МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«Юго-Западный государственный университет»

(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2017 г.

УПРАВЛЕНИЕ КОММУТАТОРОМ D-LINK

Методические указания по выполнению лабораторной и практической работы по дисциплинам «Сети и системы передачи информации», «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Курск 2017

УДК 004
Составители: И.В. Калуцкий, А.Г. Спеваков, Е.В. Шеин, К.О. Хохлач.

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» *М.О. Таныгин*

Управление коммутатором D-Link: методические указания к выполнению лабораторных и практических работ по дисциплинам / Юго-Зап. гос. Ун-т; сост. И.В. Калуцкий, А.Г. Спеваков, Е.В. Шеин, К.О. Хохлач. Курск, 2017, 22 с.: ил. 10.; Библиогр.: с. 22.

Содержат сведения по вопросам настройки и управления коммутатором D-Link. Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл. печ. л. 1,28. Уч. –изд.л. 1,16. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Коммутаторы DES-3200 входят в линейку управляемых коммутаторов D-Link уровня 2 серии xStack, предназначенную для сетей Metro Ethernet (ETTX и FTTX). Коммутаторы оснащены 8/16/24 портами 100Мбит/с Fast Ethernet, а также 2/4 комбо-портами Gigabit Ethernet/SFP. Коммутатор DES-3200-10/18 выполнен в корпусе шириной 9 дюймов для настольной установки и оснащен пассивной системой охлаждения, применимой при развертывании сетей ETTH. Коммутаторы DES-3200-28/28F обеспечивают подключение по меди или оптике на скорости Fast Ethernet, что является преимуществом для различных приложений Metro Ethernet. Устройство обладает практичным дизайном с поддержкой 4 комбо-портов Gigabit/SFP, которые обеспечивают полосу пропускания 4Гбит/с с поддержкой топологии двойного кольца сети Ethernet. Коммутатор DES-3200-28F обеспечивает подключение на расстоянии до 20 км для приложений сети Metro Ethernet.

ЦЕЛЬ РАБОТЫ

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

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Выполненное задание
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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 .

Рисунок 1 – Окно аутентификация пользователя

После аутентификации будет осуществлен переход на страницу управления .

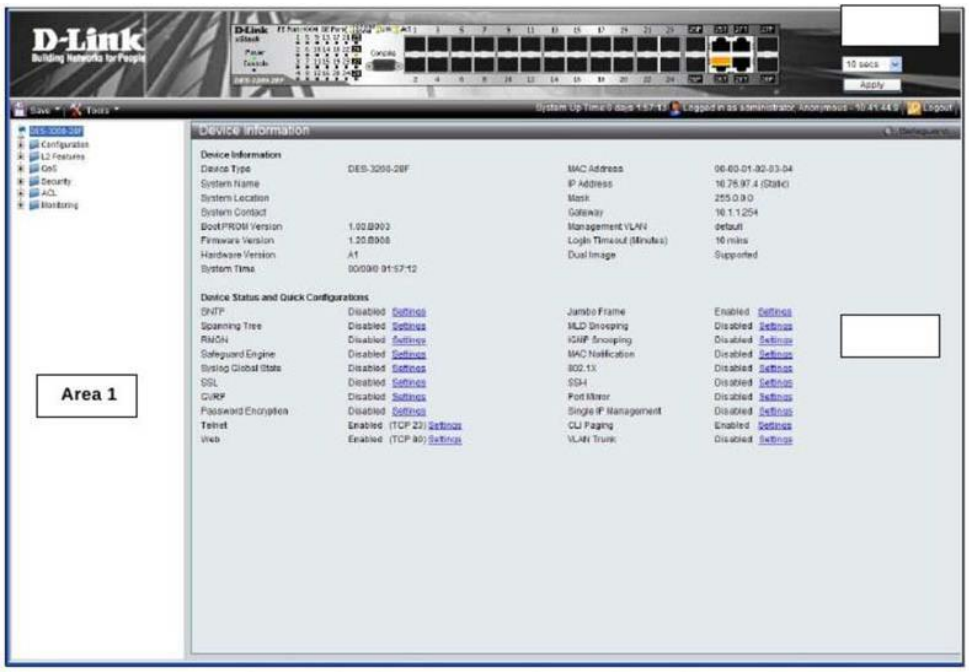

Рисунок 2 – Страница управления

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)
    - 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.

Рисунок 3 – Информация об устройстве

Полное описание всех пунктов данного окна приведено в таблице 1.

Таблица 1 - Описание всех пунктов окна Device Information

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

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.

Разделы меню управления

Раздел Port Configuration

Port Configuration состоит из нескольких разделов:

Раздел Port Settings

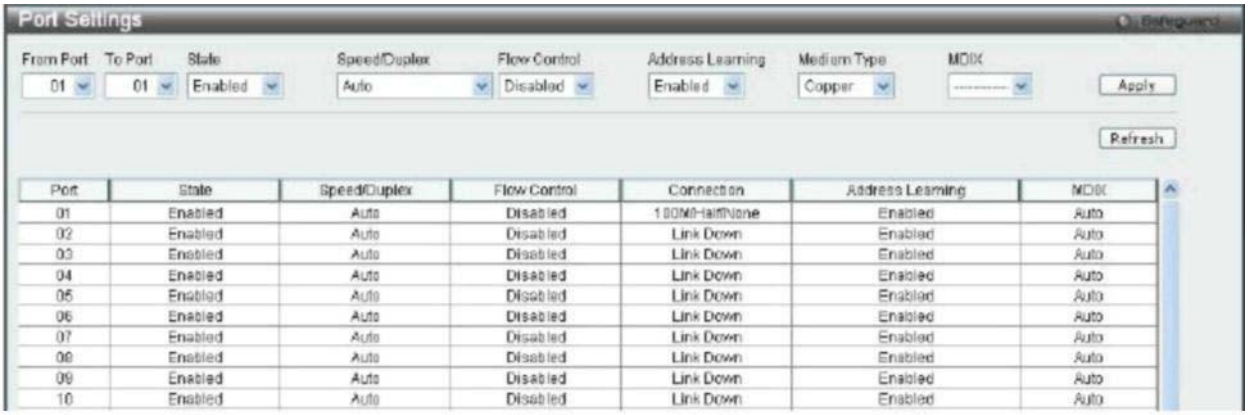

Рисунок 4 - Раздел Port Settings

Позволяет управлять настройками портов

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

Раздел Port Descriptions

Позволяет задать описания портов

Рисунок 5 - Раздел Port Descriptions

- From Port - начальный номер порта
- To Port - конечный номер порта. К выбранному диапазону портов

будут применены дальнейшие настройки

- Medium Type - тип среды (применяется для комбо-портов)
- Description - описание

Раздел Port Error Disabled

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

Рис. 6 - Раздел Port Error Disabled

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

Раздел Port Mirror

Позволяет управлять функцией зеркалирования портов

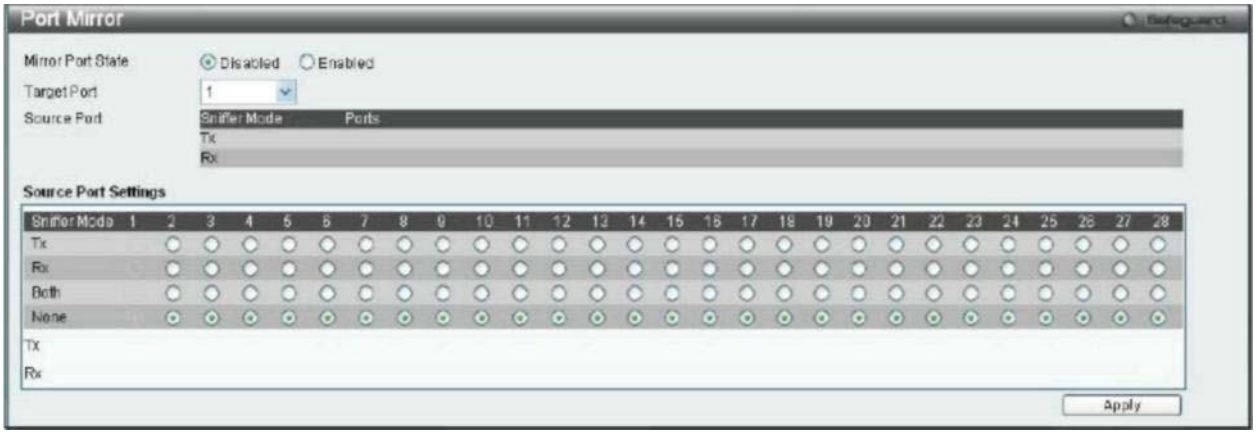

Рисунок 7 - Раздел Port Mirror

- Mirror Port State - активность функции
- Target Port - выходной порт

- Source Port - прослушиваемые порты
- Sniffer Mode - настройка прослушиваемых портов и направления трафика
  - Tx - только исходящий трафик
  - Rx - только входящий трафик
  - Both - оба направления
  - None - не прослушивать

