Семинар 3

Функциональные возможности управляемых коммутаторов

Николаев Андрей

г. Красноярск, 2016

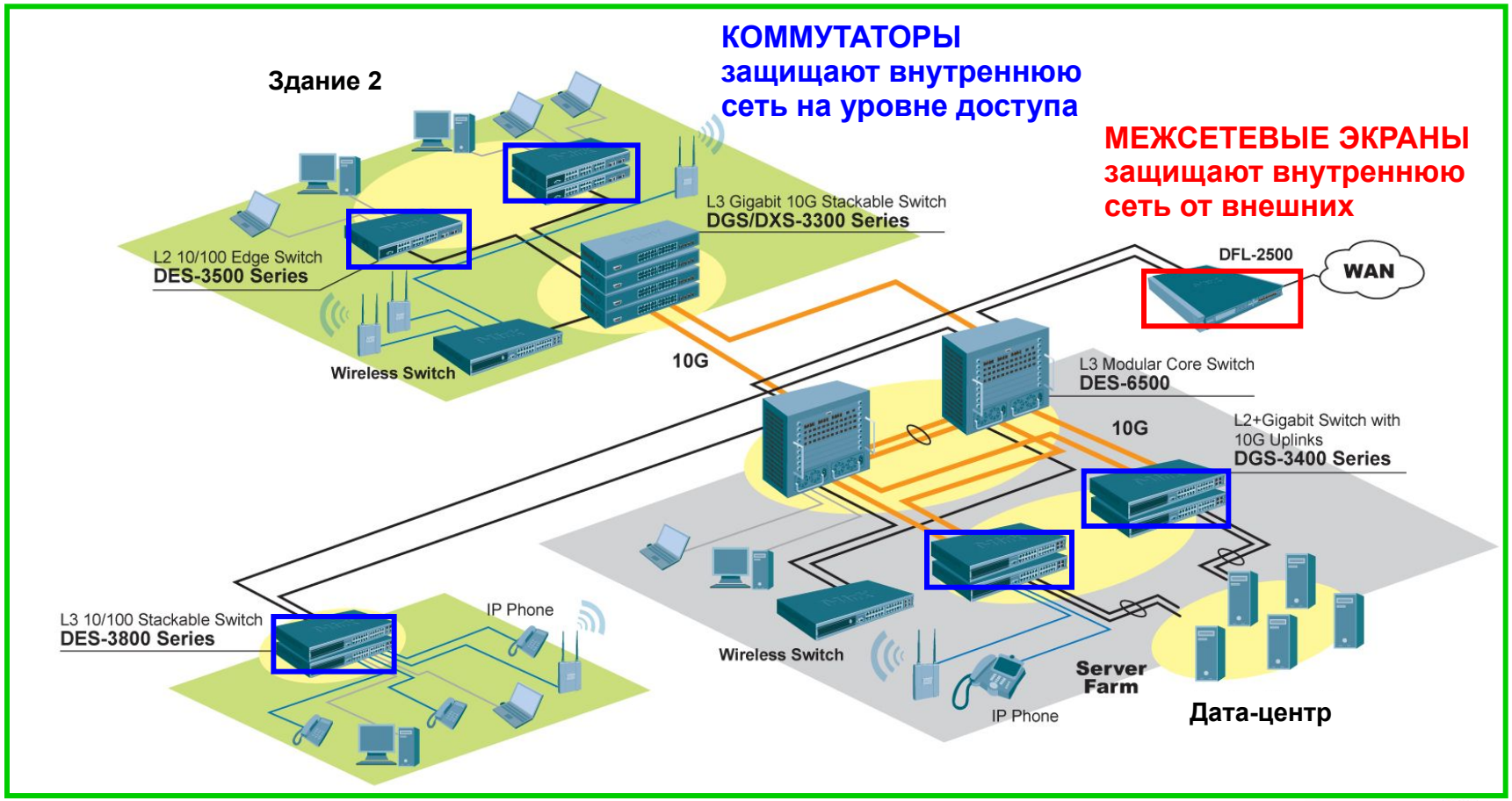
D-Link®
Building Networks for People

Содержание

- Функции сетевой защиты на уровне доступа;
- Функции защиты процессора коммутатора от перегрузок и нежелательного трафика;
- Организация многоадресной передачи с помощью управляемых коммутаторов

Функции сетевой защиты на уровне доступа

Роль активного сетевого оборудования в организации защиты ЛВС

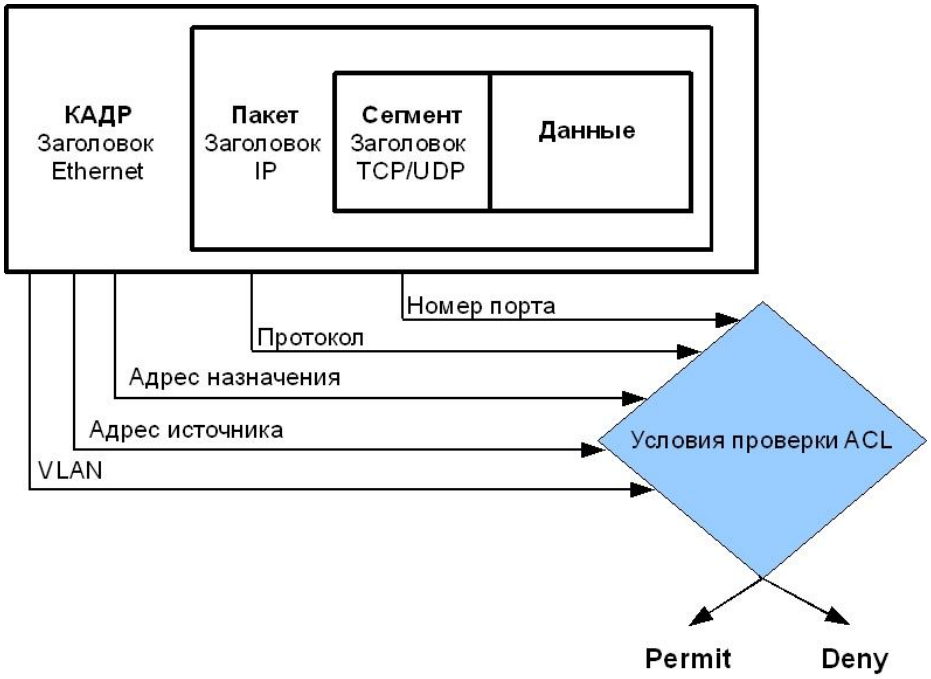


D-Link
Building Networks for People

Списки управления доступом ACL

***Списки управления доступом* (*Access Control List, ACL*)** - средство фильтрации трафика, проходящего через коммутатор без потери производительности (фильтрация выполняется на аппаратном уровне).

ACL представляют собой последовательность условий проверки параметров в протокольных заголовках Ethernet-кадра.

