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 2. Управление сетью с помощью технологии Single IP Management.

Управление сетью с помощью протокола SNMP.

Учебно-методическое пособие

Саратов – 2016

Администрирование управляемых коммутаторов

Цель работы:

Изучение технологии Single IP Management и получение практических навыков управления сетью с её помощью. Изучение способов мониторинга и управления сетью на основе протокола SNMP.

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 13
3.1. Управление коммутатором 13
4. Некоторые теоретические сведения 20
4.1 Утилиты управления сетью по протоколу SNMP 20
4.2 Сервер точного времени ISC NTPD 20
4.3 Способы управления коммутаторами 21
4.4 Протокол SNMP 30
5. Задания 45
5.1. Управление сетью с помощью технологии Single IP Management. 45
5.2. Управление сетью с помощью протокола SNMP 46

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 отрабатывали 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

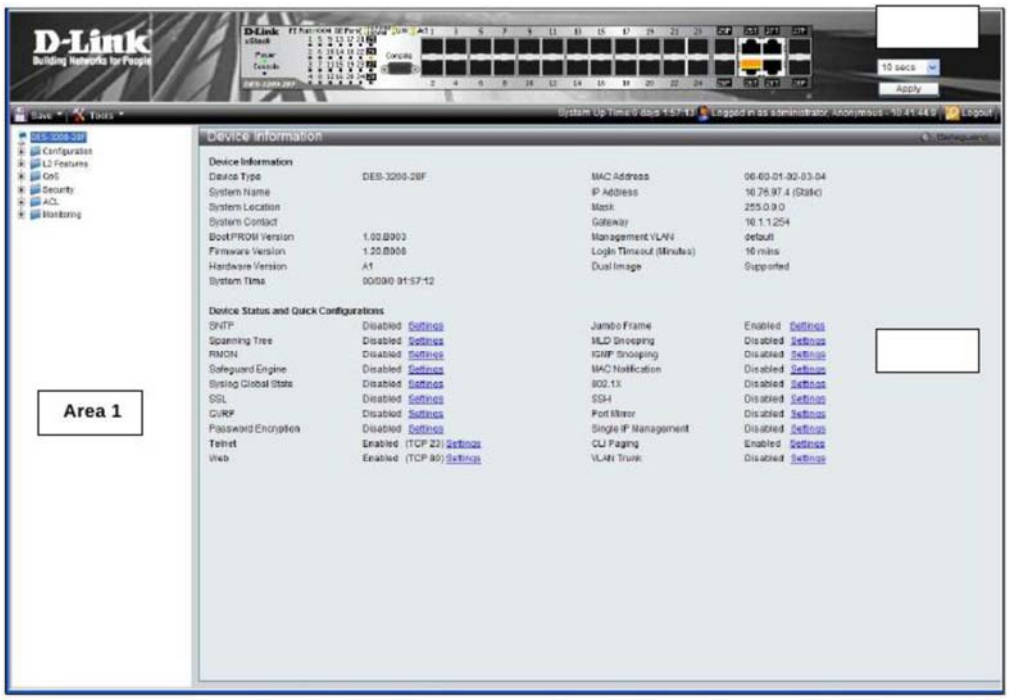
Маска подсети может задаваться либо в виде IP-адреса, либо числом, задающим количество бит, отводимых под сеть. Пример:

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)

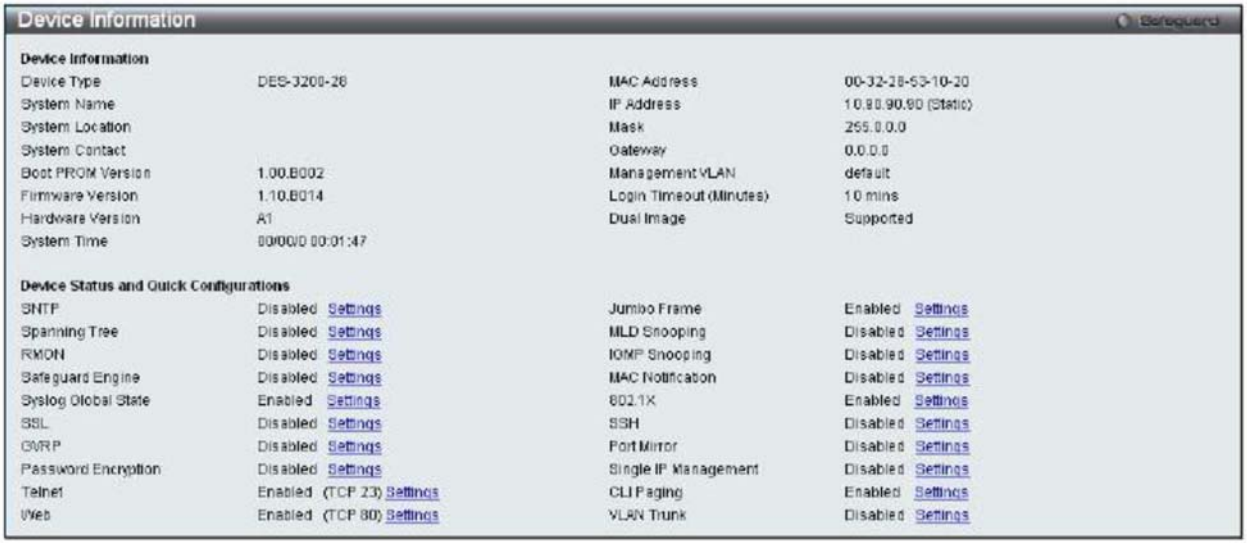
- Device Information (Информация об устройстве)
- Static ARP Settings (Статические записи ARP)
- Password Encryption (Шифрование паролей)
- CLI Paging Settings (Настройка страницы текстового интерфейса)
- Firmware Information (Информация о прошивке)

- 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)
  - 802.1QStaticVLAN (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.



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 произойдёт 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

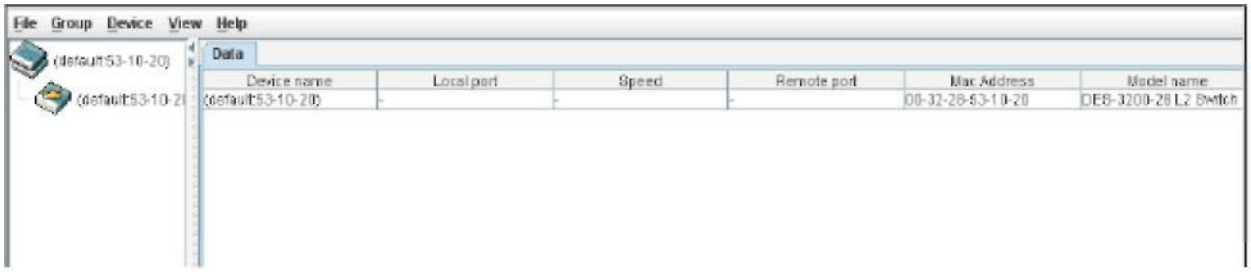
2.2.1. Раздел Single IP Management

2.2.1.1. Раздел Single IP Settings

Данное меню предназначено для настройки использования технологии Single IP Management. Все коммутаторы настроены как коммутаторы CaS согласно заводским настройкам по умолчанию, а функция Single IP Management отключена. Можно настроить следующие параметры:

- SIM State — используйте выпадающее меню для изменения SIM-состояния коммутатора. Disabled переведет все SIM функции коммутатора в нерабочее состояние.

- Role State — используйте выпадающее меню для изменения роли коммутатора в SIM-группе. Возможно два варианта:
    - Candidate - Candidate Switch (CaS) не является членом SIM-группы, но подключен к управляющему коммутатору Commander Switch (CS). Данная роль коммутатора в SIM-группе является настройкой по умолчанию.



    - Commander - выберите данный вариант, чтобы коммутатор выполнял роль управляющего. Пользователь может подключить другие коммутаторы к управляющему поверх Ethernet, чтобы они стали членами этой SIM- группы. При выборе данной роли для коммутатора, становится возможным настройка SIM.

- Discovery Interval — пользователь может установить интервал посылки коммутатором обнаруживающих пакетов (Discovery Packets) в секундах. В ответ коммутатор CS получит информацию о других коммутаторах, подключенных к нему (например, MS, CaS). Пользователь может установить Discovery Interval от 30 до 90 секунд.
- Holdtime — Данный параметр может быть установлен разово; коммутатор будет хранить информацию, посланную от других коммутаторов в течение данного интервала времени. Пользователь может установить holdtime равным от 100 до 255 секунд.

После включения коммутатора в качестве управляющего CS, в папке Single IP Management для помощи пользователю в настройке SIM через Web-интерфейс появятся три ссылки:

- Topology, Firmware Upgrade;
- Configuration Backup/Restore;
- Upload Log File.

2.2.1.2. Раздел Topology

Окно «Topology» используется для настройки и управления коммутатором без SIM - группы и требует наличие Java для правильного функционирования на компьютере.

Окно «Tree View» содержит следующую информацию:

- Device Name. Данное поле будет отображать имена устройств, то есть коммутаторов, в SIM-группе, настроенные пользователем. Если имя устройства не задано, то для идентификации оборудования будет присвоено имя по умолчанию (default), к которому добавляют шесть последних цифр MAC-адреса.
- Local Port. Отображает номер физического порта на управляющем коммутаторе CS, к которому подключен MS или CaS. У управляющего коммутатора не будет записи в данном поле.
- Speed. Отображает скорость соединения между управляющим коммутатором и MS или CaS.

- Remote Port. Отображает номер физического порта на коммутаторе MS или CaS, который подключен к управляющему коммутатору. У управляющего коммутатора не будет записи в данном поле.
- MAC Address. Отображает MAC-адрес соответствующего коммутатора.
- Model Name. Отображает полное название модели соответствующего коммутатора.

Для просмотра топологии сети «Topology Map» выберите пункт меню «View→Topology», в результате чего откроется следующее окно. Данное окно периодически обновляется (по умолчанию через 20 секунд).

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

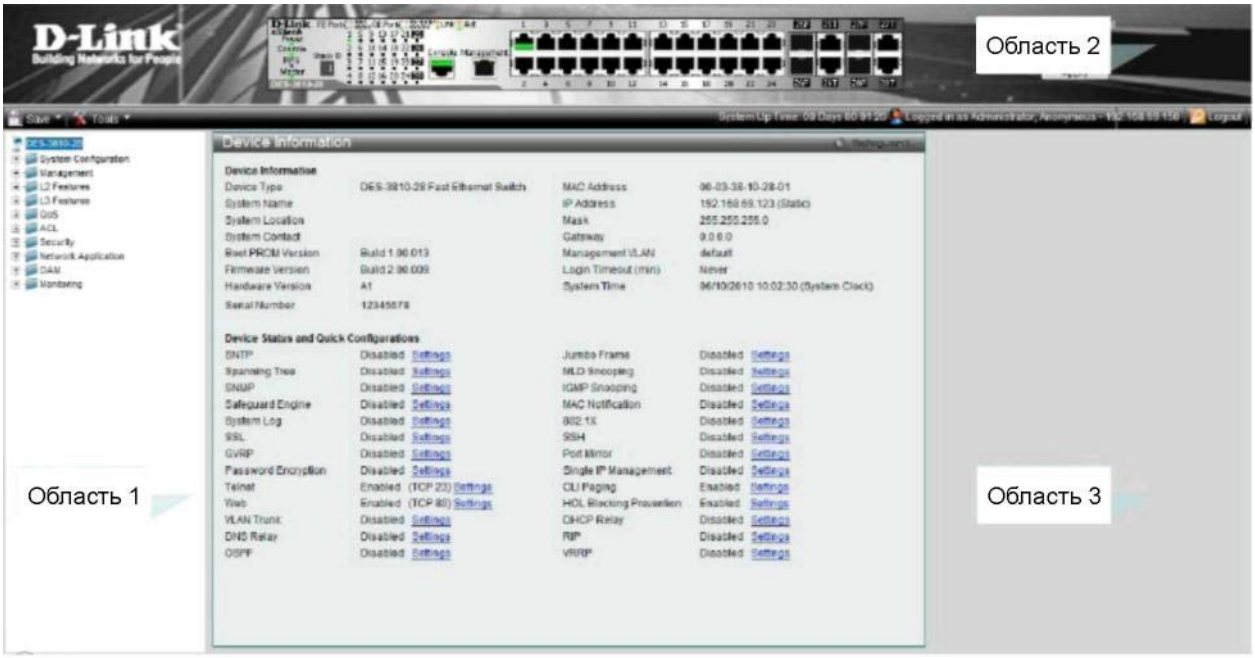
После выполнения любой команды необходимо выполнить команду *save* для сохранения заданных изменений в NVRAM коммутатора.

