

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский национально-исследовательский государственный университет
имени Н.Г. Чернышевского»

С.А. Куркин, А.А. Бадарин, А.В. Андреев, Ю.И. Левин

**АДМИНИСТРИРОВАНИЕ УПРАВЛЯЕМЫХ
КОММУТАТОРОВ**

**Часть 3. Конфигурирование портов и работа с таблицей
коммутации.**

Учебно-методическое пособие

Саратов – 2016

Администрирование управляемых коммутаторов

Цель работы:

Получение навыков настройки портов коммутатора, изучение технологии зеркалирования портов (Port Mirroring) и принципов работы со статической таблицей перенаправления коммутатора.

Оглавление

1. Типовой комплект учебного оборудования «Корпоративные компьютерные сети».....	3
1.1. Описание комплекта	3
2. Коммутаторы D-Link серии DES-3200	4
2.1. Управление коммутатором D-Link серии DES-3200	4
2.2. Разделы меню управления	10
3. Коммутаторы D-Link серии DES-3810	14
3.1. Управление коммутатором	14
4. Некоторые теоретические сведения	21
4.1 Утилиты мониторинга сети	21
5. Задания	24
5.1. Конфигурирование портов и работа с таблицей коммутации.	24

1. Типовой комплект учебного оборудования «Корпоративные компьютерные сети»

1.1. Описание комплекта

Комплект состоит из двух межсетевых экранов Cisco ASA 5505, одного коммутатора третьего уровня D-Link DES-3810-28, двух управляемых коммутаторов второго уровня D-Link DES-3200-10, двух неуправляемых коммутаторов D-Link DES-1005A, двух беспроводных маршрутизаторов D-Link DIR-300, четырёх компьютеров и коммутационной панели, которая позволяет формировать необходимую топологию сети. На компьютерах установлена операционная система ArchLinux. Все компьютеры имеют три проводных сетевых интерфейса (интегрированный в материнскую плату и на шине PCI) и один беспроводной. Внешние сетевые интерфейсы (eth1 и eth2) не поддерживают технологию MDI/MDI-X, поэтому соединение двух компьютеров напрямую возможно только накрест обжатым патч-кордом. Внешний вид комплекта представлен на рисунке 1.1.



Рисунок 1.1. Внешний вид комплекта

Для входа на рабочих станциях используйте имя пользователя «*root*» и пароль «*qwerty*». Разводка портов коммутационной панели приведена на самой панели. Ни один сетевой адаптер компьютера не включен в IP-подсеть. Сделано это для того, чтобы студенты самостоятельно отработывали навыки по настройке сетевых интерфейсов.

2. Коммутаторы D-Link серии DES-3200

2.1. Управление коммутатором D-Link серии DES-3200

Коммутаторы D-Link серии DES-3200 включают следующие модели: DES-3200-10, DES-3200-18, DES-3200-26, DES-3200-28. Управление коммутаторами данной серии (далее просто коммутаторами) возможно четырьмя различными способами:

- локально через последовательный порт коммутатора RS-232 (diagnostics port);
- через сеть по протоколу telnet;
- через сеть по протоколу http с использованием web-интерфейса;
- через сеть по протоколу SNMP.

В рамках лабораторной работы предполагается использование web-интерфейса. В любом случае, первоначальное назначение IP-адреса коммутатору должно осуществляться через консоль, подключенную к diagnostics-порту. Для этого необходимо подключить COM-кабель к коммутатору через COM-порт. Далее использовать следующую команду:

```
screen/dev/ttyS0
```

После подключения к консоли на экране появится запрос учётных данных. Если запрос не появляется, нажмите Enter 1-2 раза. Заводские настройки предполагают имя пользователя и пароль равными «admin». По умолчанию (заводские настройки) коммутатору назначен IP-адрес 10.90.90.90. Для назначения другого IP-адреса используйте следующую команду:

```
config ipif System ipaddress IP-адрес/маска_подсети
```

Маска подсети может задаваться либо в виде IP-адреса, либо числом, задающим количество бит, отводимых под сеть. Пример:

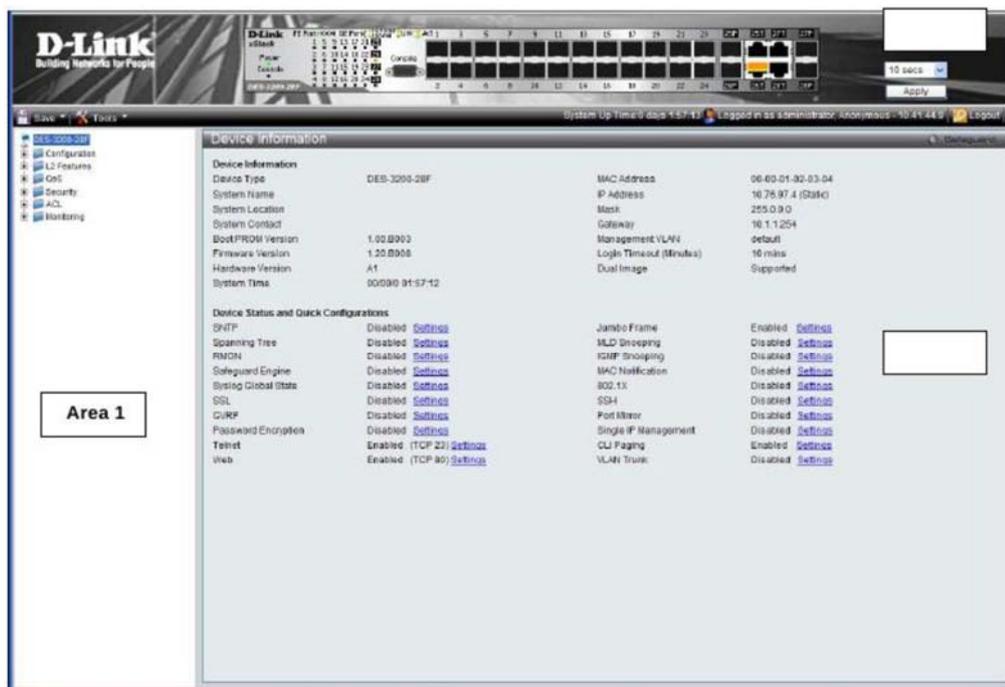
```
config ipif System ipaddress 192.168.1.5/255.255.255.0
```

```
config ipif System ipaddress 192.168.1.5/24
```

После выполнения любой команды необходимо выполнить команду *save* для сохранения заданных изменений в NVRAM коммутатора. После назначения коммутатору желаемых настроек IP-протокола можно задействовать web-интерфейс управления. Для этого на машине, которая включена в ту же IP-подсеть, что и коммутатор (любая машина в лабораторном стенде), необходимо в web-браузере ввести IP-адрес коммутатора. Появится окно аутентификации пользователя .



