

# Вопросы и ответы по Content Services Switch

## Вопросы

### [Введение](#)

[Где можно найти MIB для CSS?](#)

[Каково максимальное число сценариев поддержки активности, поддерживаемых CSS?](#)

[Как очистить или удалить файлы ядра?](#)

[Где можно найти пояснения к сообщениям журнала?](#)

[Есть ли команда, управляющая частотой отправки отчетов о загрузке от одного узла к другому?](#)

[Изменяются ли ключи лицензии с переменной версии кода?](#)

[Я потерял свой лицензионный ключ. Какие действия следует предпринять?](#)

[Сколько времени по умолчанию хранится запись в таблице Sticky-объектов?](#)

[Как настроить маску закрепления в памяти, чтобы закрыть запросы от мега-прокси, вроде Америка онлайн \(AOL\)?](#)

[Почему при использовании Secure Socket Layer \(SSL\) с улучшенным балансом не предоставляется возможность закрепления?](#)

[Какой тип шифрования используют протоколы CAPP и APP?](#)

[Что означает сообщение gratuitous arp?](#)

[Как синхронизировать конфигурации с помощью CSS в режиме обхода отказа?](#)

[Какие настройки следует использовать в терминальной программе?](#)

[Есть ли способ перепрограммировать MAC-адрес на CSS?](#)

[Как изменить приглашение на CSS так, чтобы оно сохранялось постоянно?](#)

[В чем заключается отличие между работающей и заблокированной флэш-памятью?](#)

[Почему существуют различные версии флэш-памяти?](#)

[Почему я не могу попасть на порт управления CSS с удаленного порта?](#)

[Поддерживает ли техническая поддержка Cisco сценарии обеспечения активности, написанные пользователем?](#)

[Как удалить файлы ядра с диска CSS?](#)

[Когда я аутентифицируюсь на сервере RADIUS со своим CSS, я получаю сообщение об ошибке «RADIUS-4: RADIUS Authentication failed with reason code 2». Что это значит?](#)

[Насколько велика таблица Sticky-объектов и что вызывает удаление записей в ней?](#)

[Как вывести службу из обращения?](#)

[Является ли network proximity частью расширенного набора функций?](#)

[Какие данные выдает команда show dos?](#)

[Можно ли отключить функцию DoS-защиты на линейке коммутаторов CSS?](#)

[Можно ли отключить счетчики DoS-защиты?](#)

[Как использовать диапазоны портов в списках доступа?](#)

[Дополнительная информация](#)

## [Введение](#)

В данном документе рассмотрены часто задаваемые вопросы, связанные с Cisco Content Services Switch (CSS).

Дополнительные сведения об условных обозначениях в документах см. в разделе [Технические советы Cisco. Условные обозначения](#).

### Вопрос. Где можно найти MIB для CSS?

**Ответ.** MIB хранятся на самом CSS. CSS можно рассматривать как агент в схеме сети SNMP. Вам остается только настроить параметры SNMP на CSS. Дополнительную информацию см. в документе [Настройка протокола SNMP](#).

### Вопрос. Каково максимальное число сценариев поддержки активности, поддерживаемых CSS?

**Ответ.** CSS поддерживает до 255 сценариев. См. раздел [Новые функции ПО версии 5.00 в информации о версии Cisco 11000 Series Content Services Switch](#).

### Вопрос. Как очистить или удалить файлы ядра?

**Ответ.** Выполните команду **clear core**. Команда доступна в ПО CSS 5.00 и более поздних версий в режиме отладки. Синтаксис:

```
css150(debug) #clear core filename CR
```

### Вопрос. Где можно найти пояснения к сообщениям журнала?

**Ответ.** Сообщения журнала разъясняются в документе [Сообщения журнала](#).

### Вопрос. Есть ли команда, управляющая частотой отправки отчетов о загрузке от одного узла к другому?

**Ответ.** Можно воспользоваться командой **dns-peer interval**. Кроме того, есть и другие команды – они настраиваются локально и дают более быструю оценку локальной загрузки:

- **ageout-timer** – устанавливает время устранения устаревшей информации о загрузке (в секундах).
- **teardown-timer** – устанавливает максимальный период (в секундах), по истечении которого система отправляет отчет о разрыве соединения.

