

Содержание

[Введение](#)

[Перед началом работы](#)

[Условные обозначения](#)

[Предварительные условия](#)

[Используемые компоненты](#)

[Порядок действий для настройки](#)

[Дополнительные сведения](#)

Введение

Catalyst 1900/2820 8.x Enterprise Edition выпуск программного обеспечения поддерживает TACACS + (не XTACACS). TACACS + или настройка пользователя Сервера CiscoSecure для аутентификации совпадает с для пользователей маршрутизатора. Этот практический совет описывает настройку на Catalyst 1900 и 2820.

Примечание: Аварийное переключение на 1900 и 2820 внедрено по-другому, чем на другом оборудовании Cisco. Если TACACS + сервер недоступим, локальные пароли могут использоваться, или никакая аутентификация не требуется (в зависимости от того, как коммутатор настроен). Несмотря на то, что, если TACACS + сервер будет достижим, но TACACS + демон не работает, то локальные пароли и аварийное переключение ни к какой аутентификации не будут использоваться (другими словами, вы будете заблокированы из коммутатора).

Примечание: Вебы - подключения HTTP всегда аутентифицируются с помощью локального пароля (не tacacs +). Когда TACACS + включен, использование опций меню не допустимо. TACACS + используется для аутентификации интерфейса командной строки.

Перед началом работы

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Порядок действий для настройки

1. От интерфейса командной строки (CLI) включите TACACS + аутентификация для входа в систему с помощью команды ниже.**вход в систему TACACS**
2. Используйте команду ниже для сообщения коммутатора, где сервер.**tacacs-server host 1.1.1.1**
3. Используйте команду ниже для сообщения коммутатора, каков общий ключ.**tacacs-server key cisco**
4. Выберите одну из этих двух опций ниже.Используйте команду ниже, чтобы сказать коммутатору пароль, чтобы использовать, если TACACS + сервер становится недостижимым.**Cisco уровня 1 enable password**Используйте команду ниже, чтобы сказать коммутатору использовать локальный пароль, если TACACS + сервер становится недостижимым.**пароль последнего средства tacacs-server**Используйте команду ниже, чтобы сказать коммутатору впускать пользователей без пароля, если TACACS + сервер становится недостижимым.**последнее средство tacacs-server успешно выполняется**Прежде, чем выйти из коммутатора, Telnet к коммутатору от другого сеанса, чтобы быть уверенными можно войти в использование TACACS +. Прежде, чем выйти из коммутатора, сделайте сервер недостижимым, чтобы быть уверенными, что можно войти, не используя TACACS +. Оставшиеся действия являются дополнительными.
5. Используйте команду ниже для включения TACACS + аутентификация для режима включения.**включите tacacs использования****Примечание:** Этот шаг необходим, только если включают пользователей, должны аутентифицироваться через TACACS + сервер; там также потребности быть разрешать запись в сервере для этого для работы.
6. Используйте команду ниже для включения локальной проверки подлинности для режима включения, если TACACS + сервер становится недостижимым.**Cisco уровня 15 enable password**Этот пароль допустим, только если также настроен пароль последнего средства tacacs-server.
7. Используйте команду ниже для настройки количества попыток входа, позволенных на TACACS + сервер.**номер tacacs-server attempts**
8. Используйте команду ниже для установки интервала времени ожидания, в котором демон сервера должен ответить (это является дополнительным, но могло быть необходимым в медленной сети).**tacacs-server timeout N**

Дополнительные сведения

- [Техническая поддержка - Cisco Systems](#)