После аутентификации будет осуществлен переход на страницу управления .



Развернутое меню управления коммутатором в области 1 имеет следующую структуру:

- System Configuration (Настройка)
 - System Information (Информация о системе)
 - Port Configuration (Настройки порта)
 - Jumbo Frame (Настройки джамбограмм)
 - Serial Port Settings (Настройки последовательного порта)
 - System Log Configuration (Настройки журналирования)
 - System Log (Системный журнал)
 - User Accounts (Пользовательские учётные записи)
 - Time Range Settings (Настройки временного диапазона)

- Device Information (Информация об устройстве)
- Static ARP Settings (Статические записи ARP)
- Password Encryption (Шифрование паролей)
- CLI Paging Settings (Настройка страницы текстового интерфейса)
- Firmware Information (Информация о прошивке)
- Management (Управление)
 - ARP Spoofing Prevention Settings (Настройки предотвращения ARP Spoofing)
 - Gratuitous ARP (Самообращённый ARP)
 - IPv6 Neighbor Settings (Настройки IPv6-соседей)
 - IP Address Settings (Настройки IP-адреса)
 - Single IP Management (Настройки технологии SIM)
 - SNMP Settings (Настройки протокола SMTP)
 - Telnet Settings (Настройки telnet-доступа)
 - Web Settings (Настройки Web-доступа)
- L2 Features (Возможности 2 уровня)
 - 802.1Q Static VLAN (Настройки протокола 802.1Q)
 - 802.1v Protocol VLAN (Настройки протокола 802.1v)
 - GVRP Settings (Настройки анонсирования VLAN)
 - MAC-based VLAN Settings (Настройки VLAN на основе MAC-адресов)
 - PVID Auto Assign Settings (Настройка автоназначения PVID)
 - VLAN Trunk Settings (Настройки магистральных VLAN)
 - Asymmetric VLAN Settings (Настройки асимметричных VLAN)
 - Q-in-Q (Настройки двойного тегирования)
 - Layer2 Protocol Tunneling Settings (Настройки туннелирования протокола 2 уровня)
 - Spanning Tree (Настройки протокола связующего дерева)
 - Port Trunking (Создание магистральных каналов)
 - LACP Port Settings (Настройка протокола LACP)
 - MAC Address Aging Time (Настройки времени устаревания MAC-адресов)
 - MAC Notification Settings (Настройки уведомлений о MAC-адресах)
 - IGMP Snooping (Настройки анализа IGMP-трафика)
 - MLD Snooping Settings (Настройки анализа MLD-трафика)
 - Traffic Segmentation (Сегментация трафика)
 - Loopback Detection Settings (Настройки обнаружения петель)
 - Forwarding & Filtering (Настройки перенаправления и фильтрации)

- LLDP (Настройки протокола обнаружения канального уровня)
- Ethernet OAM (Настройки протокола 802.3ah–эксплуатация, администрирование и обслуживание канала)
- Connectivity Failure Management (Настройки управления качеством физического канала)
- ERPS Settings (Настройки защищённого кольца Ethernet)
- L3 Features (Возможности 3 уровня)
 - IPv6 Interface Settings (Настройки IPv6-интерфейса)
 - IPv6 Route Settings (Настройки IPv6-маршрута)
- QoS (Управление качеством сервиса)
 - 802.1p Default Priority (Приоритеты 802.1p по умолчанию)
 - 802.1p User Priority (Пользовательская настройка приоритетов 802.1p)
 - Bandwidth Control (Управление полосой пропускания)
 - Queue Bandwidth Control Settings (Управление пропускной способностью очереди)
 - Traffic Control (Управление трафиком)
 - DSCP Map Settings (Отображение дифференцированных служб)
 - QoS Scheduling Settings (Настройки распределения важности очередей)
 - Priority Mapping (Отображение приоритетов)
 - TOS Mapping (Отображение типа сервиса)
- ACL (Списки контроля доступа)
 - ACL Configuration Wizard (Мастер настройки ACL)
 - Access Profile List (Профили доступа)
 - CPU Access Profile List (Списки контроля доступа к процессору)
 - ACL Finder (Поисковик ACL)
 - ACL Flow Meter (Настройки связи ACL с пропускной способностью канала)
- Security (Параметры безопасности)
 - 802.1X (Настройки протокола 802.1X)
 - RADIUS Attributes Assignment (Настройки назначения атрибутов протокола RADIUS)
 - MAC-based Access Control (контроль доступа на основе MAC-адресов)
 - DHCP Server Screening Settings (Настройки экранирования сервера DHCP)Safeguard Engine (управление механизмом собственной безопасности)
 - Access Authentication Control (Управление аутентификацией управляющих интерфейсов)
 - SSL Settings (Настройки SSL)
 - SSH (Настройки SSH)
 - Trusted Host (Выбор узлов для управления)
 - DoS Prevention Settings (Настройки предотвращения DoS-атак)

- IP-MAC-Port Binding (Связь IP-MAC-Port)
- Port Security (Безопасность порта)
- Network Application (Сетевые приложения)
 - DHCP Relay (Ретрансляция DHCP)
 - DHCP Auto Configuration Settings (Настройки сервера DHCP)
 - PPPoE Circuit ID Insertion Settings (Настройки добавления поля Circuit-ID в кадры PPPoE)
 - SNTP Settings (Настройки протокола SNTP)
- OAM
 - Ethernet OAM (Журнал событий и статистика операций OAM)
- Monitoring (Просмотр состояния)
 - CPU Utilization (Загрузка процессора)
 - Port Utilization (Загрузка порта)
 - Memory Utilization (Загрузка памяти)
 - Packets (Количество пакетов)
 - Errors (Количество ошибок)
 - Packet Size (Количество пакетов определённого размера)
 - Port Mirror (Настройки зеркалирования портов)
 - Ping Test (Встроенная утилита Ping)
 - Trace Route (Утилита traceroute)
 - Cable Diagnostics (Диагностика кабеля)
 - Port Access Control (Состояние доступа к порту)
 - Browse ARP Table (Таблица ARP)
 - Browse VLAN (Таблица VLAN)
 - IGMP Snooping (Состояние анализа IGMP)
 - LLDP (Статистика и информация LLDP)
 - Connectivity Fault Management (Состояние и статистика протокола CFM)
 - MAC-based Access Authentication State (Состояние аутентификации на базе MAC-адресов)
 - Browse Session Table (Таблица сеансов)
 - MAC Address Table (Таблица перенаправления)
- Save and Tools (Сохранение и утилиты)
 - Save Configuration (Сохранение настроек)
 - Save Log (Сохранение журнала)
 - Save All (Сохранение всего)
 - Configuration File Upload & Download (Загрузка и скачивание файла настройки)
 - Upload Log File (Загрузка файла журнала)
 - Reset (Сброс)
 - Download Firmware (Скачивание прошивки)
 - Reboot System (Перезагрузка)

