СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

Институт инженерной физики и радиоэлектроники

Кафедра инфокоммуникаций

Методические указания
по проведению лабораторных работ

«РЕАЛИЗАЦИЯ ПОЛОЖЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ D-LINK»

Подготовили:

А.В.Кулаев, К.В.Тарбазанов
Д.Ю.Черников

КРАСНОЯРСК

2025

Содержание

1 Настройка сетевых интерфейсов на устройствах D-Link

Зайдите в настройки сетевого устройства, например, при помощи Web-браузера, обратившись к нему по его IP-адресу (рис 1.1):

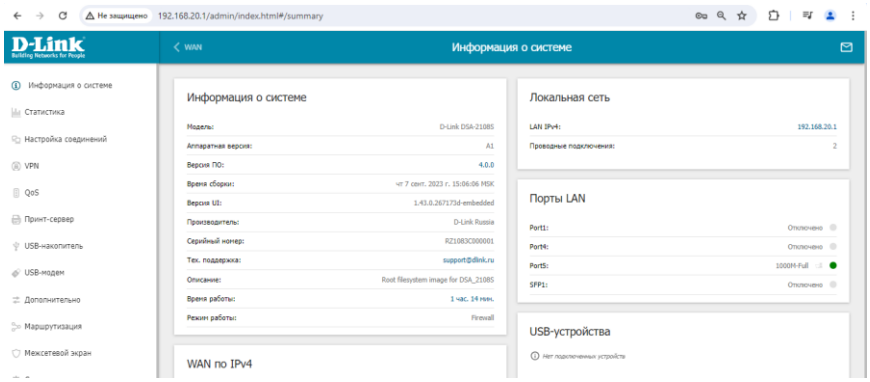

Рис 1.1

В меню **Настройка соединений** выберите подменю **WAN (расширенный режим)** (рис 1.2):

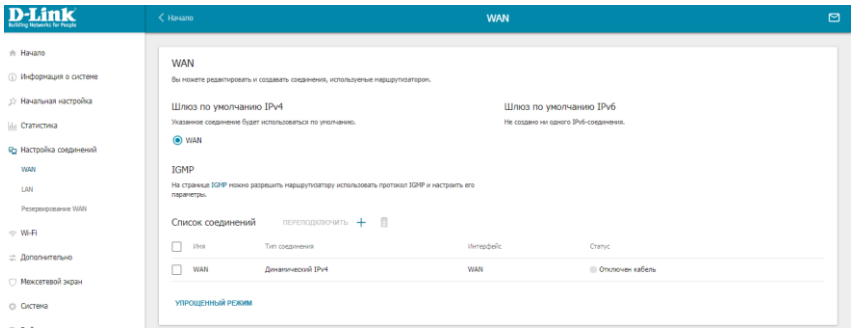

Рис 1.2

. Для добавления соединения WAN нажмите кнопку «+». В открывшимся окне выберите **Тип соединения** (рис 1.3):

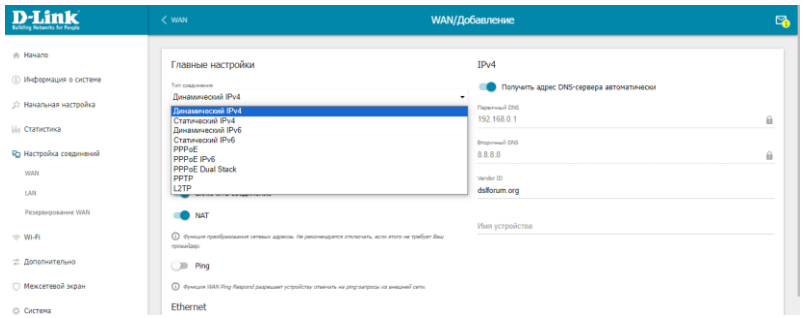

Рис 1.3

и в зависимости от типа соединения произведите необходимые настройки. Сохраните изменения.

4. В меню **Дополнительно**, подменю **Назначение WAN,** определите интерфейс, который будет выполнять роль WAN-интерфейса (рис 1.4):

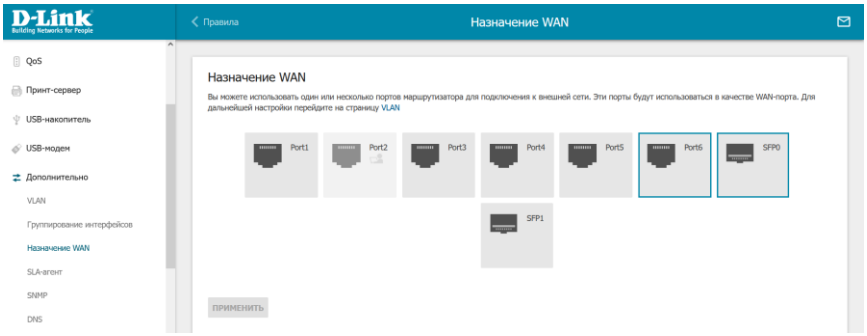

Рис 1.4

В меню **Настройка соединений** выберите подменю **LAN** (рис 1.5):

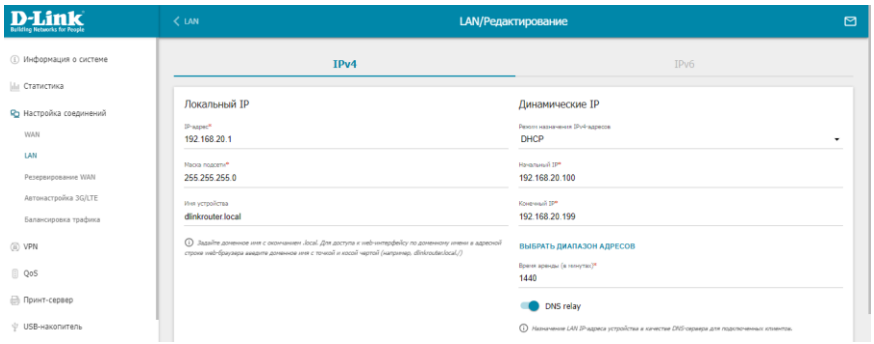

Рис 1.5

Произведите настройки IP-адреса и, при необходимости, службы DHCP. Сохраните изменения.
При подключении к сети, в меню **Статистика**, подменю **Сетевая статистика**, можно посмотреть статистику сетевых подключений (рис 1.6):

