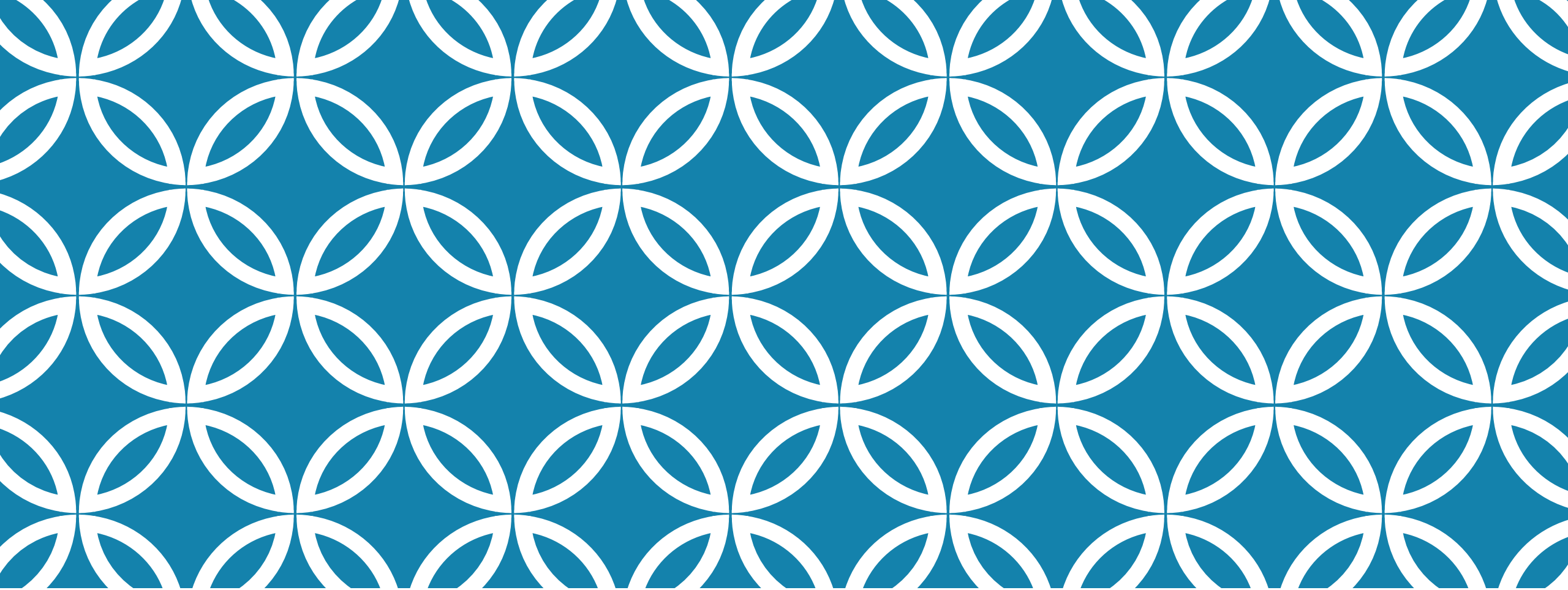


МОДУЛЬ 10. УПРАВЛЕНИЕ СЕТЬЮ

КАФЕДРА
ТЕЛЕКОММУНИКАЦИЙ

10.1 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА CDP

10.1.1 ОБЩИЕ СВЕДЕНИЯ О ПРОТОКОЛЕ CDP

Протокол Cisco Discovery Protocol (CDP) — это проприетарный протокол компании Cisco уровня 2, который служит для сбора информации об устройствах Cisco, использующих один и тот же канал передачи данных. CDP не зависит от среды передачи данных и других протоколов; он включен на всех устройствах Cisco, таких как маршрутизаторы, коммутаторы и серверы доступа.

Устройство периодически отправляет объявления CDP на подключенные устройства. Посредством объявлений осуществляется обмен информацией о типах обнаруженных устройств, их именах, количестве и типах интерфейсов.

10.1 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА CDP

10.1.2 НАСТРОЙКА И ПРОВЕРКА ПРОТОКОЛА CDP

На устройствах Cisco протокол CDP включен по умолчанию. Чтобы проверить состояние CDP и отобразить сведения о нем, введите команду **show cdp**.

Чтобы отключить CDP для определенного интерфейса, например используемого для подключения к интернет-провайдеру, введите команду **no cdp enable** в режиме настройки интерфейса. Протокол CDP по-прежнему включен на устройстве, однако объявления CDP больше не передаются через этот интерфейс. Чтобы снова включить CDP для определенного интерфейса, введите команду **cdp enable**.

Чтобы включить CDP сразу для всех поддерживаемых интерфейсов устройства, введите команду **cdp run** в режиме глобальной конфигурации. Чтобы отключить CDP сразу для всех интерфейсов устройства, введите команду **no cdp run** в режиме глобальной конфигурации.

Команда **show cdp interface** отображает интерфейсы устройства, на которых включен протокол CDP. Кроме того, выводится состояние каждого интерфейса.

10.1 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА CDP

10.1.3 ПОИСК УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА CDP

Если в сети включен протокол CDP, структуру сети можно определить с помощью команды **show cdp neighbors**.

Выходные данные показывают, что к интерфейсу G0/0/1 на R1 подключено другое устройство Cisco S1. Кроме того, S1 подключается через интерфейс F0/5.

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
S1 Gig 0/0/1 179 S I WS-C3560- Fas 0/5
```

10.1 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА CDP

10.1.3 ПОИСК УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА CDP

Администратор сети использует команду **show cdp neighbors detail** для обнаружения IP-адреса S1. Как показано в выходных данных, адрес S1 — 192.168.1.2.

```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C3560-24TS, Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

(output omitted)
```

10.2 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА LLDP

10.2.1 ОБЩИЕ СВЕДЕНИЯ О ПРОТОКОЛЕ LLDP

Протокол LLDP — это не зависящий от производителя протокол для обнаружения соседей, подобный CDP. LLDP работает с сетевыми устройствами, такими как маршрутизаторы, коммутаторы и точки доступа к беспроводной сети LAN. Этот протокол объявляет себя и свои возможности другим устройствам и получает данные от физически подключенных устройств уровня 2.

10.2 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА LLDP

10.2.2 НАСТРОЙКА И ПРОВЕРКА ПРОТОКОЛА LLDP

На устройствах Cisco протокол LLDP может быть не включен по умолчанию. Чтобы включить LLDP для всех интерфейсов сетевого устройства Cisco, введите команду **lldp run** в режиме глобальной конфигурации. Чтобы отключить протокол LLDP, введите команду **no lldp run** в режиме глобальной конфигурации.

Как и протокол CDP, протокол LLDP можно включить и отключить на конкретных интерфейсах. Однако передачу и прием пакетов LLDP необходимо настраивать отдельно, как показано на рисунке.

Чтобы убедиться в том, что протокол LLDP был включен на устройстве, введите команду **show lldp** в привилегированном режиме EXEC.

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialisation delay is 2 seconds
```

10.2 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА LLDP

10.2.3 ПОИСК УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА LLDP

Если включен протокол LLDP, можно найти соседей определенного устройства с помощью команды **show lldp neighbors**.

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time Capability Port ID
R1 Fa0/5 117 R Gi0/0/1
S2 Fa0/1 112 B Fa0/1
Total entries displayed: 2
```

10.2 ОБНАРУЖЕНИЕ УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА LLDP

10.2.3 ПОИСК УСТРОЙСТВ С ПОМОЩЬЮ ПРОТОКОЛА LLDP

Если нужна более подробная информация о соседних устройствах, можно воспользоваться командой **show lldp neighbors detail**, которая предоставляет такие сведения, как версия IOS, IP-адрес и функции соседних устройств.

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: 848a.8d44.49b0
Port id: Gi0/0/1
Port Description: GigabitEthernet0/0/1
System Name: R1
System Description: Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_.....,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

Time remaining: 111 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
(output omitted)
```

10.3 NTP
10.3.1 СЛУЖБЫ ВРЕМЕНИ И КАЛЕНДАРЯ

Основным источником информации о времени в системе являются программные часы маршрутизатора или коммутатора, Это основной источник времени для системы. Необходимо синхронизировать время на всех устройствах в сети. Если время на устройствах не синхронизировано, определить порядок событий и их причину невозможно.

