Содержание

Дополнительные сведения

Введение

В этом документе описаны причины высокой загрузки ЦП коммутаторов серии Cisco Catalyst 6500/6000 и систем, основанных на системе виртуальной коммутации (VSS) 1440. **Как и маршрутизаторы Cisco, коммутаторы используют команду show processes cpu, чтобы показать загрузку ЦП для процессора механизма управления коммутацией. Однако из-за различий в архитектуре и в механизмах пересылки между маршрутизаторами и коммутаторами Cisco типовые выходные данные команды show processes cpu существенно различаются.** Значение выходных данных отличается также. Этот документ разъясняет эти различия и описывает загрузку ЦПУ на коммутаторах и как интерпретировать выходные данные **команды show processes cpu**.

Примечание: В этом документе слова "коммутатор" и "коммутаторы" обращаются к коммутаторам Catalyst 6500/6000.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, представленные в этом документе, основаны на версиях программного и аппаратного обеспечения для коммутаторов Catalyst 6500/6000 и систем, основанных на виртуальной системе коммутации (VSS) 1440.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Примечание: Поддерживаемое программное обеспечение для Системы виртуальной коммутации (VSS) 1440 базирующихся систем является релизом 12.2 программного обеспечения Cisco IOS (33) SXH1 или позже.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Различия между ПО для CatOS и Cisco IOS

Программное обеспечение CatOS в модуле Supervisor Engine и программное обеспечение Cisco IOS на плате многоуровневой коммутации (MSFC) (гибридной): Можно использовать образ CatOS в качестве программного обеспечения системы, чтобы запустить процессор управляющего модуля на коммутаторах Catalyst 6500/6000. Если установлен

дополнительный модуль MSFC, для его запуска используется отдельный образ программного обеспечения Cisco IOS.

Программное обеспечение Cisco IOS для модуля Supervisor Engine и для платы MSFC (встроенной): Можно использовать один образ программного обеспечения Cisco IOS в качестве системного ПО для Supervisor Engine и MSFC на коммутаторах Catalyst 6500/6000.

Примечание: См. раздел Сравнение операционных систем Cisco Catalyst и Cisco IOS для коммутаторов серии Cisco Catalyst 6500 для получения более полной информации.

Общие сведения о загрузке ЦП в коммутаторах Catalyst 6500/6000

Маршрутизаторы на основе ПО Cisco используют программное обеспечение для обработки и маршрутизации пакетов. Загрузка ЦП в маршрутизаторе Cisco повышается при увеличении количества пакетов, обрабатываемых и маршрутизируемых маршрутизатором. **Таким образом, команда show processes cpu может предоставить достаточно точное отображение загрузки по обработке трафика на маршрутизаторе.**

Коммутаторы Catalyst 6500/6000 используют ЦП по-другому. Эти коммутаторы пересылают кадры в оборудовании, а не в программном обеспечении. Таким образом, в процессе принятия решения о пересылке или коммутации для большинства кадров, проходящих через коммутатор, ЦП механизма управления участия не принимает.

В коммутаторах Catalyst 6500/6000 Switches имеются два ЦП. Один ЦП является процессором механизма управления и называется процессором сетевого управления (NMP) или процессором коммутации (SP). Другой ЦП является процессором механизма маршрутизации 3 уровня и называется MSFC или процессором маршрутизации (RP).

Процессор SP выполняет следующие функции:

- Принимает участие в изучении MAC-адресов и их устаревания**Примечание:** Изучение MAC-адресов также называют установкой тракта.
- Запускает протоколы и процессы, обеспечивающие управление сетьюНапример, протокол связующего дерева (STP), протокол обнаружения Cisco (CDP), транкинговый протокол VLAN (VTP), динамический транкинговый протокол (DTP) и протокол агрегации портов (PAgP).
- Обрабатывает трафик управления сетью, предназначенный для ЦП коммутатораНапример, трафик протоколов Telnet, HTTP и SNMP.

Процессор RP выполняет следующие функции:

- Строит и обновляет таблицы маршрутизации 3 уровня и протокола разрешения адресов (ARP)
- Генерирует таблицы базы данных пересылки (FIB) CEF и таблицы смежности и загружает их на плату поддержки политик (PFC)
- Обрабатывает трафик управления сетью, предназначенный для RPНапример, трафик протоколов Telnet, HTTP и SNMP.

Ситуации и функции, которые переключают трафик на

программное обеспечение

Пакеты, предназначенные для коммутатора

Любой пакет, предназначенный для коммутатора, направляется на программное обеспечение. Такие пакеты включают:

- Пакеты управленияПакеты управления, полученные для протоколов STP, CDP, VTP, HSRP, PAgP, LACP и UDLD.
- Обновления протокола маршрутизацииПримерами таких протоколов являются RIP, EIGRP, BGP и OSPF.
- Трафик протокола SNMP, предназначенный для коммутатора
- Трафик протоколов Telnet и SSH, поступающий на коммутатор.Высокая загрузка CPU ultilization из-за SSH замечена как:Включайте эти команды в сценарий EEM, чтобы проверить, что количество Сеансов SSH установило, когда ЦП идет высоко:show usersshow line
- Ответы ARP на ARP-запросы

Пакеты и условия, требующие особой обработки

В этом списке представлены особые типы пакетов и условия, которые принудительно направляют пакеты на обработку программным обеспечением:

- Пакеты с IP-параметрами, с истекшим сроком жизни (TTL) или с инкапсуляцией, отличной от ARPA
- Пакеты со специальной обработкой, такой как туннелирование
- Фрагментация IP
- Пакеты, для которых требуются сообщения протокола ICMP от RP или SP
- Неудачная проверка максимального размера пакета (MTU)
- Пакеты с ошибками IP, включающими ошибки контрольной суммы и длины IP
- Если входящие пакеты возвращают побитовую ошибку (например одноразрядную ошибку SBE), то они отправляются на ЦП для программной обработки и исправляются. Система выделяет для них буфер и использует ресурс ЦП для их исправления.
- Если в пути потока трафика присутствует PBR и рефлексивный список доступа, пакет коммутируется программно, для чего требуется дополнительный цикл ЦП.
- Одинаковый смежный интерфейс
- **Пакеты с неудачной проверкой пересылки по обратному пути (RPF) "ошибка rpf**
- Подбор/получениеПодбор относится к пакетам, требующим разрешения ARP, а получение — к пакетам, встречающимся в случае получения.
- Трафик протокола IPX, коммутируемый программно в модуле Supervisor Engine как в Cisco IOS, так и в CatOSТрафик протокола IPX также коммутируется программно в Supervisor Engine 2/Cisco IOS Software, но коммутируется аппаратно в Supervisor Engine 2/CatOS. Трафик протокола IPX коммутируется аппаратно в Supervisor Engine 1A для обеих операционных систем.
- Трафик протокола AppleTalk
- Условия использования полностью аппаратных ресурсовЭти ресурсы включают FIB, ассоциативное запоминающее устройство (CAM) и троичное ассоциативное

запоминающее устройство (TCAM).

