или производимых, в одном цехе;

4) карта типового технологического процесса, содержащая сведения о средствах технологического оснащения и материальных нормативах для изготовления группы деталей и сборочных единиц.

Общая, или **маршрутная, технологическая карта** составляется на каждое изделие. На основании ее выполняются операционные и другие технологические документы, а также проектируются приспособления,

специальный инструмент, подбирается оборудование, схематично указанные на общей карте. В технологических картах подробно и последовательно записаны все производственные операции по изготовлению каждой детали, сборочной единицы, изделия.

В технологических картах указываются: название операций, схема установки и обработки изделия, применяемые станки, инструмент и приспособления, режим работы (скорость, тепловой режим и т.д.), время обработки (машинное и вспомогательное), специальность и разряд рабочего, стоимость каждой операции.

К технологическим документам относятся также **заводские регламенты**. По ним идет промышленное производство на химических, металлургических, целлюлозно-бумажных, нефтеперерабатывающих и других предприятиях. В заводских регламентах описываются, нормируются и в отдельных случаях схематично изображаются те физико-химические процессы (реакции, компоненты, аппаратура и др.), которые должны протекать для получения изготовляемого продукта.

2.4. Научно-исследовательская документация

Научно-исследовательская документация создается в процессе проведения научных исследований в различных отраслях техники и выполнения теоретических и прикладных научно-технических разработок, отображает теоретическое и практическое решение научно-технических проблем, внедрение их результатов в производство. Основными видами научно-исследовательской документации являются:

1) итоговые и этапные отчеты по научно-исследовательским (НИР), опытно-конструкторским (ОКР), опытно-технологическим (ОТР) и экспериментально-проектным (ЭПР) работам;

2) технические отчеты о НИР, ОКР, ОТР, ЭПР с приложениями; заключения, отзывы и рецензии о НИР, ОКР, ОТР, ЭПР;

3) аннотации на научно-исследовательские работы; паспорта, регламенты на научно-исследовательские работы;

4) монографии, диссертации и отзывы на них;

5) технические задания на НИР;

6) программы научно-исследовательских работ;

7) отчеты, доклады о работе научных экспедиций; отчеты, доклады о научных и технических командировках специалистов;

8) технико-экономические обоснования, обзоры, доклады, записки и др.;

9) первичная документация, образующаяся в процессе проведения НИР, ОКР, ОТР ЭПР (журналы записей экспериментов, результаты анализов, дневники записей показателей приборов);

10) документы на электронных носителях (дисках), фотографии, связанные с процессом исследования.

2.5. Особенности технической документации по изобретательству и стандартизации

Научно обоснованные стандарты способствуют техническому успеху, являются эталоном качества продукции.

Стандарты – это особые технические документы юридического значения. Чертеж стандартного изделия представляет собой изображение предмета с проставленными размерами и другими показателями, которые важны не для изготовления предмета, а для его применения. Конструктор, проектировщик, технолог выбирает для воплощения своей технической идеи соответствующие детали, арматуру, изделия, конструкции, изображенные на этих стандартах. Применение стандартных деталей и изделий при разработке проектов новых машин или объектов, новой технологии является обязательным. Стандартные детали и изделия изготовляются на специализированных заводах по обычным детальным и сборочным чертежам. С целью замены устаревших показателей все действующие стандарты периодически пересматриваются и устанавливаются новые с учетом достижений науки и техники.

Наиболее распространенными видами изобретательской документации являются заявки на технические предложения и изобретения, авторские свидетельства (патенты) на изобретения, удостоверения на рационализаторские предложения, свидетельства (или патенты), выдаваемые на промышленные образцы и др.

Заявка включает в себя заявление, о выдаче соответствующего документа на изобретение, техническое описание, расчет и чертеж общего вида конструкции. В заявлении содержатся: просьба о выдаче авторского свидетельства на изобретение, его краткое название, фамилия, имя, отчество автора (или авторов) предполагаемого изобретения, место работы, занимаемая должность, образование, ученая степень и домашний адрес. В заявлении должно отмечаться, публиковалось ли и рассматривалось ли содержание предполагаемого изобретения и если рассматривалось, то где, когда и кем, каковы результаты; приводятся сведения о наличии разработанной технической документации, об изготовлении опытного образца, его испытаниях и результатах этих испытаний. В конце заявления даются сведения о приложениях, указывается число их экземпляров и на скольких листах выполнен каждый документ. Кроме этого, в заявлении могут сообщаться и другие данные в зависимости от характера изобретения. Информация о технической стороне предполагаемого изобретения содержится в **описании изобретения**, которое представляет собой технико-правовой документ, иллюстрируемый чертежами.