### Вопрос. Изменяются ли ключи лицензии с переменной версии кода?

**Ответ.** Нет, ключи лицензии не меняются.

## Вопрос. Я потерял свой лицензионный ключ. Какие действия следует предпринять?

**Ответ.** Отправьте письмо с серийным номером CSS по адресу [licensing@cisco.com](mailto:licensing@cisco.com). Выходные данные команды **version** содержат набор функций, а не лицензионный ключ.

## Вопрос. Сколько времени по умолчанию хранится запись в таблице Sticky-объектов?

**Ответ.** Если не использовалась команда **sticky-inact-timeout**, время по умолчанию не установлено. Таблица Sticky-объектов используется по принципу FIFO (32 000 или 128 000 записей – в зависимости от типа устройства и доступного объема памяти), и хранится до перезагрузки CSS.

## Вопрос. Как настроить маску закрепления в памяти, чтобы закрыть запросы от мега-прокси, вроде America Online (AOL)?

**Ответ.** Если приложение требует закрепить пользователя на протяжении всего сеанса, можно использовать закрепление уровня 3. В этом случае пользователь закрепляется за сервером на основании IP-адреса пользователя. Объем таблицы Sticky-объектов в CSS – 32 000, то есть когда на узле одновременно присутствует более 32 000 пользователей, таблица сворачивается и закрепление с первого пользователя снимается. Однако узел может быть весьма масштабным – на нем может быть более 32 000 пользователей одновременно – или большая часть клиентов может приходить через мега-прокси. В таких случаях стоит использовать другой метод закрепления (например cookie, cookieurl или url) или расширять маску закрепления. Маска закрепления по умолчанию – 255.255.255.255, то есть каждая запись в таблице Sticky-объектов представляет собой отдельный IP-адрес. На некоторых мега-прокси случается, что пользователь в течение одного сеанса использует несколько IP-адресов из некоего диапазона. Это приводит к тому, что часть TCP-соединений закрепляются на одном сервере, из-за чего другие соединения, связанные с той же транзакцией, закрепляются на другом. В результате часть элементов из корзины может пропасть. Когда нет возможности использовать более сложные методы закрепления, используйте маску 255.255.240.0, если большая часть ваших клиентов приходит через один из этих мега-прокси.

## Вопрос. Почему при использовании Secure Socket Layer (SSL) с улучшенным балансом не предоставляется возможность закрепления?

**Ответ.** SSL с улучшенным балансом – это то же самое, что и SSL с закреплением.

## Вопрос. Какой тип шифрования используют протоколы CAPP и APP?

**Ответ.** По умолчанию в протоколе CAPP шифрование не используется. Сеанс APP можно настроить так, чтобы использовался алгоритм Message Digest 5 (MD5). Тип шифрования на обоих одноранговых узлах должен совпадать, иначе сеанс APP не будет установлен.

### Вопрос. Что означает сообщение gratuitous arp?

**Ответ.** Если резервный коммутатор в течение 3 секунд не обнаруживает пульсацию основного коммутатора, он замещает основной коммутатор и отправляет сообщение gratuitous arp. Оно подтверждает передачу ARP с нового основного коммутатора. В сообщении содержится MAC-адрес коммутатора, являющегося основным в данный момент времени.

### Вопрос. Как синхронизировать конфигурации с помощью CSS в режиме переключения при отказе?

**Ответ.** Для синхронизации конфигураций в ПО версии 4.0 используйте команду `commit config sync`. В ПО версии 3.10 для переноса конфигурации с одного коммутатора на другой необходимо использовать FTP. В ПО версий 6.x и 7.x синхронизация выполняется при помощи команды `commit_redundancy` для активного/аварийного резервирования или резервирования между устройствами. Для резервирования виртуальных IP (VIP) и интерфейсов можно использовать команду `commit_vip_redundancy`. Команду `show script commit_redundancy` можно использовать для просмотра доступных параметров командной строки для сценария `commit_redundancy` – они указаны в заголовке сценария. То же самое относится к команде `commit_vip_redundancy`.

