# Лекция

# Мониторинг сети

**1. Основные понятия**

Мониторинг работающей сети предоставляет сетевому администратору информацию для эффективного управления сетью и создания статистических отчетов об использовании сети для других специалистов. Активность подключений, частота появления ошибок и состояние каналов — вот лишь несколько факторов, которые позволяют сетевому администратору оценить состояние и использование сети. Сбор и просмотр этой информации в течение продолжительного времени позволяют сетевому администратору анализировать и прогнозировать рост проекта, а также помогут обнаружить и заменить неисправную деталь, прежде чем она окончательно выйдет из строя.

**2. Введение в Syslog**

При возникновении определённых событий в сети сетевые устройства, используя доверенные механизмы, уведомляют администратора с помощью подробных системных сообщений. Эти сообщения могут быть некритическими или существенно важными. В распоряжении сетевых администраторов — различные варианты хранения, интерпретации и отображения этих сообщений, а также способы отправки уведомлений о сообщениях, которые могут оказать наибольшее влияние на сетевую инфраструктуру.

Самый распространенный способ получения системных сообщений, предоставляемый сетевыми устройствами, — это использование протокола под названием syslog.

Термин syslog используется для описания стандарта. Он также используется для описания протокола, разработанного для этого стандарта. Протокол syslog был разработан для систем UNIX ещё в 80-е гг. прошлого века, но был впервые документирован сообществом IETF под названием RFC 3164 только в 2001 г. 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.

Syslog поддерживают многие сетевые устройства, включая маршрутизаторы, коммутаторы, серверы приложений, межсетевые экраны и др. Протокол syslog позволяет сетевым устройствам отправлять системные сообщения по сети на серверы syslog. Для этой цели можно развернуть специальную выделенную (out-of-band, OOB) сеть.

Существуют различные пакеты ПО сервера Syslog для Windows и UNIX. Многие из них бесплатны.

Служба журналирования syslog предоставляет три основные возможности:

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

**Принцип работы Syslog**

На сетевых устройствах Cisco протокол syslog начинает с отправки системных сообщений и вывода процесса **debug** в локальный процесс ведения журналов соответствующего устройства. Каким образом процесс ведения журналов управляет этими сообщениями и выводом, зависит от настроек устройства. Например, сообщения syslog могут отправляться по сети на внешний сервер syslog. Эти сообщения можно прочитать без необходимости доступа к самому устройству. Сообщения журнала и выходные данные, хранящиеся на внешнем сервере, могут включаться в различные отчеты для упрощения их прочтения.

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. Например, можно настроить устройство, чтобы все системные сообщения отправлялись на внешний сервер syslog. Однако сообщения уровня debug будут пересылаться во внутренний буфер и будут доступны только администратору через интерфейс командной строки.

В число популярных назначений для сообщений syslog входят следующие:

* буфер ведения журналов (ОЗУ в маршрутизаторе или коммутаторе);
* линия консоли;
* линия терминала;
* сервер syslog.

Можно удалённо наблюдать за системными сообщениями путём просмотра журналов на сервере Syslog или путём доступа к устройству по протоколам Telnet, SSH или через порт консоли.

**Формат сообщений syslog**

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

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

Каждый уровень syslog имеет собственный смысл:

* **Уровень предупреждения (warning) — уровень критического состояния (emergency)**— это сообщения о сбоях программного обеспечения или оборудования; эти типы сообщений говорят о том, что затронута работа устройства. Назначаемый уровень syslog зависит от серьёзности проблемы.
* **Уровень отладки (debugging)**— сообщения этого уровня содержат выходные данные, полученные в результате выполнения различных команд **debug**.
* **Уровень уведомления (notification)**— сообщения уровня уведомления носят исключительно справочный характер, работоспособность устройств не затрагивается. На уровне предупреждения отображаются сообщения об изменении состояния интерфейса на активное или неактивное или о перезапуске системы.

Помимо указания уровня важности 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. Например, коммутаторы Cisco серии 2960, в которых используется Cisco IOS версии 15.0(2), и маршрутизаторы Cisco 1941, в которых используется Cisco IOS версии 15.2(4), поддерживают 24 варианта объектов, которые группируются в 12 типов объектов.

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)

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

seq no: timestamp: %facility-severity-MNEMONIC: description

Поля, содержащиеся в сообщении syslog ПО Cisco IOS, поясняются на рисунке 2.

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

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

В этом примере объектом является LINK, назначен уровень серьёзности 3, в качестве КРАТКОГО КОДА выступает UPDOWN.

Наиболее распространенными сообщениями являются сообщения об изменении состояния каналов на активное и неактивное, а также сообщения, создаваемые устройством при выходе из режима настройки. Если настроено журналирование в списках контроля доступа, устройство создаёт сообщения syslog, если пакеты соответствуют заданным условиям.