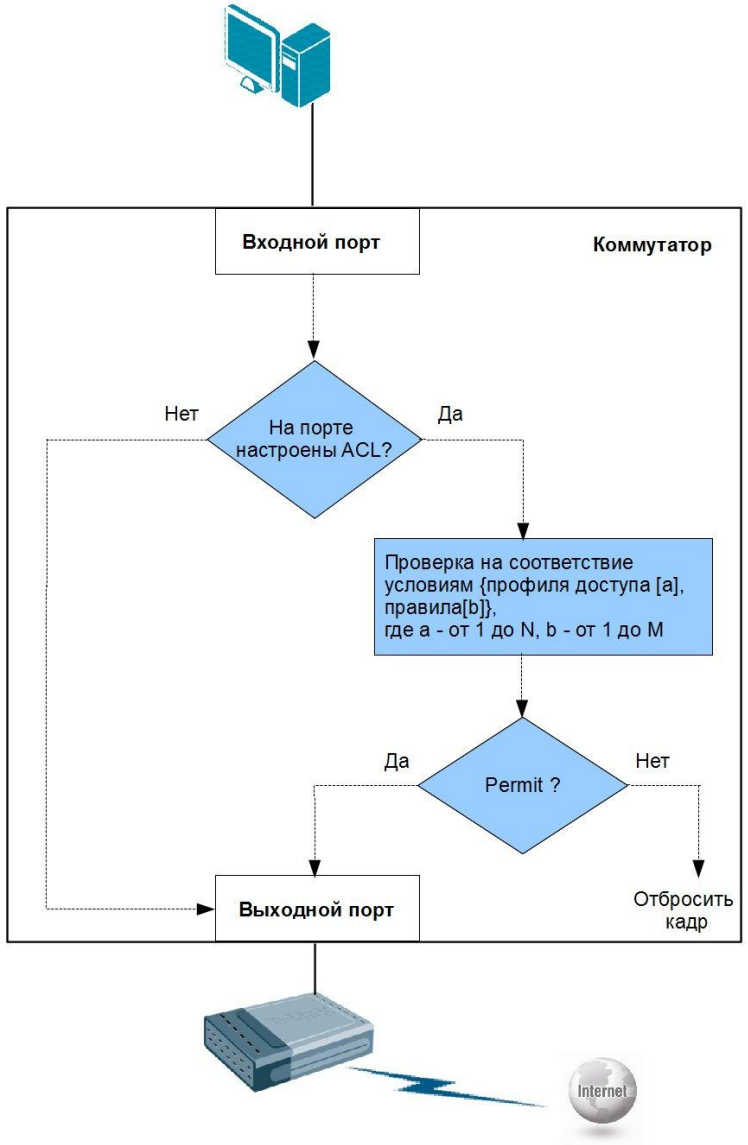


Профили доступа и правила ACL

- Списки управления доступом состоят из **профилей доступа** (Access Profile) и **правил** (Rule).
- Профили доступа определяют типы критериев фильтрации, которые должны проверяться в пакете данных (MAC-адрес, IP-адрес, номер порта, VLAN и т.д.).
- В правилах ACL указываются непосредственно значения их параметров.
- Каждый профиль может состоять из множества правил.

Профиль Ethernet **(Ethernet Profile)**	***Профиль IP*** **(IP Profile)**
Позволят фильтровать кадры по следующим типам критериев: VLAN; MAC-адрес источника; MAC-адрес назначения; 802.1p; тип Ethernet.	Поддерживает следующие типы критериев фильтрации: VLAN; маска IP-источника; маска IP-назначения; DSCP; протокол (ICMP, IGMP, TCP, UDP); номер порта TCP/UDP.
Профиль фильтрации по содержимому пакета **(Packet Content Filtering Profile)**	
Используется для идентификации пакетов, путем побайтного исследования их заголовков Ethernet.	

Принцип работы ACL



Процесс создания профиля доступа

Процесс создание профиля доступа можно разделить на следующие основные шаги:

- Анализируется задача фильтрации и определяется тип профиля доступа – Ethernet, IP или Packet Content Filtering;
- Определяется стратегия фильтрации;
- Основываясь на выбранной стратегии, определяется маска профиля доступа. Маска профиля доступа используется для указания, какие биты значений полей IP-адрес, MAC-адрес, порт TCP/UDP и т.д. должны проверяться в пакете данных, а какие игнорироваться;
- Добавляется правило профиля доступа (Access Profile Rule), связанное с этой маской.

Процесс создания профиля доступа

- Правила фильтрации формируются в соответствующие профильные группы с номером (access_id);
- Каждый профиль проверяется последовательно сверху вниз в соответствии с его номером.
- Чем меньше номер access_id, тем раньше проверяется правило. Если ни одно правило не сработало, пакет данных пропускается.

Вычисление маски профиля доступа

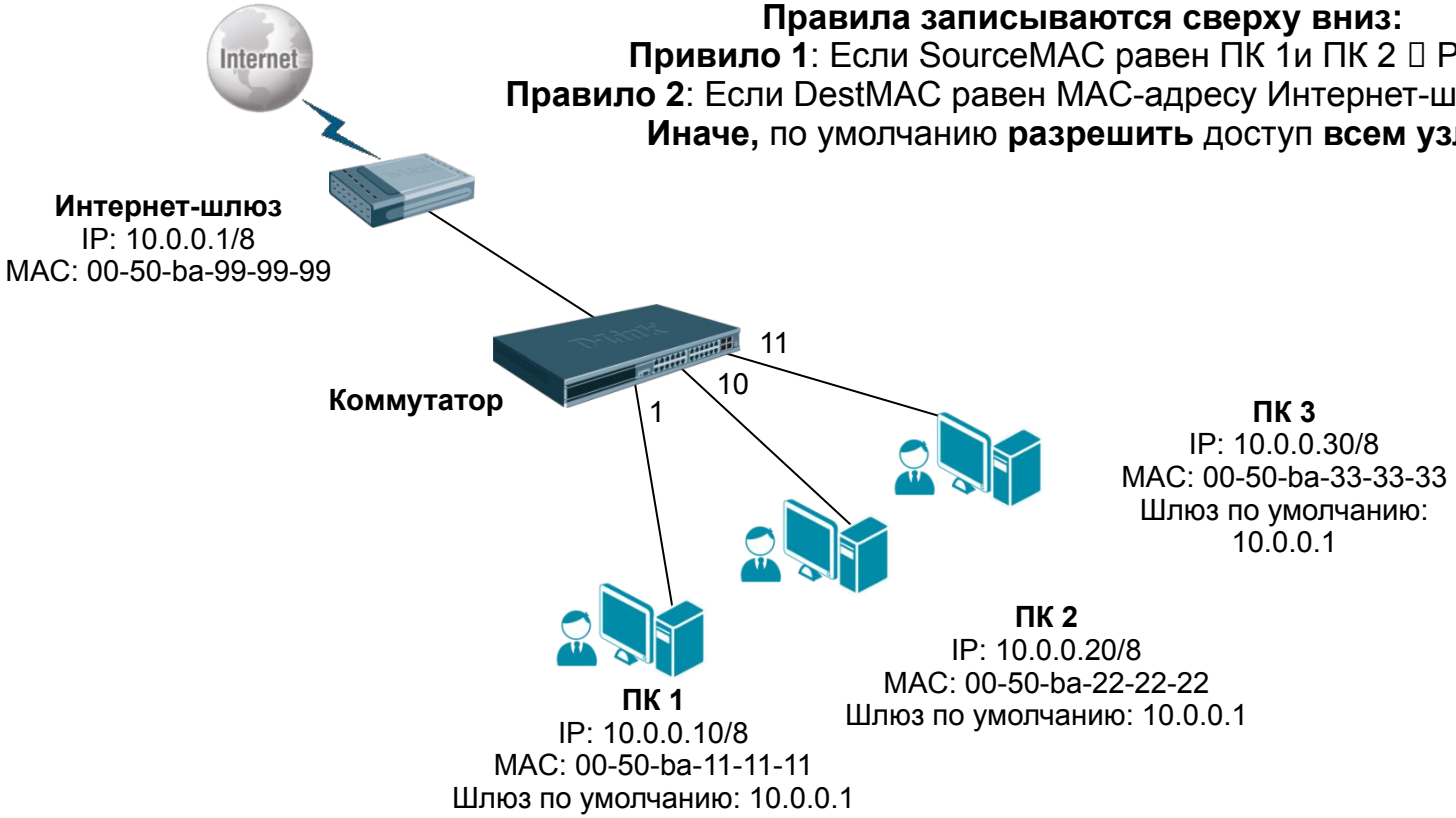
Маска профиля доступа определяет, какие биты в значениях полей IP-адрес, MAC-адрес, порт TCP/UDP и т.д. приходящих на коммутатор кадров, должны проверяться, а какие игнорироваться. Биты маски имеют следующие значения:

- **«0»** – означает игнорирование значения соответствующего бита поля пакета данных;
- **«1»** – означает проверку значения соответствующего бита поля пакета данных.

Если, например, необходимо изучать все разряды MAC-адреса, чтобы, например, запретить прохождение трафика от узла с MAC-адресом **01-00-00-00-AC-11**, маска профиля доступа для этого адреса будет равна **FF-FF-FF-FF-FF-FF**.

Пример настройки ACL

ТЗ. Пользователи ПК 1 и ПК 2 получат доступ в Интернет, т.к. их MAC-адреса указаны в разрешающем правиле 1. Как только пользователи других компьютеров попытаются выйти в Интернет, сработает правило 2, которое запрещает прохождение через коммутатор кадров с MAC-адресом назначения, равным MAC-адресу Интернет-шлюза.



