

Коммутаторы серии ESP.
Описание функциональных возможностей.
Версия документа: 1.0

Аннотация

Настоящий документ предназначен для использования сетевыми администраторами, в процессе эксплуатации коммутаторов серии ESP. В настоящем документе описываются общие функциональные возможности коммутаторов серии ESP.

Оглавление

1.Поддержка резервированных топологий сети	4
2.Объединение портов.....	7
3.Работа с MAC-адресами, ограничение доступа.....	9
4.Работа с виртуальными сетями	10
5.Отражение трафика	13
6.Поддержка качества обслуживания (QoS)	14
7.Ограничение/фильтрация входного/выходного трафика.....	15
8.Дополнительные возможности	16
9.ACL. Списки управления доступом.	17

1 Поддержка резервированных топологий сети

Коммутатор серии ESP¹ поддерживает работу со следующими резервированными топологиями сети:

- Топологией, построенной на протоколе STP, позволяющей строить односвязную сеть на основе сети с произвольным подключением коммутаторов. Описание протокола STP приведено в документе “ANSI/IEEE Std 802.1D, 1998 Edition. Part 3: Media Access Control (MAC) Bridges”.
- Топологией типа “резервированное кольцо”. В этой топологии на каждом из коммутаторов задаются два порта, соединяемых с соответствующими портами кольца на других коммутаторах. Резервированное кольцо может быть построено только на одиночных портах (работа кольца на портах, объединённых в группу, невозможна). В процессе работы автоматически выбирается один коммутатор (root), который логически разрывает подключение на одном из своих портов, тем самым превращая топологию в линейную. Если в процессе работы произойдет отказ одной из линий связи или коммутатора, то root-коммутатор восстановит связь на отключенном порту, тем самым объединяя образовавшиеся после отказа два сегмента сети в один. Таким образом, использование топологии “резервированное кольцо” может компенсировать единичный отказ в системе.

Пример топологии сети “резервированное кольцо”, состоящей из шести коммутаторов, на примере коммутатора ESP-6UC, показан на рисунке 1.

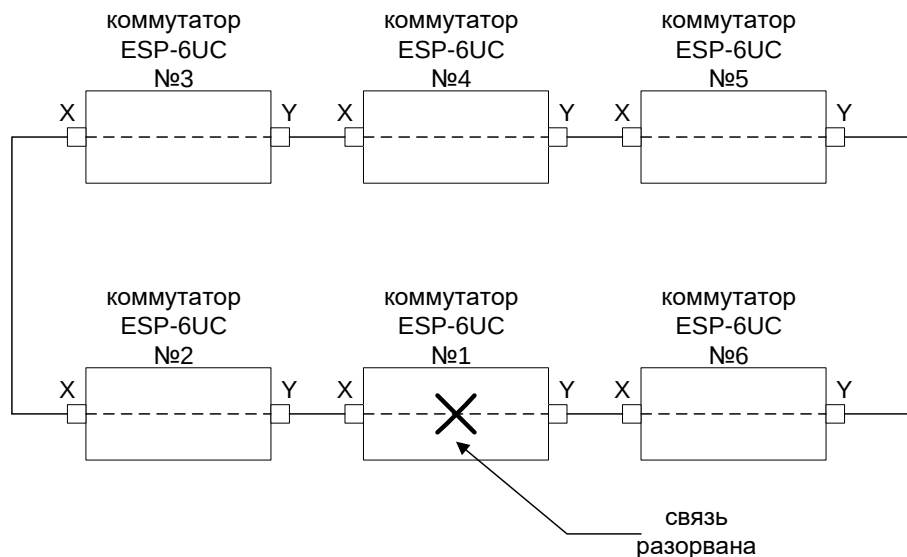


Рисунок 1 Топология сети “резервированное кольцо”

¹ Далее: коммутатор

Для соединения коммутаторов в сеть по топологии "резервированное кольцо" необходимо при конфигурировании каждого коммутатора:

- назначить два порта для связи с соседними коммутаторами (порты "X" и "Y" на рисунке 1);
- включить функцию поддержки топологии сети "резервированное кольцо";