При начальной загрузке страницы и при нажатии на корневую ссылку «DES-3200» отображается информация об устройстве и режимах работы устройства.

Device Information			
Device Information			
Device Type	DES-3200-26	MAC Address	00-32-26-63-10-20
System Name		IP Address	10.80.90.80 (Static)
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	1.00.B002	Management VLAN	default
Firmware Version	1.10.B014	Login Timeout (Minutes)	10 mins
Hardware Version	A1	Dual Image	Supported
System Time	00:00:00 00:01:47		
Device Status and Quick Configurations			
SNTP	Disabled Settings	Jumbo Frame	Enabled Settings
Spanning Tree	Disabled Settings	MLD Snooping	Disabled Settings
RMON	Disabled Settings	IGMP Snooping	Disabled Settings
SafeGuard Engine	Disabled Settings	MAC Notification	Disabled Settings
Syslog Global State	Enabled Settings	802.1X	Enabled Settings
SSL	Disabled Settings	SSH	Disabled Settings
OSRP	Disabled Settings	Port Mirror	Disabled Settings
Password Encryption	Disabled Settings	Single IP Management	Disabled Settings
Telnet	Enabled (TCP 23) Settings	CLI Paging	Enabled Settings
Web	Enabled (TCP 80) Settings	VLAN Trunk	Disabled Settings

Полное описание всех пунктов данного окна приведено в таблице.

Пункт	Назначение
Device Type	Отображает тип (коммутатор, коммутатор уровня 3, маршрутизатор) и модель устройства
System Name	Позволяет задать имя коммутатора, которое будет отображаться в меню веб-браузера при управлении коммутатором по Web или на топологии сети при управлении коммутатором по SNMP-протоколу
System Location	Позволяет задать расположение коммутатора
System Contact	Позволяет задать имя человека, ответственного за обслуживание коммутатора
Boot PROM Version	Отображает версию загрузчика ОС коммутатора
Firmware Version	Отображает версию ОС коммутатора («прошивки»)
Hardware Version	Отображает версию аппаратной части коммутатора
System Time	Отображает показание системных часов
MAC Address	Отображает MAC-адрес коммутатора
IP Address	Отображает IP-адрес коммутатора
Mask	Отображает маску адреса коммутатора
Gateway	Отображает настроенный шлюз по умолчанию
Management VLAN	Отображает имя виртуальной сети VLAN для управления. Управлять устройством можно только через те порты, которые входят в этот VLAN
Login Timeout	Отображает время неактивности (в минутах), после которого произойдет отключение от интерфейса управления
Dual Image	Отображает доступность функции дублирования загрузочного образа системы (позволяет восстановить работу коммутатора при повреждении основного образа)
SNTP	Отображает состояние протокола SNTP
Spanning Tree	Отображает, включен или отключен протокол Spanning Tree

RMON	Позволяет включить или отключить управление по RMON
Safeguard engine	Отображает состояние технологии самозащиты Safeguard
Syslog Global State	Позволяет включить или отключить системный журнал
SSL	Позволяет включить или отключить шифрование HTTP-трафика до интерфейса управления
GVRP	Позволяет включить или отключить анонсирование доступных на портах VLAN
Password Encryption	Позволяет включить или отключить шифрование паролей
Telnet	Позволяет включить или отключить управление по Telnet
Web	Позволяет включить или отключить управление по Web
MLD Snooping	Позволяет включить или отключить анализ трафика протокола MLD
IGMP Snooping	Позволяет включить или отключить анализ трафика протокола IGMP
MAC Notification	Отображает, включено или отключено уведомление о MAC-адресах
802.1x	Позволяет включить или отключить протокол IEEE 802.1x
SSH	Позволяет включить или отключить управление по SSH
PortMirror	Отображает, включено или отключено зеркалирование портов
Single IP Management	Отображает, включено или отключено управление с помощью технологии SIM
CLI Paging	Позволяет настроить способ разбиения на страницы текстового интерфейса
VLAN Trunk	Позволяет включить или отключить поддержку магистральных VLAN

Таблица 2.1. Описание всех пунктов окна “Device Information”.

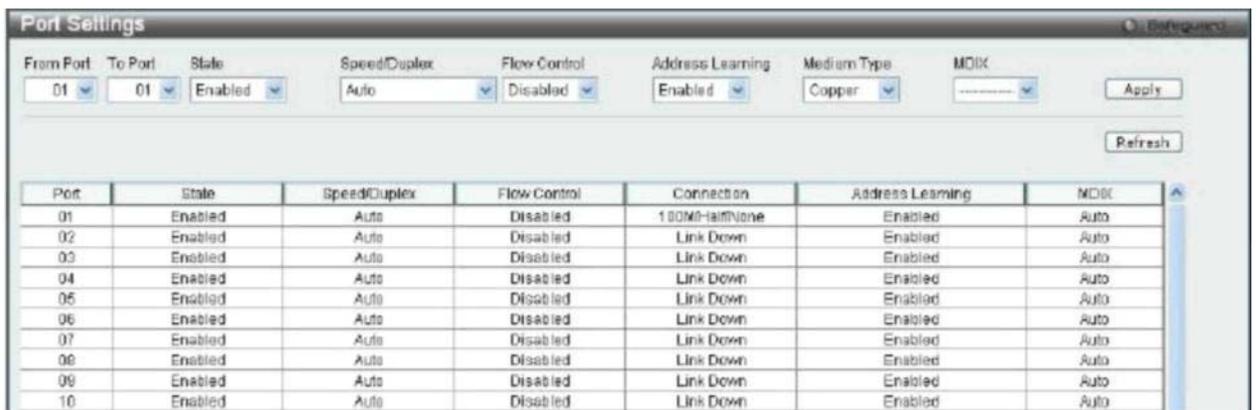
После изменения какого-либо пункта меню необходимо нажать кнопку «Apply», чтобы настройки вступили в силу.