Пример настройки ACL

Профиль 1: если MAC-адрес источника SourceMAC равен MAC-адресам ПК 1 или ПК 2, то следует разрешить трафик.

```
create access_profile ethernet source_mac FF-FF-FF-FF-FF-FF
profile_id 1 profile_name Permit_Internet
config access_profile profile_id 1 add access_id 1 ethernet
source_mac 00-50-ba-11-11-11 port 1 permit
config access_profile profile_id 1 add access_id 2 ethernet
source_mac 00-50-ba-22-22-22 port 10 permit
```

Профиль 2: если MAC-адрес назначения DestMAC равен MAC-адресу Интернет-шлюза, то следует запретить трафик.

```
create access_profile ethernet destination_mac
FF-FF-FF-FF-FF-FF profile_id 2 profile_name Deny_Internet
config access_profile profile_id 2 add access_id 1 ethernet
destination_mac 00-50-ba-99-99-99 port 11 deny
```

Иначе, по умолчанию разрешить всем узлам весь трафик.

Функция IP-MAC-Port Binding (IMPB)

Функция IP-MAC-Port Binding (IMPB) позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения.

- Администратор сети может создать записи в т. н. «белом листе» и на основе этих записей клиенты будут получать доступ к сети со своих компьютеров.
- Если при подключении клиента, связка MAC-IP-порт будет отличаться от параметров заранее сконфигурированной записи, то коммутатор будет блокировать доступ к сети для такого клиента.

Пример настройки функции IP-MAC-Port Binding

«Хакер» пытается подключиться к коммутатору. Коммутатор обнаруживает, что на порт 10 приходят кадры, связка IP-MAC для которых отсутствует в «белом листе» IMPB, и блокирует эти кадры.

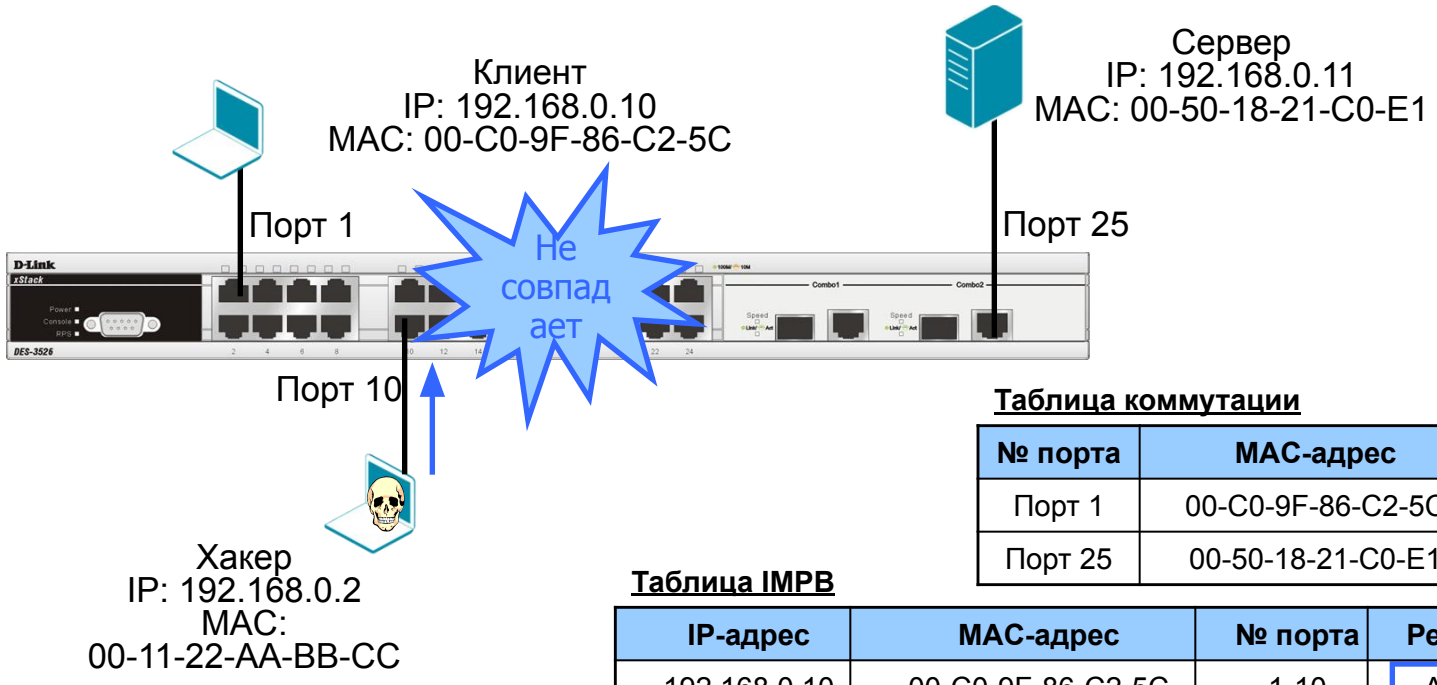


Таблица коммутации

№ порта	MAC-адрес
Порт 1	00-C0-9F-86-C2-5C
Порт 25	00-50-18-21-C0-E1

Таблица IMPB

IP-адрес	MAC-адрес	№ порта	Режим
192.168.0.10	00-C0-9F-86-C2-5C	1-10	ARP

Пример настройки функции IP-MAC-Port Binding

//Создать запись IP-MAC-Port Binding и указать режим работы //функции

```
create address_binding ip_mac ipaddress 192.168.0.10
mac_address 00-C0-9F-86-C2-5C ports 1-10
```

//Активизировать функцию на требуемых портах

```
config address_binding ip_mac ports 1-10 state enable
```

Функция Port Security

- Функция Port Security позволяет:
  - ограничивать количество подключаемых к порту пользователей;
  - контролировать доступ к порту по MAC-адресам подключаемых устройств.

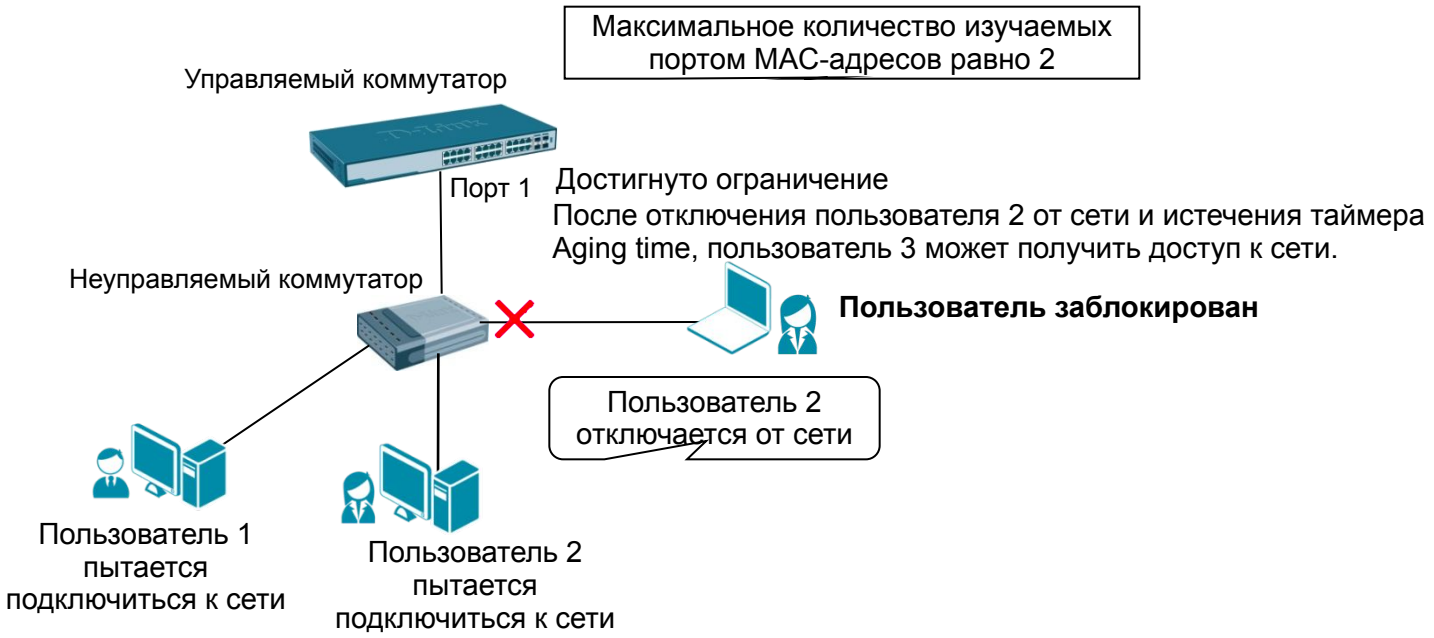


Рисунок анимирован

Режимы работы функции Port Security

Существует три режима работы функции Port Security:

- ***Permanent* (Постоянный)** – занесенные в таблицу коммутации MAC-адреса никогда не устареет, даже если истекло время, установленное таймером FDB Aging Time или коммутатор был перезагружен.
- ***Delete on Timeout* (Удалить по истечении времени)** – занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером FDB Aging Time и будут удалены.
- ***Delete on Reset* (Удалить при сбросе настроек)** – занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

Пример настройки функции Port Security

ТЗ. На портах 1-3 управляемого коммутатора настроить ограничение по количеству подключаемых пользователей равное 2. MAC-адреса подключаемых пользователей изучаются динамически. Режим работы функции - Delete on Timeout.

