

# Пояснения отказов отбрасывания пакета в ACI

## Содержание

[Введение](#)

[Управляемые объекты](#)

[Аппаратные типы счетчика сбросов](#)

[Передать](#)

[SECURITY\\_GROUP\\_DENY](#)

[VLAN\\_XLATE\\_MISS](#)

[ACL drop](#)

[SUP\\_REDIRECT](#)

[Ошибка](#)

[Буфер](#)

[Просмотр Stats отбрасывания в CLI](#)

[Управляемые объекты](#)

[Аппаратные счетчики](#)

[Лист](#)

[Позвоночник](#)

[Отказы](#)

[F11245 - входная пакетная скорость отбрасывания \(I2IngrPktsAg15min:dropRate\)](#)

[Описание:](#)

[Разрешение:](#)

[F100264 - пакетная скорость отбрасывания входного буфера \(eqptIngrDropPkts5min:bufferRate\)](#)

[Описание:](#)

[Разрешение:](#)

[F100696 - вход, передающий пакеты отбрасывания \(eqptIngrDropPkts5min:forwardingRate\)](#)

[Описание 1\) отбрасывания позвоночника](#)

[Разрешение 1\)](#)

[Описание 2\) окончные отбрасывания](#)

[Разрешение 2\)](#)

[Popor stats](#)

## Введение

Когда вы видите этот отказ, этот документ описывает каждый Тип отказа и процедуру. Во время Обычного Operaton Приложения Cisco Центральная Инфраструктура (ACI) Матрица администратор может видеть Отказы для определенных типов Отбрасывания пакета.

Внесенный Джозефом Ристэйно, Takuya Kishida, специалистами службы технической поддержки Cisco.

## Управляемые объекты

В ACI Cisco все отказы повышены под Управляемыми объектами (МО). Например, отказ "F11245 - входная пакетная скорость отбрасывания (I2IngrPktsAg15min:dropRate)" расценивает параметр *dropRate* в МО *I2IngrPktsAg15min*.

Этот раздел представляет часть **Управляемого объекта (МО)** в качестве примера отнесенные пакетные отказы отбрасывания.

	Пример	Описание	Типовой Paramte
I2IngrPkts	I2IngrPkts5min I2IngrPkts15min I2IngrPkts1h и т.д.)...	Это представляет статистику входящего пакета на VLAN в течение каждого периода	dropRate floodRate мультикастриров unicastRate
I2IngrPktsAg	I2IngrPktsAg15min I2IngrPktsAg1h I2IngrPktsAg1d и т.д.)...	Это представляет статистику входящего пакета на EPG, BD, VRF и т.д... Напр.) stats EPG представляет агрегацию stats VLAN, который принадлежит EPG	dropRate floodRate мультикастриров unicastRate
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d и т.д.)...	Это представляет входную пакетную статистику отбрасывания для интерфейса в течение каждого периода	*1 forwardingRate *1 коэффициент ошибок *1 bufferRate

\*1: Эти счетчики в eqptIngrDropPkts больше не используются от 1.3 (2) версии из-за - EX ограничение платформы в Прямом Отбрасывании с SUP\_REDIRECT.

На обратите внимание, что эта реализация могла быть изменена снова в будущем.

## Аппаратные типы счетчика сбросов

На коммутаторах Nexus 9000, работающих в Режиме ACI, существует 3 главных аппаратных счетчика по причине отбрасывания входного интерфейса на ASIC.

*dropRate* в *I2IngrPkts*, *I2IngrPktsAg* включает те счетчики. Три параметра (*forwardingRate*, коэффициент ошибок, *bufferRate*) в вышеупомянутой таблице для *eqptIngrDropPkts* представляют каждого три счетчика интерфейса.

### Передать

Передайте отбрасывания, пакеты, которые отброшены на блоке LookUp (LU) ASIC. В блоке LU решение о пересылке пакетов сделано на основе информации о заголовке пакета. Если решение состоит в том, чтобы отбросить пакет, Прямое Отбрасывание посчитано. Существует ряд причин, это может произойти, но давайте говорить о Главных:

#### SECURITY\_GROUP\_DENY

Отбрасывание из-за пропавших без вести договоров для разрешения связи.

