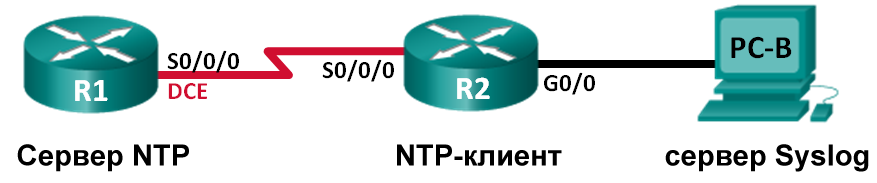
10.2.3.6 Лабораторная работа. Настройка Syslog и NTP

1. Топология



1. Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1 | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | — |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | — |
|  | G0/0 | 172.16.2.1 | 255.255.255.0 | — |
| PC-B | NIC | 172.16.2.3 | 255.255.255.0 | 172.16.2.1 |

1. Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка NTP

Часть 3. Настройка Syslog

1. Общие сведения/сценарий

Сообщения Syslog, создаваемые сетевыми устройствами, могут собираться и архивироваться на сервере Syslog. Эту информацию можно использовать для наблюдения, отладки и поиска и устранения неполадок. Администратор может настраивать место сохранения и отображения сообщений. Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP.

В этой лабораторной работе необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента Syslog и NTP. Серверное приложение Syslog (например, Tftp32d или другая аналогичная программа) будет работать на компьютере PC-B. Кроме того, вы будете контролировать уровень важности сообщений журнала, которые собираются и архивируются на сервере Syslog.

**Примечание**. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Допускается использование маршрутизаторов других моделей, а также других версий операционной системы 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 все настройки маршрутизаторов удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

1. Необходимые ресурсы

* 2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
* 1 компьютер (с операционной системой Windows 7, Vista или XP, с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32).
* Консольные кабели для настройки устройств Cisco IOS через консольные порты.
* Кабели Ethernet и последовательные кабели согласно топологии.

1. Настройка основных параметров устройств

В части 1 необходимо настроить топологию сети и базовые параметры, например IP-адреса интерфейса, маршрутизацию, доступ к устройствам и пароли.

* 1. Создайте сеть согласно топологии.
  2. Выполните запуск и перезагрузку маршрутизаторов.
  3. Произведите базовую настройку маршрутизаторов.
     1. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.
     2. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

no ip domain-lookup

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

* + 1. Настройте имена хостов в соответствии с топологией.
    2. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.
    3. Установите тактовую частоту **128000** для последовательного интерфейса DCE.
  1. Настройте маршрутизацию.

Включите RIPv2 на маршрутизаторах. Добавьте все сети в процесс RIPv2.

* 1. Настройте ПК B.

Настройте IP-адрес и шлюз по умолчанию для ПК B согласно таблице адресации.

* 1. Проверьте наличие сквозного соединения.

Убедитесь, что все устройства могут отправлять эхо-запросы на каждое другое устройство в сети. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

* 1. Сохранение текущей конфигурации в качестве начальной.

1. Настройка NTP

В части 2 необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента NTP маршрутизатора R1. Необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

* 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** |  |

* 1. Установите время.

С помощью команды **clock set** установите время на маршрутизаторе R1. Ниже приводится пример настройки даты и времени.

R1# **clock set 9:39:00 05 july 2013**

R1#

\*Jul 5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54 UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by console.

**Примечание**. Время можно также настроить с помощью команды **clock timezone** в режиме глобальной конфигурации. Для получения дополнительной информации о команде **clock timezone** посетите веб-сайт [www.cisco.com](http://www.cisco.com/web/RU/index.html) и определите часовой пояс для вашего региона.

* 1. 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**

* 1. Настройте клиент NTP.
     1. Введите команду **show clock** на маршрутизаторе R2. Запишите текущее время, отображаемое на маршрутизаторе R2, в следующей таблице.

|  |  |
| --- | --- |
| **Дата** |  |
| **Время** |  |
| **Часовой пояс** |  |

* + 1. 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**

* 1. Проверьте настройку NTP.
     1. 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

* + 1. 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**

9:43:37.122 UTC Fri Jul 5 2013

1. 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.