Патент – это документ, удостоверяющий авторство определенного лица или группы лиц на данное изобретение, дающий этим лицам исключительное право изготовлять и продавать изобретенные ими предметы.

2.6. Изготовление и оформление технической документации

Первыми техническими документами, которые возникают в процессе технического творчества, являются наброски, схемы, эскизы и предварительные расчеты. Эти документы обычно являются черновиками для создания чертежа или других технических документов.

Производственные чертежи выполняются на бумаге стандартного формата. Государственными стандартами установлены форматы листов, применяемых для выполнения чертежей во всех отраслях промышленности и строительства (таблица 1).

Таблица 1. − Размеры форматов.

Обозначение формата	Размер формата
А0	841×1189
А1	594×841
А2	420×594
А3	297×420
А4	210×297

Допускается при необходимости применять формат А5 (148х210), а также дополнительные форматы, образуемые увеличением коротких сторон основных форматов на величину, кратную их размерам (таблица 2). Обозначение производного формата состоит из обозначения основного формата и его кратности, согласно таблице 2, например: А0×2 (1189×1682).

Чертежи выполняются на ватмане, иногда используется пергаментная калька, на которой можно работать карандашом, а также эмульсированная калька. Калька, покрытая эмульсионным слоем, приобретает ценные свойства: обычный карандаш дает на ней четкие линии.

Таблица 2. – Дополнительные форматы

Кратность	А0	А1	А2	А3	А4
2	1189×1682				
3	1189×2523	841×1782	594×1261	420×891	297×630
4		841×2378	594×1682	420×1189	297×842
5			594×2102	420×1486	297×1051
6				420×1783	297×1261
7				420×2080	297×1471
8					297×1682
9					297×1892

На каждом листе чертежа вычерчивается рамка, отстоящая от краев бумаги с трех сторон на 5 мм, а с левой стороны, если чертежи подлежат брошюровке, – на 20 мм. Чертежи большого формата складываются до

размера формата А4. При этом листы складывают изображением наружу так, чтобы основная надпись (угловой штамп) оказывалась на верхней лицевой стороне сложенного листа в его правом нижнем углу.

Все надписи на чертежах сосредоточены в одном месте в специально разграфленных трафаретках или угловых штампах, расположенных в правом нижнем углу листа. В угловом штампе указываются все основные сведения о чертеже, что позволяет найти нужный документ среди массы других, установить технические данные, необходимые для изготовления изображенного на чертеже изделия (материал, масштаб, режим термообработки и др.). С помощью углового штампа можно определить разновидность чертежа (общий вид, чертеж сборочной единицы, детальный чертеж), узнать, к какому изделию относится этот чертеж, какие чертежи в свою очередь с ним связаны. Из содержания углового штампа выясняют, кто является автором данной конструкций, дату утверждения чертежа, некоторые элементы технической характеристики изделия. В угловом штампе помещаются также подписи лиц, ответственных за правильность разработки и оформления технических документов, дата выпуска.

Основная надпись сборочных, детальных, габаритных, монтажных и других чертежей имеет одни и те же графы и постоянный порядок их расположения.

Стандарт устанавливает также дополнительные графы к основной надписи, которые должны быть на всех чертежах, схемах и текстовых документах. Дополнительные графы содержат сведения об инвентарных номерах подлинника (или дубликата) данного документа, полученных в архиве конструкторской организации, об обозначении документа, взамен или на основании которого выпущен данный документ, и подписи лиц, принявших подлинники в архив. Дополнительные графы располагаются вдоль левого поля чертежа.

Выше основной надписи или на отдельном листе в виде приложения к чертежу, если это чертеж общего вида или сборочный, вычерчивается спецификация, в которой определяется состав сборочных единиц, комплекса и комплекта. В спецификации указываются: формат чертежа, зона, порядковый номер позиции сборочной единицы и деталей, производственный номер сборочной единицы и деталей, их наименования, количество сборочных единиц и деталей, необходимых для изготовления одного экземпляра изделия, примечание, в котором указываются замены сборочных единиц и деталей, наличие вариантов, заимствования из других проектов, аннулирование чертежей и пр.