Как правило, параметры даты и времени на маршрутизаторе или коммутаторе можно задать одним из двух способов. Можно вручную настроить дату и время, как показано в примере, или настроить протокол сетевого времени (NTP).

```
R1# clock set 20:36:00 nov 15 2019
R1#
*Nov 15 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been
updated from 21:32:31 UTC Fri Nov 15 2019 to 20:36:00 UTC Fri Nov 15
2019, configured from console by console.
```

10.3 NTP
10.3.1 СЛУЖБЫ ВРЕМЕНИ И КАЛЕНДАРЯ

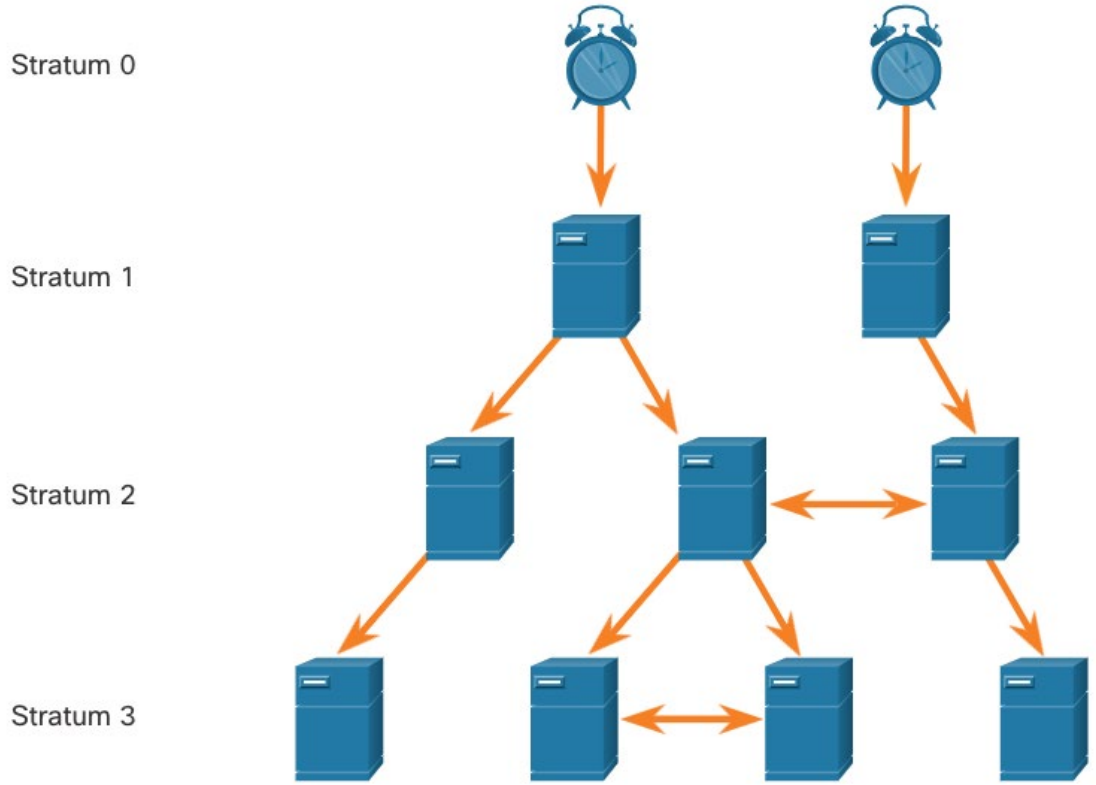
По мере роста сети становится все труднее вручную обеспечивать синхронизацию времени на всех устройствах инфраструктуры.

Более эффективным решением является настройка в сети протокола NTP. Этот протокол позволяет маршрутизаторам в сети синхронизировать свои настройки времени с NTP-сервером, что обеспечивает более согласованные настройки времени. NTP можно настроить для синхронизации с частным генератором тактовых импульсов или общедоступным сервером NTP в Интернете. Протокол NTP использует порт UDP 123 и задокументирован в RFC 1305.

10.3 NTP
10.3.2 ПРИНЦИПЫ РАБОТЫ ПРОТОКОЛА NTP

В сетях NTP используется иерархическая система источников времени. Каждый уровень этой иерархической системы называется часовым слоем (stratum). Уровень часового слоя определяется как количество переходов от доверенного источника. Для распределения синхронизированной информации о времени по сети используется протокол NTP.

Максимальное количество переходов равно 15. Часовой слой 16 имеет самый низкий уровень и указывает на то, что устройство не синхронизировано.



10.3 NTP
10.3.2 ПРИНЦИПЫ РАБОТЫ ПРОТОКОЛА NTP

Устройства слоя 0: Эти доверенные источники времени, также называемые устройствами часового слоя 0, являются высокоточными устройствами хранения времени, которые считаются точными и работают практически без задержек.

Устройства слоя 1 подключены напрямую к доверенным источникам времени. Они выступают в роли основного стандарта сетевого времени.

Слой 2 и ниже. Серверы слоя 2 подключены к устройствам слоя 1 через сеть. Устройства часового слоя 2, например клиенты NTP, синхронизируют свое время с помощью пакетов NTP, которые они получают от серверов часового слоя 1. Эти устройства могут также выступать в роли серверов для устройств часового слоя 3.

Серверы времени, находящиеся в одном часовом слое, могут работать как равноправные серверы времени на одном уровне часового слоя для обеспечения резервирования или проверки правильности времени.

10.3 NTP
10.3.3 НАСТРОЙКА И ПРОВЕРКА ПРОТОКОЛА NTP

Перед настройкой протокола NTP в сети введите команду **show clock**, которая отображает текущее время программных часов. При выборе параметра **detail** обратите внимание, что источником времени является пользовательская конфигурация. Это означает, что время было настроено вручную с помощью команды **clock**.

Используйте команду **ntp server** *ip-address* в режиме глобальной конфигурации, чтобы указать адрес 209.165.200.225 в качестве сервера NTP для маршрутизатора R1. Чтобы убедиться, что в качестве источника времени выбран NTP, выполните команду **show clock detail**. Обратите внимание, что теперь источником времени является NTP.

```
R1# show clock detail
20:55:10.207 UTC Fri Nov 15 2019
Time source is user configuration
R1# config t
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Nov 15 2019
Time source is NTP
```

10.3 NTP
10.3.3 НАСТРОЙКА И ПРОВЕРКА ПРОТОКОЛА NTP

Команды **show ntp associations** и **show ntp status** позволяют проверить, что маршрутизатор R1 синхронизирован с сервером NTP по адресу 209.165.200.225. Обратите внимание: маршрутизатор R1 синхронизирован с сервером NTP часового слоя 1 по адресу 209.165.200.225, который синхронизирован с часами GPS. Команда **show ntp status** показывает, что теперь маршрутизатор R1 является устройством часового слоя 2, которое синхронизировано с сервером NTP по адресу 209.165.220.225.

```
R1# show ntp associations

address ref clock st when poll each delay offset disp
*~209.165.200.225 .GPS.       1 61 64 377 0.481 7.480 4.261
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
(output omitted)
```

10.3 NTP
10.3.3 НАСТРОЙКА И ПРОВЕРКА ПРОТОКОЛА NTP

Часы S1 настроены на синхронизацию с R1 с помощью команды **ntp server**, а конфигурация проверяется с помощью команды **show ntp associations**.

