Пример настройки IP-MAC-Port Binding

Функция **IP-MAC-Port Binding** (**IMPB**), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP/MAC-адресов и порта подключения. Она позволяет бороться с атаками типа ARP Spoofing и атаками на протокол DHCP. Поэтому ее рекомендуется использовать на коммутаторах уровня доступа в сетях различного типа.

Работа функции основана на сравнении параметров входящих пакетов с параметрами хранящихся на коммутаторе записей, связывающих MAC- и IP-адреса клиентских устройств с портами подключения. В случае совпадения всех составляющих (IP/MAC-адресов и порта), пакеты будут передаваться, и клиенты получат доступ в сеть. Если при подключении клиента связка MAC-IP-порт будет отличаться от параметров заранее сконфигурированной записи, коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный лист».

Функция включает четыре режима работы: ARP Inspection (по умолчанию), IP Inspection, ND Snooping и DHCP/DHCPv6 Snooping.

При работе в режиме **ARP Inspection** коммутатор анализирует сообщения ARP и сопоставляет содержимое соответствующих полей с предустановленной администратором связкой IP-MAC.

В сообщениях ARP проверяется следующая информация:

- Заголовок Ethernet: поле Source Address.
- Полезная нагрузка ARP: поля Sender Hardware Address и Sender Protocol Address.

Если хотя бы один параметр не совпадает, то MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Drop» (Отбрасывать). Если все параметры совпадают, MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Allow» (Разрешен).

Порт коммутатора может быть настроен для работы в одном из двух режимов ARP Inspection:

- **Strict Mode** — в этом режиме порт по умолчанию заблокирован. Для того чтобы начать передавать данные, узел должен быть аутентифицирован.
- **Loose Mode** — в этом режиме порт по умолчанию открыт. Порт будет заблокирован, как только через него пройдет первое недостоверное сообщение ARP.

При работе в режиме **IP Inspection** коммутатор анализирует пакеты IPv4/v6 и сопоставляет содержимое соответствующих полей с предустановленной администратором связкой IP — MAC.

В IP-пакетах проверяется следующая информация:

- Заголовок Ethernet: поле Source Address.
- Заголовок IP: поле Source IP Address.

Коммутатор на основе предустановленной администратором таблицы IMPB («белый лист») создает аппаратную таблицу ACL. Любой IP-пакет, связка IP-MAC которого отсутствует в «белом листе», будет блокироваться ACL. Если режим IP Inspection отключен, правила для записей IMPB будут удалены из таблицы ACL.

Режимы ARP Inspection и IP Inspection могут работать совместно. Когда режим IP Inspection активирован и ARP Inspection отключен, все не IP-пакеты (сообщения протоколов канального уровня) будут передаваться по умолчанию.

Режим **DHCPv4/v6 Snooping** используется коммутатором для динамического создания записей IPv4/v6-MAC на основе анализа DHCP-пакетов и привязки их к портам с включенной функцией IMPB. Администратору не требуется создавать записи вручную. Таким образом, коммутатор автоматически создает «белый лист» IMPB в таблице коммутации и/или таблице ACL (если включен режим IP Inspection). Каждая создаваемая запись ассоциирована со временем аренды IP-адреса. Для обеспечения корректной работы, сервер DHCP или другой коммутатор должен быть подключен к доверенному порту с выключенной функцией IMPB. В случае подключения DHCP-сервера или коммутатора к порту, на котором включена функция IMPB, для него необходимо создать статическую связку IP-MAC-порт. В противном случае пакеты будут отбрасываться.

Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт, то есть ограничить для каждого порта с активированной функцией IMPB количество узлов, которые могут получить IP-адрес от DHCP-сервера. При работе в режиме DHCP Snooping коммутатор не будет создавать записи IP-MAC для узлов с IP-адресом, установленным вручную.

Режим **ND Snooping** используется коммутатором для динамического создания записей IPv6-MAC на основе анализа сообщений Neighbor Solicitation (NS) и привязки их к портам с включенной функцией IMPB. Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IPv6-MAC на порт.

Примечание к настройке

Рассматриваемые примеры настройки подходят для коммутаторов с D-Link-like CLI. Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключенных к коммутатору.

Задача № 1

Необходимо настроить защиту от атаки типа ARP Spoofing. Коммутатор должен обнаружить, что на порт 2 приходят ARP-ответы, связка IP-MAC для которых отсутствует в таблице IMPB, и заблокировать MAC-адрес узла. Задача может быть решена настройкой функции IP-MAC-Port Binding в режиме ARP Inspection.

Схема сети представлена на рисунке 1.

