**Packet Tracer. Ведение журналов из нескольких источников**

**Задачи**

**Часть 1. Использование системного журнала для перехвата файлов журналов из нескольких сетевых устройств**

**Часть 2. Наблюдение за доступом пользователя AAA**

**Часть 3. Ознакомление с информацией о NetFlow**

**Фоновый / сценарий**

В этом задании вам предстоит использовать Packet Tracer для просмотра сетевых данных, созданных системным журналом, AAA и NetFlow.

**Часть 1. Просмотр записей журнала с системным журналом**

**Шаг 1. Сервер системного журнала**

Системный журнал представляет собой систему обмена сообщениями, разработанную для поддержки удаленного ведения журнала. Клиенты системного журнала отправляют записи журнала на сервер системного журнала. Сервер системного журнала концентрирует и сохраняет записи журнала. Packet Tracer поддерживает базовые операции системного журнала и может использоваться для демонстрации. Сеть включает сервер системного журнала и клиентов системного журнала. Межсетевой экран, коммутатор уровня ядра, а также устройства R1 и R2 являются клиентами системного журнала . Эти устройства настроены для отправки своих записей журнала на сервер системного журнала . Сервер системного журнала собирает записи журнала и разрешает их чтение.

Записи журнала классифицируются по семи уровням критичности. Нижние уровни представляют более значимые события. Уровни: чрезвычайные ситуации (0), оповещения (1), критические сбои (2), ошибки (3), предупреждения (4), уведомления (5), информация (6) и отладка (7). Клиенты системного журнала можно настроить на отправку записей журнала на серверы системного журнала в зависимости от уровня критичности.

a. Нажмите **сервер системного журнала**, чтобы открыть его окно.

b. Выберите вкладку **Службы**ивыберите **SYSLOG**из списка служб, показанных слева.

c. Нажмите **On (Вкл.)**для включения службы системного журнала.

d. Записи системного журнала, поступающие от клиентов системного журнала, отображаются в окне справа. В настоящий момент записи отсутствуют.

e. Оставьте окно открытым и видимым и перейдите к **шагу 2**.

**Шаг 2. Включить системный журнал.**

Устройства уже настроены на отправку сообщений журнала на сервер системного журнала, но Packet Tracer поддерживает только ведение журнала для уровня отладки с помощью системного журнала. Поскольку мы должны создавать сообщения уровня отладки (уровень 7), их моно отправлять на сервер системного журнала.

a. Нажмите **R1** **> CLI**.

b. Нажмите «Ввод» для отображения командной строки и введите команду **enable** (включить).

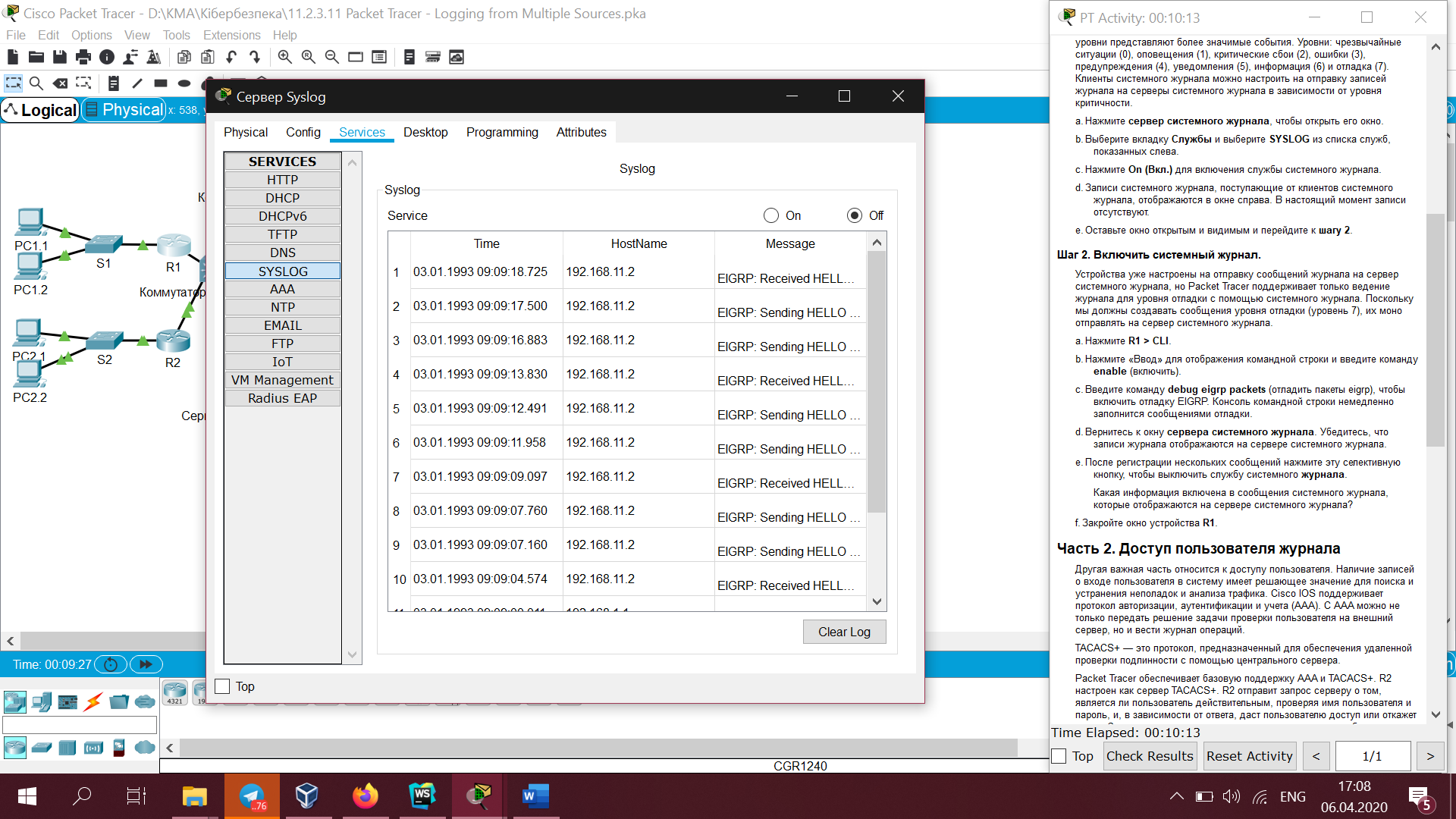
c. Введите команду **debug eigrp packets** (отладить пакеты eigrp), чтобы включить отладку EIGRP. Консоль командной строки немедленно заполнится сообщениями отладки.

