Пример настройки списков управления доступом (Access Control List, ACL)

Списки управления доступом (Access Control List, ACL) являются средством фильтрации потоков данных без потери производительности, так как проверка содержимого пакетов данных выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешённых для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS, путём классификации трафика и переопределения его приоритета.

ACL представляют собой последовательность условий проверки параметров пакетов данных: коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определёнными в ACL, и выполняет над пакетами одно из действий: **Permit** (Разрешить) или **Deny** (Запретить).

В коммутаторах D-Link со стандартным CLI списки управления доступом (ACL) можно разделить на 3 группы:

- Стандартный список доступа (standard ACL);
- Расширенный список доступа (extended ACL);
- Экспертный список доступа (expert ACL).

Среди стандартных списков доступа выделяются:

- Стандартный список доступа IP (standard IP ACL);
- Стандартный список доступа IPv6 (standard IPv6 ACL).

Среди расширенных списков доступа выделяются:

- Расширенный список доступа MAC (extended MAC ACL);
- Расширенный список доступа IP (extended IP ACL);
- Расширенный список доступа IPv6 (extended IPv6 ACL).

Каждому списку управления доступом назначается имя и номер.

Для каждого типа списка зарезервирован свой диапазон номеров:

стандартные списки доступа IP	1—1999
расширенные списки доступа IP	2000—3999
расширенные списки доступа MAC	6000—7999
экспертные списки доступа	8000—9999
стандартные списки доступа IPv6	11000—12999

расширенные списки доступа IPv6 13000—14999

Имя списка доступа должно быть уникальным. Если при создании списка доступа указывается только его имя, то автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров, соответствующего типу списка доступа, и для каждого следующего списка будет уменьшаться на единицу.

Каждый ACL может состоять из множества правил. Все правила в ACL также нумеруются.

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Если это первая запись, то будет присвоен начальный порядковый номер 10. Последующим записям правила назначается номер, больший на значение шага 10, а самый большой порядковый номер в списке доступа будет стоять в конце.

Пользователь может использовать команду **access-list resequence** для смены начального порядкового номера и значения шага записей для указанного списка доступа. После применения команды новым записям без указанного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа.

При назначении порядкового номера вручную, лучше иметь зарезервированный интервал для будущих записей с меньшим порядковым номером. Иначе будет сложно вставить запись с еще меньшим порядковым номером.

Порядковый номер должен быть уникальным в домене списка доступа. При вводе занятого порядкового номера появится сообщение об ошибке.

В стандартном IP ACL критериями фильтрации могут выступать только IP-адреса источника и получателя пакета.

В расширенном IP ACL в числе критериев фильтрации могут выступать IP-адреса источника и получателя, порты протоколов транспортного уровня, поля ToS и DSCP в заголовке IP и некоторые другие параметры.

В расширенном MAC ACL в числе критериев фильтрации выступают MAC-адреса источника и получателя, тег VLAN, значение поля Ethertype и поле приоритета CoS.

Рекомендуется нумеровать правила в ACL с определенным интервалом, например: 10, 20, 30 и т.д.

При создании правила для указания диапазона адресов используется **инверсная маска** (wildcard mask). Бит адреса, соответствующий значению 1 бита маски, будет игнорироваться. Бит, соответствующий значению 0 бита маски, будет проверяться.

После создания ACL его нужно применить на одном или нескольких портах коммутатора (интерфейсах) и указать, для какого направления трафика должен использоваться этот фильтр — для входящего (in) или исходящего (out).

Если группа доступа IP (IP access group) уже настроена на интерфейсе, примененная позднее команда заменит предыдущие настройки. К каждому интерфейсу можно

применить только один список доступа определенного типа, но списки доступа различных типов могут быть применены к одному и тому же интерфейсу.

Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы из записей фильтрации коммутатора. Если ресурсов недостаточно для активации команды появится сообщение об ошибке. Число портов ограничено. Если применение команды исчерпает выбор доступных портов, появится сообщение об ошибке.

Примечание к настройке

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

Задача 1

В локальной сети требуется разрешить доступ к серверу только пользователям с IP-адресами с 192.168.1.16/24 по 192.168.1.31/24. Остальным пользователем сети 192.168.1.0/24 с адресами, не входящими в разрешённый диапазон, доступ к серверу нужно запретить.

Решается эта задача настройкой стандартного списка доступа IP.

Схема сети представлена на рисунке 1.