**Служба меток времени**

Сообщения журнала могут сопровождаться метками времени. Также может назначаться адрес источника сообщений syslog. Это повышает эффективность отладки и управления в режиме реального времени.

Если введена команда режима глобальной конфигурации **service timestamps log uptime**, для регистрируемых событий отображается время, прошедшее с момента последней загрузки коммутатора. В более полезной версии этой команды применяется ключевое слово **datetime** вместо ключевого слова **uptime**; в этом случае для каждого зарегистрированного события будут отображаться дата и время.

При использовании ключевого слова **datetime** необходимо настроить часы сетевого устройства. Часы можно настроить одним из двух способов:

* Вручную с помощью команды **clock set**
* Автоматически с помощью протокола NTP

Протокол NTP позволяет синхронизировать настройки времени сетевых устройств с сервером NTP.

Чтобы разрешить синхронизацию программных часов с сервером времени NTP, используйте команду **ntp server** *ip-address* в режиме глобальной конфигурации. Пример настройки показан на рисунке. Маршрутизатор R1 настроен как клиент NTP, маршрутизатор R2 выступает в качестве доверенного сервера NTP. Сетевое устройство можно настроить в качестве сервера NTP (что позволяет другим устройствам синхронизироваться с его временем) или в качестве клиента NTP.

В оставшейся части главы предполагается, что часы настроены и что на всех устройствах настроена команда **service timestamps log datetime**.

# Сервер Syslog

Для просмотра сообщений syslog на рабочей станции в сети должен быть установлен сервер syslog. Существуют различные бесплатные и условно-бесплатные версии syslog, а также платные корпоративные версии. На рисунке 1 ознакомительная версия службы Kiwi Syslog отображается на компьютере с ОС Windows 7.

Сервер syslog предоставляет довольно удобный в использовании интерфейс для просмотра выходных данных syslog. Сервер анализирует выходные данные и помещает сообщения в предопределённые столбцы для упрощения их интерпретации. Если для сетевого устройства, которое является источником сообщений syslog, настроены временные метки, в качестве даты и времени каждого сообщения будут отображаться выходные данные сервера Syslog, как показано на рисунке 2.

Сетевые администраторы могут легко ориентироваться в больших объемах данных, собранных на сервере Syslog. Одним из преимуществ просмотра сообщений системного журнала на сервере Syslog является возможность детализированного поиска данных. Кроме того, сетевой администратор может быстро удалить менее важные сообщения Syslog из базы данных.

# Команды маршрутизатора и коммутатора для клиентов syslog

Настройка маршрутизатора для отправки системных сообщений на сервер syslog, где они могут храниться, фильтроваться и анализироваться, выполняется в три шага:

**Шаг 1.** Настройте имя узла назначения или IP-адрес сервера Syslog в режиме глобальной конфигурации:

R1(config)# **logging 192.168.1.3**

**Шаг 2.** Укажите, какие сообщения следует отправлять на сервер syslog с помощью команды **logging trap** *level* в режиме глобальной конфигурации. Например, чтобы отправлять только сообщения уровня 4 и ниже (0—4), используйте одну из следующих двух эквивалентных команд:

R1(config)# **logging trap 4**

R1(config)# **logging trap warning**

**Шаг 3.** При необходимости настройте интерфейс источника с помощью команды **logging source-interface** *interface-type interface number* в режиме глобальной конфигурации. Таким образом, можно настроить, чтобы пакеты syslog содержали адрес IPv4 или IPv6 конкретного интерфейса независимо от того, какой интерфейс используется для отправки пакета с маршрутизатора. Например, чтобы настроить в качестве интерфейса источника g0/0, используйте следующую команду:

R1(config)# **logging source-interface g0/0**

На рисунке 1 маршрутизатор R1 настроен для отправки сообщений журнала уровня 4 и ниже на сервер syslog по адресу 192.168.1.3. В качестве интерфейса источника настроен интерфейс G0/0. Интерфейс loopback создан, затем переведён в неактивное состояние, затем снова в активное. Эти действия отражены в выводе консоли.

Сервер syslog Tftpd32, изображённый на рисунке 2, настроен на компьютере с ОС Windows 7 с IP-адресом 192.168.1.3. Как можно видеть, на сервере Syslog отображаются только сообщения с уровнем важности 4 или меньше (более значимые). Сообщения с уровнем важности 5 или выше (менее значимые) отображаются в выходных данных консоли маршрутизатора, но не появляются в выходных данных сервера syslog, поскольку команда **logging trap** отбирает сообщения syslog, отправляемые на сервер syslog, по критерию важности.