Команда **show ntp associations** позволяет убедиться, что часы на S1 теперь синхронизированы с R1 с адресом 192.168.1.1 по протоколу NTP. Коммутатор S1 теперь является устройством часового слоя 3, которое может предоставлять службу NTP для остальных устройств в сети, например оконечных устройств.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
address ref clock st when poll reach delay offset disp
*~192.168.1.1 209.165.200.225 2 12 64 377 1.066 13.616 3.840
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
(output omitted)

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
(output omitted
```

10.4 ПРОТКОЛ SNMP
10.4.1 ВВЕДЕНИЕ В SNMP

Протокол SNMP позволяет сетевым администраторам осуществлять управление и мониторинг устройств в сети IP. С его помощью сетевые администраторы могут осуществлять мониторинг производительности сети, находить и устранять проблемы, а также планировать рост сети.

SNMP — это протокол уровня приложений, предоставляющий формат сообщения для обмена данными между диспетчерами и агентами. Система SNMP состоит из следующих трех элементов:

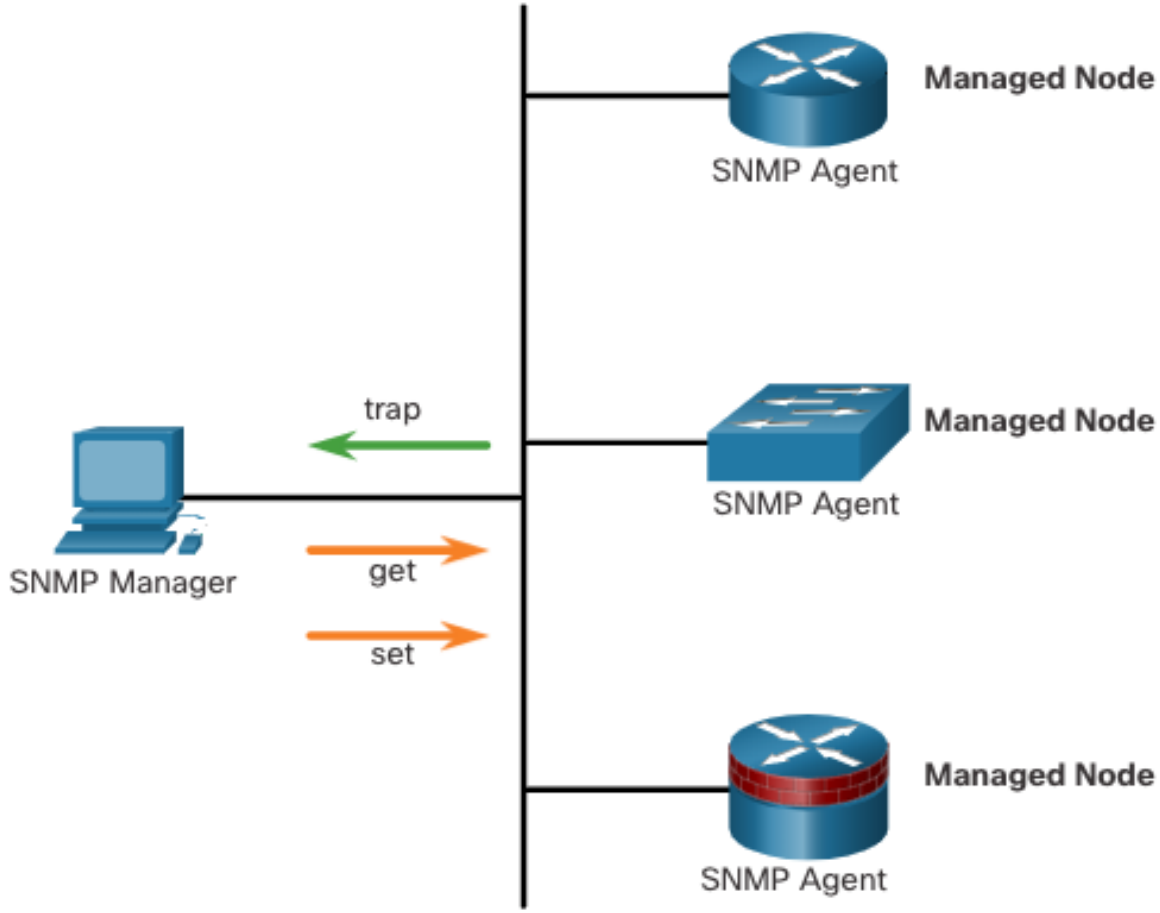
- диспетчер SNMP;
- агенты SNMP (управляемый узел);
- Management Information Base (MIB).

SNMP определяет способ обмена информацией об управлении между приложениями управления сетями и агентами управления. Диспетчер SNMP опрашивает агенты и запрашивает в MIB информацию об агентах SNMP через порт UDP 161. Агенты SNMP отправляют все ловушки SNMP в диспетчер SNMP на порт UDP 162.

10.4 ПРОТКОЛ SNMP
10.4.1 ВВЕДЕНИЕ В SNMP

Диспетчер SNMP является частью системы управления сетями (network management system — NMS). Диспетчер SNMP может собирать данные от агента SNMP с помощью запроса get и изменять настройки на агенте с помощью запроса set. Агенты SNMP могут пересылать информацию непосредственно в диспетчер сети, используя ловушки (пакеты trap).

Агент SNMP и база данных MIB размещены на клиентских устройствах SNMP. В базах данных MIB хранятся данные об устройствах и их функционировании. Они должны быть доступны для прошедших аутентификацию удаленных пользователей. Агент SNMP отвечает за предоставление доступа к локальной базе данных MIB.



10.4 ПРОТКОЛ SNMP
10.4.2 ФУНКЦИОНИРОВАНИЕ ПРОТОКОЛА SNMP

Агенты SNMP, размещенные на управляемых устройствах, собирают и сохраняют информацию об устройстве и его работе. Затем диспетчер SNMP использует агент SNMP для доступа к сведениям, хранящимся в базе MIB.

Существует два основных запроса диспетчера SNMP — get и set. В дополнение к конфигурации набор запросов может вызвать действие, например перезапуск маршрутизатора.

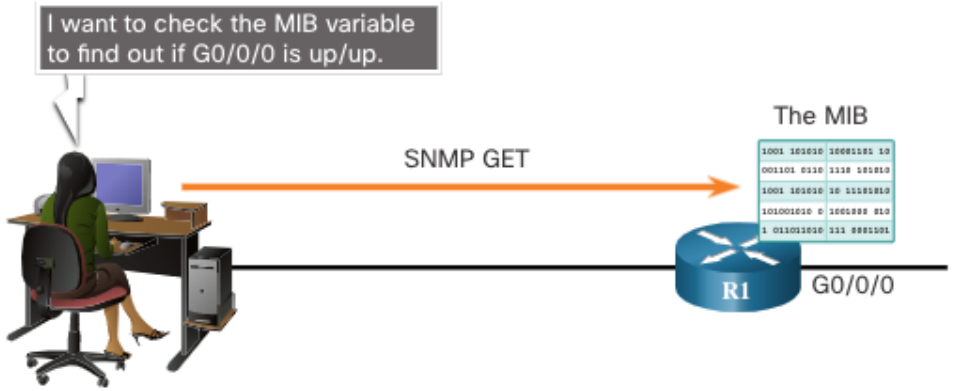
Операция	Описание
get-request	Получает значение из определенной переменной.
get-next-request	Получает значение из переменной в таблице; диспетчер SNMP не обязательно должен знать точное имя переменной. Чтобы найти необходимую переменную в таблице, выполняется последовательный поиск.
get-bulk-request	Получает большие блоки данных, например несколько строк в таблице, что обычно требует передачи многочисленных небольших блоков данных (работает только с SNMPv2 или более поздней версией).
get-response	Отвечает на запросы **get-request, get-next-request** и **set-request**, отправляемые системой NMS.
set-request	Сохраняет значение в определенной переменной.

10.4 ПРОТКОЛ SNMP
10.4.2 ФУНКЦИОНИРОВАНИЕ ПРОТОКОЛА SNMP

Агент SNMP отвечает на запросы диспетчера SNMP следующим образом.

Получение переменной MIB. Агент SNMP выполняет эту функцию в ответ на запрос GetRequest-PDU от диспетчера сети. Агент получает значение запрошенной переменной MIB и передает это значение в диспетчер сети.

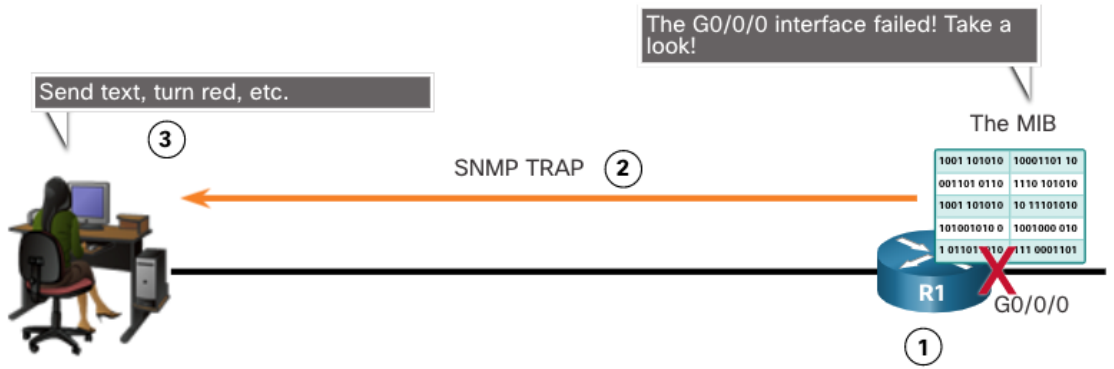
Изменение переменной MIB. Агент SNMP выполняет эту функцию в ответ на запрос SetRequest-PDU от диспетчера сети. Агент SNMP изменяет значение переменной MIB на значение, указанное диспетчером сети. Ответ агента SNMP на запрос set включает новые параметры в устройстве.



10.4 ПРОТКОЛ SNMP
10.4.3 ЛОВУШКИ АГЕНТА SNMP

Ловушки — это незапрашиваемые сообщения, предупреждающие диспетчера SNMP о каком-либо условии или событии в сети. Уведомления, направленные на ловушки, помогают сократить использование ресурсов сети и агентов, устраняя необходимость в некоторых запросах на опрос SNMP.