После подачи питания, коммутаторы автоматически выбирают один root-коммутатор (root-коммутатором является коммутатор с наименьшим MAC-адресом, пусть на рисунке 1 это будет коммутатор №1), который отключает один из выбранных портов ("X" или "Y") от сети. Таким образом, физически топология "резервированное кольцо" представляет собой кольцо, а логически – шину. На root-коммутатор также возложены задачи по проверке целостности сети. Если в каком-либо месте между коммутаторами происходит разрыв соединения, то root-коммутатор, определив такую ситуацию, автоматически подключит свой второй порт к сети и восстановит целостность сети (см. рисунок 2). В случае изменения количества коммутаторов в сети, происходит запуск процедуры "перевыборы root-коммутатора". Во время работы этой процедуры коммутаторы, составляющие топологию "резервированное кольцо", не могут коммутировать Ethernet-кадры.

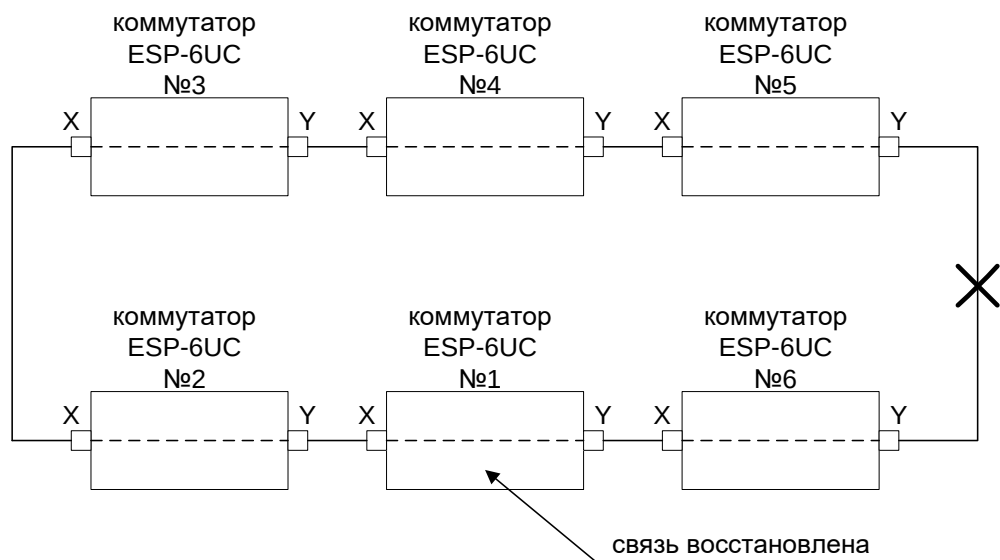


Рисунок 2 Пример восстановления сети при разрыве связи между коммутаторами №5 и №6.

Примечания:

1. Порты всех коммутаторов, назначенные для использования в топологии "резервированное кольцо" должны работать в режиме полного дуплекса.
2. Целостность резервированного кольца может быть нарушена:
 - штормом ARP запросов;

- штормом запросов DHCP (если включен режим получения IP адреса коммутатором через DHCP);
- чрезмерным количеством запросов на собственный MAC адрес коммутатора;
- штормом broadcast кадров;

Для предотвращения потери целостности резервированного кольца необходимо ограничить количество пакетов указанных типов. Рекомендуемая нагрузка – не более 100 пакетов каждого из перечисленных типов в секунду.

2 Объединение портов

Коммутатор поддерживает до 12 групп портов, в каждом из которых может быть до 8 портов. Все порты, входящие в группу, рассматриваются коммутатором как один виртуальный порт. Все порты, входящие в группу, должны иметь идентичные настройки (скорость, QoS, VLAN и т.д.).

Объединение портов используется для:

а) Увеличения пропускной способности (суммарная пропускная способность группы портов равна сумме пропускных способностей входящих в нее портов).

б) Увеличения надежности связи (выход из строя одной из связей приведет к автоматическому перераспределению трафика между остальными портами в группе).

Обычно группы портов используются для объединения друг с другом коммутаторов.

Номер порта в группе портов, по которому будет передан Ethernet-кадр, определяется в соответствии со следующим алгоритмом:

1. Определяется значение hash. Алгоритм определения значения hash приведен на рисунке 3).