- `config port_security ports 1-3 admin_state enabled max_learning_addr 2 lock_address_mode DeleteOnTimeout`

Проверить настройку функции можно с помощью команды:

- `show port_security`

Если необходимо, чтобы коммутатор «отписывался» в Log-файле при подключении неавторизованного пользователя к порту коммутатора, администратор может настроить выполнение этих действий с помощью команды:

- `enable port_security trap_log`

Пример настройки функции Port Security

Используя функцию Port Security можно полностью запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те пользователи, MAC-адреса которых указаны в статической таблице коммутации.

Настройка коммутатора

//Активизировать функцию Port Security на соответствующих портах и запретить //изучение MAC-адресов (параметр `max_learning_addr` установить равным 0).

- `config port_security ports 1-24 admin_state enabled max_learning_addr 0`

//Создать записи в статической таблице MAC-адресов (имя VLAN в примере “default”).

- `create fdb default 00-50-ba-00-00-01 port 2`
- `create fdb default 00-50-ba-00-00-02 port 2`
- `create fdb default 00-50-ba-00-00-03 port 2`
- `create fdb default 00-50-ba-00-00-04 port 2`
- `create fdb default 00-50-ba-00-00-05 port 8`
- `.....` (аналогично для всех требуемых портов)

Функции защиты процессора коммутатора от перегрузок и нежелательного трафика

Функции защиты ЦПУ коммутатора

В коммутаторах D-Link реализованы функции **Safeguard Engine** и **CPU Interface Filtering**, обеспечивающие защиту ЦПУ от обработки нежелательных пакетов и перегрузок.

Повод для использования:

- возникновение в сети многоадресных или широковещательных штормов, вызванных неправильной настройкой оборудования, петлями или сетевыми атаками,
- Неправильно рассчитанная нагрузка на коммутатор и его порты,
- неконтролируемый администратором «флуд» в сети.

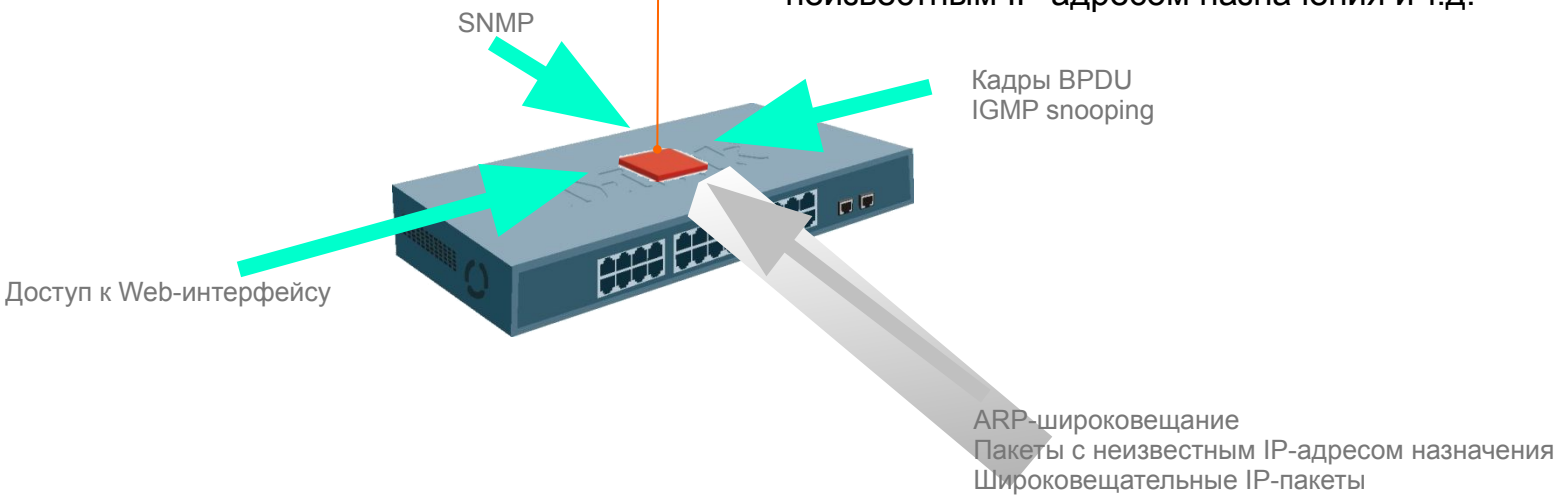
Функция Safeguard Engine

Safeguard Engine - функция для обеспечения возможности снижения загрузки процессора управляемого коммутатора.

ЦПУ испытывает сильную загрузку и не может выполнять такие важные задачи как административный доступ, STP, SNMP и т.д.

ЦПУ коммутатора предназначено для обработки пакетов протоколов STP, SNMP, осуществления доступа к Web-интерфейсу и т.д.

Также для обработки на ЦПУ отправляются некоторые специальные пакеты, такие как широковещательные ARP-пакеты, пакеты с неизвестным IP-адресом назначения и т.д.



Пример настройки функции Safeguard Engine

ТЗ: одна из рабочих станций, подключенных к коммутатору, постоянно рассылает ARP-пакеты с очень высокой скоростью. Загрузка ЦПУ коммутатора при этом меняется от нормальной до 90%.

Решение: для защиты ЦПУ от данной ситуации и снижения его загрузки, на коммутаторе настраивается функция Safeguard Engine.

Настройка коммутатора

//Активация функции Safeguard Engine.

```
config safeguard_engine  state enable
```

//Задание нижнего и верхнего порогового значения загрузки ЦПУ в процентах, при
//которых будет происходить переключение между нормальным режимом работы и
//режимом Exhausted.

```
config safeguard_engine utilization rising 70 falling 50 mode strict
```