Когда пакет вводит матрицу, коммутатор посмотрел на источник и целевой EPG, чтобы видеть, существует ли договор, который позволяет эту связь. Если источник и назначение будут в другом EPG's, и нет никакого договора, который позволяет этот тип пакета между ними, то коммутатор отбросит пакет и маркирует его как SECURITY\_GROUP\_DENY. Это инкрементно увеличивает Прямой Счетчик сбросов.

## VLAN\_XLATE\_MISS

Отбрасывание из-за несоответствующей VLAN.

Когда пакет вводит матрицу, коммутатор посмотрел на пакет, чтобы определить, позволяет ли конфигурация на порту этот пакет. Например, кадр вводит матрицу с меткой 802.1Q 10. Если коммутатор будет иметь VLAN 10 на порту, то это осмотрит содержание и сделает решение по перенаправлению на основе Получателя MAC. Однако, если VLAN 10 не будет на порту, то он отбросит его и маркирует его как VLAN\_XLATE\_MISS. Это инкрементно увеличит Прямой Счетчик сбросов.

Причина для "XLATE" или "Преобразовывает", то, потому что в ACI, окончательный коммутатор возьмет кадр с епсар 802.1Q и преобразует его в новую VLAN, которая будет использоваться для VXLAN и другой нормализации в матрице. Если кадр войдет с VLAN, не развернутой, то "трансляция" откажет.

## ACL drop

Отбрасывание из-за tcam SUP.

tcam SUP в коммутаторах ACI содержит специальные правила, которые будут применены поверх обычного решения по перенаправлению L2/L3. Правила в tcam SUP встроены и не конфигурируемы пользователем. Цель правил tcam SUP состоит в том, чтобы в основном обработать некоторые исключения или часть трафика уровня управления и не предназначенная, чтобы быть проверенной или проверенной пользователями. Когда пакет поражает правила tcam SUP, и правило состоит в том, чтобы отбросить пакет, отброшенный пакет посчитан как ACL\_DROP, и это инкрементно увеличит Прямой Счетчик сбросов. Когда это произошло, это обычно означает, что пакет собирается быть переданным против основных Передающих принципалов ACI.

Обратите внимание на то, что, даже при том, что название отбрасывания является ACL\_DROP, этот "ACL" не то же как обычный Список контроля доступа, который может быть настроен на автономных устройствах NX-OS или любых других routing/swtching устройствах.

## SUP\_REDIRECT

Это не отбрасывание.

SUP перенаправил пакет (т.е. CDP/LLDP/UDLD/BFD и т.д...) может быть посчитан, поскольку Прямое Отбрасывание даже думало, что пакет правильно обработан и передан к ЦП.

Это может произойти только в - EX платформа, такая как N9K-C93180YC-EX, который Они не должны быть посчитаны как "отбрасывание", однако, это из-за ограничений ASIC в - EX платформа.

## Ошибка

Когда коммутатор принимает недопустимый кадр, он отброшен как ошибка. Примеры этого включают кадры с FCS или ошибками CRC.

## Буфер

Когда коммутатор принимает кадр, и нет никаких буферных кредитов, доступных или для входа или для выхода, кадр будет отброшен с "Буфером". Это, как правило, намекает на перегрузку где-нибудь в сети. Ссылка, которая показывает отказ, могла быть полной, или, ссылка, содержащая назначение, может быть переполнена.

# Просмотр Stats отбрасывания в CLI

## Управляемые объекты

Secure Shell (SSH) к одному из APIC и выполняет следующие команды.

```
apic1# moquery-c l2IngrPktsAg15min
```

Это предоставит все экземпляры объектов для этого класса l2IngrPktsAg15min.

Вот пример с фильтром для запроса конкретного объекта. В данном примере фильтр должен показать только объект с dn атрибутов, который включает "tn-TENANT1/ap-APP1/epg-EPG1".

Также данный пример использует egrep для показа только обязательных атрибутов.