ВНИМАНИЕ: После изменения любых настроек коммутатора, необходимо выполнить команду на сохранение (раздел «SaveChanges»), если Вы хотите, чтобы настройки остались после выключения питания и перезагрузки коммутатора.

2.2. Разделы меню управления

2.2.1. Раздел Port Configuration

2.2.1.1. Раздел Port Settings

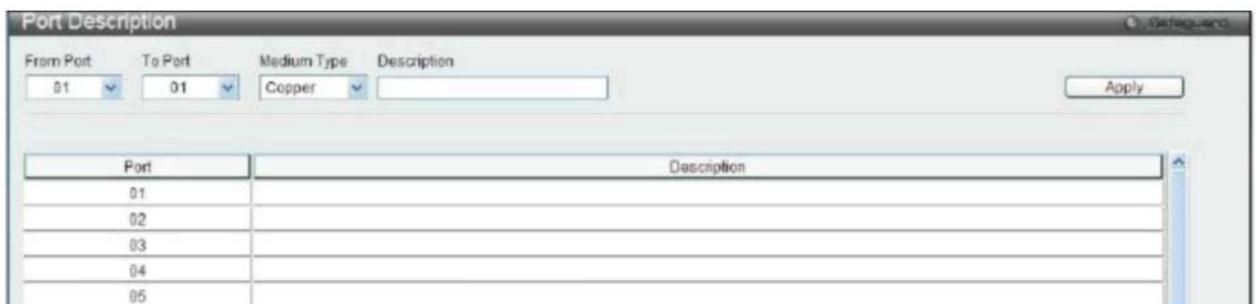


Позволяет управлять настройками портов

- From Port - начальный номер порта
- To Port - конечный номер порта. К выбранному диапазону портов будут применены дальнейшие настройки
 - State - состояние порта (включен/выключен)
 - Speed/Duplex - скорость порта и настройки дуплекса
 - Flow Control - управление потоком
- Address Learning - включить или выключить процедуры изучения адресов алгоритма прозрачного моста
 - Medium Type - тип среды (применяется для комбо-портов)
 - MDIX - полярность порта

2.2.1.2. Раздел Port Descriptions

Позволяет задать описания портов



- From Port - начальный номер порта
- To Port - конечный номер порта. К выбранному диапазону портов будут применены дальнейшие настройки
- Medium Type - тип среды (применяется для комбо-портов)
- Description - описание

2.2.1.3. Раздел Port Error Disabled

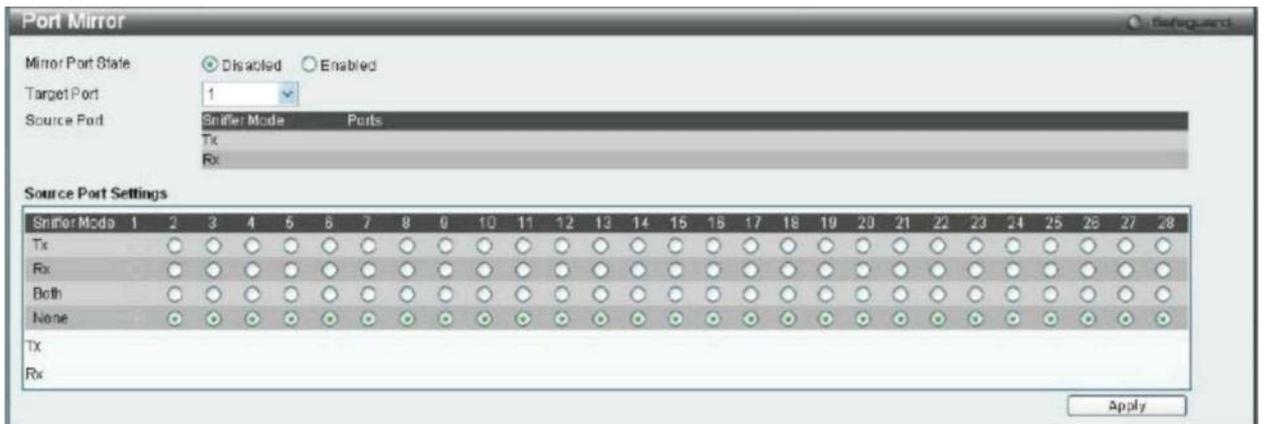
Отображает порты, отключенные в результате системной ошибки (обнаружение петли STP или административное отключение порта)



- Port - номер порта
- Port State - состояние порта
- Connection Status - состояние соединения
- Reason - причина

2.2.2. Раздел Port Mirror

Позволяет управлять функцией зеркалирования портов



- Mirror Port State - активность функции
- Target Port - выходной порт
- Source Port - прослушиваемые порты
- Sniffer Mode - настройка прослушиваемых портов и направления трафика
 - Tx - только исходящий трафик
 - Rx - только входящий трафик
 - Both - оба направления
 - None - не прослушивать

2.2.3. Раздел Forwarding & Filtering

2.2.3.1. Раздел Unicast Forwarding Settings



Позволяет управлять статическими записями таблицы коммутации

- VLAN ID - VLAN, в котором действительна запись
- MAC Address - MAC-адрес узла

- Port - порт, на котором находится узел

2.2.4. Раздел PingTest

Позволяет выполнить проверку доступности узла

The image shows two overlapping windows from a network management application. The top window is titled "Reboot System" and contains a dialog box asking "Do you want to save the settings?" with "Yes" selected. Below it, a warning states "If you do not save the settings, all changes made in this session will be lost." and a "Reboot" button. The bottom window is titled "Ping Test" and contains an "IPv4 Ping Test" section. It instructs the user to "Enter the IP address of the device or station you want to ping, then click Start." The form includes a "Target IP Address" field with "0.0.0.0", a "Repeat Pinging for" section with "infinite times" selected, and a "Timeout" field with "1" (1-99 sec). A "Start" button is located at the bottom right of the window.

