Коммутатор (MAC Switch)

Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

Пройти сертификационный экзамен

Настройка коммутатора

Настройка коммутатора заключается в настройке набора правил для групп коммутации:

- Уникальный номер группы коммутатора (1-4999) для каждой группы
- Интерфейсы, включенные в данную группу коммутации и правила, регулирующие направление определенного трафика в определенную группу коммутации
- На каждом узле можно настроить несколько групп коммутации. Каждый интерфейс устройства можно включить в несколько групп коммутации одновременно
- Группы коммутации назначаются на разных узлах сети MINT. Узлы, на которых настроены одинаковые группы коммутации, составляют «зону коммутации»
- «Зона коммутации» существует только внутри данного сегмента сети MINT.

Группы коммутации

Сеть MINT можно рассматривать как один виртуальный распределенный L2-коммутатор, где границы узлов действуют как внешние порты этого виртуального коммутатора. Задача коммутатора – транспортировка кадров из одного порта в другой. Важно понимать, что группы коммутации следует создавать только на тех узлах, где кадры приходят или уходят во внешнюю сеть относительно MINT. На узлах в режиме повторителя не требуется создавать группы коммутации.

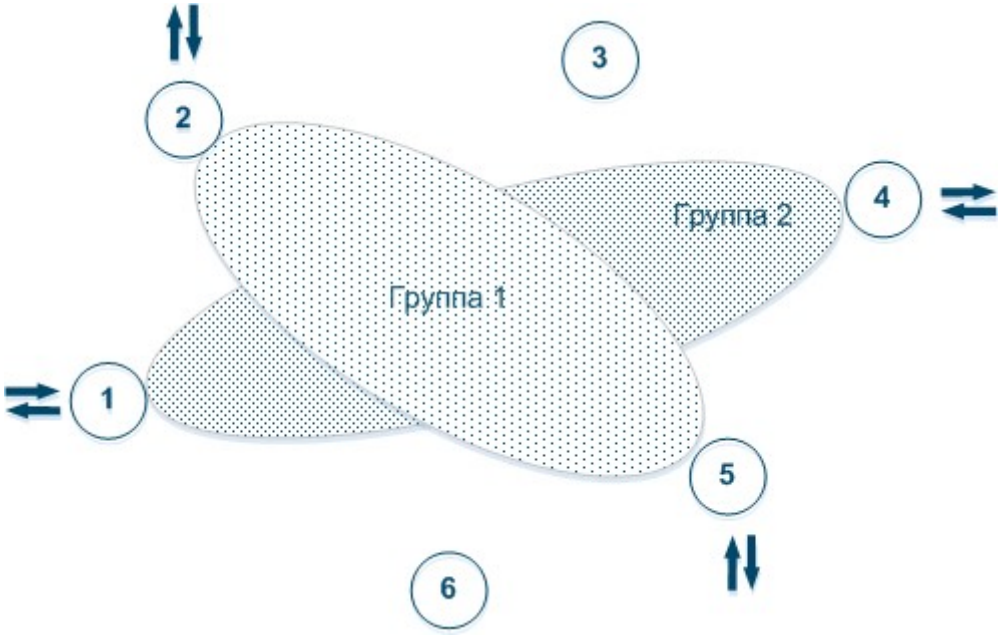


Рисунок – Группы коммутации

Для направления входящего кадра в одну из групп коммутации, используются гибкие правила, позволяющие сортировать кадры в соответствии с различными критериями, такими как:

- Порты
- Метки VLAN
- Любые PCAP-выражения
- Адреса (MAC/IP)
- Тип протокола.

Транковые группы

Транковая группа – это группа коммутации, работающая в режиме "*trunk*".

Входящий поток из проводного сегмента, предназначенный такой группе, разделяется по отдельным подгруппам (входящим в транк группам коммутации) в зависимости от метки VLAN каждого пакета. При этом номер каждой группы коммутации в транке будет соответствовать номеру VLAN коммутируемых в неё пакетов. Использование транковых групп облегчает процесс настройки коммутатора в случаях, когда нужно обеспечить передачу VLAN-потоков нескольким абонентам.

Если на базовой станции включается Транковая группа, которая будет обеспечивать передачу нескольких VLAN потоков по разным направлениям, то на абонентских терминалах следует использовать опцию "*in-trunk*" для явного указания, в состав какой транковой группы входит данная Группа коммутации.

При отправке данных через проводной коммутатор, номер группы автоматически преобразовывается в метку VLAN стандарта 802.1q и, наоборот, при получении пакета через проводной коммутатор метка VLAN преобразовывается в соответствующий номер группы.

Транковые группы могут использоваться для соединения нескольких сегментов VLAN.

