

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 1. Знакомство с учебным стендом.

Администрирование коммутаторов

Учебно-методическое пособие

Саратов – 2016

Администрирование управляемых коммутаторов

Цель работы:

Изучение структуры стенда, способов коммутации его составляющих. Получение навыков использования утилит для изучения трафика и мониторинга сети. Получение навыков в базовой настройке управляемых коммутаторов. Изучение способов оповещения администратора о системных событиях коммутатора.

Оглавление

1. Технологии передачи данных в сетях TCP/IP	3
1.1 Адресация в IP-сетях.....	3
1.2 Модель OSI	4
2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети».....	7
2.1. Описание комплекта	7
3. Коммутаторы D-Link серии DES-3200.....	8
3.1. Управление коммутатором D-Link серии DES-3200	8
3.2. Разделы меню управления.....	15
4. Коммутаторы D-Link серии DES-3810.....	19
4.1. Управление коммутатором.....	19
5. Некоторые теоретические сведения	26
5.1 Настройка сетевых параметров.....	26
5.2 Утилиты мониторинга сети	27
5.3 Сервер журналов syslog-ng.....	30
5.4 SMTP-сервер Postfix.....	31
5.5 POP/IMAP-сервер Doveco.....	33
5.6 DNS-сервер ISC BIND.....	34
5.7 Утилиты управления сетью по протоколу SNMP	37
5.8 Сервер точного времени ISC NTPD.....	38
6. Задания	39
6.1. Знакомство с учебным стендом. Администрирование коммутаторов.....	39

1. Технологии передачи данных в сетях TCP/IP

1.1 Адресация в IP-сетях

В стеке протоколов TCP/IP используется три типа адресов:

1. MAC-адрес – идентификационный номер сетевого адаптера или порта маршрутизатора, например, 00-60-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

2. Доменный адрес. Имеет иерархическую структуру и несет смысловую нагрузку, поскольку предназначен для удобства запоминания пользователем. Такой адрес состоит из нескольких частей, например, имени машины, имени организации, имени домена. Называется также DNS-именем. Например, www.susu.ac.ru.

3. Сетевой адрес. Для сетей, поддерживающих стек протоколов TCP/IP, это IP-адрес. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например: 193.233.81.15 – традиционная десятичная форма представления адреса.

IP-адресация поддерживает двухуровневую иерархию. Адрес делится на две части – номер сети, и номер узла в этой сети. Для разделения двух частей адреса используется маска – двоичное число, которое содержит единицы в разрядах, интерпретируемых как номер сети. Например, маска 255.255.255.0 (11111111. 11111111. 11111111. 00000000) для адреса 193.66.39.214 означает, что в этом адресе первые три байта будут определять номер сети, а остальные – адрес узла. Таким образом, адрес сети – 193.66.39.0. Иногда для записи маски используют следующий формат: 193.66.39.214/24. Такая запись означает, что маска содержит 24 единицы, то есть под адрес сети отведено 24 разряда.

Существует соглашение о специальных адресах. Расшифровка особых адресов приведена в следующей таблице:

Вид адреса	Пример	Назначение
Все нули	0.0.0.0	Адрес того узла, который сгенерировал пакет
(номер сети).(все нули)	230.154.17.0	Данная IP-сеть
(все нули).(номер узла)	0.0.0.192	Узел в данной IP-сети
(номер сети).(все единицы)	230.154.17.255	Все узлы данной IP-сети. Пакет, имеющий такой адрес рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательной
Все единицы	255.255.255.255	Все узлы в той же сети, что и пославший пакет. Ограниченная широковещательная рассылка
127.(что угодно)	127.0.0.1	Петля. Адрес узла, пославшего пакет. Используется для тестирования процессов в пределах одной машины

1.2 Модель OSI

Эталонная модель OSI, иногда называемая стеком OSI представляет собой 7-уровневую сетевую иерархию (рис. 1.1) разработанную Международной организацией по стандартам (International Standardization Organization - ISO). Эта модель содержит в себе по сути 2 различных модели:

- горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах
- вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине

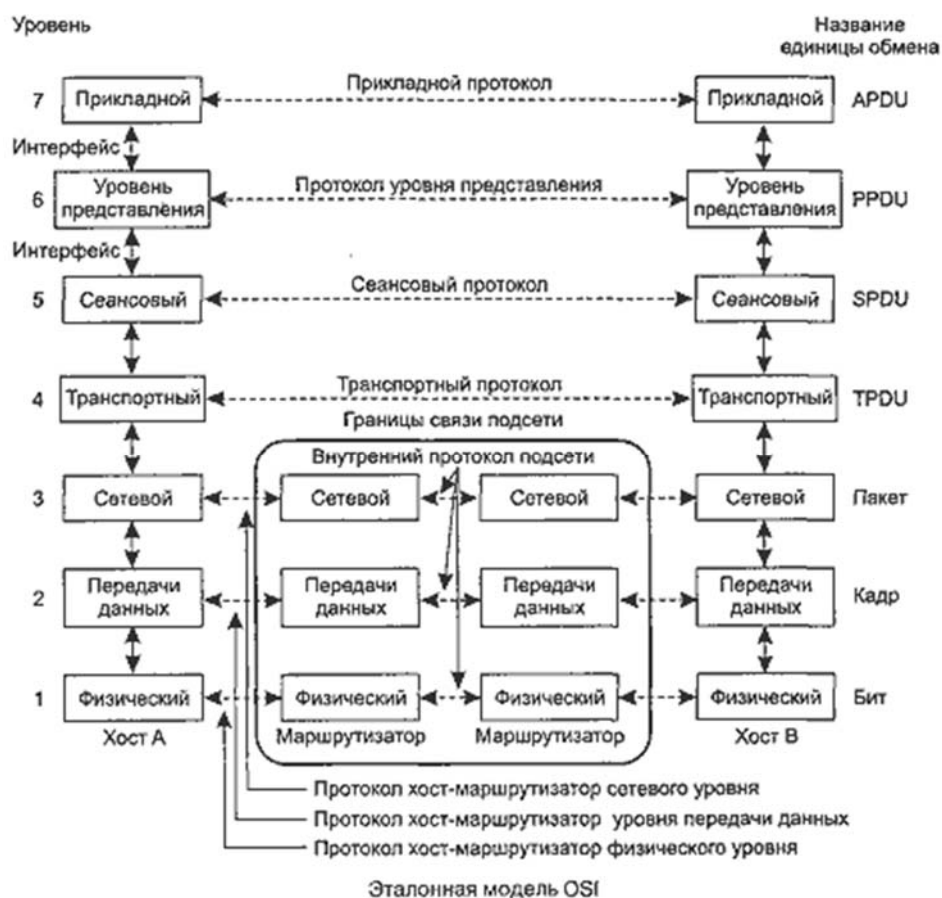


Рисунок 1.1. Семиуровневая сетевая иерархия в эталонной модели OSI.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной - соседние уровни обмениваются данными с использованием интерфейсов API.

Уровень 1, физический

Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел.

Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

- Тип кабелей и разъемов
- Разводку контактов в разъемах
- Схему кодирования сигналов для значений 0 и 1

К числу наиболее распространенных спецификаций физического уровня относятся:

- EIA-RS-232-C, CCITT V.24/V.28 - механические/электрические характеристики несбалансированного последовательного интерфейса.
- EIA-RS-422/449, CCITT V.10 - механические, электрические и оптические характеристики сбалансированного последовательного интерфейса.
- IEEE 802.3 -- Ethernet
- IEEE 802.5 -- Token ring

Уровень 2, канальный

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Спецификации IEEE 802.x делят канальный уровень на два подуровня: управление логическим каналом (LLC) и управление доступом к среде (MAC). LLC обеспечивает обслуживание сетевого уровня, а подуровень MAC регулирует доступ к разделяемой физической среде.

Наиболее часто используемые на уровне 2 протоколы включают:

- HDLC для последовательных соединений
- IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x
- Ethernet
- Token ring
- FDDI
- X.25
- Frame relay

Уровень 3, сетевой

Сетевой уровень отвечает за деление пользователей на группы. На этом уровне происходит маршрутизация пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

Наиболее часто на сетевом уровне используются протоколы:

- IP - протокол Internet
- IPX - протокол межсетевого обмена
- X.25 (частично этот протокол реализован на уровне 2)
- CLNP - сетевой протокол без организации соединений

Уровень 4, транспортный

Транспортный уровень делит потоки информации на достаточно малые фрагменты (пакеты) для передачи их на сетевой уровень.

Наиболее распространенные протоколы транспортного уровня включают:

- TCP - протокол управления передачей
- NCP - Netware Core Protocol
- SPX - упорядоченный обмен пакетами
- TP4 - протокол передачи класса 4

Уровень 5, сеансовый

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью функций трех верхних уровней модели.

Уровень 6, уровень представления

Уровень представления отвечает за возможность диалога между приложениями на разных машинах. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня. Протоколы уровня представления обычно являются составной частью функций трех верхних уровней модели.

Уровень 7, прикладной

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних уровней относятся:

- FTP - протокол переноса файлов
- TFTP - упрощенный протокол переноса файлов
- X.400 - электронная почта
- Telnet
- SMTP - простой протокол почтового обмена
- CMIP - общий протокол управления информацией
- SNMP - простой протокол управления сетью
- NFS - сетевая файловая система
- FTAM - метод доступа для переноса файлов

2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети»

2.1. 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 2.1.



Рисунок 2.1. 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.

3. Коммутаторы D-Link серии DES-3200

3.1. 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:

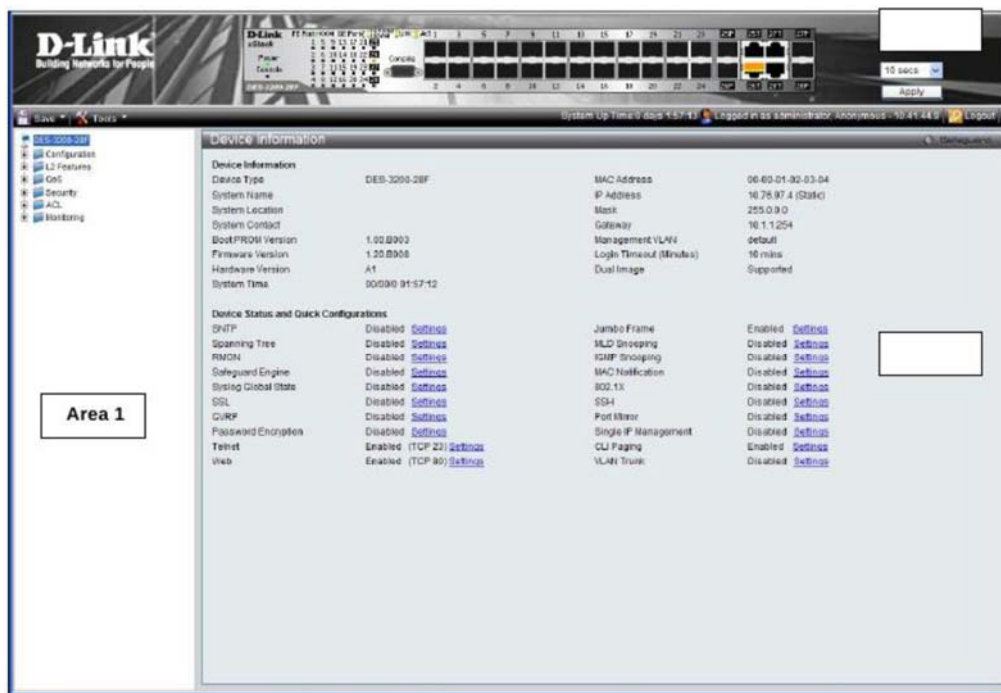
```
config ipif System ipaddress 192.168.1.5/255.255.255.0
```

```
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)
 - 802.1QStaticVLAN (Настройки протокола 802.1Q)
 - 802.1vProtocolVLAN (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 3.1.

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 3.1. Описание всех пунктов окна “Device Information”.

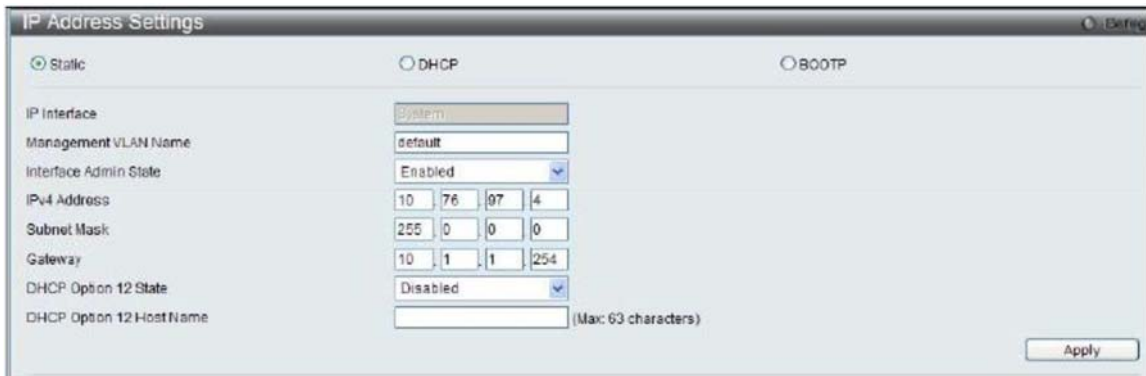
После изменения какого-либо пункта меню необходимо нажать кнопку «Apply», чтобы настройки вступили в силу.

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.

3.2. Разделы меню управления

3.2.1. Раздел IP Address Settings

Позволяет управлять IP-адресом устройства



- Static/DHCP/BOOTP—ручная настройка адреса/получение через DHCP/получение через BOOTP
- IPInterface—настраиваемый интерфейс (данный коммутатор имеет только один IP-интерфейс)
- ManagementVLANName—имя VLAN, через порты которого может осуществляться управление
- InterfaceAdminState—состояние интерфейса (включен/выключен)
- IPv4 Address—адрес IPv4
- Subnet Mask —маска адреса
- Gateway—шлюз по умолчанию
- DHCPOption12 State—включение отправки имени устройства DHCP-серверу (опция 12)
- DHCPOption12 HostName—передаваемое через опцию 12 имя

3.2.2. Раздел User Accounts

Позволяет управлять учётными записями пользователей



- User Name - имя пользователя
- Access Right - права доступа (администратор/пользователь)
- Password - пароль
- Confirm Password - подтверждение пароля

3.2.3. Раздел System Log Configuration

3.2.3.1. Раздел System Log Settings

Позволяет настраивать параметры журналирования



- System Log - включить/выключить журналирование
- Save Mode - событие, при котором происходит запись в журнал:
 - o On Demand - по требованию
 - o Time Interval - периодически
 - o Log Trigger - по срабатыванию триггера журналирования

3.2.3.2. Раздел System Log Server

Позволяет настраивать отправку журналов на сервер Syslog



- Server ID - индекс записи
- Server IP Address - IP-адрес сервера
- UDP Port - порт Syslog (по умолчанию 514)
- Severity - важность
- Facility - категория
- Status - состояние записи (активна/неактивна)

3.2.4. Раздел SMTP Settings

3.2.4.1. Раздел SMTP Service Settings

Позволяет настраивать отправку уведомлений по электронной почте

SMTP Service Settings

SMTP Global Settings

SMTP State: Enabled Disabled

SMTP Server Address:

SMTP Server Port (1-65535):

Self Mail Address: (Max:64 characters)

SMTP Mail Receiver Address

Add A Mail Receiver: (Max:64 characters)

Index	Mail Receiver Address	
1		Delete
2		Delete
3		Delete

- SMTP State - состояние функции
- SMTP Server Address - адрес SMTP-сервера
- SMTP Server Port - порт SMTP-сервера
- Self Mail Address - собственный адрес (адрес отправителя)
- Add A Mail Receiver - адрес получателя

3.2.4.2. Раздел SMTP Service

Позволяет проверить работу настроек

SMTP Service

Subject:

Content:

- Subject - тема письма
- Content - тело письма

3.2.5. Раздел Forwarding & Filtering

3.2.5.1. Раздел Unicast Forwarding Settings

Unicast Forwarding Settings

VLAN ID (1-4094): MAC Address: Port:

VLAN ID	VLAN Name	MAC Address	Port	Type
---------	-----------	-------------	------	------

Позволяет управлять статическими записями таблицы коммутации

- VLAN ID - VLAN, в котором действительна запись
- MAC Address - MAC-адрес узла
- Port - порт, на котором находится узел

3.2.6. Раздел PingTest

Позволяет выполнить проверку доступности узла

The image shows two overlapping dialog boxes from a network management application. The top dialog is titled "Reboot System" and contains a question "Do you want to save the settings?" with radio buttons for "Yes" (selected) and "No". Below this is a warning: "If you do not save the settings, all changes made in this session will be lost." A "Reboot" button is in the bottom right. The bottom dialog is titled "Ping Test" and contains the text "IPv4 Ping Test: Enter the IP address of the device or station you want to ping, then click Start." It has three input fields: "Target IP Address:" with the value "0.0.0.0", "Repeat Pinging for:" with radio buttons for "Infinite times" (selected) and a numeric field for "1-255 times", and "Timeout:" with the value "1" and "(1-99 sec)" next to it. A "Start" button is in the bottom right.

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

4. Коммутаторы D-Link серии DES-3810

4.1. 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.

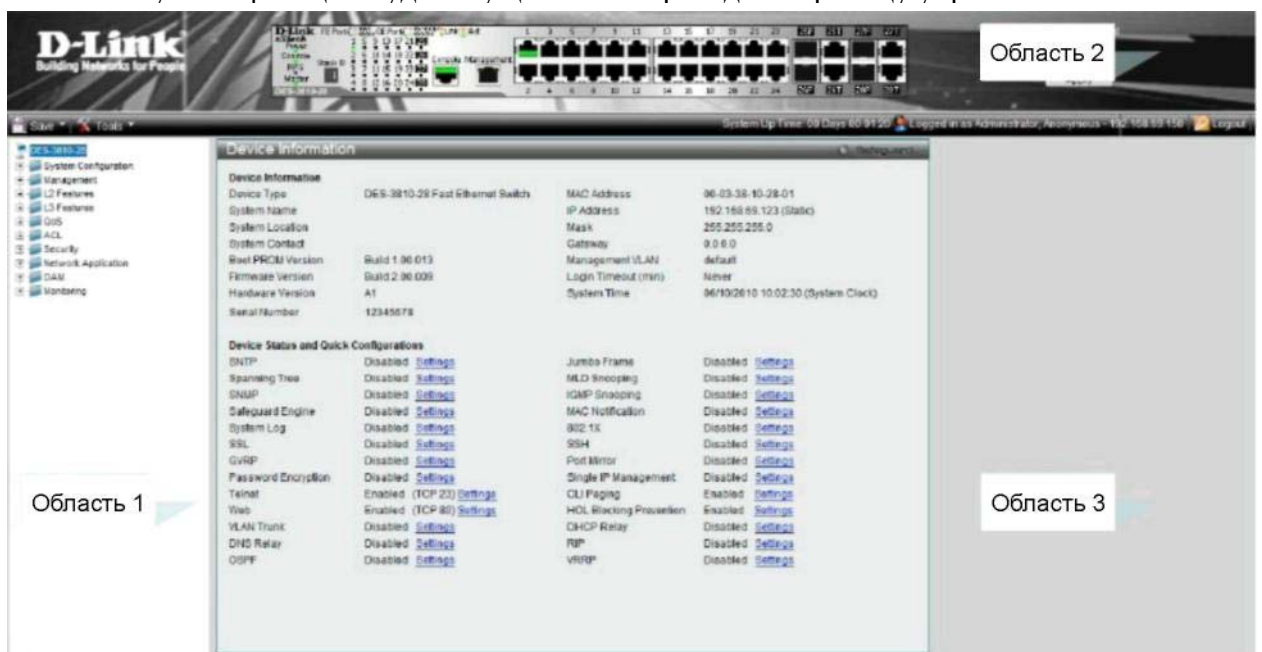
Для работы через management-порт соедините этот порт коммутатора и сетевой интерфейс компьютера патч-кордом. Порт по умолчанию имеет адрес 192.168.0.1/255.255.255.0. Сменить адрес порта можно следующими командами (в консольном интерфейсе):

```
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 Port Configuration (Настройка портов) Device Information (Информация об устройстве)
 - o System Information Settings (Информация о системе)
 - 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)