Функции, основанные на списках управления доступом

- Трафик, отклоненный списком управления доступом (ACL), с включенной функцией недостижимостей ICMP**Примечание:** !--- Это стандартный вариант.Некоторые пакеты, отклоненные ACL, доходят до MSFC, если включены недостижимости IP. Пакеты, для которых требуются недостижимости ICMP, проходят со скоростью, настраиваемой пользователем. По умолчанию скорость равна 500 пакетам в секунду (п/сек).
- Фильтрация IPX, учитывающая неподдерживаемые параметры, такие как узел-источникВ модуле Supervisor Engine 720 обработка трафика IPX 3 уровня всегда выполняется программно.
- **Записи контроля доступа (ACE), которым требуется регистрация, с ключевым словом log**Это относится к функциям регистрации ACL и VLAN ACL (VACL). ACE в том же ACL, которым не требуется регистрация, по-прежнему обрабатываются аппаратно. Модуль Supervisor Engine 720 с PFC3 поддерживает ограничение скорости пакетов, которые перенаправляются на MSFC для регистрации ACL и VACL. Модуль Supervisor Engine 2 поддерживает ограничение скорости пакетов, которые перенаправляются на MSFC для регистрации VACL. Поддержка регистрации ACL в модуле Supervisor Engine 2 запланирована для Cisco IOS Software версии 12.2S.
- **Трафик, маршрутизируемый политикой, с использованием параметров match length, set ip precedence или других неподдерживаемых параметровПараметр set interface поддерживается программно. Однако параметр set interface null 0 является исключением.** Этот трафик обрабатывается аппаратно в модуле Supervisor Engine 2 с PFC2 и Supervisor Engine 720 с PFC3.
- ACL с маршрутизацией, отличной от IP и IPX (RACL)RACL, отличные от IP, применяются ко всем механизмам управления. RACL, отличные от IPX, применяются только к Supervisor Engine 1a с PFC и Supervisor Engine 2 с PFC2.
- Широковещательный трафик, отклоненный в RACL
- Трафик, отклоненный при проверке в однонаправленной RPF (uRPF), ACL ACETакая проверка uRPF применяется к Supervisor Engine 2 с PFC2 и Supervisor Engine 720 с PFC3.
- Прокси-сервер аутентификацииТрафик, предназначенный для прокси-сервера аутентификации, может быть ограничен по скорости в Supervisor Engine 720.
- IPsec ПО Cisco IOSТрафик, предназначенный для шифрования Cisco IOS, может быть ограничен по скорости в Supervisor Engine 720.

Функции, основанные на NetFlow

Функции, основанные на NetFlow, которые описываются в этом разделе, применяются только к Supervisor Engine 2 и Supervisor Engine 720.

- Для функций, основанных на NetFlow, необходима программная обработка первого пакета в потоке. После того, как первый пакет потока достигает программного обеспечения, последующие пакеты того же потока коммутируются аппаратно.Такая обработка потока применяется к рефлексивным ACL, к протоколу WCCP и к балансировке нагрузки сервера IOS (SLB).**Примечание:** На Supervisor Engine 1, возвратном ACL, полагаются на динамические множества технических разделов для

создания ярлыков аппаратного обеспечения для отдельного потока. Принцип тот же: первый пакет потока обрабатывается программно. Последующие пакеты этого потока коммутируются аппаратно.
- С применением функции перехвата TCP трехстороннее подтверждение и завершение сеанса обрабатываются программно. Остальной трафик обрабатывается аппаратно.**Примечание:** Синхронизируйтесь (SYN), SYN подтверждают (ACK SYN), и пакеты ACK включают трехэтапное установление связи. Завершение сеанса происходит при поступлении пакета завершения (FIN) или сброса (RST).
- При применении преобразования сетевых адресов (NAT) трафик обрабатывается следующим образом:Для Supervisor Engine 720:Трафик, требующий NAT, обрабатывается аппаратно после первоначального преобразования. Преобразование первого пакета потока выполняется программно, а последующие пакеты этого потока коммутируются аппаратно. Для пакетов TCP в таблице NetFlow создается аппаратный ярлык после завершения трехстороннего подтверждения TCP.B Supervisor Engine 2 и Supervisor Engine 1:Весь траффик, требующий NAT, коммутируется программно.
- Контроль доступа на основе содержимого (CBAC) использует ярлыки NetFlow для классификации трафика, требующего проверки. После этого CBAC отправляет на программную обработку только такой трафик. CBAC является исключительно программной функцией; трафик, подлежащий проверке, не коммутируется аппаратно.**Примечание:** Трафик, который подлежит проверке, может быть с ограниченной скоростью на модуле управления Supervisor Engine 720.

Многоадресный трафик

- Отслеживание протокола многоадресной передачи (PIM)
- Отслеживание протокола управления группами Internet (IGMP) (TTL = 1)Этот трафик должен быть предназначен для маршрутизатора.
- Отслеживание протокола обнаружения многоадресного прослушивателя (MLD) (TTL = 1)Этот трафик должен быть предназначен для маршрутизатора.
- Отсутствие FIB
- Многоадресные пакеты для регистрации, которые имеют прямую связь с многоадресным источникомЭти пакеты туннелируются к точке встречи.
- Многоадресный IP версии 6 (IPv6)

Другие функции

- Сетевое распознавание приложений (NBAR)
- Проверка ARP, только в CatOS
- Функция безопасности порта, только в CatOS
- Отслеживание DHCP

Ситуации IPv6

- Пакеты с заголовком, содержащим параметры на уровне переходов
- Пакеты с адресами назначения IPv6, совпадающими с адресами маршрутизаторов
- Пакеты, не прошедшие проверку принудительного попадания в область
- Пакеты, превысившие MTU выходной линии

- Пакеты с TTL меньшим или равным 1
- Пакеты, у которых входная VLAN идентична выходной VLAN
- IPv6 uRPFURPF выполняется программно для всех пакетов.
- Рефлексивные ACL IPv6Рефлексивные ACL обрабатываются программно.
- Префиксы 6-4 для туннелей протокола ISATAP IPv6Это туннелирование обрабатывается программно. Весь остальной трафик, входящий в туннель ISATAP, коммутируется аппаратно.

