Title

Команда switch

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

Пройти сертификационный экзамен

Содержание

Описание

Команда "*switch*" предназначена для управления коммутатором (MAC Switch).

ПРЕДОСТЕРЕЖЕНИЕ

Начиная с версии "*MINT 1.22.0*" режим работы коммутатора частично несовместим с предыдущими версиями. Если в сети есть устройства, работающие в режиме коммутатора, необходимо обновление программного обеспечения на всех узлах сети. Совместимость на уровне протоколов MINT и маршрутизации сохраняется. Также сохраняется возможность обновления ПО "*Over The Air*".

Синтаксис:

```
 MAC Switch V2.06
Usage:
________ LIST commands _____________________________________

  switch list LISTNAME [{iface | mac | numrange | match}]
         {add | del} [VALUE ...]
         dump [name] [WILDCARD]
         rename  NEWNAME
         file   FILENAME
         [flush|remove]

________ GROUP commands _____________________________________

  switch group ID {add | del} IFNAME[:{TAG|0}] ...
  switch group ID {repeater|trunk|unpaired} {on|off}
  switch group ID {(up|down)stream} {SCID|0}
  switch group ID [x]vlan {TAG|LIST|0} [[no]bidir]
  switch group ID nvlan {[on]|off}
  switch group ID info INFO_STRING
  switch group ID setid NEWID
  switch group ID stp { off | on | dump }
  switch group ID stp [vlan TAG]
  switch group ID stp priority [PRIO]             #(default: 57344, step: 4096)
  switch group ID stp forwarddelay [DELAY]        #(default: 15 sec)
  switch group ID stp maxage [TIME]               #(default: 20 sec)
  switch group ID stp port IFNAME priority [PRIO] #(default: 128, step 16)
  switch group ID stp port IFNAME cost [COST]     #(default: 200000(RSTP),
                                                            65535(STP))
  switch group ID igmp { off | on }
  switch group ID igmp static-add MCAST IF_NAME [MAC]
  switch group ID igmp static-del MCAST IF_NAME [MAC]
```

```
  switch group ID igmp dump [detail] [name]
  switch group ID igmp lmqt Value
  switch group ID igmp gmi Value
  switch group ID igmp router-port { off | on }
  switch group ID igmp flood-reports { off | on }
  switch group ID igmp zero-query-permit { off | on }
  switch group ID igmp srcip IP
  switch group ID igmp join-limit [IF_NAME] N [include $ACL] [except $ACL]
  switch group ID igmp querier [vlan N] {start|stop|clear}
  switch group ID igmp querier [[no]election] [source IP] [mcast X[,Y,...]]
  switch group ID igmp querier interval Value

  switch group ID dhcp-snooping { off | on }             #(default: off)
  switch group ID dhcp-snooping [no]trust IFNAME         #(default: notrust)
  switch group ID dhcp-snooping [no]verify-mac           #(default: verify)
  switch group ID dhcp-snooping option-82 [no]insert     #(default: insert)
  switch group ID dhcp-snooping option-82 format
    { string ASCII-string | hex HEX-string | mac }       #(default: mac)
  switch group ID dhcp-snooping option-82 untrusted-policy
    { drop | keep | replace }                            #(default: drop)

  switch group ID flood-unicast { off | on }
  switch group ID inband { off | on }
  switch group ID order N
  switch group ID set NEWNUMBER
  switch group ID [setpri|addpri PRIO] [qmch CHAN]
  switch group ID {deny | permit}
  switch group ID
         dump [interface] [WILDCARD]
         [dbdelete   MACADDRESS]
         {start [discard]| stop | remove | stat | showrules | showblack}
  switch group ID {in-trunk} [{ID|0}]

________ INTERFACE commands _____________________________

  switch interface IFNAME mac-limit N

________ RULES commands _________________________________

  switch {group ID | interface IFNAME} rule NUMBER
         [not]
         [src   LIST] [dst   LIST] [vlan  LIST]
         [iface LIST] [proto LIST] [match LIST]
         [ setpri|addpri PRIO ] [qmch CHAN]
         [ deny | permit ] [ remove ]

_______  CONTROL commands ________________________________

  switch resynchronize
  switch trace { off | on | verbose | filter "pcap expr"}
  switch stptrace { off | on }
  switch stpblock { off | on }
  switch stpmint { off | on }
  switch {dump [WILDCARD]|MACADDRESS}

  switch igmp[-snooping] dump [name] [detail]
  switch {start|stop|restart|destroy|dead-interval DEAD_INTERVAL[300]}
  switch stat[istics] [(clear|help|ID)]
  switch maxsources (MAXSOURCES|0) # default 5000
```

Шаблоны поиска "*WILDCARD*" используются в качестве аргументов в различных командах для формирования поисковых запросов, позволяющих описывать определенные группы сущностей. В качестве шаблонов могут быть использованы следующие символы:

- * - звездочка обозначает наличие в данной позиции любого символа или набора символов. Набор может быть и пустым;
- ~ - знак тильды обозначает наличие в данной позиции любого одного символа.