### Пример выходных данных 1: EPG противостоят объекту (l2IngrPktsAg15min) арендатора TENANT1, профиль приложения APP1, epg EPG1.

```
apic1# moquery -c l2IngrPktsAg15min -f 'l2.IngrPktsAg15min.dn*"tn-TENANT1/ap-APP1/epg-EPG1"' |
egrep 'dn|drop[P,R]|rep'
dn : uni/tn-TENANT1/ap-APP1/epg-EPG1/CDl2IngrPktsAg15min dropPer : 30 <--- number of drop packet
in the current periodic interval (600sec) dropRate : 0.050000 <--- drop packet rate =
dropPer(30) / periodic interval(600s) repIntvEnd : 2017-03-03T15:39:59.181-08:00 <--- periodic
interval = repIntvEnd - repIntvStart repIntvStart : 2017-03-03T15:29:58.016-08:00 = 15:39 -
15:29
= 10 min = 600 sec
```

Если вы знаете объект dn, или мы могли использовать другую опцию-d вместо-c для получения конкретного объекта.

### Пример выходных данных 2: EPG противостоят объекту (l2IngrPktsAg15min) арендатора TENANT1, профиль приложения APP1, epg EPG2.

```
apic1# moquery -d uni/tn-TENANT1/ap-APP1/epg-EPG2/CDl2IngrPktsAg15min | egrep 'dn|drop[P,R]|rep'
dn : uni/tn-jw1/BD-jw1/CDl2IngrPktsAg15min
dropPer : 30
```

```
dropRate      : 0.050000
repIntvEnd    : 2017-03-03T15:54:58.021-08:00
repIntvStart  : 2017-03-03T15:44:58.020-08:00
```

## Аппаратные счетчики

Если вы видите отказы или хотите проверить Отбрасывание пакета на switchports использование CLI, лучший способ сделать, это путем просмотра счетчиков платформы в аппаратных средствах. Большинство, но не все счетчики показывают с помощью **show interface**. 3 главных причины отбрасывания могут только быть просмотрены с помощью счетчиков платформы. Для просмотра их выполните эти шаги:

## Лист

SSH к листу и выполненный эти команды.

```
ACI-LEAF# vsh_lc
порт <X> внутренних счетчиков show platform module-1#
* где X представляет номер порта
```

## Пример выходных данных для ethernet 1/31:

```
ACI-LEAF# vsh_lc
vsh_lc
module-1#
module-1# show platform internal counters port 31
Stats for port 31
(note: forward drops includes sup redirected packets too)
IF          LPort          Input              Output
           LPort          Packets            Bytes             Packets           Bytes
eth-1/31    31    Total            400719            286628225         2302918           463380330
           Unicast        306610            269471065         453831            40294786
           Multicast         0                  0                 1849091           423087288
           Flood            56783             8427482           0                  0
           Total Drops      37327              0
           Buffer              0                  0
           Error              0                  0
           Forward          37327
           LB                  0
           AFD RED              0
           ----- snip -----
```

## Позвоночник

Поскольку коробка вводит позвоночник (N9K-C9336PQ), это - точно то же как Лист.

Для модульных позвоночников (N9K-C9504 и т.д...), необходимо сначала подключить карту частичного канала, прежде чем можно будет просмотреть счетчики платформы. SSH к позвоночнику и выполненный эти команды

```
ACI-SPINE# vsh
```

```
Attach module ACI-SPINE# <X>
```

```
порт <Y> внутренних счетчиков show platform module-2#.
```

\* где X представляет номер модуля для линейной карты,

требуется просмотреть

Y представляет номер порта

### Пример выходных данных для ethernet 2/1:

```
ACI-SPINE# vsh
Cisco iNX-OS Debug Shell
This shell should only be used for internal commands and exists
for legacy reasons. User should use ibash infrastructure as this
will be deprecated.
ACI-SPINE#
ACI-SPINE# attach module 2
Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Last login: Mon Feb 27 18:47:13 UTC 2017 from sup01-ins on pts/1
No directory, logging in with HOME=/
Bad terminal type: "xterm-256color". Will assume vt100.
module-2#
module-2# show platform internal counters port 1
Stats for port 1
(note: forward drops includes sup redirected packets too)
IF          LPort          Input              Output
           Packets      Bytes             Packets    Bytes
eth-2/1     1 Total        85632884  32811563575  126611414  25868913406
           Unicast      81449096  32273734109  104024872  23037696345
           Multicast   3759719   487617769    22586542   2831217061
           Flood          0          0             0           0
Total Drops 0
Buffer      0
Error       0
Forward     0
LB          0
AFD RED     0
----- snip -----
```

## Отказы

### F11245 - входная пакетная скорость отбрасывания (I2IngrPktsAg15min:dropRate)

#### Описание:

Когда пакеты Уровня 2 отброшены с "Прямом Отбрасыванием" причина, этот отказ может инкрементно увеличиться. С тех пор существует множество других причин,

наиболее распространенный:

На - EX платформа, такая как N9K-C93180YC-EX, существует ограничение, где пакеты L2, которые должны быть перенаправлены к ЦП (т.е. CDP/LLDP/UDLD/BFD, и т.д.), будут зарегистрированы как "Прямое Отбрасывание", а также копироваться к ЦП. Это происходит из-за ограничения ASIC, используемого в моделях EX Nexus 9000.