Процесс LCP Schedular и модуль DFC

(DFC) lcp schedular, , . Процесс LCP schedular является частью кода микропрограммы. На всех модулях, не требующих DFC, микропрограмма работает на особом процессоре, называемом процессором линейной платы (LCP). Этот процессор используется для программирования оборудования ASIC и для обмена данными с центральным модулем управления.

lcp schedular . , lcp schedular . Это не влияет на производительность системы с точки зрения высокой загрузки ЦП. Процесс просто захватывает все неиспользуемые циклы ЦП до тех пор, пока они не потребуются процессу с более высоким приоритетом.

```
DFC#show process cpuPID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process  22
0         1      0   0.00%  0.00%  0.00%   0 SCP ChilisLC Lis   23           0         1      0
0.00%  0.00%  0.00%   0 IPC RTTYC Messag   24           0         9      0   0.00%  0.00%  0.00%
0 ICC Slave LC Req   25           0         1      0   0.00%  0.00%  0.00%   0 ICC Async mcast
26           0         2      0   0.00%  0.00%  0.00%   0 RPC Sync           27           0
1      0   0.00%  0.00%  0.00%   0 RPC rpc-master     28           0         1      0   0.00%
0.00%  0.00%   0 Net Input          29           0         2      0   0.00%  0.00%  0.00%   0
Protocol Filteri   30           8       105     76   0.00%  0.00%  0.00%   0 Remote Console P
31          40      1530     26   0.00%  0.00%  0.00%   0 L2 Control Task    32          72
986     73   0.00%  0.02%  0.00%   0 L2 Aging Task      33           4        21    190   0.00%
0.00%  0.00%   0 L3 Control Task    34          12       652     18   0.00%  0.00%  0.00%   0
FIB Control Task   35        9148       165  55442   1.22%  1.22%  1.15%   0 Statistics Task
36           4       413      9   0.00%  0.00%  0.00%   0 PFIB Table Manag   37      655016
64690036     10  75.33% 77.87% 71.10%   0 lcp schedular      38           0       762      0
0.00%  0.00%  0.00%   0 Constellation SP
```

Общие причины и решения проблем высокой загрузки ЦП

Недостижимости IP

Если группа доступа отклоняет пакет, MSFC отправляет сообщения о недостижимости ICMP. Это действие происходит по умолчанию.

С включенной по умолчанию командой ip unreachables механизм управления сбрасывает большинство отклоненных пакетов на аппаратную обработку. После этого механизм управления отправляет только небольшое количество пакетов с максимальной скоростью 10 п/сек на MSFC для сброса. Это действие генерирует сообщения о недостижимостях ICMP.

Сброс отклоненных пакетов и генерация сообщений о недостижимостях ICMP создают нагрузку на ЦП MSFC. **Для устранения этой нагрузки можно выполнить команду конфигурации интерфейса no ip unreachables.** Эта команда отключает сообщения о недостижимостях ICMP, что позволяет сбрасывать на аппаратную обработку все пакеты,

отклоненные группой доступа.

Сообщения о недостижимостях ICMP не отправляются, если пакет отклонен VACL.

Преобразования NAT

NAT использует и аппаратную и программную пересылку пакетов. Первоначальная установка преобразований NAT должна выполняться программно, а дальнейшая пересылка выполняется аппаратно. NAT также использует таблицу Netflow (максимум 128 кБ). Поэтому если таблица Netflow заполнена, коммутатор начнет применять программную пересылку NAT. Обычно это случается при высоких всплесках трафика и приводит к увеличению загрузки ЦП коммутатора 6500.

Использование табличного пространства CEF FIB в кэш-таблице потока

Supervisor Engine 1 имеет кэш-таблицу потока, которая поддерживает 128000 записей. Однако по соображениям эффективности алгоритма хэширования эти записи адресуются от 32000 до 120000. В Supervisor Engine 2 таблица FIB генерируется и программируется в PFC. Таблица содержит до 256000 записей. Supervisor Engine 720 с PFC3-BXL поддерживает до 1000000 записей. После превышения этого пространства пакеты начинают коммутироваться программно. Это может вызвать высокую загрузку ЦП в RP. Чтобы проверить число маршрутов в таблице CEF FIB, используйте следующие команды:

```
Router#show processes cpuCPU utilization for five seconds:  99.26%                      one
minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs    5Sec
1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- --- -----
----------1   0           0          0          0.74%   0.00%   0.00% -2  Kernel and Idle2   2
245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0           1          0
0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0          0.00%   0.00%
0.00% -2  L2L3PatchRev   5   653         11737      1000       0.00%   0.00%   0.00% -2  SynDi!-
-- Output is suppressed.26 10576 615970 1000 0.00% 0.00% 0.00% 0 L3Aging 27 47432 51696 8000
0.02% 0.00% 0.00% 0 NetFlow 28 6758259 1060831 501000 96.62% 96.00% 96.00% 0   Fib            29
0           1          0          0.00%   0.00%   0.00% -2  Fib_bg_task  !--- Output is
suppressed.CATOS% show mls cefTotal L3 packets switched:           124893998234Total L3 octets
switched:          530193789624 95Total route entries:                       112579  IP route
entries:                        112578  IPX route entries:                           1  IPM
route entries:                             0IP load sharing entries:                   295IPX
load sharing entries:                        0Forwarding entries:
112521Bridge entries:                                 56Drop entries:
2IOS% show ip cef summaryIP Distributed CEF with switching (Table Version 86771423), flags=0x0
112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)  112567 leaves, 6888 nodes, 21156688
bytes, 86771426inserts, 86658859invalidations  295 load sharing elements, 96760 bytes, 112359
references  universal per-destination load sharing algorithm, id 8ADDA64A  2 CEF resets, 2306608
revisions of existing leaves  refcounts:  1981829 leaf, 1763584 node!--- You see these messages
if the TCAM space is exceeded:%MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM exception, Some entries will
be software switched%MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM exception cleared, all CEF entries
will be hardware switched
```

В Supervisor Engine 2 число записей FIB уменьшается наполовину, если настроена проверка RPF на интерфейсах. Такая настройка может привести к программной коммутации большинства пакетов и, в результате, к высокой загрузке ЦП.

Чтобы решить проблему высокой загрузки ЦП, включите суммирование маршрутов. Суммирование маршрутов может минимизировать задержку в сложной сети, уменьшая нагрузки на ЦП, требования к памяти и требование полосы пропускания.

Дополнительные сведения об использовании и оптимизации TCAM см. в разделе Общие

сведения по ACL в коммутаторах серии Catalyst 6500.

Оптимизированное ведение журнала ACL

Оптимизированное ведение журнала ACL (OAL) обеспечивает аппаратную поддержку для ведения журнала ACL. Если OAL не настроено, обработка пакетов, требующих регистрации в журнале, выполняется полностью программно в MSFC3. OAL разрешает или сбрасывает пакеты на аппаратную обработку в PFC3. OAL использует оптимизированную процедуру отправки данных на MSFC3 для генерации сообщений регистрации.

