Настройка пакетных фильтров на D-Link DSLAM DAS-3248

DAS-3248 обладает широкими возможностями по фильтрации и маркированию пакетов. Данный функционал достигается путем использования двух технологий: Generic Filter и Access Control Lists. Ниже будут рассмотрены особенности функционирования данных технологий и приведены примеры настройки.

Generic Filter

Generic Filter является абстрактным уровнем над интерфейсом-классификатором и покрывает поля наиболее часто используемых протоколов в заголовках пакетов, что открывает широкие возможности по фильтрации и обеспечению QoS. В отличие от деревьев классификатора, generic фильтры могут быть применены как на входящие, так и на исходящие интерфейсы с некоторыми ограничениями.

Generic Filter является удобной в использовании абстракцией и удовлетворяет большинству потребностей пользователя. Поддерживаются следующие уровни протоколов:

- Ethernet Layer
  - Source MAC address
  - Destination MAC address
  - EtherType
  - VLAN ID
  - Priority Tag
  - Destination Service Access Point (DSAP) 802.2 LLC кадра
  - Source Service Access Point (SSAP) 802.2 LLC кадра

- IP Layer
  - Destination IP Address
  - Source IP Address
  - IP Protocol Type

- TCP Layer
  - Destination Port
  - Source Port

- UDP Layer
  - Destination Port
  - Source Port

- ICMP Layer
  - ICMP Type
  - ICMP Code

- IGMP Layer
  - IGMP Type
  - IGMP Code
  - Group Address

- PPP Layer

- PPP Protocol Type

Кроме этого Generic Filter может производить анализ пакетов по смещениям от начала заголовков Ethernet, PPP, PPPoE, IP, TCP, UDP, IGMP, ICMP.

Общие принципы

Generic Filter Rule

Правило – это набор подправил, используемых для классификации пакетов. Правило может быть применено к одному или нескольким интерфейсам (eth-xx, eoa-xx).

К данному интерфейсу может быть применено одно или несколько правил Generic Filter. Во время привязки правила к интерфейсу необходимо указать OrderID. OrderID задает порядок выполнения правил в случае, если к одному и тому же интерфейсу применено несколько правил. Правила с меньшим OrderID будут выполнены раньше, чем те, что имеют больший OrderID.

Каждое правило имеет свой уникальный идентификатор RuleID.

После того, как найден пакет, соответствующий какому-либо правилу, к пакету может быть применено одно из следующих действий:

- **Forward exit:** передать пакет в выходную очередь. Игнорировать все последующие этапы. Этапы обработки пакетов будут описаны ниже в данном документе.
- **Allow:** пакет прошел данный этап обработки и будет передан первому правилу следующего этапа на данном интерфейсе.
- **Drop:** отбросить пакет
- **Set Output Priority:** установить внутренний приоритет для пакета который будет использоваться совместно с traffic class mapping table egress порта для определения выходной очереди для данного пакета.
- **Retag Priority:** установить тег приоритета (802.1p) для выходящего пакета. Данное значение приоритета будет использоваться совместно с traffic class mapping table egress порта для определения выходной очереди для данного пакета.
- **Go To Next Rule:** передать пакет следующему правилу данного интерфейса.
- **Classifier Defined:** используется для того, чтобы присоединить дерево классификатора как правило generic фильтра.

ЗАМЕЧАНИЕ: каждое правило может иметь несколько действий в добавлении к тому, которое указано как часть правила. Концепция нескольких действий для одного правила будет описана далее в этом документе.

Во время создания правила пользователь может задать приоритет для него. Данный приоритет определяет тип памяти, которая будет использована для хранения правила. DAS-3248 поддерживает следующие приоритеты:

- High: высокоскоростная память
- Low: низкоскоростная память

Правила, ожидаемая частота срабатывания которых велика, должны создаваться как High priority.