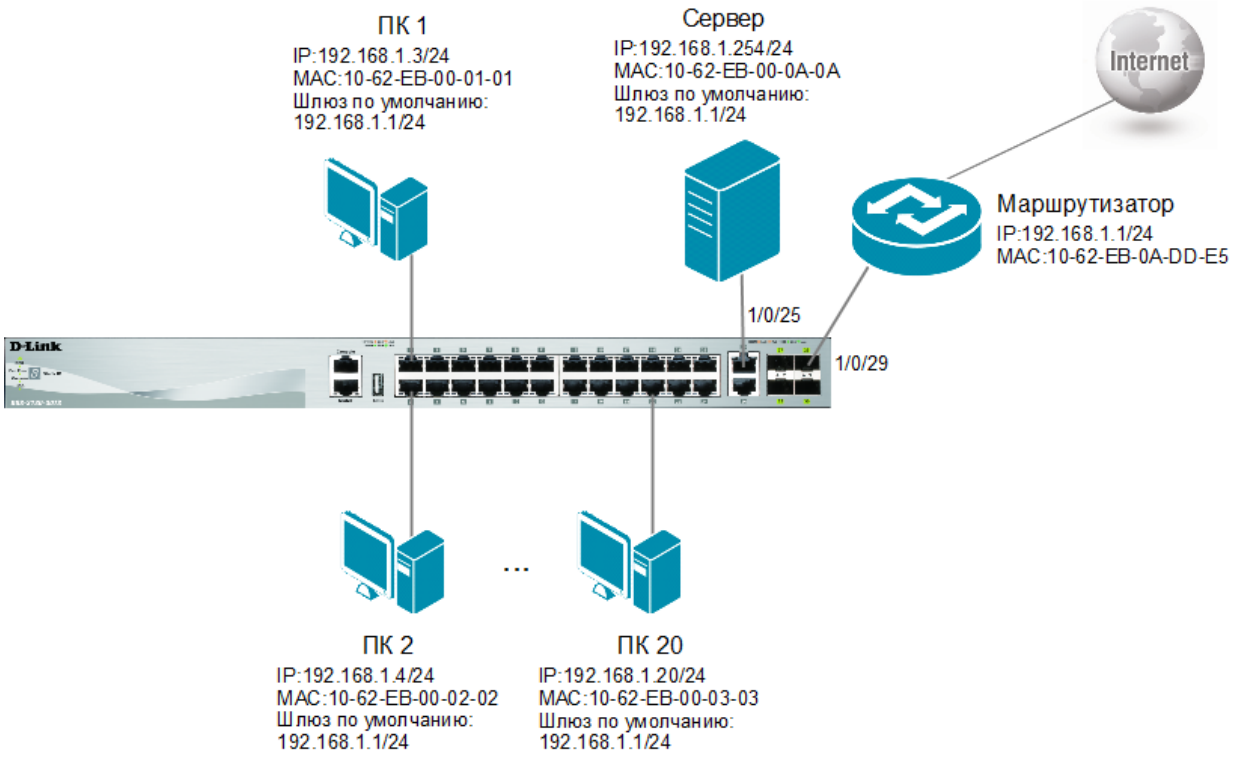

Рисунок 1. Схема подключения

Настройка коммутатора

1. Создайте стандартный список доступа с именем **std1** и номером 10, осуществляющий фильтрацию трафика по IP-адресам:

```
Switch# configure terminal
Switch(config)# ip access-list std1 10
```

2. Создайте правило для списка доступа **std1**, разрешающее доступ для подсети 192.168.1.16 — 192.68.1.31/24:

```
Switch(config-ip-acl)# permit 192.168.1.16 0.0.0.15 host 192.168.1.254
```

3. Добавьте в список доступа **std1** правило, запрещающее остальным станциям доступ к серверу:

```
Switch(config-ip-acl)# deny any host 192.168.1.254
Switch(config-ip-acl)# exit
```

4. Привяжите созданный список доступа к портам с 1/0/1 по 24. Список должен фильтровать входящий трафик:

```
Switch(config)# interface range ethernet 1/0/1-24
Switch(config-if-range)# ip access-group 10 in
Switch(config-if-range)# end
```

> **Примечание**
> Проверить выполненные настройки можно при помощи команд:
>
> Switch# **show access-list**
> Switch# **show access-list ip std1**
> Switch# **show access-group**

Задача 2

В локальной сети пользователям, которые подключены к портам с 1/0/1 по 10, доступ в Интернет запрещен.

Схема сети представлена на рисунке 2.

Решается эта задача настройкой расширенного списка доступа MAC.

Политика по умолчанию разрешает прохождение через коммутатор всего трафика. Поэтому надо создать правило, запрещающее прохождение через коммутатор кадров с MAC-адресом назначения, равным MAC-адресу маршрутизатора от устройств, подключенных к портам с 1/0/1 по 10. Ко всему остальному трафику, будет применяться политика по умолчанию.

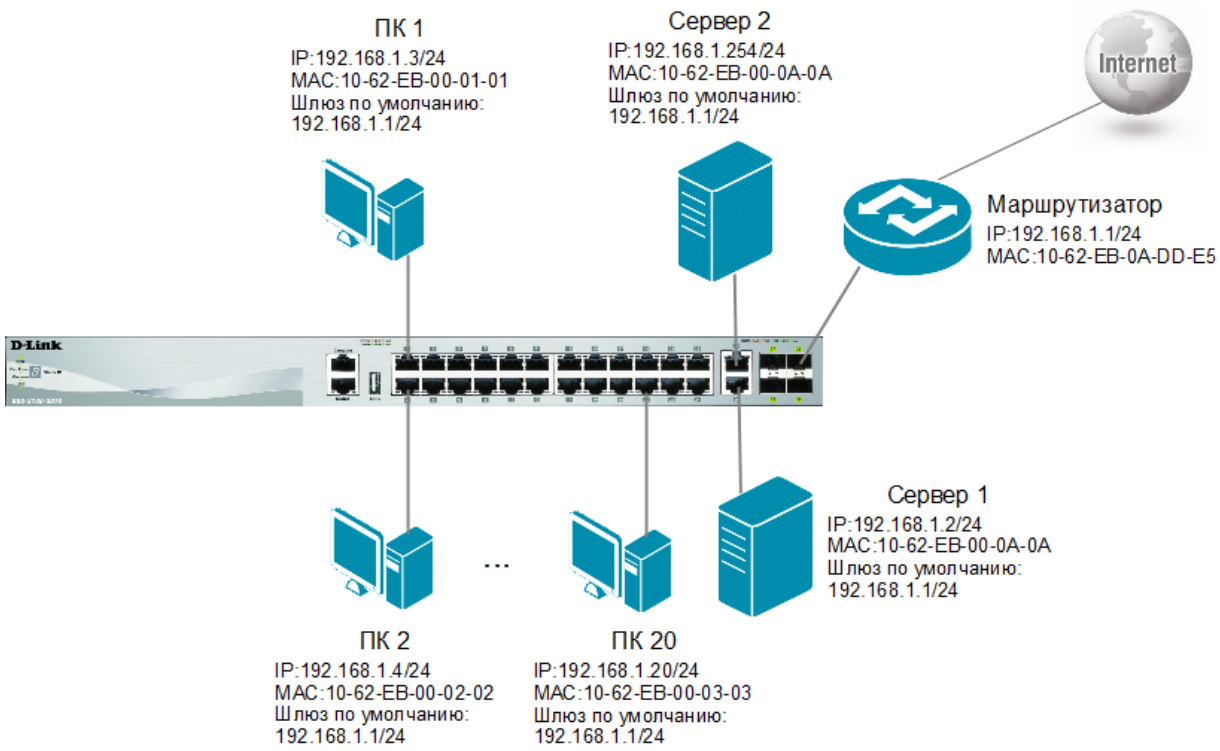

Рисунок 2. Схема подключения

Настройка коммутатора

1. Создайте расширенный список доступа MAC с именем **mac1** и номером 6010:

```
Switch# configure terminal
Switch(config)#mac access-list extended mac1 6010
```

2. Создайте для списка доступа **mac1** правило, запрещающее передачу трафика, если MAC-адрес назначения равен MAC-адресу маршрутизатора:

```
Switch(config-mac-ext-acl)#deny any host 1062.EB0A.DDE5
Switch(config-mac-ext-acl)#exit
```

3. Привяжите созданный список доступа к портам с 1/0/1 по 10. Список должен фильтровать входящий трафик:

```
Switch(config)# interface range ethernet 1/0/1-10
Switch(config-if-range)# ip access-group mac1 in
Switch(config-if-range)# end
```

4. По умолчанию весь трафик от устройств, подключенных к другим портам коммутатора, разрешен.

> **Примечание**
> Проверить выполненные настройки можно при помощи команд:
>
> Switch# **show access-list**
> Switch# **show access-list mac mac1**
> Switch# **show access-group**

Задача 3

В локальной сети нужно разрешить тестировать доступность шлюза по умолчанию при помощи утилиты ping только с рабочей станции администратора, IP-адрес которой 192.168.1.20/24. Весь остальной трафик с других рабочих станций на шлюз по умолчанию разрешен.

Схема сети представлена на рисунке 3.

Решается эта задача настройкой расширенного списка доступа IP.

В этом списке доступа надо создать 2 правила:

- Правило 1: разрешить передачу ICMP-пакетов, у которых IP-адрес источника совпадает с адресом рабочей станции администратора 192.168.1.20/24, а IP-адрес получателя равен адресу шлюза по умолчанию 192.168.1.1/24.
- Правило 2: запретить передачу ICMP-пакетов с любым IP-адресом источника и IP-адресом получателя равным адресу шлюза по умолчанию 192.168.1.1/24.

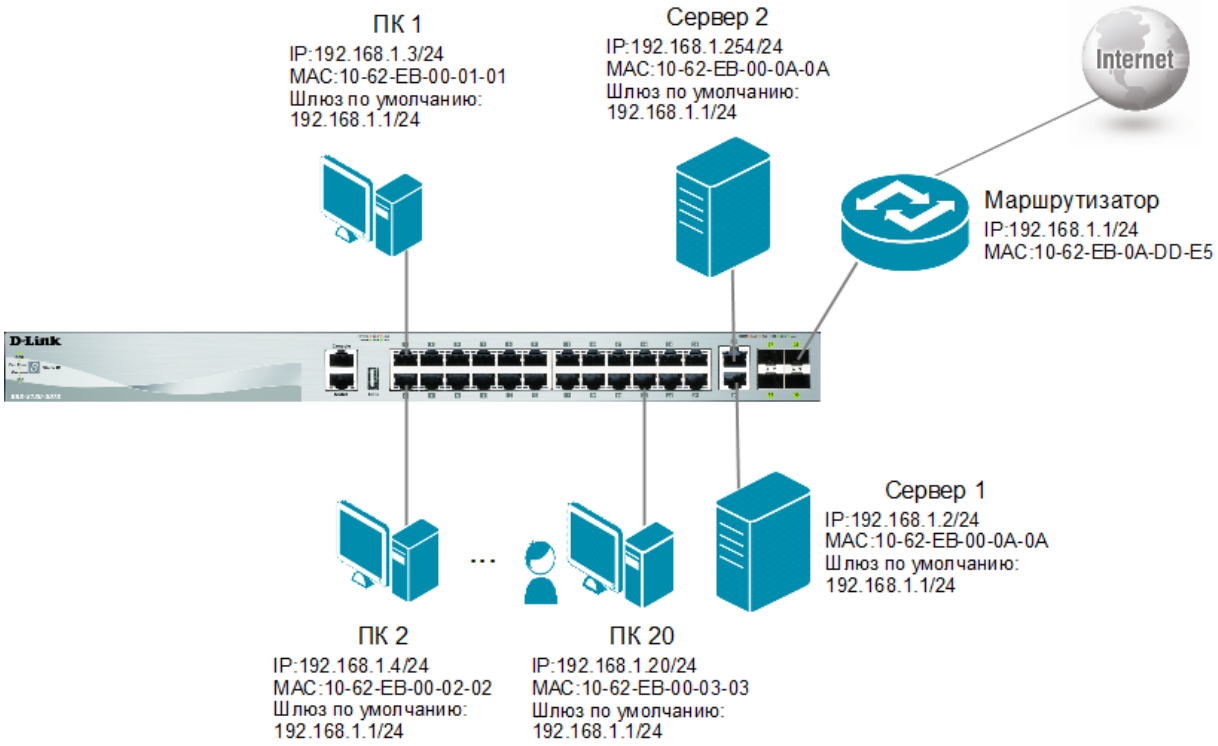

Рисунок 3. Схема подключения

Настройка коммутатора

1. Создайте расширенный список доступа IP с именем **ext1** и номером 2010:

```
Switch# configure terminal
Switch(config)#ip access-list extended ext1 2010
```

2. Добавьте в список доступа **ext1** правило, разрешающее передачу ICMP-пакетов с IP-адреса 192.168.1.20/24 на IP-адрес 192.168.1.1/24:

```
Switch(config-ip-ext-acl)#permit icmp host 192.168.1.20 host 192.168.1.1
```

3. Добавьте в список доступа **ext1** правило, запрещающее передачу ICMP-пакетов с IP-адресом назначения 192.168.1.1/24 от остальных узлов:

```
Switch(config-ip-ext-acl)#deny icmp any host 192.168.1.1
Switch(config-ip-ext-acl)#exit
```

4. Привяжите созданный список доступа **ext1** к портам с 1/0/1 по 24. Список должен фильтровать входящий трафик:

```
Switch(config)# interface range ethernet 1/0/1-24
Switch(config-if-range)# ip access-group ext1 in
Switch(config-if-range)# end
```

Примечание
Проверить выполненные настройки можно при помощи команд:

Switch# **show access-list**
Switch# **show access-list ip ext1**
Switch# **show access-group**