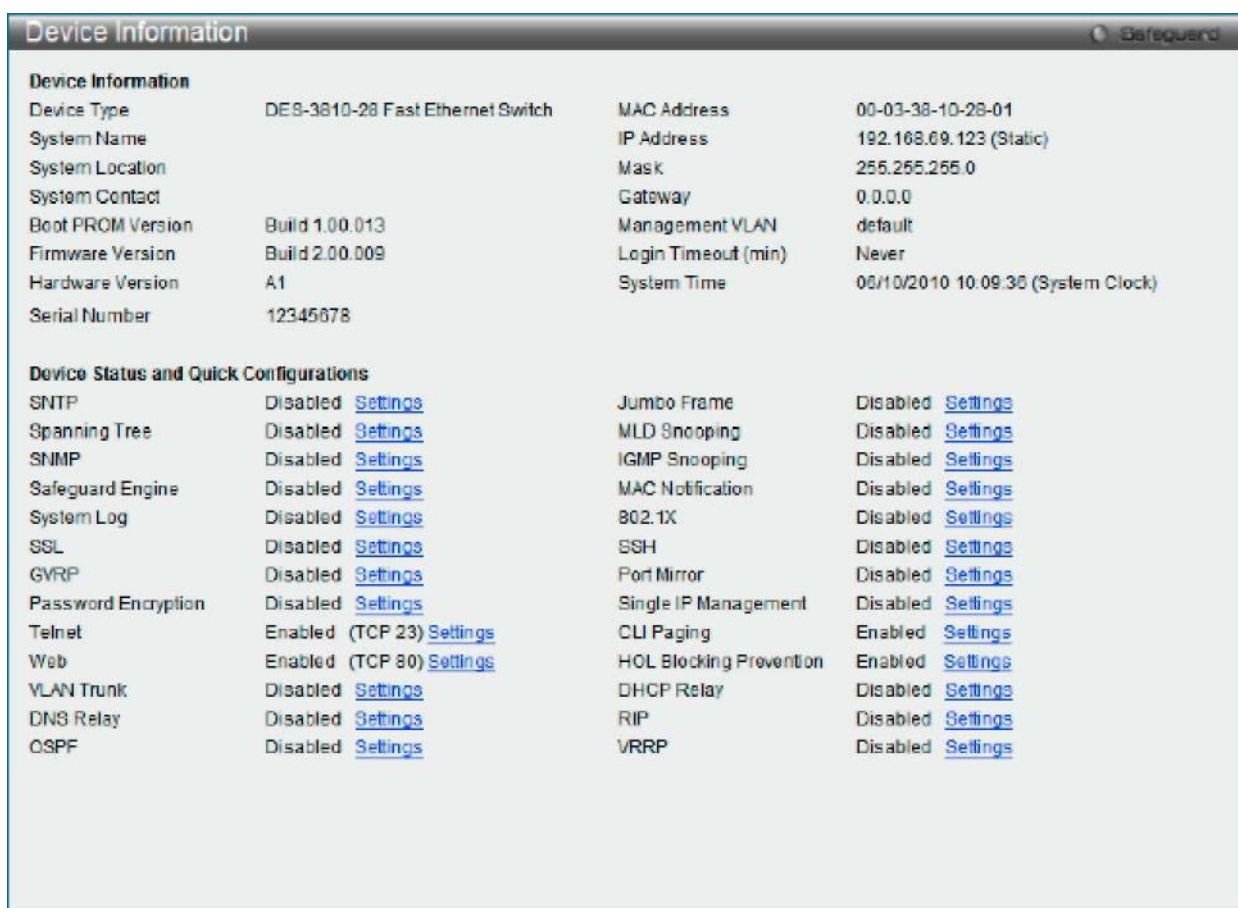
- o Link Aggregation (Объединение каналов)
- o FDB (Таблица коммутации)
- o L2 Multicast Control (Управление групповым вещанием)
- o Multicast Filtering (Фильтрация группового вещания)
- o ERPS Settings (Настройки защищённого кольца коммутации Ethernet)
- o Local Loopback Port Settings (Настройки интерфейса 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.

5. Некоторые теоретические сведения.

5.1 Настройка сетевых параметров

5.1.1 Настройка сетевого проводного интерфейса

Чтобы задать адрес сетевому интерфейсу, можно использовать команду `ifconfig`:

```
$ ifconfig <имя_интерфейса> <ip-адрес>
```

Для стандартных зарезервированных внутренних адресов сетевая маска и широковещательный адрес будут заданы автоматически. Для явного задания сетевой маски и широковещательного адреса можно использовать следующую команду:

```
$ ifconfig <имя_интерфейса> <ip-адрес> netmask <сетевая_маска_записанная_октетами>  
broadcast <широковещательный_адрес>
```

Например:

```
$ ifconfig eth0 10.10.10.10 netmask 255.255.255.0 broadcast 10.10.10.255
```

Для включения интерфейса (если он отключен) используется также команда `ifconfig`:

```
$ ifconfig <имя_интерфейса> up
```

Для отключения:

```
$ ifconfig <имя_интерфейса> down
```

5.1.2 Автонастройка сетевого интерфейса при запуске системы

Чтобы интерфейсам присваивались адреса (и прочие параметры) при старте системы, необходимо указать интерфейсы и параметры в файле `/etc/rc.conf` следующим образом:

```
<имя_интерфейса>="параметры_запуска"
```

Например, настройка интерфейса по протоколу DHCP:

```
eth0="dhcp"
```

Простое включение интерфейса, без дополнительной настройки:

```
eth0="eth0 up"
```

Присвоение адреса интерфейсу:

```
eth0="192.168.10.10"
```

Задание сетевой маски:

```
eth0="192.168.10.10 netmask 255.255.0.0"
```

Теперь эти интерфейсы необходимо перечислить в секции `INTERFACES=()`:

```
INTERFACES=(eth0)
```

Маршруты настраиваются аналогично. Например, создание маршрута по умолчанию:

```
gateway="default gw 192.168.0.1"
```

Указываем его в секции `ROUTES=()`:

ROUTES=(gateway)

5.2 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 отправки 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
```

arp

Для проверки ARP-таблиц, содержащих соответствие между IP-адресом и MAC-адресом, используется утилита ARP. В некоторых случаях бывает полезно просмотреть или изменить содержание ARP-таблицы, например, когда вы подозреваете, что двойной адрес является причиной сетевой неустойчивости. Одна из проблем, которая может потребовать, чтобы вы вручную добавили IP-адрес к ARP-таблице, это когда по некоторым причинам ARP-запросы для удаленного хоста не доходят, например, когда есть сбой ARP-драйвера, или имеется другой хост в сети, который ошибочно опознает себя с IP-адресом другого хоста. Твердая установка IP-адреса в ARP-таблице также является мерой защиты себя от хостов в вашем Ethernet, которые выдают себя за кого-то другого.

Синтаксис командной строки:

```
arp [-v] [-t hwtype] -a [hostname]
```

```
arp [-v] [-t hwtype] -s hostname hwaddr
```

```
arp [-v] -d hostname [hwaddr]
```

Аргумент hostname может быть как именем, так и IP адресом. Первая строка отображает ARP-запись для IP-адреса, указанного хоста или всех известных хостов, если hostname не задается.

Пример:

```
arp -a
IP address           HW type           HW address
172.16.1.3           10Mbps Ethernet  00:00:C0:5A:42:C1
172.16.1.2           10Mbps Ethernet  00:00:C0:90:B3:42
172.16.2.4           10Mbps Ethernet  00:00:C0:04:69:AA
```

При использовании опции -t вы увидите информацию только о том типе аппаратных средств, который укажете. Это могут быть:

- ether
- ax25

- *pronet (Ethernet 10Mbps)*
- *AMPR AX.25*
- *IEEE 802.5*

Опция `-s` используется, чтобы добавить Ethernet-адрес хоста к ARP-таблицам.

Аргумент `hwaddr` определяет адрес аппаратных средств, который по умолчанию предполагается Ethernet-адресом, указанным как шесть шестнадцатеричных байт, разделяемых двоеточиями. Вы можете также устанавливать адреса для других типов аппаратных средств, используя опцию `-t`.

Вызов `arp` с использованием ключа `-d` удаляет все ARP-записи, касающиеся данного хоста. Это может быть необходимо, чтобы вынудить интерфейс повторно получить Ethernet-адрес для данного IP. Это полезно, когда переконфигурированная система имеет неправильную ARP-информацию.

5.3 Сервер журналов `syslog-ng`

Сервер `syslog-ng` – это сервер, на который отправляются журналы со всех устройств в сети, поддерживающих протокол `syslog`. Такое решение позволяет иметь все журналы в исходном виде, даже в случае взлома устройства, которое использует сервер журналирования, или его поломки (например, выхода из строя жесткого диска). Кроме того, снимается нагрузка на жесткий диск клиентской системы.

Основное понятие сервера журналов – это поток (Facility) – это класс событий, которые записываются в один определённый пункт назначения (например, файл). Существуют предопределённые потоки (например, `mail` — поток для событий почтовых серверов, `auth` — для событий авторизации) и потоки, которые пользователь может использовать по своему усмотрению (`local0-local7`).

В Arch Linux по умолчанию используется демон `syslog-ng`, конфигурационный файл которого расположен по адресу `«/etc/syslog-ng.conf»`. Обратите внимание: настройки по умолчанию достаточно хороши, но демон не настроен на работу в качестве сетевого сервера! Рассмотрим пример конфигурационного файла сервера журналирования. Жирным курсивом будут выделены строки, уже присутствующие в конфигурационном файле по умолчанию.

```
#Начало секции источников событий
source src {
# Приём событий из устройства
unix-stream("/dev/log");
# Приём внутренних событий
internal();
# Приём событий из файла
file("/proc/kmsg");
# Приём событий через UDP-сокеты - необходим для приёма событий из сети
udp();
};

# Секция описания приёмников журналов
destination authlog { file("/var/log/auth.log"); }; destination syslog { file("/var/log/syslog.log"); };
destination cron { file("/var/log/cron.log"); };

# Создадим новый приёмник журналов с именем "des", который будет вести
# запись в файл /var/log/des-3838.log destination des { file("/var/log/des-3828.log"); };
```

```

# Секция описания фильтров
filter fauth { facility(auth); };
filter fauthpriv { facility(auth, authpriv); };
filter fsyslog { program(syslog-ng); };

# Создадим новый фильтр с именем fdes, выделяющий события от потока
# local0
filter fdes { facility(local0); };

# Секция связки источника, фильтра и приёмника
log { source(src); filter(facpid); destination(acpid); flags(final);
};
log { source(src); filter(fauthpriv); destination(authlog); };
log { source(src); filter(fsyslog); destination(syslog); };

# Создадим новую связку - источник src, фильтр fdes и приёмник des
log { source(src); filter(fdes); destination(des); };

```

Сохраните файл и перезапустите демон syslog-ng, выполнив команду

```
/etc/rc.d/syslog-ng restart
```

Проверьте ответ команды

```
netstat -lnup
```

Вы должны увидеть демон syslog-ng, ожидающий соединения на 518 порту по протоколу udp.

5.4 SMTP-сервер Postfix

Postfix – это SMTP-сервер, сочетающий в себе мощь, функциональность, гибкость и простоту настройки. Запуск Postfix для обслуживания одного домена занимает 5-10 минут

40 ООО НПП «Учтех-Профи» – Управление операционной системой Arch Linux 2012 (без настройки фильтрации). Настройки Postfix обеспечивают достаточную производительность и степень безопасности для сервера небольшой организации (по крайней мере, этот сервер не превратится в публичный). Postfix является модульным сервером (и число частей, на которые он разбит, достаточно велико).

Рассмотрим пример настройки Postfix для обслуживания домена example.com

- Основной (и единственный, интересный нам) конфигурационный файл -

```
/etc/postfix/main.cf.
```

```

• # Каталог, в котором будут содержаться очереди сообщений
• queue_directory = /var/spool/postfix
• # Путь по умолчанию для команд вида post*
• command_directory = /usr/sbin
• # Каталог, содержащий всех демонов, составляющих Postfix.
  Владелльцем
• # каталога должен быть пользователь root
• daemon_directory = /usr/lib/postfix
• # Каталог, в котором хранятся данные Postfix (кеши,
  случайные числа и

```


- # т.д.). Владелцем каталога должен быть пользователь, указанный в
- # параметре mail_owner
- **data_directory = /var/lib/postfix**
- # Указывает пользователя-владельца почтовых очередей и большинства
- # демонов, составляющих Postfix. Нельзя указывать уже используемую
- # кем-то учётную запись
- **mail_owner = postfix**
- # Определяет имя сервера
- **myhostname = example.com**
- # Определяет доменную часть почтового адреса отправителя
- ЛОКАЛЬНЫХ
- # сообщений. Так, почта, локально отправленная от имени пользователя
- # user, будет содержать имя отправителя user@\$myhostname
- # (user@example.com). Все значения параметров, начинающиеся с символа
- # \$, являются макросами и заменяются при запуске Postfix на значения
- # одноимённых параметров
- **myorigin = \$myhostname**
- # Ожидать соединения на всех доступных сетевых адресах
- **inet_interfaces = all**
- # Имена доменов, для которых надо принимать почту
- **mydestination = \$myhostname, localhost.\$mydomain, localhost**
- # Определяет локальных получателей почты
- # В данном случае используется системная база пользователей
- # (/etc/passwd) и база псевдонимов, заданная параметром alias_maps
- **local_recipient_maps = unix:passwd.byname \$alias_maps**
- # Код, с которым будет отклоняться почта для неизвестного получателя
- **unknown_local_recipient_reject_code = 550**
- # Определяет сети, почта из которых будет отправляться без прохождения
- # авторизации. Возможны следующие варианты:
- # host – только с этого же хоста
- # subnet – из подсети, которой принадлежит данный хост
- # class – из сетей, относящихся к тому же классу, что и сеть, в
- # которую входит данный хост
- **mynetworks_style = host**
- # Определяет путь до базы псевдонимов
- **alias_maps = hash:/etc/postfix/my_tables/aliases**
- # Определяет путь до базы псевдонимов, созданной командой newaliases.
- # При изменении файла псевдонимов необходимо выполнить команду
- # newaliases и заставить Postfix перечитать настройки.
- Необходим, так
- # как необязательно все базы из параметра alias_maps находятся под
- # контролем Postfix