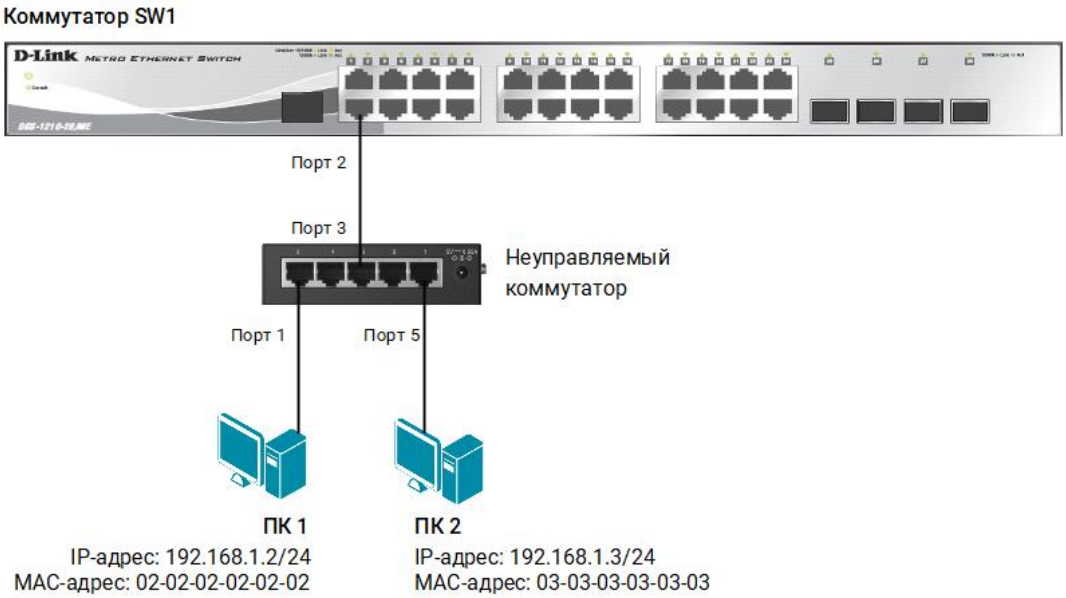

Рис. 1 Схема подключения

Настройка коммутатора SW1

1. Создайте записи IP-MAC-Port Binding, связывающие IP- и MAC-адреса узла с портами подключения:

```
create address_binding ip_mac ipaddress 192.168.1.2 mac_address 02-02-02-02-02-02 ports 2

create address_binding ip_mac ipaddress 192.168.1.3 mac_address 03-03-03-03-03-03 ports 2
```

2. Активируйте функцию на требуемых портах, укажите режим работы портов (в примере настроен режим Loose):

```
config address_binding ip_mac ports 2 state enable arp_inspection loose
```

Задача № 2

Необходимо запретить пользователям локальной сети изменять MAC- и/или IP-адреса своих компьютеров, а также менять порт подключения к сети. Компьютеры используют статические адреса. Задача может быть решена настройкой функции IMPB в режиме IP Inspection.

Схема сети представлена на рисунке 2.

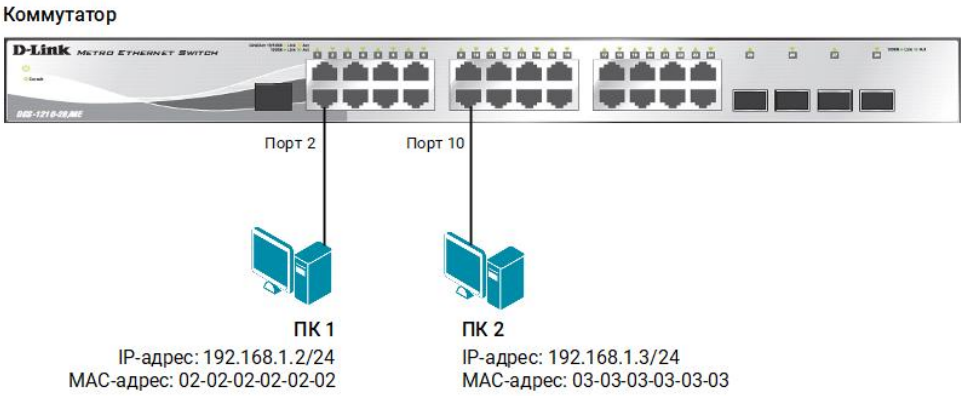

Рис. 2 Схема подключения

Настройка коммутатора

1. Создайте записи IP-MAC-Port Binding, связывающие IP- и MAC-адреса узла с портами подключения:

```
create address_binding ip_mac ipaddress 192.168.1.2 mac_address 02-02-02-02-02-02 ports 2
create address_binding ip_mac ipaddress 192.168.1.3 mac_address 03-03-03-03-03-03 ports 10
```

2. Активируйте функцию на требуемых портах:

```
config address_binding ip_mac ports 2,10 state enable ip_inspection enable
```

> **Примечание**
>
> Посмотреть созданную таблицу IMPB можно с помощью команды:
>
> ```
> show address_binding ip_mac
> ```
>
> Посмотреть настройки функции на портах можно с помощью команды:
>
> ```
> show address_binding ports
> ```

Задача № 3

Необходимо настроить коммутатор, чтобы он динамически создавал запись IMPB после того как клиент получит IP-адрес от DHCP-сервера. Задача может быть решена настройкой функции IP-MAC-Port Binding в режиме DHCPv4 Snooping.