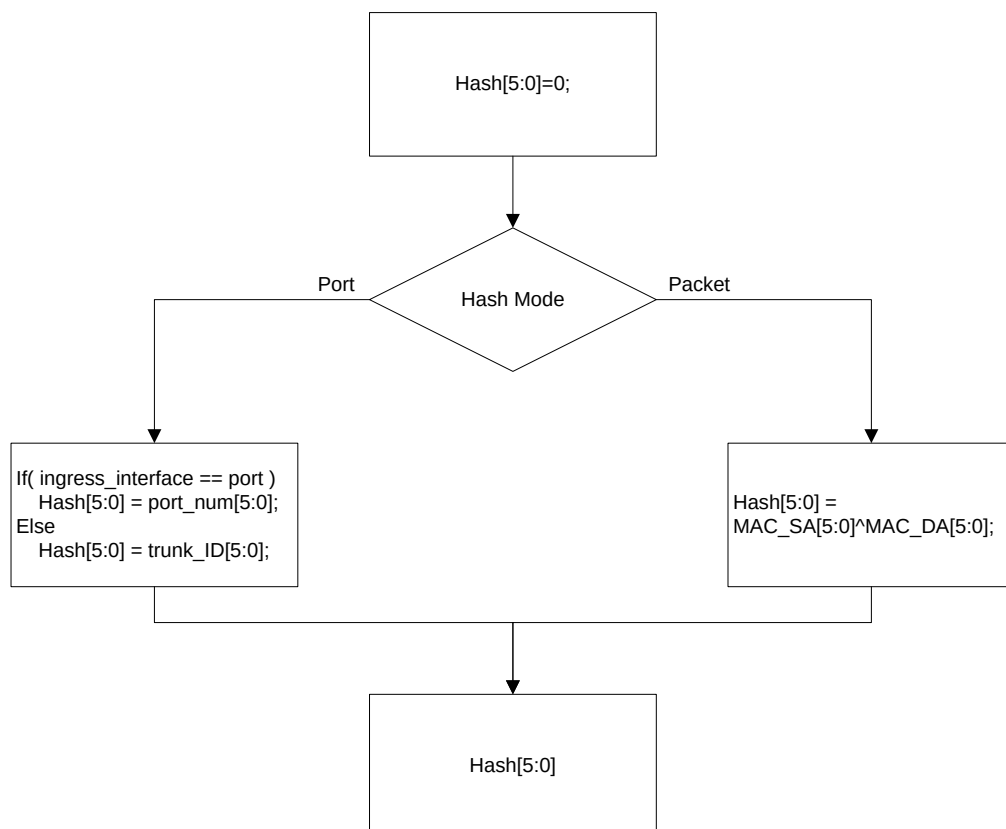


Рисунок 3. Алгоритм определения значения hash

Значение hash определяется в соответствии с заданным режимом Hash Mode (значение этого параметра задается командой CLI *config aggregation <balancing>* или через Web-интерфейс).

MAC_SA и **MAC_DA** – MAC адреса источника и приемника соответственно.

Параметр **ingress_interface** задает тип интерфейса, принявшего пакет (порт (port) или группа портов (trunk)).

Параметр **port_num** равен номеру порта, принявшего пакет, минус 1.

Параметр **trunk_ID** равен номеру группы портов (number_trunk). Значение number_trunk (1-12) задается при вызове команды *config trunk <number_trunk> enable <list_of_ports>*.

2. Для одноадресных пакетов определяется номер выходного порта в группе портов в виде остатка от деления: $\text{selected_trunk_member} = \text{hash} \% X$,
где X - количество портов в группе;
3. Для многоадресных и широковещательных пакетов номер выходного порта в группе портов определяется на основе 3-х младших битов значения hash.

Примечание:

При использовании групп портов для увеличения пропускной способности канала связи, необходимо иметь в виду, что нагрузка может распределяться между портами группы неравномерно. В этом случае возможна потеря пакетов, связанная с перегрузкой одного (или нескольких) портов группы. Для предотвращения разбалансированности при загрузке портов внутри одной группы необходимо в системе пользователя при **реальной** загрузке сети с помощью статистики портов определить их загрузку. В случае необходимости поменять способ балансировки нагрузки и провести анализ повторно.