Generic Filter Subrule

Подправило определяет поле пакета, которое будет использоваться при фильтрации. DAS-3248 поддерживает следующие типы подправил:

- Ethernet
- IP
- TCP
- UDP
- ICMP
- IGMP
- PPP
- Generic (на основе смещений)

Существуют следующие типы операций сравнения, поддерживаемых в правилах:

- Equal (равно)
- Not equal (не равно)
- Less than (меньше, чем)
- Less than equal (меньше или равно)
- Greater than (больше чем)
- Greater than equal (больше или равно)
- In range (находится в интервале)
- Ex range (находится вне интервала)
- In Generic List (используется только для Generic подправил и адресов IP source и IP destination IP подправила)
- Not In Generic List (используется только для Generic подправил и адресов IP source и IP destination IP подправила)
- In Named List (только для Generic подправила)
- Not In Named List (только для Generic подправила)

Во время создания подправила пользователь может задать его приоритет. Данный приоритет определяет тип памяти, которая будет использоваться для хранения данного подправила. DAS-3248 поддерживает следующие приоритеты:

- High: высокоскоростная память
- Low: низкоскоростная память
- As in Rule: использовать настройки родительского правила

Рекомендуется для часто срабатывающих правил использовать высокий приоритет.

Для подправил третьего уровня и выше (IP, TCP, UDP, ICMP и IGMP) пользователь может указать тип протокола второго уровня: Ethernet или PPPoE.

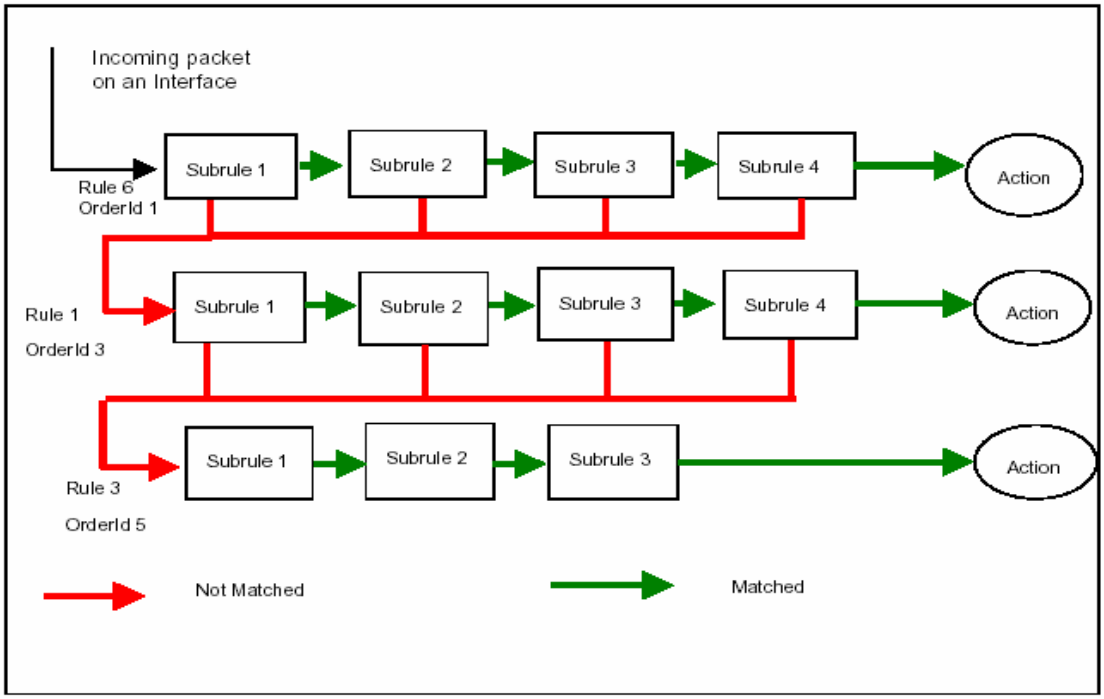

Рисунок1: Порядок исполнения правил и подправил

Порядок действий при создании правила Generic Filter:

- Создать правило generic фильтра
- Добавить одно или несколько подправил к правилу
- Включить правило
- Применить правило к интерфейсу

Примеры использования Generic Filter

1. **Фильтр для запрета icmp echo (type 8 code 0) сообщений на определенном интерфейсе (eoa-x, eth-x)**

create filter rule entry ruleid 2 action drop ruleprio high

Создаем главное правило:

1. action drop – отбрасывать
2. ruleprio high – правило будет загружаться в высокоприоритетную память (рекомендуется для «часто срабатывающих» правил)

create filter subrule icmp ruleid 2 subruleid 1 icmptype 8 icmptypecmp eq subruleprio asinrule

