Проверка подлинности PPP с использованием команд ppp chap hostname и ppp authentication chap callin

Содержание

Введение

Согласование PPP включает в себя несколько этапов, таких как согласование протокола управления каналом (LCP), согласование аутентификации и согласование протокола управления сетью (NCP). Если обе стороны не могут прийти к согласию с корректными параметрами, то соединение разрывается. После установления соединения обе стороны выполняют проверку подлинности по протоколу, выбранному в ходе согласования LCP. До начала согласования NCP необходимо успешно завершить аутентификацию.

PPP поддерживает два протокола аутентификации: Протоколы проверки пароля PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol).

Предварительные условия

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco IOS® Software Release 11.2 или более новой версии

Теоретические сведения

Аутентификация PAP включает двусторонее представление, куда имя пользователя и пароль передается через ссылку в открытом тексте; следовательно, Аутентификация PAP не предоставляет защиты от воспроизведения и анализа линии.

Аутентификация CHAP, с другой стороны, периодически проверяет идентичность удаленного узла с помощью трехэтапного установления связи. После того, как Канал "PPP" установлен, хост передает сообщение "challenge" к удаленному узлу. Удаленный узел отвечает вычисленным использованием значения функции однонаправленного хэширования. Хост проверяет ответ против своего собственного вычисления ожидаемого значения хеша. Если значения совпадают, аутентификация подтверждена; в противном случае происходит разъединение подключения.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Для получения дополнительной информации о командах, встречающихся в этом документе, используйте средство поиска команд

Настройка однонаправленной аутентификации CHAP

Когда два устройства обычно используют Аутентификацию CHAP, каждая сторона отсылает проблему, на которой другая сторона отвечает и аутентифицируется претендентом. Каждый примыкает, аутентифицирует друг друга независимо. Если вы хотите действовать с маршрутизаторами отличный от Cisco, которые не поддерживают аутентификацию вызывающим маршрутизатором или устройством, необходимо использовать **команду ppp authentication chap callin**. При использовании **команды ppp authentication** с **ключевым словом callin** Сервер доступа будет только аутентифицировать удаленное устройство, если удаленное устройство инициировало вызов (например, если удаленное устройство "призвало"). В этом случае аутентификация задана на входящих (полученных) вызовах только.

Настройка имени пользователя, отличного от имени в маршрутизаторах

Когда удаленный маршрутизатор Cisco соединяется или с Cisco или с центральным маршрутизатором не-Cisco другого административного контроля, интернет-провайдера

(ISP) или ротации центральных маршрутизаторов, необходимо настроить имя пользователя для проверки подлинности, которое отличается от имени хоста. В этой ситуации имя хоста маршрутизатора не предоставлено или другое в разное время (ротация). Кроме того, имя пользователя и пароль, которое выделено интернет-провайдером, может не быть именем хоста удаленного маршрутизатора. **В такой ситуации используется команда ppp chap hostname, чтобы определить альтернативное имя пользователя, которое будет использоваться для аутентификации.**

Например, рассмотрите ситуацию, где несколько удаленных устройств набирают в центральный узел. Использование обычной Аутентификации CHAP, имя пользователя (который был бы именем хоста) каждого удаленного устройства и общего секретного ключа должно быть настроено на центральном маршрутизаторе. В этом сценарии конфигурация центрального маршрутизатора может стать длинной и громоздкой для управления; однако, если удаленные устройства используют имя пользователя, которое отличается от их имени хоста, этого можно избежать. Центральный узел может быть настроен с одиночным именем пользователя и общим секретным ключом, который может использоваться для аутентификации множественных клиентов входящих звонков.

Схема сети

Если бы маршрутизатор 1 инициирует вызов к маршрутизатору 2, маршрутизатор 2 отправил бы запрос к маршрутизатору 1, но маршрутизатор 1 не отправил бы запрос к маршрутизатору 2. Это происходит, потому что **команда ppp authentication chap callin** настроена на маршрутизаторе 1. Это пример однонаправленной аутентификации.

В этой настройке команда **ppp chap hostname alias-r1** настроена на маршрутизаторе 1. Маршрутизатор 1 использует "alias-r1" в качестве своего имени хоста для Аутентификации CHAP вместо "r1". Название схемы набора номеров маршрутизатора 2 должно совпасть с ppp chap hostname маршрутизатора 1; иначе устанавливаются два B канала, по одному для каждого направления.