- Target IP Address –адрес узла
- Repeat Pinging For –количество повторов
- Timeout –задержка ожидания ответа

3. Коммутаторы D-Link серии DES-3810

3.1. Управление коммутатором

Управление коммутаторами данной серии (далее просто коммутаторами) возможно четырьмя различными способами:

- локально через последовательный порт коммутатора RS-232 (подписан «Console», выполнен в формате гнезда RJ-45);
- локально через порт управления коммутатора (подписан «Management», выполнен в формате гнезда RJ-45);
- через сеть по протоколу telnet;
- через сеть по протоколу http с использованием web-интерфейса;
- через сеть по протоколу SNMP.

В рамках лабораторных работ предполагается использование web-интерфейса. В любом случае, первоначальное назначение IP-адреса коммутатору должно осуществляться через консоль, подключенную к RS-232-порту либо через порт Management. Для работы с портом RS-232 необходимо подключить COM-кабель к коммутатору через Console-порт. Далее использовать следующую команду:

```
screen /dev/ttyS0 115200
```

После подключения к консоли на экране появится запрос учётных данных. Если запрос не появляется, нажмите Enter 1-2 раза. Заводские настройки предполагают имя пользователя и пароль пустыми. По умолчанию (заводские настройки) коммутатору назначен IP-адрес 10.90.90.90. Для назначения другого IP-адреса используйте следующую команду:

```
config ipif System ipaddress IP-адрес/маска_подсети
```

Маска подсети может задаваться либо в виде IP-адреса, либо числом, задающим количество бит, отводимых под сеть. Пример:

```
config ipif System ipaddress 192.168.1.5/255.255.255.0
```

```
config ipif System ipaddress 192.168.1.5/24
```

После выполнения любой команды необходимо выполнить команду *save* для сохранения заданных изменений в NVRAM коммутатора.

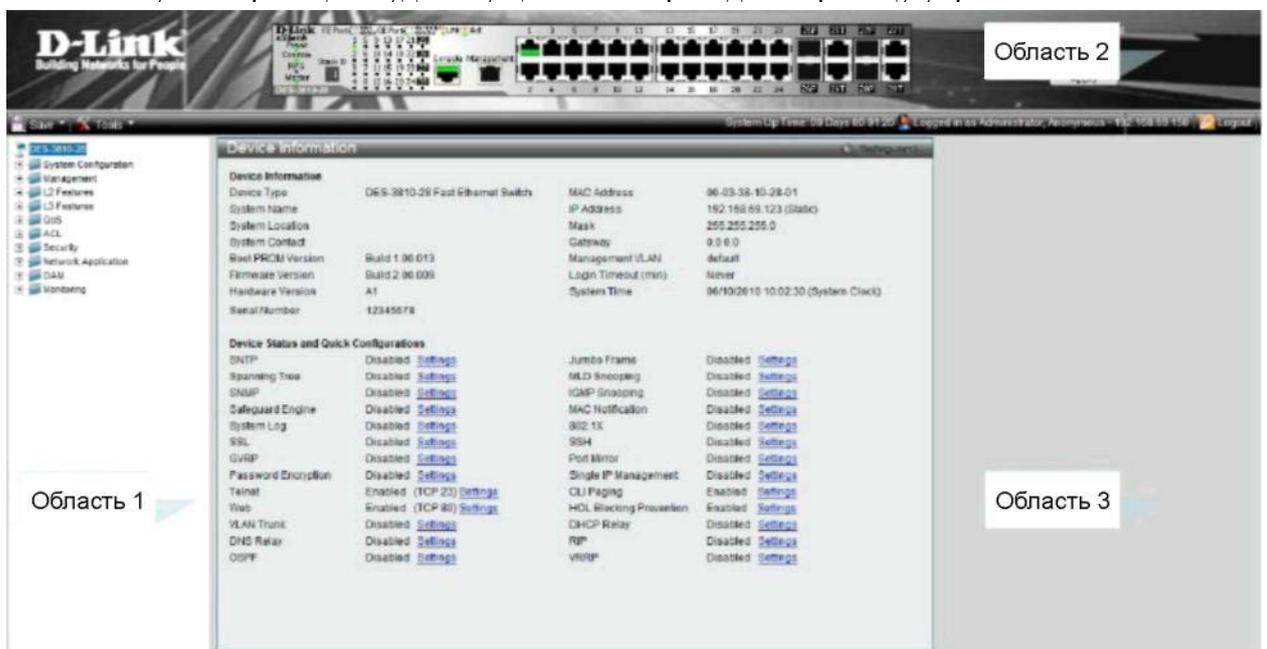
Для работы через management-порт соедините этот порт коммутатора и сетевой интерфейс компьютера патч-кордом. Порт по умолчанию имеет адрес 192.168.0.1/255.255.255.0. Сменить адрес порта можно следующими командами (в консольном интерфейсе):

```
config out_band_ipif ipaddress <адрес>
```

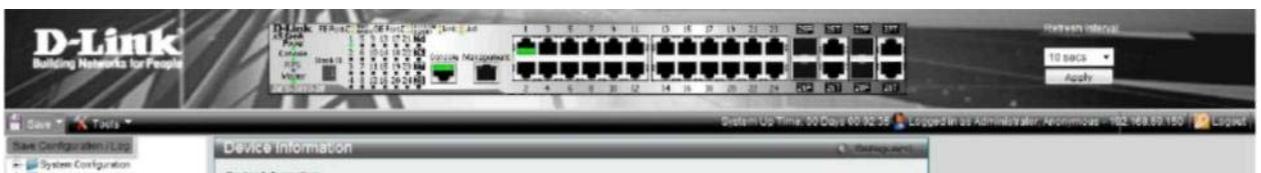
После назначения коммутатору желаемых настроек IP-протокола можно задействовать web-интерфейс управления. Для этого на машине, которая включена в ту же IP-подсеть, что и коммутатор (любая машина в лабораторном стенде), и подключена к любому порту коммутатора, либо к порту Management, необходимо в web-браузере ввести IP-адрес коммутатора или порта Management. Появится окно аутентификации пользователя.



После аутентификации будет осуществлен переход на страницу управления.



На границе 2 области расположено выпадающее меню.



