Работа 2 Каналы и интерфейсы управления сетевыми устройствами

(Сохранена нумерация разделов пособия)

3.1. Каналы и интерфейсы управления сетевыми устройствами

Сетевые коммуникационные устройства должны обеспечивать возможность как локального, так и удаленного управления. Локальное управление осуществляется, как правило, посредством подключения к устройству консоли через выделенный порт. (Консольное управление). Удаленное управление предусматривает использование сетевой инфраструктуры для связи УК администратора с устройством.

В большинстве случаев удаленное управление коммуникационными устройствами строится на основе модели "менеджер-агент". При этом под агентом понимают программное средство, функционирующее на управляемом коммуникационном устройстве и непосредственно взаимодействующее с управляемым объектом, а под менеджером – управляющую программу, функционирующую на компьютере администратора. Как правило, это компьютер общего назначения.

Агент обслуживает базу данных управляемых (наблюдаемых) параметров и отвечает за соответствие базы реальному состоянию объекта.

Менеджер может в любой момент запросить информацию о состоянии объекта, выполняя операцию чтения, и агент, в ответ на этот запрос, обязан передать содержимое всей базы или ее части. Операция записи в базу заставляет агента применить управляющее воздействие к объекту.

Обмен сообщениями между агентами и менеджерами может происходить как по тем же каналам связи, по которым передаются "полезные" данные, так и по отдельным каналам. В связи с этим различают внутриполосное (in-band) управление, то есть управление по тому же каналу, по которому передаются пользовательские данные, и внеполосное (out-of-band) управление, при котором управляющая информация передается по отдельному каналу управления.

Управление in-band более экономично, так как не требует создания отдельной инфраструктуры управления. Недостатками являются дополнительная загрузка сети управляющим трафиком, проблема безопасности управления и некоторые ограничения на функции управления.

Управление out-of-band менее экономично, но является более защищенным и обеспечивает полную независимость функций управления от состояния управляемой сети.

Для связи встроенных агентов с внешним менеджером используются или стандартные протоколы прикладного уровня - Telnet, SSH (Управление через Telnet), HTTP, HTTPS (WEB-управление) или специальные протоколы управления (SNMP, CMIP).

3.1.1. Консольное управление

Консольное управление относится к внеполосному - к управляемому устройству подключают внешний терминал (консоль), как правило, алфавитно-цифровой. Для подключения используют либо специальный консольный порт, либо последовательный интерфейс RS-232C. Терминал должен поддерживать определенную систему команд (например, VT-52, VT-100), на которую рассчитано управляемое устройство. В качестве терминала часто используют ПК с программой эмуляции терминала (Putty. TeraTerm и др.), подключенный через COM-порт.

Форма диалога с устройством определяется встроенным ПО, чаще всего используется интерфейс командной строки или меню.

Консольное управление позволяет настраивать любые параметры устройства, независимо от состояния сети передачи данных. С его помощью настраивают параметры для удаленного управления (как внеполосного, так и внутриполосного). К таким параметрам относятся адрес, маска, имя устройства, адрес маршрутизатора, параметры протоколов удаленного управления (SNMP, Telnet), пароль на доступ и др.

3.1.2. Управление через Telnet (SSH)

Управление через Telnet позволяет удаленно управлять устройством по сети. Возможны реализации как внеполосного, так и внутриполосного управления через Telnet. По сути, это вариант удаленного консольного управления с доступом по протоколу Telnet или SSH. Пользовательский интерфейс управления при этом определяется встроенным ПО управляемого устройства и используемой на УК клиентской программой.

Управление через Telnet требует использования протокола IP. Для него на управляющем компьютере необходимо запустить приложение Telnet – эмуляцию

терминала со связью через протокольный стек TCP/IP (или его безопасный вариант - SSH). В этом приложении необходимо установить связь с управляемым устройством, указав его IP-адрес и введя пароль. После установления соединения компьютер будет играть роль удаленного терминала управляемого устройства, работа с которым аналогична вышеописанному консольному управлению.