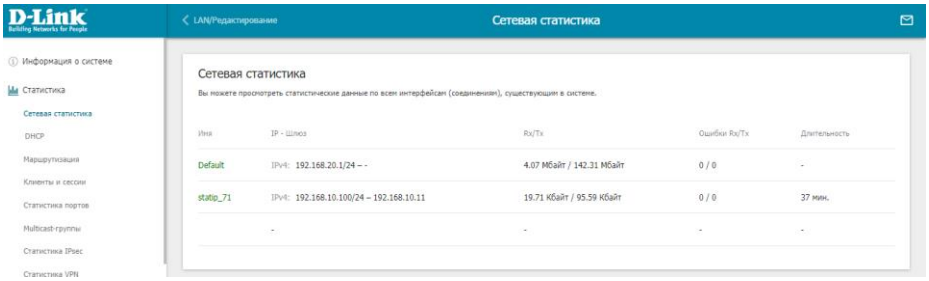

Рис 1.6

2 Принципы работы в режиме CLI с коммутаторами D-Link

Режимы команд

У коммутаторов D-Link есть несколько режимов команд в CLI (command-line interface). Наборы доступных для пользователя команд зависят как от того режима, в котором в данный момент находится пользователь, так и от его уровня привилегий

CLI имеет пять уровней привилегий и три режима выполнения команд:

Basic User – уровень привилегий 1 (Privilege Level 1). Это самый низкий уровень привилегий для аккаунта пользователя. Пользователь с таким уровнем привилегий сможет только осуществлять базовую проверку системы.

Advanced User – уровень привилегий 3 (Privilege Level 3). Пользователю с таким уровнем доступа разрешено конфигурировать настройки терминала. Этот пользователь может просматривать ограниченную информацию, не связанную с безопасностью.

Power User – уровень привилегий 8 (Privilege Level 8). Такой пользователь может выполнять меньшее количество команд, чем пользователь с уровнем привилегий Operator и Administrator

Operator – уровень привилегий 12 (Privilege Level 12). Такой уровень привилегий даётся пользователям, которым нужно изменять или просматривать конфигурацию системы, за исключением настроек, связанных с безопасностью, таких как аккаунты пользователей , SNMP и т.д.

Administrator – уровень привилегий 15 (Privilege Level 15). Это уровень привилегий администратора, который может просматривать и изменять любые настройки.

Режимы выполнения команд:

User EXEC Mode (пользовательский режим);

Privileged EXEC Mode (привилегированный режим);

Global Gonfiguration Mode (режим глобального конфигурирования).

Для перехода в режим глобальной конфигурации используется команда `configure terminale`

Создание пользователя

Создаем пользователь с именем **admin** и паролем **admin**, и задаем доступный ему уровень привилегий – 15-й

```
Switch# enable
Switch# configure terminal
Switch (config)# username admin password admin
Switch (config)# username admin privilege 15
Switch (config)# line console
Switch (config-line)# login local
```

Установка пароля для доступа в привилегированный режим

```
Switch# enable
Switch# configure terminal
Switch(config)# enable password {Password}
Switch# disable
Switch# enable
Password:***************
Switch# show privilege
Current privilege level is 15
Switch#
```

Переход в режим конфигурирования интерфейса

Все настройки, относящиеся к конкретному порту (интерфейсу) выполняются в режиме конфигурирования интерфейса:

```
Switch# configure terminal
Switch (config)# interface ethernet 1/0/1
Switch (config-if)# speed 1000
Switch (config-if)#
```

Настройка IP-адреса коммутатора

По умолчанию на коммутаторе существует один VLAN с идентификатором ID=1. Адрес по умолчанию у этого VLAN – 10.90.90.90 с маской 255.0.0.0. Его можно изменить, а также настроить вторичные IP-адреса.

IP-адреса на интерфейсах других VLAN настраиваются аналогично:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)#     ip     address     10.108.1.27
255.255.255.0
Switch(config-if)#     ip     address     192.31.7.17
255.255.255.0 secondary
Switch(config-if)#     ip     address     192.31.8.17
255.255.255.0 secondary
```

Завершение сессии терминала

Для завершения активной сессии терминала используется команда `logout`.

Для завершения режима конфигурирования и возврата на верхний уровень используется команда `end`.

Для завершения режима конфигурирования и возврата на прошлый уровень используется команда `exit`.

Сохранение конфигурации

Все изменения, сделанные в настройках коммутатора, сохраняются только в текущей конфигурации (`running-config`) и будут утеряны при включении или перезагрузке коммутатора. Для того, чтобы эти изменения остались, текущую конфигурацию нужно сохранить в энергонезависимую память (NV-RAM) – в файл `startup-config`.

