

# Настройте XE IOS для отображения полного show running config для пользователей с низкими Уровнями привилегий

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Проблема конфигурации](#)

[Решение для конфигурации и проверка](#)

[Заключение](#)

## Введение

Этот документ описывает действия настройки о том, как отобразить полную рабочую конфигурацию для пользователей, в которых входят к маршрутизатору с низкими уровнями привилегий. Для понимания ниже проблемы и обходного пути, необходимо понять уровни привилегий. Доступные уровни привилегий колеблются от 0 до 15 и позволяют администратору настраивать, какие команды доступны в какой уровень привилегий. По умолчанию эти три уровня привилегий на маршрутизаторе:

- **Уровень 0** – Включает только основные команды (отключите, включите, выйдите, помогите, и выход из системы),
- **Уровень 1** – Включает все команды, доступные в Пользовательский командный режим EXEC
- **Уровень 15** – Включает все команды, доступные в Привилегированный командный режим EXEC

Остающиеся уровни, промежуточные, эти минимальные и максимальные уровни не определены, пока администратор не назначает команды и/или пользователей им. Поэтому администратор может назначить пользователей другие уровни привилегий, промежуточные эти минимальные и максимальные уровни привилегий разделять, у каких других пользователей есть доступ также. Администратор может тогда выделить отдельные команды (и различные другие опции) к отдельному уровню привилегий для предоставления доступа к этому доступным для любого пользователя на этом уровне. Пример:

```
Маршрутизатор (config) # привилегия user1 имени пользователя 7
паролей P@ssw0rD1
Маршрутизатор (config) # show access-lists уровня 7 exec привилегии
```

С этой конфигурацией, когда 'user1' соединился с маршрутизатором, они были бы в состоянии выполнить команду 'show access-lists', и/или что-либо еще включило в том уровне привилегий. Однако, то же не может быть сказано для включенного команда 'show running config', как будет обсужден ниже с нашей постановкой задачи.

# Предварительные условия

## Требования

Основное понимание уровней привилегий Cisco требуется, чтобы понимать этот документ, вышеупомянутое введение должно быть достаточным для объяснения понимания уровней привилегий, которое требуется.

## Используемые компоненты

Используемые компоненты для примеров конфигурации в этом документе были ASR1006.

## Проблема конфигурации

При настройке других уровней доступа к маршрутизатору для других пользователей это - распространенное применение для администратора сети, чтобы попытаться назначить некоторым пользователям только иметь доступ, чтобы 'показать' команды и не предоставить доступ к любым командам 'конфигурации'. Это - простая задача для большинства команд показа, поскольку можно предоставить доступ через простую конфигурацию согласно ниже:

```
Маршрутизатор (config) # имя пользователя test_user привилегия 10
паролей testP@ssw0rD
Маршрутизатор (config) # уровень 10 exec привилегии показывает
Маршрутизатор (config) # show running config уровня 10 exec
привилегии
```

С конфигурацией данного примера вторая линия позволит, что 'test\_user' для имени доступа ко множеству показывают связанные команды, которые обычно не доступны в этом уровне привилегий. Однако команда show running-config рассматривается по-другому к большинству команд показа. Даже с третьей линией примера кода, только опустил/сократил 'show running config', будет отображен для пользователя несмотря на команду, задаваемую на уровне соответствующих полномочий.

Проверка пользовательского доступа

```
Username: test_user
Password:
Маршрутизатор
Привилегия Router#show
Текущий уровень привилегий равняется 10
Маршрутизатор
Router# show running-config
Создание конфигурации...
```

Текущая конфигурация: 121 байт

```
!
! Последнее изменение конфигурации в 21:10:08 UTC понедельник 28
августа 2017
!
boot-start-marker
```

```
boot-end-marker
!
!
!
конец
```

## Маршрутизатор

Как вы можете видеть эти выходные данные не показывают конфигурации и не были бы полезны пользователю, пытающемуся собирать информацию о конфигурации маршрутизатора. Это вызвано тем, что команда `show running-config` только отобразит все команды, которые пользователь в состоянии модифицировать в их текущем уровне привилегий. Это разработано как конфигурация безопасности, чтобы препятствовать тому, чтобы пользователь имел доступ к командам, которые были настроены от выше их текущего уровня привилегий. Это - проблема при попытке создать пользователя с доступом к командам показа, как `'show running config'` является стандартной командой для инженеров для начального сбора при устранении проблем.