На рисунке показано использование ловушки SNMP для уведомления сетевого администратора о сбое интерфейса G0/0. Программное обеспечение NMS может отправлять сетевым администраторам текстовые сообщения, отображать всплывающие окно поверх ПО NMS или включать красный значок маршрутизатора в графическом интерфейсе пользователя NMS.



10.4 ПРОТКОЛ SNMP
10.4.4 ВЕРСИИ SNMP

SNMPv1 - устаревший стандарт, определенный в RFC 1157. Использует простой метод проверки подлинности на основе строки сообщества. Не следует использовать из-за рисков безопасности.

SNMPv2c - определяется в RFC 1901-1908. Использует простой метод проверки подлинности на основе строки сообщества. Содержит опции массового извлечения, а также более подробные сообщения об ошибках.

SNMPv3 - определяется в RFC 3410-3415. Использует аутентификацию пользователя, обеспечивает защиту данных с помощью HMAC-MD5 или HMAC-SHA и шифрование с использованием DES, 3DES или AES шифрования.

10.4 ПРОТКОЛ SNMP
10.4.5 СТРОКИ СООБЩЕСТВА

В версиях SNMPv1 и SNMPv2c для контроля доступа к MIB используется модель строки сообщества (community string). Строки сообщества представляют собой незашифрованный пароль. Строки сообщества SNMP производят аутентификацию доступа к объектам MIB.

Существует два типа строк сообщества:

Только чтение (Read-only - ro) — предоставляет доступ к переменным MIB, но не позволяет менять эти переменные. Поскольку версия 2c предоставляет минимальную безопасность, многие организации используют SNMPv2c в режиме только для чтения.

Чтение и запись (Read-write - rw) Предоставляет доступ для чтения и записи ко всем объектам в MIB.

Чтобы просмотреть или настроить переменные MIB, пользователь должен указать тип соответствующей строки сообщества — для чтения или для записи.

10.4 ПРОТКОЛ SNMP
10.4.6 ИДЕНТИФИКАТОР ОБЪЕКТА MIB

Переменные в MIB организованы иерархически. Фактически MIB определяет каждую переменную в качестве идентификатора объекта (OID). Идентификаторы OID уникальным образом определяют управляемые объекты. MIB организует OID на основе стандартов RFC, формируя иерархию OID, которая обычно представляется в виде дерева.

Дерево базы MIB для любого устройства включает несколько ветвей с переменными, общими для многих сетевых устройств, и несколько ветвей с уникальными переменными конкретного устройства или поставщика.

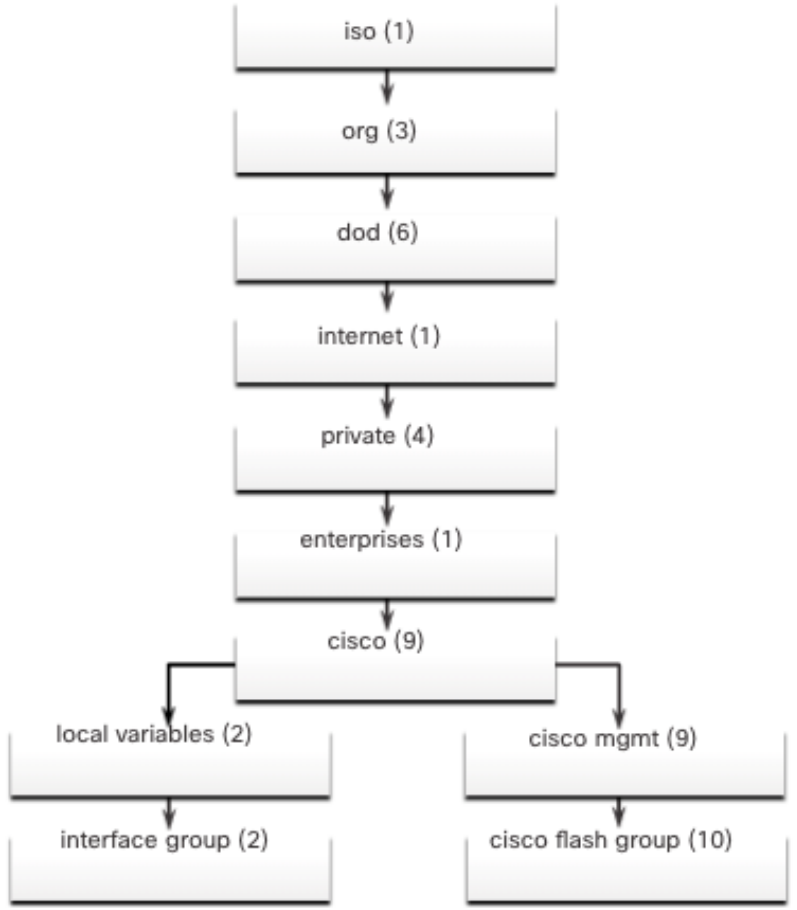
Некоторые общедоступные переменные определены в документах RFC. Большинство устройств используют эти переменные MIB. Кроме того, поставщики сетевого оборудования, такие как Cisco, могут определять собственные частные ветви дерева для добавления новых переменных, которые будут использоваться только для их устройств.

10.4 ПРОТКОЛ SNMP
10.4.6 ИДЕНТИФИКАТОР ОБЪЕКТА MIB

На рисунке показаны части структуры MIB, определенные Cisco. Обратите внимание, что OID может быть определен с помощью слов или чисел, что помогает найти определенную переменную в дереве.

OID, принадлежащие Cisco, пронумерованы следующим образом: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9).

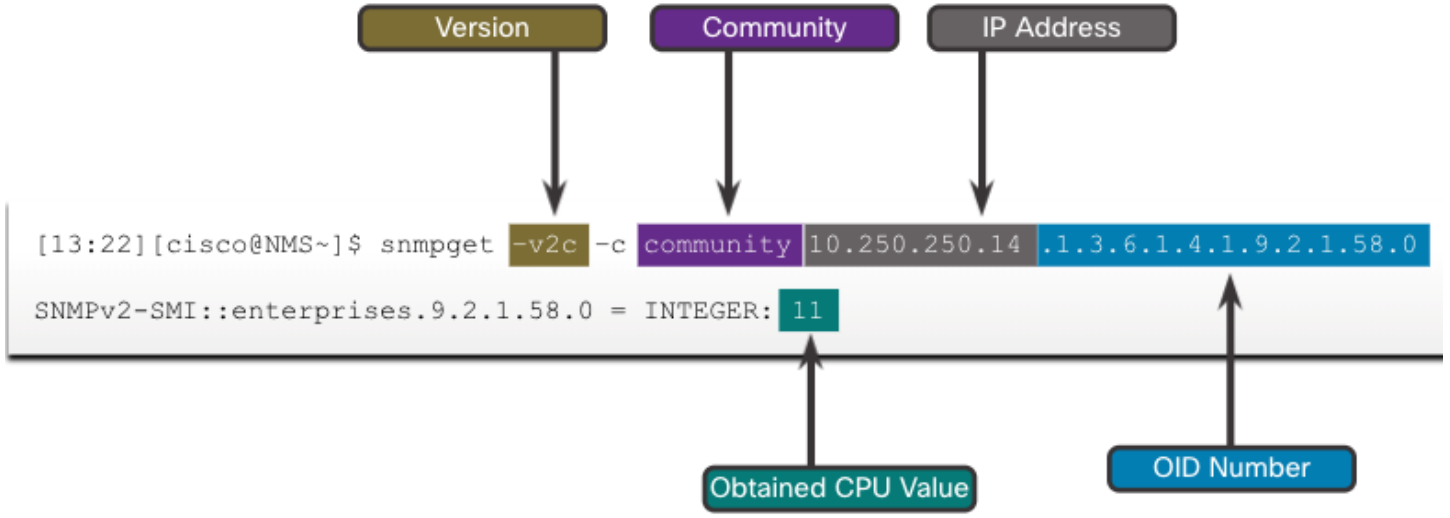
Таким образом, OID — 1.3.6.1.4.1.9.



10.4 ПРОТКОЛ SNMP
10.4.7 СЦЕНАРИЙ ОПРОСА SNMP

SNMP может использоваться для наблюдения за использованием ЦП в течение определенного периода времени опрашивающими устройствами. Статистика ЦП собирается в системе NMS и представляется в виде графика. Это создает базовый уровень информации для сетевого администратора.

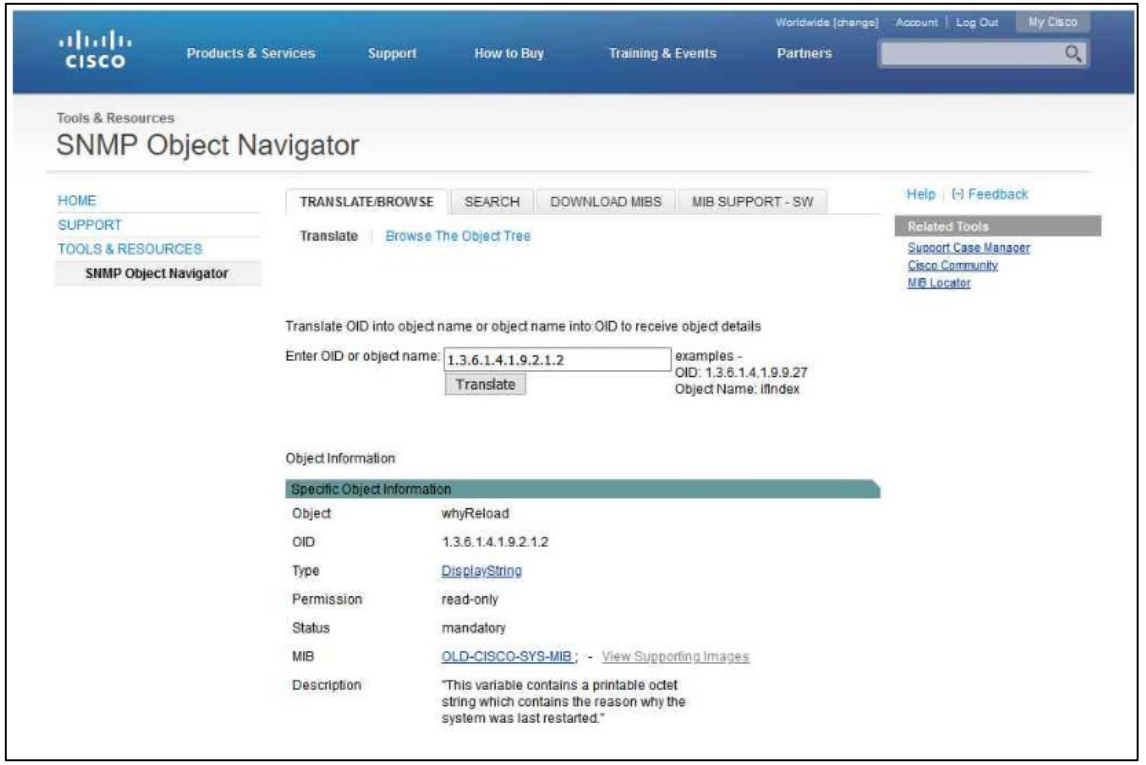
Данные извлекаются с помощью служебной программы snmpget и передаются в систему NMS. С помощью утилиты snmpget можно вручную извлекать данные в реальном времени или запустить отчет NMS. Этот отчет даст вам период времени, в течение которого вы можете использовать данные для получения среднего значения.



10.4 ПРОТКОЛ SNMP
10.4.8 SNMP OBJECT NAVIGATOR

Данная служебная программа дает некоторое представление о базовых механизмах работы SNMP. Однако работа с длинными именами переменных MIB, такими как 1.3.6.1.4.1.9.2.1.58.0, может представлять проблему для обычного пользователя. Чаще всего персонал, обслуживающий сеть, использует решение для управления сетями с простым и удобным графическим интерфейсом пользователя, причем все имена переменных MIB прозрачны для пользователя.

Cisco SNMP Navigator на веб-сайте http://www.cisco.com позволяет сетевому администратору исследовать подробности о конкретном OID.

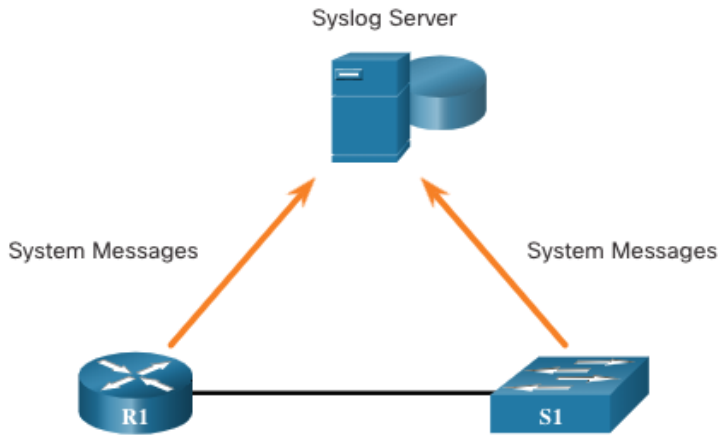


10.5 СИСТЕМНЫЙ ЖУРНАЛ
10.5.1 ВВЕДЕНИЕ В SYSLOG