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

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

Развернутое меню управления коммутатором в области 1 имеет следующую структуру:

- System Configuration (Настройка)
  - Device Information (Информация об устройстве)
  - System Information Settings (Информация о системе)
  - Port Configuration (Настройка портов)
  - Serial Ports Settings (Настройка последовательного порта)
  - Warning Temperature Settings (Настройка критической температуры)
  - System Log Settings (Настройка системного журнала)
  - Time Range Settings (Настройка временных периодов)
  - Time Settings (Настройка часов)
  - User Account Settings (Управление учётными записями пользователей)
- Management (Управление)
  - ARP (Настройки ARP)
  - Gratuitous ARP (Настройки самонаправленного ARP)
  - I Pv6 Neighbor Settings (Настройки соседей I Pv6)
  - IP Interface (Настройки IP)
  - Management Settings (Настройки работы коммутатора)
  - Out of Band Management Settings (Настройки порта Management)
  - Session Table (Таблица сеансов управления)
  - Single IP Management (Настройки функции SIM)
  - SNMP Settings (Настройки SNMP)
  - Telnet Settings (Настройки Telnet)
  - Web Settings (Настройки Web-интерфейса)
- L2 Features (Возможности 2 уровня)
  - VLAN (802.1Q) (Настройки виртуальных локальных сетей 802.1Q)
  - QinQ (настройки вложенного тегирования)
  - Layer 2 Protocol Tunneling Settings (Настройки протокола туннелирования 2 уровня)
  - Spanning Tree Protocol (STP) (Настройки связующего дерева STP)

- Link Aggregation (Объединение каналов)
- FDB (Таблица коммутации)
- L2 Multicast Control (Управление групповым вещанием)
- Multicast Filtering (Фильтрация группового вещания)
- ERPS Settings (Настройки защищённого кольца коммутации Ethernet)
- Local Loopback Port Settings (Настройки интерфейса локальной петли)
- Link Layer Discovery Protocol (LLDP) (Настройки протокола обнаружения канального уровня)

- L3 Features (Возможности 3 уровня)
  - IPv4 Static/DefaultRouteSettings(Настройки статической маршрутизации IPv4)
  - IPv4 RouteTable(Таблица маршрутизации IPv4)
  - IPv6 Static/DefaultRouteSettings(Настройки статической маршрутизации IPv6)
  - IPv6 RouteTable(Таблица маршрутизации IPv4)
  - PolicyRouteSettings(Настройки маршрутизации по политикам)
  - IPForwardingTable(Таблица перенаправления IP)
  - RoutePreferenceSettings(Настройки предпочтительности маршрутов)
  - ECMPAlgorithmSettings(Настройки алгоритма ECMP)
  - RouteRedistributionSettings(Настройки распространения маршрутной информации)
  - OSPF (Настройки протокола OSPF)
  - RIP (Настройки протокола RIP)
  - VRRP (Настройки протокола VRRP)
  - MD5 Settings (Настройки хеширования MD5)

- QoS(Управление качеством сервиса)
  - 802.1 p Settings (Настройки протокола 802.1 p)
  - Bandwidth Control (Управление полосой пропускания)
  - Traffic Control Settings (Настройки контроля трафика)
  - DSCP (Настройки дифференцированного обслуживания)
  - HOL Blocking Prevention (Предотвращение блокирования очереди)

- 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)

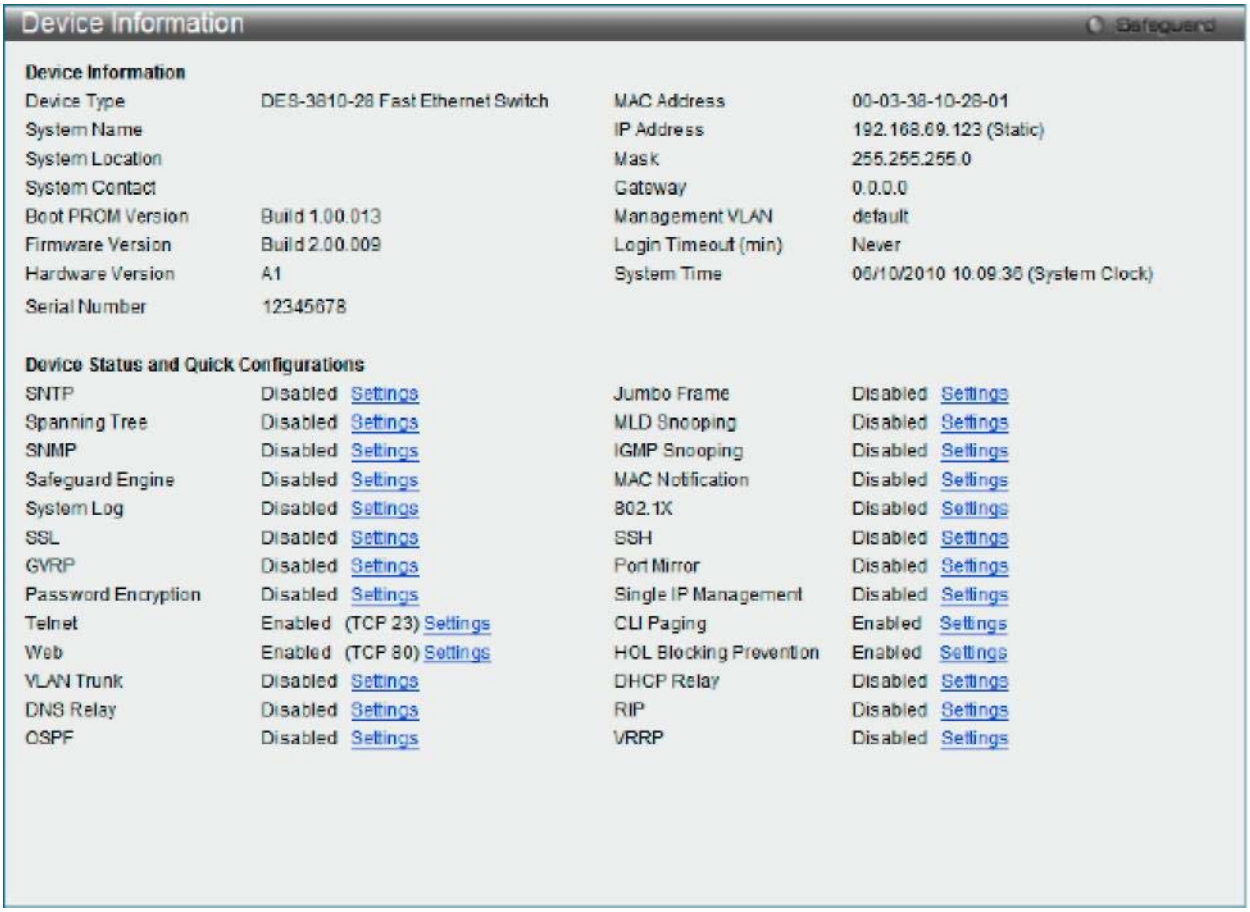
- 802.1X (Настройки протокола 802.1X)
- RADI US (Настройки серверов RADI US)
- IP-MAC-Port Binding (IMPB) (Настройки привязки IP-MAC-номер порта)
- MAC-Based Access Control (Контроль доступа на базе MAC-адресов)
- Web-based Access Control (WAC) (Контроль доступа к веб-интерфейсу)
- Compound Authentication (Комбинированная аутентификация)
- Port Security (Безопасность порта)
- ARP Spoofing Prevention Settings (Настройки защиты от атаки ARP Spoofing)
- BPDU Attack Protection (Настройки защиты от атаки на BPDU)
- Loopback Detection Settings (Настройки обнаружения петель)
- Traffic Segmentation Settings (Настройки разделения трафика)
- NetBIOS Filtering Settings (Настройки фильтрации протокола NetBIOS)
- DHCP Server Screening (Настройки экранирования DHCP-сервера)
- Access Authentication Control (Настройки аутентификации доступа)
- SSL Settings (Настройки SSL)
- Secure Shell (SSH) (Настройки SSH)
- Trusted Host Settings (Настройки узлов управления)
- Safeguard Engine Settings (Настройки механизма самозащиты)

- Network Application (Сетевые службы)
  - DHCP (Сервер DHCP)
  - Domain Name System (DNS) (Ретранслятор DNS)
  - PPPoE Circuit ID Insertion Settings (Настройки подстновки поля Circuit-ID в PPPoE-пакеты)
  - RCP Server Settings (Настройки сервера RCP)
  - SMTP Settings (Настройки почтовых уведомлений)
  - SNTP (Настройки синхронизации времени)
  - Flash File System Settings (Настройки файловой системы флеш-диска)
- OAM (Методы доступа к объектам)
  - Connectivity Fault Management (CFM) (Настройки протокола CFM)
  - Ethernet OAM (Настройки процедур обслуживания и экспплуатации Ethernet)
  - Cable Diagnostics (Диагностика кабеля)
- Monitoring (Просмотр состояния)
  - Utilization (Загруженность)

- Statistics (Статистика)
- Mirror (Зеркалирование портов)
- sFlow (Отправка информации о потоках трафика)o Ping Test (Утилита ping)
- Trace Route (Утилита traceroute)
- 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 управления сетью по протоколу SNMP

4.1.1 *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»

4.1.2 *Утилита mbrowse*

Данная утилита входит в стандартный пакет программного обеспечения операционной системы Arch Linux и используется для просмотра и изменения параметров удалѐнной системы по протоколу SNMP. Для еѐ 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 определѐнного 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).

4.2 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). Ещѐ 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 трѐх
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 *.

4.3 Способы управления коммутаторами

4.3.1. Технология Single IP Management

Введение

Объединение устройств в стек требует наличия специальных модулей и кабелей для стекирования, что ограничивает возможность включения в стек коммутаторов различных моделей, кроме того требуется установка коммутаторов в один монтажный шкаф. Устранить эти ограничения позволяет использование новой технологии Single IP Management.

Технология Single IP Management (SIM) – это технология управления виртуальным стеком через единый IP-адрес (рисунок 4.1).

Рисунок 4.1

Технология SIM позволяет:

- ✓ устранить ограничения на модели коммутаторов, объединяемых в стек;
- ✓ уменьшить количество управляющих IP-адресов сети;
- ✓ устранить необходимость использования специализированных модулей и кабелей, предназначенных для стекирования;
- ✓ преодолеть ограничения, связанные с длиной кабелей в стеке.

В отличие от стеков, построенных с использованием традиционных методов стекирования, виртуальный стек на основе технологии SIM позволяет включить в группу большее количество коммутаторов. Например, компания D-Link позволяет включить до 32 коммутаторов в виртуальный стек, в то время как традиционные стеки того же производителя ограничены максимум 12 коммутаторами. При этом виртуальный стек может быть расширен коммутаторами разного типа – от недорогих коммутаторов 2-го уровня до высокопро-изводительных коммутаторов на основе шасси (для ядра сети).

Объединение коммутаторов в SIM-стек не требует использования специальных соединительных кабелей. Трафик, передаваемый между устройствами стека, проходит через полнодуплексные интерфейсы Fast Ethernet, Gigabit Ethernet или 10 Gigabit Ethernet по обычным медным или оптическим кабелям. Отказ от использования специализированных стекирующих кабелей позволяет преодолеть ограничения, связанные с их длиной. В стек могут быть объединены устройства, расположенные в любом месте сети. Расстояния между узлами виртуального стека определяется лишь ограничениями соответствующего стандарта IEEE 802.3 и может достигать десятки километров.
Ниже (рисунок 4.2) приведена архитектура SIM.