До использования Telnet управляемое устройство должно быть сконфигурировано, как правило, через консоль. Ему должен быть назначен IP-адрес, маска подсети и адрес маршрутизатора. В целях обеспечения безопасности на управляемом устройстве задают пароль доступа. В последнее время вместо протокола Telnet чаще используется его защищенный аналог - протокол безопасного соединения (SSH или другой) с шифрацией потоков данных.

Управление через Telnet позволяет с одного компьютера управлять множеством устройств. Как и консольный вариант, Telnet-управление подразумевает непосредственный диалог с человеком-администратором и не подходит для создания сложных автоматизированных систем управления.

3.1.3. WEB-управление

Основная идея WEB-управления заключается в обеспечении возможности выполнения администратором управляющих действий через графический интерфейс стандартного WEB-браузера. Для этого в ПО управляемого устройства вводятся функции WEB-сервера, формирующего страницы интерфейса управления. Эти страницы могут отображаться в графическом виде WEB-браузером любого узла, с которого управляемое устройство доступно по протоколу HTTP (HTTPS). Вид интерфейса определяется ПО управляемого устройства. В отличие от графических оболочек управляющих программ, использующих SNMP, WEB-управление не требует установки специализированного ПО на управляющем компьютере. Для управления может использоваться любой компьютер общего назначения со стандартным WEB-браузером.

Для обеспечения WEB-управления устройству должны быть указаны параметры его IP-подключения (адрес, маска, адрес маршрутизатора).

Безопасность управления обеспечивается паролями доступа, ограничением списка разрешенных узлов и возможностью шифрования данных (протокол HTTPS).

3.1.4. Протоколы управления SNMP и CMIP.

В настоящее время применяются два семейства стандартов управления сетями:

- стандарты Интернет, на базе протокола SNMP;
- стандарты ISO/ITU-T, на базе протокола CMIP.

Традиционно в компьютерных сетях применяется в основном управление на основе SNMP, а протокол CMIP используется в телекоммуникационных системах.

Концепция SNMP-управления стандартизирует следующие элементы:

- Протокол взаимодействия агента и менеджера.
- Язык описания информационной базы управления (Management Information Base - MIB) и сообщений SNMP – язык ASN.1.
- Несколько конкретных моделей MIB (MIB-1, MIB-II, RMON, RMON2).

Все остальное определяется разработчиком системы управления.

Протокол SNMP – протокол прикладного уровня стека TCP/IP. Взаимодействие агента с менеджером организуется по типу запрос-ответ. Протокол используется для чтения/записи значений параметров, хранящихся в базе данных MIB.

Протокол использует очень ограниченный набор команд:

get (getNext, getBulk) - для получения данных от агента

set – для передачи управляющих воздействий агенту.

trap – для передачи по инициативе агента сообщения (прерывания) менеджеру о возникновении особой ситуации.

Информационная база управления (MIB) представляет собой иерархически организованную систему объектов. Каждый объект MIB является одним из множества параметров управляемого устройства.

Существуют стандарты, определяющие структуру MIB, в том числе набор типов объектов, их имена и допустимые операции над этими объектами. Древовидная структура MIB позволяет помимо обязательных (стандартных) поддеревьев включать и частные поддеревья, позволяющие управлять специфическими функциями устройств.

До использования SNMP управляемое устройство должно быть сконфигурировано. Ему должны быть заданы IP-адрес, маска подсети, адрес маршрутизатора, адрес узла, на который отсылаются сообщения-о событиях и ряд параметров протокола SNMP.

3.2 Управление межсетевым экраном ССПТ-2

Рассматриваемый в данном пособии МЭ позволяет ознакомиться с различными способами как локального, так и удаленного подключения управляющих средств, а также с различными пользовательскими интерфейсами управления.