```
Switch# copy running-config startup-config
Destination filename startup-config? [y/n]: y
Saving all configurations to NV-RAM..... Done.
Switch#
```

3 Настройка правил межсетевого экрана на сетевых устройствах D-Link

1. В адресной строке Web-браузера введите адрес сетевого устройства.
2. Перейдите в меню **Межсетевой экран**, подменю **Правила**.
3. Для создания нового правила нажмите кнопку «+» (рис 3.1);

Рис 3.1

4. В открывшимся окне произведите следующие настройки (рис3.2) :

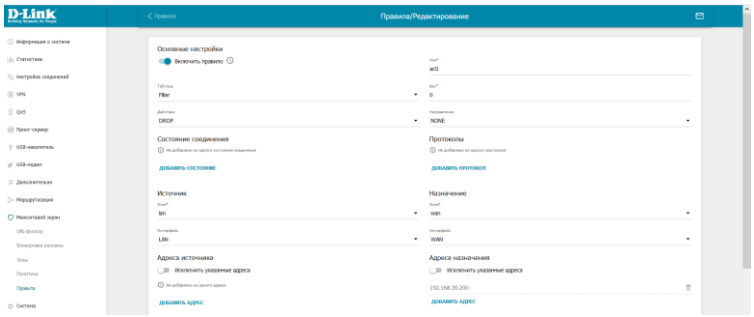

Рис 3.2

Имя – введите имя создаваемого правила;

Таблица – **Filter** (таблица, предназначенная для фильтрации пакетов по определенным параметрам), **NATFilter** (правило добавляется в таблицу **NAT**, при этом в таблицу **Filter** автоматически добавляется правило, обеспечивающее прохождение соответствующих пакетов), **NAT** (таблица, предназначенная для трансляции сетевых адресов), **Mangle** (таблица, содержащая правила для модификации заголовков пакетов.

Действия – **ACCEPT** (пакет принимается), **DROP** (пакет отбрасывается), **REJECT** (пакет отбрасывается с сообщением об ошибке отправителю), **RETURN** (пакет возвращается в вышестоящую цепочку или обрабатывается в соответствии с политикой по умолчанию), **REDIRECT** (пакет перенаправляется на другой порт), **MASQUERADE** (для исходящих пакетов адрес источника заменяется на адрес интерфейса, с которого отправляется пакет), **DNAT** (текущий и все последующие пакеты из того же потока подвергаются преобразованию адреса назначения), **SNAT** (текущий и все последующие пакеты из того же потока подвергаются преобразованию адреса источника), **POLICY** (действие, соответствующее политике в данной цепочке), **LOG** (запись информации о пакетах по данному правилу добавляется в системный журнал), **TTL** (изменяется значение поля TTL в заголовке пакета).

Источник Зона – выберите зону маршрутизатора для ограничения действий правила;

Назначение Зона – выберите зону маршрутизатора для ограничения действий правила;

Адреса источника – в открывшимся окне введите адрес или диапазон адресов;

Адреса назначения – в открывшимся окне введите адрес или диапазон адресов.

5. Сохраните изменения.

6. При правильной настройке сигнализатор **Статус** будет окрашен в зеленый цвет (рис 3.3):

Рис 3.3

4
Настройка VLAN на сетевых устройствах D-Link

Порядок настройки VLAN в терминальном режиме

1. Подключитесь к сетевому устройству в режиме CLI. Используйте для этого терминальные программы, например telnet, Putty.
2. Перейдите в режим глобальной конфигурации.
3. Создайте VLAN, например VLAN 10. Присвойте созданной VLAN имя. Для этого используйте команды:

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
```

4. Настройте порты 1/0/1-8 как порты доступа в VLAN 10. Используйте команды:

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
```

5. Настройте порт 1/0/24 как магистральный (trunk) для созданных VLAN 1, 10:

```
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,10
Switch(config-if)#end
```

6. Сохраните сделанные изменения командой:

```
copy running-config startup-config
```

Порядок настройки VLAN в режиме Web-интерфейса

1. Подключитесь к сетевому устройству через Web-браузер. Для этого в адресной строке введите его IP-адрес (по умолчанию 10.90.90.90).
2. Перейдите в раздел меню **Configuration**, подменю **802.1Q VLAN** (рис 4.1):

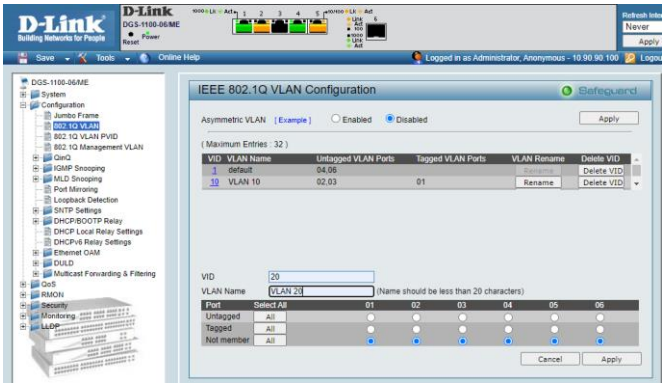

Рис 4.1

4. Заполните поля:
- **VID** – введите ID создаваемого VLAN;
- **VLAN Name** – введите имя создаваемого VLAN.
5. Определите порты, которые будут включены в создаваемую VLAN и их тип.
6. Определите **taggert-порт** (**trunk**).
7. Сохраните изменения, нажав кнопку **Apply**.
8. Проверьте сделанные настройки (рис 4.2)

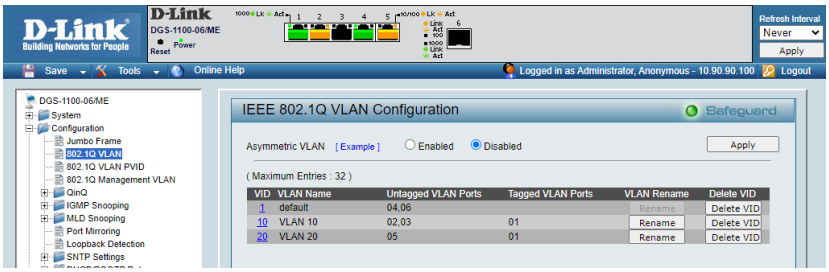

Рис 4.2

5 Настройка управляемого коммутатора D–Link DSG-1100

1. В браузере наберите IP-адрес устройства (адрес по умолчанию **http://10.90.90.90**).

2. В разделе **System**, подразделе **System Information Settings,** страница **IPv4 Interface** выберите режим, например, **Static** и установите требуемые значения **IP-адреса устройства**, **маски подсети** и **шлюза сети** (рис 5.1):

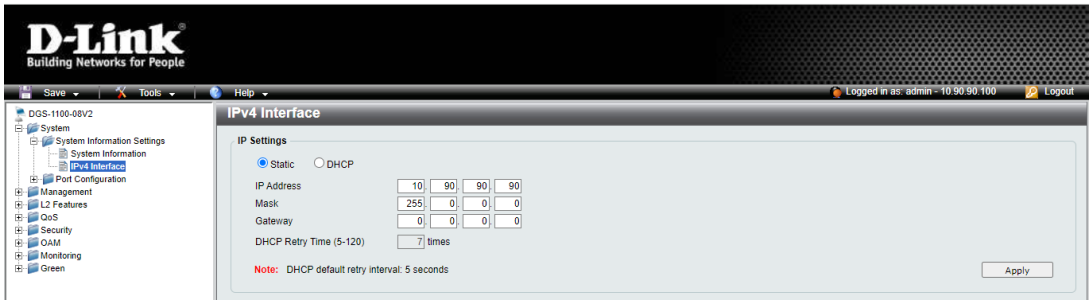

Рис 5.1

3. Сохраните изменения, нажав кнопку **Apply**.

4. Для настройки пропускной способности порта коммутатора войдите в раздел **QoS**, страница **Port Rate Limiting** (рис 5.2):

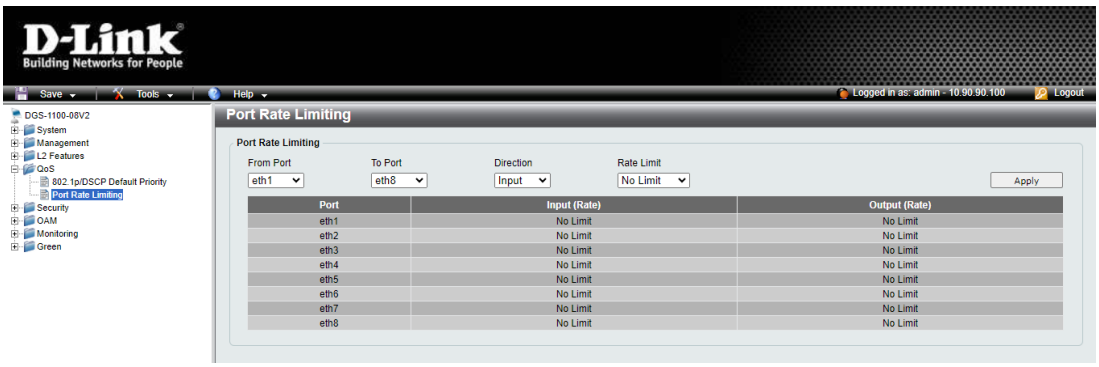

Рис 5.2

5. Выберите порт, пропускную способность которого необходимо изменить. Установите необходимую скорость порта **Rate** и вид передачи **Type**. Для применения настроек нажмите кнопку **Apply** (рис 5.3):

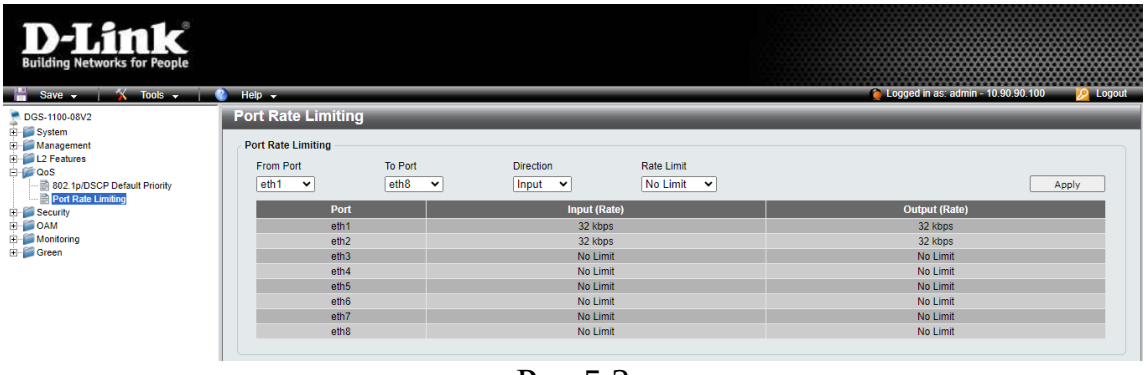

Рис 5.3

6. Для включения режима зеркалирования портов войдите в раздел **Monitoring**, страница **Mirroring Settings** (рис 5.4):

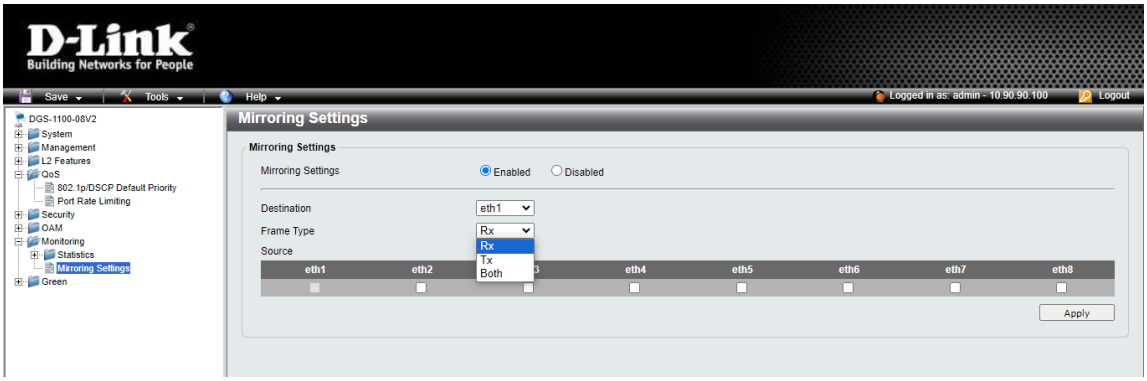

Рис 5.4

7. Включите функцию **Port Mirroring**, выберите порт-получатель траффика **Destination**, тип кадров **Frame Type** и порты-источника траффика **Source** для зеркалирования.