# Проверка syslog

Для просмотра любых зарегистрированных сообщений используйте команду **show logging**. Для буфера ведения журналов высокой ёмкости полезно использовать функцию конвейера (|) с командой **show logging**. Конвейер позволяет администратору более конкретно определить сообщения, которые следует отображать.

Например, команда **show logging** | **include changed state to up**, показанная на рисунке 1, обеспечивает отображение только уведомлений об интерфейсе, сообщающих об изменении состояния интерфейса на «активен».

Команда **show logging** | **begin June 12 22:35**, также показанная на рисунке 1, отображает содержимое буфера ведения журналов, начиная с 12-го июня.

Используйте средство проверки синтаксиса на рисунке 2 для настройки и проверки syslog на маршрутизаторе R1.

**3. Знакомство с SNMP**

**SNMP (Simple Network Management Protocol**— простой протокол управления сетями).

Протокол SNMP был разработан, чтобы администраторы могли управлять узлами, такими как серверы, рабочие станции, маршрутизаторы, коммутаторы и устройства безопасности, в сети IP. Он позволяет сетевым администраторам контролировать работу сети, выполнять поиск и разрешение сетевых проблем, а также планировать рост сети.

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

* диспетчер SNMP;
* агенты SNMP (управляемый узел);
* информационная база управления (MIB).

Для настройки SNMP на сетевом устройстве сначала необходимо указать отношения между диспетчером и агентом.

Диспетчер SNMP является частью системы управления сетями (network management system — NMS). Диспетчер SNMP запускает ПО для управления SNMP. Как показано на рисунке, диспетчер SNMP может собирать данные от агента SNMP с помощью запроса get и изменять настройки на агенте с помощью запроса set. Кроме того, агенты SNMP могут пересылать информацию непосредственно в NMS с использованием уведомлений («ловушек», trap).

Агент SNMP и MIB размещены на клиентах сетевого устройства. Сетевые устройства, которыми необходимо управлять, такие как коммутаторы, маршрутизаторы, серверы, межсетевые экраны и рабочие станции, оборудованы программным модулем агента SMNP. В базах MIB хранятся данные о работе устройств; они должны быть доступны для прошедших проверку подлинности удалённых пользователей. Агент SNMP отвечает за предоставление доступа к локальной базе объектов MIB, которая содержит сведения о ресурсах и активности.

SNMP определяет способ обмена информацией об управлении между приложениями управления сетями и агентами управления. SNMP использует UDP, номер порта 162, для получения и отправки информации по управлению.

**Принцип работы SNMP**

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

Существует два основных запроса диспетчера SNMP — get и set. Запрос get используется системой управления сетью NMS для отправки на устройство запроса о получении данных. Запрос set используется системой управления сетью NMS для изменения переменных настройки в устройстве агента. Запрос set также может инициировать определённые действия с устройством. Например, запрос set может вызвать перезагрузку маршрутизатора, отправку конфигурационного файла или получение конфигурационного файла. Диспетчер SNMP использует запросы get и set для выполнения операций.

Агент SNMP отвечает на запросы диспетчера SNMP следующим образом:

* **Получение переменной MIB.** Агент SNMP выполняет эту функцию в ответ на запрос GetRequest-PDU от системы NMS. Агент получает значение запрошенной переменной MIB и передаёт это значение системе NMS.
* **Установка переменной MIB.** Агент SNMP выполняет эту функцию в ответ на запрос SetRequest-PDU от системы NMS. Агент SNMP изменяет значение переменной MIB на значение, определённое системой NMS. Ответ агента SNMP на запрос set включает новые параметры в устройстве.

# Ловушки агента SNMP

NMS периодически проводит опрос агентов SNMP, размещенных на управляемых устройствах, запрашивая данные у устройства с помощью запроса get. С помощью этого процесса приложение для управления сетями может собирать информацию для мониторинга транспортной нагрузки и проверять настройки управляемых устройств. Информация может отображаться через графический интерфейс пользователя в системе NMS. Можно вычислить минимальные, средние и максимальные значения, создать графическое представление данных или установить пороговые значения, при превышении которых будут отправляться соответствующие уведомления. Например, система NMS может контролировать использование центрального процессора маршрутизатора Cisco. Диспетчер SNMP осуществляет периодическую выборку значений и представляет эту информацию в графическом виде, чтобы сетевой администратор могу использовать её для вычисления базовых показателей.

Периодический опрос SNMP имеет свои недостатки. Во-первых, существует задержка между временем обнаружения события и временем отправки соответствующего уведомления (путём опроса) системой NMS. Во-вторых, существует компромисс между частотой опроса и использованием пропускной способности.