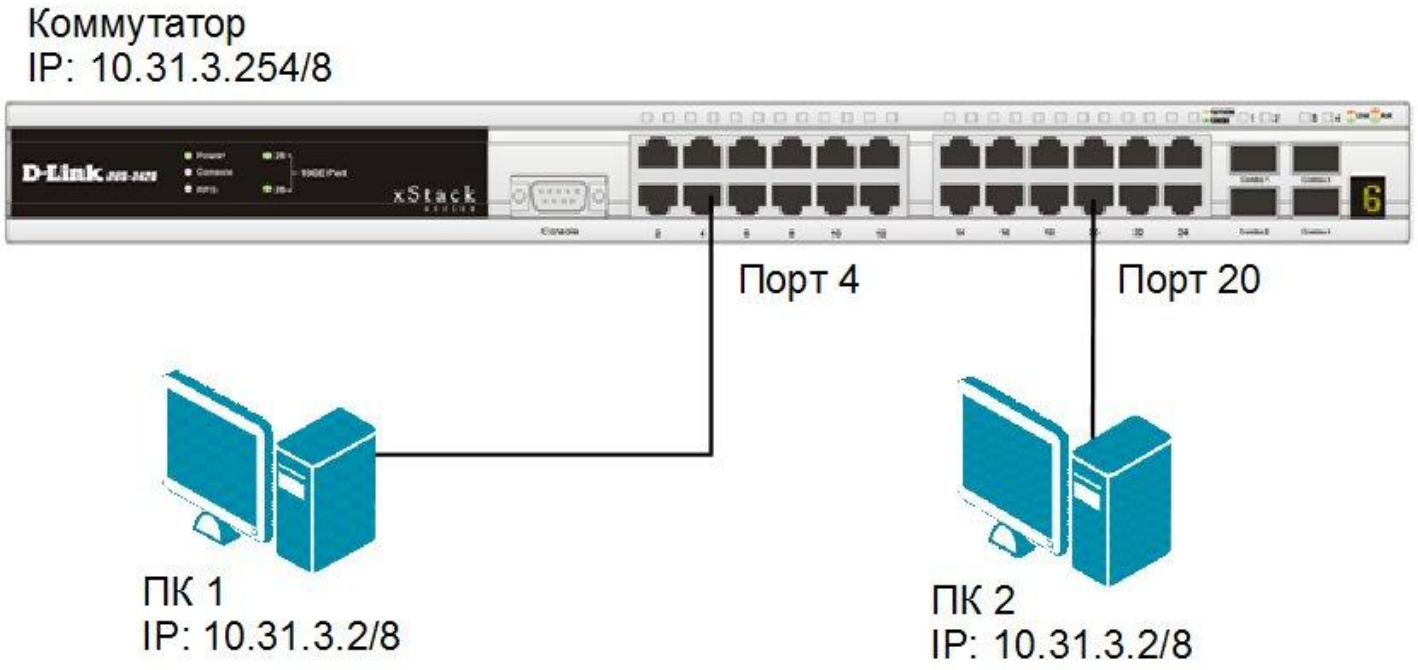
Функция CPU Interface Filtering

CPU Interface Filtering – функция, позволяющая ограничивать пакеты, поступающие для обработки на ЦПУ, путем фильтрации нежелательного трафика на аппаратном уровне.

По своей сути функция CPU Interface Filtering представляет собой списки управления доступом к интерфейсу ЦПУ и обладает аналогичными стандартным ACL принципами работы и конфигурации.

Пример настройки функции CPU Interface Filtering

ТЗ: необходимо настроить коммутатор таким образом, чтобы пакеты ICMP (например, команда Ping), передаваемые компьютером ПК 2, не отправлялись на обработку на ЦПУ, но при этом ПК 2 мог передавать подобные пакеты другим устройствам, например ПК 1.



Пример настройки функции CPU Interface Filtering

//Активация функции CPU Interface Filtering на коммутаторе

```
enable cpu_interface_filtering
```

//Создание профиль доступа для интерфейса ЦПУ

```
create cpu access_profile ip source_ip_mask
255.255.255.255 icmp profile_id 1
```

//Создание правила в профиле доступа

```
config cpu access_profile profile_id 1 add access_id 1
ip source_ip 10.31.3.2 icmp deny
```

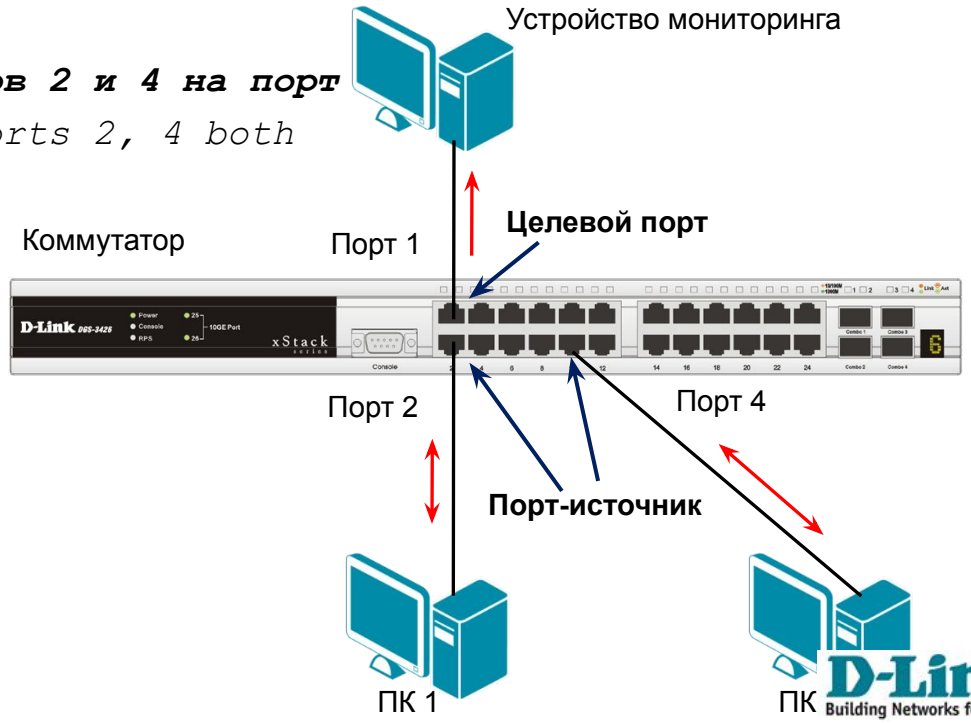
Доп. функция контроля трафика

Функция Port Mirroring

- Функция *Port Mirroring* (Зеркалирование портов) позволяет отображать (копировать) кадры, принимаемые и отправляемые портом-источником (Source port) на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга с целью анализа проходящих через интересующий порт пакетов.
- Целевой порт и порт-источник должны принадлежать одной VLAN и иметь одинаковую скорость работы.

Настройка коммутатора

```
//Настройка зеркалирования с портов 2 и 4 на порт
config mirror port 1 add source ports 2, 4 both
//Включение зеркалирования
enable mirror
```



Организация многоадресной передачи с помощью управляемых коммутаторов

Виды передачи данных

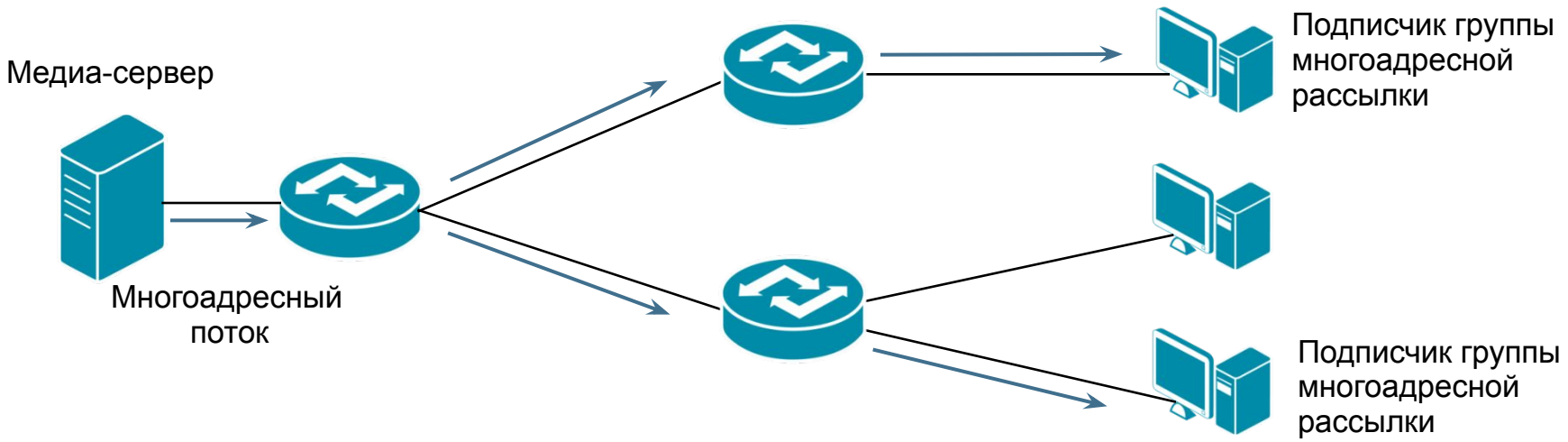
- **одноадресная передача (*Unicast*)** - поток данных передается от узла-отправителя на индивидуальный *IP-адрес конкретного узла-получателя*;

- **широковещательная передача (*Broadcast*)** - поток данных передается от узла-отправителя множеству узлов-получателей, подключенных к сети, используя *широковещательный IP-адрес*;

- **многоадресная рассылка *(Multicast*)** - поток данных передается группе узлов на множество IP-адресов *группы многоадресной рассылки*.

Многоадресная рассылка

- У группы многоадресной рассылки нет географических ограничений: узлы могут находиться в любой точке мира.
- Узлы, которые заинтересованы в получении данных для определенной группы, должны присоединиться к этой группе (подписаться на рассылку) при помощи **протокола IGMP** (Internet Group Management Protocol).
- После подписки узла на группу пакеты многоадресной рассылки IP, будут поступать в том числе и на этот узел.