### Вопрос. Какие настройки следует использовать в терминальной программе?

**Ответ.** Используйте следующие настройки:

- 9600 бод
- 8 бит
- без контроля четности
- 1 стоповый бит
- без контроля потока

### Вопрос. Есть ли способ перепрограммировать MAC-адрес на CSS?

**Ответ.** Да, такой способ существует.

**Примечание:** MAC-адрес и серийный номер указаны на задней стороне устройства.

Для перепрограммирования серийного номера и MAC-адреса выполните следующие действия. Это пример для MAC-адреса в шасси CS800:

1. Откройте **автономный диагностический монитор (ODM)**.
2. В основном меню ODM нажмите **Shift-T**, чтобы перейти в меню инженера.
3. Выберите пункт **1** (Настройка).
4. Выберите пункт **5** (Установить информацию производителя).
5. Выберите пункт **2** (Установить информацию производителя объединительной карты).
6. Следуя подсказкам, введите соответствующие данные: серийный номер, MAC-адрес. Данные эти можно найти на крышке шасси CS800.
7. Перезапустите сервер.

## Вопрос. Как изменить приглашение на CSS так, чтобы оно сохранялось постоянно?

**Ответ.** Войдите в систему устройства CSS как пользователь fred и используйте собственные данные для входа. Чтобы изменить приглашение, выполните следующую команду:

```
Css100#prompt Redsox
<cr>
Redsox#
```

Чтобы сохранить изменения, выполните следующую команду:

```
Redsox#save_profile
```

Эта команда сохраняет профиль пользователя. Теперь при каждом входе пользователя в систему CSS будет использоваться одно и то же приглашение. При этом – как при использовании файлов ресурсов ?? в UNIX – создается уникальный профиль для каждого пользователя.

Когда вы возвращаетесь в CSS и входите в систему под учетной записью администратора, изменений приглашения вы не видите. Изменения действуют только для одного пользователя, то есть команды **prompt** и **save\_profile** нужно выполнить для каждого пользователя, желающего использовать другое приглашение.

## Вопрос. В чем заключается отличие между работающей и заблокированной флэш-памятью?

**Ответ.** В данном примере показаны различные типы флэш-памяти, которые указаны в выходных данных команды **show version**:

```
CSS150-2#show version
Version:                ap0401049s (4.01 Build 49)
Flash (Locked):        3.10 Build 33
!--- , CSS. !--- , CSS !--- - - .

Flash (Operational):  5.00 Build 10-
!--- , CSS. : PRIMARY Licensed Cmd Set(s): Standard Feature Set
Enhanced Feature Set SSH Server
```

## Вопрос. Почему существуют различные версии флэш-памяти?

**Ответ.** Заблокированная флэш-память отражает ту версию программного обеспечения, которая была изначально установлена на CSS. Эта версия не изменяется, она используется только в качестве резервной. Версия, хранящаяся в работающей флэш-памяти – это версия, которая в данный момент запущена на CSS.

## Вопрос. Почему я не могу попасть на порт управления CSS с удаленного порта?

**Ответ.** В Cisco WebNS до версии 5.03 порт управления не являлся маршрутизируемым интерфейсом. В версии 5.03 он может быть маршрутизируемым: для этого нужно добавить к порту управления шлюз по умолчанию.

## Вопрос. Поддерживает ли техническая поддержка Cisco сценарии обеспечения активности, написанные пользователем?

**Ответ.** Нет, [служба технической поддержки Cisco](#) не поддерживает пользовательские сценарии обеспечения активности.