Примечание: Для получения информации о OAL обратитесь к *Оптимизированной Регистрации ACL с* разделом *PFC3* Понимания Поддержки ACL Cisco IOS.

Ограничение скорости пакетов для ЦП

В Supervisor Engine 720 ограничители скороти могут управлять скоростью, с которой пакеты могут поступать на программную обработку. Такое управление скоростью помогает предотвратить атаки, нацеленные на отказ в обслуживании (DoS). Несколько таких ограничителей скорости также можно использовать и в Supervisor Engine 2:

```
Router#show mls rate-limit   Rate Limiter Type       Status     Packets/s   Burst---------------
------   ----------   ---------   -----         MCAST NON RPF   Off                -       -
MCAST DFLT ADJ   On              100000     100      MCAST DIRECT CON   Off                -
-        ACL BRIDGED IN   Off                  -       -       ACL BRIDGED OUT   Off
-       -           IP FEATURES   Off                -       -          ACL VACL LOG   On
2000       1           CEF RECEIVE   Off                  -       -             CEF GLEAN   Off
-       -      MCAST PARTIAL SC   On             100000     100        IP RPF FAILURE   On
500      10           TTL FAILURE   Off                -       -ICMP UNREAC. NO-ROUTE   On
500      10ICMP UNREAC. ACL-DROP   On                500      10         ICMP REDIRECT   Off
-       -           MTU FAILURE   Off                -       -           LAYER_2 PDU   Off
-       -            LAYER_2 PT   Off                -       -             IP ERRORS   On
500      10           CAPTURE PKT   Off                -       -            MCAST IGMP   Off
-       -Router(config)#mls rate-limit ?  all        Rate Limiting for both Unicast and
Multicast packets  layer2     layer2 protocol cases  multicast  Rate limiting for Multicast
packets  unicast    Rate limiting for Unicast packets
```

Например:

```
Router(config)#mls rate-limit layer2 l2pt 3000
```

Чтобы ограничить скорость всех пакетов, отправляемых CEF на MSFC, выполните команду, приведенную в этом примере:

```
Router(config)#mls ip cef rate-limit 50000
```

Чтобы уменьшить число пакетов, отправляемых на ЦП из-за TTL=1, выполните следующую команду:

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

Например, это - выходные данные **перехвата netdr**, который показывает, что TTL IPv4 равняется 1:

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

Причиной высокой загрузки ЦП также могут быть пакеты с TTL=1, которые доходят до ЦП. Чтобы ограничить число пакетов, проходящих на ЦП, настройте аппаратный ограничитель скорости. Ограничители скорости могут ограничивать скорость пакетов, которые проходят

из пути аппаратных данных на путь программных данных. Ограничители скорости защищают путь программных данных от перегрузки, сбрасывая трафик, превышающий настроенную скорость. **Ограничение скорости настраивается с помощью команды mls rate-limit all ttl-failure.**

Физическое слияние VLAN из-за неправильной проводки кабелей

Высокая загрузка ЦП также может быть результатом слияния двух или более VLAN из-за неправильной проводки кабелей. Высокая загрузка ЦП может возникнуть, если на тех портах, через которые происходит слияние VLAN, отключен протокол STP.

Чтобы решить эту проблему, определите ошибки проводки кабелей и исправьте их. Если это не противоречит вашим требованиям, вы также можете включить протокол STP на соответствующих портах.

Широковещательный шторм

Широковещательный шторм возникает в LAN, когда широковещательные или многоадресные пакеты переполняют LAN, что создает избыточный трафик и ухудшает производительность сети. Широковещательный шторм может быть вызван ошибками в реализации стека протокола или в конфигурации сети.

Архитектура платформы серии Catalyst 6500 такова, что широковещательные пакеты всегда сбрасываются только на программном уровне.

Подавление широковещания предотвращает разрыв интерфейсов LAN из-за широковещательного шторма. Подавление широковещания использует фильтрацию, которая измеряет широковещательную активность в LAN с периодичностью в 1 секунду и сравнивает результат измерений с предопределенным пороговым значением. При достижении порогового значения дальнейшая широковещательная активность подавляется на протяжении заданного периода времени. Подавление широковещания по умолчанию отключено.

Примечание: VRRP, колеблющийся от резервной копии до ведущего устройства, вызванного широковещательными штормами, мог бы вызвать высокую загрузку ЦП.

Чтобы понять, как работает подавление широковещания и как включить эту функцию, см. раздел:

- Настройка подавления широковещания (системное ПО Cisco IOS)
- Настройка подавления широковещания (системное ПО CatOS)

Отслеживание адресов следующего перехода BGP (процесс сканера BGP)

Процесс сканера BGP просматривает таблицу BGP и подтверждает достижимость следующих узлов. Этот процесс также проверяет условные объявления, чтобы определить, должен ли BGP объявлять префиксы состояния, и проводит разгрузку маршрутов. По умолчанию процесс выполняет сканирование каждые 60 секунд.

Кратковременные высокие загрузки ЦП могут быть предсказуемы, если процесс сканера BGP выполняется на маршрутизаторе, несущем большую таблицу Интернет-

маршрутизации. Раз в минуту сканер BGP просматривает таблицу базы данных маршрутизации BGP (RIB) и выполняет важные задачи обслуживания. Выполняются следующие действия:

- Проверка следующего перехода, на который ссылается таблица BGP маршрутизатора
- Проверка доступности устройств следующего перехода

Таким образом, большая таблица BGP занимает равнозначно большой промежуток времени для прохождения и проверки. Процесс сканера BGP просматривает таблицу BGP для обновления структур данных, а таблицу маршрутизации — для перераспределения маршрутов. Эти таблицы хранятся в памяти маршрутизатора раздельно. Обе таблицы могут быть очень большими и, следовательно, потреблять циклы ЦП.

Дополнительные сведения о загрузке ЦП процессом сканера BGP см. в разделе Высокая загрузка ЦП сканером BGP главы Устранение проблем высокой загрузки ЦП, вызванной процессами сканера BGP или маршрутизатора BGP.

Дополнительные сведения о функции отслеживания адреса следующего перехода BGP и о процедуре включения/отключения и настройки интервала сканирования см. в разделе Поддержка отслеживания адреса следующего перехода BGP.

Многоадресный не-RPF трафик

Многоадресная маршрутизация (в отличие от одноадресной маршрутизации) связана только с источником данного потока многоадресных данных. То есть с IP-адресом устройства, являющегося источником многоадресного трафика. Основной принцип заключается в том, что устройство-источник "выталкивает" поток на неопределенное число приемников (внутри многоадресной группы). Все многоадресные маршрутизаторы создают деревья распространения, управляющие путем, по которому многоадресный трафик проходит через сеть для доставки трафика всем получателям. Существует два основных типа деревьев распределения многоадресного трафика: деревья-источники и разделяемые деревья. RPF является ключевым понятием в многоадресной пересылке. Он позволяет маршрутизаторам правильно пересылать многоадресный трафик на дерево распределения. RPF использует существующую таблицу одноадресной маршрутизации для определения верхних и нижних соседей. Маршрутизатор пересылает многоадресный пакет, только если он получен на восходящем интерфейсе. Такая проверка RPF помогает гарантировать, что дерево распределения не содержит петель.