Из-за этого, когда много протоколов уровня управления включено на интерфейсе,

могут быть повышены эти отказы.

#### **Разрешение:**

С тех пор существует влияние по service, рекомендации по оптимальному использованию должны увеличить порог для отказа как показано в Пороговом разделе Stats. Чтобы сделать это, см. инструкции в Пороге Stats.

### **F100264 - пакетная скорость отбрасывания входного буфера (eqptIngrDropPkts5min:bufferRate)**

#### **Описание:**

Этот отказ может инкрементно увеличиться, когда пакеты отбрасываются на порту с причиной "Буфер" , Как упомянуто выше, это, как правило, происходит, когда существует перегрузка на интерфейсе или во входе или в выходном направлении.

#### **Разрешение:**

Этот отказ представляет фактически отброшенные пакеты в среде из-за перегрузки. Отброшенные пакеты могут вызывать проблемы с приложениями, работающими в матрице ACI. Администраторы сети должны изолировать поток пакетов и определить, происходит ли перегрузка из-за неожиданных трафиков, неэффективного распределения нагрузки, и т.д.; или ожидаемое использование на тех портах.

### **F100696 - вход, передающий пакеты отбрасывания (eqptIngrDropPkts5min:forwardingRate)**

**Примечание:** При начале в версии 1.3 (2) Прямые Отбрасывания удалены из Объекта eqptIngrDropPkts5min, таким образом, этот отказ не должен быть замечен для этой проблемы.

Этот отказ вызван несколькими сценариями. Наиболее распространенный:

#### **Описание 1) отбрасывания позвоночника**

Когда пакет ARP или IP передан позвоночнику для поиска прокси, и конечная точка неизвестна в матрице, специальный подобранный пакет будет генерироваться и передаваться ко всем листам на соответствующем BD

адрес группы многоадресной рассылки. Это инициирует запрос ARP от каждого листа в Домене моста (BD) для обнаружения конечной точки. Из-за ограничения, подобранный пакет, полученный листом, также отражен

назад в матрицу и триггеры передающее отбрасывание на ссылке позвоночника. Прямое Отбрасывание только инкрементно увеличено на Аппаратных средствах Позвоночника Поколения 1.

#### **Разрешение 1)**

Так как вы знаете, что проблема вызвана устройством, передав Трафик с конкретным адресом Unkown в Матрицу ACI, необходимо выяснить, какое устройство вызывает это, и посмотрите, можно ли предотвратить его. Это обычно вызывается устройствами, которые просматривают или зондируют для IP-адресов на подсетях для мониторинга целей. Для обнаружения то, что IP передает этому трафику, SSH на лист, который связан с интерфейсом позвоночника показ отказа.

Оттуда, можно выполнить эту команду для наблюдения IP - адреса источника (sip), который инициирует подобранный пакет:

```
ACI-LEAF# show ip arp internal event-history event | grep glean | grep sip | more
[116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip
= 192.168.20.100;info = Rece
ived glean packet is an IP packet
[116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip
= 192.168.20.100;info = Rece
ived glean packet is an IP packet
[116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip
= 192.168.20.100;info = Rece
ived glean packet is an IP packet
[116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip
= 192.168.20.100;info = Rece
ived glean packet is an IP packet
```

Оттуда, можно заняться расследованиями, почему 192.168.21.150 передает этот трафик в матрицу, и посмотрите, можно ли смягчить его оттуда.

## Описание 2) оконечные отбрасывания

Если этот отказ замечен на оконечном интерфейсе, наиболее вероятный casue происходит из-за упомянутых отбрасываний SECURITY\_GROUP\_DENY.