Правила коммутации

Title

Правила коммутации используются для определения коммутационной группы, в которую будут направлены пакеты, принятые, через интерфейсы "*eth**". Коммутация сетевого пакета будет осуществляться группой, правилам коммутации которой удовлетворяет данный пакет. Соответствующая группа коммутация принимает решение о необходимости пересылки пакета через указанный сетевой интерфейс.

Правила коммутации представляют собой перечень правил (rules) и решение по умолчанию (deny/permit). Каждое правило состоит из порядкового номера, условия и решения (deny/permit). При просмотре списка определяется, удовлетворяет ли пакет условию каждого правила. Если удовлетворяет, то в отношении данного пакета принимается решение этого правила. Иначе просмотр списка правил будет продолжен. Порядок просмотра правил производится в соответствии с их порядковыми номерами, по возрастанию. Если пакет не удовлетворяет условию ни одного из правил, то принимается решение по умолчанию данной группы или интерфейса.

Каждое условие включает в себя один или более элементов, сопоставляемых со следующими параметрами пакета:

1. Интерфейс, через который осуществляется отправка пакета.
2. MAC-адрес источника пакета (src).
3. MAC-адрес получателя (dst).
4. Метка VLAN.
5. Номер протокола уровня Ethernet (proto).

В каждом элементе условия указывается имя списка допустимых значений соответствующего параметра пакета. Кроме того, в условии может присутствовать выражение, записанное на языке фильтров PCAP (tcpdump). Это выражение рассматривается как псевдо-параметр пакета и называется "*match*". Таким образом, пакет признается удовлетворяющим условию, если все его параметры принадлежат соответствующим спискам допустимых значений параметра, а весь пакет в целом удовлетворяет выражению "*match"*. Если в условии отсутствует элемент для какого-либо параметра пакета, то данный параметр пакета, вне зависимости от своего значения, считается удовлетворяющим такому условию.

Параметры

Параметры	Описание
Управление списками значений	
list	Параметр, отвечающий за управление списками значений. Списки значений используются в качестве набора допустимых значений для элементов условий (rule).
LISTNAME	Имя списка значений. Каждый список должен иметь уникальное имя, которое может состоять из произвольного сочетания букв и цифр, но не должно начинаться с цифры. Имя списка нечувствительно к регистру.
[{iface | mac | numrange | match}]	Каждый список должен быть отнесен к одному из типов: • "*iface*" – список содержит сетевые интерфейсы. • "*mac*" – список содержит набор значений MAC-адресов. • "*numrange*" – список содержит набор диапазонов целочисленных положительных значений. Диапазон значений указывается в виде "*<min>[-<max>]"*. Диапазон может содержать единственное значение в случае, если "*<min>=<max>"*. При добавлении в список диапазона, пересекающегося с уже существующим, происходит их объединение. При удалении диапазона, пересекающегося с существующим(и) в списке, происходит удаление полностью вложенных диапазонов и/или дробление пересекающихся с удаляемым. • "*match*" – по контексту применения, "*match"* выражения идентичны спискам значений, но состоят из единственного элемента – выражения. Выражение определяется в формате PCAP. Если выражение содержит пробелы, то оно должно быть заключено в кавычки.
{add | del} [VALUE ...]	Параметры "*add"* и "*del"* предназначены для добавления и удаления значений в указанный список (за исключением "*match").* • "*VALUE*" – одно или несколько значений, которые должны быть добавлены.
dump [name] [WILDCARD]	Вывод содержимого списка. • "*name*" – имя списка значений. • "*WILDCARD"* – шаблон поиска.
rename NEWNAME	Переименование списка. • "*NEWNAME*" – новое имя списка.

file FILENAME	Для списков допускается указание источника значений, который представляет собой текстовый файл, построчно хранящий набор значений. Файл может быть расположен на FTP-сервере, к которому у настраиваемого устройства есть сетевой доступ. Загрузка значений в список из источника происходит автоматически при старте коммутатора или при изменении имени источника.
[flush|remove]	• "*flush*" – удалить все значения из списка. • "*remove*" – удалить список значений.
Управление группами коммутации	
group	Параметр, отвечающий за управление группами коммутации.
ID	Числовой идентификатор группы в диапазоне от 1 до 4999

{add | del} IFNAME[:{TAG|0}] ...	Параметры используются для включения или исключения указанных сетевых интерфейсов из группы коммутации:
	