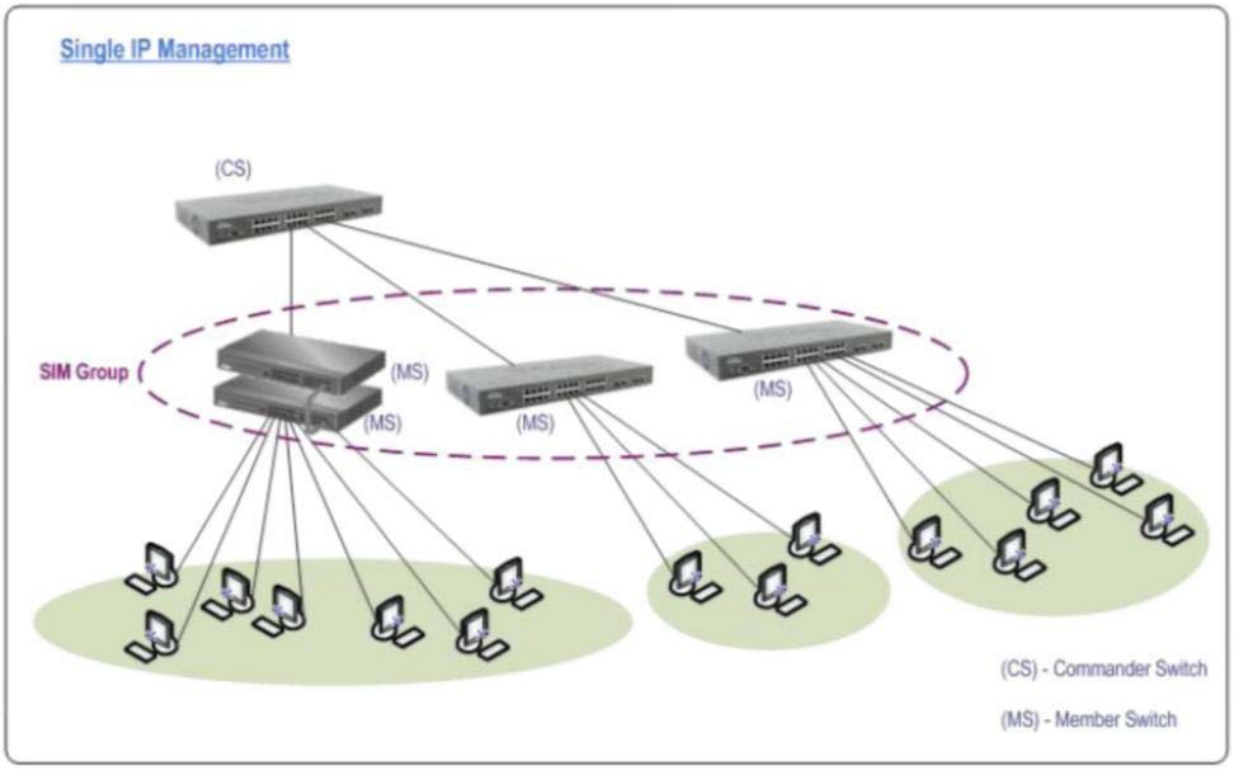


Рисунок 4.2.

Группа SIM состоит из трѐх компонент:

- ✓ Commander Switch (CS) – командный коммутатор;
- ✓ Member Switch (MS) – коммутатор-участник;
- ✓ Candidate Switch (CaS) – коммутатор-кандидат.

Рисунок 42. Группа SIM состоит из трѐх компонент:

- ✓ Commander Switch (CS) – командный коммутатор;
- ✓ Member Switch (MS) – коммутатор-участник;
- ✓ Candidate Switch (CaS) – коммутатор-кандидат.

Каждая группа SIM состоит из одного командного коммутатора и максимум 32 коммутаторов-участников.

Командный коммутатор используется для управления всеми коммутаторами в группе SIM и обладает следующими характеристиками:

- ✓ имеет назначенный IP-адрес;
- ✓ не является командным коммутатором или коммутатором участником другой группы SIM;
- ✓ подсоединѐн к коммутаторам-участникам через собственную управляющую VLAN.

Коммутатор-участник является коммутатором, который входит в группу SIM, доступен с командного коммутатора и обладает следующими характеристиками:

- ✓ не является командным или коммутатором-участником другой группы SIM;
- ✓ подсоединѐн к другим коммутаторам-участникам через общую VLAN.

Коммутатор-кандидат – это коммутатор, который готов вступить в группу SIM, но пока не является членом ни одной группы. Коммутатор-кандидат может вступить в группу SIM, используя автоматическую функцию, встроенную в SIM-коммутаторы, или путѐм ручной

настройки. Коммутатор, сконфигурированный как CaS, не является членом SIM и обладает следующими характеристиками:

- ✓ не является командным или коммутатором-участником другой группы SIM;
- ✓ подсоединѐн к другим коммутаторам-участникам через общую VLAN.

После настройки одного коммутатора в качестве управляющего SIM-группы, другие коммутаторы могут стать членами группы через непосредственное подключение к управляющему коммутатору. Только управляющий коммутатор может обращаться к CaS, он является своеобразной точкой доступа к членам группы. IP-адрес управляющего коммутатора станет адресом для всех членов группы, управление же доступом ко всем членам группы будет осуществляться через пароль администратора CS и/или аутентификацию. Когда функция SIM включена, приложения управляющего коммутатора будут перенаправлять пакеты вместо их обработки. Приложения будут декодировать пакет от администратора, видоизменять некоторые данные и затем отправлять его членам группы. После выполнения этих действий управляющий коммутатор может получить ответный пакет, который закодирует и отправит обратно администратору. После того, как управляющий коммутатор станет обыкновенным членом SIM-группы, он будет членом первой SNMP-группы (включая права чтения/записи и права только чтения), к которой принадлежал управляющий коммутатор. Однако если у коммутатора MS есть свой собственный IP-адрес, то он может принадлежать к SNMP-группе, в которой другие коммутаторы SIM-группы не состоят.

Версии SIM

Существуют следующие версии SIM: 1.0, 1.5 и 1.6. Ниже они будут рассмотрены в сравнении.

Версии 1.0 и 1.5

Версия SIMv1.5 предлагает следующие улучшения по сравнению с версией 1.0:

✓ Возможность сохранения списка всех коммутаторов-участников в энергонезависимой памяти командного коммутатора. В версии SIMv1.0 командный коммутатор не имел возможности сохранять информацию о коммутаторах-участниках в своей памяти. Следовательно, если коммутатор-участник перегружался, он принимал статус коммутатора CaS. В версии SIMv1.5, если информация о коммутаторе-участнике была сохранена в памяти командного коммутатора, то после перезагрузки коммутатору-участнику автоматически присваивался статус MS. Если же перегружается командный коммутатор, то он заново собирает информацию о топологии сети.

✓ Возможность отображения информации о магистральных группах (trunks) в топологической карте сети. В версии SIMv1.0 отображалась только пропускная способность порта вне зависимости от его принадлежности к магистральной группе. Версия SIMv1.5 показывает пропускную способность всей магистральной группы, а не порта. Когда организована магистральная группа, на топологической карте отражается множество линий.

- ✓ Меньший размер программного обеспечения.
- ✓ Поддержка масштабирования топологической карты при просмотре через web-браузер.
- ✓ Поддержка нескольких конфигурационных загрузочных файлов.

Версии 1.5 и 1.6

Несмотря на улучшения по сравнению с предыдущей версией версия SIMv1.5 имеет несколько недостатков, связанных с безопасностью. Большинство подобных недостатков связаны с передачей пакетов без возможности их шифрования. Таким образом, версия SIMv1.6 призвана улучшить безопасность технологии SIM путѐм добавления механизмов шифрования/дешифрования. Существует обратная совместимость версий 1.6 и 1.5.

Формат пакета

Ниже (рисунок 4.3) приведѐн формат пакета для версии 1.6. Данный формат пакета применим для пакетов обнаружения (Discovery Packets), пакетов отчѐта (Report Packets), пакетов поддержки (Maintence Packets), конфигурационных пакетов (Configuration Packets) и пакетов перенаправления (Redirection Packets) и не применим для пакетов построения топологии (Topology Packets). Также стоит отметить, что, когда устройство, не поддерживающее шифрование, получает зашифрованный пакет, то данное устройство будет отбрасывать пакеты обнаружения и отчѐтов.

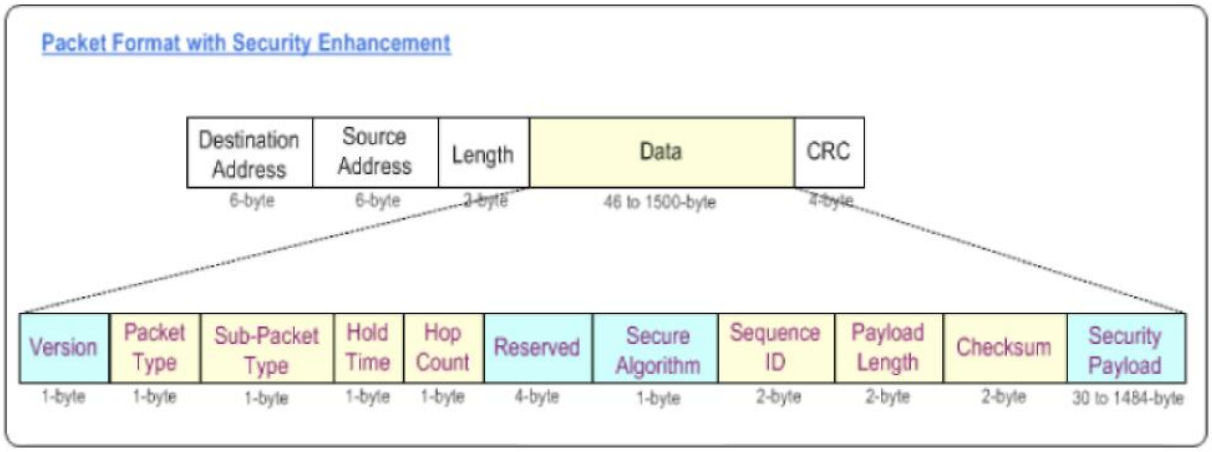


Рисунок 4.3.

Назначение полей в пакете формата secure то же самое, что в пакете формата unsecure, за исключением следующих полей:

- Version – версия пакета SIM. Версия пакета представленного формата – 0x02.
- Reserved – длина этого поля меняется от 5 до 4 байт. Значение поля всегда составляет 0x00.
- Secure Algorithm – алгоритм шифрования:

✓ 0x00 – отсутствует;
✓ 0x01 – внутренний алгоритм D-Link (XOR);
✓ 0x01 … 0xFF – зарезервировано для дальнейшего использования.

- Payload – полезная зашифрованная нагрузка.

Операции SIMv1.6

Операции SIM версии 1.6 разделены на три уровня (этапа):

✓ Collection – сбор информации;
✓ Maintenance – поддержка;
✓ Managment – управление.

Этап сбора информации (Collection Stage)

На данном этапе командный коммутатор CS периодически рассылает пакеты отчѐта Report (как зашифрованные, так и нет) коммутатором-кандидатам CaS, а кандидаты с той же периодичностью рассылают пакеты обнаружения Discovery. Пакеты Report/Discovery с поддержкой механизма безопасности будут зашифрованы алгоритмом по умолчанию. Дополнительно некоторая информация о механизмах безопасности включается в полезную нагрузку. Это данные о максимальных и предпочитаемых уровнях безопасности, которые поддерживает устройство. Следующая диаграмма (рисунок 44) иллюстрирует операции, производимые коммутатором CS после получения данных от коммутаторов CaS:

1. Коммутатор CaS посылает одновременно два Discovery-пакета (один зашифрованный, другой – нет).
2. Когда коммутатор CS получает незашифрованный пакет, он ждѐт 20 секунд до получения зашифрованного Discovery-пакета. Если в течение данного интервала времени зашифрованный пакет будет получен, то командный коммутатор определит коммутатор CaS как коммутатор, поддерживающий механизмы безопасности. Иначе коммутатор CaS будет определѐн как коммутатор, не поддерживающий механизмы безопасности.
3. Далее информация о коммутаторе CaS будет записана в базу данных коммутаторов CaS.