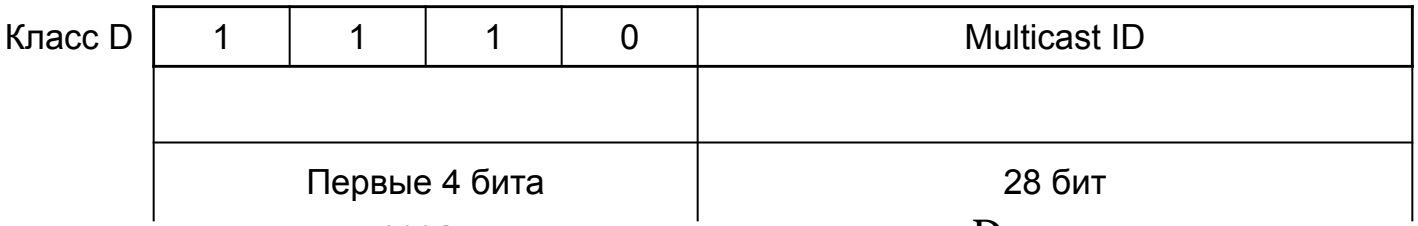


Многоадресная рассылка

Принципы адресации MULTICAST в IPv4

- Источник многоадресного трафика направляет пакеты многоадресной рассылки на групповой IP-адрес.
- Групповые адреса определяют произвольную группу IP-узлов, присоединившихся к этой группе и желающих получать адресованный ей трафик.
- **Агентство IANA** (Internet Assigned Numbers Authority), выделило для многоадресной рассылки адреса IPv4 класса D в диапазоне от 224.0.0.0 до 239.255.255.255.

• Формат IP-адреса **класса D**:



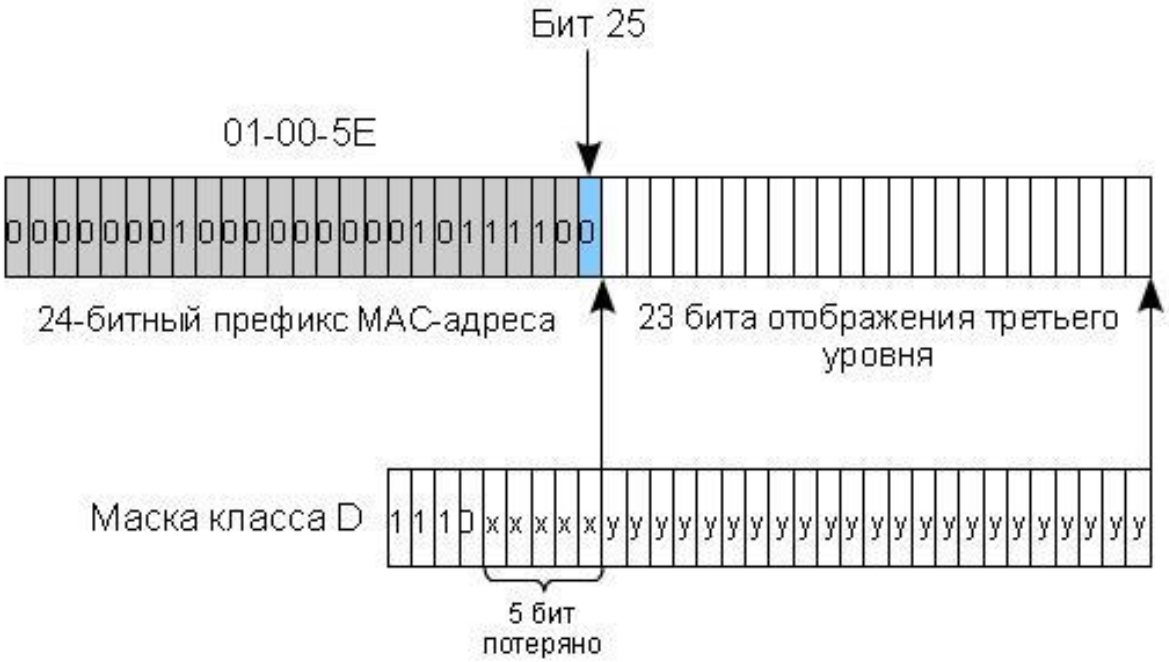
• Первые 4 бита – всегда равны 1110 и определяют класс сети D;

• Остальные 28 бит – используются для идентификации конкретной группы получателей многоадресного трафика.

Многоадресная рассылка

Принципы адресации MULTICAST на канальном уровне

- MAC-адрес групповой рассылки начинается с префикса, состоящего из 24 бит – **0x01-00-5E**. Следующий 25-й бит (или бит высокого порядка) приравнивается к 0. Последние 23 бита MAC-адреса формируются из 23 младших бит группового IP-адреса.
- При преобразовании теряются 5 битов 1-го октета IP-адреса, получившийся адрес не является уникальным.
- Каждому MAC-адресу соответствует 32 IP-адреса групповой рассылки.



Многоадресная рассылка

Подписка и обслуживание групп

- **Протокол IGMP** используется для динамической регистрации отдельных узлов в многоадресной группе локальной сети.

- В настоящее время существуют три версии протокола IGMP:
  - IGMPv1 (RFC 1112), IGMPv2 (RFC 2236), IGMPv3 (RFC 3376).

- Узлы сети определяют принадлежность к группе, посылая IGMP-сообщения на свой локальный многоадресный маршрутизатор. По протоколу IGMP маршрутизаторы (коммутаторы L3) получают IGMP-сообщения и периодически посылают запросы, чтобы определить, какие группы активны или неактивны в данной сети.

- В общем случае протокол IGMP определяет следующие типы сообщений:
  - **запрос о принадлежности к группе** (Membership Query);
  - **ответ о принадлежности к группе** (Membership Report);
  - **сообщение о выходе из группы** (Leave Group Message).

Многоадресная рассылка

IGMP Snooping

Основная проблема – эффект «флудинга» при передаче multicast-трафика коммутатором L2 (передача многоадресного трафика через все порты).

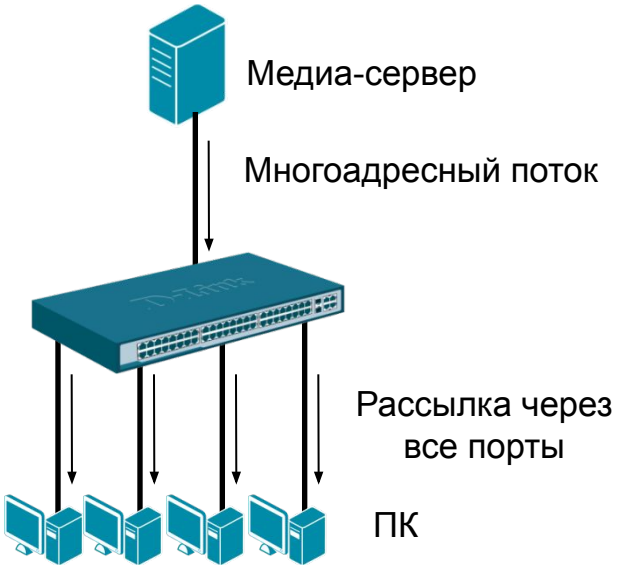
Управление многоадресной рассылкой на коммутаторе L2 может быть выполнено двумя способами:

- Созданием статических записей в таблицах коммутации для портов, к которым не подключены подписчики многоадресных групп;
- Использованием функции **IGMP Snooping** (прослушиванием multicast- трафика).