	• "*add|del"* – добавить/удалить указанные сетевые интерфейсы в группу. Если указан параметр "*add"*, а группы с идентификатором ID не существовало, то она будет создана автоматически.
	• "*IFNAME"* – имя сетевого интерфейса, который должен быть добавлен или удален из группы коммутации.
	• "*TAG"* – аргумент, который позволяет управлять маркировкой пакета, если он направляется в данный интерфейс. При этом возможны следующие варианты:
	  • TAG указан для интерфейса и его значение >0. Это означает, что любому пакету, направляемому коммутатором в данный интерфейс, будет присвоен номер VLAN, равный TAG. Если пакет уже имел метку VLAN, то она будет заменена на TAG.
	  • TAG не указан. Это означает, что значение метки VLAN пакета не будет изменено или добавлено.
	  • TAG указан, и его значение равно 0. Это означает, что у пакета, направляемого в сетевой интерфейс, будет удалена метка VLAN, или он будет передан без изменений в случае ее отсутствия.

{repeater|trunk|uncoupled} {on|off}	Включение/выключение режима коммутации. Пользователю WANFleX доступны следующие режимы: • "*repeater*" – группа коммутирует пакеты простой ретрансляцией из интерфейса, через который пакет был принят, во все остальные интерфейсы, включенные в данную группу. • "*trunk*" – группа коммутирует все пакеты, принятые через сетевые интерфейсы "*eth**" таким образом, что, при передаче их в интерфейсы "*rf*",* она отправляет их с номером группы, равным "*vlan"* этих пакетов. При этом, по умолчанию, сами пакеты не изменяются. При приеме пакетов с интерфейсов "*rf**", группа в режиме "*trunk*" отправляет эти пакеты в интерфейсы "*eth**", устанавливая метку "*vlan"* в значение, равное номеру группы коммутации, с которой они были приняты через интерфейс "*rf**". • "*uncoupled*" – если сеть с кольцевой структурой подключена к вышестоящей сети в нескольких точках, то возникает опасность образования коммутационных петель через внешнюю сеть. В этом случае протокол STP не позволяет одновременно использовать все подключения для равномерной и эффективной загрузки сети. Группы, имеющие признак "*uncoupled*", не участвуют в передаче коммутируемого трафика между собой, даже если имеют одинаковый номер группы, что исключает возможность возникновения петель, но не мешает инжектировать трафик в сеть. Для исходящего трафика промежуточные узлы будут использовать только ближайший к себе "*uncoupled*" узел (определяемый по времени доступа), что способствует более равномерной загрузке сети.
{(up|down) stream} {SCID|0}	Для решения часто возникающей задачи передачи восходящих потоков "*multicast"* в системах видеонаблюдения вводятся два дополнительных параметра*:* • *"downstream"* – устройство используется для передачи нисходящего трафика. • "*upstream*" – для передачи восходящего трафика. • *"SCID|0"* – идентификатор канала коммутации 0, 1, 2. Должен совпадать на "*upstream"* и "*downstream"* устройстве.
in-trunk [{ID|0}]	Параметр позволяет создавать несколько непересекающихся транковых групп в пределах одной сети, с одинаковыми потоками VLAN внутри.

[x]vlan {TAG|LIST|0} [[no]bidir]	Параметр определяет, что группа ID будет коммутировать только пакеты, метка VLAN которых равна одному из следующих значений: • "*TAG*" – значение маркировки, указанное явно. • "*LIST*" – значение, принадлежащее указанному списку типа "*numrange*". • "*0*" – отменяет фильтрацию по VLAN у данной группы. • "*bidir"* – позволяет производить проверку входящих пакетов на соответствие указанным меткам для каждого из интерфейсов группы (входящие из проводного сегмента и приходящие через беспроводной канал). Данный параметр будет полезен при передаче набора VLAN через сеть с кольцевой структурой, с отбором некоторых из них в промежуточных узлах кольца. • *"[x]"* – данный параметр позволяет группе обрабатывать пакеты без метки VLAN. **ВНИМАНИЕ** Примечание: при включенном таким образом фильтре по VLAN, остальные правила коммутации не действуют.
nvlan {[on] |off}	Параметр определяет, что группа будет коммутировать только немаркированные пакеты.
info INFO_STRING	Параметр позволяет добавить описание группы.
setid NEWID	Устанавливает новый идентификатор коммутационной группы.
dump [interface] [WILDCARD]]	Выводит базу данных MAC-адресов. • "*interface"* – выводит базу данных известных MAC-адресов с группировкой по интерфейсам. • "*WILDCARD"* – шаблон поиска, позволяющий выводить информацию, отвечающую заданному критерию.
stat	Выводит статистику по указанной группе.
showrules | showblack	• "*showrules*" – отображает детальную информацию по правилам классификации группы, включая счётчик срабатывания каждого правила • "*showblack*" – показывает список MAC-адресов, заблокированных по причине неопределённости места нахождения адресата.
dbdelete MACADDRESS	Удаляет все записи из базы данных MAC-адресов, связанные с указанным MAC-адресом.
start [discard] |stop | remove	Активирует/деактивирует указанную коммутационную группу, удаляет указанную группу из конфигурации коммутатора.
stp { off | on | dump }	Коммутатор поддерживает протокол STP, а именно две его версии: STP и RSTP. Данный параметр включает или выключает поддержку протокола STP для данной группы. • "*dump*" – позволяет посмотреть текущее состояние STP для данной группы.
stp priority [PRIO]	Устанавливает приоритет STP коммутатора. • "*PRIO"* – значение приоритета. Если значение приоритета не указано, то устанавливается значение по умолчанию, равное 57344. При указании значения приоритета следует учитывать, что оно будет автоматически округлено в меньшую сторону до значения кратного 4096.
stp forwarddelay [DELAY]	Устанавливает значение параметра STP "*forward delay*", определяющего время нахождения коммутатора в состояниях "*listening*" и "*learning*". • "*DELAY"* – значение данного параметра в секундах. Если значение не указано, то устанавливается значение по умолчанию, равное 15 секундам.

stp maxage [TIME]	Определяет значение параметра STP "*MAX age*", определяющего время ожидания коммутатором пакета BPDU. • "*TIME"* – значение данного параметра в секундах. Если значение не указано, то устанавливается значение по умолчанию, равное 20 секундам.
stp port IFNAME priority [PRIO]	Устанавливает приоритет STP порта коммутатора. • "*IFNAME"* – имя интерфейса порта. • "*PRIO"* – значение приоритета порта. Если значение приоритета не указано, то устанавливается значение по умолчанию, равное 128. При указании значения приоритета следует учитывать, что указанное значение будет автоматически округлено в меньшую сторону до значения кратного 16.
stp port IFNAME cost [COST]	Устанавливает значение параметра STP "*cost*" порта коммутатора, определяющего стоимость порта коммутатора. • "*COST"* – значение данного параметра. Если значение не указано, то устанавливается значение по умолчанию, равное 200000 для RSTP, 65535 для STP.
stp [vlan TAG]	Определяет метку VLAN для протокола STP, активированного для группы коммутации.
igmp { off | on }	Позволяет отключить/включить функцию "*IGMP-snooping*" для определенной группы коммутации.
setpri|addpri PRIO	Устанавливает/повышает приоритет пакетов, проходящих через группу. • "*setpri"* – явно устанавливает приоритет для пакета. При использовании значения – 1, у пакета сбрасывается его приоритет. • "*addpri"* – изменяет приоритет только в том случае, если вновь устанавливаемый приоритет выше, чем уже имеющийся у пакета (чем меньше число, тем выше приоритет). То есть, с помощью параметра "*addpri"* приоритет можно только повысить.
qmch CHAN	Данная команда при попадании Ethernet-фрейма в группу коммутации ID позволяет назначить ему класс обслуживания "*CHAN*". Классы обслуживания создаются командой "*qm chan*".
{deny | permit}	Запрещает/разрешает обрабатывать и отправлять пакеты, принадлежащие данной группе.
igmp dump [detail] [name]	Выводит список IGMP-узлов (клиентов), подписанных на группу multicast. • "*detail"* – позволяет вывести детальную информацию о подписчиках. • "*name*" – выводит информацию для конкретного шлюза.
igmp lmqt Value	Устанавливает значение "*Last Member Query Time*" – максимальное время, в течение которого коммутатор будет ждать ответа от активных подписчиков, перед тем как закрыть доставку multicast-пакетов на данный шлюз после приема пакета "*IGMP leave*". В качестве шлюза может выступать либо Ethernet интерфейс, либо радио интерфейс и MAC-адрес клиента, находящегося на другой стороне радио соединения.
igmp gmi Value	Устанавливает значение "*Group Membership Interval*" – максимально возможное время, за которое коммутатор решит, что на данном шлюзе не осталось активных подписчиков (нет пакетов "*IGMP report*" на данную группу).
igmp static-add MCAST IF_NAME [MAC]	Создает статическую подписку клиента на multicast-адрес.
igmp static-del MCAST IF_NAME [MAC]	Удаляет статическую подписку клиента на multicast-адрес.
igmp router-port { off | on }	Включает режим трансляции multicast-пакетов не только в порты подписчикам, но и во все порты, к которым подключены маршрутизаторы (Querier).
igmp flood-reports { off | on }	Включает/выключает трансляцию "*IGMP report*" пакетов во все порты коммутатора, а не только в те, к которым подключены маршрутизаторы (Querier). По умолчанию – "*off*".

igmp srcip IP	Меняет IP-адрес источника в пакетах "*IGMP Report*" на IP-адрес, указанный в параметре "*IP*" данной команды.
igmp zero-query-permit { off | on }	Разрешает обработку и трансляцию пакетов с исходным IP-адресом 0.0.0.0. По умолчанию – "*off*".
igmp querier [vlan N] {start|stop|clear}	Включает/выключает функцию "*Querier*", заменяющую функции multicast-маршрутизатора при организации систем видеонаблюдения с использованием "*IGMP Snooping*". • "*vlan N*" – включает передачу multicast-пакетов с использованием vlan. • "*clear*" – очищает конфигурацию "*IGMP Querier*".
igmp querier [[no]election] [source IP] [mcast X[, Y,...]]	• "*[no]election*" – при активной функции "*IGMP Querier*", запрещает/разрешает участвовать в выборах "*IGMP Querier*" в данном сегменте сети. Согласно принятым стандартам в каждом сегменте должен быть только один активный "*Querier*", имеющий наименьший IP-адрес. По умолчанию – включено. • "*source X*" – устанавливает адрес источника для multicast-пакетов. • "*mcast X[,Y,...]*" – устанавливает номер группы (или групп), на которую разрешена подписка.
igmp querier interval Value	Устанавливает интервал отправки пакетов "*IGMP Querier*" в секундах.
igmp join-limit [IF_NAME] N [include $ACL] [except $ACL]	Ограничивает количество адресов активных уникальных multicast групп в режиме "*IGMP Snooping*". При превышении указанного лимита, новые IGMP-подписки блокируются. • "*IF_NAME*" – сетевой интерфейс, на который действует ограничение. • "*include $ACL*" – список, содержащий перечень адресов/сетей, на которые действует ограничение. • "*except $ACL*" – список, содержащий перечень исключений.
flood-unicast { off | on }	Включает/выключает режим "*flood-unicast*", позволяющий пересылать unicast-пакеты как широковещательные, отправляя их через все интерфейсы, включенные в группу коммутации.
inband { off | on }	Если трафик передаваемый группой коммутации не содержит (не должен содержать) информации, предназначенной данному устройству (только транзитный поток), то можно отключить анализ широковещательных (broadcast) пакетов, что позволяет снизить нагрузку на процессор. По умолчанию анализ включен.
order N	В процессе распределения пакетов данных по группам коммутации группы просматриваются в порядке появления их в конфигурации. Выбирается первая группа, правилам которой удовлетворяет пакет, на этом просмотр заканчивается. Данный параметр позволяет изменить порядок следования групп. Она указывает, в каком порядке определенная группа будет просматриваться при распределении.
dhcp-snooping { off | on }	Активирует/деактивирует функцию DHCP-snooping, обеспечивающую защиту от атак при помощи протокола DHCP. По умолчанию выключена.
dhcp-snooping [no] trust IFNAME	Отмечает интерфейс как доверенный/недоверенный. По умолчанию все интерфейсы отмечены как недоверенные.
dhcp-snooping [no] verify-mac	Активирует/деактивирует проверку на соответствие MAC-адресов отправителя с указанными в DHCP-запросе.
dhcp-snooping option-82 [no]insert	Включает/выключает добавление опции 82 в DHCP-запрос. По умолчанию включено.
dhcp-snooping option-82 format { string ASCII-string | hex HEX-string | mac }	Устанавливает формат идентификатора DHCP-ретранслятора в опции 82. • "*mac*" – MAC-адрес по умолчанию. • "*ASCII-string*" – идентификатор в кодировке ASCII. • "*HEX-string*" – идентификатор в кодировке HEX.

dhcp-snooping option-82 untrusted-policy { drop | keep | replace }	Настраивает действие, выполняемое в случае попадания пакета, содержащего опцию 82 на недоверенный интерфейс. По умолчанию пакеты отбрасываются.
Управление интерфейсом	
interface IFNAME mac-limit N	Используется для ограничения количества MAC-адресов, доступных через указанный сетевой интерфейс. При превышении указанного лимита, новые MAC-адреса не будут вноситься в таблицу коммутации, и весь трафик с этих адресов будет блокирован.
Управления правилами коммутации	
group ID | interfce IFNAME	Номер группы/имя интерфейса.
rule NUMBER	Порядковый номер правила.
set NEWNUMBER	Устанавливает новый порядковый номер правила.
remove	Удаляет правило.
src, dst, vlan, iface, proto, match LIST	Устанавливают списки допустимых значений для соответствующего параметра пакета. Подробнее данные параметры описаны в подразделе "Правила коммутации". • *"LIST"* – имя списка допустимых значений.
deny | permit	Определяет соответствующее решение данного правила.
setpri|addpri PRIO	Устанавливает/повышает приоритет пакетов, принятых конкретным правилом классификации. • "*setpri"* – явно изменяет приоритет на указанный в команде. При использовании значения -1, у пакета сбрасывается его приоритет. • "*addpri"* – изменит приоритет только в том случае, если вновь устанавливаемый приоритет выше, чем уже имеющийся у пакета (чем меньше число, тем выше приоритет). То есть, с помощью параметра "*addpri*" приоритет можно только повысить.
Команды управления	
resynchronize	Производит принудительную перезагрузку содержимого списка допустимых значений, источником данных которого был указан файл.
trace { off | on | verbose | filter "pcap expr"}	Включает/выключает запись в системный лог диагностической информации. • "*verbose*" – запись более детальной информации. • "*filter "pcap expr*" – позволяет проследить процесс обработки коммутатором пакетов соответствующих указанному фильтру PCAP.
stptrace { off | on }	Включает/выключает вывод служебной информации STP, такой как изменение состояния портов, изменение связей, в системный журнал. По умолчанию выключено.
stpblock { off | on }	• "*on*" – предотвращает сквозную коммутацию STP-фреймов, если поддержка STP на устройстве отключена. • "*off*" – разрешает сквозную коммутацию STP-фреймов.
stpmint { off | on }	Включает/выключает 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.