Оно содержит следующие пункты:

- Save (Сохранение)
 - o Save Configuration/Log (Сохранение настроек или журнала)
- Tools (Инструменты)
 - o Download Firmware (Скачивание прошивки)
 - o Upload Firmware (Загрузка прошивки)
 - o Download Configuration (Скачивание конфигурации)

- o Upload Configuration (Загрузка конфигурации)
- o Upload Log File (Загрузка журнала)
- o Reset (Сброс настроек)
- o Reboot System (Перезагрузка)

Развернутое меню управления коммутатором в области 1 имеет следующую структуру:

- System Configuration (Настройка)
 - o Device Information (Информация об устройстве)
 - o System Information Settings (Информация о системе)
 - o Port Configuration (Настройка портов)
 - o Serial Ports Settings (Настройка последовательного порта)
 - o Warning Temperature Settings (Настройка критической температуры)
 - o System Log Settings (Настройка системного журнала)
 - o Time Range Settings (Настройка временных периодов)
 - o Time Settings (Настройка часов)
 - o User Account Settings (Управление учётными записями пользователей)
- Management (Управление)
 - o ARP (Настройки ARP)
 - o Gratuitous ARP (Настройки самонаправленного ARP)
 - o IPv6 Neighbor Settings (Настройки соседей IPv6)
 - o IP Interface (Настройки IP)
 - o Management Settings (Настройки работы коммутатора)
 - o Out of Band Management Settings (Настройки порта Management)
 - o Session Table (Таблица сеансов управления)
 - o Single IP Management (Настройки функции SIM)
 - o SNMP Settings (Настройки SNMP)
 - o Telnet Settings (Настройки Telnet)
 - o Web Settings (Настройки Web-интерфейса)
- L2 Features (Возможности 2 уровня)
 - o VLAN (802.1Q) (Настройки виртуальных локальных сетей 802.1Q)
 - o QinQ (настройки вложенного тегирования)
 - o Layer 2 Protocol Tunneling Settings (Настройки протокола туннелирования 2 уровня)
 - o Spanning Tree Protocol (STP) (Настройки связующего дерева STP)

- o Link Aggregation (Объединение каналов)
- o FDB (Таблица коммутации)
- o L2 Multicast Control (Управление групповым вещанием)
- o Multicast Filtering (Фильтрация группового вещания)
- o ERPS Settings (Настройки защищённого кольца коммутации Ethernet)
- o Local Loopback Port Settings (Настройки интерфейса локальной петли)
- o Link Layer Discovery Protocol (LLDP) (Настройки протокола обнаружения канального уровня)
- L3 Features (Возможности 3 уровня)
 - o IPv4 Static/DefaultRouteSettings(Настройки статической маршрутизации IPv4)
 - o IPv4 RouteTable(Таблица маршрутизации IPv4)
 - o IPv6 Static/DefaultRouteSettings(Настройки статической маршрутизации IPv6)
 - o IPv6 RouteTable(Таблица маршрутизации IPv6)
 - o PolicyRouteSettings(Настройки маршрутизации по политикам)
 - o IPForwardingTable(Таблица перенаправления IP)
 - o RoutePreferenceSettings(Настройки предпочтительности маршрутов)
 - o ECMPAlgorithmSettings(Настройки алгоритма ECMP)
 - o RouteRedistributionSettings(Настройки распространения маршрутной информации)
 - o OSPF (Настройки протокола OSPF)
 - o RIP (Настройки протокола RIP)
 - o VRRP (Настройки протокола VRRP)
 - o MD5 Settings (Настройки хеширования MD5)
- QoS(Управление качеством сервиса)
 - o 802.1 p Settings (Настройки протокола 802.1 p)
 - o Bandwidth Control (Управление полосой пропускания)
 - o Traffic Control Settings (Настройки контроля трафика)
 - o DSCP (Настройки дифференцированного обслуживания)
 - o HOL Blocking Prevention (Предотвращение блокирования очереди)
- ACL (Списки контроля доступа)
 - o ACL Configuration Wizard (Мастер настройки ACL)
 - o Access Profile List (Профили доступа)
 - o CPU Access Profile List (Списки контроля доступа к процессору)
 - o ACL Finder (Поисковик ACL)
 - o ACL Flow Meter (Настройки связи ACL с пропускной способностью канала)
- Security (Параметры безопасности)

- o 802.1X (Настройки протокола 802.1X)
- o RADIUS (Настройки серверов RADIUS)
- o IP-MAC-Port Binding (IMPB) (Настройки привязки IP-MAC-номер порта)
- o MAC-Based Access Control (Контроль доступа на базе MAC-адресов)
- o Web-based Access Control (WAC) (Контроль доступа к веб-интерфейсу)
- o Compound Authentication (Комбинированная аутентификация)
- o Port Security (Безопасность порта)
- o ARP Spoofing Prevention Settings (Настройки защиты от атаки ARP Spoofing)
- o BPDU Attack Protection (Настройки защиты от атаки на BPDU)
- o Loopback Detection Settings (Настройки обнаружения петель)
- o Traffic Segmentation Settings (Настройки разделения трафика)
- o NetBIOS Filtering Settings (Настройки фильтрации протокола NetBIOS)
- o DHCP Server Screening (Настройки экранирования DHCP-сервера)
- o Access Authentication Control (Настройки аутентификации доступа)
- o SSL Settings (Настройки SSL)
- o Secure Shell (SSH) (Настройки SSH)
- o Trusted Host Settings (Настройки узлов управления)
- o Safeguard Engine Settings (Настройки механизма самозащиты)
- Network Application (Сетевые службы)
 - o DHCP (Сервер DHCP)
 - o Domain Name System (DNS) (Переносчик DNS)
 - o PPPoE Circuit ID Insertion Settings (Настройки подстановки поля Circuit-ID в PPPoE-пакеты)
 - o RCP Server Settings (Настройки сервера RCP)
 - o SMTP Settings (Настройки почтовых уведомлений)
 - o SNTP (Настройки синхронизации времени)
 - o Flash File System Settings (Настройки файловой системы флеш-диска)
- OAM (Методы доступа к объектам)
 - o Connectivity Fault Management (CFM) (Настройки протокола CFM)
 - o Ethernet OAM (Настройки процедур обслуживания и эксплуатации Ethernet)
 - o Cable Diagnostics (Диагностика кабеля)
- Monitoring (Просмотр состояния)
 - o Utilization (Загруженность)

- o Statistics (Статистика)
- o Mirror (Зеркалирование портов)
- o sFlow (Отправка информации о потоках трафика)
- o Ping Test (Утилита ping)
- o Trace Route (Утилита traceroute)
- o Device Environment (физические характеристики устройства)

Многие пункты меню повторяют соответствующие пункты меню коммутаторов серии DES-3200. В данной главе будут описаны только пункты, специфичные для коммутатора DES-3810-28.