Для подключения технических средств управления в МЭ предусмотрены 3 физических интерфейса:

- КОНСОЛЬ – включает разъемы подключения монитора и клавиатуры
- COM – последовательный порт RS 232C.
- EthC – Ethernet-интерфейс управления.

Подчеркнем, что эти интерфейсы предназначены только для управления и никак не связаны с рабочими (фильтрующими) интерфейсами МЭ. То есть в МЭ ССПТ-2 реализован принцип внеполосного управления.

В соответствии с приведенной выше терминологией МЭ позволяет реализовать:

- Консольное управление;
- Управление через telnet (FNPtel);
- WEB-управление.

Наличие нескольких физических интерфейсов управления позволяет реализовать различные схемы связи МЭ с УК или консолью администратора.

A). Непосредственное подключение “консоли” к МЭ.

B). Локальное подключение “консоли” (терминала) к COM-порту МЭ.

C). Подключение УК к COM-порту МЭ с использованием стека TCP/IP.

D). Подключение УК к МЭ по сети Ethernet с использованием стека TCP/IP.

В качестве консоли может использоваться монитор и клавиатура (вариант A) или УК в режиме эмуляции терминала (вариант B).

Перечисленные варианты подключения различаются необходимыми техническими средствами, предварительными настройками и предоставляемыми возможностями.

Конфигурирование и управление работой МЭ осуществляется администратором в форме диалога. При этом обеспечивается возможность использования двух пользовательских интерфейсов управления:

- Интерфейс командной строки,

- WEB-интерфейс управления.

Первые два варианта (консольное управление) предоставляют доступ только к командному интерфейсу администратора. Остальные схемы позволяют использовать как командный, так и WEB-интерфейс администратора.

Использование Ethernet-управления (вариант D) требует предварительного конфигурирования МЭ (задание IP-адреса, маски подсети, адреса маршрутизатора, и др.), которое может быть осуществлено через консоль или COM-порт (варианты A, B).

При использовании подключения по варианту C необходимое конфигурирование осуществляется автоматически при установлении PPP-соединения.

Первый запуск МЭ всегда осуществляется через интерфейс командной строки и требует прохождения двух уровней авторизации:

- Авторизация в операционной системе МЭ,
- Авторизация пользователя МЭ ССПТ-2.

3.2.1 Непосредственное подключение консоли к МЭ

В качестве “консоли” используется монитор и клавиатура. Для подключения консоли необходимо выполнить следующие действия:

1. Подключить монитор к разъему “Console”, а клавиатуру к разъему “Kbd” МЭ.
2. Включить МЭ и монитор. По окончании загрузки ОС МЭ на монитор будет выведена информация о состоянии МЭ и приглашение операционной системы - **login:**
3. Ввести имя - **fnpsh_**и пароль - **FilterD**. При успешной системной авторизации на монитор будет выведена информации о версии командного интерфейса МЭ и приглашение – **Имя пользователя:**
4. Ввести имя пользователя **– admin** и пароль - **FilterD**. Добиться появления на экране подсказки “fnpsh”, означающей, что интерфейс командной строки готов к работе и ожидает ввода команд. (При данном варианте подключения WEB-интерфейс управления недоступен).

3.2.2 Локальное подключение “консоли” к COM-порту МЭ.

В качестве консоли (терминала) можно использовать УК с программой эмуляции терминала (Putty). При этом локальное подключение “консоли” осуществляется

соединением COM-портов УК и МЭ с помощью кабеля. Для определенности УК с запущенной программой эмуляции терминала будем называть далее терминалом.
Последовательный порт (RS-232) на УК должен иметь следующие настройки:
Скорость передачи **115200 бит/с;**
Биты данных – **8 бит**
Четность – **не проверяется**
Стоповые биты – **1 бит**
Управление потоком - **аппаратное**
Для локального подключение консоли к МЭ необходимо выполнить следующие операции:
3.2.2.1. Установить на УК программу эмуляции терминала и настроить ее параметры. В качестве примера рассмотрим настройку параметров программы Putty.