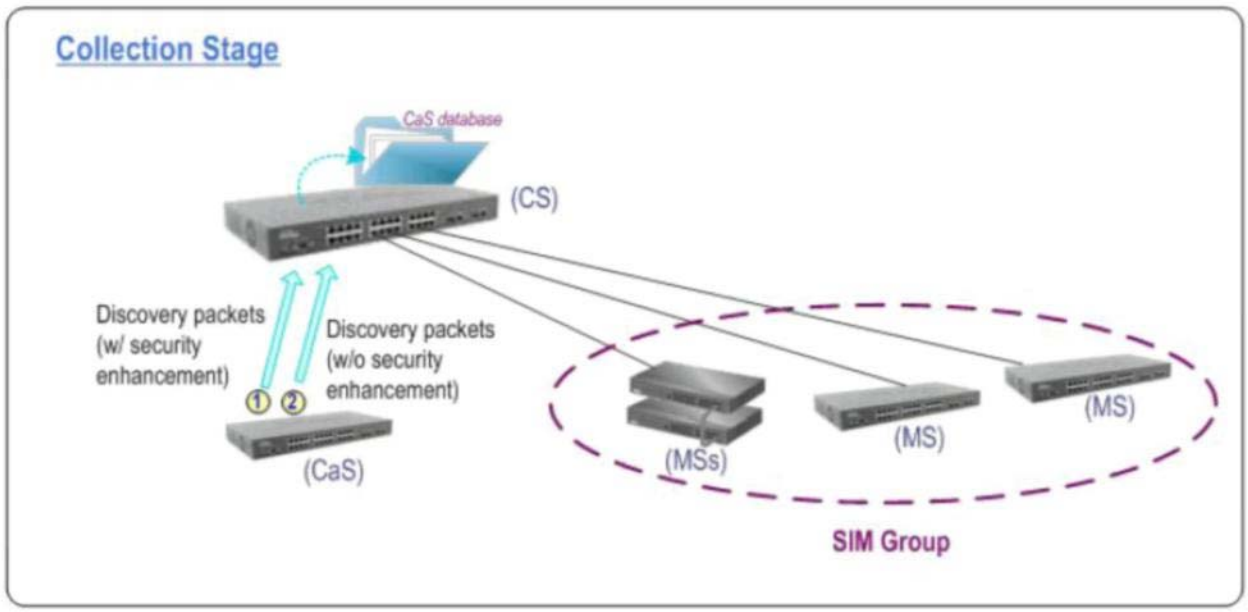


Рисунок 4.4.

Этап поддержки (Maintenance Stage)

После обмена Discovery/Report-пакетами наступает этап поддержки. Следующий рисунок 4.5 показывает операции, выполняемые в командном коммутаторе, по добавлению и конфигурированию коммутаторов CaS как членов его SIM-группы и операции, выполняемые в коммутаторе CaS, по получению команды для присоединения к SIM-группе.

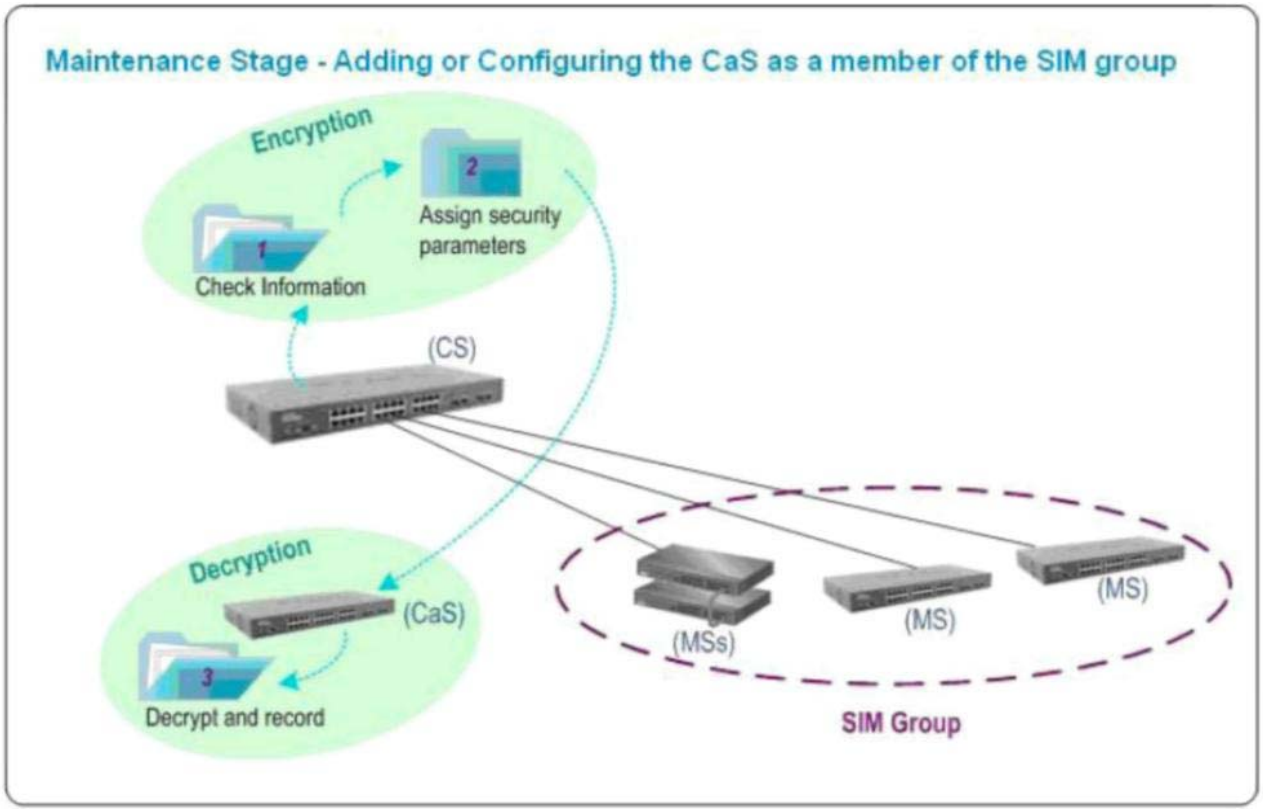


Рисунок 4.5. *Этап управления*

Назначение данного этапа перевести коммутатора-кандидата в роль коммутатора-участника (MS). Новый коммутатор MS примет и последует методу обмена информацией, установленном на данном этапе, для взаимодействия с остальными коммутаторами-участниками и командным коммутатором своей группы.

Взаимодействия в топологии SIM

Взаимодействие между коммутаторами в топологии SIM могут осуществляться в 5 различных режимах (в зависимости от того, поддерживает ли командный коммутатор механизмы безопасности или нет):

1. Когда командный коммутатор не поддерживает механизмы безопасности, всѐ взаимодействие между ним и остальными участниками группы происходит без применения шифрования. Возможные режимы обмена для данного случая показаны на рисунке 4.6.

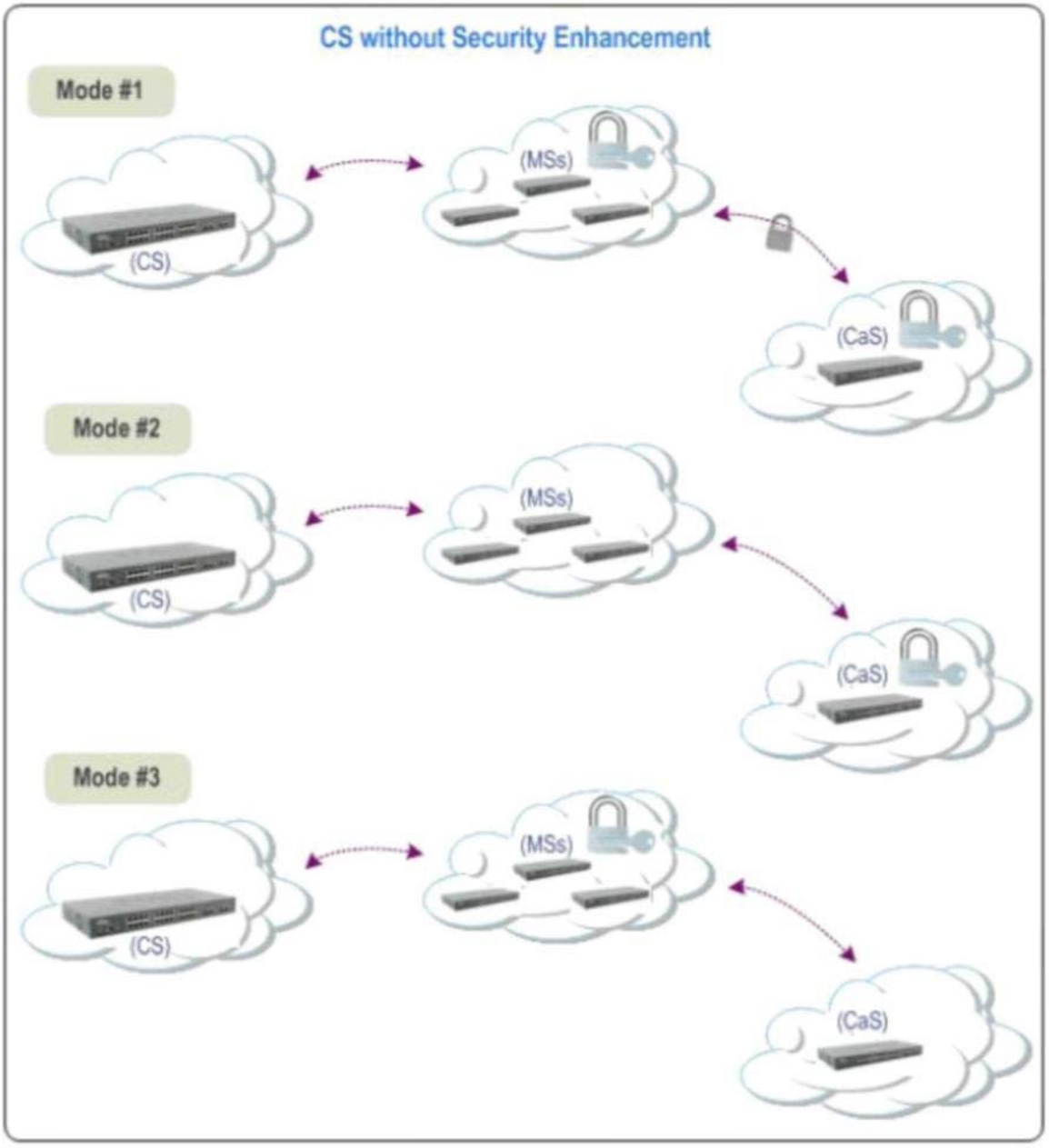


Рисунок 4.6.

2. Когда все коммутаторы группы (CS, MSs, CaSs) поддерживают механизмы безопасности, все взаимодействия между ними производятся только в безопасном режиме. Данная концепция проиллюстрирована в режиме 1 (Mode #1) на рисунке 47. Остальные режимы иллюстрируют ситуации, когда тот или иной член группы не поддерживает механизмы безопасности.