При начальной загрузке страницы и при нажатии на корневую ссылку «DES-3810-28» отображается информация об устройстве и режимах работы устройства. Данное меню идентично меню коммутаторов D-Link серии DES-3200



Дополнительно присутствуют следующие пункты:

Пункт	Назначение
DNS Relay	Позволяет управлять ретранслятором DNS-запросов
DHCP Relay	Позволяет управлять ретранслятором DHCP-запросов
RIP	Позволяет управлять протоколом динамической маршрутизации RIP
OSPF	Позволяет управлять протоколом динамической маршрутизации OSPF

HOL Blocking Prevention	Позволяет управлять функцией предотвращения падения производительности коммутатора из-за невозможности доставить кадры из буфера порта, следующие за кадром, который не может быть доставлен по назначению из-за занятости порта назначения
VRRP	Позволяет управлять протоколом резервирования маршрутизатора VRRP

ВНИМАНИЕ: После изменения любых настроек коммутатора, необходимо выполнить команду на сохранение (меню «Save → Save Configuration/Log»), если Вы хотите, чтобы настройки остались после выключения питания и перезагрузки коммутатора.

4. Некоторые теоретические сведения.

4.1 Утилиты мониторинга сети

Ниже приведён ряд утилит, использующихся в операционных системах семейства Linux для работы с сетью.

ping

Используется для проверки соединения с удаленным узлом. Утилита Ping использует пакеты эхо-запроса (echo request) и эхо-ответа (echo reply) протокола ICMP (Internet Control Message Protocol) для проверки доступности и работоспособности определенного узла TCP/IP. Действует посредством посылки ICMP пакетов и ожидания ответа в течение 1 секунды (значение по умолчанию). На экран выводится время в миллисекундах, затраченное на ожидание отклика.

Синтаксис командной строки:

ping IP-address или DNS-имя удаленного хоста

Пример:

```
ping 193.233.81.1
PING 193.233.81.1 (193.233.81.1): 56 data bytes
64 bytes from 193.233.81.1: icmp_seq=0 ttl=63 time=83.716 ms
64 bytes from 193.233.81.1: icmp_seq=6 ttl=63 time=1.949 ms
64 bytes from 193.233.81.1: icmp_seq=7 ttl=63 time=31.293 ms
^C
--- 193.233.81.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.949/18.160/83.716/26.597 ms
```

В поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного узла и возвращается на ваш узел. Поле ttl указывает время жизни пакета. После приостановки выполнения утилиты она выдает статистику: сколько пакетов послано, сколько получено и утеряно, время задержки (минимальное, среднее и максимальное).

Вместо IP-адреса хоста может быть указан широковещательный адрес. В этом случае результатом работы утилиты будет список узлов, откликнувшихся на запрос. Откликнутся все узлы сети, активные в настоящий момент и имеющие IP-адрес, соответствующий указанной маске.

tcpdump

Одним из мощных средств анализа всей сетевой активности является утилита tcpdump. Она переводит сетевой интерфейс в режим приема всех пакетов (promiscuous) и выводит информацию на экран. В Linux такое переключение возможно только для суперпользователя, то есть для полноценного использования tcpdump необходимо

зарегистрироваться под пользователем root. На других системах требования немного другие и они представлены в документации к tcpdump.

Синтаксис командной строки tcpdump следующий: *tcpdump* [*<опции...>*] *<выражение фильтра>*

Наиболее используемые опции tcpdump:

-c *<число пакетов>*

Сколько пакетов считать. После считывания последнего пакета, tcpdump завершает работу. Например, «*tcpdump -c 50*» считывает только 50 пакетов. Если этот параметр не указывается, то будут считываться все пакеты, пока работа tcpdump не будет завершена комбинацией клавиш Ctrl+C.

-i *<интерфейс>*

На каком интерфейсе осуществлять съём информации. Например, «*tcpdump -i eth1*» осуществляет съём данных на втором ethernet-интерфейсе eth1. Данная опция полезна, когда на используемом компьютере имеются 2 и более сетевых карт.

-s *<число байт>*

Сколько байт начала каждого пакета считывать. По умолчанию используется значение 68 байт. Этого должно хватать для расшифровки данных из заголовков пакетов большинства протоколов, однако может возникнуть необходимость использовать большее значение.

-w *<имя файла>*

Записывать содержимое пакетов в файл. Полезно для съёма информации в неурочное время или при больших объёмах передаваемой информации.

-r *<имя файла>*

Анализ информации записанной с помощью опции *-w*.

<выражение фильтра> позволяет отсеивать явно ненужную информацию, захватывая лишь пакеты, которые удовлетворяют условиям этого выражения. Полный синтаксис выражений можно найти в документации по tcpdump.

Пример:

```
tcpdump host 192.168.3.255
tcpdump: listening on eth0
12:23:19.493594 809-01.comp.chelcom.ru.netbios-ns>192.168.3.255.netbios-ns:
>>NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
```

На экран выведены IP-адрес (или имя) отправителя пакета, через точку указывается порт. После знака ">" указывается получатель пакета (или его имя) и также порт. Затем будет идти либо сразу служебная информация идущая в пакете, либо протокол. В служебной информации может быть указано либо состояние флагов в пакете, либо расшифрованная информация.

Реакция tcpdump на попытку подключения к закрытому порту 23/tcp:

```
21:56:14.381091 IP 192.168.56.1.54040 > 192.168.56.33.23: Flags [S], seq 2956835311,  
  win 5840, options [mss 1460,sackOK,TS val 5164501 ecr 0,nop,wscale 7], length 0  
21:56:14.381688 IP 192.168.56.33.23 > 192.168.56.1.54040: Flags [R.],  
  seq 0, ack 2956835312, win 0, length 0
```

В данном примере с системы 192.168.56.1 делается попытка подключиться к несуществующему TCP-сервису на узле 192.168.56.33. Удаленная система реагирует отправкой сегмента с установленным флагом RST (сброса соединения).

Перед завершением работы tcpdump печатает статистику работы: количество перехваченных, полученных фильтром и отброшенных ядром пакетов:

```
4 packets captured  
4 packets received by filter  
  0 packets dropped by kernel
```

5. Задания.

5.1. Конфигурирование портов и работа с таблицей коммутации.

Порядок выполнения работы:

1. Изучите раздел «Port Configuration» коммутатора DES-3200-10.
2. Постройте топологию сети, показанную на рисунке 5.1.