Многоадресный трафик всегда видим для всех маршрутизаторов в мостовой LAN (уровень 2), согласно спецификации IEEE 802.3 CSMA/CD. В стандарте 802.3 нулевой бит первого октета используется для обозначения широковещательного и/или многоадресного кадра, а любой кадр 2 уровня с этим адресом является переполненным. Это также верно, даже если настроено отслеживание CGMP или IGMP. Это происходит потому, что многоадресные маршрутизаторы должны видеть многоадресный трафик для того, чтобы принимать правильные решения о пересылке. Если каждый из многоадресных маршрутизаторов имеет интерфейс в общую LAN, то только один маршрутизатор пересылает данные (выбранный процессом выбора). Из-за возможности переполнения LAN резервный маршрутизатор (маршрутизатор, который не пересылает многоадресный трафик) получает эти данные на исходящем интерфейсе данной LAN. Резервный маршрутизатор обычно сбрасывает этот трафик, поскольку он прибыл на неверный интерфейс и потому не пройдет проверку RPF. Трафик, который не проходит проверку RPF, называется не-RPF трафиком или пакетами, не прошедшими проверку RPF, так как они были переданы в обратную сторону по отношению к потоку от источника.

Catalyst 6500 с установленным MSFC можно настроить для работы в качестве полноценного многоадресного маршрутизатора. При использовании многоадресной многоуровневой коммутации (MMLS) трафик RPF обычно пересылается аппаратно в коммутаторе. ASIC передаются данные из состояния многоадресной маршрутизации (например, (*,G) и (S,G)), так что аппаратный ярлык можно запрограммировать в таблице Netflow и/или FIB. Такой не-RPF трафик все еще необходим в некоторых случаях и требуется ЦП MSFC (на уровне процессов) для механизма объявления PIM. В других случаях он сбрасывается путем быстрой программной коммутации (если быстрая программная коммутация не отключена на интерфейсе RPF).

Catalyst 6500, использующий резервирование, может обрабатывать не-RPF трафик неэффективно в определенных топологиях. Для не-RPF трафика обычно не имеется состояния (*,G) или (S,G) в резервном маршрутизаторе, и поэтому нельзя создать ни аппаратные, ни программные ярлыки для сброса пакета. Каждый многоадресный пакет должен проверяться процессором маршрутизации MSFC индивидуально, и это часто называют трафиком прерывания ЦП. С аппаратной коммутацией 3 уровня и несколькими интерфейсами/VLAN, подключенными к одному набору маршрутизаторов, не-RPF трафик, который попадает на ЦП резервного MSFC, усиливается в "N" раз относительно скорости исходного источника (где "N" — это число LAN, к которым резервно подключен маршрутизатор). Если скорость не-RPF трафика превышает способность системы сбрасывать пакеты, это может привести к высокой загрузке ЦП, переполнениям буфера и общей нестабильности системы.

В Catalyst 6500 имеется модуль списка доступа, позволяющий осуществлять фильтрацию при максимальной пропускной способности. Эту функцию в некоторых ситуациях можно использовать для более эффективной обработки не-RPF трафика групп разреженного режима. Метод на основе ACL можно использовать только в "сетях-заглушках" разреженного режима, где отсутствуют нисходящие многоадресные маршрутизаторы (и соответствующие приемники). Кроме того, из-за схемы пересылки пакетов в Catalyst 6500 внутренние резервные MSFC не могут использовать такую реализацию. Этот вопрос рассмотрен в документе по ошибке Cisco ID CSCdr74908 (только для зарегистрированных пользователей) . Для групп плотного режима не-RPF пакеты должны быть видны на маршрутизаторе, чтобы механизм объявления PIM работал правильно. Для управления неудачными проверками RPF в сетях плотного режима и в транзитных сетях разреженного режима используются различные решения, такие как ограничение скорости и качество обслуживания (QoS) на основании Netflow или CEF.

В Catalyst 6500 имеется модуль списка доступа, позволяющий осуществлять фильтрацию при максимальной пропускной способности. Эту функцию можно использовать для более эффективной обработки трафика не-RPF групп разреженного режима. Чтобы реализовать это решение, разместите список доступа на входящем интерфейсе "сети-заглушки" для фильтрации многоадресного трафика, который не исходит от "сети-заглушки". Список доступа определяется аппаратной частью коммутатора. Список доступа не дает CPU возможности увидеть пакет и позволяет устройству отбросить трафик, не относящийся к RPF.

Примечание: Не размещайте этот список доступа в транзитный интерфейс. Он предназначен только для сетей-заглушек (сетей, содержащих только узлы).

Дополнительные сведения см. в следующих документах:

- Проблемы резервного маршрутизатора с многоадресными IP в сетях-заглушках
- Обработка не-RPF трафика

команды "show"

Загрузка ЦП при выполнении команды show всегда составляет почти 100%. Высокая загрузка ЦП при выполнении команды show является нормальным явлением и обычно сохраняется всего несколько секунд.

Например, для процесса Virtual Exec повышение загрузки при выполнениии команды show tech-support нормально, так как выходные данные этой команды управляются прерыванием. Проблемой может быть только повышение загрузки ЦП в процессах, отличных от команд show.

Команда show cef not-cef-switched показывает, почему пакеты плывутся на плоскодонке к MSFC (получите, IP опция, никакая смежность, и т.д.), и сколько. Пример:

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

Показ ibc и **команды show ibc brief** показывают очередь ЦП и могут использоваться при мониторинге состояния ЦП.

Процессы Exec

Процесс Exec в ПО Cisco IOS отвечает за обмен данными по линиям TTY (консоль, вспомогательный, асинхронный) маршрутизатора. Процесс Virtual Exec отвечает за линии VTY (сеансы Telnet). Процессы Exec и Virtual Exec имеют средний приоритет, так что при наличии других процессов с более высоким приоритетом (высоким или критическим) процессы с более высоким приоритетом получают ресурсы ЦП.

Если через эти сеансы передается большой объем данных, загрузка ЦП процессом Exec возрастает. Это происходит потому, что когда маршрутизатор отправляет простой символ через эти линии, он использует некоторые ресурсы ЦП:

- Для консоли (Exec) маршрутизатор использует одно прерывание на символ.
- Для линии VTY (Virtual Exec) сеанс Telnet должен построить один пакет TCP на символ.