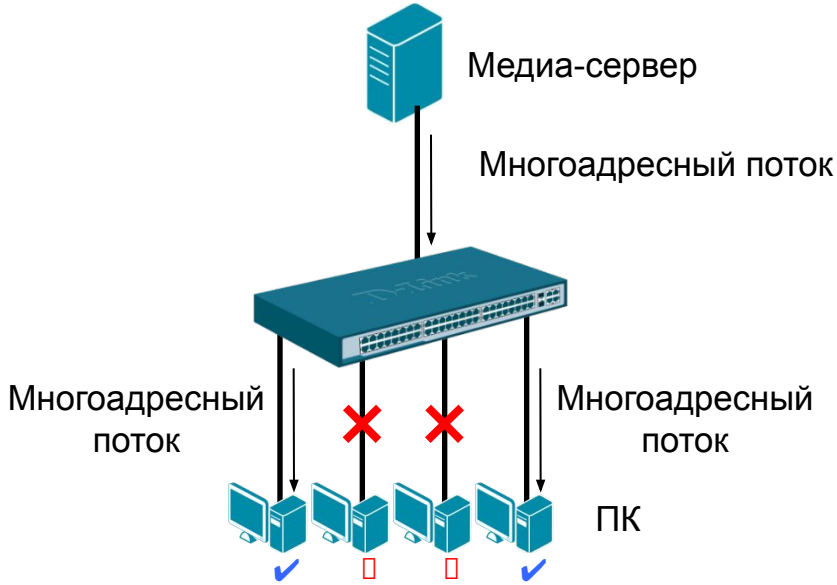
Многоадресная рассылка

Функция IGMP Snooping

- **IGMP Snooping** – это функция, которая позволяет коммутаторам L2 изучать членов многоадресных групп, подключенных к его портам, прослушивая IGMP-сообщения (запросы и ответы), передаваемые между узлами-подписчиками и маршрутизаторами (коммутаторами L3).



Без поддержки IGMP Snooping



С поддержкой IGMP Snooping

Рисунок анимирован

Многоадресная рассылка

Функция IGMP Snooping

1) Когда узел, подключенный к коммутатору, хочет вступить в многоадресную группу или отвечает на IGMP-запрос, полученный от маршрутизатора многоадресной рассылки, он отправляет IGMP-ответ, в котором указан адрес многоадресной группы.
2) Коммутатор просматривает информацию в IGMP-ответе и создает в своей **ассоциативной таблице коммутации IGMP Snooping** запись для этой группы (если она не существует). Эта запись связывает порт, к которому подключен узел-подписчик, порт, к которому подключен маршрутизатор (коммутатор уровня 3) многоадресной рассылки, и MAC-адрес многоадресной группы.
3) Если коммутатор получает IGMP-ответ для этой же группы от другого узла данной VLAN, то он добавляет номер порта в уже существующую запись ассоциативной таблицы коммутации IGMP Snooping.

- Формируя таблицу коммутации многоадресной рассылки, коммутатор осуществляет передачу многоадресного трафика только тем узлам, которые в нем заинтересованы.
- Когда коммутатор получает IGMP-сообщение о выходе узла из группы, он удаляет номер порта, к которому подключен этот узел, из соответствующей записи таблицы коммутации IGMP Snooping.

Многоадресная рассылка

Процесс создания таблицы коммутации IGMP Snooping

Таблица коммутации IGMP Snooping

Номер порта	Многоадресная группа	MAC-адрес многоадресной группы
1, 10, 25	239.192.1.10	01-00-5E-40-01-0A

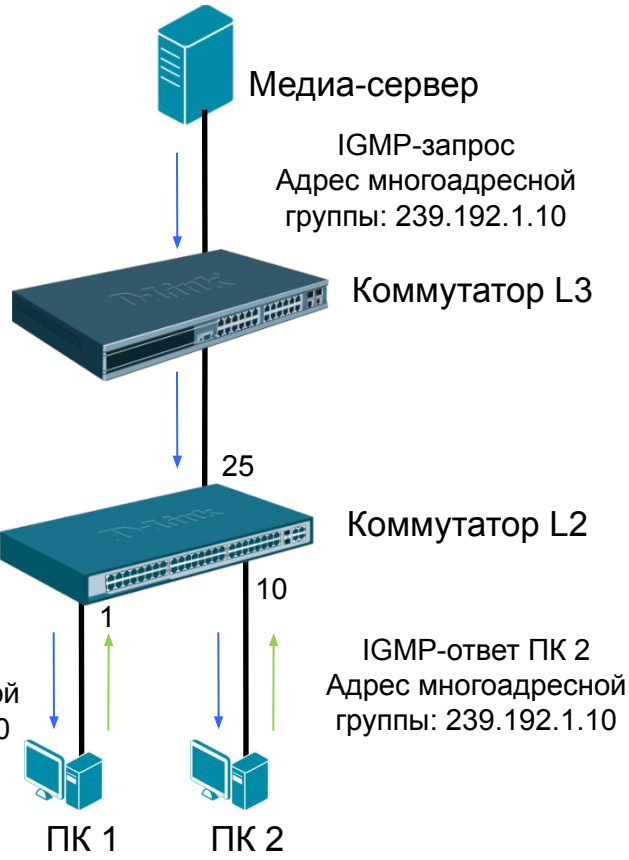
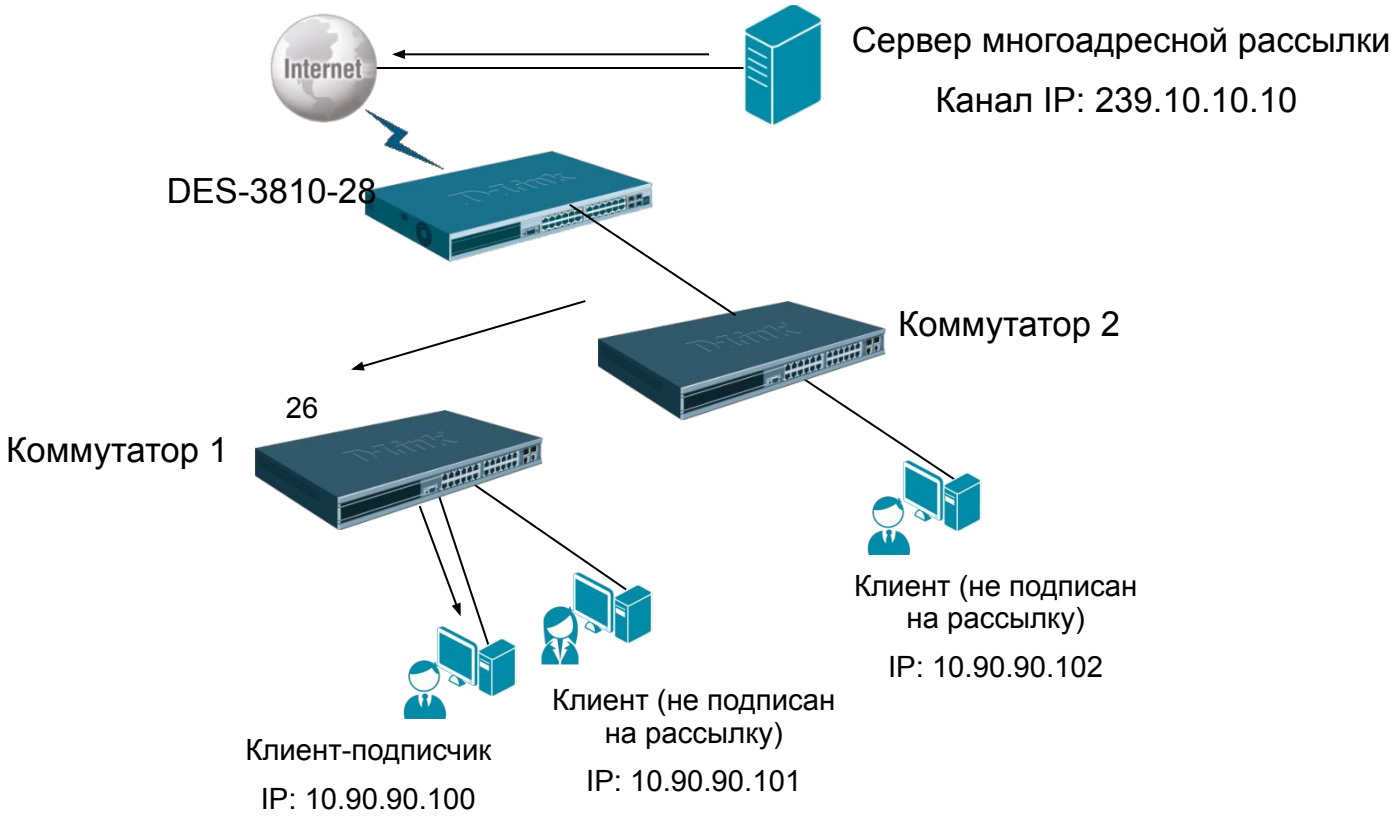