Создаем подправило, в котором указываем, что же все-таки фильтровать:

1. ruleid 2 subruleid 1 – первое подправило второго правила
2. icmptype 8 icmptypecmp eq – все icmp type 8 пакеты
3. subruleprio asinrule – приоритет подправила такой же, как у правила

create filter rule map ifname eoa-23 stageid 1 ruleid 2

Применяем правило к конкретному интерфейсу (eoa-xx, eth-x)

modify filter rule entry ruleid 2 status enable

Включаем фильтр в работу

2. **Фильтр для запрета icmp echo (type 8 code 0) сообщений на определенном интерфейсе (eoa-xx, eth-x) с определенного ip адреса**

create filter rule entry ruleid 2 action drop ruleprio high

Создаем главное правило:

1. action drop – отбрасывать
2. ruleprio high – правило будет загружаться в высокоприоритетную память (рекомендуется для «часто срабатывающих» правил)

create filter subrule ip ruleid 2 subruleid 1 srcipaddrfrom 192.168.100.197 srcaddrcmp eq dstaddrcmp any ipsrcaddrmask 0xffffffff subruleprio asinrule

Создаем первое подправило, в котором указываем, что нас интересует трафик от хоста 192.168.100.197:

1. ruleid 2 subruleid 1 - первое подправило второго правила
2. srcipaddrfrom 192.168.100.197 – нижнее значение диапазона ip адресов источников трафика (т.к. srcaddrcmp равен eq, верхнее можно не указывать)
3. dstaddrcmp any – ip адрес назначения любой
4. ipsrcaddrmask 0xffffffff – маска источника 255.255.255.255
5. subruleprio asinrule – приоритет подправила такой же, как у правила

create filter subrule icmp ruleid 2 subruleid 2 icmptype 8 icmptypecmp eq subruleprio asinrule

Создаем подправило, в котором указываем, что из ранее выбранного ip трафика от хоста 192.168.100.197 нас интересуют icmp echo сообщения:

1. ruleid 2 subruleid 2 – второе подправило второго правила
2. icmptype 8 icmptypecmp eq – все icmp type 8 пакеты
3. subruleprio asinrule – приоритет подправила такой же, как у правила

create filter rule map ifname eoa-23 stageid 1 ruleid 2

Применяем правило к конкретному интерфейсу (eoa-xx, eth-x)

modify filter rule entry ruleid 2 status enable

Включаем фильтр в работу

3. **Фильтр для привязки IP адреса к adsl порту (ATM PVC)**

create filter rule entry ruleid 2 action allow

Создаем разрешающее правило для нужного ip адреса:

1. action allow – принимать пакеты

create filter subrule ip ruleid 2 subruleid 1 srcipaddrfrom 192.168.100.207 srcaddrcmp eq dstaddrcmp any ipsrcaddrmask 0xffffffff

Создаем подправило, в котором указываем, что нас интересует трафик от хоста 192.168.100.207:

1. ruleid 2 subruleid 1 - первое подправило второго правила
2. srcipaddrfrom 192.168.100.207 – нижнее значение диапазона ip адресов источников трафика (т.к. srcaddrcmp равен eq, верхнее можно не указывать)
3. dstaddrcmp any – ip адрес назначения любой
4. ipsrcaddrmask 0xffffffff – маска источника 255.255.255.255

```
create filter rule entry ruleid 3 action drop
```

Создаем правило, запрещающее весь остальной трафик.

```
create filter subrule ip ruleid 3 subruleid 1 srcaddrcmp any dstaddrcmp any
```

Подправило, задающее весь трафик.

```
create filter rule map ifname eoa-23 stageid 1 ruleid 2
create filter rule map ifname eoa-23 stageid 1 ruleid 3
```

Применяем ранее созданные правила к конкретному интерфейсу (eoa-xx, eth-x)

```
modify filter rule entry ruleid 2 status enable
modify filter rule entry ruleid 3 status enable
```

Включаем фильтр в работу

Многоэтапная обработка пакетов

Иногда возникает необходимость осуществлять фильтрацию в несколько этапов. Например, первый этап может использоваться для отбрасывания неавторизованных пакетов, а на втором этапе может осуществляться приоритезация. Для того чтобы удовлетворять этим требованиям, фильтрация и приоритезация пакетов в DAS-3248 может быть разделена на несколько этапов. Этап, во время которого будет работать данное правило, определяется во время его приложения к конкретному интерфейсу.