Syslog использует порт UDP 514 для отправки сообщений с уведомлением о событиях по сетям IP на средства сбора сообщений о событиях, как показано на рисунке.

Сервис ведения системного журнала выполняет три основные функции:

- сбор информации в журнал для мониторинга и устранения неполадок;
- выбор типа информации, сбор которой будет осуществляться;
- определение получателей собранных сообщений syslog.



10.5 СИСТЕМНЫЙ ЖУРНАЛ
10.5.2 ПРИНЦИПЫ РАБОТЫ С СИСТЕМНЫМ ЖУРНАЛОМ

Протокол системного журнала (syslog) начинает с отправки системных сообщений и выходных данных команд debug в локальный процесс ведения журналов соответствующего устройства. Конфигурация Syslog может отправлять эти сообщения по сети на внешний сервер syslog, где они могут быть получены без необходимости доступа к фактическому устройству.

Кроме того, сообщения syslog могут отправляться во внутренний буфер. Сообщения, отправленные во внутренний буфер, можно просматривать только через интерфейс командной строки устройства.

Наконец, сетевой администратор может указать, какие типы системных сообщений будут отправляться в различные места назначения. В число популярных назначений для сообщений syslog входят следующие:

- буфер ведения журналов (ОЗУ в маршрутизаторе или коммутаторе);
- порт консоли;
- линия терминала;
- сервер Syslog.

10.5 СИСТЕМНЫЙ ЖУРНАЛ
10.5.2 ПРИНЦИПЫ РАБОТЫ С СИСТЕМНЫМ ЖУРНАЛОМ

Устройства Cisco создают сообщения syslog при определенных сетевых событиях. Во всех сообщениях syslog указывается уровень строгости (severity level) и объект (facility).

Чем меньше назначаемое число, тем более важным является оповещение syslog. В настройках уровня строгости сообщений можно установить, куда отправлять сообщения каждого типа (например, на консоль или в другие места назначения). Полный перечень уровней syslog представлен в таблице.

Название уровня строгости	Уровень строгости	Описание
Чрезвычайная ситуация	Уровень 0	Систему нельзя использовать
Предупреждение	Уровень 1	Требуется принять немедленные меры
Критический	Уровень 2	Критическое состояние
Ошибка	Уровень 3	Состояние ошибки
Предупреждение	Уровень 4	Состояние предупреждения
Уведомление	Уровень 5	Нормальное, но требующее внимания состояние
Информационный	Уровень 6	Информационное сообщение
Отладка	Уровень 7	Сообщение отладки

10.5 СИСТЕМНЫЙ ЖУРНАЛ
10.5.3 ОБЪЕКТЫ SYSLOG

Помимо указания уровня строгости в сообщениях syslog также содержатся сведения об объекте. Объекты syslog (syslog facilities) — это идентификаторы сервисов, которые определяют и классифицируют данные о состоянии системы для отчетов об ошибках и событиях. Доступные варианты объектов ведения журнала зависят от конкретного сетевого устройства.

Ниже приведены некоторые из общепринятых объектов сообщений syslog, которые регистрируются на маршрутизаторах Cisco IOS:

- IP
- Протокол OSPF
- Операционная система SYS
- Протокол IPSec
- IP интерфейса (IF)

10.5 СИСТЕМНЫЙ ЖУРНАЛ
10.5.3 ОБЪЕКТЫ SYSLOG

По умолчанию формат сообщений syslog в ПО Cisco IOS выглядит следующим образом:

%facility-severity-MNEMONIC: description

Пример выходных данных об изменении состояния канала EtherChannel коммутатора Cisco на активное будет выглядеть следующим образом:

%LINK-3-UPDOWN: Interface Port-channel1, changed state to up

В этом примере объектом является LINK, назначен уровень строгости 3, в качестве КРАТКОГО КОДА (MNEMONIC) выступает UPDOWN.

10.5 СИСТЕМНЫЙ ЖУРНАЛ
10.5.4 НАСТРОЙКА ВРЕМЕННОЙ МЕТКИ СИСТЕМНОГО ЖУРНАЛА

По умолчанию в сообщениях журнала нет метки времени. Сообщения журнала должны иметь метку времени. Потому что, когда они отправляются следующему адресату, например на сервер системного журнала, появляется запись о создании сообщения. Команда **service timestamps log datetime** позволяет принудительно отображать дату и время для зарегистрированных событий.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.1 ФАЙЛОВАЯ СИСТЕМА МАРШРУТИЗАТОРА

Файловая система Cisco IOS (IFS) позволяет администраторам перемещаться по различным каталогам, отображать список файлов в каталоге. Администратор также может создавать подкаталоги во флэш-памяти или на диске. Для различных устройств перечень доступных папок может отличаться.

В примере показан результат выполнения команды **show file systems**, которая выводит список всех доступных файловых систем на маршрутизаторе Cisco 1941.

Звездочкой обозначена текущая файловая система по умолчанию. Знак # указывает загрузочный диск. Оба они назначаются файловой системе флэш-памяти по умолчанию