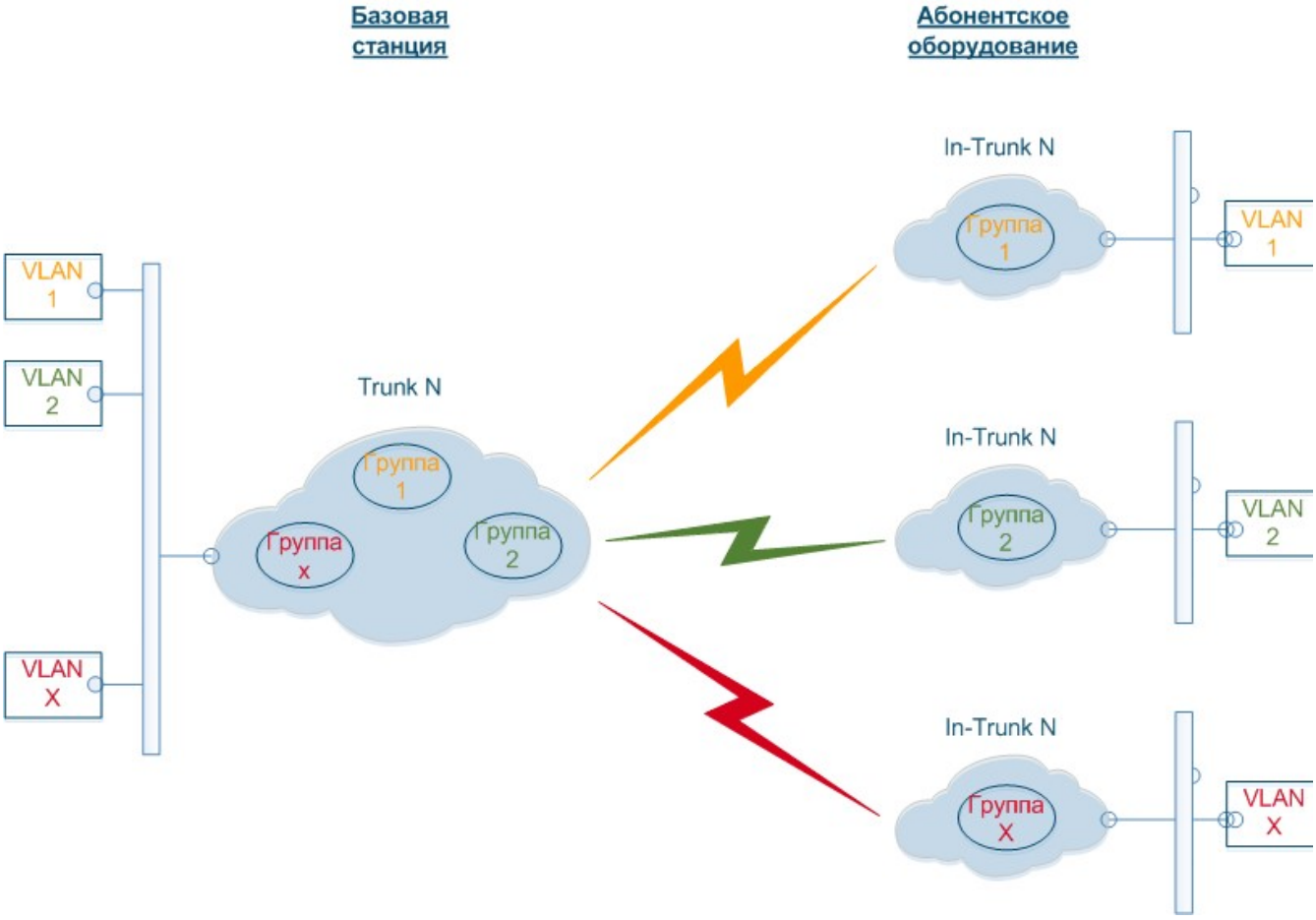


Рисунок – Транковые группы

Специальные правила для интерфейсов позволяют гибко управлять метками VLAN: удалять, назначать, менять (подробнее см. Руководство ОС WANFleX).

Настройка управления устройством

Для целей управления необходимо создать специальную Группу коммутации, общую для всех устройств в сети MINT и привязать её к интерфейсу SVI.

SVI представляет собой L3-интерфейс Группы коммутации. Он обеспечивает обработку на канальном уровне (L3) пакетов, входящих или выходящих через все порты, связанные с данной Группой коммутации.

Назначьте IP-адреса прямо на интерфейс SVI для непосредственного управления. Все пакеты, отправляемые через интерфейс SVI, будут распределяться только внутри соответствующей ему Группы коммутации.

Универсальный способ настройки VLAN управления через специальную Группу управления - назначить нужный IP-адрес интерфейсу SVI M, который является управляющим интерфейсом Группы M, в которую включены интерфейсы VLAN X (с родительским интерфейсом "*eth0")* и "*rf5.0*": (Подробнее см. раздел "Удаленное управление устройствами R5000"):

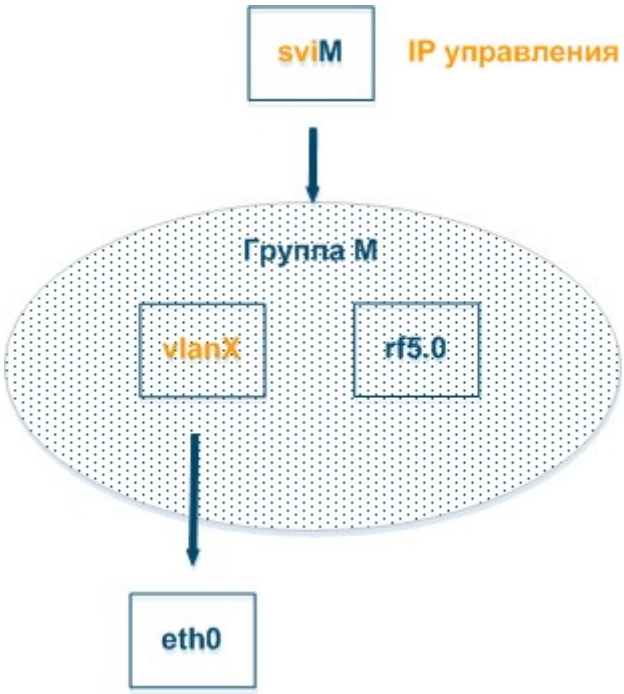


Рисунок – Настройка управления

Правила групп коммутации

Кадр, предназначенный одной из групп коммутации, не выйдет из этой группы, пока не достигнет одного из внешних портов. Правила групп коммутации применяются только тогда, когда кадр приходит в сеть MINT через один из внешних портов. Чтобы покинуть сеть, кадру не требуется никаких правил, т.к. он уже принадлежит одной из групп коммутации и автоматически перенаправляется на внешний порт (или порты), который принадлежит этой группе коммутации.