Конфигурации

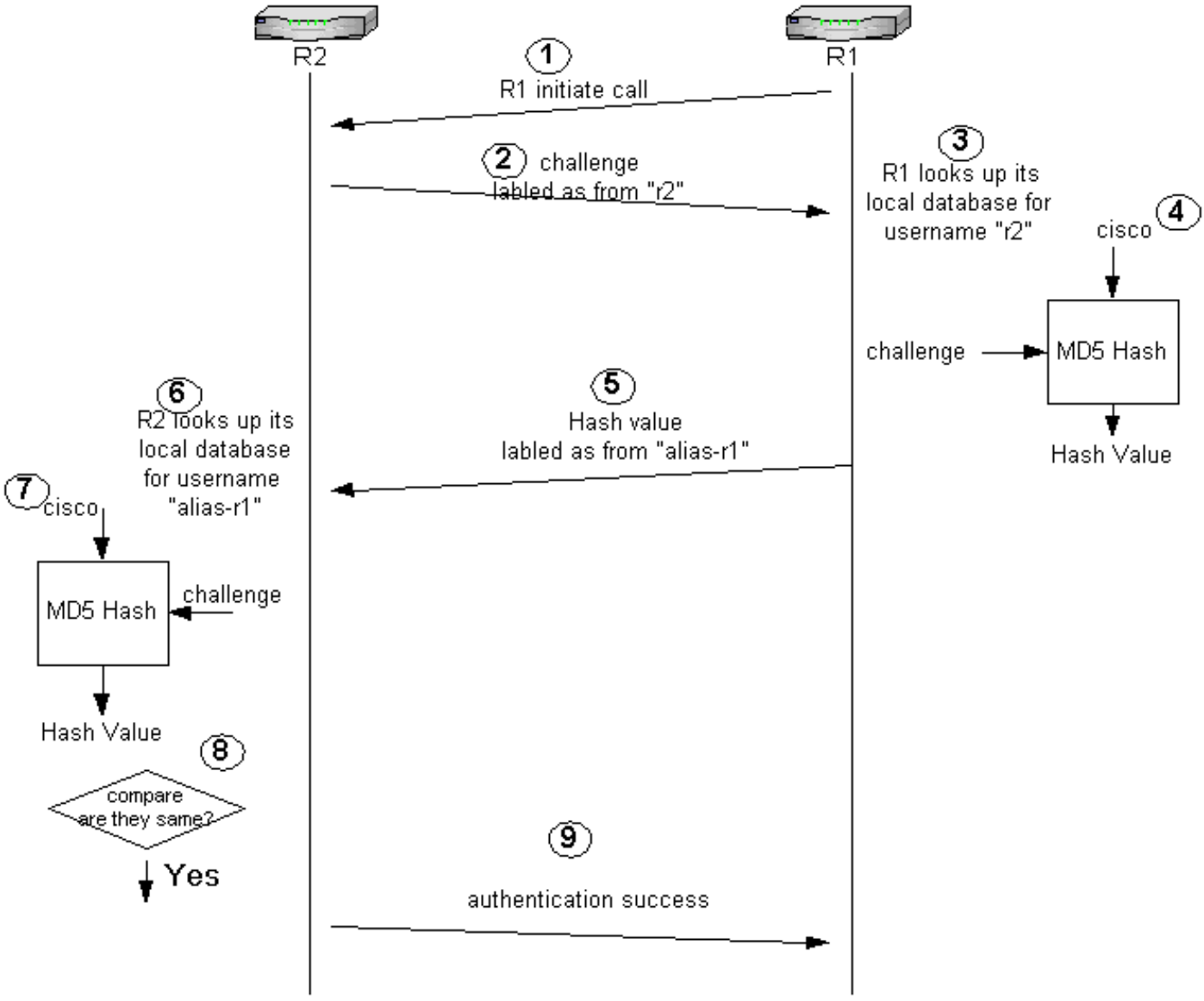
Маршрутизатор 1

```
!
 isdn switch-type basic-5ess
 !
 hostname r1 ! username r2 password 0 cisco ! --
Hostname of other router and shared secret ! interface
BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip directed-
broadcast encapsulation ppp dialer map ip 20.1.1.2 name
r2 broadcast 5772222 dialer-group 1 isdn switch-type
basic-5ess ppp authentication chap callin ! --
Authentication on incoming calls only ppp chap hostname
alias-r1 ! -- Alternate CHAP hostname ! access-list 101
permit ip any any dialer-list 1 protocol ip list 101 !
```

Маршрутизатор 2
! isdn switch-type basic-5ess ! hostname r2 ! **username alias-r1 password 0 cisco** *! -- Alternate CHAP hostname and shared secret. ! -- The username must match the one in the* ***ppp chap hostname*** *! -- command on the remote router.* ! interface BRI0/0 ip address 20.1.1.2 255.255.255.0 no ip directed-broadcast encapsulation ppp dialer map ip 20.1.1.1 name **alias-r1** broadcast 5771111 *! -- Dialer map name matches alternate hostname "alias-r1".* dialer-group 1 isdn switch-type basic-5ess ppp authentication chap ! access-list 101 permit ip any any dialer-list 1 protocol ip list 101 !

Объяснение конфигурации

См. номера ниже этого рисунка для получения объяснений:



1. В этом примере маршрутизатор 1 инициирует все вызовы. **Поскольку маршрутизатор 1 настроен с помощью команды ppp authentication chap callin, он не вызывает**

вызывающую сторону, то есть маршрутизатор 2.

2. Когда маршрутизатор 2 принимает вызов, он отправляет запрос к маршрутизатору 1 для аутентификации. По умолчанию для этой аутентификации, имя хоста маршрутизатора используется для определения себя. *Если настроена команда ppp chap hostname name, вместо имени хоста для идентификации маршрутизатора используется имя*. В этом примере вызов маркируется как поступающий от "r2"."
3. Маршрутизатор 1 принимает вызов маршрутизатора 2 и ищет в его локальной базе данных имя пользователя "r2"."
4. Маршрутизатор 1 находит "r2" пароль, который является "Cisco". Маршрутизатор 1 использует этот пароль и вызов со стороны маршрутизатора 2 как параметры ввода хэш-функции MD5. Генерируется значение хэша.
5. Маршрутизатор 1 передает выходное значение хеша к маршрутизатору 2. **Поскольку команда ppp chap hostname конфигурируется как "alias-r1, ответ маркируется как пришедший от "alias-r1."**."
6. Маршрутизатор 2 получает ответ и выполняет поиск пароля для имени пользователя "alias-r1" в локальной базе данных.
7. Маршрутизатор 2 находит, что пароль для "alias-r1" является "Cisco". Маршрутизатор 2 использует пароль, и проблема отослала ранее в маршрутизатор 1 как параметры ввода для хэш-функции MD5. Функция хеширования генерирует значение хеширования.
8. Маршрутизатор 2 сравнивает значение хеша, созданное им, с полученным от маршрутизатора 1.
9. Так как параметры ввода (проблема и пароль) идентичны, значение хеш-функции - то же приводящее к успешной аутентификации.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Перед попыткой выполнения любой команды отладки ознакомьтесь с важной информацией о командах Debug

Пример результата отладки

Ниже приведен пример вывода команды debug ppp authentication:

Маршрутизатор 1

```
r1#ping 20.1.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 20.1.1.2,
timeout is 2 seconds: *Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to
up *Mar 1 20:06:27.183: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 *Mar 1
20:06:27.187: BR0/0:1 PPP: Treating connection as a callout *Mar 1 20:06:27.223: BR0/0:1 CHAP: I
CHALLENGE id 57 len 23 from "r2" ! -- Received a CHAP challenge from other router (r2) *Mar 1
20:06:27.223: BR0/0:1 CHAP: Using alternate hostname alias-r1 ! -- Using alternate hostname
```

configured with ! -- ppp chap hostname command *Mar 1 20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" *! -- Sending response from "alias-r1" ! -- which is the alternate hostname for r1* *Mar 1 20:06:27.243: BR0/0:1 CHAP: I SUCCESS id 57 Len 4 *! -- Received CHAP authentication is successful ! -- Note that r1 is not challenging r2* .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1# *Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2

Маршрутизатор 2

```
r2#

  20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
  20:05:20: BR0/0:1 PPP: Treating connection as a callin
  20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
  ! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
"alias-r1" ! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1
20:05:21: BR0/0:1 CHAP: O SUCCESS id 57 Len 4 ! -- Sending out CHAP authentication is successful
20:05:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up
20:05:26: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111 alias-r1
```

Дополнительные сведения

- Команды PPP для глобальной сети
- Основные сведения о протоколе PPP и его аутентификации
- Отладочные сведения об ISDN