```
Router# show file systems
File Systems:
       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
*   7194652672    6294822912      disk     rw   bootflash: flash:
    256589824     256573440      disk     rw   usb0:
    1804468224    1723789312      disk     ro   webui:
             -             -    opaque     rw   null:
             -             -    opaque     ro   tar:
             -             -   network     rw   tftp:
             -             -    opaque     wo   syslog:
      33554432      33539983     nvram     rw   nvram:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -   network     rw   sftp:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
Router#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.1 ФАЙЛОВАЯ СИСТЕМА МАРШРУТИЗАТОРА

Поскольку флеш-память является файловой системой по умолчанию, то в результатах выполнения команды **dir** указывается содержимое флеш-памяти. Особый интерес представляет последняя запись. Это имя текущего образа файла Cisco IOS, запущенного в ОЗУ.

```
Router# dir
Directory of bootflash:/
   11  drwx            16384   Aug 2 2019 04:15:13 +00:00  lost+found
370945  drwx             4096   Oct 3 2019 15:12:10 +00:00  .installer
338689  drwx             4096   Aug 2 2019 04:15:55 +00:00  .ssh
217729  drwx             4096   Aug 2 2019 04:17:59 +00:00  core
379009  drwx             4096  Sep 26 2019 15:54:10 +00:00  .prst_sync
80641  drwx              4096   Aug 2 2019 04:16:09 +00:00  .rollback_timer
161281  drwx             4096   Aug 2 2019 04:16:11 +00:00  gs_script
112897  drwx           102400   Oct 3 2019 15:23:07 +00:00  tracelogs
362881  drwx             4096  Aug 23 2019 17:19:54 +00:00  .dbpersist
298369  drwx             4096   Aug 2 2019 04:16:41 +00:00  virtual-instance
   12  -rw-               30   Oct 3 2019 15:14:11 +00:00  throughput_monitor_params
 8065  drwx             4096   Aug 2 2019 04:17:55 +00:00  onep
   13  -rw-               34   Oct 3 2019 15:19:30 +00:00  pnp-tech-time
249985  drwx             4096  Aug 20 2019 17:40:11 +00:00  Archives
   14  -rw-            65037   Oct 3 2019 15:19:42 +00:00  pnp-tech-discovery-summary
   17  -rw-          5032908  Sep 19 2019 14:16:23 +00:00
isr4200_4300_rommon_1612_1r_SPA.pkg
   18  -rw-        517153193  Sep 21 2019 04:24:04 +00:00  isr4200-
universalk9_ias.16.09.04.SPA.bin
7194652672 bytes total (6294822912 bytes free)
Router#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.1 ФАЙЛОВАЯ СИСТЕМА МАРШРУТИЗАТОРА

Чтобы просмотреть содержимое NVRAM, необходимо изменить текущую файловую систему по умолчанию, используя команду **cd** (изменить каталог), как показано в примере.

Команда отображения текущего рабочего каталога - **pwd**. Эта команда подтверждает, что просматривается именно каталог NVRAM. И наконец, команда **dir** отображает список содержимого NVRAM. Хотя в списке представлено несколько файлов конфигурации, в первую очередь нас интересует файл конфигурации начальной загрузки.

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/
32769  -rw-             1024                    startup-config
32770  ----               61                    private-config
32771  -rw-             1024                    underlying-config
    1  ----                4                    private-KS1
    2  -rw-             2945                    cwmp_inventory
    5  ----              447                    persistent-data
    6  -rw-             1237                    ISR4221-2x1GE_0_0_0
    8  -rw-               17                    ecfm_ieee_mib
    9  -rw-                0                    ifIndex-table
   10  -rw-             1431                    NIM-2T_0_1_0
   12  -rw-              820                    IOS-Self-Sig#1.cer
   13  -rw-              820                    IOS-Self-Sig#2.cer
33554432 bytes total (33539983 bytes free)
Router#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.2 ФАЙЛОВАЯ СИСТЕМА КОММУТАТОРА

Используя файловую систему флеш-памяти коммутатора Cisco 2960, можно скопировать файлы конфигурации и архивировать (скачивать и закачивать) образы ОС.

Для просмотра файловых систем на коммутаторе Catalyst используется та же команда, что и для маршрутизатора Cisco: **show file systems**.

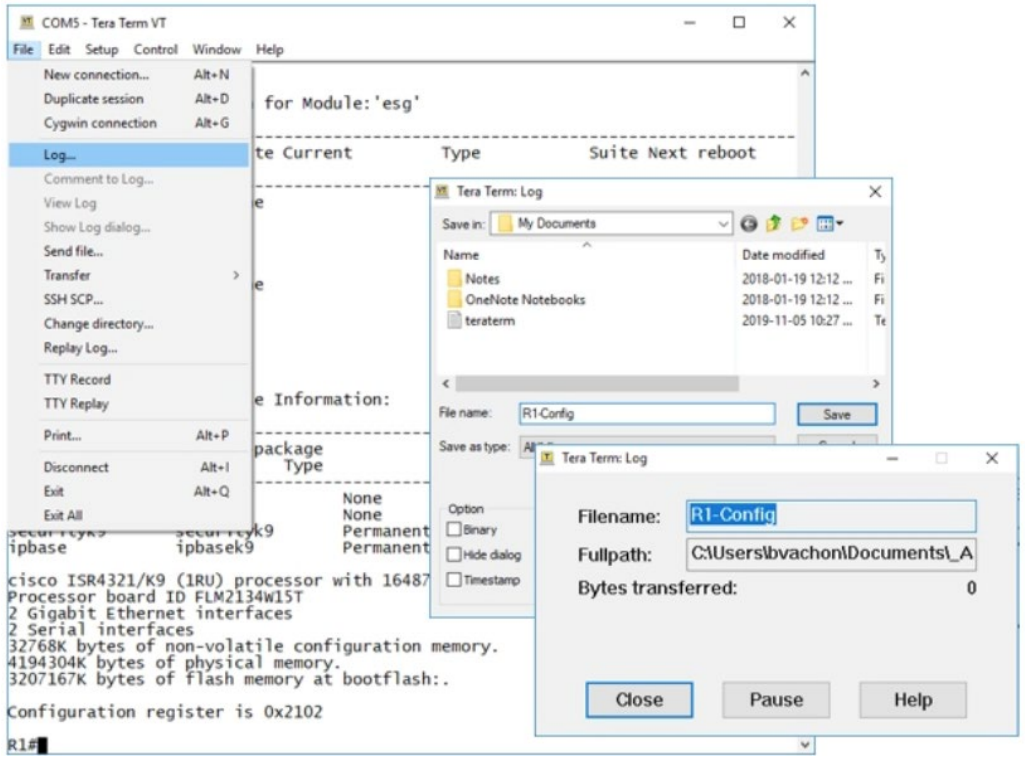
```
Switch# show file systems
File Systems:
       Size(b)     Free(b)      Type  Flags  Prefixes
*     32514048    20887552     flash     rw    flash:
           -           -      opaque     rw       vb:
           -           -      opaque     ro       bs:
           -           -      opaque     rw   system:
           -           -      opaque     rw   tmpsys:
       65536       48897      nvram     rw    nvram:
           -           -      opaque     ro   xmodem:
           -           -      opaque     ro   ymodem:
           -           -      opaque     rw     null:
           -           -      opaque     ro      tar:
           -           -     network     rw     tftp:
           -           -     network     rw      rcp:
           -           -     network     rw     http:
           -           -     network     rw      ftp:
           -           -     network     rw      scp:
           -           -     network     rw    https:
           -           -      opaque     ro      cns:
Switch#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.3 ИСПОЛЬЗОВАНИЕ ТЕКСТОВОГО ФАЙЛА ДЛЯ СОЗДАНИЯ РЕЗЕРВНОЙ КОПИИ КОНФИГУРАЦИИ

