# Конфигурирование протоколов управления оборудованием

При выполнении заданий данного параграфа используйте схему сети, изображенную на рис. 2.15. Все ПО, необходимое для выполнения заданий, установлено в ОС образа VMware XP\_VMnet2, ярлыки для запуска программ расположены на рабо- чем столе.

* + 1. ***Сохранение и загрузка файлов конфигурации с использованием протоколов tftp и ftp***

## ВЫПОЛНИТЬ!

1. Запустить программу 3CDaemon, перейти на вкладку tftp сервера. Запустить захват трафика. В привилегированном режиме на маршрутизаторе lab1 выполнить команду **copy run tftp://10.0.0.5/router-lab1.cfg**. Подтвердить запросы маршрутизатора и дождаться окончания копирования.
2. В окне анализатора трафика найти пакеты, принадлежащие протоколу tftp. Какой транспортный протокол использует tftp? Каким образом передаются команды и содержимое файла?
3. На XP\_VMnet2 перейти в рабочий каталог tftp-сервера 3CDaemon (e:\dir-tftp). Найти только что скопированный файл и открыть его любым текстовым редактором. Этот файл содержит текущую конфигурацию устройства. Найти в файле параметры, установленные Вами в ходе лаборатор- ной работы.
4. На маршрутизаторе lab1 удалить файл стартовой конфигурации (команда **erase startup-config**).
5. Загрузить сохраненный на сервере файл **router-lab1.cfg** в качестве файла стартовой конфигурации (команда **copy tftp: startup-config**).
6. Выполнить пункты 1 ÷ 5 для маршрутизатора lab2, используя протокол ftp. Для возможности сохранения файла конфигурации по протоколу ftp необходимо создать соответствующую учетную запись на сервере (рис. 2.16).
	* 1. ***Доступ к маршрутизатору по протоколам Telnet и SSH***

## ВЫПОЛНИТЬ!

1. На маршрутизаторах lab1 и lab2 создать учетную запись пользователя с именем **cisco**, паролем **secret** и уровнем привилегий **0**.



Рис. 2.16. Cоздание учетной записи на сервере FTP

1. На маршрутизаторах lab1 и lab2 установить пароль **enable**

для входа в привилегированный режим.

1. На маршрутизаторах lab1 и lab2 сконфигурировать линии виртуальных терминалов vty0 ÷ vty4 на аутентификацию с использованием локальной базы устройства.
2. Подключиться к маршрутизатору lab1 по протоколу Telnet.

В Wireshark проанализировать трафик сессии.

1. Указать на маршрутизаторе lab2 имя домена с помощью команды **ip domain-name <имя>**, где параметр **<имя>** – это имя произвольного домена, например, lab.net.
2. Сгенерировать ключ шифрования RSA длиной более 1024 бит с помощью команды **crypto key generate rsa**. После выполнения этой команды на маршрутизаторе начинает функционировать сервер SSH.
3. Подключиться к маршрутизатору lab2 по протоколу SSH, используя программу Putty (ярлык на рабочем столе). В Wireshark проанализировать трафик сессии.
4. Установить для линий виртуальных терминалов маршрутизатора lab2 возможность подключения только с использованием протокола SSH, выполнив команду **transport input ssh**. Убедитесь, что подключение пользователя по протоколу Telnet сбрасывается маршрутизатором.
5. Отобразить и проанализировать с помощью команд **show ssh** и **show ip ssh** информацию о сессиях по протоколу SSH и настройках сервера SSH по умолчанию.
	* 1. ***Доступ к маршрутизатору по протоколу HTTP и HTTPS***

## ВЫПОЛНИТЬ!

1. На маршрутизаторе lab1 сконфигурировать доступ по протоколу HTTP на аутентификацию с использованием локальной базы устройства с помощью команды **ip http authentication local**.
2. Проверить в текущей конфигурации маршрутизатора запущен ли HTTP-сервер (команда **ip http server**) и в случае необходимости запустить его. Подключиться к маршрутизатору по web-интерфейсу. В Wireshark проанализировать трафик сессии. Изучить возможности web-доступа по конфигурированию устройства.
3. Остановить на маршрутизаторе HTTP-сервер и запустить HTTPS-сервер (команда **ip http secure-server**). Подключиться к маршрутизатору по web-интерфейсу. В Wireshark проанализировать трафик сессии.

### Регистрация событий

Диагностические сообщения о системных событиях выводятся маршрутизатором по умолчанию только на консольную линию. Для того чтобы эти сообщения дублировались в виртуальные тер- миналы (то есть в telnet-соединения), в контексте администратора в соответствующем сеансе используется команда

# lab1#terminal monitor.

При конфигурировании линий виртуальных терминалов для этой цели выполняется команда **monitor**. Вывод сообщений мож-

но направить также во внутренний буфер устройства или на syslog-

сервер. Направление в буфер:

# lab1(config)#logging buffered <размер>.

Буфер организован в виде очереди указанного размера (в бай- тах), самые старые сообщения удаляются из него при поступлении новых. Размер буфера по умолчанию – 4096 байт. Просмотр буфера (и параметров процесса регистрации событий):

# lab1#show logging.

Очистка буфера производится командой

# lab1#clear logging.

Пример отправки сообщений на syslog-сервер: **lab1(config)#logging <IP-адрес сервера> lab1(config)#logging facility local7 lab1(config)#logging trap debugging.**

Последние две команды определяют источник сообщений (facility в терминах syslog, используется для определения способа обработки сообщений на сервере) и степень важности (debugging – минимальная) сообщений, протоколируемых в системном журнале. По умолчанию диагностические сообщения имеют метки вре- мени, которые отсчитываются с момента загрузки устройства (system uptime), поэтому для того чтобы время выводилось в обыч- ном формате (дата, время суток), в конфигурации необходимо ука-

зать:

# lab1(config)#service timestamps log datetime lo- caltime

**lab1(config)#service timestamps debug datetime locatime.**

## ВЫПОЛНИТЬ!

1. Реализовать вывод диагностических сообщений в виртуальный терминал.
2. Запустить syslog-сервер 3CDaemon на XP\_VMnet2.
3. Сконфигурировать маршрутизаторы lab1 и lab2 для отправки на сервер сообщений о **всех** системных событиях, указав различные источники для идентификации маршрутизаторов, например, для lab1 – local1, а для lab2 – local2.
4. Запустить захват сетевого трафика. На маршрутизаторах перейти в режим конфигурации интерфейса FastEthernet0/1, выключить его, а затем через некоторое время снова включить. Какие сообщения получил syslog сервер?
5. Сравнить диагностические сообщения, выводимые в виртуальном терминале и на syslog-сервере.
6. В анализаторе сетевого трафика найти пакеты, относящиеся к протоколу syslog. Какой транспортный протокол используется для их передачи? Какая информация содержится в этих пакетах? Какие механизмы позволяют отследить отправителя пакета, и насколько они надежны?

### Протокол обнаружения соседних устройств CDP

Протокол CDP используется устройствами Cisco по умолча- нию, поэтому в целях безопасности для запрета его функциониро- вания на маршрутизаторе в целом в режиме глобальной конфигу- рации необходимо ввести команду **no cdp run**. Для использования протокола на конкретных интерфейсах устройства применяется команда **cdp enable** в режиме конфигурирования интерфейса. Параметры функционирования CDP отображаются ко- мандой **show cdp** в режиме глобального конфигурирования.

## ВЫПОЛНИТЬ!

1. Убедиться, что команда **no cdp run** отсутствует в текущей конфигурации устройства (**show running- config**). Запросить у маршрутизатора lab1 информацию о его соседях: **show cdp neighbors**. Какие устройства и каким образом соединены с маршрутизатором? Какую опасность может представлять протокол CDP?
2. Отобразить и проанализировать параметры функциониро- вания протокола CDP по умолчанию.
3. Выполнить команду **show cdp detail**. Какая информация из выведенного перечня была бы полезна для потенциального злоумышленника? Найти в выведенных параметрах IP-адреса соседних устройств.
4. На узле XP\_VMnet2 захватить CDP-пакеты, передающиеся через его интерфейс локальной сети. Какой транспорт

используется протоколом CDP? С какой периодичностью передаются сообщения протокола?