d. Вернитесь к окну **сервера системного журнала**. Убедитесь, что записи журнала отображаются на сервере системного журнала.

e. После регистрации нескольких сообщений нажмите эту селективную кнопку, чтобы выключить службу системного **журнала**.

Какая информация включена в сообщения системного журнала, которые отображаются на сервере системного журнала?

f. Закройте окно устройства **R1**.



**Часть 2. Доступ пользователя журнала**

Другая важная часть относится к доступу пользователя. Наличие записей о входе пользователя в систему имеет решающее значение для поиска и устранения неполадок и анализа трафика. Cisco IOS поддерживает протокол авторизации, аутентификации и учета (AAA). С AAA можно не только передать решение задачи проверки пользователя на внешний сервер, но и вести журнал операций.

TACACS+ — это протокол, предназначенный для обеспечения удаленной проверки подлинности с помощью центрального сервера.

Packet Tracer обеспечивает базовую поддержку AAA и TACACS+. R2 настроен как сервер TACACS+. R2 отправит запрос серверу о том, является ли пользователь действительным, проверяя имя пользователя и пароль, и, в зависимости от ответа, даст пользователю доступ или откажет в нем. Сервер хранит учетные данные пользователя и способен вести запись о входах пользователя в систему. Выполните следующие действия, чтобы войти в систему на R2 и отобразить записи журнала , которые относятся к входу в систему.

a. Нажмите **сервер системного журнала**, чтобы открыть его окно.

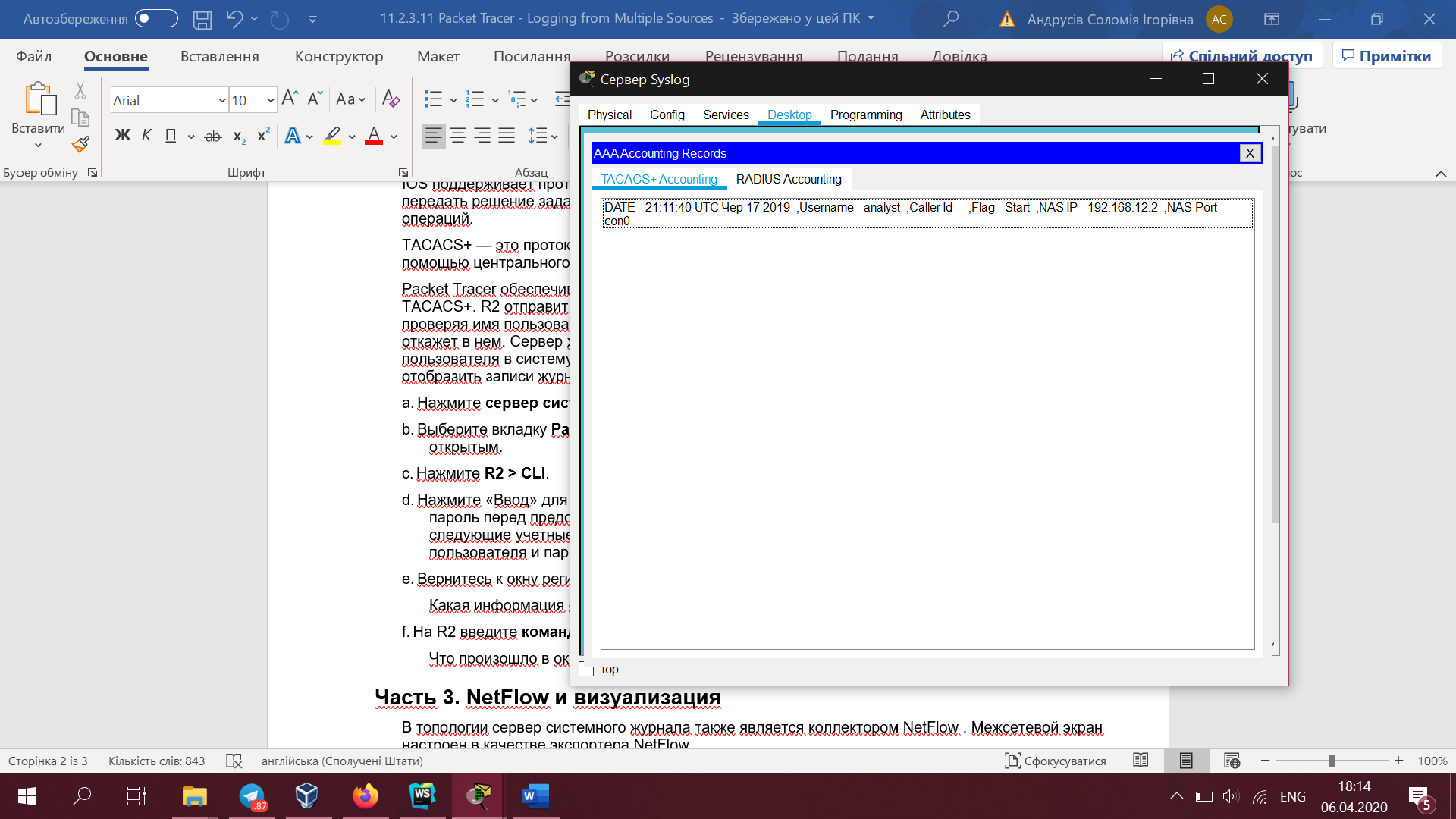
b. Выберите вкладку **Рабочий стол** и выберите **AAA Accounting (ААА Учет)**. Оставьте это окно открытым.

c. Нажмите **R2 > CLI**.

d. Нажмите «Ввод» для отображения командной строки. **R2**запросит имя пользователя и парольперед предоставлением доступа к своему интерфейсу командной строки. Введите следующие учетные данные пользователя: **analyst**и **cyberops** в качестве имени пользователя и пароля соответственно.

e. Вернитесь к окну регистрации учетных данных AAA сервера системного журнала.

Какая информация содержится в записи журнала?



f. На R2 введите**команду** выхода из системы.

Что произошло в окне учета AAA?

добавився ще один запис подібний до попереднього(окрім дати), тільки Flag= stop

**Часть 3. NetFlow и визуализация**

В топологии сервер системного журнала также является коллектором NetFlow . Межсетевой экран настроен в качестве экспортера NetFlow.

a. Нажмите **сервер системного журнала,** чтобы развернуть его окно. Закройте окно учетных записей AAA .

b. На вкладке **Рабочий стол**выберите **коллектор Netflow**. Службы коллектора NetFlow должны быть включены.

c. На любом ПК выполните ping-запрос корпоративного веб-сервера на 209.165.200.194. После кратковременной задержки обновится круговая диаграмма для отображения нового потока трафика.

**Примечание.** Отображаемые круговые диаграммы будут различаться в зависимости от трафика в сети. Другие потоки пакетов, такие как трафик, связанный с EIGRP, передаются между устройствами. NetFlow захватывает эти пакеты и экспортирует статистику в коллектор NetFlow. Чем дольше NetFlow работает в сети, тем больше статистики по трафику будет перехвачено.

**Вопросы для повторения**

Поскольку присутствующие в задании инструменты являются полезными, каждый из них имеет собственную службу и должен запускаться на абсолютно разных устройствах. Лучшим способом, который будет рассматриваться далее в рамках этого курса, является концентрирование всей информации о входе в систему в одном инструменте, что позволяет легко организовать перекрестные ссылки и предоставит мощные возможности поиска. Платформы управления событиями и данными в системе информационной безопасности (SIEM) могут собирать файлы журнала и информацию из различных источников, а также интегрировать информацию для доступа к одному инструменту.