Раздел Forwarding & Filtering

Forwarding & Filtering состоит из нескольких разделов:

Раздел Unicast Forwarding Settings

Рисунок 8 – Раздел Unicast Forwarding Settings

Позволяет управлять статическими записями таблицы коммутации

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

Раздел PingTest

Позволяет выполнить проверку доступности узла

Рисунок 9 - Раздел PingTest

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

Утилиты мониторинга сети

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

ping

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

Синтаксис командной строки:

ping IP-address или DNS-имя удаленного хоста

Пример:
ping 193.233.81.1

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

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

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

tcpdump

Одним из мощных средств анализа всей сетевой активности является утилита tcpdump. Она переводит сетевой интерфейс в режим приема всех пакетов (promiscuous) и выводит информацию на экран. В Linux такое переключение возможно только для суперпользователя, то есть для полноценного использования tcpdump необходимо зарегистрироваться под пользователем root. На других системах требования немного другие и они представлены в документации к tcpdump.

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

Наиболее используемые опции tcpdump:

-c <число пакетов>

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

-i <интерфейс>

На каком интерфейсе осуществлять съѐм информации. Например, *«tcpdump -i eth1»* осуществляет съѐм 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 съѐма информации в неурочное время или при больших объѐмах 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 подключится 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

ЗАДАНИЕ

Конфигурирование портов и работа с таблицей коммутации.

1. Изучите раздел «Port Configuration» коммутатора DES-3200-28.
2. Постройте топологию сети, показанную на рисунке 10.

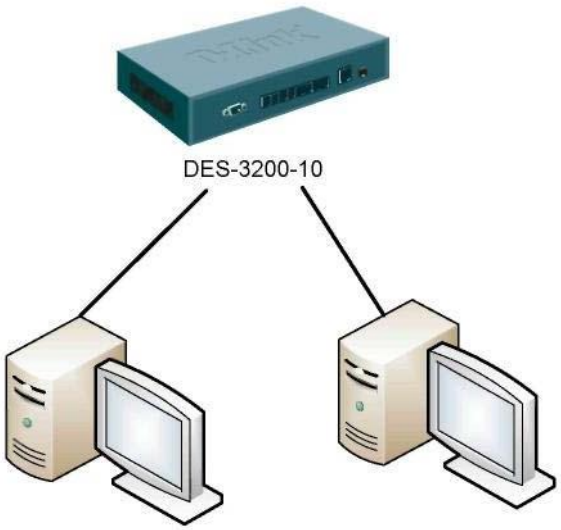

Рисунок 10 - Топология коммутируемой сети.

3. Выключите один из портов коммутатора, к которому подключен один из компьютеров.
4. Попробуйте осуществить взаимодействие компьютеров. Сделайте выводы на основе полученного результата.
5. Изучите раздел «Port Mirroring» коммутатора DES-3200-10.
6. Настройте на коммутаторе зеркало для любого из портов, к которому подключен один из компьютеров.
7. Запустите на машинах, подключенных к порту-источнику и порту-приемнику (зеркалу), утилиту tcpdump. Активизируйте сетевую активность. Сравните результаты работы утилит на обеих машинах. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назовите протоколы передачи файлов?
2. Назовите основные этапы закачки файлов на файловый сервер?
3. Каково назначение FTP-сервера?
4. Каким образом производится настройка vsftpd?
5. Каково назначение сетевого протокола SSH?
6. Какие основные параметры рекомендуется менять при настройки SSH с точки зрения его безопасности и почему?

СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

1. Сергеев А.Н. Основы локальных компьютерных сетей [Текст]/ А.Н. Сергеев, Изд.: «Лань», 2016. 184 с.

2. Безопасность сетей. [Электронный ресурс]: / Internet. - http://www.intuit.ru/department/security/netsec/10/netsec_10.html (22.10.17).

3. Администрирование управляемых коммутаторов. [Электронный ресурс]: / Internet. - http://sgu.ru/sites/default/files/method_info/2016/administrirovanie_upravlyaemyh_kommutatorov_ch3_0.pdf (22.10.17).