Этапы выполняются согласно их StageID. Т.е. правила меньших этапов будут выполнены перед правилами этапов с большим значением StageID.

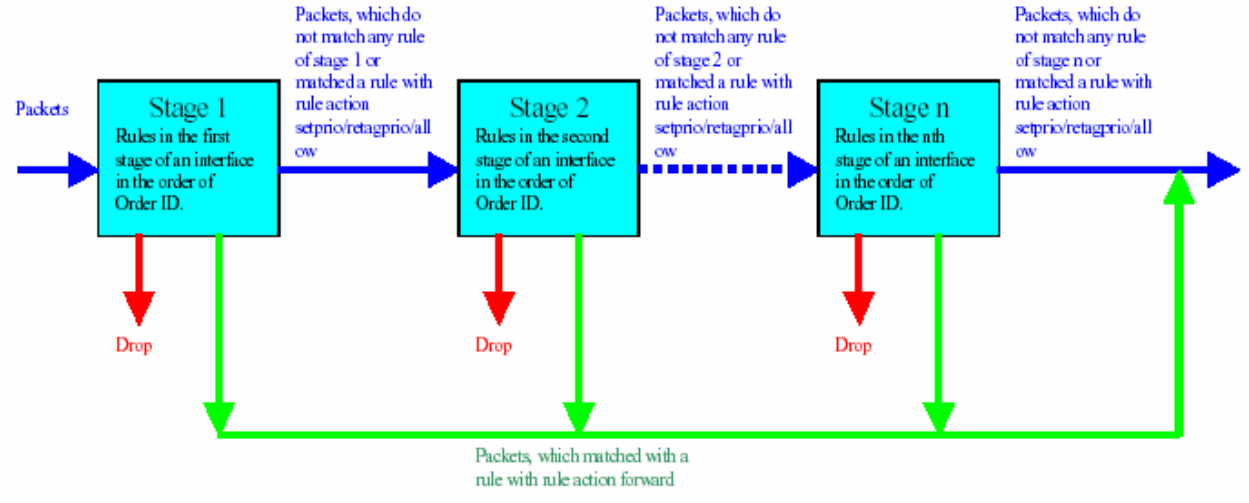

Рисунок 2: Многоэтапность обработки пакетов.

Пакет не будет передан на следующий этап если:

- на текущем этапе пакет соответствует правилу с действием Drop. В этом случае пакет будет отброшен, никаких правил к нему больше применяться не будет.

Пакет будет передан на следующий этап если:

- если текущий этап является последним, пакет будет поставлен в исходящую очередь
- пакет не совпал ни с одним из правил на текущем этапе
- пакет совпал с правилом allow. В этом случае к данному пакету на текущем этапе больше ни одного правила применено не будет.
- пакет совпал с правилом setprio или retagprio. В этом случае к данному пакету на текущем этапе больше ни одного правила применено не будет.

Максимальное число этапов во входящем и выходящем направлениях может быть различно.

Несколько действий одного правила (Action Map)

В DAS-3248 одно и то же правило может иметь несколько действий (allow, setprio, etc). Все эти действия будут выполнены в случае соответствия пакета данному правилу. Это очень полезно если над некоторым типом пакетов нужно произвести сразу несколько действий. Дополнительные действия ассоциируются с правилом уже после того, как оно создано. Каждое действие имеет свой orderindex, который определяет порядок выполнения всех действий, ассоциированных с правилом.

Причем:

- в первую очередь выполняются действия из action map в порядке возрастания их Order Index
- после этого выполняется действие, указанное при создании правила

Итак, для того, чтобы ассоциировать несколько действий с одним правилом нужно:

1. Создать правило Generic Filter
2. Создать соответствие действия правилу (rule to action map) для данного правила Generic фильтра:

```
create filter rule actionmap ruleid 1 orderindex 1 action copytocontrol
create filter rule actionmap ruleid 1 orderindex 2 action retagprio priority 2
```

3. Создать подправила данного правила
4. Включить правило
5. Приложить правило на интерфейс

Быстрое изменение последовательности правил

Пользователь DAS-3248 может заменить последовательность выполнения правил одного этапа путем выполнения всего одной команды. То же самое можно получить путем изменения значений OrderId всех правил. Однако в этом случае, в процессе изменения порядка следования правил, возможно, появление ошибочной их последовательности, которая может повлечь нарушения в работе сети. Для того чтобы этого избежать, в DAS-3248 пользователь может заменить целиком одну последовательность применения правил другой последовательностью.