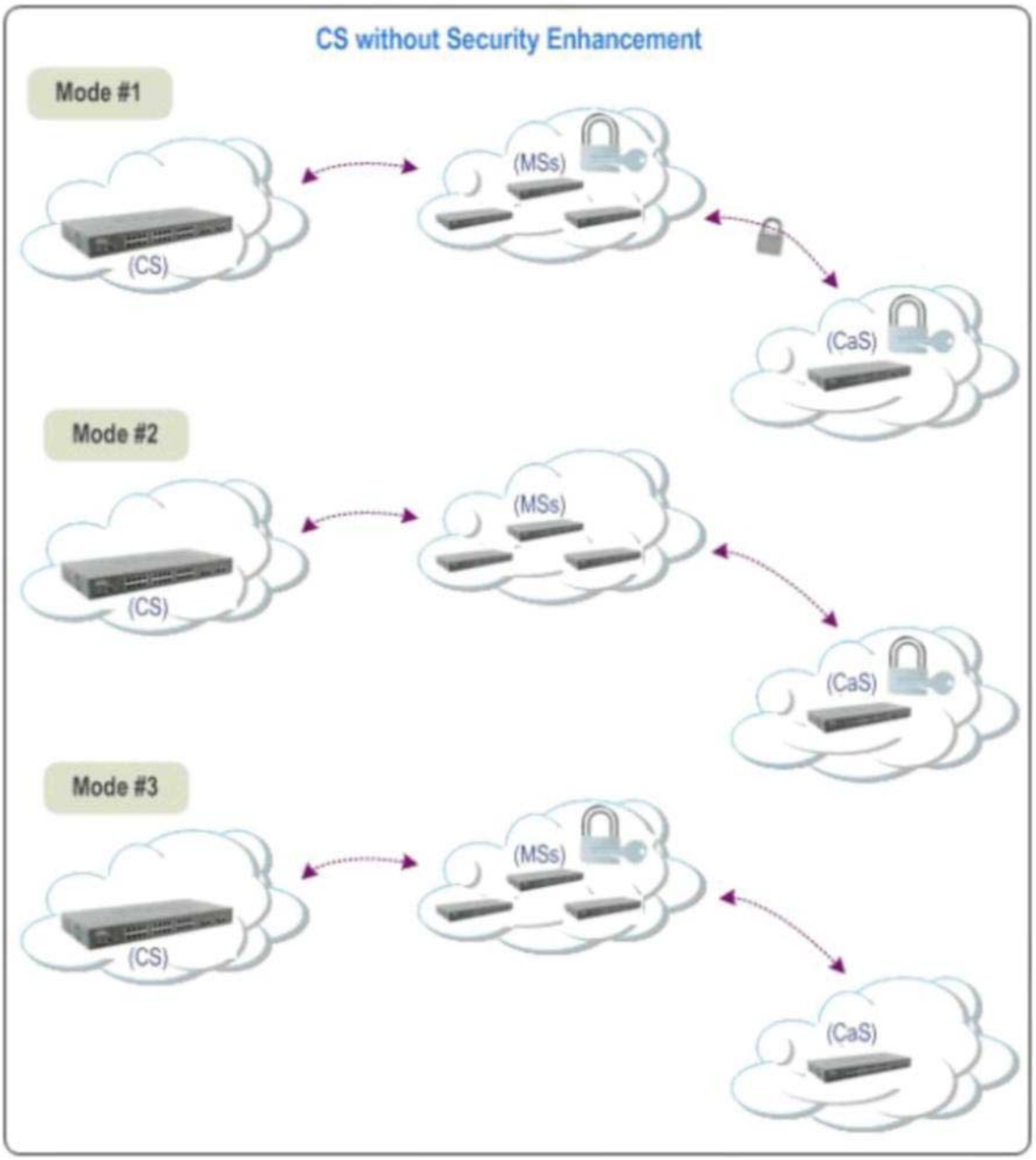

CS without Security Enhancement
Mode #1
(MSs)
(CS)
(CaS)
Mode #2
(MSs)
(CS)
(CaS)
Mode #3
(MSs)
(CS)
(CaS)

Рисунок 4.7.

4.4 Протокол SNMP

4.4.1. Определение и функции протокола

Протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью) является протоколом Прикладного уровня, разработанный для выполнения двух задач:

- мониторинг сетевых устройств и сети в целом;
- управление сетевыми устройствами.

Протокол SNMP предоставляет возможность станциям управления считывать и изменять настройки шлюзов, маршрутизаторов, коммутаторов и прочих сетевых устройств.

4.4.2. Версии протокола SNMP

Опишем различия между версиями протокола SNMP и документы, определяющие эти версии. По состоянию на 2006 год единственной не устаревшей версией SNMP является SNMPv3, определѐнная в RFC 3411-3418.

SNMPv1

Первые RFC, описывающие стандарты SNMP, появились в 1988 году. Версия 1 подверглась критике за еѐ посредственную модель безопасности на основе сообществ. В то время безопасность в Интернете не входила в круг первоочередных задач рабочих групп IETF.

SNMPv2

Версия 2, известная так же, как Party-based SNMPv2, или SNMPv2p, не получила широкого распространения из-за серьѐзных разногласий по поводу инфраструктуры безопасности в стандарте. SNMPv2 улучшал версию 1 в области быстродействия, безопасности, конфиденциальности и взаимодействий «менеджер-менеджер». Он представил новый тип PDU Get-Bulk-Request, альтернативу Get-Next-Request для получения больших объѐмов информации при помощи одного запроса. Тем не менее, новая система безопасности на основе сторон выглядела для многих как чересчур сложная и не была широко признана.

SNMPv2c

Community-based SNMPv2, или SNMPv2c, представил SNMPv2 без новой модели безопасности версии 2. Вместо неѐ предлагалось использовать старую модель безопасности версии 1 на основе сообществ. Соответствующее предложение RFC было принято только как черновик стандарта, однако стало де факто стандартом SNMPv2. Безопасность SNMP снова оказалась нерешѐнным вопросом.

SNMPv2u

User-based SNMPv2, или SNMPv2u, является компромиссом между незащищѐнностью SNMPv1 и чрезмерной сложностью SNMPv2p. Предложенная модель безопасности на основе пользователей была положена в основу SNMPv3.

SNMPv3

SNMPv3 наконец-то решил проблемы с безопасностью способом, который многие посчитали приемлемым. Версия 3 SNMP принята IETF как стандарт Интернета (IETF STD 62). Почти все предыдущие RFC признаны устаревшими. Документы, описывающие протокол SNMPv3, приведены ниже:

- *Общая информация.*

  RFC 3411. An Architecture for Describing SNMP Management Frameworks.

  - *Обработка сообщений.*

  > Привязки к транспорту.

    RFC 3417. Transport Mappings for the SNMP.

  > Разбор и диспетчеризация сообщений.

    RFC 3412. Message Processing and Dispatching for the SNMP.

  > *Безопасность.*

    RFC 3414. User-based Security Model (USM) for SNMPv3.

- Обработка PDU.

  > Операции протокола.

    RFC 3416. Version 2 of the Protocol Operations for SNMP.

  > Приложения SNMP.

    RFC 3413. SNMP Applications.

  > Управление доступом.

    RFC 3415. View-based Access Control Model (VACM) for the SNMP.

- Модули MI B.

  RFC 3418. MIB for the SNMP.

4.4.3. Модель протокола SNMP Общая модель

Модель приведена на рисунке 70. Основными взаимодействующими элементами протокола являются агенты (agent) и системы управления сетью (NMS, network management system). С точки зрения концепции «клиент-сервер» роль сервера выполняют агенты, то есть те самые устройства, для опроса состояния которых используется протокол SNMP. Соответственно, роль клиентов отводится системам управления - сетевым приложениям, необходимым для сбора информации о функционировании агентов. Взаимодействие агентов и систем управления осуществляется на основе сообщений протокола SNMP.

Агентами в SNMP являются программные модули, которые работают в управляемых устройствах. Агенты собирают информацию об управляемых устройствах, в которых они работают. Агент содержат всю информация об управляемом сетевом устройстве в базе управляющей информации (MIB, management information base). MIB представляет собой совокупность объектов, доступных для операций записи-чтения.

В любой управляемой сети может иметься одна или более NMS. NMS выполняют прикладные программы сетевого управления, которые представляют информацию управления конечному пользователю.

Структура базы MIB

На данный момент существует четыре типа информационной базы MIB:

1. Internet MIB – информационная база объектов для обеспечения диагностики ошибок и конфигураций. Включает в себя 171 объект (в том числе и объекты MIB I).
2. LAN manager MIB – база из 90 объектов – пароли, сессии, пользователи, общие ресурсы.
3. WINS MIB – база объектов, необходимых для управления и диагностики WINS-сервера (в серверах Microsoft Windows физически находится в файле WINSMIB.DLL).
4. DHCP MIB – база объектов, необходимых для управления и диагностики DHCP-сервера (в серверах Microsoft Windows физически находится в файле DHCPMIB.DLL).

Структуру MIB определяет документ, называемый SMI (Structure of Management Information, структура управляющей информации). Все MIB имеют иерархическую древовидную структуру. Все базы содержат десять корневых алиасов (ветвей), представленных на рисунке 4.9:

1. *System* – данная группа MIB II содержит в себе семь объектов, каждый из которых служит для хранения информации о системе (версия ОС, время работы и т.д.).
2. *Interfaces* – содержит 23 объекта, необходимых для ведения агентами статистики по сетевым интерфейсам управляемого устройства (количество интерфейсов, размер MTU, скорость передачи данных, физические адреса и т.д.).
3. *AT* – содержит 3 объекта, отвечающих за трансляцию адресов. Более не используется. Была включена в MIB I. Примером использования объектов AT может послужить простая ARP таблица соответствия физических (MAC) адресов сетевых карт IP адресам машин. В SNMP v2 эта информация была перенесена в MIB для соответствующих протоколов.
4. *IP* – содержит 42 объекта, в которых хранятся данные о проходящих IP пакетах.
5. *ICMP* – содержит 26 объектов со статистикой об ICMP-сообщениях.
6. *TCP* – содержит 19 объектов, хранящих статистику по протоколу TCP (соединения, открытые порты и т.д.).
7. *UDP* – содержит 6 объектов, хранящих статистику по протоколу UDP (входящие/исходящие датаграммы, порты, ошибки).
8. *EGP* – содержит 20 объектов – данные о трафике Exterior Gateway Protocol.
9. *Transmission* – зарезервирована для специфических задач.
10. *SNMP* – содержит 29 объектов, в которых хранится статистика по SNMP-протоколу (входящие/исходящие пакеты, ограничения пакетов по размеру, ошибки, данные об обработанных запросах и многое другое).

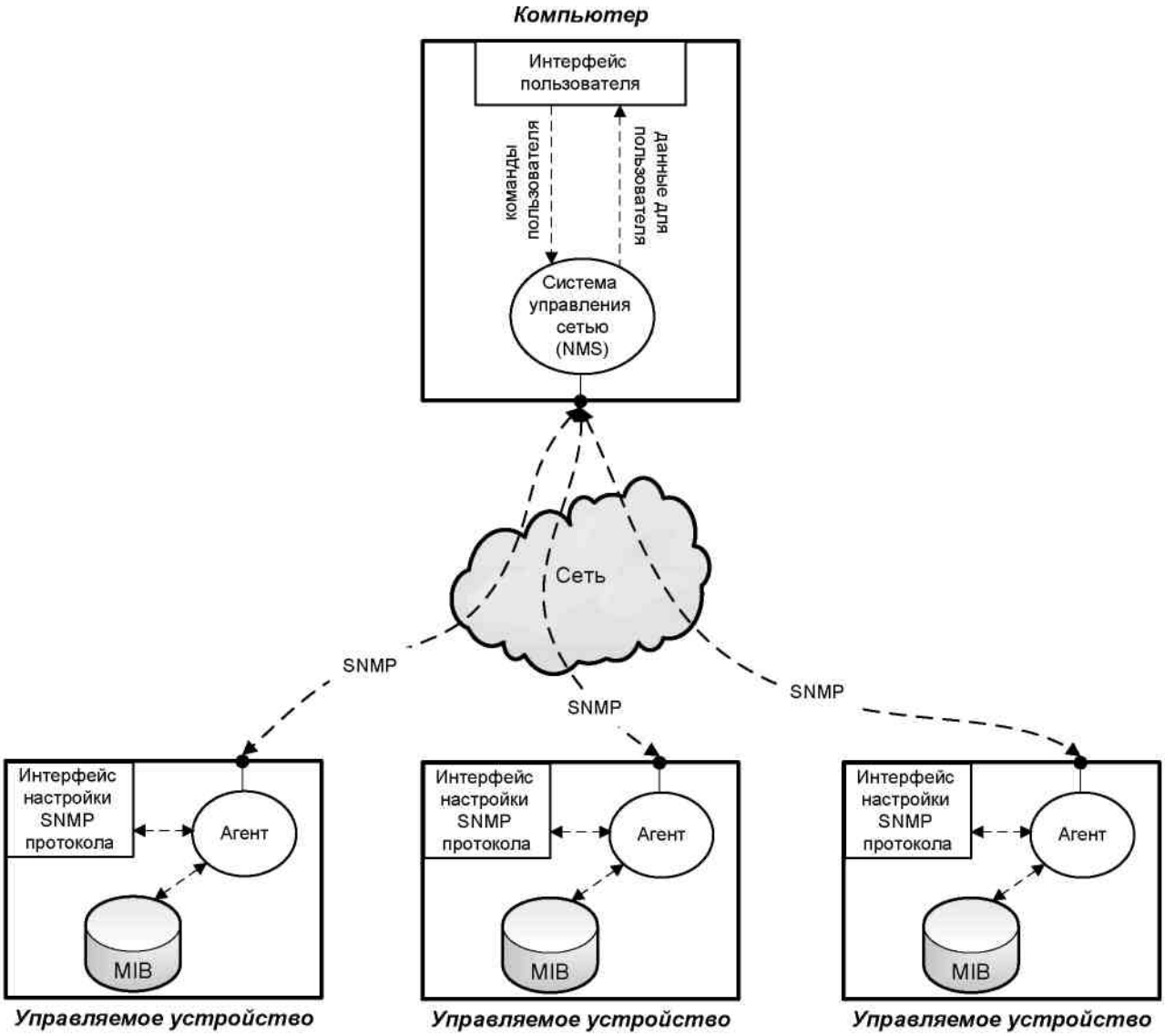

Компьютер
Интерфейс пользователя
команды пользователя
данные для пользователя
Система управления сетью (NMS)
Сеть
SNMP
SNMP
SNMP
Интерфейс настройки SNMP протокола
Агент
MIB
Управляемое устройство
Интерфейс настройки SNMP протокола
Агент
MIB
Управляемое устройство
Интерфейс настройки SNMP протокола
Агент
MIB
Управляемое устройство

Рисунок 4.8.