```

alias_database = $alias_maps
# Определяет строку, выдаваемую сервером в начале SMTP-диалога
smtpd_banner = $myhostname ESMTP $mail_name
# Путь до команды sendmail из состава Postfix
sendmail_path = /usr/sbin/sendmail
# Путь до команды newaliases из состава Postfix
newaliases_path = /usr/bin/newaliases
# Путь до команды mailq из состава Postfix
• mailq_path = /usr/bin/mailq

```

Запустите почтовый сервер, выполнив команду `/etc/rc.d/postfix start`. Чтобы заставить Postfix перечитать настройки, выполните команду `/etc/rc.d/postfix reload`.

5.5 POP/IMAP-сервер Dovecot

Dovecot является производительным и гибким POP/IMAP-сервером. Может работать с различными базами пользователей, поддерживает SSL и TLS.

Конфигурационный файл Dovecot разбит на несколько: основная часть находится в файле `/etc/dovecot/dovecot.conf`, а прочие настройки по группам содержатся в каталоге `/etc/dovecot/conf.d`, причём используются только файлы с расширением «.conf». Важно понимать, что все настройки, включающиеся из других файлов, могут быть записаны и в один файл.

Рассмотрим пример файла `/etc/dovecot/dovecot.conf`:

```

# Протоколы, с которыми сервер будет работать
# LMTP (Local Mail Transfer Protocol) – протокол локальной доставки
# почты
# (например, между SMTP-сервером и сервером, обслуживающим почтовые
# ящики,
# например, Dovecot
protocols = imap pop3 lmtp
# Адреса, на которых будет работать Dovecot
# Элементы списка разделяются запятыми
# * - все адреса Ipv4
# :: - все адреса IPv6
listen = *, ::
# Приветствие, выдаваемое клиенту
login_greeting = Dovecot ready
На этом основные настройки закончены. Далее рассмотрим важные
настройки из дополнительного набора. 42 000 НПП «Учтех-Профи» –
Управление операционной системой Arch Linux 2012
10-auth.conf – настройки процесса аутентификации
# Управление функцией аутентификации прямым текстом (plaintext)
# Значение yes или no разрешает или запрещает такую аутентификацию
# при условии неиспользования SSL соответственно
disable_plaintext_auth = no
# Разрешённые механизмы аутентификации
# Учитывайте ключ disable_plain_auth
auth_mechanisms = plain
# Включение части файла, содержащего сведения о базе
# из которой берутся учётные данные пользователей
# Самый простой пример такой базы – база, формируемая системой PAM.
!include auth-system.conf.ext
auth-system.conf.ext
# Определение базы учётных данных пользователей, получаемой из PAM

```

```

# Через эту базу происходит аутентификация клиентов
# Настройки PAM хранятся в файле /etc/pam.d/dovecot
passdb {
driver = pam
}
# Определение базы информации о пользователях, получаемой из NSS
# Через эту базу происходит поиск дополнительных сведений о
пользователе
# (например, домашнего каталога)
userdb {
driver = passwd
}
10-mail.conf – настройки расположения почтовых ящиков
# Расположение почтового ящика пользователя
# Можно применять следующие переменные:
# %u – имя пользователя
# %n – часть имени пользователя до символа @
# %d – часть имени пользователя после символа @
# %h – домашний каталог пользователя
# Требуется указывать формат почтового ящика – mbox или Maildir
mail_location = mbox:/var/mail/%u
10-master.conf – настройки основного рабочего процесса
# Определение служб аутентификации для почтовых протоколов
# Можно изменить порт, на котором располагается та или иная служба
service imap-login {
inet_listener imap {
port = 143
}
}
service pop3-login
inet_listener pop3 {
port = 110
}
}
10-ssl.conf – настройки использования SSL
# Параметр, отключающий необходимость использования SSL
ssl = no
# Естественно, необходимо закомментировать строки, указывающие на
сертификаты

```

На этом базовая настройка простейшего POP/IMAP-сервера, обслуживающего системных пользователей, завершена. Так как все файлы конфигурации Dovecot снабжены подробными комментариями, несложно расширить функциональность сервера под ваши нужды.

Запуск сервера производится командой

```
# /etc/rc.d/dovecot start.
```

5.6 DNS-сервер ISC BIND

ISC BIND является стандартом де-факто в Интернет. Этот DNS-сервер является очень гибким, конфигурируемым, производительным и надёжным. Для работы серверу необходимы следующие данные:

1. Основные параметры (адрес, порт, расположение журналов).

2. Описание обслуживаемых зон.
3. Собственно зоны.

BIND может являться как первичным, так и вторичным сервером. Может содержать так называемые зоны-заглушки (stub). Может являться авторитетным или кеширующим сервером. В Arch Linux BIND запускается от имени пользователя named (в целях безопасности), поэтому все файлы, содержащие зоны, должны быть доступны для чтения этому пользователю. Рассмотрим пример настройки BIND как первичного сервера зоны localhost.

Основная настройка сервера

Все базовые настройки BIND хранятся в файле `/etc/named.conf`. Формат файла является C-подобным.

```
// начало основных настроек
options {
// корневой каталог для зон
directory "/var/named";
// файл, содержащий PID процесса
pid-file "/var/run/named/named.pid";
// указание, что данный сервер – авторитетный (в случае невозможности
// выполнения запроса по причине отсутствия сведений об объекте из //
запроса будет возвращён ответ non-existing domain (NX-DOMAIN) с //
установленным битом авторитетности ответа)
auth-nxdomain yes;
// способ ограничения памяти, потребляемой сервером
datasize default;
// хосты, для которых разрешены рекурсивные запросы к вышестоящим //
серверам
allow-recursion { 127.0.0.1; };
// адрес, на котором сервер будет ожидать запросы. any – любой //
доступный адрес
listen-on { any; };
// то же, что и listen-on, но для протокола IPv6
listen-on-v6 { any; }; };
//описание зоны localhost
zone "localhost" IN {
//тип обслуживания. master – значит, этот сервер первичный для этой
//зоны
type master;
//файл, в котором содержится зона
file "localhost.zone";
//хосты, которым разрешено динамически изменять зону (например, через
//связку DNS-DHCP)
allow-update { none; };
//список подчиненных, вторичных серверов
allow-transfer { any; }; };
//описание обратной зоны 127.0.0.0/24
zone "0.0.127.in-addr.arpa" IN {
type master;
file "127.0.0.zone";
allow-update { none; };
allow-transfer { any; }; };
//описание корневых серверов
zone "." IN {
type hint;
file "root.hint"; };
```

```

//описание обратной зоны 192.168.100.0/24
zone "100.168.192.in-addr.arpa" IN {
type master;
file "192.168.100.zone";
allow-update { none; };
allow-transfer { none; }; };
//настройки журналирования
logging {
//создаём новый канал
channel xfer-log {
//файл, в который будут записываться события
file "/var/log/named.log";
//указывать категорию события
print-category yes;
//указывать степень опасности события
print-severity yes;
//указывать время события
print-time yes;
//записывать события со степенью опасности не ниже информационных
severity info; };
//записывать события приёма зоны с первичного сервера в канал xfer-
log
category xfer-in { xfer-log; };
//записывать события передачи зоны на вторичный сервер в канал xfer-
//log
category xfer-out { xfer-log; };
//записывать оповещения в канал xfer-log
category notify { xfer-log; }; };

```

Зоны

Важно понимать, что для BIND все строки, не оканчивающиеся точкой – это не полностью определённые имена домена (non-fqdn), поэтому эти имена будут дополнены до fqdn путём дописывания в конец доменной части, определяемой директивой \$ORIGIN. Если такой директивы нет – в файле зоны все имена доменов должны быть указаны в формате fqdn, то есть быть полностью определёнными.

Если несколько записей подряд относятся к одному и тому же домену (например, подряд идущие записи SOA, A, NS и MX для зоны), то имя домена можно указывать один раз. Все записи имеют следующий вид:

имя_домена TTL тип тип_записи параметры

Ниже приведён пример зоны localhost, определённой в файле /var/named/localhost.zone.