Рисунок анимирован

Многоадресная рассылка

Пример настройки IGMP Snooping



Многоадресная рассылка

Настройка коммутатора 1

//Активизировать функцию IGMP Snooping глобально на //коммутаторе

- `enable igmp_snooping`

//Активизировать функцию IGMP Snooping в указанной VLAN (в //данном примере VLAN по умолчанию)

- `config igmp_snooping vlan default state enable`

//Включить фильтрацию многоадресного трафика, чтобы //избежать его передачи узлам, не являющимся подписчиками //многоадресной рассылки

- `config multicast vlan_filtering_mode vlan default filter_unregistered_groups`

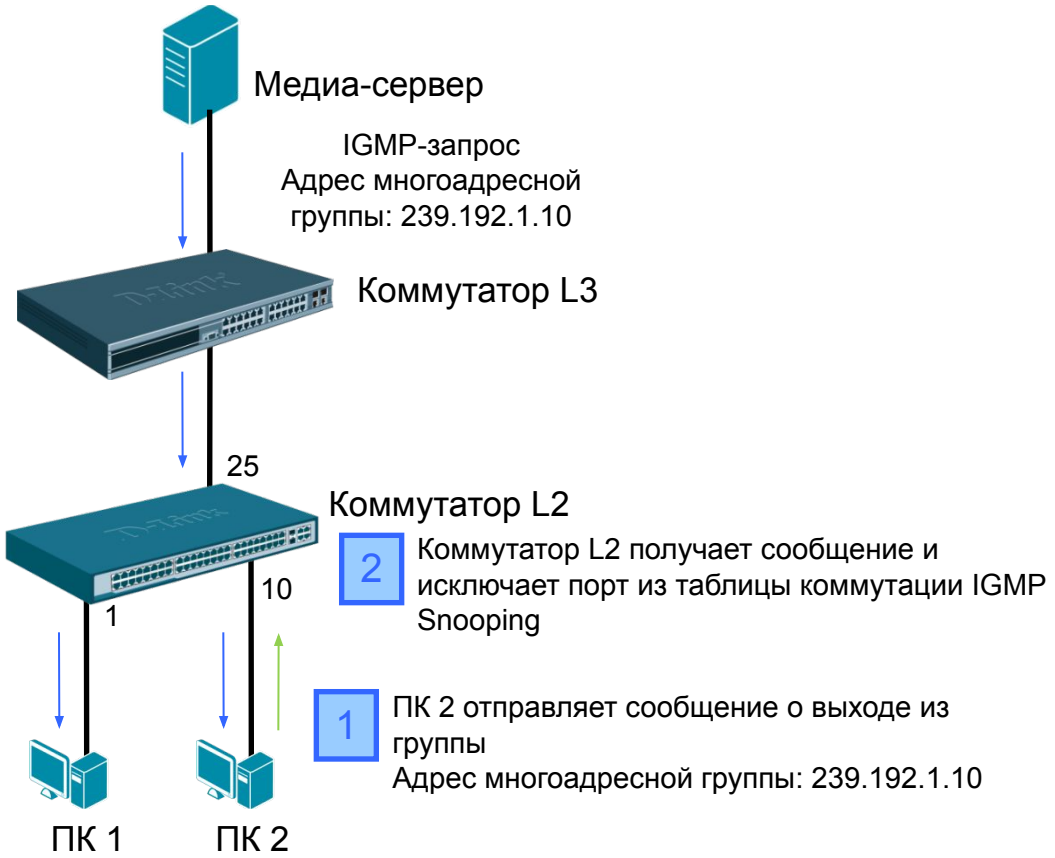
Многоадресная рассылка

Функция IGMP Snooping Fast Leave

- Функция IGMP Snooping Fast Leave, активизированная на коммутаторе, позволяет мгновенно исключить порт из таблицы коммутации IGMP Snooping при получении им сообщения о выходе из группы.
- Порт 25 будет удален из таблицы коммутации IGMP Snooping только в том случае, если к нему не будет подключен ни один узел-подписчик.

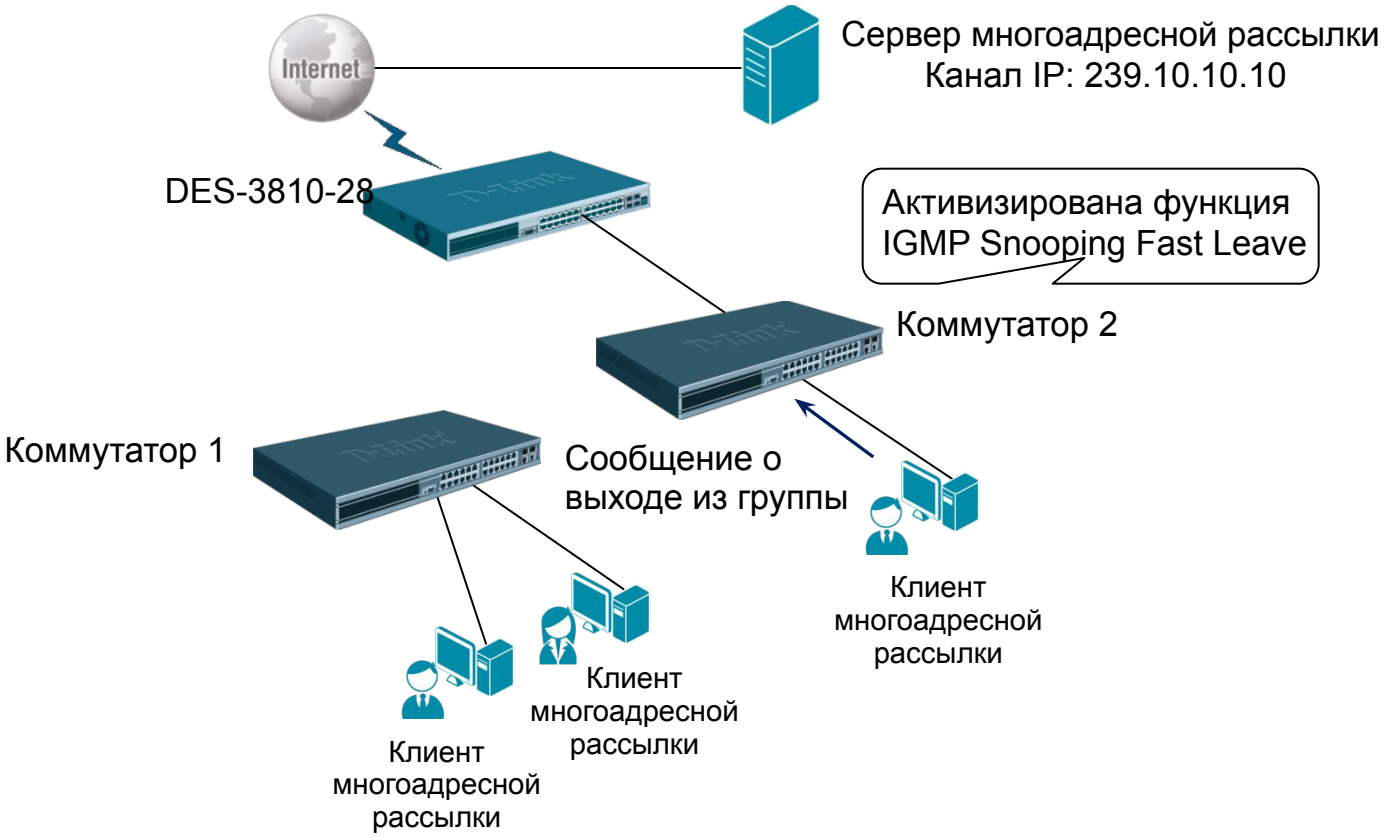
Таблица коммутации IGMP Snooping

Номер порта	Многоадресная группа	MAC-адрес многоадресной группы
1, 25	239.192.1.10	01-00-5E-40-01-0A



Многоадресная рассылка

Пример настройки IGMP Snooping Fast Leave



Многоадресная рассылка

Настройка коммутатора 2

//Активизировать функцию IGMP Snooping глобально на коммутаторе и //в указанной VLAN (в данном примере VLAN по умолчанию). Включить //фильтрацию многоадресного трафика.

- `enable igmp_snooping`
- `config igmp_snooping vlan default state enable`
- `config multicast vlan_filtering_mode vlan default filter_unregistered_groups`

//Активизировать функцию IGMP Snooping Fast Leave в указанной VLAN.

- `config igmp_snooping vlan default fast_leave enable`

Ваши вопросы…