> **ВНИМАНИЕ**
>
> Кадры, созданные узлами сети "*mint*" (например, *RIP/OSPF, PING* и т.д.), не принадлежат никакой группе коммутации, а значит, не могут покинуть сеть MINT путем коммутации через внешний порт.

Правила используются для следующих целей:

- Выбор подходящей группы коммутации, если пакет получен через интерфейс "*ethX*". Пакет коммутируется только той группой, правилам которой он полностью соответствует.

> **ПРЕДОСТЕРЕЖЕНИЕ**
>
> Пакет, который не принадлежит ни с одной из групп коммутации, не коммутируется устройством и может быть уничтожен.

- Если пакет назначен группе коммутации, группа решает, пересылать ли пакет через один из интерфейсов или отбросить его. Пакет будет переслан, только если удовлетворяет правилам интерфейса

Правила состоят из условий и решений (разрешение/отказ). Анализируя список правил, коммутатор проверяет, соответствует ли пакет условию текущего правила. Если соответствует, то к нему применяется действие, соответствующее текущему правилу. Если нет, список правил просматривается дальше. Может быть применено только одно из правил. Если пакет не удовлетворяет ни одному из условий, к нему применяется действие, заданное по умолчанию для данной группы или интерфейса.

Условие определяет, какие пакеты будут соответствовать данной группе. Только пакеты, для которых условие является ИСТИНОЙ, будут соотнесены с данной группой. Условие может состоять из одного или нескольких примитивов. Примитивы обычно состоят из ID (номера группы или имени интерфейса) и одного или более классификатора.

Примеры правил фильтрации пакетов:

Одна IP-подсеть:

```
net 192.168.1.0/24
```

Несколько IP-подсетей:

```
net 192.168.1.0/24 or net 192.168.100.0/24
```

Несколько IP-подсетей с исключениями:

```
net 192.168.1.0/16 and not net (192.168.100.0/24 or 192.168.200.0/24)
```

Несколько IP-подсетей внутри VLAN:

```
vlan 50 and (net 192.168.1.0/24 or net 192.168.100.0/24)
```

Трафик PPPoE:

```
pppoed or pppoes
```

или (синонимично):

```
ether proto 0x8863 or ether proto 0x8864
```

Запретить передачу на групповые и широковещательные IP-адреса:

```
not ip multicast
```

Подробное описание синтаксиса правил фильтрации

Правило фильтрации определяет, какие пакеты выбираются фильтром для дальнейшей обработки. Если нет ни одного фильтра, выбираются все пакеты. Во всех других случаях, будут выбраны только пакеты, для которых выражение является ИСТИНОЙ.

Существует три вида классификаторов:

Классификатор	Описание
type	• Классификаторы сообщают, к какому ID (номеру группы или имени интерфейса) относятся фильтры • Возможные типы: *host, net, port, portrange* • Например: “*host foo*”, “*net 128.3*”, “*port 20*”, “*portrange 6000-6008*” • Если классификатор "*type*" не указан, то подразумевается "*host*"

dir	• Классификаторы уточняют определенное направление передачи к и/или от ID • Возможные направления: *src, dst, src* или *dst* и *src* и *dst* • Например: “*src 1.1.1.1*”, “*dst net 128.3*”, “*src or dst port 21*”. • Если классификатор "*dir"* не указан, то подразумевается "*src"* или "*dst"*

proto	• Классификаторы ограничивают по признаку соответствия определенному протоколу
	• Возможные протоколы: *ether, ip, ip6, arp, rarp, tcp* и *udp*
	  • Например: “*ether src 00:12:13:14:15:16*”, “*arp net 128.3*”, “*tcp port 21*”, “*udp portrange 7000-7009*”
	• Если классификатор "*proto"* не указан, то подразумеваются все протоколы, соответствующие типу
	  • Например: “*src 1.1.1.1*” значит “*(ip or arp or rarp) src foo*” (если последнее разрешено синтаксисом), “*net 1.2.3.0/24*” значит “*(ip or arp or rarp) net 1.2.3.0/24*” и “*port 53*” значит “*(tcp or udp) port 53*”

Таблица - Классификаторы

Кроме того, существует несколько специальных «примитивных» ключевых слов, которые не соответствуют шаблонам: *broadcast, greater, less, арифметические выражения*. Они описаны ниже.

Сложные выражения фильтрации строятся с использованием слов and, or и not для соединения примитивов. Например, “*host foo and not port ftp and not port ftp-data*”. Для экономии времени, одинаковые классификаторы могут быть пропущены. Например, “*tcp dst port ftp or ftp-data or domain*” эквивалентно “*tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain*”.

Применимые примитивы:

Примитив	Описание
dst host *host*	• ИСТИНА, если IPv4-поле назначения пакета "*host"*, что может быть как адресом, так и именем
src host *host*	• ИСТИНА, если IPv4-поле источника пакета "*host"*
host *host*	• ИСТИНА, если IPv4-поле источника или назначения пакета "*host"* • Любое из описанных выражений с "*host"* может иметь в качестве префикса ключевые слова *ip, ip6, arp, rarp*. Например: “ip host host”, что эквивалентно “ether proto \ip and host *host*”
ether dst *ehost*	• ИСТИНА, если Ethernet-адрес назначения "*ehost"* • *"Ehost"* должен иметь числовой формат: XX:XX:XX:XX:XX:XX
ether src *ehost*	• ИСТИНА, если Ethernet-адрес источника "*ehost"*
ether host *ehost*	• ИСТИНА, если Ethernet-адрес источника или назначения "*ehost"*
dst net *net*	• ИСТИНА, если IPv4-адрес назначения пакета имеет номер сети *net*
src net *net*	• ИСТИНА, если IPv4-адрес источника пакета имеет номер сети "*net"*
net *net*	• ИСТИНА, если IPv4-адрес источника или назначения пакета имеет номер сети "*net"*
net *net* **mask** *n etmask*	• ИСТИНА, если IPv4-адрес соответствует сети с определенной сетевой маской *"netmask".* • Может быть уточнен с помощью "*src"* или "*dst"*

net *net/len*	• ИСТИНА, если IPv4-адрес соответствует сети с *len* – битной сетевой маской. • Может быть уточнен с помощью "*src"* или "*dst"*
dst port *port*	• ИСТИНА, если пакет "*ip/tcp"*, "*ip/udp"* и имеет значение порта назначения "*port".*
src port *port*	• ИСТИНА, если значение порта источника "*port".*
port *port*	• ИСТИНА, если значение порта источника или порта назначения пакета *port.*
dst portrange *port1-port2*	• ИСТИНА, если пакет "*ip/tcp"*, "*ip/udp"* и имеет значение порта назначения между *port1* и *port2* • *"port1"* и "*port2"* интерпретируются аналогично параметру "*port"*
src portrange *port1-port2*	• ИСТИНА, если пакет имеет значение порта источника между "*port1"* и "*port2"*
portrange *port1-port2*	• ИСТИНА, если значение порта источника или порта назначения пакета между "*port1"* и "*port2"* • Любое из описанных выражений с "*port"* или "*portrange"* может иметь в качестве префикса ключевые слова "*tcp"* или "*udp"*. Например: "*tcp src port port*", что означает «только tcp пакеты с портом источника *port*»
less *length*	• ИСТИНА, если длина пакета меньше или равна "*length"* • Эквивалентно выражению: "*len <= length*"
greater *length*	• ИСТИНА, если длина пакета больше или равна "*length"* • Эквивалентно выражению: "*len >= length*"
ip proto *protocol*	• ИСТИНА, если пакет является пакетом IPv4 с типом протокола "*protocol"* • *"Protocol"* может быть номером или одним из следующих имен *icmp, icmp6, igmp, igrp, pim, ah, esp, vrrp, udp,* или *tcp* • Идентификаторы "*tcp"*, "*udp"* и "*icmp"* также являются ключевыми словами и должны отделяться обратной косой чертой \, что соответствует \\ в C-shell • Этот примитив не отслеживает последовательности заголовков протоколов
ip protochain *protocol*	• ИСТИНА, если пакет является пакетом IPv4 и содержит заголовки протокола с типом "*protocol* в последовательности заголовков протоколов • Например, "*ip protochain 6*" соответствует любому пакету IPv4 с заголовком протокола TCP в последовательности заголовков протоколов • Пакет может содержать между заголовком IPv4 и заголовком TCP, например, заголовок аутентификации, заголовок маршрутизации или заголовок "*hop-by-hop option"* • Код, генерируемый этим примитивом, сложен и не может быть оптимизирован, что может замедлять работу
ether broadcast	• ИСТИНА, если пакет является широковещательным Ethernet-пакетом • Ключевое слово "*ether"* не является обязательным
ether multicast	• ИСТИНА, если пакет является многоадресным (или широковещательным) Ethernet-пакетом • Ключевое слово "*ether"* не является обязательным • Эквивалентно выражению "*ether[0] & 1 != 0*"

ip multicast	• ИСТИНА, если пакет является многоадресным (или широковещательным) пакетом IPv4

ether proto *protocol*	• ИСТИНА, если значение поля "*ether type*" пакета "*protocol*"
	• *Protocol* может быть номером или одним из следующих имен *ip, ip6 ,arp, rarp, atalk, aarp, sca, lat, mopdl, moprc, iso, stp, ipx,* или *netbeui*
	• Эти идентификаторы также являются ключевыми словами и должны отделяться обратной косой чертой \
	• В Ethernet **OC WANFleX** проверяет поле ether type для большинства из этих протоколов. Исключения:
	  • *iso, stp, и netbeui*
	OC WANFleX проверяет на наличие кадров 802.3, а затем проверяет заголовок LLC так же, как для FDDI, Token Ring и 802.11
	  • *atalk*
	OC WANFleX проверяет на наличие "AppleTalk etype" в кадре Ethernet и на наличие пакетов формата SNAP так же, как для FDDI, Token Ring и 802.11
	  • *aarp*
	OC WANFleX проверяет на наличие "AppleTalk ARP etype" в кадре Ethernet или 802.2 SNAP кадра с уникальным идентификатором (OUI) 0x000000
	  • *ipx*
	OC WANFleX проверяет на наличие "IPX etype" в кадре Ethernet, IPX DSAP в заголовке LLC, 802.3-with-no-LLC-header инкапсуляции IPX и IPX etype в кадре SNAP

ip, **arp**, **rarp**, **atalk**, **aarp**, **iso**, **stp**, **ipx**, **netbeui**	• Сокращенные варианты **ether proto p**, где **p** - один из вышеупомянутых протоколов
svlan *[vlan_id]*	• ИСТИНА, если пакет является пакетом IEEE 802.1Q Service VLAN (ether proto 0x88a8)
vlan *[vlan_id]*	• ИСТИНА, если пакет является пакетом IEEE 802.1Q VLAN (ether proto 0x8100) • Если "*[vlan_id]*" указан, ИСТИНА, только если пакет имеет указанный "*vlan_id*" • Первое ключевое слово "*vlan*" или "*svlan*", встретившееся в *выражении* изменяет расчет смещения полей для оставшейся части *выражения,* исходя из того, что это VLAN пакет • Выражение "*vlan*" "*[vlan_id]*" может использоваться более одного раза, для фильтрации по иерархии VLAN • Каждое использование этого выражения увеличивает смещение фильтра на 4 • Например: "*svlan 100 && vlan 200*" фильтрует по VLAN 200, инкапсулированному в Service VLAN 100, а "*vlan 300 && ip*" фильтрует протоколы IPv4, инкапсулированные в VLAN 300, а "*svlan 100*" фильтрует все пакеты, инкапсулированные в Service VLAN 100
mpls *[label_num]*	• ИСТИНА, если пакет является пакетом MPLS • Если "*[label_num]*" указан, ИСТИНА, только если пакет имеет указанный *"label_num"* • Первое ключевое слово "*mpls*", встретившееся в *выражении* изменяет расчет смещения полей для оставшейся части *выражения,* исходя из того, что это IP-пакет, инкапсулированный в MPLS • *Выражение* "*mpls*" "*[label_num]*" может использоваться более одного раза, для фильтрации по иерархии MPLS • Каждое использование этого выражения увеличивает смещение фильтра на 4 • Например: "*mpls 100000 && mpls 1024* " фильтрует пакеты с внешней меткой 100000 и внутренней меткой 1024, а "*mpls && mpls 1024 && host 192.9.200.1*" фильтрует пакеты к или от 192.9.200.1 с внутренней меткой 1024 и любой внешней меткой
pppoed	• ИСТИНА, если пакет является пакетом PPP-over-Ethernet Discovery (ether proto 0x8863)
pppoes	• ИСТИНА, если пакет является пакетом PPP-over-Ethernet Session (ether proto 0x8864) • Первое ключевое слово "*pppoes*", встретившееся в *выражении* изменяет расчет смещения полей для оставшейся части *выражения,* исходя из того, что это пакет PPPoE session • Например: "*pppoes && ppp proto 0x21*" фильтрует протоколы IPv4, инкапсулированные в PPPoE
tcp, **udp**, **icmp**	• Сокращенные варианты "*ip proto p*", где "*p*" - один из вышеупомянутых протоколов

iso proto *protocol*	• ИСТИНА, если пакет является пакетом OSI типа "*protocol*" • *"Protocol"* может быть номером или одним из следующих имен "*clnp*", "*esis*", или "*isis*"
clnp, **esis**, **isis**	• Сокращенные варианты "*iso proto p*", где "*p*" - один из вышеупомянутых протоколов

expr relop expr	• ИСТИНА, если имеет место данное соотношение, где "*relop*" – один из следующих знаков >, <, >=, <=, =, !=, а *expr* – арифметическое выражение, составленное из целочисленных констант (выраженных в стандартном синтаксисе C), бинарных операторов [+, -, *, /, &, |, <<, >>], длины оператора и специального пакета данных средств доступа
	  • Обратите внимание, что все сравнения беззнаковые, так что, например, 0x80000000 и 0xffffffff будут > 0
	• Чтобы получить доступ к данным внутри пакета, используйте следующий синтаксис: “proto [expr : size]”
	  • *Proto* – один из следующих протоколов: *ether, fddi, tr, wlan, ppp, slip, link, ip, arp, rarp, tcp, udp, icmp*, и обозначает уровень протокола для операции с индексом (*ether, fddi, wlan, tr, ppp, slip* и *link* предполагают канальный уровень)
	  • *tcp*, *udp* и другие типы протоколов верхнего уровня применяются только к IPv4
	  • Смещение в байтах, связанное с указанным уровнем протокола, задается при помощи "*expr*"
	  • *Size* – необязательный элемент и указывает число байтов в интересующем поле. Может быть равен 1, 2 или 4, по умолчанию 1
	• Оператор длины, обозначаемый ключевым словом *len*, задает длину пакета
	  • Например, “ether[0] & 1 != 0” перехватывает весь многоадресный трафик
	  • Выражение “ip[0] & 0xf != 5” перехватывает все пакеты IPv4 с опциями
	  • Выражение “ip[6:2] & 0x1fff = 0” перехватывает только дефрагментированные датаграммы IPv4 и фрагменты frag zero фрагментированных датаграмм IPv4
	  • Эта проверка неявно применяется к "*tcp*" и "*udp*" операциям с индексами
	  • Например, "*tcp[0]*" всегда значит первый байт заголовка TCP, и никогда не означает первый байт промежуточного фрагмента
	• Некоторые смещения и значения поля могут быть выражены именами, а не числовыми значениями
	• Возможны следующие смещения полей заголовка протокола: *icmptype* (поле типа ICMP), *icmpcode* (поле кода ICMP) и *tcpflags* (поле метки TCP)
	  • Возможные значения поля типа ICMP: *icmp-echoreply, icmp-unreach, icmp-sourcequench, icmp-redirect, icmp-echo, icmp-routeradvert, icmp-routersolicit, icmp-timxceed, icmp-paramprob, icmp-tstamp, icmp-tstampreply, icmp-ireq, icmp-ireqreply, icmp-maskreq, icmp-maskreply*
	  • Возможные значения поля метки TCP: *tcp-fin, tcp-syn, tcp-rst, tcp-push, tcp-ack, tcp-urg*

Таблица - Примитивы

Примитивы можно комбинировать, используя:

- Группы примитивов и операторов в круглых скобках (скобки используются специально для Shell и должны иметь измененный регистр)
- Инверсию (`!' или `not')
- Конъюнкцию (`&&' или `and')
- Дизъюнкцию (`||' или `or').

Инверсия имеет наивысший приоритет. Дизъюнкция и конъюнкция имеют равный приоритет и сопоставляются слева на право. Обратите внимание, что явный указатель и метки, не расположенные рядом, требуется сцепить. Если идентификатор задан без ключевого слова, предполагается последнее использованное слово. Например, “*not host 1.1.1.1 and 2.2.2.2*” – сокращение для “*not host 1.1.1.1 and host 2.2.2.2*” – не следует путать с “*not (host 1.1.1.1 or 2.2.2.2)*”.

Параметры групп коммутации

В разделе "Коммутатор (MAC Switch)" представлена информация о существующих группах коммутации и правилах, включая группу управления, а также предусмотрена возможность редактирования параметров групп и правил, их удаления и создания новых групп и правил.

Основные элементы управления в данном разделе:

- Включить Switch - позволяет включить/отключить коммутацию.
- Max Sources - ограничивает таблицу MAC-адресов коммутатора. Количество записей по умолчанию равно 5000.
- STP MINT mode - позволяет включить/отключить режим "STP MINT mode". "STP MINT mode" используется для исключения влияния проводных коммутаторов с настроенным протоколом STP на работу сети. Режим блокирует передачу кадров BPDU протокола STP, настроенного на проводных коммутаторах, чтобы коммутатор не смог обнаружить петлю и заблокировать свои порты. "STP MINT mode" в совокупности с протоколом RSTP, активированном в группе коммутации беспроводных устройств Инфинет, позволяет одновременно и разорвать петлю, в случае её возникновения, и сохранить функционирование протокола PRF, работающего через проводной сегмент.

ПРЕДОСТЕРЕЖЕНИЕ

Отключение коммутатора при отсутствии настроек маршрутизации может привести к прекращению передачи пакетов через устройство.

Область настроек группы коммутации:

Параметр коммутатора	Описание
Группа #	Показать номер группы коммутации или назначить идентификатор группы коммутации (должен быть уникальным в рамках сегмента сети MINT)
Состояние	Выбрать состояние: работает, остановлен или "*discard*"
Интерфейсы	Выбрать Ethernet и/или Radio и/или (для специфических целей) созданный ранее виртуальный интерфейс (интерфейсы) в качестве интерфейса группы коммутации в окне, вызываемом нажатием кнопки "**Ports**". Выбор: "pass" (по умолчанию), "*strip*" или "*tag*" для настройки меток VLAN для каждого выбранного интерфейса. Каждый интерфейс поддерживает три возможных сценария: • "*Pass*" – прозрачный режим, трафик остается неизменным; • "*Strip*" – все метки снимаются; • "*Tag*" – все пакеты тегируются указанной меткой VLAN. Удалить добавленный интерфейс (интерфейсы)
STP	Включить/отключить поддержку STP. Добавить номер VLAN для STP , в случае если поддержка STP включена
Repeater	Включить/отключить поддержку режима "*Repeater*". Устройство действует как повторитель, транслируя пакеты во все порты, кроме порта источника
IGMP	Включить/отключить поддержку IGMP snooping. Подробнее см. раздел IGMP snooping
Флуд	Разрешить/запретить неограниченный одноадресный флуд без защитного фильтра
Inband	Разрешить/запретить доступ к устройству внутри полосы (при использовании широковещательного/многоадресного трафика). Разрешено по умолчанию
Режим	Установить рабочий режим группы коммутации: *normal, trunk, in-trunk* (номер должен соответствовать номеру транковой группы, созданной на базовой станции), *upstream, downstream* • "*Normal*" (стандартный режим) – работа группы коммутации основана на настроенных правилах, пакеты обрабатываются без изменений (установлен по умолчанию); • "*Trunk*" – трафик внутри не тегирован и располагается в группах коммутации в соответствии с меткой VLAN; • "*In-Trunk*" – позволяет отфильтровывать трафик, который принадлежит определенной группе коммутации, входящей в транковую группу; • "*Upstream*" – используется в основном в системах видеонаблюдения для восходящих многоадресных потоков; • "*Downstream*" - используется в системах видеонаблюдения для нисходящего трафика
Описание	Добавить текстовое описание для текущей группы коммутации (латиницей)
Стандартное действие	Установить действие по умолчанию: разрешение/отказ. В отсутствие каких-либо правил коммутации, или в случае, если пакет не соответствует ни одному из правил коммутации, выполняется действие по умолчанию для данной группы или интерфейса
Default QM Channel	Назначить логический канал по умолчанию. Логический канал по умолчанию сначала должен быть создан в разделе "Traffic Shaping". В отсутствие каких-либо правил коммутации, или в случае, если пакет не соответствует ни одному из правил коммутации, назначается канал по умолчанию О том, как создать логический канал, см. раздел "Приоритезация трафика"

Стандартный приоритет	Назначить приоритет по умолчанию для всех пакетов, проходящих через группу коммутации: • "*Up to*" – повышает приоритет пакета до указанной величины, если он имел более низкий приоритет; • "*Set*" – назначает пакету новый приоритет независимо от того, какой приоритет он имел до этого. В отсутствие каких-либо правил коммутации, или в случае, если пакет не соответствует ни одному из правил коммутации, назначается приоритет по умолчанию