## Разрешение 2)

На листе вы поддерживаете, журнал пакетов запретил должный заключить нарушения. Этот журнал не перехватывает всех их для защиты ресурсов ЦПУ, однако, он все еще предоставляет вас огромное количество журналов.

Получить журналы, что вы хотите, если интерфейс отказ повышен на, - часть port-channel, необходимо использовать эту команду и grep для port-channel. В противном случае можно использовать физический интерфейс:

Этот журнал может быть быстро перевернут в зависимости от суммы отбрасываний договора.

```
ACI-LEAF# show logging ip access-list internal packet-log deny | grep port-channel2 | more
[ Sun Feb 19 14:16:12 2017 503637 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3, SPort: 0, DPort: 0, Src
Intf: port-channel2, Pr
oto: 1, PktLen: 98
[ Sun Feb 19 14:16:12 2017 502547 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3, SPort: 0, DPort: 0, Src
Intf: port-channel2, Pr
oto: 1, PktLen: 98
[ Sun Feb 19 14:16:12 2017 500387 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
```



```

Id: 59, SMac: 0x8c604
f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3, SPort: 0, DPort: 0, Src
Intf: port-channel2, Pr
oto: 1, PktLen: 98
[ Sun Feb 19 14:16:12 2017 499779 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3, SPort: 0, DPort: 0, Src
Intf: port-channel2, Pr
oto: 1, PktLen: 98
[ Sun Feb 19 14:16:12 2017 499624 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3, SPort: 0, DPort: 0, Src
Intf: port-channel2, Pr
oto: 1, PktLen: 98

```

В этом случае, 192.168.21.150 пытается передать сообщения ICMP (Протокол "IP" номер 1) к 192.168.20.3. Однако нет никакого договора между 2 EPG's, которые позволяют ICMP, таким образом, отброшен пакет. Если ICMP, как предполагается, позволен, договор может быть добавлен между двумя EPG's.

## Порог stats

В этом разделе описывается изменить порог для объекты статистики, которые могли потенциально повысить отказ against счетчик сбросов.

Следующий пример должен изменить порог для Прямого *Понижения eqptIngrDropPkts*.

1. Перейдите к **Матрице> Оптоволоконная Политика> Контролирующая Политика> По умолчанию> Политика Сбора статистических данных**.
2. От выпадающего **Объекта мониторинга** выберите **Layer 1 Physical Interface Configuration (I2. PhysIf)** и **Тип Stats**, выберите **Ingress Drop Packets**

The screenshot shows the Cisco Fabric Manager interface. The top navigation bar includes System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, and Operations. The main content area is titled 'Stats Collection Policies'. A table lists the configuration for a specific policy:

Monitoring Object	Stats Type
Layer 1 Physical Interface Configuration (I1.Ph)	Ingress Drop Packets

Below this table, there are two columns: Granularity and Admin State. The Granularity is set to 5 Minute, and the Admin State is inherited.

3. Щелкните + затем, чтобы сконфигурировать пороги

Inventory | Fabric Policies | Access Policies

### Stats Collection Policies

Monitoring Object: Layer 1 Physical Interface Configuration (1.Ph) Stats Type: Ingress Drop Packets

Granularity	Admin State	History Retention Period	Config Thresholds
5 Minute	inherited	inherited	

#### 4. Отредактируйте порог для сбросов буфера

### Thresholds For Collection 5 Minute

#### Config Thresholds

Property	Edit Threshold
Ingress Buffer Drop Packets rate	
Ingress Forwarding Drop Packets rate	
Ingress Error Drop Packets rate	

CLOSE

5. Рекомендация состоит в том, чтобы отключить верхние пороги, чтобы сконфигурироваться для важного, главного, незначительного, и предупреждение для передачи уровня сброса.



Ingress Forwarding Drop Packets rate

Normal Value: 0

Threshold Direction: **Both** Rising Falling

- Rising Thresholds to Config:
- Critical
  - Major
  - Minor
  - Warning

CHECK ALL UNCHECK ALL

- Falling Thresholds to Config:
- Critical
  - Major
  - Minor
  - Warning

CHECK ALL UNCHECK ALL

Rising

	Set	Reset
Critical	10000	9000
Major	5000	4900
Minor	500	490
Warning	10	9

Falling

	Reset	Set
Warning	0	0
Minor	0	0
Major	0	0
Critical	0	0

SUBMIT

CANCEL