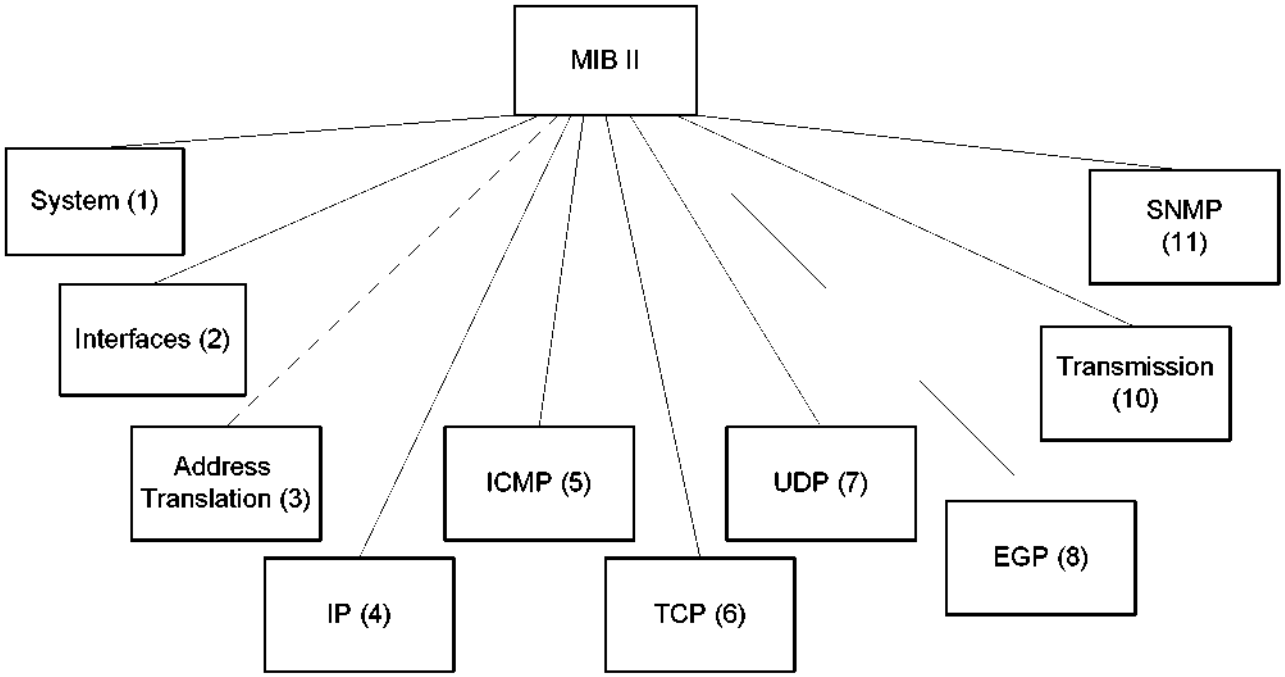


Рисунок 4.9.

Каждая из ветвей в свою очередь также представима в виде дерева. Например, к адресу администратора мы можем обратиться посредством такого пути: system.sysContact.0, ко времени работы системы system.sysUpTime.0. С другой стороны те же данные могут задаваться и в точечной нотации. Так system.sysUpTime.0 соответствует значение 1.3.0, так как system имеет индекс «1» в группах MIB II, а sysUpTime – «3» в иерархии группы system. Ноль в конце пути говорит о скалярном типе хранимых данных. В процессе работы SNMP-протокол использует точечную нотацию, то есть если менеджер запрашивает у агента содержимое параметра system.sysDescr.0, то в строке запроса ссылка на объект будет преобразована в «1.1.0».

Дерево MIB расширяемо благодаря экспериментальным и частным ветвям. Например, поставщики могут определять свои собственные ветви для включения реализаций своих изделий. В настоящее время вся работа по стандартизации ведется на экспериментальной ветви.

SMI определяет следующие типы данных MIB:

1. Network addresses (сетевые адреса) – символьные строки, представляющие адреса из конкретного стека протоколов. В настоящее время единственным примером сетевых адресов являются 32-битовые IP-адреса.
2. Counters (счетчики) – неотрицательные целые числа, которые монотонно увеличиваются до тех пор, пока не достигнут максимального значения, после чего они сбрасываются до нуля. Примером счетчика является общее число байтов, принятых интерфейсом.
3. Gauges (измерители) – неотрицательные целые числа, которые могут увеличиваться или уменьшаться, но фиксируются при достижении максимального значения. Примером типа «gauges» является длина очереди, состоящей из выходных пакетов.

4. Ticks (тики) – сотые доли секунды, прошедшие после какого-нибудь события. Примером типа «ticks» является время, прошедшее после вхождения интерфейса в свое текущее состояние.
5. Opaque (непрозрачный) – произвольное тип данных. Используется для передачи произвольных информационных последовательностей, находящихся вне пределов точного печатания данных, которое использует SMI.

Основные команды системы NMS

Если NMS хочет проконтролировать какое-либо из управляемых устройств, она делает это путем отправки ему сообщения с указанием об изменении значения одной из его переменных. В целом управляемые устройства отвечают на четыре типа команд (или инициируют их):

1. Reads.

   Для контролирования управляемых устройств NMS считывают переменные, поддерживаемые этими устройствами.

2. Writes.

   Для контролирования управляемых устройств NMS записывают переменные, накопленные в управляемых устройствах

3. Traversal operations.

   NMS используют операции прослеживания, чтобы определить, какие переменные поддерживает управляемое устройство, а затем собрать информацию в таблицы переменных.

4. Traps.

   Управляемые устройства используют «ловушки» для асинхронных сообщений в NMS о некоторых событиях.

4.4.4. Протокол SNMPv3

Начиная с января 1998 года, выпущен набор документов, посвященных SNMPv3. В этой версии существенно расширена функциональность, разработана новая система безопасности.

Протокол обмена данными

Ниже на рисунке 4.10 приведена временная диаграмма, на которой в общем виде представлен протокол обмена SNMP-сообщениями. Для своей работы протокол SNMP использует транспортный протокол UDP, в основном 161 порт. Но для trap-сообщений используется 162 порт. Возможные команды протокола SNMPv3 приведены в таблице 4.1.

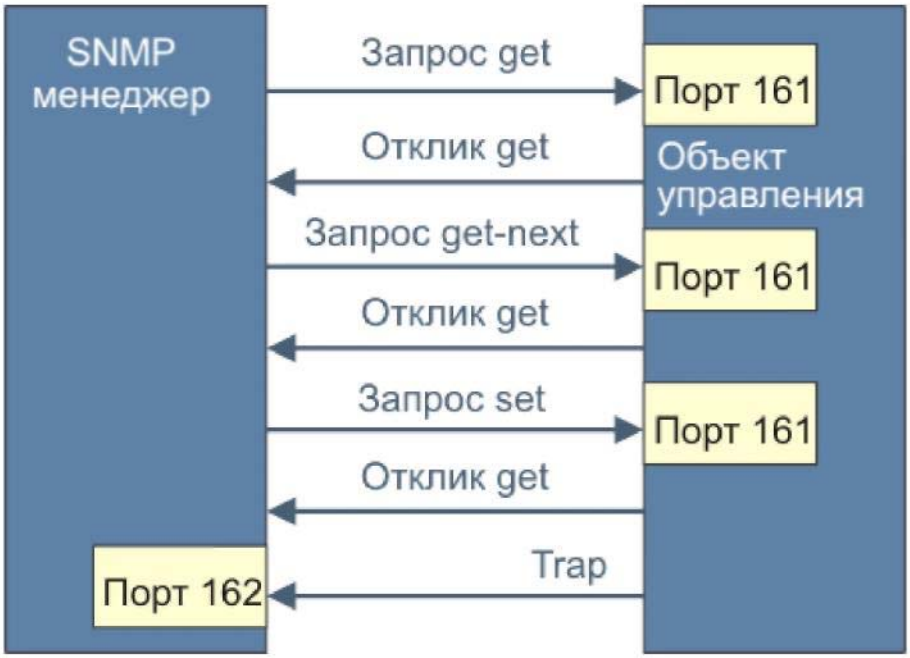


Рисунок 4.10

Команда SNMP	Тип PDU	Назначение
GET-request	0	Получить значение указанной переменной или информацию о состоянии сетевого элемента.
GET-next-request	1	Получить значение переменной, не зная точного еѐ имени (следующий логический идентификатор на дереве MIB).
SET-request	2	Присвоить переменной соответствующее значение. Используя для описания действия, которое должно быть выполнено.
GET-response	3	Отклик на GET-request, GET-next-request и SET-request. Содержит также информацию о состоянии (коды ошибок и другие данные).
TRAP	4	Отклик сетевого объекта на событие или на изменение состояния.
GetBulkRequest	5	Запрос пересылки больших объемов данных, например, таблиц.
InformRequest	6	Менеджер обращает внимание партнѐра на определенную информацию в MIB.
SNMPv3-Trap	7	Отклик на событие (расширение по отношению к v1 и v2).
Report	8	Отчѐт (функция пока не задана).

Таблица 4.1 Основные команды протокола SNMPv3.

Формат SNMP-сообщения

Полное описание формата сообщения протокола SNMPv3 дано в документе RFC-3412 в

разделе 6 «The SNMPv3 Message Format». Формат сообщения представлен на рисунке 4.11.

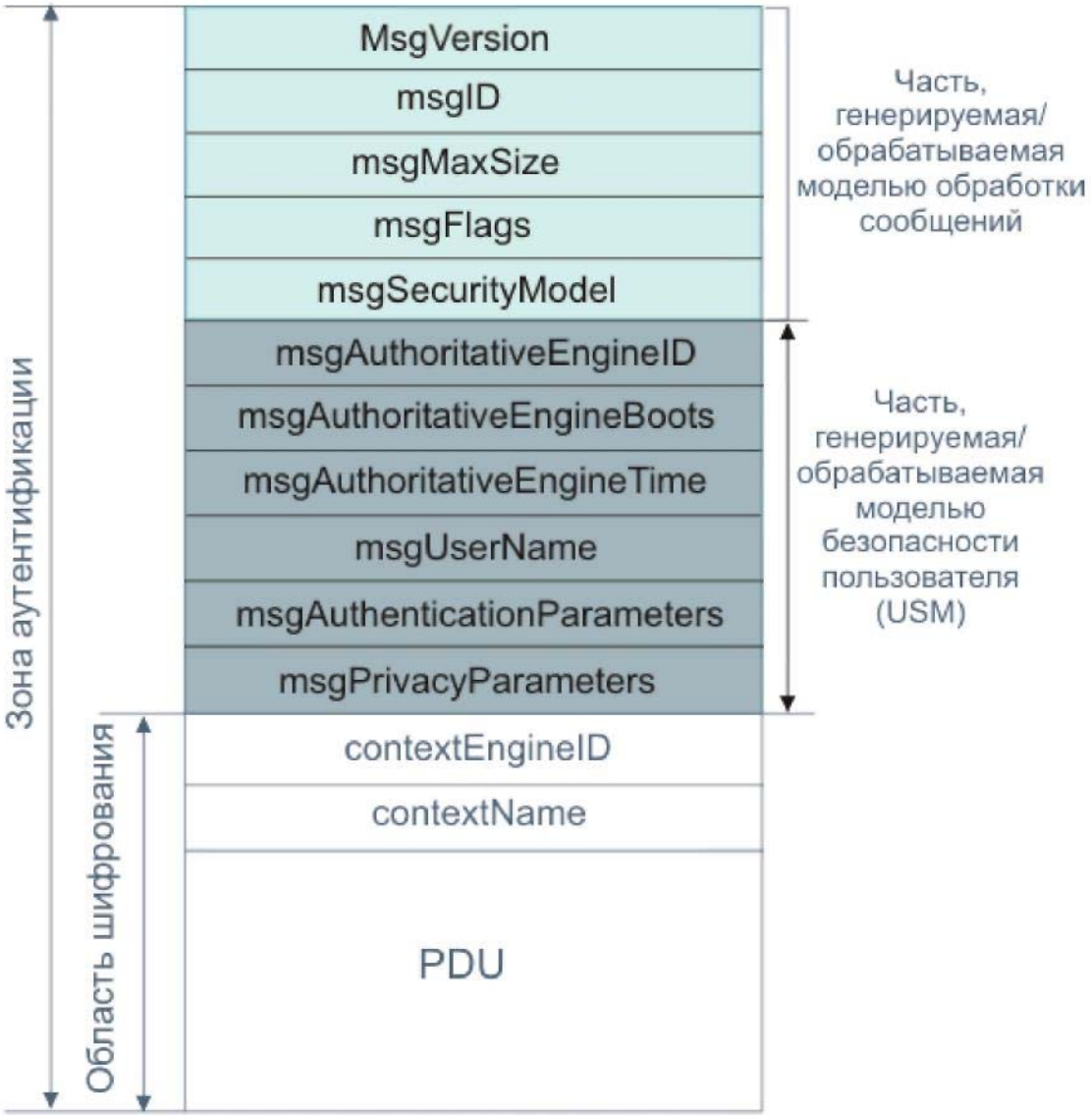


Рисунок 4.11.