- Запустить программу "Putty" (Эмуляция терминала)
- Определить номер порта (Пуск-Панель управления-Система-Диспетчер устройств-COM порты).
- Установить в настройках Putty номер порта и укаазанные выше параметры порта.
- Нажать Open. Появится окно соединения.
- Нажать Ввод. Появится приглашение ОС МЭ
- Ввести имя **fnpsh** пароль **FilterD**. Появится приглашение экрана ССПТ-2.
- Ввести имя **admin** и пароль **FilterD**.
- Нажатием Enter добиться появления на экране подсказки "fnpsh", означающей, что интерфейс командной строки готов к работе и ожидает ввода команд. (При данном варианте подключения WEB-интерфейс управления недоступен).

1.0.1. 3.2.3. Подключение УК к COM-порту МЭ с использованием стека TCP/IP.

В данной лабораторной работе этот вариант подключения не используется.

3.2.4. Подключение УК к МЭ по сети Ethernet с использованием стека TCP/IP.

Для обеспечения возможности управления несколькими МЭ с одного УК, в МЭ предусмотрена возможность организации управления по сети Ethernet. Для этого в МЭ выделен специальный Ethernet-интерфейс ("Eth C"), предназначенный только для целей управления.

К управляющей сети кроме УК и одного или нескольких МЭ могут быть подключены серверы хранения регистрационных файлов.

Для подключения МЭ к управляющей сети необходимо использовать кабель ”витая пара” соответствующей категории.

Для организации управления по сети эту управляющую сеть следует предварительно сконфигурировать, то есть назначить IP-адреса и маски всем подключенным к сети устройствам, а также, при необходимости, назначить шлюз по умолчанию.

Как уже говорилось, активизацию управляющего Ethernet-интерфейса МЭ и назначение ему IP-адреса можно осуществить как из интерфейса командной строки, так и из WEB-интерфейса управления, подключившись к МЭ по любой из описанных выше схем подключения (пп. 3.2.1 – 3.2.3).

В интерфейсе командной строки для конфигурирования управляющего Ethernet-интерфейса предусмотрена группа команд **interface control xxx.** Ниже рассмотрены некоторые команды из этой группы:

- Назначение IP-адреса управляющему Ethernet-интерфейсу

`interface control address <IP-адрес>/<маска подсети>.`

Например, команда

```
fnpsh> interface control address 192.168.20.1/255.255.255.0
```

назначает управляющему Ethernet-интерфейсу IP-адрес 192.168.20.1 с маской подсети 255.255.255.0,

- Включение управляющего Ethernet-интерфейса

`interface control enable.`

Например, команда

```
fnpsh> interface control enable
```

устанавливает управляющий Ethernet-интерфейс в активное состояние.

- Вывод на экран состояния и параметров управляющего Ethernet-интерфейса

interface control show.

Например, команда

```
fnpsh> interface control show
```

выводит на экран терминала настройки и текущее состояние управляющего Ethernet-интерфейса.

С перечнем и форматом инструкций интерфейса командной строки можно ознакомиться, набрав команду **help**.

В WEB-интерфейсе конфигурирование управляющего Ethernet-интерфейса осуществляется заполнением соответствующих форм. Однако, по умолчанию, после первого запуска WEB-интерфейс управления МЭ выключен. Для активизации WEB-интерфейса управления необходимо выполнить команду

system web enable,

доступную только в режиме консольного управления.

При конфигурировании следует помнить, что при отсутствии или запрете шлюза по-умолчанию, доступ к управляющему Ethernet-интерфейсу возможен только из IP-подсети, образованной маской подсети в настройках управляющего Ethernet-интерфейса МЭ.

Процедура назначения IP-адреса сетевому интерфейсу УК определяется используемой на УК операционной системой.

Таким образом, для подключения УК к МЭ по сети Ethernet необходимо выполнить следующие действия:

3.2.4.1. Спланировать управляющую сеть Ethernet. Определить IP-адреса и маски подсетей всех подключаемых к ней устройств (интерфейсов).