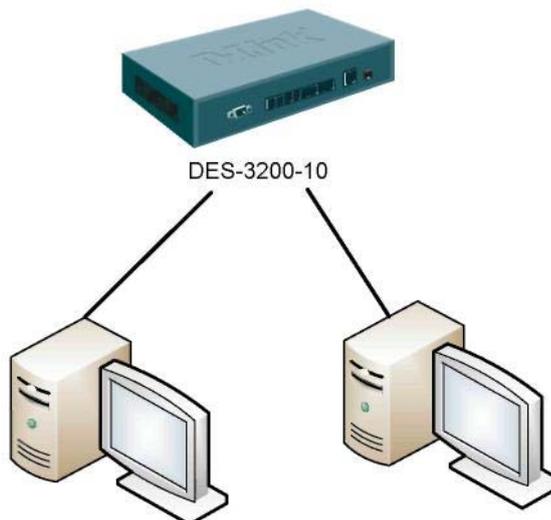


Рисунок 5.1. Топология коммутируемой сети.

3. Выключите один из портов коммутатора, к которому подключен один из компьютеров.
4. Попробуйте осуществить взаимодействие компьютеров. Сделайте выводы на основе полученного результата.
5. Изучите раздел «Port Mirroring» коммутатора DES-3200-10.
6. Настройте на коммутаторе зеркало для любого из портов, к которому подключен один из компьютеров.
7. Запустите на машинах, подключенных к порту-источнику и порту-приемнику (зеркалу), утилиту tcpdump. Активизируйте сетевую активность. Сравните результаты работы утилит на обеих машинах.
8. Силами двух бригад соберите топологию сети, представленную на рисунке 5.2. Все линия связи должны быть подключены к портам с пропускной способностью 100 Мбит/с. Обязательно соблюдайте нумерацию портов.
9. Установите пропускную способность портов коммутатора DES-3200-10, к которому подключены машины 3 и 4, равной 10 Мбит/с.
10. Настройте зеркало на коммутаторе DES-3200-10, к которому подключены машины 1 и 2, следующим образом: машина 1 – приёмник, машина 2 – источник.
11. «Пингуйте» (утилита ping) одновременно машину 2 с машин 3 и 4.

12. Запустите на машинах 1 и 2 утилиту `tcpdump`. Сравните результаты работы утилит на обеих машинах.
13. Прodelайте действия пунктов 8-12 в обратную сторону.

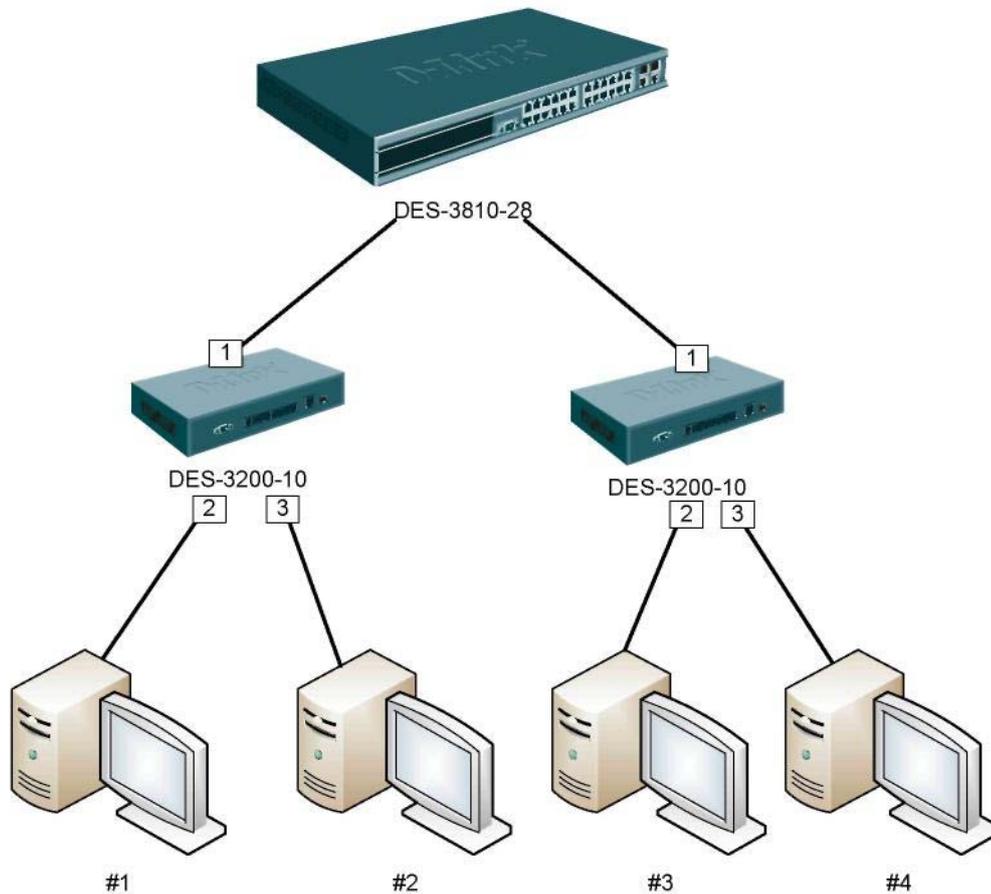


Рисунок 5.2. Топология коммутируемой сети.

14. Изучите раздел «Forward and Filtering» коммутатора DES-3200-10 в пособие по управлению стендом.
15. Создайте в статической таблице перенаправления коммутатора DES-3200-10, к которому подключены машины 1 и 2, следующую некорректную запись: машина #4 подключена к порту 3. Вторая бригада должна сделать то же самое на своём коммутаторе – создать следующую некорректную запись: машина #1 подключена к порту 2.
16. Удалите из таблицы перенаправления все записи, полученные коммутатором в режиме самообучения.
17. «Пингуйте» машину #4 с машины #1 и машину #1 с машины #4.
18. На машинах #2 и #3 запустите утилиту `tcpdump` и убедитесь, что коммутатор перенаправляет пакеты в соответствии с созданными Вами некорректными записями в таблице коммутации.

19. Сбросьте настройки коммутатора в заводские и перезагрузите его.

При подготовке данного учебно-методического пособия использовались материалы лабораторного практикума «Корпоративные компьютерные сети» НПП «Учтех-Профи».