Пример настройки IP-MAC-Port Binding

Функция **IP-MAC-Port Binding** (IMPB) позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, VLAN и порта подключения. 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, VLAN и порта), пакеты будут передаваться, и клиенты получат доступ в сеть. Если при подключении клиента, связка MAC-IP-порт-VLAN будет отличаться от параметров заранее сконфигурированной записи (binding entry), коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный лист».

При активизации функции IMPB на порту нужно указать режим её работы: **Strict Mode** (в этом режиме порт по умолчанию заблокирован) или **Loose Mode** (в этом режиме порт по умолчанию открыт).

Работа функции IMPB опирается на работу функций **IP Source Guard** и **Dynamic ARP Inspection**. Функция IMPB не будет работать, если не активированы обе или одна из этих функций.

Функция **IP Source Guard** является фильтром IP-пакетов на каждом интерфейсе, которая позволяет их передачу только при совпадении параметров пакетов с параметрами любой из записей, связывающих IP-MAC-порт-VLAN .

Функция **IP Source Guard** получает информацию о привязке IP-MAC-порт-VLAN из двух источников:

- статических записей, созданных вручную администратором сети (static binding entry);
- динамических записей из таблицы привязки DHCP Snooping (DHCP Snooping binding database).

Коммутатор на основе статических или динамических записей создает аппаратный ACL на порту (Port ACL). IP-пакеты, приходящие на порт, будут проверяться списком управления доступом порта. Пакет, не прошедший проверку, будет отброшен.

Функция **Dynamic ARP Inspection** (DAI) анализирует пакеты ARP, получаемые в соответствующей VLAN. DAI определяет легитимность пакета ARP на основе привязок IP- и MAC-адресов, хранящихся в таблице DHCP Snooping, при условии, что эта функция включена в соответствующей VLAN на коммутаторе. DAI также может использовать списки управления доступом ARP (ARP ACL), настроенные администратором сети, для проверки пакетов ARP от узлов со статическими IP-адресами.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязки DHCP Snooping. Если пакету явно запрещен доступ списком управления доступа, пакет будет отброшен. Если пакету неявно запрещен доступ, он будет дополнительно сопоставлен с записями привязки DHCP Snooping, если не указано ключевое слово «static». Если пакету неявно запрещен доступ и указано ключевое слово «static», пакет будет отброшен.

Примечание к настройке

Рассматриваемый пример настройки подходит для следующих серий коммутаторов: DGS-1250, DGS-1510, DGS-1520, DGS-3130, DGS-3630, DXS-3610.

Задача

В локальной сети нужно запретить пользователям изменять MAC- и/или IP-адреса своих компьютеров, а также менять порт подключения к сети. Компьютеры используют статические адреса, DHCP не используется.

Задача решается настройкой совместной работы функций IP-MAC-Port Binding, IP Source Guard и Dynamic ARP Inspection.

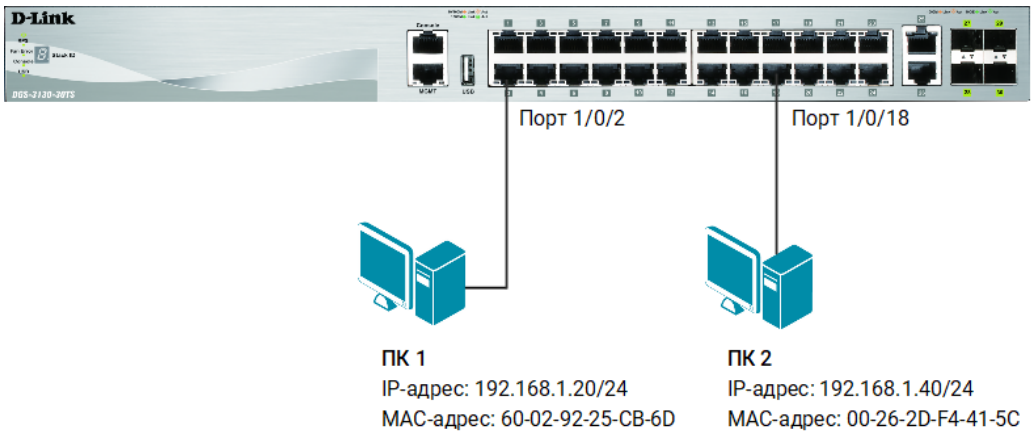

Рис. 1 Схема подключения

Настройка коммутатора

1. Создайте записи IP Source Guard для компьютеров ПК1 и ПК2:

```
Switch(config)#ip source binding 6002.9225.CB6D vlan 1 192.168.1.20 interface ethernet 1/0/2
Switch(config)#ip source binding 0026.2DF4.415C vlan 1 192.168.1.40 interface ethernet 1/0/18
```

> **Примечание**
>
> VLAN 1 существует на коммутаторе по умолчанию. Если используется VLAN с другим VID, то укажите его вместо 1.

2. Создайте ARP ACL с именем LIST1 и добавьте в него записи о ПК1 и ПК2:

```
Switch(config)#arp access-list LIST1
Switch(config-arp-nacl)#permit ip host 192.168.1.20 mac host 6002.9225.CB6D
Switch(config-arp-nacl)#permit ip host 192.168.1.40 mac host 0026.2DF4.415C
Switch(config-arp-nacl)#exit
```

3. Включите Dynamic ARP Inspection в VLAN:

```
Switch(config)#ip arp inspection vlan 1
Switch(config)#ip arp inspection validate
```

4. Укажите Dynamic ARP Inspection использовать созданный ARP ACL с именем LIST1 для фильтрации пакетов в VLAN:

```
Switch(config)#ip arp inspection filter LIST1 vlan 1
```

5. Включите IP-MAC-Port Binding на всех портах коммутатора в режиме strict:

```
Switch(config)#interface range ethernet 1/0/1-24
Switch(config-if-range)#ip ip-mac-port-binding strict
Switch(config-if-range)#ip verify source vlan dhcp-snooping ip-mac
Switch(config-if)#exit
```

6. При необходимости можно включить регистрацию событий Dynamic ARP Inspection:

```
Switch(config)#ip arp inspection vlan 1 logging acl-match all
```