Чтобы смягчить воздействие этих недостатков, агенты SNMP могут создавать и отправлять ловушки, сообщая системе NMS о некоторых событиях немедленно. Ловушки — это незапрашиваемые сообщения, предупреждающие диспетчера SNMP о каком-либо условии или событии в сети. Примерами условий ловушек, помимо прочего, являются следующие: неправильная аутентификация пользователей, перезапуски, изменение состояния канала (на активное или неактивное), отслеживание MAC-адресов, закрытие подключения TCP, потеря подключения к соседнему узлу или другие важные события. Уведомления, направленные на ловушки, помогают сократить использование ресурсов сети и агентов, устраняя необходимость в некоторых запросах на опрос SNMP.

**Версии SNMP**

Существует несколько версий SNMP, включая следующие:

* **SNMPv1** — простой протокол управления сетями, полноценный стандарт Интернета, описанный в документе RFC 1157.
* **SNMPv2c** — описан в серии документов RFC 1901—1908; использует среду администрирования на базе строки сообщества.
* **SNMPv3** — обеспечивающий взаимодействие протокол на основе стандартов, первоначально определённый в серии документов RFC 2273—2275; обеспечивает защищённый доступ к устройствам с помощью аутентификации и шифрования пакетов в сети. Данная версия протокола включает следующие функции обеспечения безопасности: контроль целостности сообщений для защиты пакетов от искажения при пересылке; аутентификация для подтверждения достоверности источника сообщения и шифрование для предотвращения прочтения содержимого сообщения несанкционированным источником.

Во всех версиях используются диспетчеры SNMP, агенты SNMP и база MIB. ПО Cisco IOS поддерживает все три версии. Версия 1 является устаревшим решением и редко используется в современных сетях, поэтому данный курс ориентирован на версии 2c и 3.

В SNMPv1 и SNMPv2c используется модель безопасности на основе сообществ (community). Сообщество диспетчеров, имеющих доступ к базе MIB агента, определяется списком контроля доступа и паролем.

В отличие от SNMPv1, версия SNMPv2c предусматривает механизм массового извлечения записей и более подробное информирование станций управления об ошибках. Механизм массового извлечения получает таблицы и большие объёмы информации, сводя к минимуму затраты времени на двустороннее согласование. Усовершенствованная обработка ошибок в SNMPv2c предусматривает расширенные коды ошибок для различных условий возникновения ошибок. Эти условия обозначаются одним кодом ошибки в SNMPv1. Коды возврата по ошибке в SNMPv2c включают тип ошибки.

**Примечание**. SNMPv1 и SNMPv2c включают минимальный набор средств обеспечения безопасности. В частности, SNMPv1 и SNMPv2c не обеспечивают ни аутентификацию источника сообщения управления, ни шифрование. Наиболее обновлённое описание версии SNMPv3 содержится в серии документов RFC 3410—3415. В эту версию протокола добавлены методы обеспечения безопасной передачи наиболее важных данных между управляемыми устройствами.

SNMPv3 предусматривает как модели безопасности, так и уровни безопасности. Модель безопасности — это стратегия аутентификации, настроенная для пользователя и группы, в которой данный пользователь находится. Уровень безопасности характеризует допустимую степень безопасности в модели. Сочетание уровня безопасности и модели безопасности определяет, какой механизм безопасности будет использоваться при обработке пакета SNMP. Доступные модели безопасности — SNMPv1, SNMPv2c и SNMPv3.

На рисунке перечислены характеристики различных моделей сочетаний моделей и уровней безопасности.

Сетевой администратор должен настроить агент SNMP для использования версии SNMP, поддерживаемой станцией управления. Поскольку агент может взаимодействовать с несколькими диспетчерами SNMP, можно настраивать программное обеспечение для поддержки связи с помощью SNMPv1, SNMPv2c или SNMPv3.

**Строки сообщества**

Для обеспечения функционирования SNMP система NMS должна иметь доступ к MIB. Для проверки подлинности запросов на доступ необходимо использовать ту или иную форму аутентификации.

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. Воспроизведите анимацию на рисунке, чтобы увидеть, как SNMP работает со строкой сообщества.

**Примечание**. Незашифрованные пароли не считаются механизмом безопасности. Это связано с уязвимостью незашифрованных паролей для атак с подслушиванием типа «человек-посередине», в которых пароли выясняются путём сбора пакетов.

**Идентификатор объекта информационной базы управления (MIB)**

Переменные в MIB организованы иерархически. Переменные MIB позволяют программному обеспечению осуществлять наблюдение за сетевым устройством и контроль над ним. Фактически MIB определяет каждую переменную в качестве идентификатора объекта (OID). OID представляют собой уникальные управляемые идентификаторы в иерархии MIB. 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. На рисунке 1 представлены некоторые части структуры MIB, определённые корпорацией Cisco Systems, Inc. Обратите внимание, что OID может быть определён с помощью слов или чисел, что помогает найти определённую переменную в дереве.