3 Работа с MAC-адресами, ограничение доступа

Все MAC-адреса источников, изученные коммутатором в процессе работы, сохраняются в таблице MAC-адресов коммутатора. Для предотвращения переполнения этой таблицы введен механизм устаревания MAC-адресов. Т.е. если в течение некоторого времени коммутатор не получит пакетов с ранее изученным адресом источника, то данный адрес будет удален из таблицы. Реальное время, по истечении которого MAC-адрес будет удален из таблицы MAC-адресов, составляет от 6/7 до 1 от заданного времени. Задать время устаревания MAC-адресов можно с помощью WEB-интерфейса или CLI. По умолчанию установлено время устаревания равное 300 сек.

Коммутатор позволяет обучить на выбранных портах один или несколько (до 16) MAC-адресов статически. Статические MAC-адреса не устаревают и не удаляются из таблицы MAC-адресов никогда.

На каждом порту коммутатора может быть включен запрет на обучение MAC-адресов. При включении этого запрета все входящие пакеты, MAC-адрес которых не привязан к данному порту, будут отбрасываться. Эта возможность может быть использована совместно с запретом на обучение MAC-адресов для ограничения доступа к коммутатору.

В случае необходимости коммутатор позволяет изменить свой уникальный MAC-адрес. В каждой конфигурации может быть установлен свой MAC-адрес. Например, команда CLI «*show switch*» отображает текущий MAC-адрес коммутатора (current) и уникальный MAC-адрес, присвоенный коммутатору при изготовлении (global). При задании в конфигурации MAC-адреса 00:00:00:00:00:00 или выборе несуществующей конфигурации коммутатор будет использовать свой уникальный MAC-адрес (global).

По умолчанию управление коммутатором (редактирование конфигураций, запрос статистики и т.д.) возможны при подключении к любому из Ethernet портов. В случае необходимости можно запретить управление коммутатором с части портов.

Запрет управления коммутатором (с одного или нескольких портов) осуществляется принудительной фильтрацией (отбрасыванием) всех пакетов (см. примечание), идущих с указанных портов на порт управления (подключенный к процессору управления коммутатора).

Примечание:

Не подвергаются фильтрации следующие категории пакетов:

а) Многоадресные пакеты с адресом 01:80:C2:00:00:00 (если включена поддержка “резервированного кольца”);

б) Широковещательные пакеты DHCP (если установлен режим получения IP адреса коммутатором через механизм DHCP).

4 Работа с виртуальными сетями

Любой пакет, поступающий в коммутатор, может содержать полный тег VLAN (tagged), содержать тег VLAN со значением VLAN ID = 0 (priority tagged) и не содержать тега VLAN (untagged). Принадлежность каждого пакета к одному из этих классов определяется на основе анализа пакета (см. рисунок 4).

На рисунке 4 приведены: пакет без VALN тега (a, untagged), пакет с VLAN тегом (b, если VLAN ID = 0 – priority tagged, иначе – tagged) и структура VLAN тега (c).



Рисунок 4. Тегирование пакетов

Решение о продвижении пакета внутри коммутатора принимается на основе следующих правил:

- правила входящего трафика (ingress rules) – позволяют классифицировать получаемые пакеты относительно принадлежности к VLAN;
- правила продвижения между портами (forwarding rules) – позволяют принять решение о продвижении или отбрасывании пакета;
- правила исходящего трафика (egress rules) – позволяют определить - нужно или нет сохранять тег VLAN перед выдачей в порт.

Правила входящего трафика (ingress rules)

Выполняется анализ поступившего пакета и добавление (в случае необходимости) VLAN тега. Присвоение тега каждому входящему пакету производится в соответствии с алгоритмом, приведенным на рисунке 5.

Примечание: В коммутаторе все пакеты имеют тег.

Таким образом, всем пакетам без тега или тегированным пакетам с VLAN ID = 0, в качестве VLAN ID присваивается значение VID равное PVID порта принявшего кадр (Port VLAN ID). PVID задается индивидуально для каждого порта коммутатора. Также возможна принудительная замена VLAN ID для кадров с тегом на значение PVID.