В этом списке раскрыты некоторые возможные причины высокой загрузки ЦП в процессе Exec:

- **Слишком много данных отправляется через порт консоли.**Проверьте, не запущены ли на маршрутизаторе процессы отладки, с помощью команды show debugging.**Отключите ведение журнала консоли на маршрутизаторе, используя форму no команды logging console.**Проверьте, не выводится ли на консоль большой объем выходных данных. Например, выходные данные команды show tech-support или show memory.
- Команда exec настраивается для асинхронных и вспомогательных линий.Если на линии имеется только исходящий трафик, отключите процесс Exec для этой линии. Иначе, если устройство (например модем), подключенное к этой линии, отправит незапрошенные данные, это запустит процесс Exec на этой линии.**Если маршрутизатор используется как терминальный сервер (для обращения Telnet на консоли других устройств), рекомендуется настроить команду no exec на линиях, которые подключены к**

консолям других устройств. Иначе данные, поступающие с консоли, могут запустить процесс Exec, который использует ресурсы ЦП.

Возможная причина высокой загрузки ЦП в процессе Virtual Exec:

- **Слишком много данных отправляется через сеансы Telnet.**Самой распространенной причиной высокой загрузки ЦП в процессе Virtual Exec является передача слишком больших объемов данных от маршрутизатора сеансу Telnet. **Это может происходить, когда команды с большим объемом выходных данных, например show tech-support, show memory и т.п., выполняются из сеанса Telnet.** *Объем данных, переданных через каждый сеанс VTY, можно проверить командой show tcp vty <line number>.*

Процесс устаревания 3 уровня

Если процесс устаревания 3 уровня экспортирует большое количество значений ifindex, используя экспорт данных NetFlow (NDE), загрузка ЦП может достигнуть 100%.

При возникновении такой проблемы проверьте, включены ли эти две команды:

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

Если включить эти команды, процесс должен экспортировать все целевые и исходные значения ifindex, используя NDE. *Загрузка процесса устаревания 3 уровня возрастает, так как он должен выполнить поиск FIB для всех целевых и исходных значений ifindex.* Из-за этого таблица заполняется, загрузка процесса устаревания 3 уровня повышается, а загрузка ЦП достигает 100%.

Чтобы решить эту проблему, отключите следующие команды:

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

Используйте эти команды для проверки значений:

- show mls cef summary
- show mls cef maximum-routes

BPDU-шторм

Связующее дерево поддерживает среду уровня 2, исключающую зацикливание, в резервных коммутаторах и мостах сети. Без использования STP фреймы зацикливаются или размножаются неопределенным образом. Это вызывало бы критическую перегрузку сети, так как все устройства широковещательного домена прерывались бы интенсивным трафиком.

В некоторых отношениях STP является ранним протоколом, разработанным для низкоскоростных программных спецификаций мостовых соединений (IEEE 802.1D), однако STP может быть усложнен для применения его в крупных коммутируемых сетях, имеющих следующие функции:

- Большое количество VLAN
- Большое количество коммутаторов в STP-домене
- Обслуживание у нескольких поставщиков
- Новейшие разработки IEEE

Если в сети часто выполняются рассчеты связующего дерева или коммутатор должен обрабатывать больше BPDU, это может привести к высокой загрузке ЦП, а также к сбросам BPDU.

Чтобы обойти эти проблемы, выполните одно из следующих действий:

1. Отсеките VLAN от коммутаторов.
2. Используйте улучшенную версию STP, например MST.
3. Обновите аппаратное обеспечение коммутатора.

Также используйте проверенные приемы реализации протокола связующего дерева в сети.

- Рекомендации по настройке и управлению для коммутаторов серии Catalyst 4500/4000, 5500/5000 и 6500/6000, работающих под управлением CatOS
- Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software

Сеансы SPAN

Основанные на архитектуре коммутаторов серии Catalyst 6000/6500, сеансы SPAN не влияют на производительность коммутатора, но если сеанс SPAN включает интенсивный трафик / каскадный порт или EtherChannel, он может увеличить нагрузку на процессор. Если он к тому же выделяет особую VLAN, то увеличивает нагрузку еще больше. Если на линии имеется "плохой трафик", это также увеличивает нагрузку.

В некоторых сценариях функция RSPAN может вызвать петли и вызвать быстрай рост нагрузки на процессор. Дополнительные сведения см. в разделе Почему сеанс SPAN создает мостовую петлю?

Коммутатор может пропустить трафик как обычно, так как обработка происходит на аппаратном уровне, но ЦП может пострадать, если попытается вычислить, какой трафик необходимо обработать. Рекомендуется настраивать сеансы SPAN только когда это обязательно.

ИСКЛЮЧЕНИЕ %CFIB-SP-STBY-7-CFIB: Исключение FIB TCAM, некоторые входы будут коммутироваться программно

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

Это сообщение об ошибке выдается, когда превышено количество доступного пространства в TCAM. Это приводит к высокой загрузке ЦП. Это ограничение FIB TCAM. При заполнении TCAM устанавливается флаг и выдается исключение FIB TCAM. При этом прекращается добавление новых маршрутов в TCAM. Поэтому все будет коммутироваться программно. Удаление маршрутов не поможет возобновить аппаратную коммутацию. Если TCAM входит в состояние исключения, систему необходимо перезагрузить, чтобы выйти из этого состояния. **Максимальное количество маршрутов, которые могут быть установлены в TCAM, увеличивается командой mls cef maximum-routes.**

Catalyst 6500/6000, работающий с высокой загрузкой CPU, имеет ACL IPv6 с портами L4

Включите mls ipv6 acl compress address unicast. Если ACL IPv6 совпадает на номерах портов протокола L4, эта команда необходима. Если эта команда не будет выполнена, то трафик IPv6 будет плыться на плоскодонке к ЦП для обработки программного обеспечения. Эта команда не настроена по умолчанию.

Медные SPF

В коммутаторах Ethernet серии Cisco ME 6500 медным SFP требуется большее взаимодействие с микропрограммой, чем другим типам SFP, что увеличивает загрузку ЦП.

Программные алгоритмы, управляющие медными SFP, были улучшены в версиях Cisco IOS SXH.

Модульные IOS

В коммутаторах серии Cisco Catalyst 6500 под управлением модульного ПО IOS нормальная загрузка ЦП немного выше, чем при немодульном ПО IOS.

Модульное ПО IOS требует больше ресурсов для своей работы, но расходует меньше ресурсов из расчета на пакет. Модульное ПО IOS обслуживает процессы, потребляя определенные ресурсы ЦП даже если пакетов немного, поэтому потребление ресурсов ЦП не основано на фактическом трафике. Однако когда скорость обрабатываемых пакетов увеличивается, потребление ресурсов ЦП в модульном ПО IOS не должно превышать потребление немодульного ПО IOS.