dead-interval <DEAD_INTERVAL_IN_SECONDS>	База данных MAC-адресов коммутатора- – это таблица маршрутизации MAC-уровня, содержащая информацию о способе доставки пакета до адресата назначения (*dst*). Каждая группа коммутации имеет независимую базу данных. Записи в таблице образуются автоматически на основании MAC-адресов источников пакетов. Кроме того база данных всегда содержит записи, соответствующие MAC-адресам интерфейсов коммутационной группы. Эти записи называются локальными. Каждая запись, кроме локальной, имеет "время жизни". Параметр устанавливает "время жизни" записи. В случае, если ни один из интерфейсов за указанный интервал времени не принял ни одного пакета с MAC-адресом источника, соответствующего записи базы данных, то данная запись удаляется. По умолчанию равно 300 секунд.
{start | stop | restart}	Запуск/останов/перезагрузка коммутатора.
{destroy}	Удаление конфигурации коммутатора.
statistics [(clear|help|ID)]	Отображает статистику работы коммутатора. Выгружает информацию по отправленным, отброшенным и flood-пакетам, а также по записям таблицы MAC-адресов коммутатора (DB Records). Статистика по unicast, broadcast и flood-пакетам ведется отдельно. • "*clear*" – обнуляет статистику. • "*help*" – отображает справку по причинам отбрасывания пакетов, которые используются в выводе статистики. • "*ID*" – идентификатор коммутационной группы. Если указан – статистика будет отображена для этой группы, с разделением по всем входящим в нее VLAN.
igmp[-snooping] dump [name] [detail]	Выводит список IGMP-узлов (клиентов), подписанных на группу multicast по всем группам. • "*detail"* – позволяет вывести детальную информацию о подписчиках. • "*name*" – выводит информацию для конкретного шлюза.
MACADDRESS	Выводит информацию для данного MAC-адреса.
maxsources (MAXSOURCES|0)	Ограничивает таблицу MAC-адресов коммутатора. Количество записей по умолчанию равно 5000. При использовании значения "0", устанавливается минимально допустимое значение, равное 500.

Примеры

Следующий пример показывает способ применения шаблона для вывода информации о сетевых интерфейсах "*eth0*" и "*eth1*". Применение шаблона "*eth~*" сообщает команде "*switch*", что данные должны быть выведены только для интерфейсов, у которых имя начинается с eth и в конце содержит один любой символ. "*Cost"* – стоимость (метрика) маршрута. *"UsCNT"* – счётчик указывающий сколько раз использовалась эта запись, т.е. сколько пакетов было отправлено на этот MAC-адрес.

```
switch group 1 dump eth~
 Bridge group 1(normal), READY STARTED Interfaces : eth0(F) eth1(F) rf5.0(F)
 Total records 5
   DST MAC        L   Int.   GateWay MAC   Cost   UsCNT    Dead    Vlan
 ==============   =  ====  ========= ==   =====  =====    ====   =======
 001111144693       eth0   000000000000     0      3987      300       1
 000435018822    *  eth0   000000000000     0       0          0       1
 000435118822    *  eth1   000000000000     0       0          0       1
```

Создадим список типа "*iface*" с именем "*my_iface*", в который добавим имена сетевых интерфейсов "*eth0*" и "*rf5.0*".

```
switch list my_iface iface add eth0 rf5.0
```

Создадим список диапазонов значений с именем "*vlans",* в который добавим: значение 10, диапазон значений от 20 до 30 и значение 40.

```
switch list vlans numrange add 10 20-30 40
```

Создадим список типа "*match*", в который добавим фильтр, под действие которого будут попадать сетевые пакеты любых протоколов, источником или получателем которых являются IP-адреса из сети "*195.38.45.64/26*".

```
switch list ip_mynet match add net 195.38.45.64/26
```