Схема сети представлена на рисунке 3.

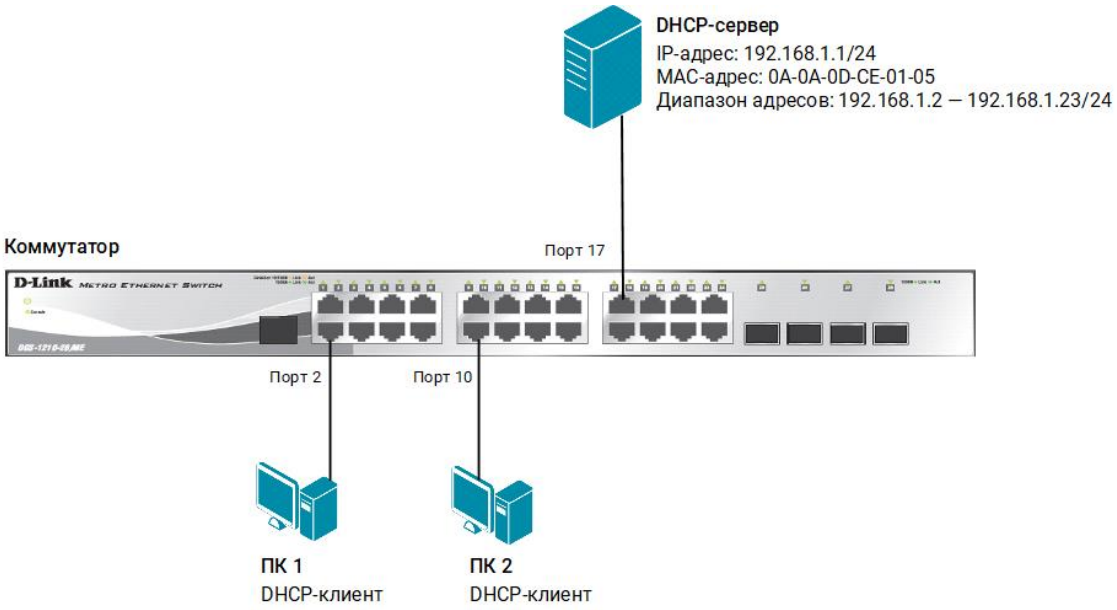

Рис. 3 Схема подключения

> **Примечание**
>
> Чтобы проводилась проверка входящих пакетов, режим DHCP Snooping должен использоваться совместно с режимами ARP Inspection или IP Inspection.

Настройка DHCP-сервера isc-dhcp-server

1. Откройте конфигурационный файл `/etc/dhcp/dhcpd.conf` и добавьте строки:

```
$ sudo gedit /etc/dhcp/dhcpd.conf

default-lease-time 120;
max-lease-time 600;

subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.2 192.168.1.23;
   option subnet-mask 255.255.255.0;
}
```

2. Имя сетевого интерфейса, на котором запущен DHCP-сервер, передается ему в качестве аргумента при вызове. В ОС Linux аргументы и ключи вызова программ задаются в каталоге `/etc/default`. Укажите сетевой интерфейс, на котором сервер будет прослушивать запросы от клиентов. Для этого откройте файл `/etc/default/isc-dhcp-server` и введите:

```
$ sudo gedit /etc/default/isc-dhcp-server

# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
```

3. Запустите DHCP-сервер:

```
$ sudo systemctl start isc-dhcp-server
```

> **Примечание**
>
> Каждый раз после изменения конфигурационного файла DHCP-сервера перезапускайте сервер с помощью команды:
>
> ```
> $ sudo systemctl restart isc-dhcp-server
> ```

4. Проверьте статус DHCP-сервера:

```
$ sudo systemctl status isc-dhcp-server
```

Настройка коммутатора

1. Активируйте режим DHCP Snooping на всех портах коммутатора:

```
enable address_binding dhcp_snoop ports 1-24
```

2. Укажите максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт:

```
config address_binding dhcp_snoop max_entry ports 1-24 limit 2
```

3. Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес DHCP-сервера с портом 17:

```
create address_binding ip_mac ipaddress 192.168.1.1 mac_address 0A-0A-0D-CE-01-05 ports 17
```

4. Активируйте функцию IP-MAC-Port Binding на портах и укажите режимы их работы. Для корректной работы протокола DHCP при активированной функции IMPB рекомендуется включить параметры **allow_zeroip** и **forward_dhcppkt**, которые позволяют передавать широковещательные сообщения DHCPDISCOVER от клиентов с IP-адресом источника 0.0.0.0:

```
config address_binding ip_mac ports 1-24 state enable arp_inspection loose allow_zeroip enable forward_dhcppkt enable
```

> **Примечание**
>
> Посмотреть созданные в режиме DHCP Snooping динамически записи и другие параметры можно с помощью команды:
>
> ```
> show address_binding dhcp_snoop
> ```