Файлы конфигурации можно сохранить в текстовом файле, используя программу Tera Term.

Шаг 1. В меню File (Файл) выберите пункт Log (Журнал).
Шаг 2. Выберите путь для сохранения файла. Программа Tera Term запустит процесс захвата текста.
Шаг 3. После начала данного процесса в отобразившейся командной строке привилегированного режима EXEC выполните команду **show running-config** или **show startup-config**. Текст, отображаемый в окне терминала, будет отправлен в выбранный файл.
Шаг 4. По окончании захвата текста нажмите Close (Закрыть) в окне журнала Tera Term.
Шаг 5. Просмотрите файл, чтобы убедиться в том, что он не поврежден.



10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.3 ИСПОЛЬЗОВАНИЕ ТЕКСТОВОГО ФАЙЛА ДЛЯ СОЗДАНИЯ РЕЗЕРВНОЙ КОПИИ КОНФИГУРАЦИИ

Конфигурацию можно скопировать из файла, а затем напрямую вставить на устройство. Это означает, что файл необходимо будет отредактировать, чтобы зашифрованные пароли имели текстовый формат. Также необходимо удалить сообщения операционной среды IOS и весь не относящийся к командам текст типа «--More--».

Кроме того, перед вставкой конфигурации может потребоваться добавить команды **enable** и **configure terminal** в начало файла или перейти в режим глобальной конфигурации. Вместо копирования и вставки конфигурацию можно восстановить из текстового файла с помощью Tera Term. При использовании программы Tera Term необходимо выполнить следующие действия.

Шаг 1. В меню File (Файл) выберите пункт Send file (Отправить файл).
Шаг 2. Укажите путь к файлу, который необходимо скопировать на данное устройство, и нажмите Open (Открыть).
Шаг 3. После этого программа Tera Term вставит этот файл в память устройства.

В интерфейсе CLI текстовое содержимое этого файла будет использоваться в качестве команд и станет текущей конфигурацией устройства.

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.4 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ С ПОМОЩЬЮ ПРОТОКОЛА TFTP

Для резервного копирования текущей конфигурации на TFTP-сервер выполните указанные ниже действия.

Шаг 1. Введите команду **copy startup-config tftp**.
Шаг 2. Введите IP-адрес узла, куда следует сохранить файл конфигурации.
Шаг 3. Введите имя, которое следует присвоить файлу конфигурации.
Шаг 4. Нажмите клавишу Enter для подтверждения каждого последующего действия.

Для восстановления текущей конфигурации с TFTP-сервера выполните указанные ниже действия.