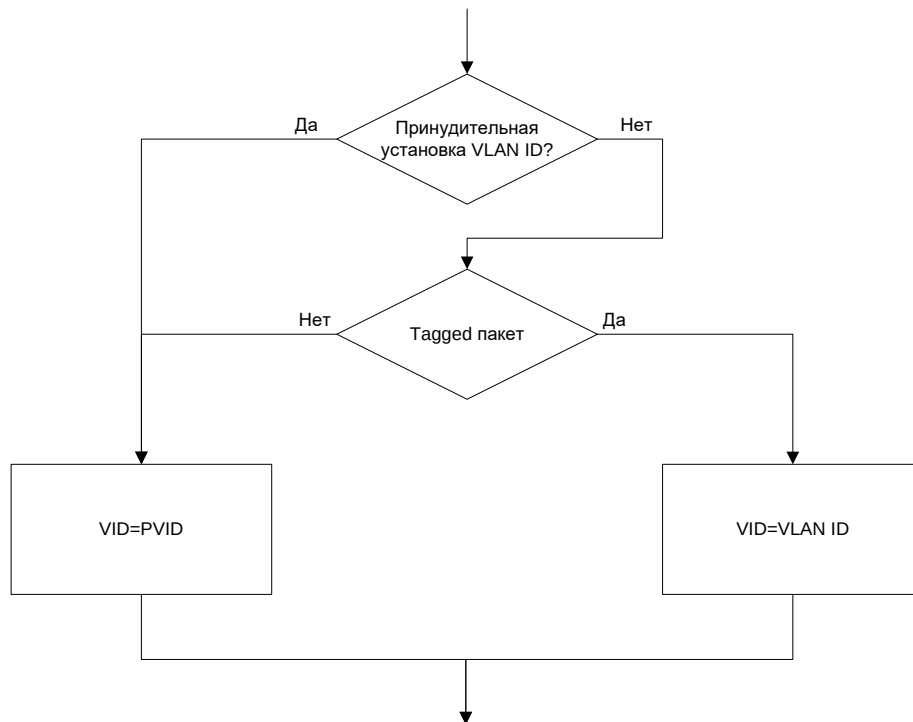


Рисунок 5. Алгоритм присвоения VLAN тега

Правила продвижения (forwarding rules)

Если входной кадр маркированный, то коммутатор определяет, является ли входной порт членом той же VLAN путем сравнения идентификатора VLAN ID в заголовке кадра и набора идентификаторов VLAN ID, ассоциированных с портом. Если нет, то такой пакет отбрасывается, иначе пакет передается дальше. Далее определяется, является ли порт назначения членом той же VLAN. Если нет, то пакет отбрасывается. В противном случае пакет передается в порт назначения.

Правила исходящего трафика (egress rules)

В зависимости от настроек пакет может быть выдан с тегом (tagged) или без (untagged). При добавлении в VLAN каждый порт может быть помечен как тегированный (выдает пакеты с тегом) или нет. Один и тот же порт в различных VLAN может быть помечен тегированный для одних VLAN и не тегированный для других.

5 Отражение трафика

Коммутатор позволяет настраивать отражение входного и/или выходного трафика одного порта в другой. Возможно одновременное отражение входного и выходного трафика порта. Данный режим может использоваться для контроля передаваемого абоненту трафика (например, с целью отладки).

6 Поддержка качества обслуживания (QoS)

Коммутатор позволяет производить широкие настройки приоритетов и качества обслуживания входящих пакетов на основе профилей качества обслуживания. Алгоритм выбора профиля качества обслуживания для входящего трафика показан на рисунке 6.

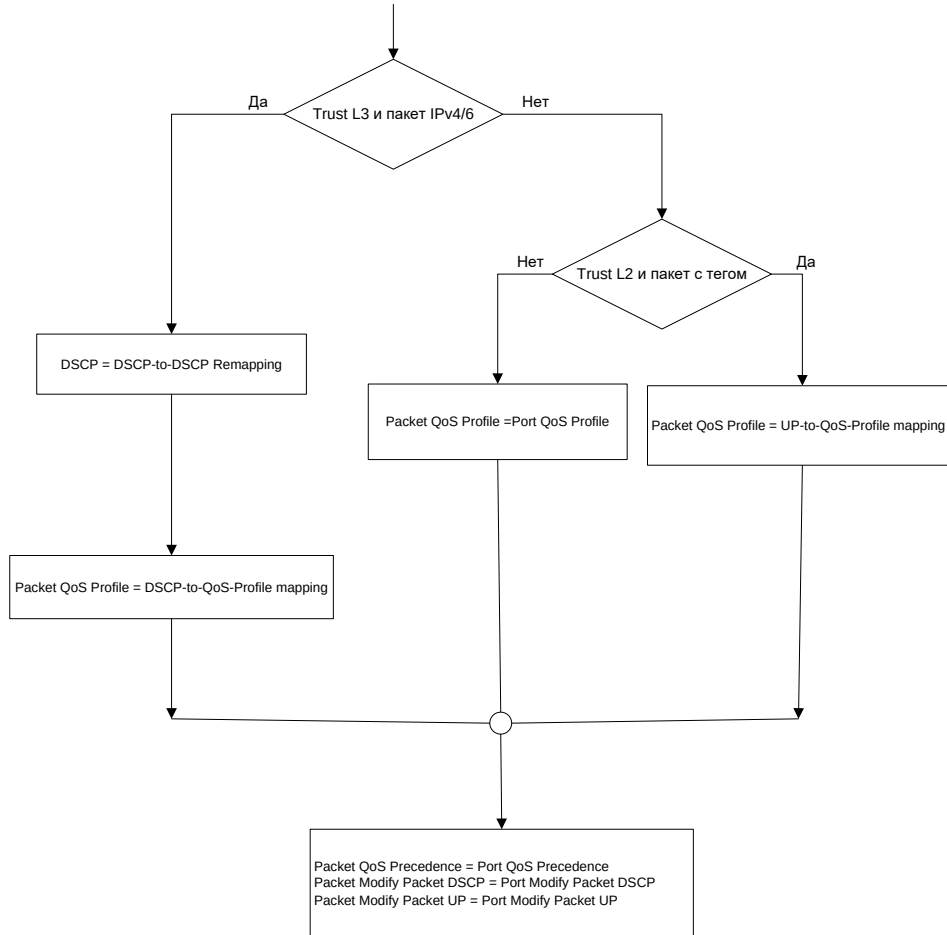


Рисунок 6. Алгоритм выбора профиля качества обслуживания для входящего трафика

Примечание:

Коммутатор поддерживает три режима QoS: L2, L3, L2L3. В таблице 1 приведены значения флагов Trust L2 и Trust L3 (эти флаги используются в алгоритме на рисунке 6) в зависимости от выбранного режима QoS.

Таблица 1. Значения флагов Trust L2 и Trust L3 в разных режимах QoS

Режим QoS	Trust L2	Trust L3
untrusted	0	0
L2	1	0
L3	0	1
L2L3	1	1

7 Ограничение/фильтрация входного/выходного трафика

Коммутатор позволяет настраивать фильтрацию (принудительный отброс) выходного многоадресного и/или затопляющего (одноадресный с неизвестным адресом назначения) трафика на каждом из портов.

Коммутатор позволяет задавать ограничение для одного или нескольких типов входного трафика (одноадресного, многоадресного, широковещательного, затопляющего) для каждого из портов. При превышении объема входного трафика над указанным значением, в течение временного окна, лишние пакеты начнут отбрасываться. Для задания степени ограничения необходимо установить размер временного окна (в мкс) для всех скоростей обмена (10/100/1000Мбит) и для каждого порта - максимальное количество пакетов (0-4194240, шаг 64) в этом временном окне.

8 Дополнительные возможности

Коммутатор позволяет выдавать стандартные сообщения snmp trap (при включении, при изменении состояния порта). Для их передачи необходимо задать IP-адрес узла сети, принимающего данные от коммутатора.

Коммутатор позволяет выдавать сообщения на сервер syslog. Сообщения выдаются при наступлении определенных событий (включение коммутатора, изменение состояния портов, авторизация и т.д.). Выдаваемые сообщения делятся на несколько групп в зависимости от их важности. При настройке можно указать сообщения, каких групп следует выдавать, а каких отбрасывать (например, для снижения нагрузки на сервер syslog). Коммутатор позволяет настраивать до 4-х различных адресов серверов syslog.

9 ACL. Списки управления доступом.

ACL – последовательный набор правил, разрешающих или запрещающих прохождение пакета.

Коммутатор последовательно проверяет каждый входящий пакет на соответствие правилам. Правила проверяются в порядке увеличения номера правила (идентификатора профиля).