Generic Filter Sequence – последовательность выполнения правил. Логически она состоит из Generic Filter Sequence Information (задает идентификатор данной последовательности) и Generic Filter Sequence entries (набор правил данной последовательности).

Для примера рассмотрим следующую ситуацию:

Пусть к интерфейсу eoa-2 приложены следующие правила во входящем направлении:

ruleid 1 Orderid 1
ruleid 3 Orderid 2
ruleid 5 Orderid 3
ruleid 6 Orderid 4

Требуется сменить данную последовательность на:

ruleid 5 Orderid 1
ruleid 2 Orderid 2
ruleid 7 Orderid 3

Для того чтобы сменить последовательность надо:

1. Создать sequence information путем задания sequence ID

   create filter seq info seqid 1

2. Создать членов искомой последовательности

   create filter seq entry seqid 1 ruleid 2 orderid 2
   create filter seq entry seqid 1 ruleid 5 orderid 1
   create filter seq entry seqid 1 ruleid 7 orderid 3

3. Применить получившуюся последовательность

   modify filter seq entry seqid 1 ifname eoa-2 stageid 1 seqdir in

Access Control List в DAS-3248

Access Control List позволяет задать пользователю список MAC адресов, которым будет разрешен или наоборот запрещен доступ. Данные списки могут быть созданы для каждого bridge порта в отдельности или для всего DSLAM-а в целом.

- Per port ACL: данный список создается для конкретного bridge порта. MAC адресам, указанным в этом списке, доступ разрешен.
- Global ACL: данный список создается целиком для устройства. Если выбрана опция Deny, MAC адресам, находящимся в этом списке доступ запрещен.

Per Port ACL

- Создается для конкретного bridge порта
- Все входящие пакеты, у которых source MAC адрес совпадает с одним из адресов, перечисленных в списке, имеют доступ к данному bridge порту. Все остальные входящие пакеты доступа к данному bridge порту не имеют, т.е. отбрасываются.
- Если список MAC адресов пуст, любые адреса имеют доступ на данный Bridge порт.
- Только unicast MAC адреса могут быть добавлены в список.

Global ACL

- Создается на глобальном уровне (целиком на DAS-3248)
- Всем пакетам, имеющим source MAC адрес, совпадающий с одним из адресов, перечисленных в списке, может быть запрещен доступ путем выбора опции Deny.
- Данный список может быть использован для отслеживания содержащихся в нем MAC адресов. В этом случае при перемещении MAC адреса на другой порт будет сгенерирован SNMP Trap.
- Только unicast MAC адреса могут быть добавлены в список.

Замечание: ACL применяется после классификаторов и правил Generic Filter.

Примеры использования Global ACL

- Добавление MAC адреса в глобальный список MAC адресов и включение опции deny:

```
create acl global macentry macaddr 00:11:95:90:26:46 deny enable
```

- Добавление MAC адреса в глобальный список MAC адресов и включение опции слежения:

```
create acl global macentry macaddr 00:11:95:90:26:46  track enable
```

- Добавление MAC адреса в глобальный список MAC адресов и включение обеих опций deny и слежения:

```
create acl global macentry macaddr 00:11:95:90:26:46 deny enable track
```

enable

- Создание bridge порта с включенными опциями Global ACL (по умолчанию данные опции включены)

  create bridge port intf ifname eoa-0 portid 1 aclGlbDenyApply enable aclGlobalTrackApply enable

Созданную запись в глобальном списке MAC адресов можно удалить командой:

delete acl global macentry macaddr xx:xx:xx:xx:xx:xx

например:

delete acl global macentry macaddr 00:11:95:90:26:46

Пример использования Per Port ACL

- Соответствующий bridge порт должен существовать до создания ACL
- Добавление MAC адреса в список для данного порта:

  create acl port macentry portid 2 macaddr 00:50:34:8D:AF:76:4A