## Вопрос. Как удалить файлы ядра с диска CSS?

**Ответ.** Если в выходных данных команды **show core** перечислены файлы ядра, их можно удалить двумя способами:

**Примечание:** Выбор способа зависит от версии кода.

```
CSS50-1(config)#llama

!--- CSS . CSS50-1(debug)#clear core corefilename

CSS50-1(config)#llama

!--- CSS . CSS50-1(debug)#dir c:/Core/?

!--- !--- c:/Core. CSS50-1(debug)#ap_file delete c:/Core/
corefilename

!--- .
```

## Вопрос. Когда я аутентифицируюсь на сервере RADIUS со своим CSS, я получаю сообщение об ошибке «RADIUS-4: RADIUS Authentication failed with reason code 2». Что это значит?

**Ответ.** Это сообщение об ошибке говорит о том, что ответ доставлен на CSS и с ним что-то не так. Причина может состоять в том, что на сервере RADIUS не удалось установить значение administrative для атрибута типа службы. Проверьте сервер RADIUS и атрибуты типа службы.

## Вопрос. Насколько велика таблица Sticky-объектов и что вызывает удаление записей в ней?

**Ответ.** Размер таблицы Sticky-объектов в CSS составляет 32 000 или 128 000 (в зависимости от типа модели и доступного объема памяти). В таблице содержатся записи, соответствующие sticky source-ip и закрепленным SSL. Таблица Sticky-объектов не поддерживает закрепленные cookie на CSS. Записи из таблицы удаляются в следующих случаях:

- По умолчанию работает принцип FIFO. Записи хранятся в таблице, пока не заполнится буфер размером 32 000 или 128 000. После этого появление каждой новой записи на CSS приводит к удалению другой записи по принципу FIFO.
- Используется также период sticky-inact-timeout (указывается в минутах). В правиле контента можно указать предельный период неактивности, по прошествии которого CSS будет удалять запись из таблицы Sticky-объектов. Пример приведен ниже:

```
CSS50-1(config)#llama
---
!---      CSS      . CSS50-1(debug)#dir c:/Core/?
-----
!---      !---      c:/Core. CSS50-1(debug)#ap file delete c:/Core/
corefilename
!---      .
```

**Примечание:** CSS отклоняет запрос на закрепление, если выполняются все перечисленные ниже условия:

- Используется параметр sticky-inact-timeout.
- Буфер в 32 000 или 128 000 на CSS заполнен.
- Нет записей, у которых истекает период хранения.
- Правило контента. При продлении или повторной активации правила контента производится удаление записей таблицы Sticky-объектов, к которым применимо данное правило.

Дополнительные сведения см. в документе Настройка Sticky-параметров для правил контента.

## Вопрос. Как вывести службу из обращения?

**Ответ.** На основании настройки правила контента (уровень 3, 4 или 5) CSS работает по-другому: можно вручную приостановить службу, при этом сервер предоставлять службу не будет. Очень часто разработчикам веб-приложений приходится временно приостанавливать службы, чтобы вносить в веб-страницы изменения, связанные с администрированием. Поскольку такие изменения могут вноситься в рабочее время, существующие соединения со службой или

службами во время ручной приостановки могут быть прерваны, что нежелательно. Обновление служб следует выполнять, когда работа службы приостановлена.

В данном примере показаны правила контента уровня 5, 4 и 3:

```
CSS50-1(config)#llama

!--- CSS . CSS50-1(debug)#dir c:/Core/?

!--- !--- c:/Core. CSS50-1(debug)#ap_file delete c:/Core/
corefilename
!--- .
```

CSS переадресует существующие соединения при использовании правил уровня 3 и 4. Если происходит приостановка службы при использовании правил уровня 3 или 4, CSS переадресует каждое установленное соединение и перенаправит все последующие TCP-запросы на активную службу согласно соответствующему правилу контента.

При ручной приостановке службы по правилу уровня 5 CSS восстановит соединения, связанные с данной службой.