Поскольку ЦП является одним из основных ресурсов, его показатели должны постоянно измеряться. Статистика ЦП собирается в системе NMS и представляется в виде графика. Наблюдая за статистикой использования ЦП в течение длительного периода, администратору может предоставить предварительную оценку коэффициента использования ЦП. На основании этой оценки устанавливаются пороговые значения. Когда уровень использования ЦП превышает это пороговое значение, отправляются соответствующие уведомления. Средство построения графиков SNMP может периодически опрашивать агенты SNMP, например маршрутизатор, и создавать график полученных значений. Данные извлекаются с помощью служебной программы snmpget и передаются в систему NMS. С помощью служебной программы snmpget можно вручную получить значения среднего процента использования ЦП. Служебная программа snmpget требует настройки версии SNMP, правильного сообщества, IP-адреса сетевого устройства, которому направляется запрос, и номера OID. На рисунке 3 показано использование бесплатной служебной программы snmpget, которая предоставляет простой способ получения информации из базы MIB.

# Этапы настройки SNMP

Сетевой администратор может настроить SNMPv2 для получения информации о сети от сетевых устройств. Как показано на рисунке, основные шаги настройки SNMP выполняются в режиме глобальной конфигурации.

**Шаг 1.** (Обязательно) Настройте строку сообщества и уровень доступа («только чтение» или «чтение и запись») с помощью команды **snmp-server community** *string* **ro** | **rw**.

**Шаг 2.** (Дополнительно) Документально зафиксируйте местоположение устройства с помощью команды **snmp-server location** *text*.

**Шаг 3.** (Дополнительно) Документально зафиксируйте системный контакт с помощью команды **snmp-server contact** *text*.

**Шаг 4.** (Дополнительно) Ограничьте доступ по SNMP, разрешив его только узлам NMS (диспетчерам SNMP), которые разрешены списком контроля доступа: определите список контроля доступа, затем укажите ссылку на этот список контроля доступа с помощью команды **snmp-server community** *string access-list-number-or-name*. Эту команду можно использовать как для определения строки сообщества, так и для ограничения доступа SNMP с помощью списков контроля доступа. При желании шаги 1 и 4 можно объединить в один; сетевое устройство Cisco объединяет две команды в одну, если они вводятся по отдельности.

**Шаг 5.** (Дополнительно) Укажите получателя операций ловушки SNMP с помощью команды **snmp-server host** *host-id* [**version**{**1**| **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*. По умолчанию диспетчеры ловушек не определены.

**Шаг 6.** (Дополнительно) Включите ловушки на агенте SNMP с помощью команды **snmp-server enable traps** *notification-types*. Если в этой команде не определены типы уведомлений-ловушек, отправляются все типы ловушек. Если требуется применить конкретные типы ловушек, необходимо повторное использование этой команды.

**Примечание**. По умолчанию в SNMP не установлены ловушки. Без этой команды диспетчеры SNMP должны будут проводить опрос для получения всей существенной информации.

# Проверка настройки SNMP

Существует несколько программных решений для просмотра выходных данных SNMP. В рамках нашего курса сервер Syslog Kiwi отображает сообщения SNMP, связанные с ловушками SNMP.

ПК 1 и R1 настроены для отображения выходных данных, связанных с ловушками SNMP, в диспетчере SNMP.

Как показано на рисунке 1, компьютеру ПК 1 назначен IP-адрес 192.168.1.3/24. Сервер Syslog Kiwi установлен на ПК 1.

После настройки маршрутизатора R1 при возникновении события, подходящего под определение ловушки, на диспетчер SNMP отправляются ловушки SNMP. Например, если состояние интерфейса меняется на активное, на сервер отправляется ловушка. Изменения настройки на маршрутизаторе также вызывают отправку ловушек SNMP диспетчеру SNMP. Список из более чем 60 типов уведомлений-ловушек можно увидеть с помощью команды **snmp-server enable traps?.** В настройке R1 в команде **snmp-server enable traps** *notification-types* не указаны типы уведомлений-ловушек, поэтому отправляются все ловушки.

На рисунке 2 в меню **Setup** (Настройка) установлен флажок. Это означает, что администратору сети нужно, чтобы программное обеспечение диспетчера SNMP принимало ловушки SNMP через порт UDP 162.

На рисунке 3 верхняя строка выходных данных ловушки SNMP означает, что состояние интерфейса GigabitEthernet0/0 изменилось на активное. Кроме того, при каждом входе в режим глобальной конфигурации из привилегированного режима диспетчер SNMP принимает ловушку, как показано в выделенной строке.