В данном примере также создается список-выражение типа "*match*", но в этом случае действие фильтра распространяется только на IP-пакеты, принадлежащие сети "*195.38.45.64/26*".

```
switch list ip_mynet match add ip net 195.38.45.64/26
```

В качестве источника значений укажем текстовый файл.

```
switch list MACGROUP1 file ftp://1.2.3.4/switches/list/macgroup1.txt
```

В указанном примере файл "*macgroup1.txt*" может содержать следующие строки:

```
#
00:01:02:03:04:05  #
00:11:12:13:14:15  #
<EOF>
```

К узлам 1,2,3,4,5 и 6 подключены цифровые видеокамеры, которые транслируют изображение с помощью пакетов multicast, и все эти потоки нужно передать на сервер оптимальным способом, не подвергая сеть дополнительной нагрузке, создаваемой широковещательным трафиком.

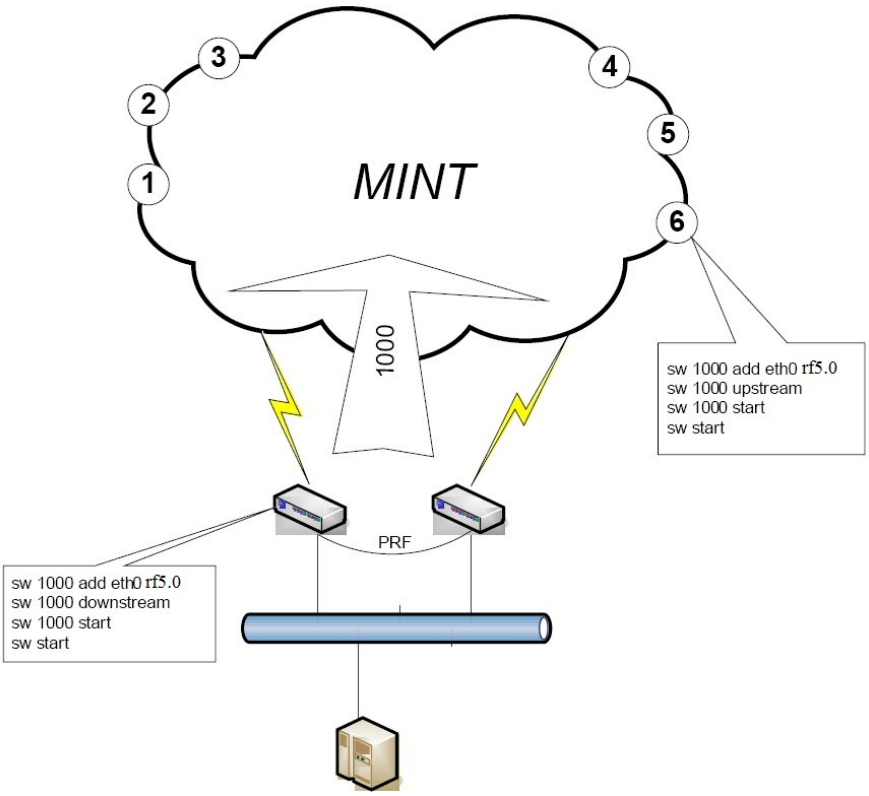

Рисунок - Пример

Весь нисходящий трафик(от сервера к камерам), если таковой имеется, передаётся в группе 1000, в которой находятся все узлы сети. Однако восходящие потоки от каждой камеры передаются непосредственно к ближайшему коммутатору своей группы.

Особенностью такого решения является возможность установки нескольких коммутаторов с одинаковым номером группы. Для устранения проблемы широковещательного шторма, который мог бы возникнуть из-за того, что коммутаторы включены в разные порты одного проводного коммутатора, в MINT введено ограничение – транковые (передающие оба типа трафика) и "*downstream*" коммутаторы никогда не используют друг друга для передачи трафика. Кроме того, наличие параметра "*upstream*" гарантирует, что оконечные узлы будут выбирать для отправки пакетов только один коммутатор, а именно – кратчайший путь к ближайшему коммутатору.

Группа коммутации 100 на клиентском устройстве входит в состав транковой группы 5, в конфигурации коммутатора клиентского устройства следует дать команду:

```
switch group 100 in-trunk 5
```

Выведем информацию о текущем состоянии STP при помощи команды "*switch group ID stp dump*".

```
switch 1 stp dump
 STP state for passive group 1:
 ID:       0000000000000000 Priority: 57344 ID ext: 0
 ROOT:     0000000000000000 Priority: 0     ID ext: 0
 Ports:
  Name  Prio    Cost    PVer    Role      State
 ====== ==== ========== ==== ========== ==========
 eth0    128    2000000 RSTP DISABLED   DISCARDING
 rf5.0   128     180844 RSTP DESIGNATED DISCARDING
```

В указанном примере все пакеты, коммутируемые группой 3 будут маркироваться VLAN 10 при отправке через интерфейс "*rf5.0*" и метки будут сниматься при отправке через интерфейс "*eth0*".