После первого же совпадения принимается решение о разрешении коммутации или об отбрасывании пакета, и дальше правила не обрабатываются.

Если ни одно из правил не подошло, то пакет коммутируется как обычно.

Проверка правил ACL осуществляется на аппаратном уровне без потерь производительности.

Правила ACL могут фильтровать пакеты, основываясь на информации разных уровней (см. Таблицу 2). Вся информация, получаемая из пакетов, может быть закрыта маской для удобства формирования правил - общих для различных пакетов. Правилами будут анализироваться только те биты информации пакета, для которых значение бита маски равно 1.

Правила ACL могут быть сконфигурированы как для работы с одним портом, так и со всеми портами коммутатора сразу.

Таблица 2. Информация пакета, используемая ACL.

Информация пакета \ Тип ACL	Ethernet	IP
Идентификатор VLAN	+	+
MAC адрес источника	+	+
MAC адрес приемника	+	+
Приоритет IEEE 802.1p	+	+
Тип пакета Ethernet	+	- (всегда 0x800)
IP адрес источника	-	+
IP адрес приемника	-	+
IP протокол	-	+
Порт источника	-	+
Порт приемника	-	+
Содержимое пакета в пределах первых 128 байт	до 6 байт, общих для всех правил	до 6 байт, общих для всех правил

Настройка правил ACL.

1. На основе требований к задаче фильтрации выберите тип правила: Ethernet или IP.
2. Выберите поля пакета необходимые для реализации задачи фильтрации и маски для них.
3. Выберите действие для правила (пропустить пакет/отбросить пакет).
4. Выберите порт/порты для правила.
5. Выберите значение идентификатора профиля для создаваемых правил.
6. Создайте правило фильтрации.

Для реализации некоторых правил может быть необходимо (или выгоднее) создать несколько правил. Например, если необходимо разрешить прохождение пакетов через порты 1-3, и запретить прохождение через все остальные, то можно создать по одному правилу разрешающему правилу для портов 1-3 и одно запрещающее правило для всех портов (со значением идентификатора большим, чем у разрешающих правил). В таком случае разрешающие правила будут просмотрены коммутатором первыми.

Пример 1. Запрет доступа к компьютеру по MAC-адресу с части портов

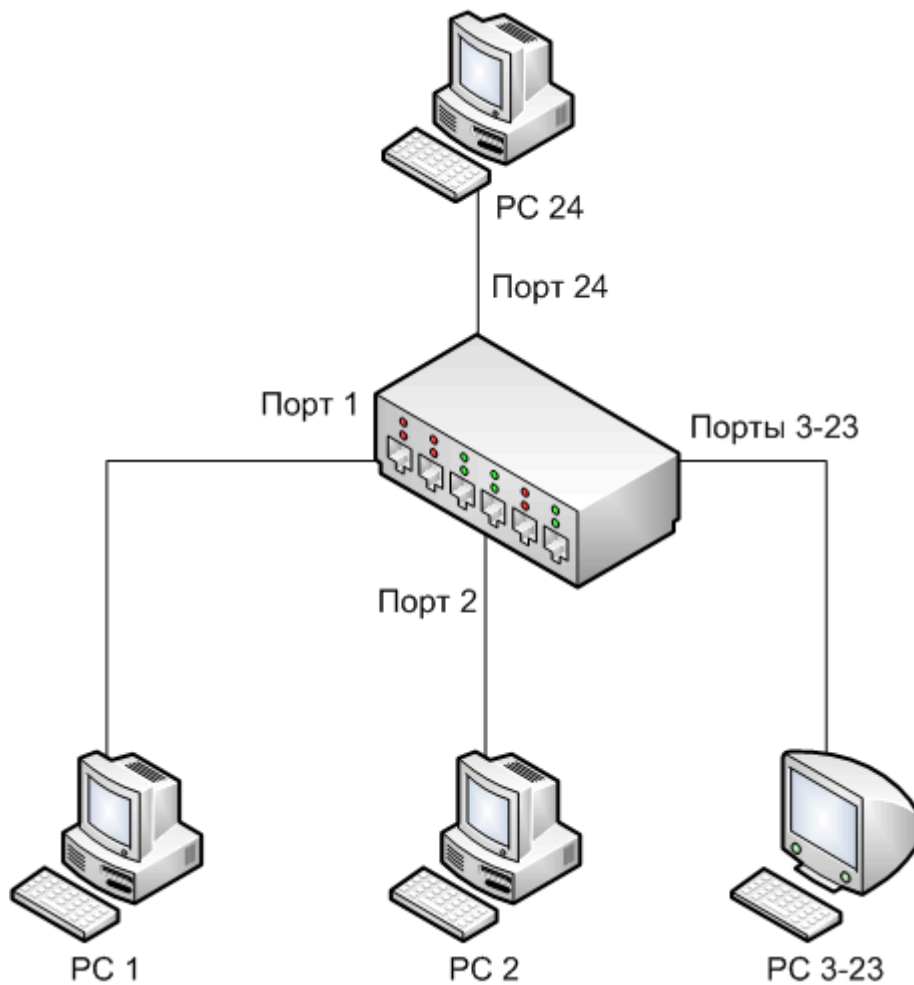
Необходимо:

С портов 1 (PC 1) и 2 (PC 2) разрешить доступ к компьютеру PC 24, подключенному к порту 24. С других портов доступ к PC 24 запретить.

MAC адрес PC 24 - 00:25:22:AE:0E:24.

Правила:

1. Если MAC адрес назначения равен MAC адресу PC24 и порт 1 или 2, то разрешить.
2. В противном случае запретить.



Формирование правил:

1. Т.к. используется только MAC адрес приемника, то можно использовать Ethernet ACL.
2. Для фильтрации используется MAC адрес 00:25:22:AE:0E:24 с маской FF:FF:FF:FF:FF:FF.
3. Необходимо создать 3 правила, для портов 1 и 2 – разрешающие коммутацию и для всех портов – отбрасывающее пакеты.
4. Для корректной работы два первых правила должны иметь идентификаторы меньшие, чем третье. Поэтому пусть у первого правила будет id 100, у второго 101 а у третьего 102.

5. Создаем правила:

```
create access_profile profile_id 100 ethernet destination_mac 0:25:22:ae:e:24 mask ff:ff:ff:ff:ff:ff
port 1 permit
create access_profile profile_id 101 ethernet destination_mac 0:25:22:ae:e:24 mask ff:ff:ff:ff:ff:ff
port 2 permit
create access_profile profile_id 102 ethernet destination_mac 0:25:22:ae:e:24 mask ff:ff:ff:ff:ff:ff
port all deny
```

Пример 2. Разрешение передачи IP кадров только одной подсети

Необходимо:

Разрешить передачу кадров с IP адресами источника и IP адресами приемника в подсети 192.168.0.0/24.

Правила:

1. Если IP адреса источника и приемника лежат в подсети 192.168.0.0/24, то разрешить.
2. В противном случае запретить.

Формирование правил:

1. Т.к. используются IP адреса, то используем IP ACL (и Ethernet ACL для запрещающего правила).
2. Для фильтрации используется IP адрес 192.168.0.0 с маской 255:255:255:00.
3. Создаются два правила для всех портов. Первое правило – разрешающее коммутацию для заданной подсети и второе – отбрасывающее все кадры.
4. Пусть id первого правила будет 200, id второго должно быть больше (201).
5. Создаем правила:

```
create access_profile profile_id 200 ip source_ip 192.168.0.0 mask 255.255.255.0 destination_ip 192.168.0.0 mask 255.255.255.0 port all permit
```

```
create access_profile profile_id 201 ethernet ethernet_type 0x800 mask 0xffff port all deny
```

Пример 3. Запрет приема ICMP Request на порту 1

Необходимо:

Запретить прием ICMP Request на порту 1.

Правила:

1. Если приходит ICMP запрос на порт 1, то отбросить.
2. В противном случае разрешить.

Формирование правил:

1. Т.к. используются ICMP протокол, то используем IP ACL.
2. Для фильтрации используется: IP протокол (равен 1 – icmp), байт 20 заголовка L3 (равен 8 – request).
3. Создается одно правило для порта 1. Действие – отбрасывать кадры.
4. Пусть id правила будет 150.
5. Создаем правило:

```
config access_profile offset1 l3 20
```

```
create access_profile profile_id 150 ip protocol_ip 1 mask 0xff offset1 0x8 mask 0xff port 1 deny
```