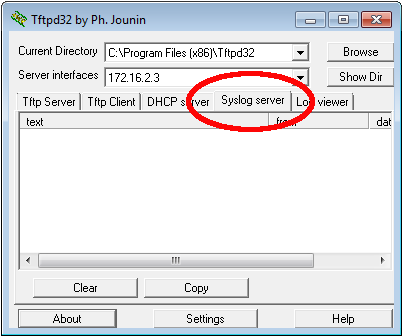
* 1. (Дополнительно) Установите сервер Syslog.

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/>

* 1. Запустите сервер Syslog на компьютере ПК B.

После запуска приложения Tftpd32 перейдите на вкладку **Syslog server**.



* 1. Убедитесь, что на маршрутизаторе R2 включена служба меток времени.

С помощью команды **show run** проверьте, что служба меток времени включена для журналирования на маршрутизаторе R2.

R2# **show run | include timestamp**

service timestamps debug datetime msec

service timestamps log datetime msec

Если служба меток времени не включена, используйте следующую команду, чтобы включить ее.

R2(config)# **service timestamps log datetime msec**

* 1. Настройте R2 для сохранения сообщений журнала на сервере Syslog.

Настройте маршрутизатор R2 для отправки syslog-сообщений на сервер Syslog (компьютер PC-B). IP-адрес сервера Syslog на PC-B: 172.16.2.3.

R2(config)# **logging host 172.16.2.3**

* 1. 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? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Настройте и проверьте результат настройки уровней важности для журналирования на маршрутизаторе R2.
     1. С помощью команды **logging trap ?** определите доступность различных уровней сообщений. 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 Систему нельзя использовать (серьезность=0)

errors Состояние ошибки (серьезность=3)

informational Информационные сообщения (серьезность=6)

notifications Нормальное, но значащее состояние (серьезность=5)

warnings Состояние предупреждения (серьезность=4)

<cr>

Если введена команда **logging trap warnings**, сообщения с какими уровнями важности будут регистрироваться?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Укажите уровень важности для журналирования равный 4.

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

или

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

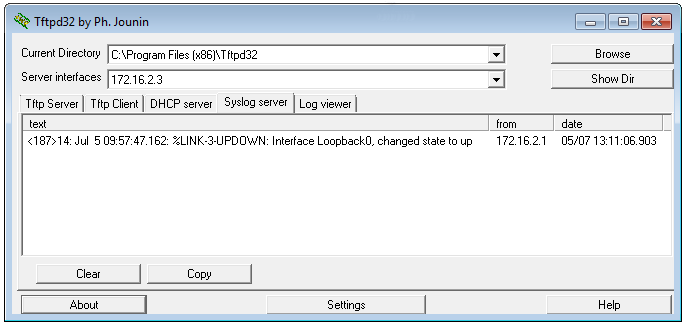
* + 1. Создайте интерфейс Loopback0 на маршрутизаторе R2 и просмотрите сообщения журнала как в окне терминала, так и в окне сервера Syslog на ПК B.

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



* + 1. 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 серьезности 4? Если какие-либо сообщения журнала отображаются, объясните, какие сообщения отображаются и почему.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Укажите уровень важности для журналирования равный 6.

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

или

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

* + 1. Удалите все записи в журнале Syslog на компьютере PC-B. Для этого щелкните **Clear** (Очистить) в диалоговом окне Tftpd32.
    2. 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

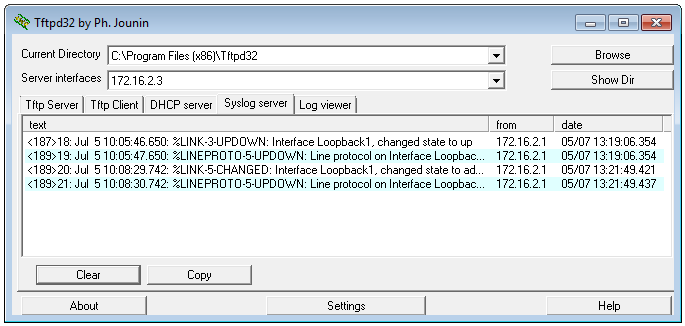
* + 1. Удалите интерфейс Loopback 1 с маршрутизатора R2.

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



* + 1. Проанализируйте выходные данные сервера Syslog. Сравните эти результаты с результатами на уровне важности 4. Каковы ваши наблюдения?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Вопросы для повторения

Какая проблема возникает при настройке слишком высокого (самый маленький номер) или слишком низкого (самый большой номер) уровня важности для Syslog?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 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. | | | | |