```

// определяем общую доменную часть адреса. Символ @ означает ссылку
на
// эту часть
$ORIGIN localhost.
// SOA-запись
// Параметры:
// Имя первичного DNS-сервера, обслуживающего эту зону
// Почтовый адрес человека, ответственного за сервер. Вместо символа
@
//в качестве разделителя используется точка
@          1D IN SOA          @ root (

```

```

// серийный номер зоны. Обычно в формате <год><месяц><число><номер
реvisions>
42 ; serial (yyyymmdd##)
// период между обновлениями зоны на клиентских кешах
3H ; refresh
// период между повторными запросами, если сервер недоступен
15M ; retry
// время жизни зоны, если сервер недоступен
1W ; expiry
// время жизни зоны, если сервер доступен
1D ) ; minimum ttl
// NS-запись. Перечисляются все сервера (первичные и вторичные),
// ответственные за зону
1D IN NS @
// A-запись. Требуется, если данный сервер является авторитетным для
// данной зоны
1D IN A 127.0.0.1

```

Запуск DNS-сервер осуществляется командой

```
/etc/rc.d/named start
```

При изменении настройки сервера или зон, используйте команду `rndc reload`, чтобы BIND перечитал свои настройки и файлы зон. Журнал BIND по умолчанию пишется в файл `«/var/log/messages.log»`. Просмотреть записи, относящиеся только к BIND, можно, выполнив команду

```
grep named /var/log/messages.log.
```

5.7 Утилиты управления сетью по протоколу SNMP

5.7.1 Утилита *iReasoning MIB Browser*

Данная утилита является стандартным обозревателем базы данных MIB, поддерживаемой технологией SNMP. Утилита является кросс-платформенной, так как написана на языке Java. Для запуска утилиты запустите файл `/root/Desktop/SNMP/mibbrowser/browser.sh`. По умолчанию в программе загружаются две базы MIB. Если необходимо загрузить дополнительные базы, то используйте пункт меню «File→Load MIBs».

Для работы с определенным сетевым устройством необходимо в поле «Address» ввести IP-адрес данного устройства. Для того, чтобы получить значение записи в базе MIB устройства, необходимо выбрать нужную запись и нажать «CTRL-G» или выбрать пункт меню «Operations→Get» или нажав правую кнопку мыши выбрать команду «Get». Для того, чтобы получить значение всей базы выберите пункт меню «Operations→Walk». Для того, чтобы просмотреть содержимое таблицы необходимо выбрать команду «Table View»

5.7.2 Утилита *mbrowse*

Данная утилита входит в стандартный пакет программного обеспечения операционной системы Arch Linux и используется для просмотра и изменения параметров удаленной системы по протоколу SNMP. Для её запуска откройте терминал и введите:

```
$ mbrowse
```

Окно программы состоит из следующих областей:

- 1 — Поле ввода адреса (имени) транслятора SNMP
- 2 — Поле ввода имени группы для чтения
- 3 — Поле ввода имени группы для чтения/записи
- 4 — Кнопка получения значения параметра
- 5 — Кнопка рекурсивного обхода дерева параметров, начиная с выделенного раздела
- 6 — Поле просмотра дерева доступных параметров
- 7 — Поле просмотра значений параметров

Для получения данных с определённого агента SNMP необходимо:

1. В поле 1 указать адрес или имя агента.
 2. В поле 2 указать имя группы для чтения.
 3. В поле 6 выбрать нужный параметр и нажать кнопку 4.
 4. Либо в поле 6 выбрать нужную ветку дерева и нажать кнопку 5.
- В поле 7 отобразится запрошенная информация (при правильной работе агента и наличии запрошенных параметров).

5.8 Сервер точного времени ISC NTPD

Протокол Network Time Protocol позволяет поддерживать одинаковое время на всех компьютерах и прочих сетевых устройствах. Одинаковое время необходимо, если в сети используются сервисы авторизации, основанные на взаимной проверке сервера авторизации и клиента (например, Kerberos). Ещё один плюс одинакового времени на всех устройствах – вы точно знаете, когда произошло некоторое событие (например, при чтении журналов). В любой более-менее крупной сети использование этого протокола вполне оправданно и даже необходимо (равно как и прочие синхронизации).

Существует несколько реализаций серверов NTP, но стандартом де-факто в настоящее время является ISC NTPD (как и многие другие сетевые сервисы от ISC). Рассмотрим пример настройки сервера точного времени на основе ISC NTPD. Конфигурационный файл единственный - /etc/ntp.conf.

```
# Указываем вышестоящие серверы точного времени (если к таковым есть
# доступ). Хотя бы одна действительная директива server обязана
# присутствовать в файле! Желательно указывать не менее трёх
серверов,
# если такая возможность есть.
# Имеет смысл только в случае доступности указанного сервера
server ru.pool.ntp.org
# Путь до файла, в котором NTPD хранит смещение времени относительно
# эталонного
driftfile /var/lib/ntp/ntp.drift
# Указываем системный таймер в качестве источника точного времени
# При наличии более точных источников делать такое не рекомендуется
server 127.127.1.1
fudge 127.127.1.1 stratum 0 refid NIST
# Запрещаем изменять конфигурацию сервера отовсюду, кроме локальной
# машины
restrict default nomodify nopeer restrict 127.0.0.1
# Разрешаем нашей подсети снимать показания с данного сервера, но
# запрещаем изменять настройку сервера
restrict 192.168.10.0 mask 255.255.255.0 nomodify nopeer notrap
```

Запустите NTPD, выполнив команду `/etc/rc.d/ntpd start`. Проверить состоя связи созданного сервера с источниками точного времени можно, выполнив команду