Для проверки настройки SNMP используйте любые варианты команды **show snmp** в привилегированном режиме. Самой полезной является просто команда **show snmp**, так как она отображает информацию, которая обычно представляет интерес при проверке настройки SNMP. Если речь идёт о настройке SNMPv3, при использовании большинства других параметров команды отображаются только отдельные части выходных данных команды **show snmp**. На рисунке 4 представлен пример выходных данных **show snmp**.

В выходных данных команды **show snmp** не отображаются сведения, касающиеся строки сообщества SNMP или связанного списка контроля доступа, если таковой существует. На рисунке 5 представлена строка сообщества SNMP и данные списка контроля доступа, выведенные с помощью команды **show snmp community**.

**4. Практические рекомендации по обеспечению безопасности**

Хотя протокол SNMP полезен для мониторинга и отладки, он может привести к возникновению уязвимостей с точки зрения безопасности. По этой причине перед внедрением SNMP изучите лучшие практические рекомендации по обеспечению безопасности.

В SNMPv1 и SNMPv2c используются строки сообщества SNMP в незашифрованном виде для аутентификации доступа к объектам MIB. Строки сообщества, как и любой другой пароль, следует тщательно выбирать, чтобы их было непросто взломать. Кроме того, строки доступа необходимо регулярно менять в соответствии с политиками безопасности сети. Например, строки изменяются, если сетевой администратор меняет роли или уходит из компании. Если протокол SNMP используется только для наблюдения за устройствами, используйте сообщества только для чтения.

Убедитесь, что сообщения SNMP не распространяются за пределы консолей управления. Для предотвращения попадания сообщений SNMP за пределы необходимых устройств используйте списки контроля доступа. Для предоставления доступа только системам управления на контролируемых устройствах также должен использоваться список контроля доступа.

Рекомендуется использовать протокол SNMPv3, обеспечивающий аутентификацию и шифрование. Существует ряд других команд режима глобальной конфигурации, которые сетевой администратор может применять, чтобы воспользоваться преимуществами поддержки аутентификации и шифрования, предоставляемой протоколом SNMPv3:

* Команда **snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} создаёт новую группу SNMP на устройстве.
* Команда **snmp-server user** *username groupname* **v3** [**encrypted**] [**auth** {**md5** | **sha**} auth-password] [***priv*** {**des** | **3des** | **aes** {**128** | **192** | **256**}} priv-password] используется для добавления нового пользователя в группу SNMP, определённую в команде **snmp-server group** *groupname*.

# 5. Краткое описание протокола NetFlow

NetFlow — это технология Cisco IOS, предоставляющая статистические данные о пакетах, проходящих через маршрутизатор или многоуровневый коммутатор Cisco. NetFlow представляет собой стандарт сбора операционных данных IP в IP сетях.

Исторически сложилось так, что протокол NetFlow был разработан потому, что специалистам по сетевым технологиям был необходим простой и эффективный способ для отслеживания потоков TCP/IP в сети, а возможностей протокола SNMP было недостаточно. Протокол SNMP предоставляет широчайший диапазон функций и возможностей управления сетями, в то время как NetFlow предназначен, прежде всего, для предоставления статистики о пакетах IP, проходящих через сетевые устройства.

Протокол NetFlow предоставляет данные, которые позволяют добавить к мониторингу сети и контролю безопасности, планированию сети и анализу трафика такие возможности, как обнаружение узких мест сети и учет IP для выставления счетов. Например, на рисунке ПК 1 подключен к ПК 2 с помощью приложения, такого как HTTPS. Протокол NetFlow может контролировать это подключение уровня приложений, отслеживая количество байт и пакетов для данного потока. Затем он передаёт статистические данные на внешний сервер, который называется сборщиком данных (collector) NetFlow.

Протокол NetFlow стал стандартом мониторинга и теперь широко поддерживается в сетевой отрасли.

Flexible NetFlow — это новейшая технология NetFlow. Flexible NetFlow расширяет возможности первоначального протокола NetFlow, позволяя настраивать параметры анализа трафика в соответствии с конкретными требованиями сетевого администратора. Технология Flexible NetFlow позволяет создавать более сложные настройки для анализа трафика и экспорта данных с помощью компонентов настройки, которые можно использовать повторно.

Flexible NetFlow использует формат экспорта версии 9. Отличительной особенностью формата экспорта NetFlow версии 9 является то, что он основан на шаблонах. Шаблоны обеспечивают возможность расширения формата записи, что позволяет обновлять сервисы NetFlow в будущем без необходимости одновременных изменений основного формата записи потока. Важно отметить, что много полезных команд Flexible NetFlow были введены вместе с версией Cisco IOS 15.1.