## Вопрос. Является ли network proximity частью расширенного набора функций?

**Ответ.** Функции network proximity не входят в набор расширенных функций, на них требуется отдельная лицензия. Если попытаться выполнить команду proximity на CSS без соответствующей лицензии, вы получите сообщение об ошибке:

```
CSS50-1(config)#proximity db 0 tier1
^
%% Invalid License to execute command.
This command belongs to the Proximity Database. Refer
to the user manual or contact Cisco Systems, Inc for
further information concerning license keys.
```

Приобрести лицензию вы можете у официального дилера Cisco в вашем регионе. Если вы приобрели лицензию и вам требуется замена, отправьте письмо по адресу [licensing@cisco.com](mailto:licensing@cisco.com).

## Вопрос. Какие данные выдает команда show dos?

**Ответ.** Cisco CSS может предоставлять сведения о недавно произошедших атаках:

- IP-адреса источника и назначения
- тип события
- сколько раз событие возникало

Если происходит несколько атак с одним типом DoS и одинаковыми адресами



источника и назначения, CSS пытается объединить их в одно событие. Это сокращает объем отображаемой информации о событиях.

Выполните команду **show dos**, чтобы получить следующие сведения:

- общее число атак с момента загрузки CSS
- типы атак и максимальное число атак в секунду
- первый и последний случай возникновения атаки

Ниже приведен пример выходных данных команды **show dos**:

```
CSS50-1#show dos
Denial of Service Attack Summary:
Total Attacks: 0
SYN Attacks:                0 Maximum per second:
    0
LAND Attacks:                0 Maximum per second:
    0
Zero Port Attacks:          0 Maximum per second:
    0
Illegal Src Attacks:        0 Maximum per second:
    0
Illegal Dst Attacks:        0 Maximum per second:
    0
Smurf Attacks:              0 Maximum per second:
    0

No attacks detected
```

В следующем списке приведены краткие описания полей выходных данных команды:

- **Total Attacks** – общее число DoS-атак, обнаруженных с момента загрузки устройства. Описания типов атак, указываемых в списке, и их число приводятся ниже.
- **SYN Attacks** – TCP-соединения, которые источник инициирует, но не подтверждает (не происходит трехэтапное установление TCP-соединения).
- **LAND Attacks** – пакеты, у которых адрес источника совпадает с адресом назначения. CSS не позволяет использовать внутренние IP-адреса в качестве источника потока. Кроме того, CSS не допускает совпадения адреса источника фрейма и адреса назначения.
- **Zero Port Attacks** – фреймы, содержащие TCP- или UDP-порты, равные нулю.

**Примечание:** ПО SmartBits более старых версий может отправлять фреймы с нулевыми портами источника или назначения. CSS регистрирует их как DoS-атаки и сбрасывает.

- **Illegal Src Attacks** – недопустимый адрес источника.
- **Illegal Dst Attacks** – недопустимый адрес назначения.
- **Smurf Attacks** – эхо-тесты, для которых указан широковещательный адрес назначения. CSS по умолчанию не поддерживает направленные

широковещательные рассылки. Атаки типа `Smurf Attack` используют ICMP-эхо на широковещательный адрес. CSS может блокировать доступ к эхо-портам UDP при помощи списков ACL.

- `Maximum per second` – максимальное число событий в секунду. Используйте эту информацию для настройки пороговых значений ловушки SNMP.

**Примечание:** Максимальное значение событий в секунду вычисляется по каждому SFP отдельно. На CSS 11800, к примеру, может быть до четырех SFP, а значит максимальное число событий в секунду фактически может в четыре раза превышать значение, указанное в выходных данных.

**Примечание:** Часто задается вопрос о том, можно ли отключить DoS-защиту на CSS. Нет, нельзя. DoS-защита является частью процесса допуска потока. Ее задача – защищать ресурсы CSS и сервера, стоящего за CSS. DoS настраивать нельзя. DoS-защита должна быть прозрачной при правильной работе протоколов. Процесс создания потока тесно связан с функциями DoS. Они помогают CSS сохранять быстрые маршруты и позволяют защитить устройства, с которыми взаимодействует CSS. Функции DoS есть во всех версиях ПО начиная с версии 3.0.

Для обнаружения возможных DoS-атак можно также использовать различные SNMP-ловушки. Ловушки доступны следующие:

- **`snmp trap-type enterprise`** — чтобы включить SNMP-ловушки enterprise и настроить их типы, используйте команду **`snmp trap-type enterprise`**. Команда **`no snmp trap-type enterprise`** отключает все ловушки. Ловушки enterprise должны включаться до настройки параметра ловушек. Можно настроить CSS так, чтобы ловушки enterprise создавались автоматически при DoS-атаке, неудачном входе в систему или изменении состояния службы CSS.
- **`dos_attack_type`** — создает SNMP-ловушку при DoS-атаке. Ловушка создается каждую секунду, если число атак в секунду превышает пороговое значение, установленное для DoS-атак. Возможные варианты:

- **`dos-illegal-attack`** – создает ловушку для недопустимых адресов – как источника, так и назначения. К недопустимым адресам относятся:
  - возвратные адреса источника
  - широковещательные адреса источника
  - возвратные адреса назначения
  - многоадресные адреса источника
  - собственные адреса источника

Стандартное пороговое значение ловушки для этого типа атак – одна в секунду.

- **`dos-land-attack`** – создает ловушки для пакетов, у которых адрес источника совпадает с адресом назначения. Стандартное пороговое значение для этого типа атак – одна в секунду.
- **`dos-ping-attack`** – создает ловушки, если число эхо-тестов превышает пороговое значение. Стандартное пороговое значение для этого типа атак – 30 в секунду.

**Примечание:** В этом варианте не отслеживаются смертельные DoS-атаки.

- **dos-smurf-attack** – создает ловушки, если число эхо-тестов с широковещательным адресом назначения превышает пороговое значение. Стандартное пороговое значение для этого типа атак – одна в секунду.
- **dos-syn-attack** – создает ловушки, когда число TCP-соединений, которые были инициированы, но не подтверждены источником (не было выполнено трехэтапное установление соединения) превышает пороговое значение. Стандартное пороговое значение для этого типа атак – 10 в секунду.

/li>

## Вопрос. Можно ли отключить функцию DoS-защиты на линейке коммутаторов CSS?

**Ответ.** В имеющейся на данный момент линейке ПО для CSS (Cisco WebNS) DoS-защита не отключается.

## Вопрос. Можно ли отключить счетчики DoS-защиты?

**Ответ.** Счетчики, регистрирующие атаки DoS/SYN, не отключаются. **Примечание:** Дополнительные сведения по атакам DoS и SYN см. в ответе на вопрос [Какие данные выдает команда show dos?](#)

## Вопрос. Как использовать диапазоны портов в списках доступа?

**Ответ.** Использование диапазонов портов в списках ACL помогает уменьшить число настраиваемых ACL, если нужно блокировать доступ пользователя к нескольким портам TCP/UDP. Допустим, нужно блокировать порты 20 – 23 для всех пользователей из внешней сети. Пусть внешняя сеть или общедоступная сторона CSS находится в сети VLAN 2, а внутренняя или серверная сторона сети находится в сети VLAN 1. ACL настраивается следующим образом:

```
CSS50-1#show dos
Denial of Service Attack Summary:
Total Attacks: 0
SYN Attacks:                0 Maximum per second:
0
LAND Attacks:                0 Maximum per second:
0
Zero Port Attacks:          0 Maximum per second:
0
Illegal Src Attacks:        0 Maximum per second:
0
Illegal Dst Attacks:        0 Maximum per second:
0
Smurf Attacks:              0 Maximum per second:
0
```

No attacks detected

## Дополнительные сведения

- [Объявление о завершении продаж Cisco CSS 11000 Series](#)
- [Бюллетени по коммутаторам служб контента Cisco CSS 11000 Series](#)
- [Техническая поддержка для коммутаторов служб контент CSS 11000 Series](#)
- [Центр программного обеспечения \(загрузки\) - передача содержимого по сети \(только для зарегистрированных клиентов\)](#)
- [Техническая поддержка и документация - Cisco Systems](#)