# Лабораторная работа. 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
РС-В	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 и устранения неполадок. Администратор может настраивать место сохранения и отображения сообщений. Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP.

В этой лабораторной работе необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента Syslog и NTP. Приложение сервера Syslog, например Tftp32d или другая аналогичная программа, будет выполняться на ПК В. Кроме того, необходимо настроить уровень важности сообщений журнала, которые будут собираются и архивироваться на сервере Syslog.

Примечание. В практических лабораторных работах ССNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

**Примечание**. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

## Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) МЗ (образ universal) или аналогичная модель);
- 1 компьютер (c OC Windows 7, Vista или XP или с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

## Часть 1: Базовая настройка устройств

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

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

## Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

## Шаг 3: Произведите базовую настройку маршрутизаторов.

- а. Отключите поиск DNS.
- b. Настройте имя устройства.
- с. 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 В.

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

## Шаг 6: Проверьте связь между конечными устройствами.

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

## Шаг 7: Сохраните текущую конфигурацию в загрузочную.

## Часть 2: Настройка NTP

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

## Шаг 1: Выведите на экран текущее время.

Введите команду show clock для отображения текущего времени на R1.

#### R1# show clock

```
*12:30:06.147 UTC Tue May 14 2013
```

Запишите отображаемые сведения о текущем времени в следующей таблице.

Дата	
Время	
Часовой пояс	

## Шаг 2: Установите время.

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

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul 5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54
UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by
console.
```

**Примечание**. Время можно также настроить с помощью команды **clock timezone** в режиме глобальной конфигурации. Для получения дополнительной информации о команде **clock timezone** посетите веб-сайт <u>www.cisco.com</u> 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	

В данном документе содержится общедоступная информация корпорации Cisco.

b. Настройте R2 в качестве клиента NTP. Используйте команду ntp server, чтобы указать на IP-адрес или имя компьютера сервера NTP. Команда ntp update-calendar периодически обновляет календарь на основе времени NTP.

R2(config)# **ntp server 10.1.1.1** R2(config)# **ntp update-calendar** 

## Шаг 5: Проверьте настройку NTP.

a. Используйте команду **show ntp associations**, чтобы проверить, что маршрутизатор R2 связан через NTP с маршрутизатором R1.

```
R2# show ntp associations
```

address ref clock st when poll reach delay offset disp \*~10.1.1.1 127.127.1.1 5 11 64 177 11.312 -0.018 4.298 \* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

b. Введите команду show clock на маршрутизаторах R1 и R2 и сравните метку времени.

**Примечание**. Синхронизация метки времени на маршрутизаторе R2 с меткой времени на маршрутизаторе R1 может занять несколько минут.

```
R1# show clock
09:43:32.799 UTC Fri Jul 5 2013
R2# show clock
09:43:37.122 UTC Fri Jul 5 2013
```

## Часть 3: Настройте Syslog

Сообщения Syslog от сетевых устройств могут собираться и архивироваться на сервере Syslog. В этой лабораторной работе в качестве программного обеспечения сервера Syslog используется Tftpd32. Администратор может настраивать типы сообщений, которые можно отправлять на сервер Syslog.

## Шаг 1: (Дополнительно) Установите сервер Syslog.

Если сервер Syslog еще не установлен на компьютере, загрузите и установите последнюю версию сервера Syslog, например Tftpd32. Последнюю версию Tftpd32 можно найти по следующей ссылке:

http://tftpd32.jounin.net/

## Шаг 2: Запустите сервер Syslog на компьютере ПК В.

После запуска приложения Tftpd32 перейдите на вкладку Syslog server.

🏘 Tftpd32 by Ph. Jounin 📃	, • 💌
Current Directory C:\Program Files (x86)\Tftpd32	Browse Show Dir
Tftp Server Tftp Client DHCP server Syslog server Lo	viewer
text from	dat
•	•
Clear Copy	
About Settings	Help

#### Шаг 3: Убедитесь, что на маршрутизаторе R2 включена служба меток времени.

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

R2# show run | include timestamp service timestamps debug datetime msec service timestamps log datetime msec

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

R2(config)# service timestamps log datetime msec

#### Шаг 4: Настройте R2 для сохранения сообщений журнала на сервере Syslog.

Настройте R2 для отправки сообщений Syslog на сервер Syslog — ПК В. IP-адрес сервера Syslog ПК В — 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.

а. 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
               Immediate action needed
 alerts
                                              (severity=1)
 critical
              Critical conditions
                                              (severity=2)
             Debugging messages
 debugging
                                              (severity=7)
 emergencies System is unusable
                                              (severity=0)
             Error conditions
 errors
                                               (severity=3)
 informational Informational messages
                                               (severity=6)
 notifications Normal but significant conditions (severity=5)
             Warning conditions
 warnings
                                              (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

с. Создайте интерфейс Loopback0 на маршрутизаторе R2 и просмотрите сообщения журнала как в окне терминала, так и в окне сервера Syslog на ПК В.

```
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
```

🏘 Tftpd32 by Ph. Jounin		- • ×
Current Directory C:\Program Files (x86)\Tftpd32	•	Browse
Server interfaces 172.16.2.3	•	Show Dir
Tftp Server   Tftp Client   DHCP server   Syslog server   Log viewer		
text	from	date
<187>14: Jul 5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up	172.16.2.1	05/07 13:11:06.903
Clear Copy		
About Settings		Help

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.

е. Укажите уровень важности для журналирования равный 6.

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

или

<sup>©</sup> Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены. В данном документе содержится общедоступная информация корпорации Cisco.

R2(config) # logging trap 6

- f. Удалите записи Syslog на ПК В. 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

🏘 Tftpd32 by Ph. Jounin		
Current Directory C:\Program Files (x86)\Tftpd32	•	Browse
Server interfaces 172.16.2.3	•	Show Dir
Tftp Server Tftp Client DHCP server Syslog server Log viewer		
text	from	date
<187>18: Jul 5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up <189>19: Jul 5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopbac <189>20: Jul 5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to ad <189>21: Jul 5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopbac	172.16.2.1 172.16.2.1 172.16.2.1 172.16.2.1 172.16.2.1	05/07 13:19:06.354 05/07 13:19:06.354 05/07 13:21:49.421 05/07 13:21:49.437
Clear Copy		
About Settings		Help

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 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)

## Сводная таблица интерфейсов маршрутизаторов

**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.