**Общие сведения о NetFlow**

Существует много вариантов использования статистических данных, предоставляемых протоколом NetFlow; однако большинство организаций используют NetFlow для некоторых (или всех) из следующих основных целей сбора данных:

* Учёт использования сетевых ресурсов (кто использует, какие ресурсы, с какой целью).
* Отчётность и выставление счетов в соответствии с уровнем использования ресурсов.
* Использование результатов измерений для более эффективного планирования сети, с согласованием распределения и развертывания ресурсов с требованиями заказчиков.
* Использование информации для более эффективного структурирования и настройки набора доступных приложений и сервисов в соответствии требованиям пользователя и обслуживания клиентов.

При сравнении функций SNMP с функциями NetFlow в качестве аналогии для SNMP можно использовать ПО для дистанционного управления для автоматического транспортного средства, в то время как аналогией для NetFlow является простой, но подробный счёт за телефон. Детализованный счёт за телефонные переговоры предоставляет как подробную, так и сводную статистику по всем вызовам, что позволяет лицу, оплачивающему счета, отслеживать длительные вызовы, частые вызовы или вызовы, которые не следовало выполнять.

В отличие от SNMP, NetFlow использует модель пассивного приёма. Сборщик данных просто ждёт трафик NetFlow, а сетевые устройства отправляют данные NetFlow на сборщик в соответствии с изменениями в кэше потоков. Еще одно отличие между NetFlow и SNMP заключается в том, что NetFlow собирает только статистические данные о трафике, как показано на рисунке, в то время как SNMP может также собирать множество других рабочих показателей, например ошибки интерфейсов, использование ЦП и памяти. С другой стороны, статистика трафика, собранная с помощью NetFlow, отличается гораздо большей степенью детализации по сравнению со статистикой трафика, которую можно собрать при помощи SNMP.

**Примечание**. Не следует путать назначение и результаты NetFlow с назначением и результатами оборудования и программного обеспечения для сбора пакетов. В то время как средства сбора пакетов записывают всю возможную информацию, приходящую на сетевое устройство или выходящую с него для последующего анализа, NetFlow собирает только определённую статистическую информацию.

При разработке протокола NetFlow инженеры Cisco руководствовались двумя основными критериями:

* Технология NetFlow должна быть абсолютно прозрачна для приложений и устройств в сети.
* Для функционирования протокола NetFlow не обязательная его поддержка всеми устройствами в сети.

Выполнение этих технических условий обеспечило простоту развертывания NetFlow в самых сложных современных сетях.

**Примечание**. Несмотря на простоту развёртывания протокола NetFlow и его прозрачность для сетевых устройств и приложений, он потребляет дополнительную память на устройстве Cisco, поскольку сохраняет записанную информацию в кэше на устройстве. Размер кэша по умолчанию зависит от платформы, и администратор может изменить это значение.

**Потоки в сети**

NetFlow обрабатывает соединения TCP/IP для ведения статистического учёта, используя понятие потока. «Поток» (flow) — это однонаправленная последовательность пакетов между определённой системой-источником и определённым назначением. На рисунке иллюстрируется понятие потока.

Для протокола NetFlow, построенного на основе TCP/IP, источник и назначение определяются IP-адресами сетевого уровня, а также номерами порта источника и портов назначения транспортного уровня.

Существует несколько поколений технологии NetFlow, каждое из которых отличается усовершенствованиями в области определения потоков трафика. Первоначально протокол NetFlow различал потоки с помощью сочетания из семи характеристик. Если значение одного из этих полей отличается от значения другого пакета, можно с уверенностью утверждать, что эти пакеты относятся к разным потокам:

* IP-адрес источника;
* IP-адрес назначения;
* номер порта источника;
* номер порта назначения;
* тип протокола уровня 3;
* маркировка ToS (тип обслуживания);
* логический входной интерфейс.

Первые 4 поля, используемые NetFlow для определения потока, вам уже знакомы. IP-адреса источника и назначения, а также порты источника и назначения определяют связь между исходным и конечным приложением. Тип протокола уровня 3 определяет тип заголовка, следующий за заголовком IP (обычно TCP или UDP, но возможны другие варианты включая ICMP). Байт ToS в заголовке IPv4 содержит сведения о том, как устройства должны применять правила качества обслуживания (QoS) к пакетам в данном потоке.

Flexible NetFlow поддерживает больше различных параметров в записях данных о потоках. Flexible NetFlow позволяет администратору определять записи для кэша контроля потока Flexible NetFlow, выбирая определяемые пользователем дополнительные и обязательные поля для настройки сбора данных в соответствии с конкретными требованиями. Записи для кэша контроля потока Flexible NetFlow называются определяемыми пользователем записями. Значения в дополнительных полях добавляются к потокам для предоставления дополнительной информации о трафике в потоках. При изменении значения дополнительного поля новый поток не создаётся.

**Определение функциональных возможностей сборщика данных NetFlow**

Сборщик данных NetFlow — это компьютер, на котором выполняется прикладное программное обеспечение. Это программное обеспечение специально предназначено для обработки «сырых» данных NetFlow. Сборщик данных можно настроить для получения информации NetFlow от многих сетевых устройств. Сборщики данных NetFlow объединяют и упорядочивают данные NetFlow в соответствии с указаниями сетевых администраторов в рамках ограничений программного обеспечения.

На сборщике NetFlow данные NetFlow записываются на диск через заданные промежутки времени. Администратор может выполнять несколько схем или потоков сбора данных одновременно. Например, различные сегменты данных могут храниться для поддержки планирования вместо учёта вызовов и времени разговора абонента; сборщик данных NetFlow может легко создать подходящие схемы агрегации.

На рисунке 1 представлен сборщик данных NetFlow, пассивно прослушивающий экспортируемые датаграммы NetFlow. Приложение сбора данных NetFlow представляет собой многофункциональное, простое в использовании, масштабируемое решение для регулирования потребления экспортируемых данных NetFlow с различных устройств. Предполагаемое использование в организациях варьируется, однако часто целью является поддержка важных потоков, связанных с приложениями пользователей. Сюда относятся учёт, выставление счетов, планирование сети и её мониторинг.

На рынке существует несколько сборщиков данных NetFlow. Эти средства обеспечивают анализ трафика в сети, показывая ведущие (или наиболее активные) компьютеры, наиболее активно используемые приложения, а также другие данные о трафике, как показано на рисунке 2. Сборщик данных NetFlow отображает типы трафика (сетевой, почтовый, FTP, пиринговый и т. п) в сети, а также устройства, которые отправляют и получают большую часть трафика. Сбор информации предоставляет администратору сети сведения о наиболее активных отправителях, о наиболее активных узлах и наиболее активных получателях. Поскольку данные сохраняются через определённые промежутки времени, анализ сетевого трафика, выполняемый постфактум, поможет определить тенденции использования сети.

В зависимости от характера использования анализаторов NetFlow, сетевой администратор может выявить следующую информацию:

* Кто наиболее активно передаёт данные и кому?
* Какие часто посещаемые веб-сайты и загружаемые материалы?
* Кто создаёт больше всего трафика?
* Достаточно ли пропускной способности для поддержки наиболее важной деятельности?
* Кто монополизировал всю пропускную способность?

Количество информации, которая может быть проанализирована сборщиком данных NetFlow, зависит от используемой версии NetFlow, поскольку различные форматы экспорта NetFlow состоят из определённых типов записи NetFlow. Записи NetFlow содержат конкретную информацию о фактическом трафике, который составляет поток NetFlow.

Сборщик данных NetFlow предоставляет визуализацию и анализ записанных и объединенных данных потока в режиме реального времени. Можно указать маршрутизаторы и поддерживаемые коммутаторы, а также схему агрегации и продолжительность хранения данных до следующего периодического анализа. Можно выполнять упорядочение и визуализацию данных удобным для пользователей способом: в виде столбчатых диаграмм, круговых диаграмм или гистограмм упорядоченных отчётов. Данные после этого можно экспортировать в электронные таблицы, например Microsoft Excel, для более детального анализа, определения тенденций и отчётности.

**Заключение**

Время на сетевых устройствах Cisco можно синхронизировать с помощью NTP.

Сетевые устройства Cisco могут сохранять сообщения syslog на внутренний буфер, консоль, терминальную линию или внешний сервер syslog. Сетевой администратор может настроить типы сообщений, которые следует собирать, а также место назначения для отправки этих сообщений с метками времени.

Протокол SNMP состоит из трёх элементов: диспетчер, агент и MIB. Диспетчер SNMP размещается в системе NMS, в то время как агент и MIB размещаются на клиентских устройствах. Диспетчер SNMP может опрашивать клиентские устройства для получения информации или использовать сообщение-ловушку, получив которое, клиент немедленно сообщает о достижении заданного порогового значения. SNMP может также использоваться для изменения настройки устройства. SNMPv3 является рекомендуемым вариантом, поскольку эта версия протокола обеспечивает наивысший уровень безопасности. SNMP — это комплексное и многостороннее средство удалённого управления. При использовании протокола SNMP доступны почти все элементы, доступные с помощью команды **show**.

NetFlow — это технология Cisco IOS, являющаяся стандартом для сбора данных о работе IP-сетей. NetFlow эффективно определяет, какие сетевые ресурсы используются и для каких целей. NetFlow использует поля заголовка, чтобы различать потоки данных. Технология NetFlow основана на принципе пассивного приёма, при котором клиентское устройство инициирует отправку данных на настроенный сервер.