3.2.4.2. Сконфигурировать управляющий интерфейс МЭ в соответствии с п. 3.2.4.1, подключившись к МЭ любым из описанных в пп. 3.2.1-3.2.3 способов и используя приведенные выше команды.

3.2.4.3. Подключить УК к МЭ по управляющей сети спланированной конфигурации.

Данный вариант подключения обеспечивает доступ как к командному, так и к WEB-интерфейсу управления (при условии выполнения команды **system web enable**).

Для доступа к WEB-интерфейсу следует запустить стандартный браузер и послать https-запрос по IP-адресу управляющего Ethernet-интерфейса МЭ.

Самостоятельная практическая работа (Работа N 2)

Цель работы

- Ознакомление со способами управления сетевыми устройствами.
- Получение практических навыков локального и удаленного управления сетевыми устройствами.
- Ознакомление с конкретными реализациями пользовательского интерфейса управления (командная строка, WEB-интерфейс).

Программа работы

1. Подключить COM-порт МЭ к COM-порту ПК.
2. Подключить управляющий интерфейс “Eth C” межсетевого экрана к сетевому адаптеру ПК с помощью кабеля и переходного адартера.
3. Включить ПК
4. Включить МЭ
5. Определить IP-адреса и маски сетевых интерфейсов ПК. Для подключения к МЭ выбрать интерфейс с приватным адресом. Записать его адрес и маску.
6. Определить свободные IP-адреса приватной подсети и выбрать адрес для управляющего интерфейса (Eth C) МЭ. Записать в отчет адрес и маску для EthC.
7. Выполнить локальное подключение “консоли” к COM-порту МЭ согласно п. 3.2.2. В качестве консоли использовать программу Putty.
8. Пройти двойную авторизацию, описанную в п. 3.2.1.
9. Командами МЭ установить на управляющем интерфейсе (Eth C) IP-адрес и маску, определенные в п.6. Команды приведены в п. 3.2.4.
10. Командами МЭ убедиться, что управляющий Ethernet-интерфейс сконфигурирован. Занести в отчет схему подключения к МЭ с указанием используемых портов, интерфейсов и IP-адресов.
11. Командами МЭ добавить нового пользователя МЭ (Piter) без указания привилегий. Убедиться, что новый пользователь добавлен. Записать в отчет использованные команды.
12. Завершить сеанс работв пользователя admin с командным интерфейсом. Заисать в отчет использованные команды.

    Подключение УК к WEB-интерфейсу МЭ.

13. Запустить на УК браузер. Создать https–запрос к МЭ по адресу EthC (п.9).
14. При необходимости подтвердить доверие к соединению.
15. Войти в Web-интерфейс МЭ под именем Piter. Ввести пароль.
16. Инициировать Останов фильтра. Описать в отчете совершенные действия и объяснить результат.
17. Завершить работу пользователя Piter с WEB-интерфейсом управления.
18. Получить доступ к WEB-интерфейсу под именем admin пароль FilterD.
19. Изменить настройки МЭ: задать имена интерфейсов, включить систему регистрации.
20. Вывести на экран файл регистрации событий. Для этого последовательно выбрать “Регистрация” - “События” – “Показать”. Найти записи, регистрирующие действия, осуществленные в рамках данной работы.
21. Скопировать записи в файл (<фамилия>_lab1.txt) и пояснить.

22. Завершить сеанс работы пользователя admin с WEB-интерфейсом управления. Выключить МЭ.

В отчете привести

1. Схему подключения УК к МЭ через COM-порт и по сети Ethernet с указанием IP-адресов и обозначением всех задействованных интерфейсов устройств.
2. Команды конфигурирования МЭ с комментариями.
3. Описания действий и результаты по пп. 5 – 22.
4. Распечатку файла регистрации событий (<фамилия>_lab1.txt) с записями действий, осуществленных в рамках данной работы. Отметить регистрацию действий по п.5-22.