Проверка загрузки ЦП

При высокой загрузке ЦП выполните сначала команду show processes cpu. Выходные данные показывают загрузку ЦП коммутатора, а также потребление ресурсов ЦП каждым процессом.

```
Router#show processes cpu CPU utilization for five seconds: 57%/48%; one minute: 56%; five
minutes: 48% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process    1
0         5          0  0.00%  0.00%  0.00%   0 Chunk Manager       2          12     18062
```

```
0  0.00%  0.00%  0.00%   0 Load Meter          4      164532     13717      11994  0.00%  0.21%
0.17%   0 Check heaps         5           0         1          0  0.00%  0.00%  0.00%   0 Pool
Manager     !--- Output is suppressed. 172 0 9 0 0.00% 0.00% 0.00% 0 RPC aapi_rp 173      243912
2171455        112  9.25%  8.11%  7.39%   0 SNMP ENGINE       174          68       463
146  0.00%  0.00%  0.00%   0 RPC pm-mp  !--- Output is suppressed.
```

В этих выходных данных общая загрузка ЦП составляет 57 процентов, а загрузка ЦП прерываниями — 48 процентов. Эти показатели отображаются полужирным шрифтом. Коммутация трафика прерываний процессором приводит к загрузке ЦП прерываниями. В выходных данных команды перечисляются процессы, которые приводят к разнице между этими двумя загрузками. В данном случае причиной является процесс SNMP.

В механизме управления, который работает под управлением CatOS, выходные данные выглядят так:

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

— Kernel and Idle — . Этот процесс обычно наверху, если какие-либо другие процессы не потребляют циклы ЦП. SptBpduRx .

Если причиной высокой загрузки ЦП является один из этих процессов, можно провести диагностику и определить, почему этот процесс приводит к высокой загрузке. Но если ЦП загружен из-за трафика, поступающего на него, необходимо определить, почему приходит этот трафик. При этом можно определить происхождение трафика.

Для устранения проблем используйте этот пример сценария EEM для сбора выходных данных от коммутатора при испытании высокой загрузки ЦП:

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

Примечание: Когда ЦП является причиной высокой загрузки к коммутации в контексте процесса пакетов вместо аппаратных средств, **команда debug netdr capture rx** полезна. Когда команда выполнена, это перехватывает 4096 пакетов, поступающих к ЦП. Команда абсолютно безопасна и является самым удобным программным средством для проблем высокой загрузки CPU на 6500. Это не вызывает дополнительную загрузку к ЦП.

Служебные программы и средства для определения трафика, поступающего на ЦП

В этом разделе определяются некоторые служебные программы и средства, которые могут помочь изучить этот трафик.

Системное программное обеспечение Cisco IOS

В ПО Cisco IOS процессор коммутатора в механизме управления называется SP, а MSFC называется RP.

Команда show interface дает основную информацию о состоянии интерфейса и скорости трафика на интерфейсе. В этой команде также предусмотрены счетчики ошибок.

```
Router#show interface gigabitethernet 4/1GigabitEthernet4/1 is up, line protocol is up
(connected)  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
Internet address is 100.100.100.2/24  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255  Encapsulation ARPA, loopback not set  Keepalive
set (10 sec)  Half-duplex, 100Mb/s  input flow-control is off, output flow-control is off  Clock
mode is auto  ARP type: ARPA, ARP Timeout 04:00:00  Last input 00:00:00, output 00:00:00, output
hang never  Last clearing of "show interface" counters never  Input queue: 5/75/1/24075
(size/max/drops/flushes); Total output drops: 2  Queueing strategy: fifo  Output queue: 0/40
(size/max)  30 second input rate 7609000 bits/sec, 14859 packets/sec  30 second output rate 0
bits/sec, 0 packets/sec  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast  L3 out Switched:
ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes     2982871 packets input, 190904816 bytes, 0 no
buffer     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles     1 input errors, 1 CRC, 0
frame, 28 overrun, 0 ignored     0 input packets with dribble condition detected     1256
packets output, 124317 bytes, 0 underruns     2 output errors, 1 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred     0 lost carrier, 0 no carrier     0 output buffer
failures, 0 output buffers swapped out
```

В этих выходных данных можно увидеть, что входящий трафик коммутируется на 3 уровне вместо коммутации 2 уровня. Это показывает, что трафик поступает на ЦП.

Команда show processes cpu показывает, являются ли эти пакеты пакетами обычного трафика или пакетами управления.

```
Router#show processes cpu | exclude 0.00              CPU utilization for five seconds: 91%/50%;
one minute: 89%; five minutes: 47% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY
Process   5      881160     79142      11133  0.49%  0.19%  0.16%   0 Check heaps       98
121064   3020704         40 40.53% 38.67% 20.59%   0 IP Input         245      209336    894828
233  0.08%  0.05%  0.02%   0 IFCOM Msg Hdlr
```

  , , IP Input . Чтобы увидеть эти пакеты, выполните такую команду:

show buffers input-interface

```
Router#show buffers input-interface gigabitethernet 4/1 packetBuffer information for Small
buffer at 0x437874D4  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280  linktype 7
(IP), enctype 1 (ARPA), encsize 14, rxtype 1  if_input 0x505BC20C (GigabitEthernet4/1),
if_output 0x0 (None)  inputtime 00:00:00.000 (elapsed never)  outputtime 00:00:00.000 (elapsed
never), oqnumber 65535  datagramstart 0x8060F7A, datagramsize 60, maximum size 308  mac_start
0x8060F7A, addr_start 0x8060F7A, info_start 0x0  network_start 0x8060F88, transport_start
0x8060F9C, caller_pc 0x403519B4  source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000,
ttl: 63,  TOS: 0 prot: 17, source port 63, destination port 6308060F70:
000A 42D17580            ..BQu.08060F80: 00000000 11110800 4500002E 00000000
........E.......08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..?.?08060FA0:
001A261F 00010203 04050607 08090A0B  ..&.............08060FB0: 0C0D0E0F 101164
......d
```

Если трафик коммутируется прерываниями, то эти пакеты нельзя увидеть с помощью команды show buffers input-interface. Чтобы увидеть пакеты, поступающие на ЦП для коммутации на уровне прерываний, можно выполнить захват SPAN порта RP.

Примечание: См. этот документ для дополнительных сведений о коммутируемом с

прерываниями по сравнению с загрузкой ЦПУ процессной коммутации:

- *Высокая загрузка ЦП из-за прерываний в разделе Решение проблемы высокой загрузки ЦП на маршрутизаторах Cisco*

Внутренняя полоса связи RP и SP SPAN

SPAN для порта RP или SP в ПО Cisco IOS доступен в версии Cisco IOS Software Release 12.1(19)E и более поздних.