> **ВНИМАНИЕ**
>
> У всех пакетов, адресатом которых является сам коммутатор, метка VLAN всегда удаляется.

```
switch group 3 add rf5.0:10 eth0:0
```

Включим на устройстве транковую группу, которая будет обеспечивать передачу нескольких потоков VLAN по разным направлениям.

```
switch group 12 trunk on
```

На клиентских устройствах следует использовать опцию "*in-trunk*" для явного указания, в состав какой транковой группы входит данная группа.

```
switch group 12 in-trunk 0
```

Группа 10 будет обрабатывать пакеты с метками VLAN 100, 200, 300, а также немаркированные пакеты, такие пакеты будут отправляться в сеть MINT с собственным номером группы, (в данном случае - 10), маркированные - с номерами групп, совпадающими с меткой VLAN.

```
switch list MYNET numrange add 100 200 300
switch group 10 xvlan MYNET
switch group 10 trunk on
```

Группа 20 обрабатывает только маркированные пакеты из списка MYNET и передаёт их, преобразовывая значение метки VLAN, в соответствующий номер группы (и наоборот).

```
switch list MYNET numrange add 100 200 300
switch group 20 vlan MYNET
switch group 20 trunk on
```

Группа 30 обрабатывает только маркированные пакеты из списка MYNET и передаёт их с сохранением номера группы.

```
switch list MYNET numrange add 100 200 300
switch group 30 vlan MYNET
switch group 30 trunk off
```

Title

В данном примере создается группа коммутации "*1*". Для неё включается поддержка стандартного STP протокола и устанавливается STP приоритет коммутатора, равный 36864.

```
switch group 1 add eth0 rf5.0
switch group 1 stp priority 36864
switch group 1 stp on
switch group 1 start
```

В указанном примере создаются три группы коммутации.

1. В группе коммутации 5 создается правило 10, в котором запрещены пакеты с MAC-адресами источника пакета (указанные в группе MACGROUP1), находящиеся в определенных VLAN (список VLAN ID находится в группе VGROUP и состоит из 10, 40 и диапазона от 20 до 30 включительно), в том случае, если это IP и ARP-пакеты, принадлежащие сети, указанной в списке IP_NET3845.
2. В группе коммутации 5 создается правило 20, в котором запрещены пакеты с MAC-адресами получателя пакета (указанные в группе MACGROUP1), находящиеся в определенных VLAN (список VLAN ID находится в группе VGROUP и состоит из 10, 40 и диапазона от 20 до 30 включительно), в том случае, если это IP и ARP-пакеты, принадлежащие сети, указанной в списке IP_NET3845.
3. В группе коммутации 1 пакетам устанавливается приоритет 10.

```
switch list MACGROUP1 mac add 00:01:02:03:04:05 00:11:12:13:14:15
switch list VGROUP numrange add 10 20-30 40
switch list IP_NET3845 match add arp net 195.38.45.64/26 || ip net 195.38.45.64/26
switch group 5 rule 10 src MACGROUP1 vlan VGROUP match IP_NET3845 deny
switch group 5 rule 20 dst MACGROUP1 vlan VGROUP match IP_NET3845 deny
switch group 1 rule 1 setpri 10
```

Включим запись в системном журнале для отображения процесса обработки пакетов коммутатором, предназначаемых для MAC-адреса "*00:11:22:33:44:55*" и подсети "*1.2.3.0/24*".

```
sw trace filter "ether host 00:11:22:33:44:55"
sw trace filter "net 1.2.3.0/24"
```

Пример конфигурации, в которой создаются три коммутационные группы. Группой 5 коммутируются пакеты с VLAN метками 10, 20-30 и 40. Группой 15 коммутируются пакеты с любой меткой VLAN, кроме коммутируемых группой 5. Группой 25 коммутируются любые пакеты без метки VLAN. Кроме того, группой 25 будут передаваться межкоммутаторный трафик.

```
switch list VGROUP numrange add 10 20-30 40

switch list ALL_VLAN numrange add 0-4999

switch group 5 add eth0 rf5.0
switch group 5 rule 10 vlan VGROUP permit
switch group 5 deny
switch group 5 start

switch group 15 add eth0 rf5.0
switch group 15 rule 10 vlan VGROUP deny
switch group 15 rule 11 vlan ALL_VLAN permit
switch group 15 deny
switch group 15 start

switch group 25 add eth0 rf5.0
switch group 25 rule 10 vlan ALL_VLAN deny
switch group 25 permit
switch group 25 start
switch start
```