8. Для применения настроек нажмите кнопку **Apply.**

6 Настройка Wi-Fi маршрутизатора D-Link DIR-615

1. Загрузите Web-интерфейс маршрутизатора (адрес по умолчанию **http://192.168.0.1**). В окне авторизации введите логин и пароль.

2. Для настройки сетевого интерфейса WAN перейдите в раздел **Connection Setup** подраздел **WAN** (рис 6.1):

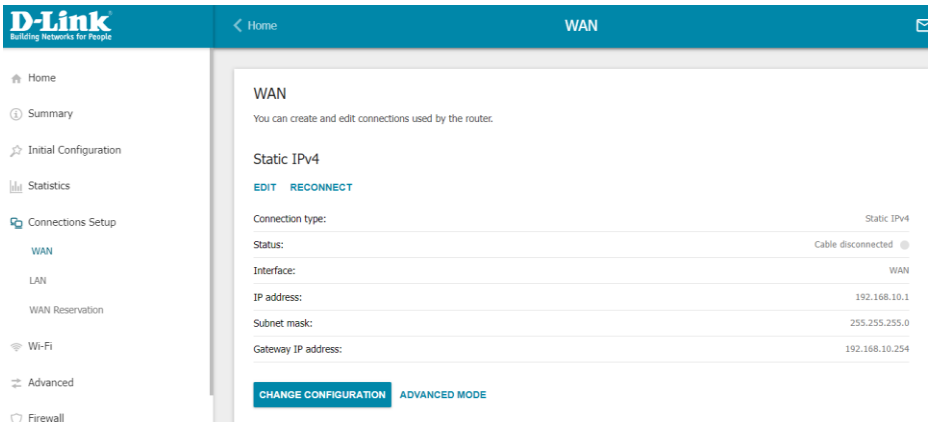

Рис 6.1

Выберите тип соединения и при необходимости заполните поля: **Ip-address**, **Subnet mask**, **Gateway IP address**. После ввода данных нажмите кнопку **Change Configuration**.

3. Для настройки сетевого интерфейса LAN перейдите в раздел **Connection Setup**, а затем в подраздел **LAN** (рис 6.2):

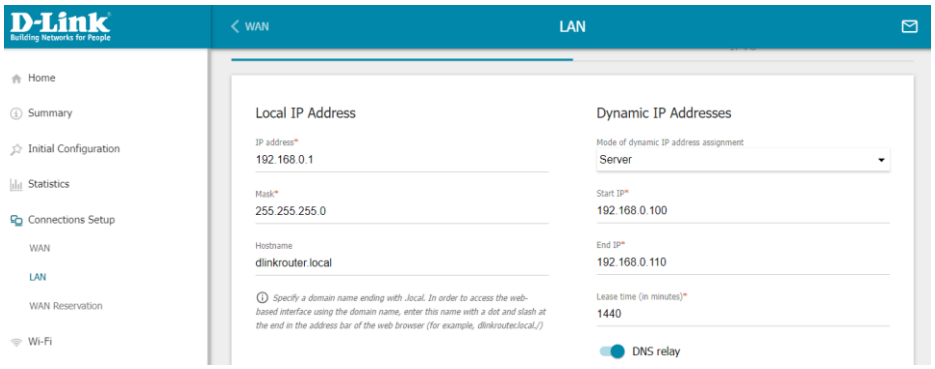

Рис 6.2

Заполните поля: **Ip-address**, **Subnet mask**, **hostname**. Сохраните изменения.

4. Настройка Wi-Fi сети производится в разделе **Wi-Fi**. Для ввода базовых настроек перейдите в подраздел **Basic Settings** (рис. 6.3) и введите имя Wi-Fi-сети, выберите **страну**, **режим работы беспроводной сети**:

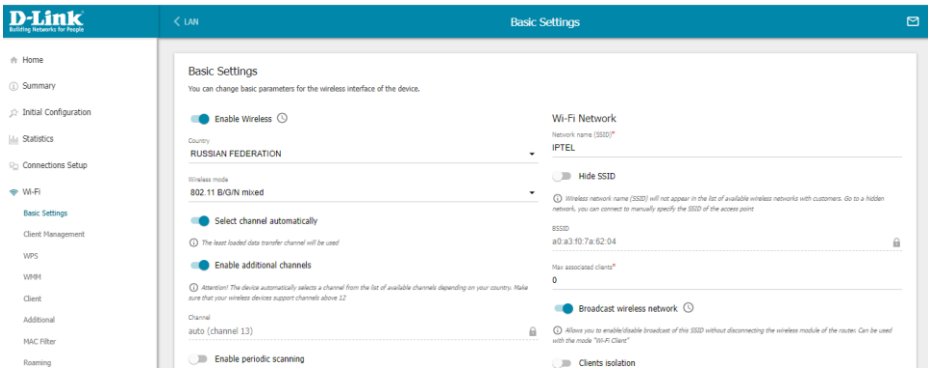

Рис 6.3

5. Настройки безопасности Wi-Fi сети осуществляются в подразделе **Basic Settings** в пункте **Security Settings**. Здесь выбирается **тип аутентификации** и вводится **пароль** Wi-Fi сети (рис 6.4):

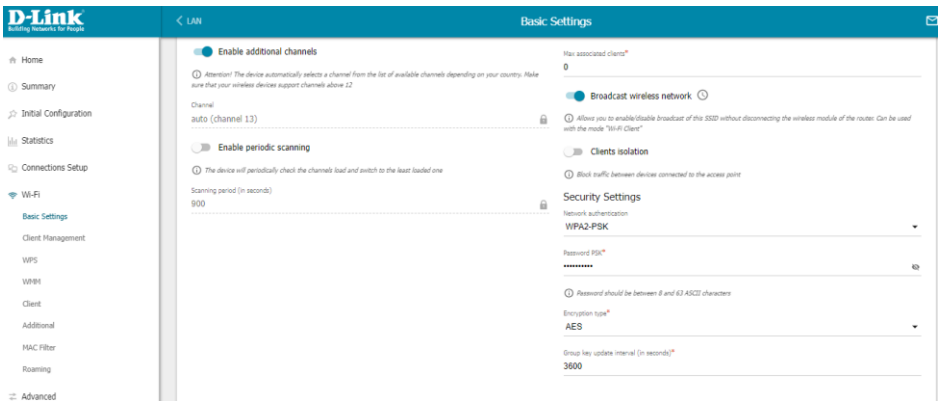

Рис 6.4

6. Для просмотра клиентов, подключенных к Wi-Fi сети маршрутизатора, перейдите в меню **Wi-Fi**, подменю **Управление клиентами** (рис 6.5):

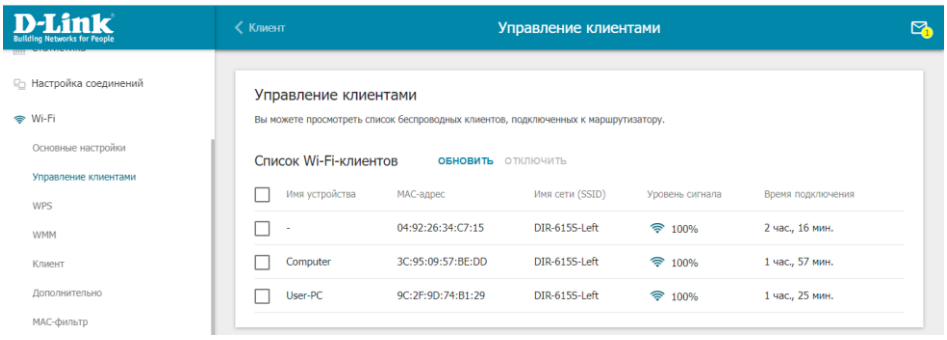

Рис 6.5

7. Ограничения на доступ клиентов к Wi-Fi сети маршрутизатора можно посмотреть в меню **Wi-Fi**, подменю **MAC-фильтр** (рис 7.6):

Рис 6.6

8. По окончании настройки устройства сохраните изменения.

7 Настройка PPTP-сервера на ОС Debian

1. Установите пакеты службы PPTP сервера. Используйте команду:

```
su --c 'apt install pptpd'
```

2.Откройте для редактирования файл `/etc/pptpd.conf`. В нем задайте количество одновременных подключений, для этого в параметре `connections` указываем нужное значение:

```
connections 200
```

При необходимости передачи по виртуальной сети широковещательных пакетов, раскоментируйте параметр `bcrelay` и укажите интерфейс передачи:

```
bcrelay eth1
```

Определите IP-адреса:

`localip {IP-адрес}` – IP-адрес сервера в локальной сети

`remoteip {диапазон IP-адресов}` – диапазон выдаваемых клиентам
IP-адресов

`listen {IP-адрес2}` – внешний IP-адрес для прослушивания интерфейсов для приёма входящих подключений. Если третий адрес не указать, прослушиваться будут все доступные внешние адреса.

3. Сохраните изменения в файле.
4. Откройте для редактирования файл `/etc/ppp/pptpd-options`. В нем определите используемый метод аутентификации, указав соответственную опцию. Например:

```
require-mschap-v2
```

Будет использоваться метод аутентификации `mschap-v2`.

Также раскомментируйте опцию `proxyarp` и для разрешения или запрета множественных подключений одного пользователя разрешите или запретите опцию `lock`.
5. Сохраните изменения в файле.
6. Создайте пользователей для подключения к серверу. Для этого внесите изменения в файл `/etc/ppp/chap-secrets`. В этом файле на каждого пользователя отводится одна строка, в которой последовательно (разделитель – пробел) указывается его имя, удалённый адрес, пароль и локальный адрес.
Например:

```
user1 * password1 *
```

```
user2 {IP-адрес3} password2 *
user3 * password3 {IP-адрес4}
```

Для пользователя `user1` подключения будут приниматься с любого внешнего адреса, локальный будет выделяться первый доступный. Для `user2` будет выделять первый доступный локальный адрес, но подключения будут приниматься только с адреса `{IP-адрес3}`. Для `user3` подключения принимаются из любой точки, но локальный адрес всегда будет выделяться `{IP-адрес4}`, который для него зарезервирован.

7. Сохраните изменения в файле.
8. Перезапустите службу pptpd командой:

```
sudo service pptpd restart
```

8 Настройка PPTP-клиента на устройстве D-Link

1. Через Web-браузер войдите на сетевое устройство D-Link.
В меню **Соединения,** в подменю **WAN,** в разделе **Список соединения** нажмите кнопку «+» для создания нового соединения. В открывшимся окне, в разделе **Тип соединения** выберите **PPTP** (рис 8.1):

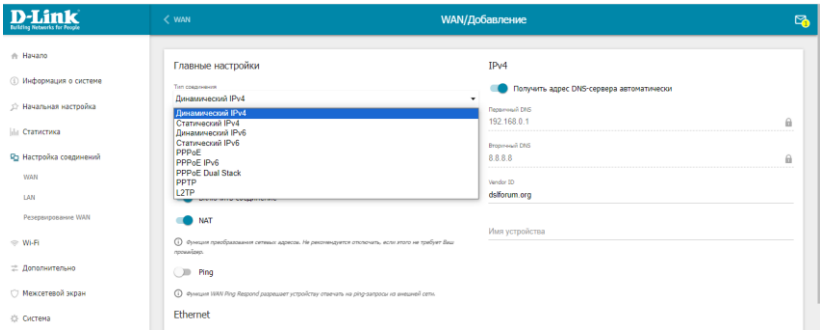

Рис 8.1

Настройте параметры PPTP-соединения. Заполните поле **Имя соединения**, данные авторизации (**Имя пользователя**, **Пароль**, **Адрес VPN-сервера**), установите **Протокол аутентификации** такой же, как и на PPTP-сервере и сохраните введенные данные (рис 8.2):

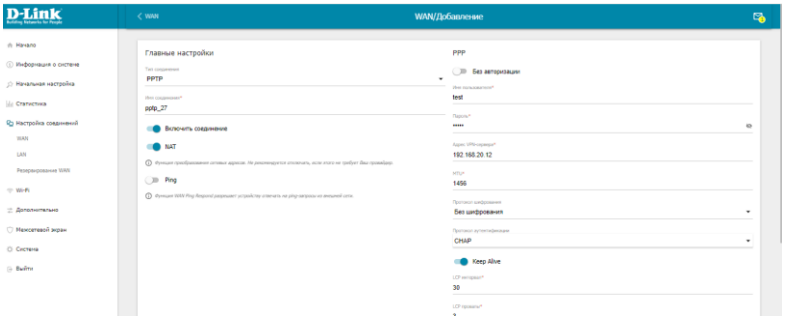

Рис 8.2

4. Определите соединения, которые необходимо будет использовать при PPTP-подключении (рис 8.3):

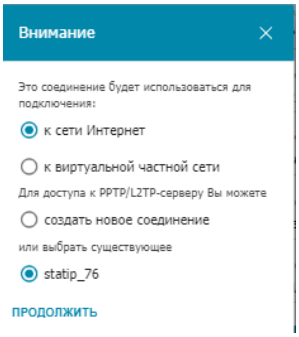

Рис 8.3

После создания PPTP-соединения проверьте правильность выбора **Шлюза по умолчанию** (должно быть выбрано динамическое или статическое IPv4-соединение) (рис 8.4):

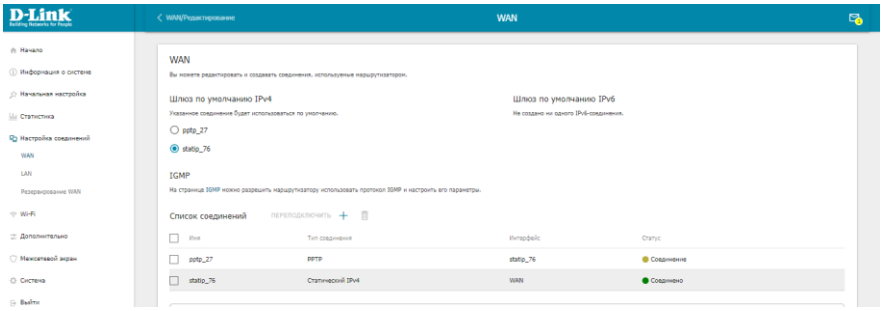
D-Link
WAN/Редактирование
WAN
Начало
Информация о системе
Начальная настройка
Статистика
Настройка соединений
WAN
LAN
Резервирование WAN
Wi-Fi
Дополнительно
Межсетевой экран
Система
Выйти
WAN
Вы можете редактировать и создавать соединения, используемые маршрутизатором.
Шлюз по умолчанию IPv4
Указанное соединение будет использоваться по умолчанию.
pptp_27
statip_76
Шлюз по умолчанию IPv6
Не создано ни одного IPv6-соединения.
IGMP
На странице IGMP можно разрешить маршрутизатору использовать протокол IGMP и настроить его параметры.
Список соединений
ПЕРЕПОДКЛЮЧИТЬ
Имя
Тип соединения
Интерфейс
Статус
pptp_27
PPTP
statip_76
Соединение
statip_76
Статический IPv4
WAN
Соединено

Рис 8.4

9 Установка системы Snort на ОС Linux

1. Установите среду `snort`. Для этого в терминальном режиме воспользуйтесь командами:

```
apt update
apt install snort
```

2. Проверьте установку пакетом командой:

```
snort --version
```

3. При правильной установке на экране будет выведено:

```
,,_ -*> Snort! <*
- o" )~ Version 2.9.2.2 IPv6 GRE (Build 121)
''''   By   Martin   Roesch   &   The   Snort   Team:
http://www.snort.org/snort/snort-team
Copyright (C) 1998-2012 Sourcefire, Inc., et al.
Using libpcap version 1.3.0
Using PCRE version: 8.30 2012-02-04
Using ZLIB version: 1.2.7
```

4. Проверьте, а при необходимости отредактируйте файл snort.conf. В файле конфигурации `snort.conf` проверьте, включены ли правила контроля протокола icmp. Если нет, добавьте их, включив строку:

```
include /etc/snort/rules/icmp.rules
```

5. Откройте файл правил icmp `icmp.rules` и включите правило, указанное ниже:

```
alert icmp any any -> any any (msg: "ICMP Packet";
sid: 477; rev: 3;)
```

Приведенное выше основное правило предупреждает о наличии ICMP-пакета (ping).

6. Запустите snort из командной строки, как указано ниже.

```
snort -c /etc/snort/snort.conf -l /var/log/snort/
```

здесь `-c` указывает на файл с правилами и `-l` на каталог журнала.

7. При наличии другого интерфейса для сетевого подключения, используйте опцию `-dev -i`. В этом примере сетевой интерфейс – eth0.

```
    snort -dev -i eth0 -c /etc/snort/snort.conf -l
/var/log/snort/
```

8. При необходимости добавьте опцию `-D` для запуска snort в качестве демона.

```
    snort -D -c /etc/snort/snort.conf -l /var/log/snort/
```

9. Для остановки пакета snort используйте команду:

```
    sudo systemctl stop snort
```

10. Для просмотра статуса пакета snort используйте команду:

```
    sudo systemctl status snort
```

10 Настройка сетевого интерфейса в ОС Linux Mint

1. Наведите указатель мыши на значок **«Сетевые соединения»** и кликнете по нему левой клавишей мыши.
2. Откроется окно с выбором сетевых подключений и их параметрами (рис 10.1). Выберите тип подключения, например **Wired** и нажмите кнопку **Настройка.**

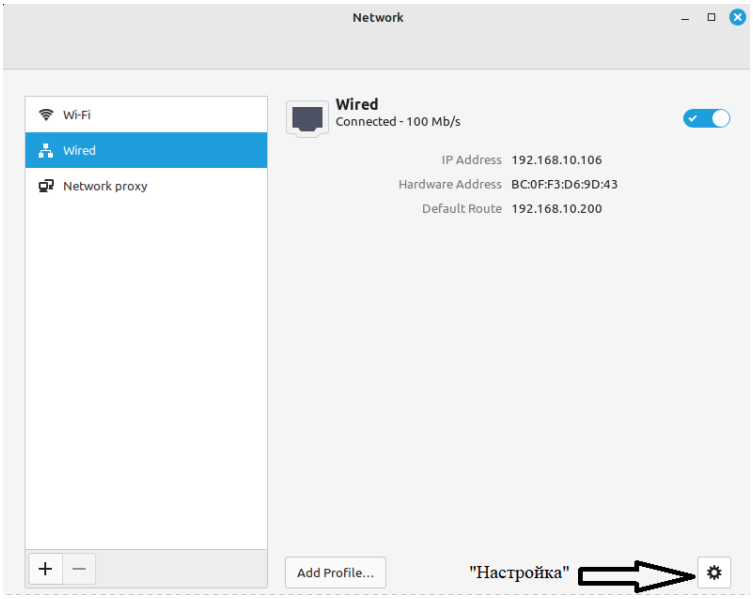

Рис 10.1

3. В открывшимся окне выберите протокол подключения, например **IPv4** (рис 10.2):

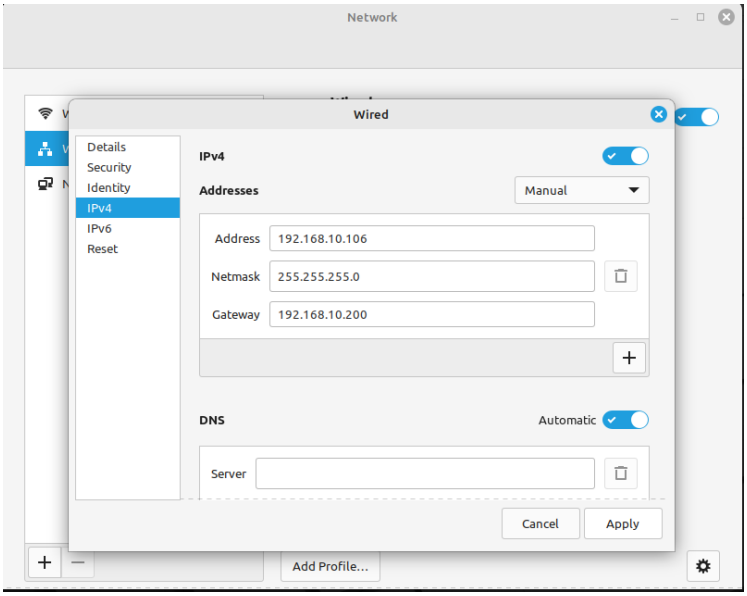

Рис 10.2

4. Отредактируйте свойства сетевого подключения. В конце редактирования нажмите кнопку **Apply**. Для применения настроек выключите и включите сетевой интерфейс (рис 10.3):

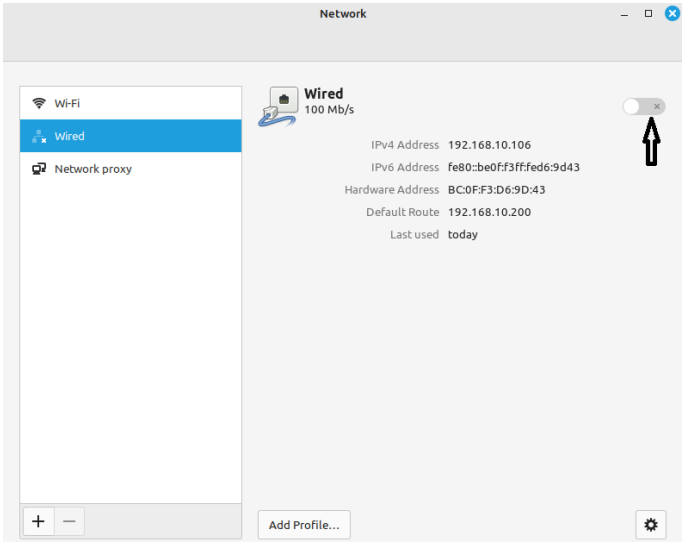
Network
Wi-Fi
Wired
Network proxy
Wired
100 Mb/s
IPv4 Address 192.168.10.106
IPv6 Address fe80::be0f:f3ff:fed6:9d43
Hardware Address BC:0F:F3:D6:9D:43
Default Route 192.168.10.200
Last used today
Add Profile...

Рис 10.3

11 Запуск службы SNMP на ОС Linux Debian

1. Установите SNMP демон, клиент и дополнительные библиотеки командой:

```
apt install snmpd snmp libsnmp-dev
```

2. Создайте резервную копию файла `/etc/snmp/snmpd.conf` командой:

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.orig
```

3. Внесите изменения в файл, изменив директиву `agentAdress`. Ее текущие настройки разрешают доступ только с локального компьютера. Для включения удаленного мониторинга необходимо определить IP-адрес интерфейса:

```
# AGENT BEHAVIOUR
#
# Listen for connections from the local system only
agentAddress udp:127.0.0.1:161,udp:<ip-адрес>:161
```

4. Для настройки аутентификации внесите изменения в раздел `directive community [source [OID]]`. Директива `rocommunity` предоставляет доступ только на чтение, а `rwcommunity` дает доступ к чтению/записи.
5. В раздел `Access Control section` поместите строку:

```
rocommunity S3CUrE <ip-адрес>
```

6. Для включения запроса с локального хоста добавьте директиву `rocommunity S3CUrE localhost`:

```
rouser authOnlyUser
wuser authPrivUser priv
rocommunity S3CUrE localhost
rocommunity S3CUrE <ip-адрес>
```

6. Для применения изменений нужно перезапустить SNMP:

```
systemctl restart snmpd
```

7. Чтобы добавить сервис в автозагрузку, введите:

```
systemctl enable snmpd
```