Таблица – Коммутатор (MAC Switch)

- Кнопка "**Удалить L3 интерфейс**" – позволяет удалить интерфейс sviX, используемый для управления устройством.
- Кнопка "**Создать L3 интерфейс**" – позволяет добавить интерфейс sviX для управления устройством через веб-интерфейс (см. примеры конфигурации в Главе Сценарии настройки оборудования)

Чтобы добавить новое правило для группы коммутации, откройте меню "Правила" в области настроек данной группы и нажмите кнопку "**Добавить правило**":

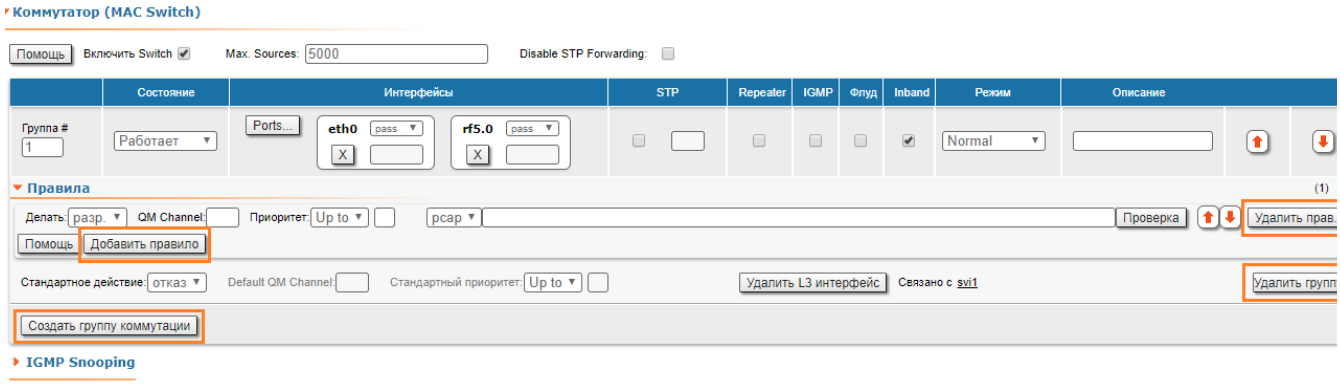


Рисунок – Настройки группы

Чтобы удалить правило, нажмите кнопку "**Удалить прав.**" в правой части строки данного правила

Чтобы изменить порядок групп коммутации в списке, используйте стрелки "**вверх**/**вниз**" в правой части области настройки групп коммутации.

Чтобы удалить группу, нажмите кнопку "**Удалить группу**" в правом нижнем углу области настроек данной группы.

Чтобы создать новую группу, нажмите кнопку "**Создать группу коммутации**" под списком существующих групп.

Набор правил применяется ко всем пакетам внутри группы коммутации. Вы можете создать несколько правил коммутации внутри группы коммутации. С помощью правил коммутации могут быть настроены следующие параметры:

Параметр правила коммутации	Описание
Делать	Установить действие для пакетов, которые соответствуют правилу: разрешение/отказ
QM Channel	Назначить логический канал, если он был создан в разделе "Контроль трафика". Если указать номер логического канала, не заданного в разделе "Контроль трафика", он никак не отразится на конфигурации данного правила. О том, как создать логический канал, см. в разделе "Контроль трафика")
Приоритет	Назначить приоритет для всех пакетов, проходящих через данное правило фильтра: • "*Up to*" – повышает приоритет пакета до указанной величины, если он имел более низкий приоритет • "*Set*" – назначает пакету новый приоритет независимо от того, какой приоритет он имел до этого
Выражение фильтра Packet capture	Установить фильтр "*packet capture*" для коммутации. Синтаксис называется PCAP-выражение. См. Подробное описание синтаксиса правил фильтрации, чтобы проверить синтаксис правила, нажмите кнопку "**Проверка**"

Список VLAN	Установить VLAN ID. Доступен для прежних версий продукта. Может быть установлен как PCAP-выражение, не допустимо в режиме "*trunk/in-trunk*". Например, vlan 100 (при выбранном значении pcap в раскрывающемся списке). Чтобы проверить синтаксис правила, нажмите кнопку "**Проверка**"

Таблица – Правила групп коммутации

> **ВНИМАНИЕ**
>
> Фильтры в разделах "Коммутатор (MAC Switch)", "IP Firewall" и "Контроль трафика" имеют одинаковый синтаксис для установки правил - PCAP-выражение. Это универсальный инструмент для создания правил.

IGMP Snooping

Данная вкладка позволяет настроить параметры IGMP для групп, у которых поддержка IGMP была активирована (у такой группы должен быть отмечен флажок "IGMP" в разделе "Коммутатор".

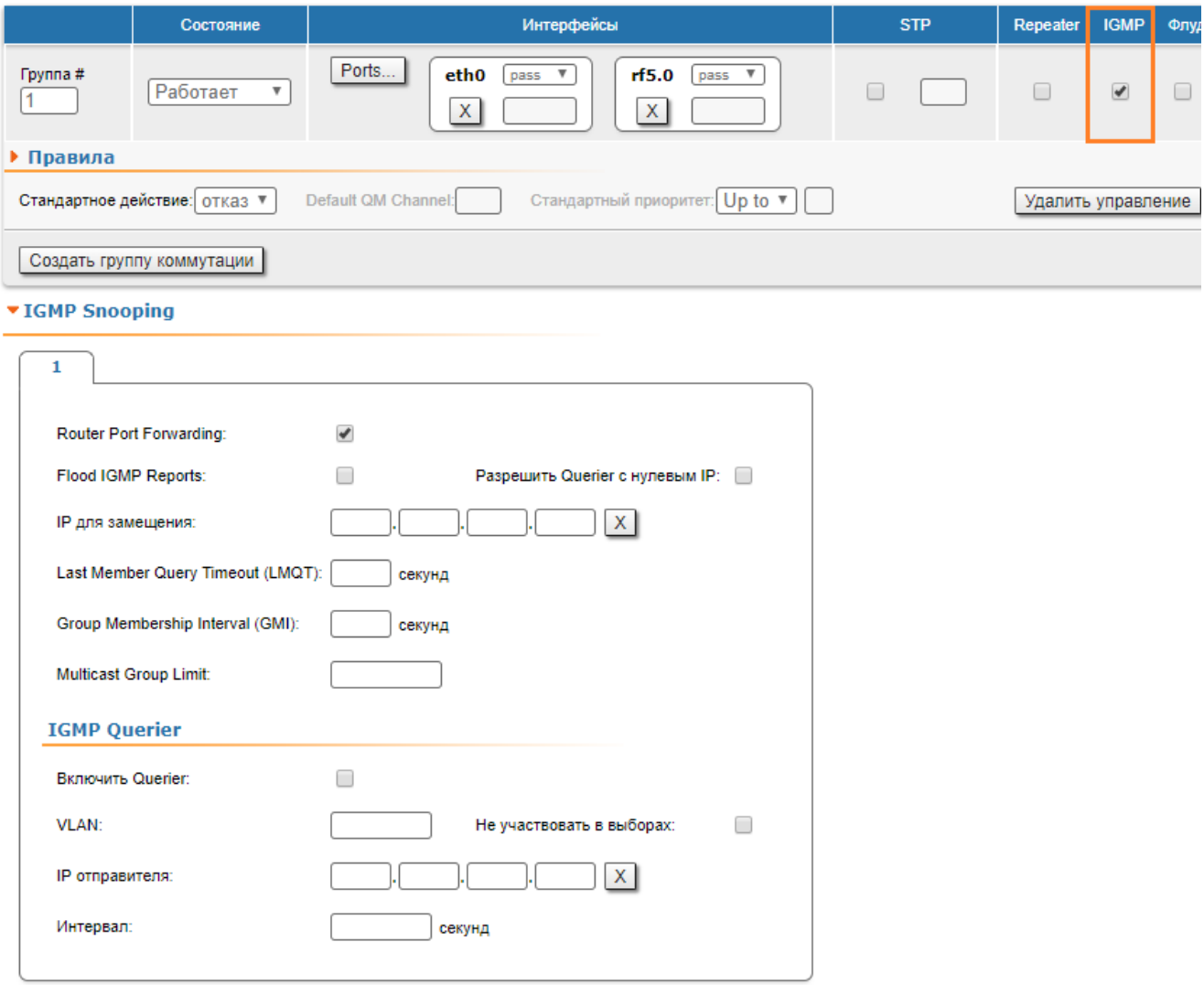


Рисунок - Настройки IGMP Snooping

IGMP Snooping – механизм сдерживания для multicast-рассылки, работающий на устройствах канального уровня (L2), служит для контроля и управления multicast-группами. Устройство с поддержкой IGMP Snooping прослушивает и анализирует сообщения IGMP, составляя карту соответствия портов с multicast MAC-адресами, на основании которой в последствии производит пересылку multicast-данных.

Title

Для работы функции IGMP Snooping необходимо, чтобы в сети был multicast-маршрутизатор генерирующий IGMP-запросы. Таблицы составляемые для данной функции (соответствие порта участника каждой группе коммутации) должны быть привязаны к multicast-маршрутизатору, без маршрутизатора такие таблицы не будут генерироваться, и IGMP Snooping работать не будет. Кроме того, все коммутаторы участвующие в IGMP Snooping должны безоговорочно пропускать общие IGMP-запросы.

Параметры IGMP Snooping, которые могут быть настроены в разделе "Коммутатор":

Параметр	Описание
Router Port Forwarding	Разрешить/Запретить пересылку на порт маршрутизатора
Flood IGMP Reports	Включает/выключает трансляцию пакетов IGMP report во все порты коммутатора, а не только в те, к которым подключен маршрутизатор
Разрешить Querier с нулевым IP	Разрешить/Запретить обработку и трансляцию пакетов с исходным IP-адресом 0.0.0.0
IP для замещения	Заменяет IP-адрес источника во всех IGMP уведомлениях/запросах
Last Member Query Timeout (LMQT)	Устанавливает максимальное время, в течение которого коммутатор будет ждать ответа от активных подписчиков, перед тем как закрыть доставку multicast-пакетов на данный порт (в секундах)
Group Membership Interval (GMI)	Устанавливает максимально возможное время, за которое коммутатор решит, что на данном шлюзе не осталось активных подписчиков (в секундах)
Multicast Group Limit	Ограничивает количество адресов активных multicast групп. При превышении указанного лимита, новые IGMP-подписки блокируются
Включить Querier	Включает/выключает функцию Querier, назначающую функции multicast-маршрутизатора. В каждом сегменте должен быть только один активный Querier
VLAN	Устанавливает VLAN ID для IGMP Querier
Не участвовать в выборах	Запрещает/разрешает участвовать в выборах IGMP Querier в данном сегменте
IP отправителя	Назначает адрес отправителя IGMP-пакетов, по умолчанию 0.0.0.0
Интервал	Устанавливает интервал отправки пакетов "IGMP Querier" в секундах