Шаг 1. Введите команду **copy startup-config tftp**.
Шаг 2. Введите IP-адрес узла, на котором хранится файл конфигурации.
Шаг 3. Введите имя, которое следует присвоить файлу конфигурации.
Шаг 4. Нажмите клавишу Enter для подтверждения каждого последующего действия.

```
R1# copy running-config tftp
Remote host []?192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2019
Write file R1-Jan-2019 to 192.168.10.254? [confirm]
Writing R1-Jan-2019 !!!!!! [OK]
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.5 ИСПОЛЬЗОВАНИЕ ПОРТОВ USB НА МАРШРУТИЗАТОРЕ CISCO

Функция хранения с использованием USB обеспечивает поддержку USB-накопителей отдельными моделями маршрутизаторов Cisco. Поддержка USB-накопителей обеспечивает дополнительные функции хранения и возможность использования дополнительного загрузочного устройства. На рисунке показаны порты USB маршрутизатора Cisco 4321.

Чтобы просмотреть содержимое USB-накопителя, выполните команду **dir**.

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.5 ИСПОЛЬЗОВАНИЕ ПОРТОВ USB НА МАРШРУТИЗАТОРЕ CISCO

Выполните команду **show file systems**, чтобы проверить наличие USB-накопителя и подтвердить его имя. В этом примере файловая система USB называется usbflash0:.

Далее используйте команду **copy run usbflash0:/**, чтобы скопировать файл конфигурации на USB-накопитель. Обязательно используйте то имя флеш-накопителя, которое указано в файловой системе. Косую черту вводить необязательно (она обозначает корневой каталог USB-накопителя).

IOS запросит имя файла. Если этот файл уже существует на USB-накопителе, маршрутизатор предложит перезаписать его

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.5 ИСПОЛЬЗОВАНИЕ ПОРТОВ USB НА МАРШРУТИЗАТОРЕ CISCO

Используйте команду **dir** для просмотра файла на USB-накопителе, а также команду **more** для просмотра содержимого файла.

Для восстановления конфигураций с помощью флэш-накопителя USB необходимо отредактировать файл R1-Config с помощью текстового редактора. Если предположить, что именем файла будет R1-Config, используйте команду **copy usbflash0:/R1-Config running-config**, чтобы восстановить текущую конфигурацию.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config
4050042880 bytes total (3774144512 bytes free)
R1#
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
R1#
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.6 ВОССТАНОВЛЕНИЕ ПАРОЛЯ

Пароли на устройствах служат для защиты от несанкционированного доступа. Если пароль зашифрован (как, например, секретные пароли для входа в режим настройки), то после восстановления его необходимо заменить. В зависимости от устройства, подробная процедура восстановления пароля варьируется.

Однако все процедуры восстановления пароля основаны на том же принципе:

Шаг 1. Войдите в режим ROMMON.
Шаг 2. Измените значение регистра конфигурации.
Шаг 3. Скопируйте startup-config в running-config.
Шаг 4. Измените пароль
Шаг 5. Сохраните running-config как новый startup-config.

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

10.6.6 ВОССТАНОВЛЕНИЕ ПАРОЛЯ

Шаг 1. Войдите в режим ROMMON.

При наличии консольного доступа пользователь может войти в режим ROMMON используя специальную комбинацию клавиш во время процесса загрузки или вынув внешнюю флеш-память, когда устройство отключено.

При успешном выполнении отображается запрос rommon 1 > , как показано в примере.

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ
10.6.6 ВОССТАНОВЛЕНИЕ ПАРОЛЯ

Шаг 2. Измените значение регистра конфигурации.

Команда **confreg 0x2142** позволяет пользователю установить регистр конфигурации 0x2142, что заставляет устройство игнорировать файл конфигурации запуска во время запуска.

Изменив значение регистра конфигурации на 0x2142, введите **reset** в командной строке, чтобы перезапустить устройство.

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ
10.6.6 ВОССТАНОВЛЕНИЕ ПАРОЛЯ

Шаг 3. Скопируйте startup-config в running-config.

После того, как устройство завершит перезагрузку, введите команду **copy startup-config running-config**.

ВНИМАНИЕ: Не вводите **copy running-config startup-config**. Эта команда удалит исходную загрузочную конфигурацию.

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ
10.6.6 ВОССТАНОВЛЕНИЕ ПАРОЛЯ

Шаг 4. Измените пароль.

Поскольку вы находитесь в привилегированном режиме EXEC, вы можете настроить все необходимые пароли.

Примечание. Пароль cisco является ненадежным и используется здесь только для примера.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable secret cisco
```

10.6 ОБСЛУЖИВАНИЕ ФАЙЛОВ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ
10.6.6 ВОССТАНОВЛЕНИЕ ПАРОЛЯ

Шаг 5. Сохраните running-config как новый startup-config.

После настройки новых паролей измените значение регистра конфигурации обратно на 0x2102 с помощью команды **config-register 0x2102** в режиме глобальной конфигурации. Сохраните running-config в startup-config.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration... [OK]
R1#
```

10.7 УПРАВЛЕНИЕ ОБРАЗАМИ IOS
10.7.1 ИСПОЛЬЗОВАНИЕ СЕРВЕРОВ TFTP ДЛЯ ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ

По мере роста сети образы и файлы конфигурации Cisco IOS можно хранить на центральном TFTP-сервере. Это позволяет контролировать количество образов IOS и их версии, а также нуждающиеся в обслуживании файлы настроек ОС.

Производственные сети обычно занимают обширные области и содержат несколько маршрутизаторов. В любой сети рекомендуется сохранить резервную копию образа ОС Cisco IOS на случай повреждения или случайного удаления образа системы на маршрутизаторе.

Маршрутизаторам, находящимся на большом расстоянии друг от друга, необходим источник или место для хранения резервных образов программного обеспечения Cisco IOS. Использование сетевого TFTP-сервера позволяет загружать файлы образов и конфигураций по сети. Такой TFTP-сервер может быть маршрутизатором, рабочей станцией или хостом.

10.7 УПРАВЛЕНИЕ ОБРАЗАМИ IOS
10.7.2 СОЗДАНИЕ РЕЗЕРВНОЙ КОПИИ ОБРАЗА IOS НА СЕРВЕРЕ TFTP

Чтобы обслуживать сеть с минимальным временем простоя, необходимо вовремя создавать резервные копии образов Cisco IOS. Тогда сетевые администраторы смогут быстро восстановить стертый или поврежденный образ IOS. Выполните следующие действия:

Шаг 1. Отправьте эхо-запрос на TFTP-сервер. Проверьте связь с TFTP-сервером.

Шаг 2. Проверьте размер образа во флэш-памяти. Убедитесь, что на диске TFTP-сервера достаточно места для размещения образа программного обеспечения Cisco IOS. Для определения размера файла образа Cisco IOS можно воспользоваться командой **show flash:** на маршрутизаторе.

Шаг 3. Скопируйте образ на TFTP-сервер. Скопируйте образ на TFTP-сервер с помощью команды **copy** *source-url destination-url*. После выполнения команды с использованием заданных URL-адресов источника и назначения пользователь получит запрос на ввод имени файла источника, адреса удаленного узла и имени файла назначения. После этого начнется передача.

10.7 УПРАВЛЕНИЕ ОБРАЗАМИ IOS
10.7.3 КОПИРОВАНИЕ ОБРАЗА IOS НА УСТРОЙСТВО

Шаг 1. Отправьте эхо-запрос на TFTP-сервер. Проверьте связь с TFTP-сервером.

Шаг 2. Проверьте количество свободной флеш-памяти. Убедитесь, что на обновляемом устройстве достаточно места для флэш-памяти с помощью команды **show flash:**. Сравните свободный объем флеш-памяти с размером нового файла образа.

Шаг 3. Скопируйте файл образа IOS с TFTP-сервера на маршрутизатор. Выполните команду **copy tftp: flash:**. После выполнения этой команды с указанными URL-адресами источника и назначения пользователь получит запрос на ввод IP-адреса удаленного узла, имен файлов источника и назначения.

```
R1# copy tftp: flash:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200- universalk9_ias.16.09.04.SPA.bin...
Loading isr4200-universalk9_ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0/0): !!!!!!!!!!!!!!!!!!!

[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

10.7 УПРАВЛЕНИЕ ОБРАЗАМИ IOS
10.7.4 КОМАНДА BOOT SYSTEM

После запуска маршрутизатора загрузчик ищет в файле загрузочной конфигурации (startup configuration) команды **boot system** с указанными в них именем и расположением образа Cisco IOS, который он должен будет загрузить. Чтобы обеспечить отказоустойчивую загрузку, можно ввести несколько команд **boot system**.

Если в конфигурации нет команд **boot system**, маршрутизатор по умолчанию загружает первый допустимый образ Cisco IOS из флеш-памяти и запускает его.

Чтобы выполнить обновление до скопированного образа IOS после его сохранения во флеш-памяти маршрутизатора, укажите маршрутизатору использовать новый образ во время загрузки с помощью команды **boot system**. Сохраните конфигурацию. Перезагрузите маршрутизатор, чтобы он загрузился с новым образом.

```
R1# configure terminal
R1(config)# boot system flash0:isr4200-universalk9_ias.16.09.04.SPA.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```