## Решение для конфигурации и проверка

Как решение этой дилеммы, существует другая версия традиционной команды `show run`, которая обойдет это ограничение команды.

```
Маршрутизатор (config) # полное представление show running config
Маршрутизатор (config) # полное представление show running config
уровня 10 exes привилегии
```

Добавление 'представления, полного' к команде, (и в свою очередь уровень привилегий команды для предоставления пользовательского доступа к команде), теперь позволяет пользователю просматривать полный `show running config` без любых опущенных команд.

```
Username: test_user
Password:
Маршрутизатор
Привилегия Router#show
Текущий уровень привилегий равняется 10
Маршрутизатор
Полное представление running-config Router#show
```

Создание конфигурации...

```
Текущая конфигурация: 2664 байта
!
! Последнее изменение конфигурации в 21:25:45 UTC понедельник 28
августа 2017
!
версия 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
никакая поддержка активности избыточного направления платформы
disable-kernel-core
!
```

```
hostname Router
!
boot-start-marker
boot system flash bootflash: packages.conf
boot system flash bootflash: asr1000rp1-adventerprisek9.03.13.06a.
S.154-3. S6a-ext.bin
boot-end-marker
!
Mgmt-intf vrf definition
!
  ipv4 address-family
  exit-address-family
!
address-family ipv6
  exit-address-family
!
enable password <опущен>
!
no aaa new-model
!
no ip domain lookup
!
абонент, обрабатывающий по шаблону
!
имя многоканальной связки аутентифицировалось
!
spanning-tree extend system-id
!
имя пользователя test_user привилегия 10 паролей 0 testP@ssw0rD
!
резервирование
  режим sso
!
cdp run
!
интерфейс GigabitEthernet0/2/0
  no ip address
  отключение
  negotiation auto
!
интерфейс GigabitEthernet0/2/1
  no ip address
  отключение
  negotiation auto
!
интерфейсный GigabitEthernet0
  Mgmt-intf пересылки "VRF"
  IP-адрес <опущен>
  negotiation auto
  cdp enable
!
ip forward-protocol без обозначения даты
!
```

```
плоскость управления
!
!
полное представление show running config уровня 10 exec привилегии
полное представление show running config show running config exec
псевдонима
!
line con 0
  -Стоповые разряды: 1
line aux 0
  exec-timeout 0 1
  no exec
  transport output ни один
  -Стоповые разряды: 1
line vty 0 4
login local
!
конец
Маршрутизатор
```

Однако, это действительно тогда поднимает вопрос путем обеспечения пользовательского доступа к этой версии команды, разве это не повышает начальную угрозу безопасности, которая пыталась быть решенной путем разработки опущенной версии?

Как обходной путь к решению и гарантировать непротиворечивость в дизайне защищенной сети, мы можем создать псевдоним для пользователя, который выполнит полную версию команды `show running-config`, не предоставляя доступ/знание к пользователю, как показано ниже:

```
Маршрутизатор (config) # искажает полное представление show running
config show running config exec
```

В данном примере `'show running config'` является названием псевдонима, и когда пользователь зарегистрирован в маршрутизатор, они могут тогда ввести это имя псевдонима вместо команды и получить ожидаемые выходные данные без ведома фактической команды, которая выполняется.

## Заключение

В заключение это - всего один пример того, как иметь больший контроль, когда административное создание полномочий пользователя обращается на разных уровнях. Существует множество опций для создания различных уровней привилегий и доступа к другим командам, и это - пример того, как гарантировать, что у пользователя 'только показа' все еще есть доступ к полному `running-config`, когда у них нет доступа ни к каким командам настройки.