SNMP-сообщение логически разделено на три части:

1. Часть, которая формируются отправителем в рамках модели обработки сообщений и обрабатываются получателем.
2. Часть, отвечающая за функции безопасности.
3. Собственно поле данных.

Для реализации модели обработки сообщений используются следующие поля:

- **msgVersion**. Версия протокола. Для протокола SNMPv3 значение в поле равно 3.
- **msgID.** Уникальный идентификатор, используемый SNMP-сущностями для установления соответствия между запросом и откликом. Значение msgID лежит в диапазоне 0 - (2^{31}-1).**msgMaxSize.** Максимальный размер сообщения в октетах, поддерживаемый отправителем. Его значение лежит в диапазоне 484 - (2^{31}-1) и равно максимальному размеру сегмента, который может воспринять отправитель.
- **msgFlags.** Однобайтовая строка, содержащая три флага в младших битах:

- *reportableFlag.* Если reportableFlag=1, то должно быть прислано сообщение с отчѐтом (команда Report). Флаг reportableFlag устанавливается отправителем во всех сообщениях запроса (команды Get, Set, Inform). Флаг устанавливается равным нулю в откликах и Trap-уведомлениях;
- *privFlag;*
- *authFlag.*

Флаги privFlag и authFlag устанавливаются отправителем для индикации уровня безопасности для данного сообщения. Для privFlag=1 используется шифрование, а для authFlag=0 - аутентификация. Допустимы любые комбинации значений флагов кроме privFlag=1 AND authFlag=0 (шифрование без аутентификации).

- **msgSecurityModel**. Идентификатор со значением в диапазоне 0 - (2^{31}-1), который указывает на модель безопасности, используемую при формировании данного со общения. Зарезервированы значения 1 - для SNMPv1, 2 и 3 - для SNMPv3.

4.4.5. Безопасность протокола SNMPv3 Модели безопасности протоколов SNMPv1-v3

Перечислим модели безопасности, применяющиеся в соответствующих версиях протокола SNMP:

1. *SNMPv1*

   SNMPv1 - Community-based Security Model

2. *SNMPv2*

   SNMPv2p - Party-based Security Model SNMPv2c - Community-based Security Model SNMPv2u - User-based Security Model

3. *SNMPv3*

   SNMPv3 - USM User-based Security Model

Модель безопасности на основе сообществ

Модель безопасности на основе сообществ (Community-based Security Model) была первой, самой простой и самой небезопасной. Она подразумевает лишь аутентификацию на основе «строки сообщества», фактически, пароля, передаваемого по сети в теле сообщения SNMP в открытом тексте. Эта модель безопасности не в состоянии бороться ни с одной из угроз информационной безопасности. Тем не менее, она часто используется до сих пор в связи со своей простотой, а также благодаря наличию внешних, не связанных с SNMP систем безопасности, например, межсетевых экранов.

Модель безопасности на основе сторон

Модель безопасности на основе сторон (Party-based Security Model) подразумевает введение понятие стороны. Сторона — это виртуальное окружение исполнения, в котором набор допустимых операций ограничен административно. Сущность SNMP при обработке сообщения действует как сторона, поэтому ограничена операциями, определѐнными для этой стороны. Сторона определяется следующими параметрами:

1. Уникальный идентификатор стороны.
2. Логический сетевой адрес (адрес транспортного протокола).

3. Протокол аутентификации и параметры, требующиеся для аутентификации всех сообщений стороны.
4. Протокол шифрования и параметры, требующиеся для шифрования всех сообщений стороны. Могут использоваться различные алгоритмы для протоколов аутентификации и шифрования. Обычно в качестве алгоритма для протокола аутентификации используют хэш-функцию Message Digest 5 (MD5), а для протокола шифрования — алгоритм Data Encryption Standard (DES) в режиме Cipher Block Chaining (CBC). При использовании соответствующих протоколов аутентификации и шифрования модель успешно справляется с большинством угроз безопасности. Данная модель безопасности не была широко принята, поскольку показалась многим слишком сложной и запутанной.

Модель безопасности на основе пользователей

Модель безопасности на основе пользователей (User-based Security Model) вводит понятие пользователя, от имени которого действует сущность SNMP. Этот пользователь характеризуется именем пользователя, используемыми протоколами аутентификации и шифрования, а также закрытым ключом аутентификации и шифрования. Аутентификация и шифрование являются необязательными. Модель безопасности во многом похожа на модель на основе сторон, но она упрощает идентификацию пользователей, распределение ключей и протокольные операции.

Модель безопасности USM

Модель безопасности USM (User-Based Security Model) использует концепцию авторизованного сервера (authoritative Engene). При любой передаче сообщения одна или две сущности, передатчик или приемник, рассматриваются в качестве авторизованного SNMP-сервера. Это делается согласно следующим правилам:

1. Когда SNMP-сообщение содержит поле данных, которое предполагает отклик (например, Get, GetNext, GetBulk, Set или Inform), получатель такого сообщения считается авторизованным.
2. Когда SNMP-сообщение содержит поле данных, которое не предполагает посылку отклика (например, SNMPv2-Trap, Response или Report), тогда отправитель такого сообщения считается авторизованным.

Таким образом, сообщения, посланные генератором команд, и сообщения Inform, посланные отправителем уведомлений, получатель является авторизованным. Для сообщений, посланных обработчиком команд или отправителем уведомлений Trap, отправитель является авторизованным. Такой подход имеет две цели:

1. Своевременность сообщения определяется с учетом показания часов авторизованного сервера. Когда авторизованный сервер посылает сообщение (Trap, Response, Report), оно содержит текущее показание часов, так что неавторизованный получатель может синхронизовать свои часы. Когда неавторизованный сервер посылает сообщение (Get, GetNext, GetBulk, Set, Inform), он помещает туда текущую оценку показания часов места назначения, позволяя получателю оценить своевременность прихода сообщения.
2. Процесс локализации ключа, описанный ниже, устанавливает единственного принципала, который может владеть ключом. Ключи могут храниться только в авторизованном сервере, исключая хранение нескольких копий ключа в разных местах.

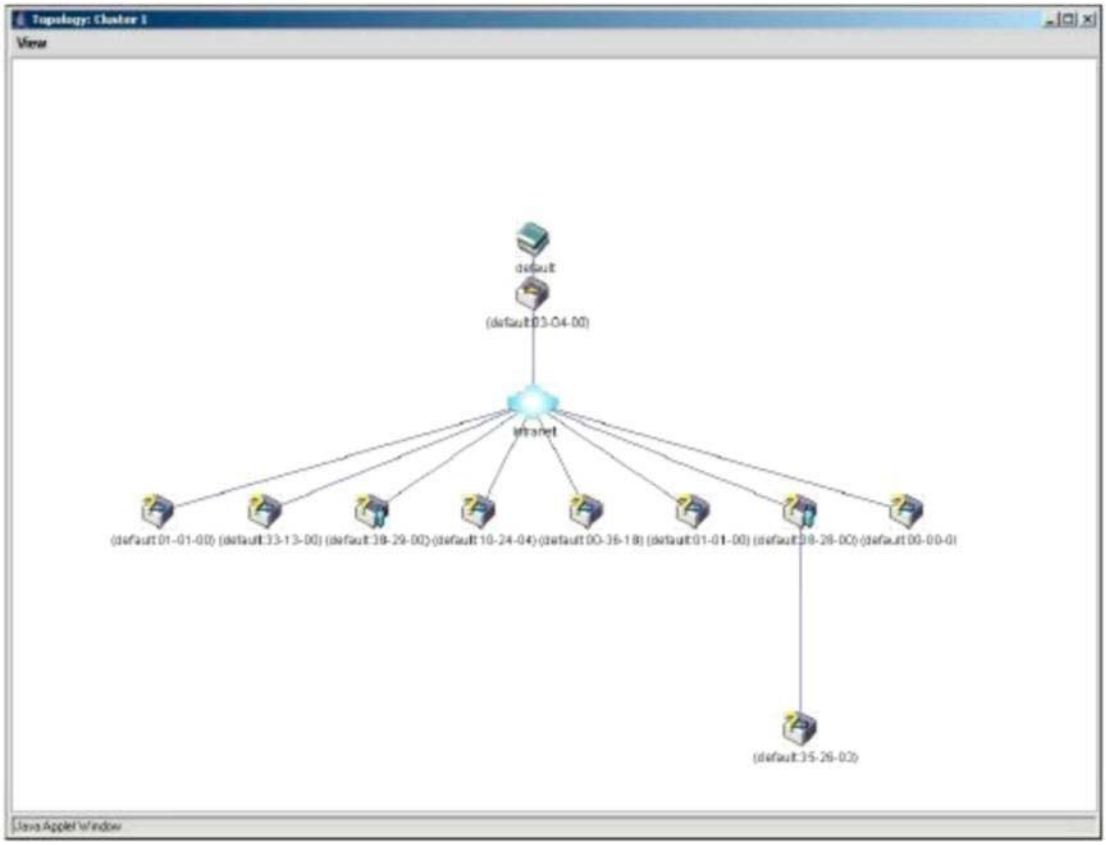
Когда исходящее сообщение передается процессором сообщений в USM, USM заполняет поля параметров безопасности в заголовке сообщения. Когда входное сообщение передается обработчиком сообщений в USM, обрабатываются значения параметров безопасности, содержащихся в заголовке сообщения. В параметрах безопасности содержатся следующие поля:

- **msgAuthoritativeEngeneID.** Идентификатор авторизованного сервера, участвующего в обмене. Это значение идентификатора отправителя для Trap, Response или Report или адресата для Get, GetNext, GetBulk, Set или Inform.
- **msgAuthoritativeEngeneBoots.** snmpEngeneBoots авторизованного сервера, участвующего в обмене. Объект snmpEngeneBoots содержит целочисленные значения в диапазоне 0 - (2^{31}-1). Это поле содержит число, показывающее сколько раз SNMP-сервер был перезагружен с момента конфигурирования.
- **msgAuthoritativeEngeneTime.** Время работы авторизованного сервера, участвующего в обмене. Значение этого поля лежит в диапазоне 0 - (2^{31}-1). Это поле характеризует число секунд, которое прошло с момента последней перезагрузки сервера. Каждый авторизованный сервер должен инкрементировать это поле один раз в секунду.
- **msgUserName.** Имя пользователя, который послал сообщение.
- **msgAuthenticationParameters.** Поле содержит ноль, если при обмене не используется аутентификация. В противном случае данное поле содержит аутентификационный параметр.
- **msgPrivacyParameters.** Поле содержит ноль, если не требуется соблюдения конфиденциальности. В противном случае данное поле содержит параметр безопасности. В действующей модели USM используется алгоритм шифрования DES.