Имеются некоторые особенности в содержании и оформлении основных надписей и чертежей, применяемых в области строительства, в электротехнике и радиопромышленности, дорожном строительстве, горном деле.

Основные сведения, которые обычно указываются в угловых штампах строительных чертежей: наименования проектной организации и вышестоящего органа, название комплекса, объекта, чертежа,

производственный номер комплекса, стадия проектирования, часть проекта, номер листа, формат чертежа.

Текстовые технические документы могут быть выполнены машинописным, рукописным и типографским способами. Схема получения текстового технического документа выглядит следующим образом: составление проекта документа автором, перепечатка его на пишущей машине или компьютере, согласование и корректирование, подписание руководящими лицами.

Для размещения утверждающих и согласовывающих подписей к текстовым документам составляется титульный лист.

На нем указываются:

- наименование министерства или ведомства, в ведении которого находится организация, разработавшая данный документ;
- название самой организации;
- наименование изделия или его составной части;
- должности и подписи исполнителей и ответственных лиц;
- дата разработки документа.

В научно-исследовательских, конструкторско-технологических, проектных организациях, научно-исследовательских лабораториях вузов, промышленных предприятий составляются технические документы научно-исследовательского характера. Основным из них, в котором излагаются исчерпывающие сведения о выполненных экспериментах и этапах научного исследования, является **отчет о теме**.

Структуру отчета о НИР:

- титульный лист,
- список исполнителей,
- реферат,
- содержание (оглавление),
- перечень сокращений,
- символов и специальных терминов с их определениями,
- условных обозначений;
- введение,
- основная часть,
- заключение,
- список использованных источников и литературы,
- приложения.

На титульном листе отчета о НИР указывается:

1) официальное название организации-исполнителя, Министерства (ведомства), которому подчиняется организация;

2) номер государственной регистрации, инвентарный номер отчета о НИР; надписи о согласовании и утверждении отчета, в которых, кроме должностей, фамилий и инициалов, указываются ученые степени и звания лиц, утвердивших и подписавших документ;

3) наименование темы, отчета (если последнее не совпадает с наименованием темы) и – в скобках – тип отчета (промежуточный, заключительный, этапный отчет и т.п.);

4) номер (шифр) темы, присвоенный ей в организации (ведомстве);

5) должности, ученые степени и звания, фамилии и инициалы руководителей подразделений организации, руководителей НИР и ответственных исполнителей;

6) место и год выпуска отчета.

3. Контрольные вопросы

1. Раскройте понятии и виды конструкторской документации
2. Раскройте понятии и виды проектно-сметной документации
3. Раскройте понятии и виды технологической документации
4. Раскройте понятии и виды научно-исследовательской документации
5. Особенности технической документации по изобретательству и стандартизации
6. Раскройте особенности изготовления и оформления технической документации

Печатные издания

1. Н.В. Максимов, И.И. Попов. Компьютерные сети [Электронный ресурс]: учеб. Пособие -М.: ФОРУМ: ИНФРА-М 2017.

2. Новожилов, Е.О. Компьютерные сети.–М.: ОИЦ «Академия, 2013.

3. Кузин, А.В. Компьютерные сети: Учебное пособие / А.В. Кузин. - 3-е изд., перераб. и доп. - М.: Форум: ИНФРА-М, 2014. - 192 с.

4. Виснадул, Б.Д. Основы компьютерных сетей: Учебное пособие / Б.Д. Виснадул, С.А. Лупин, С.В. Сидоров.; Под ред. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ Инфра-М, 2015. - 272 с.

Электронные издания (электронные ресурсы)

1. Российская национальная библиотека [Электронный ресурс]. — Режим доступа: http://www.nlr.ru/ , свободный.

2. Полная энциклопедия Windows [Электронный ресурс] http://windata.ru/windows-xp/localnaya-set-xp/nastrojka-lokalnoj-seti/.

Дополнительные источники

1. Ватаманюк А. Создание, обслуживание и администрирование сетей на 100%. С-Пб.: Питер, 2014 г.

2. Макаренко С.И. Журнал «Системы управления, связи и безопасности». Выпуск №2/2015 «Время сходимости протоколов маршрутизации при отказах в сети»