```
# ntpq -c peers -n
      remote                refid                st t when poll reach  delay  offset  jitter
=====
 127.127.1.1      .NIST.                0 l   53   64   377    0.000    0.000    0.001
+193.233.85.131  147.45.15.34         3 u   16 1024   377    1.641   -3.145    5.337
 193.233.85.60   193.233.85.132      4 u   512 1024    17    0.502   -4.567    1.506
*193.233.85.132  147.45.15.34         3 u   23 1024   377    4.922  -35.893    0.097
```

сервер синхронизируется с теми серверами, записи о которых в выводе эт утилиты отмечены знаком + или *.

6. Задания.

6.1. Знакомство с учебным стендом. Администрирование коммутаторов.

Порядок выполнения работы:

1. Изучите раздел «Описание комплекта». Найдите все описанные элементы комплекта.
2. С помощью проводов соедините патч-панель и коммутаторы таким образом, чтобы получить топологию, представленную на рисунке 6.1.

Внимание: далее каждая бригада работает по отдельности со своим коммутатором **DES-3200-10**

3. Включите рабочие станции и зарегистрируйтесь на них (пользователь – root, пароль – qwerty).
4. Изучите разделы «Управление коммутатором» для DES-3200-10 и DES-3810-28.
5. Изучите раздел «Утилиты мониторинга сети».
6. С помощью утилиты *ifconfig* определите параметры вашего узла. На рисунке отметьте MAC- и IP- адреса всех компьютеров.
7. С помощью утилиты *ping* проверьте связь каждой рабочей станции со всеми другими рабочими станциями созданной сети.
8. С помощью утилиты *arp* просмотрите таблицу ARP на каждой рабочей станции.
9. Изучите разделы «Ping Test» и «IP Address Settings» коммутатора DES-3200-10
10. Назначьте коммутатору DES-3200-10 IP-адрес из диапазона свободных адресов IP-сети, в которой находятся рабочие станции. На рисунке 6.1 отметьте IP-адрес коммутатора.
11. С помощью системной утилиты коммутатора Ping проверить связь коммутатора с каждой машиной в сети.
12. Используя утилиту *tcpdump* на любой из машин в сети, убедиться в том, что до заданной машины доходят ICMP-запросы от коммутатора.
13. Изучите раздел «User Accounts» коммутатора DES-3200-10 .
14. Создайте на коммутаторе пользователя со статусом «Admin».

17. Выйдите из системы (logout).
18. Зарегистрируйтесь на коммутаторе, используя учётную запись вновь созданного пользователя.
19. Создайте на коммутаторе пользователя со статусом «User».
20. Выйдите из системы (logout).
21. Зарегистрируйтесь на коммутаторе, используя учётную запись пользователя со статусом «User».
22. Попробуйте выполнить любые действия, связанные с изменением текущих настроек коммутатора. Сделайте выводы об ограниченности прав пользователя со статусом «User».
23. Удалите все созданные Вами учётные записи пользователей.
24. Изучите раздел «Сервер журналов syslog-ng», затем раздел «System Log Configuration» коммутатора DES-3200-10.
25. Настройте на одном из компьютеров сервер syslog таким образом, чтобы он мог принимать информацию из сети и записывать её в один определённый файл.
26. Настройте коммутатор таким образом, чтобы он отправлял информацию о системных событиях на сервер журналирования.
27. Сохраните настройки, выйдите из системы и выключите питание коммутатора.
28. Включите питание коммутатора, зарегистрируйтесь на нём, а затем отключите и включите линию связи, подключенную к любому порту коммутатора.
29. При помощи утилиты tcpdump изучите диалог syslog-клиента и syslog-сервера.
30. Проанализируйте содержимое сообщения, полученного сервером журналирования.
31. Изучите раздел «SMTP Settings» коммутатора DES-3200-10, а также разделы «SMTP-сервер Postfix», «POP/IMAP-сервер Dovecot» и «DNS-сервер ISC BIND».
32. Запустите на одном из компьютеров сервер DNS.
33. Создайте и настройте DNS-зону «lab.org».
34. На этом же компьютере настройте и запустите SMTP-сервер для зоны «lab.org».
35. Заведите на почтовом сервере следующие учётные записи пользователей: info@lab.org и switch@lab.org.
36. Настройте коммутатор таким образом, чтобы он отсылал информацию о системных событиях на созданные Вами почтовые адреса.
37. Используя почтового клиента «kmail» на втором компьютере, проверьте почту и убедитесь в работоспособности настроенного Вами механизма уведомления о системных событиях коммутатора через почтовые сообщения.
38. При помощи утилиты tcpdump изучите диалог smtp-клиента и smtp-сервера, port3-

клиента и рор3-сервера.

39. Изучите раздел «SNTP Settings» коммутатора DES-3200-10 в пособие по управлению стендом и раздел «Сервер точного времени ISC NTPD».
40. На двух компьютерах настройте сервер NTP.
41. Активируйте на коммутаторе клиента SNTP и настройте его на получение информации о времени с настроенных Вами серверов NTP через каждые 30 секунд.
42. При помощи утилиты tcpdump изучите диалог ntp-клиента и ntp-сервера.
43. Определите источник полученной информации о времени и сверьте системное время коммутатора.
44. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

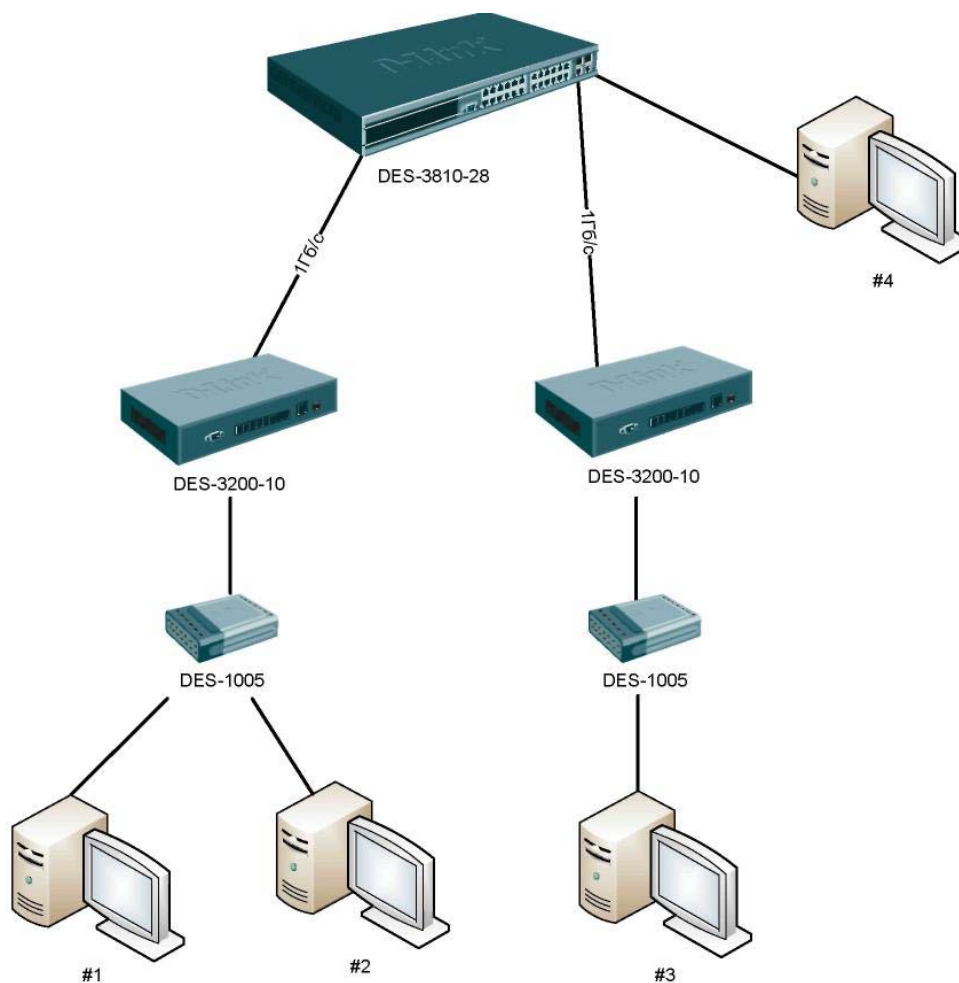


Рисунок 6.1. Топология коммутируемой сети.

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