Механизм аутентификации в SNMPv3 предполагает, что полученное сообщение действительно послано пользователем, имя которого содержится в заголовке сообщения, и это имя не было модифицировано во время доставки сообщения. Для реализации аутентификации каждый из пользователей, участвующих в обмене должен иметь секретный ключ аутентификации, общий для всех участников (определяется на фазе конфигурации системы). В посылаемое сообщение отправитель должен включить код, который является функцией содержимого сообщения и секретного ключа. Одним из принципов USM является проверка своевременности сообщения, что делает маловероятной атаку с использованием копий сообщения.

Модель управления доступом

Система конфигурирования агентов позволяет обеспечить разные уровни доступа к базе MIB для различных SNMP-менеджеров. Это делается путем ограничения доступа некоторым агентам к определенным частям MI B, а также с помощью ограничения перечня допустимых операций для заданной части MI B. Такая схема управления доступом называется VACM (View-Based Access Control Model). В процессе управления доступом анализируется контекст (vacmContextTable), а также специализированные таблицы vacmSecurityToGroupTable, vacmTreeFamilyTable и vacmAccessTable.



Данное окно покажет, каким образом устройства из группы SIM подключены к

Значок	Описание
	Группа
	Управляющий коммутатор второго уровня
	Управляющий коммутатор третьего уровня
	Управляющий коммутатор CS другой группы
	Коммутатор MS второго уровня
	Коммутатор MS третьего уровня
	Коммутатор MS, который является членом другой группы
	Коммутатор CaS второго уровня
	Коммутатор CaS третьего уровня
	Неизвестное устройство
	Устройство, не поддерживающее SIM-технологию.

другим группам и устройствам. В этом окне могут встретиться следующие значки:

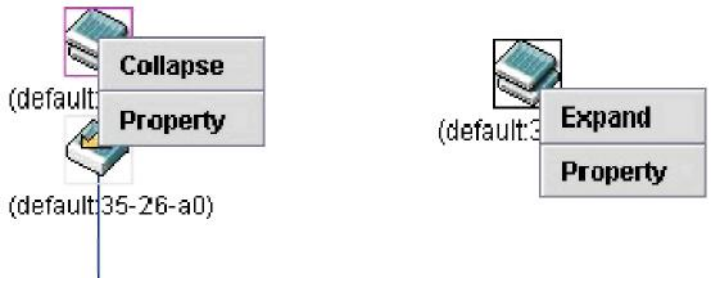
Получение информации о сети

В окне «Topology View» мышка играет важную роль в настройке и просмотре информации об устройстве. Подведите курсор мышки к интересующему вас устройству, изображенному на топологии, после чего появится информация о данном устройстве.

Установите курсор мышки над линией, соединяющей два устройства, и появится сообщение о скорости соединения между ними.

Нажатие правой кнопки мышки на устройстве позволит пользователю работать с различными функциями, зависящими от роли коммутатора в SIM-группе. Следующие опции могут быть доступны пользователю при нажатии правой кнопкой мыши:

- Collapse - свернуть группу чтобы она была представлена одним значком.
- Expand - развернуть SIM-группу для детального рассмотрения.
- Property - показать на экране информацию о группе.



Линейка меню

В окне «Single IP Management» для настройки устройств есть линейка меню. Меню File содержит следующие пункты:

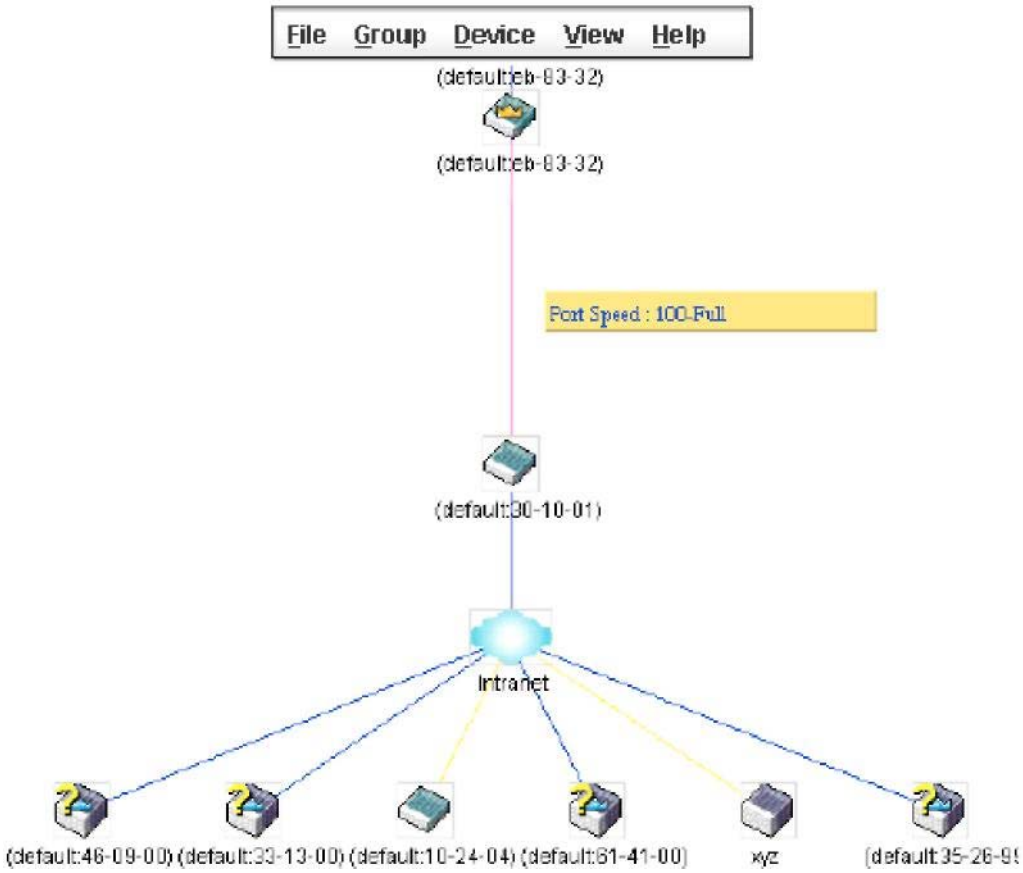
- Print Setup - просмотреть изображение перед печатью;
- Print Topology - напечатать топологию;
- Preference - показать такие свойства, как интервал между опросами и варианты просмотра топологий во время запуска SIM.

Меню Group содержит следующие пункты:

- Add to group - добавить к группе коммутатор CaS. При нажатии на «Add to group» появится диалоговое окно, в котором пользователя попросят ввести пароль для аутентификации CaS для его присоединения к SIM-группе.
- Remove from Group - удалить коммутатор MS из SIM-группы.

Меню Device содержит следующие пункт Configure, предназначенный для открытия Web-менеджера для настройки устройства. Меню View содержит следующие пункты:

- Refresh - обновить окна просмотра;
- Topology - показать топологию (окно «Topology View»).



4.10 Утилиты управления сетью по протоколу SNMP

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»

Утилита mbrowse

Данная утилита входит в стандартный пакет программного обеспечения операционной системы Arch Linux и используется для просмотра и изменения параметров удалѐнной системы по протоколу SNMP. Для еѐ 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 определѐнного 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.

5. Задания

5.1. Управление сетью с помощью технологии Single IP Management.

Порядок выполнения работы:

1. Изучите раздел «Способы управления коммутаторами. Технология Single IP Management». Найдите все описанные элементы комплекта.
2. Изучите раздел «Single IP Managment» коммутатора DES-3200-10.
3. Соберите топологию сети, представленную на рисунке 5.1.

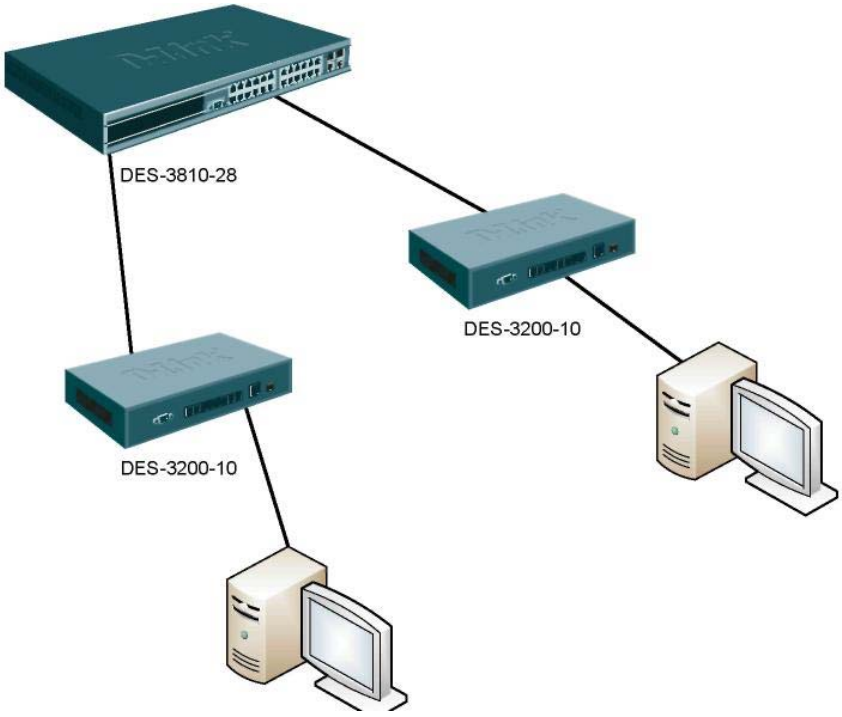


Рисунок 5.1. Топология коммутируемой сети.

4. Настройте коммутатор DES-3810-28 как командный коммутатор виртуального стека, а коммутаторы DES-3200-10 как коммутаторы-кандидаты.
5. Используя веб-интерфейс управления DES-3810-28, изучите карту сети, построенную коммутатором и ответьте на следующие вопросы:

    1. *Почему на топологии сети не отображаются компьютеры?*
    2. *Какова пропускная способность всех линий связи?*
    3. *MAC-адрес коммутатора DES-3810-28?*

6. Из интерфейса управления коммутатора DES-3810-28 установите любому коммутатору DES-3200-10 новый IP-адрес.
7. Проверьте доступность коммутатора DES-3200-10 по новому IP-адресу.
8. Сбросьте настройки коммутаторов в фабричные и перезагрузите их.

5.2. Управление сетью с помощью протокола SNMP.

Порядок выполнения работы: 1.

1. Постройте топологию сети, показанную на рисунке 5.2.

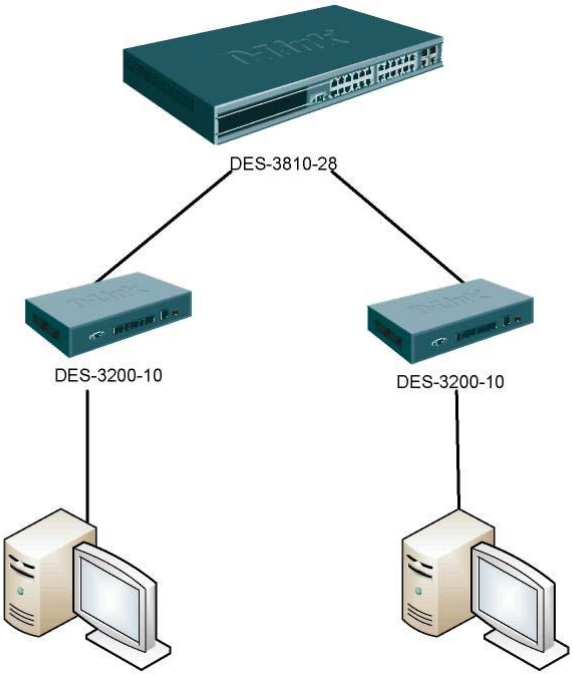


Рисунок 5.2. Топология коммутируемой сети.

2. Изучите раздел «Протокол SNMP».
3. Настройте SNMP-протокол на коммутаторах.
4. Изучите раздел «Утилиты управления сетью по протоколу SNMP» .
5. Запустите утилиту iReasoning MIB Browser.
6. Загрузите базу MIB RFC-1213.
7. На обоих коммутаторах (DES-3200-10 и DES-3810-28) выясните следующие параметры:

• название устройства, время работы устройства, службы, запущенные на устройстве (ветвь system);

• количество интерфейсов на устройстве, содержимое таблицы интерфейсов, назначение двух дополнительных виртуальных портов (ветвь interfaces);

• IP-адрес устройства, содержимое таблицы маршрутизации (ветвь ip);

• TCP-соединения, установленные устройством (ветвь tcp).

8. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

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