 [Перевод: английский - русский - www.onlinedoctranslator.com](https://www.onlinedoctranslator.com/ru/?utm_source=onlinedoctranslator&utm_medium=docx&utm_campaign=attribution)

Packet Tracer - Logging from Multiple Sources

Цели

**Часть 1. Использование системного журнала для захвата файлов журнала с нескольких сетевых устройств**

**Часть 2. Наблюдение за журналом доступа пользователей AAA**

**Часть 3. Просмотр информации NetFlow**

# Предыстория/сценарий

В этом упражнении вы будете использовать Packet Tracer для просмотра сетевых данных, созданных системным журналом, AAA и NetFlow.

# инструкции

## Просмотр записей журнала с помощью Syslog

### Сервер системного журнала

Packet Tracer поддерживает основные операции системного журнала. Устройства IOS в топологии настроены на отправку своих записей журнала на сервер системного журнала. Сервер системного журнала собирает записи журнала и позволяет их читать.

Записи журнала классифицируются по семи уровням серьезности. Более низкие уровни представляют более серьезные события. Уровни: аварийные (0), оповещения (1), критические (2), ошибки (3), предупреждения (4), уведомления (5), информационные (6) и отладочные (7). Клиенты системного журнала можно настроить для отправки записей журнала на серверы системного журнала в зависимости от уровня серьезности.

* + - 1. Щелкните сервер системного журнала, чтобы открыть его окно.
      2. Перейдите на вкладку Службы и выберите SYSLOG из списка служб, показанного слева.
      3. Нажмите «Вкл.», чтобы включить службу системного журнала.
      4. Держите это окно открытым и видимым.

### Включить системный журнал.

Устройства уже настроены для отправки сообщений журнала на сервер системного журнала, но Packet Tracer поддерживает ведение журнала только для уровня серьезности отладки с помощью системного журнала. Из-за этого мы должны генерировать сообщения уровня отладки (уровень 7), чтобы их можно было отправить на сервер системного журнала.

* + - 1. Нажмите R1 > вкладка CLI.
      2. Введите команду отладки пакетов eigrp, чтобы включить отладку EIGRP. Консоль командной строки немедленно заполнится отладочными сообщениями.
      3. Вернитесь в окно Syslog Server. Убедитесь, что там отображаются записи журнала.
      4. После регистрации нескольких сообщений щелкните переключатель, чтобы отключить службу системного журнала.

#### Вопросы:

Какая информация содержится в сообщениях системного журнала, отображаемых на сервере системного журнала?

Введите свои ответы здесь.

## Журнал доступа пользователей

Другой важный тип журнала относится к доступу пользователей. Наличие записей о входах пользователей в систему имеет решающее значение для устранения неполадок и анализа трафика. Cisco IOS поддерживает аутентификацию, авторизацию и учет (AAA). С помощью AAA можно не только делегировать задачу проверки пользователя внешнему серверу, но и регистрировать действия.

TACACS+ — это протокол, предназначенный для удаленной аутентификации через централизованный сервер.

Packet Tracer предлагает базовую поддержку AAA и TACACS+. Когда кто-то попытается войти в систему R2, R2 спросит сервер TACACS+, действителен ли этот пользователь, подтвердив имя пользователя и пароль. Сервер не только хранит учетные данные пользователя, но и регистрирует транзакции входа пользователя. Выполните следующие шаги, чтобы войти в R2 и отобразить записи журнала, связанные с этим входом:

* + - 1. Щелкните сервер системного журнала, чтобы открыть его окно.
      2. Выберите вкладку «Рабочий стол» и выберите «Учет AAA». Оставьте это окно открытым.
      3. Щелкните R2 > CLI.
      4. Введите следующие учетные данные пользователя: admin и ccnp\_8 в качестве имени пользователя и пароля.
      5. Вернитесь к окну AAA Accounting Records сервера Syslog.

#### Вопрос:

Какая информация содержится в записи журнала?

Введите свои ответы здесь.

* + - 1. На маршрутизаторе R2 введите команду выхода из системы.

#### Вопрос:

Что произошло в окне учета AAA?

Введите свои ответы здесь.

## NetFlow и визуализация

В топологии Syslog Server также является коллектором NetFlow. Маршрутизатор брандмауэра настроен как экспортер NetFlow.

* + - 1. Щелкните сервер системного журнала и закройте окно учетных записей AAA.
      2. На вкладке «Рабочий стол» выберите Netflow Collector. Убедитесь, что служба сборщика NetFlow включена.
      3. С любого ПК отправьте эхо-запрос на веб-сервер корпорации по адресу 209.165.200.194. После небольшой задержки круговая диаграмма обновится, чтобы показать новый поток трафика.
      4. Щелкните сегменты круговой диаграммы, чтобы просмотреть информацию о каждом потоке.

#### Вопрос:

Какая информация предоставляется NetFlow?

Введите свои ответы здесь.

**Примечание**: Отображаемые круговые диаграммы будут различаться в зависимости от трафика в сети. Между устройствами присутствуют другие потоки пакетов, например трафик, связанный с EIGRP. NetFlow перехватывает эти пакеты и экспортирует статистику в NetFlow Collector. Чем дольше NetFlow работает в сети, тем больше статистики трафика будет собрано.

Конец документа