Синтаксис команды выглядит так:

```
test monitor session 1-66 add {rp-inband | sp-inband} [rx | tx | both]
```

Для ПО Cisco IOS версий 12.2 SX используйте следующий синтаксис:

```
test monitor add {1..66} {rp-inband | sp-inband} {rx | tx | both}
```

Примечание: Для выпуска SXH необходимо использовать **команду monitor session**, чтобы настроить сеанс локального анализатора SPAN, и затем использовать эту команду для соединения Сессии SPAN к ЦП:

```
source {cpu {rp | sp}} | single_interface | interface_list | interface_range |
mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]
```

Примечание: Для получения дополнительной информации об этих командах обратитесь к Локальному анализатору SPAN Настройки (Режим Конфигурации SPAN) в *Руководстве по конфигурации программного обеспечения Выпуска 12.2SX Catalyst 6500*.

Пример консоли RP:

```
Router#monitor session 1 source interface fast 3/3!--- Use any interface that is
administratively shut down.Router#monitor session 1 destination interface 3/2
```

Теперь перейдем к консоли SP. Например:

```
Router-sp#test monitor session 1 add rp-inband rx
```

Примечание: В Cisco IOS 12.2 версий SX команда была изменена для **тестирования монитора, добавляет 1 внутриполосный армированным пластиком rx**.

```
Router#show monitor Session 1---------Type : Local SessionSource Ports :Both : Fa3/3Destination
Ports : Fa3/2SP console:Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1
Egress Source Ports: 3/3 Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans:
<empty>Destination Ports: 3/2
```

Примечание: В Cisco IOS 12.2 версий SX команда была изменена для **тестирования монитора, показывают 1**.

Пример консоли SP:

```
Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1 Egress Source Ports: 3/3
Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans: <empty>Destination Ports:
3/2
```

Системное ПО CatOS

Для коммутаторов под управлением системного ПО CatOS механизм управления работает под управлением CatOS, а MSFC работает под управлением ПО Cisco IOS.

Если выполнить команду show mac, можно увидеть число кадров, поступивших на MSFC. Порт 15/1 — это подключение механизма управления к MSFC.

Примечание: Порт является 16/1 для Supervisor Engine в слоте 2.

```
Console> (enable) show mac 15/1Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast-
------- -------------------- -------------------- --------------------15/1
193576                    0                   1Port     Xmit-Unicast         Xmit-Multicast
Xmit-Broadcast-------- ------------------- ------------------- --------------------15/1
3                    0                    0Port     Rcv-Octet            Xmit-Octet-------- ----
---------------- --------------------15/1                 18583370                    0MAC
Dely-Exced MTU-Exced  In-Discard Out-Discard-------- ---------- ---------- ---------- ----------
-15/1              0          -          0           0
```

Быстрое увеличение этого числа показывает, что пакеты поступают на MSFC, что приводит к высокой загрузке ЦП. Можно увидеть пакеты следующим образом:

- SPAN MSFC Port 15/1 или 16/1
- SPAN sc0

SPAN MSFC Port 15/1 или 16/1

Настройте сеанс SPAN, в котором источником является порт 15/1 (или 16/1), а получателем — порт Ethernet.

Например:

```
Console> (enable) set span 15/1 5/10Console> (enable) show spanDestination     : Port 5/10Admin
Source    : Port 15/1Oper Source     : NoneDirection       : transmit/receiveIncoming Packets:
disabledLearning        : enabledMulticast       : enabledFilter          : -Status          :
active
```

Если собрать анализатор трафика на порте 5/10, то он покажет пакеты, которые передаются на MSFC и обратно. **Настройте сеанс SPAN как tx, чтобы захватить только те пакеты, которые предназначены для MSFC.**

SPAN sc0

Настройте сеанс SPAN с интерфейсом sc0 в качестве источника, чтобы захватить кадры, которые поступают на ЦП механизма управления.

```
Console> (enable) set span ?  disable                  Disable port monitoring  sc0
Set span on interface sc0  <mod/port>                Source module and port numbers  <vlan>
Source VLAN numbers
```

Примечание: Для Оптических Сервисных модулей (OSM) вы не можете выполнить перехват SPAN трафика.

Рекомендации

Загрузка ЦП механизма управления не отражает аппаратную производительность пересылки коммутатора. Однако, следует контролировать загрузку ЦП механизма управления.

1. Базовое использование ЦП модулем Supervisor Engine в стабильном состоянии сети с нормальными шаблонами трафика и загрузки.Обратите внимание на то, какие

процессы создают самую высокую загрузку ЦП.
2. При диагностировании загрузки ЦП ответьте на следующие вопросы:Какие процессы создают самую высокую загрузку? Отличаются ли эти процессы от базовых?Постоянно ли увеличивается загрузка ЦП выше базового уровня? Или наблюдаются вспышки высокой загрузки, которые сменяются базовыми уровнями?Поступают ли из сети уведомления о смене топологии (TCN)?**Примечание:** Переброски портов или порты хоста с STP portfast отключили TCN причины.Присутствует ли избыточный трафик широковещательной рассылки или групповой адресации в управляющих подсетях/VLAN?Присутствует ли избыточный управляющий трафик, например опрос SNMP, на коммутаторе?
3. В течение времени высокой загрузки CPU (когда ЦП составит 75% или выше), соберите выходные данные от этих команд:show clockshow versionshow processes cpu сортированистория ЦПУ show procshow log
4. Если возможно, изолируйте управляющую VLAN от VLAN с трафиком пользовательских данных, особенно с большим объемом широковещательного трафика.Например, с трафиком протоколов IPX RIP/SAP, AppleTalk и другим широковещательным трафиком. Такой трафик может повлиять на загрузку ЦП механизма управления, а в крайних случаях помешать нормальной работе коммутатора.
5. Если загрузка ЦП повышается из-за поступления трафика на RP, определите происхождение этого трафика и причины его поступления.Чтобы это определить, используйте служебные программы, описанные в разделе Служебные программы и средства для определения трафика, поступающего на ЦП.

Дополнительные сведения

- Полезные команды для устранения проблем высокой загрузки CPU на Catalyst 6500 с Sup720
- Общие сообщения об ошибках CatOS в коммутаторах Catalyst серии 6000/6500
- Наиболее распространенные сообщения об ошибках коммутаторов Catalyst серий 6500/6000 с программным обеспечением Cisco IOS
- Поиск неполадок оборудования и распространенные вопросы по переключателям семейства Catalyst 6500/6000 Series Switches, запускающим системное программное обеспечение Cisco IOS
- Односторонняя лавинная маршрутизация в коммутируемых сетях кампуса
- Коммутаторы серии Cisco Catalyst 6500 — Поддержка
- Сценарий EEM для сбора данных во время Неустойчивой проблемы Высокой загрузки CPU
- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация