

# Решение проблемы высокой загрузки ЦП процессом IP-входа

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[IP-ввод](#)

[Пример сеанса отладки IP-пакета](#)

[Дополнительные сведения](#)

## [Введение](#)

В данном документе описано решение проблемы высокой загрузки ЦП процессом IP-входа.

**Примечание.** Данный документ не содержит стратегии предотвращения атак различных типов.

## [Предварительные условия](#)

### [Требования](#)

Прежде чем изучать данный документ, рекомендуется ознакомиться с документом [Решение проблемы высокой загрузки ЦП на маршрутизаторах Cisco](#).

### [Используемые компоненты](#)

Данный документ применим для любого оборудования и программного обеспечения.

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по умолчанию. При работе с реально функционирующей сетью необходимо полностью осознавать возможные последствия выполнения команд до их применения.

### [Условные обозначения](#)

Дополнительную информацию об условных обозначениях в документе см. в разделе [Технические советы Cisco. Условные обозначения](#).

## [IP-вход](#)

Процесс ПО Cisco IOS®, называемый «IP-вход», осуществляет коммутацию процессов IP-пакетов. Если процесс IP-входа использует слишком много ресурсов ЦП, маршрутизатор

осуществляет коммутацию большого объема IP-трафика. Проверьте следующее:

### **Коммутация прерываний выключена на интерфейсах с большим объемом трафика.**

Коммутация прерываний связана с использованием алгоритмов коммутации, отличных от коммутации процессов. Например, быстрая коммутация, оптимальная коммутация, коммутация Cisco Express Forwarding и т. д. (дополнительную информацию см. в разделе [Основы настройки производительности](#)). По выходным данным команды **show interfaces switching** определите интерфейс, перегруженный трафиком. По выходным данным команды **show ip interface** можно определить метод коммутации, используемый на каждом интерфейсе. Отмените запрет на коммутацию при прерывании на этом интерфейсе. Следует помнить, что обычная быстрая коммутация настраивается на выходных интерфейсах: если для интерфейса настроена быстрая коммутация, пакеты, выходящие из такого интерфейса, являются пакетами быстрой коммутации. Метод коммутации Cisco Express Forwarding настраивается на входных интерфейсах. Чтобы создать базу данных переадресации (FIB) и записи таблицы смежности для определенного интерфейса, настройте коммутацию Cisco Express Forwarding на всех интерфейсах, связанных маршрутом с этим интерфейсом.

### **Быстрая коммутация на этом же интерфейсе выключена**

Если интерфейс имеет много вторичных адресов или субинтерфейсов и имеется большой объем трафика, исходящий из интерфейса на адрес этого же интерфейса, тогда все эти пакеты обрабатываются коммутацией процессов. В этой ситуации необходимо включить **ip route-cache same-interface** на этом интерфейсе. Когда используется коммутация Cisco Express Forwarding, нет необходимости отдельно включать коммутацию Cisco Express Forwarding на том же интерфейсе.

### **Быстрая коммутация на интерфейсе, обеспечивающем политику маршрутизации, выключена**

Если на интерфейсе настроена карта маршрутизации и большой объем трафика обрабатывается этой картой, тогда маршрутизатор использует коммутацию процессов для трафика. В этой ситуации необходимо включить параметр **ip route-cache policy** на этом интерфейсе. Проверьте ограничения, указанные в разделе «Включение маршрутизации на основе политики, обрабатываемой быстрой коммутацией».

### **Приходит трафик, который не коммутируется на уровне прерывания**

Это может быть любой из следующих типов трафика. Чтобы получить дополнительную информацию щелкните соответствующую ссылку.

Пакеты, для которых нет записи в кэше коммутации

Если настроена быстрая, оптимальная коммутация или Cisco Express Forwarding, пакет, для которого нет записи в кэше быстрой коммутации, FIB или таблицах смежности, все равно обрабатывается. Затем создается запись в соответствующем кэше или таблице, а все последующие пакеты, соответствующие этим критериям, обрабатываются быстрой, оптимальной или CEF-коммутацией. В нормальных условиях эти обрабатываемые пакеты не приводят к чрезмерной загруженности ЦП.

Однако, если в сети имеется устройство, которое: 1) генерирует пакеты с чрезвычайно высокой скоростью для устройств, достижимых через маршрутизатор, и 2) использует другой IP-адрес источника или назначения, для этих пакетов нет соответствия в кэше коммутации или таблице, тогда пакеты обрабатываются процессом IP-входа (если настроена коммутация NetFlow, TCP порты источника и назначения также сравниваются с записями в кэше NetFlow). Устройство, являющееся источником пакетов, может находиться в аварийном состоянии или осуществлять атаку.

(\*) Только с подобранными смежностями. Дополнительную информацию о смежностях Cisco Express Forwarding см. в документации [Cisco Express Forwarding](#).

Пакеты, предназначенные для маршрутизатора

Ниже приведены примеры пакетов, предназначенных для маршрутизатора.

Обновления маршрутизации, которые поступают с чрезвычайно высокой скоростью. Если маршрутизатор получает чрезвычайно большое число обновлений маршрутизации, которые необходимо обработать, эта задача может привести к перегрузке ЦП. Как правило, этого не происходит в стабильной сети. Способ сбора данных зависит от настроенного протокола маршрутизации. Однако целесообразно начать регулярно проверять выходные данные команды **show ip route summary**. Быстро меняющиеся значения – признак нестабильности сети. Частые изменения в таблице маршрутизации означают повышенную обработку протокола маршрутизации, что приводит к повышенной загрузке ЦП. Дополнительную информацию о решении этой проблемы см. в разделе [Поиск и устранение неисправностей TCP/IP](#) в руководстве по поиску и устранению неисправностей объединенной сети.

Любой другой тип трафика, предназначенного для маршрутизатора. Проверьте, кто зарегистрирован на маршрутизаторе, и просмотрите действия пользователя. Если кто-то зарегистрирован и выполняет команды, которые выдают большой объем выходных данных, за высокой загрузкой ЦП процессом IP-входа последует еще более высокая загрузка ЦП процессом [Virtual Exec](#).

Атака на основе подмены адресов (спуфинг). Чтобы идентифицировать проблему, определите объем IP-трафика с помощью команды **show ip traffic**. Если возникла проблема, становится значительным число полученных пакетов с локальным адресатом. Далее проверьте выходные данные команд **show interfaces** и **show interfaces switching**, чтобы определить интерфейс, принимающий пакеты. После определения принимающего интерфейса, включите **ip accounting** на исходящем интерфейсе и проверьте наличие шаблона. При атаке адрес источника почти всегда отличается, а адрес назначения остается неизменным. Для временного решения проблемы можно настроить список доступа (предпочтительно на устройстве, ближайшем к источнику пакетов), но полное решение заключается в отслеживании устройства, являющегося источником пакетов, и остановки атаки.

Широковещательный трафик

Проверьте число широковещательных пакетов в выходных данных команды **show interfaces**. Если сравнить число широковещательных пакетов с общим числом пакетов, полученных интерфейсом, можно сделать вывод о чрезмерности числа широковещательных пакетов. Если к маршрутизатору подключена локальная сеть с несколькими коммутаторами, тогда это может указывать на проблему с связующим деревом.

IP-пакеты с параметрами

Пакеты, которым требуется преобразование протокола

Многоканальный протокол PPP (поддерживается в методе коммутации Cisco Express Forwarding)

Сжатый трафик

Если в маршрутизаторе отсутствует адаптер службы сжатия (CSA), сжатые пакеты должны обрабатываться коммутацией процессов.

Зашифрованный трафик

Если в маршрутизаторе отсутствует адаптер службы шифрования (ESA), зашифрованные пакеты должны обрабатываться коммутацией процессов.

Пакеты, проходящие через последовательные интерфейсы с инкапсуляцией X.25

В [наборе протоколов X.25](#) управление потоком реализуется на втором уровне модели взаимодействия открытых систем (OSI).

Большое число пакетов, поступающих с чрезвычайно высокой скоростью для адресата в непосредственно подключенной подсети, для которого нет записи в таблице протокола разрешения адресов (ARP). Это не должно иметь место в случае TCP-трафика из-за оконного механизма, однако может происходить с UDP трафиком. Чтобы определить проблему, повторите действия, рекомендованные для отслеживания атак спуфинга.

Через маршрутизатор передается большой объем многоадресного трафика. К сожалению, простого способа определения объема многоадресного трафика нет. Команда **show ip traffic** отображает только сводную информацию. Однако, если на маршрутизаторе настроена многоадресная маршрутизация, можно включить быструю коммутацию многоадресных пакетов командой настройки интерфейса **ip mroute-cache** (быстрая коммутация многоадресных пакетов выключена по умолчанию).

Превышен лимит подписки для маршрутизатора. Если маршрутизатор используется чрезмерно интенсивно и не может обработать объем трафика, попробуйте перераспределить нагрузку на другие маршрутизаторы или установите маршрутизатор с более высокой производительностью.

На маршрутизаторе настроено преобразование сетевых IP-адресов и большое число DNS пакетов передается через маршрутизатор. UDP- или TCP-пакеты с портом 53 (DNS) источника или назначения всегда передаются преобразованием NAT на уровень обработки.

Существуют пакеты других типов, которые передаются на обработку.

Чем бы ни была вызвана высокая загрузка ЦП в процессе IP-входа, источник проблемы можно определить путем отладки IP-пакетов. Поскольку загрузка ЦП уже высокая, процесс отладки необходимо осуществлять очень осторожно. Процесс отладки порождает большое число сообщений, поэтому следует настраивать только **logging buffered**.

Ведение журнала на консоли приводит к излишнему увеличению прерываний для ЦП и повышает его загрузку. Ведение журнала на узле (или контролирующее ведение журнала) генерирует дополнительный трафик на интерфейсах.

Процесс отладки можно начать с команды **debug ip packet detail**. Этот сеанс должен длиться не более 3 – 5 секунд. Сообщения отладки записываются в буфер регистрации. Пример данных сеанса отладки приведен в разделе [Пример сеанса отладки IP-пакета](#) данного документа. После того как будет найдено исходное устройство, от которого поступают нежелательные IP-пакеты, можно будет отключить его от сети, или создать на маршрутизаторе список доступа, при помощи которого будет происходить отбрасывание пакетов с этого устройства.

## [Пример сеанса отладки IP-пакета](#)

Настроенные приемники данных протоколирования необходимо сначала проверить командой **show logging**:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 52 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 148 messages logged
  Trap logging: level informational, 64 message lines logged
    Logging to 192.168.100.100, 3 message lines logged
    Logging to 192.168.200.200, 3 message lines logged
--More--
```

Отключите все приемники данных протоколирования за исключением буфера регистрации и очистите этот буфер:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#no logging console
router(config)#no logging monitor
router(config)#no logging 192.168.100.100
router(config)#no logging 192.168.200.200
router(config)#^Z
router#clear logging
Clear logging buffer [confirm]
router#
```

Для облегчения восприятия выходных данных отладки следует включить дату и время в миллисекундах:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#service timestamps log datetime msec
router(config)#service timestamps debug datetime msec
router(config)#end
router#
```

Теперь можно начать сеанс отладки:

```
router#debug ip packet detail
IP packet debugging is on (detailed)
```

Отладка должна длиться не более 3 – 5 секунд. Сеанс отладки можно остановить командой **undebug all**:

```
router#undebug all
All possible debugging has been turned off
```

Результаты можно проверить командой **show logging**:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level debugging, 145 messages logged
  Trap logging: level informational, 61 message lines logged
Log Buffer (64000 bytes):

*Mar  3 03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
  (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205
  (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206
  (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.328: ICMP type=8, code=0
...
```

В журнале указано следующее:

Пакет принимается каждые четыре миллисекунды

IP-адрес источника 192.168.40.53

Пакеты поступают на интерфейс Ethernet0/1

Пакеты имеют разные IP-адреса назначения

Пакеты отправлены из интерфейса Ethernet0/0

IP-адрес следующего узла 10.200.40.1

Пакеты представляли собой ICMP-запросы (тип=8)

В этом примере высокая загрузка ЦП в процессе IP входа была вызвана лавиной эхо-запросов с IP-адреса 192.168.40.53.

Затопление пакетами SYN можно без труда обнаружить этим способом, поскольку наличие флага SYN указано в выходных данных отладки:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level debugging, 145 messages logged
  Trap logging: level informational, 61 message lines logged
Log Buffer (64000 bytes):

*Mar  3 03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
  (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205
  (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206
  (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.328: ICMP type=8, code=0
...
```

## Дополнительные сведения

- [Решение проблемы высокой загрузки ЦП на маршрутизаторах Cisco](#)
- [Команда show processes](#)
- [Высокая загрузка ЦП коммутаторов Catalyst 2900XL/3500XL](#)
- [Основы настройки производительности](#)
- [Техническая поддержка – Cisco Systems](#)