

Устранение неисправностей аутентификации PPP (CHAP или PAP)

Содержание

[Введение](#)

[Предварительные условия](#)

[Терминология](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Блок-схема устранения неполадок](#)

[Какую аутентификацию проводит маршрутизатор - CHAP или PAP?](#)

[Маршрутизатор выполняет двустороннюю или одностороннюю аутентификацию по протоколу с предварительным согласованием вызова?](#)

[Ошибка входных данных?](#)

[Имя пользователя в исходящем запросе или ответе то же самое, что имя узла?](#)

[Является ли удаленный компьютер маршрутизатором Cisco, к которому есть доступ?](#)

[Устранение неполадок исходящего трафика CHAP](#)

[Маршрутизатор использует схему No AAA или Only Local AAA](#)

[Поиск и устранение общих серверных проблем аутентификации, авторизации и учета](#)

[Дополнительные сведения](#)

Введение

Проблемы аутентификации протокола PPP относятся к числу наиболее распространенных причин сбоев канала удаленного доступа. В этом документе представлены некоторые Процедуры поиска и устранения неисправностей аутентификации PPP.

Предварительные условия

- [Включите debug ppp negotiation и debug ppp authentication.](#)
- Фаза аутентификации PPP не начинается, пока фаза Протокола управления каналом (LCP) не завершена и находится в открытом состоянии. Если в выходных данных команды `debug ppp negotiation` не указано, что LCP открыт, устраните эту проблему перед продолжением.
- Необходимо настроить аутентификацию PPP на обеих сторонах. Выполните эти команды как соответствующие: [ppp authentication chap на обоих маршрутизаторах для двусторонней аутентификации CHAP](#), [ppp authentication chap callin в вызывающем маршрутизаторе для односторонней аутентификации](#), [pap аутентификации "PPP" на обоих маршрутизаторах, для Аутентификации PAP.](#)

Терминология

- **Локальный компьютер** (или локальный маршрутизатор) - Это - система, в которой в настоящее время выполняется сеанс отладки. Если сеанс отладки перемещается с одного маршрутизатора на другой, термин "локальный компьютер" будет применяться к другому маршрутизатору.
- **Узел** - другой конец канала типа точка-точка. Следовательно, устройство не является локальным компьютером. Например, при выдаче команды [debug ppp negotiation](#) на RouterA тогда это - локальный компьютер, и RouterB является узлом. Однако при смещении отладки в RouterB тогда это становится локальным компьютером, и RouterA становится узлом.

Примечание: Термины "Локальная машина" и "Равноправный узел" не подразумевают отношений клиент-сервер. В зависимости от того, где выполняется сеанс отладки, клиент входящих звонков может быть локальным компьютером или одноранговым узлом.

Требования

Компания Cisco рекомендует ознакомиться с этой темой:

- Пользователь должен разбираться в выходных данных команды `debug ppp negotiation`. [Дополнительные сведения см. в документе "Общие сведения о результатах команды debug ppp negotiation"](#).

Используемые компоненты

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

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Блок-схема устранения неполадок

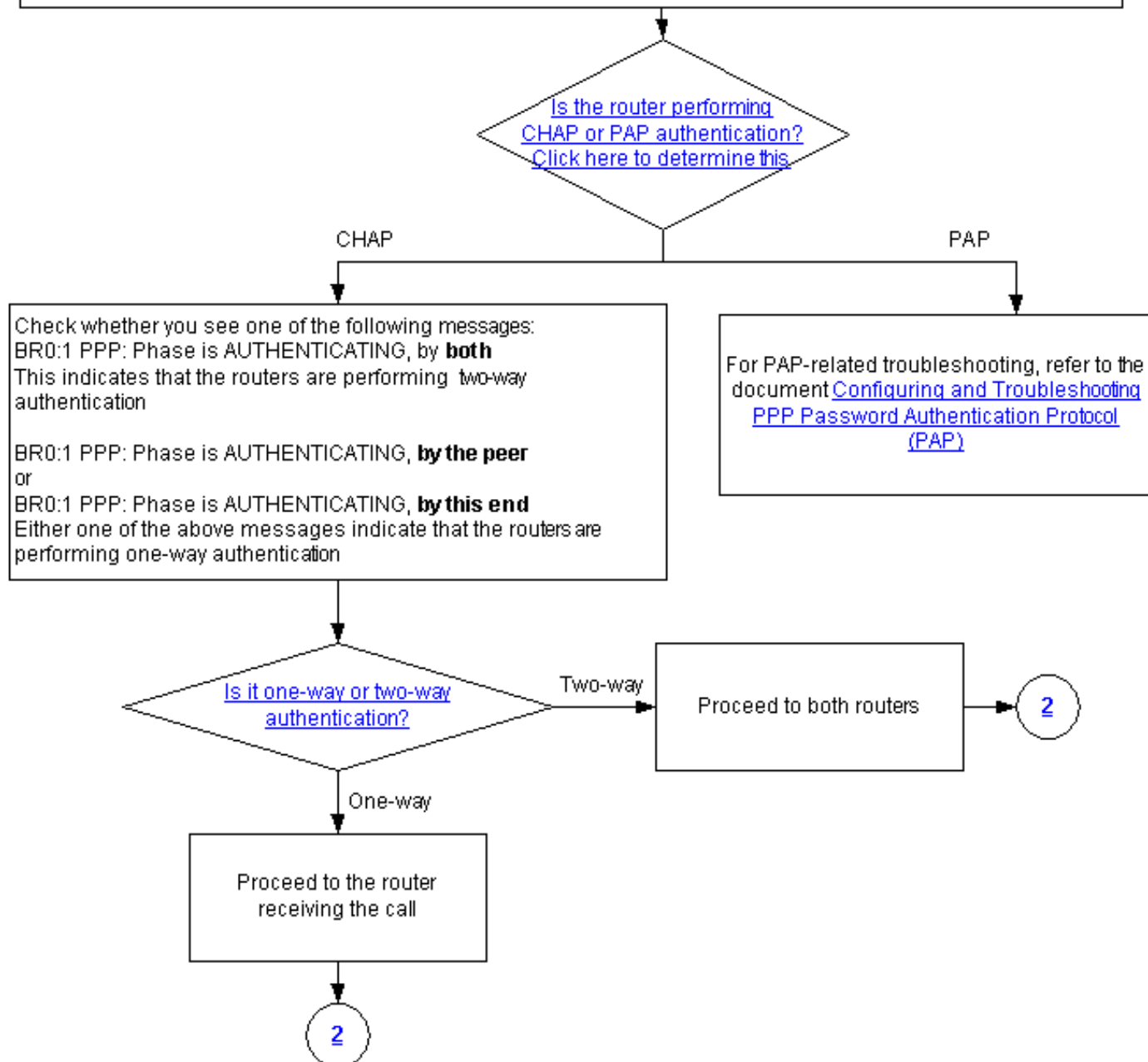
В этот документ включено несколько блок-схем, описывающих процедуры устранения проблем. Можно перейти к следующей блок-схеме, щелкнув пронумерованные кружки.

Note: Please do not skip any steps in this flowchart

Authentication can be done by both, either or neither side of the connection. Cisco highly recommends using authentication as a way of securing the network against intrusion. Authentication failures are one of the most common problems encountered in PPP negotiation.

Note: This document assumes that the LCP state is open. If the LCP state is not open, troubleshoot that issue before proceeding with this document

Enable the following debugs **debug ppp negotiation** and **debug ppp authentication**.



[Какую аутентификацию проводит маршрутизатор - CHAP или PAP?](#)

Чтобы определить, выполняет ли маршрутизатор CHAP или Аутентификацию PAP, ищите эти линии в выходных данных **debug ppp authentication** и **debug ppp negotiation**:

CHAP

Ищите CHAP в АУТЕНТИФИЦИРУЮЩЕЙСЯ фазе:

```
*Mar 7 21:16:29.468: BR0:1 PPP: Phase is AUTHENTICATING, by this end *Mar 7 21:16:29.468: BR0:1  
CHAP: O CHALLENGE id 5 len 33 from "maui-soho-03"
```

PAP

Ищите PAP в АУТЕНТИФИЦИРУЮЩЕЙСЯ фазе:

```
*Mar 7 21:24:11.980: BR0:1 PPP: Phase is AUTHENTICATING, by both *Mar 7 21:24:12.084: BR0:1  
PAP: I AUTH-REQ id 1 len 23 from "maui-soho-01"
```

Маршрутизатор выполняет двустороннюю или одностороннюю аутентификацию по протоколу с предварительным согласованием вызова?

Ищите одно из этих сообщений в выходных данных `debug ppp negotiation`:

```
BR0:1 PPP: Phase is AUTHENTICATING, by both
```

Вышеприведенное сообщение указывает на то, что маршрутизаторы выполняют двустороннюю аутентификацию.

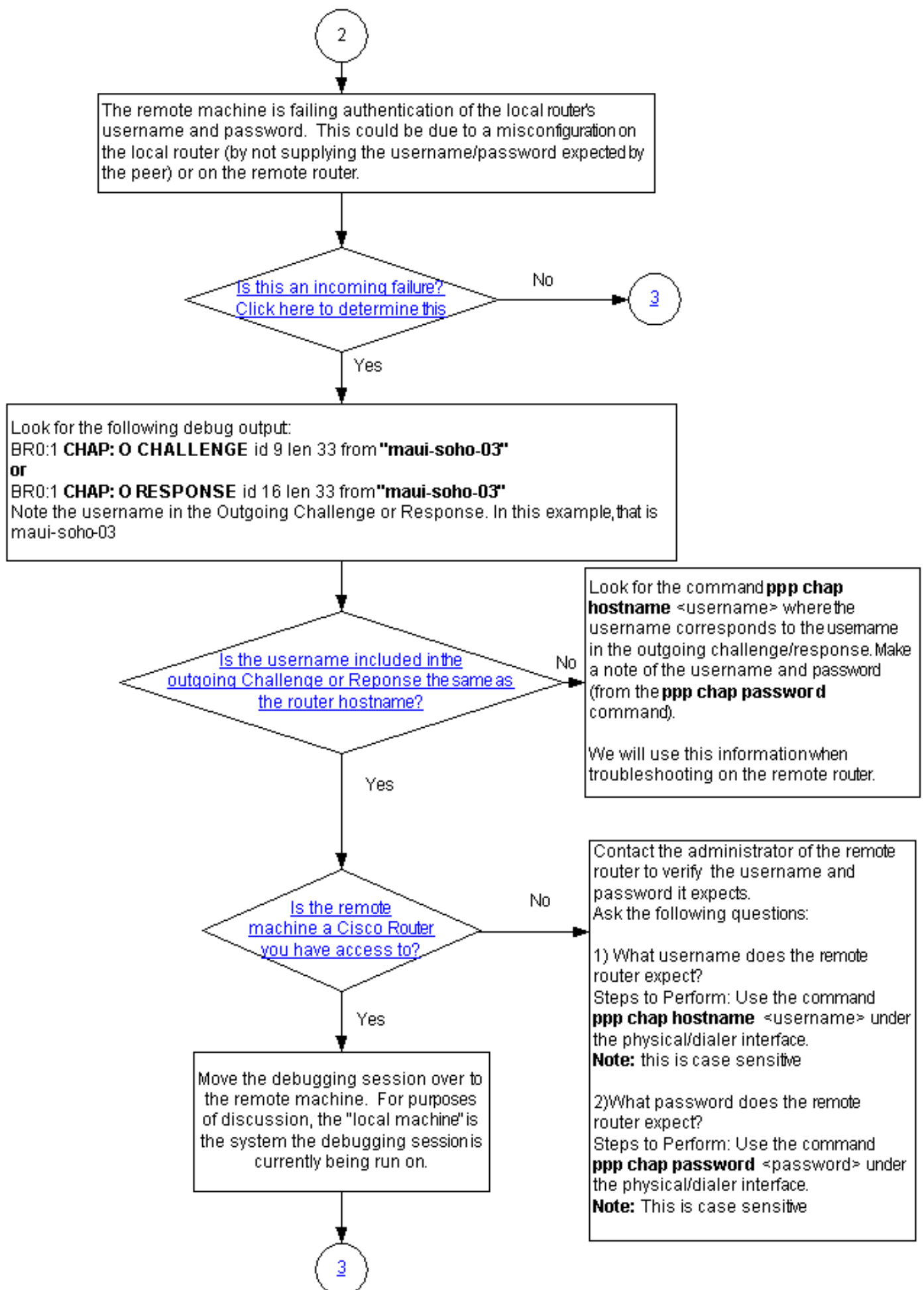
Любое из сообщений ниже указывает, что маршрутизаторы выполняют одностороннюю проверку подлинности:

```
BR0:1 PPP: Phase is AUTHENTICATING, by the peer
```

ИЛИ

```
BR0:1 PPP: Phase is AUTHENTICATING, by this end
```

Ошибка входных данных?



Проверьте, чтобы видеть, получаете ли вы поступление termreq или сообщения об ошибках.

Помните, что "I" указывает, что сообщение является входящим сообщением:

```
BR0:1 LCP: I TERMREQ
```

или

```
BR0:1 CHAP: I FAILURE
```

Сбой на входе указывает, что узел не в состоянии аутентифицировать имя пользователя и пароль локального маршрутизатора. Это может произойти из-за неверной конфигурации на локальном маршрутизаторе (если не указаны ожидаемые равноправным узлом имя пользователя и пароль) либо на удаленном маршрутизаторе.

Имя пользователя в исходящем запросе или ответе то же самое, что имя узла?

Ищите придерживающееся в выходных данных `debug ppp negotiation`:

```
BR0:1 CHAP: O CHALLENGE id 9 len 33 from "maui-soho-03"
```

или

```
BR0:1 CHAP: O RESPONSE id 16 len 33 from "maui-soho-03"
```

Обратите внимание на имя пользователя в исходящей проблеме или ответе. В данном примере это - **maui-soho-03**. Вам нужно это, чтобы проверить, что имя пользователя и пароль, используемое для аутентификации, совпадает с той, ожидаемой удаленной стороной. Например, если локальный маршрутизатор определяет себя к узлу как А, но узел ожидал В, то аутентификация отказывает.

Если имя пользователя в исходящей проблеме не является тем же как именем хоста, ищите [<username> команды ppp chap hostname](#), где имя пользователя соответствует имени пользователя в исходящей проблеме. Обратите внимание на имя пользователя и пароль (в сопроводительной команде `ppp chap password`). Вы будете использовать эту информацию при устранении проблем удаленного маршрутизатора.

Является ли удаленный компьютер маршрутизатором Cisco, к которому есть доступ?

Поскольку было выяснено, что маршрутизатор получил входящую ошибку, ясно, что ошибка происходит на одноранговом узле. Если вы имеете доступ к удаленному маршрутизатору Cisco, то устраняете неполадки на том устройстве.

Если у вас нет доступа к удаленному маршрутизатору, свяжитесь с администратором того маршрутизатора для проверки имени пользователя и пароля, которое это ожидает.

Задайте эти вопросы:

1. Какое имя пользователя ожидает удаленный маршрутизатор? Используйте команду [<username> ppp chap hostname](#) под медосмотром или интерфейсом номеронабирателя. Настройте имя пользователя, введенное удаленным администратором здесь. **Примечание:** Необходимо учитывать регистр.
2. Какой пароль удаленный маршрутизатор ожидает? Используйте команду [<password> пароля "ppp chap"](#) под медосмотром или интерфейсом номеронабирателя. **Примечание:** Необходимо учитывать регистр.

[Для получения дополнительной информации обратитесь к документу Проверка подлинности PPP с использованием команд ppp chap hostname и ppp authentication chap callin.](#)

[Устранение неполадок исходящего трафика CHAP](#)

If the peer detects an incoming failure message, this means the local router has failed to authenticate the peer and has sent out the message. Hence we must now move troubleshooting to the router on which the Outgoing Failure is seen.

The following messages on the local router indicates an outgoing failure:
 BR0:1 CHAP: O FAILURE id 10 len 26 msg is "Authentication failure"
 or
 BR0:1 LCP: O TERMREQ [Open] id 22 len 4

Does the local router use Server-based AAA
(Radius/TACACS+)?

yes

4

No, it uses either No AAA or
local AAA

Choose from one the following error messages

BR0:1 CHAP: I RESPONSE id 18 len 33 from "<username>"
 BR0:1 CHAP: Unable to validate Response. Username <username>
 not found
 BR0:1 CHAP: O FAILURE id 18 len 26 msg is "Authentication failure"
 BR0:1 PPP: Phase is TERMINATING [0 sess, 0 load]

Configure the username and shared secret for
the chap challenge
Use the command
username <username> password <password>
Note: The username should be identical to the
username in the incoming CHAP message, while
the password should be the common secret

BR0:1 CHAP: Username <username> not found
 BR0:1 CHAP: Unable to authenticate for peer
 BR0:1 PPP: Phase is TERMINATING
 BR0:1 LCP: O TERMREQ [Open] id 22 len 4

Configure the username and shared secret for
the chap challenge
Use the command
username <username> password <password>
Note: The username should be identical to the
username in the incoming CHAP message, while
the password should be the common secret

BR0:1 CHAP: I RESPONSE id 16 len 33 from "<username>"
 BR0:1 CHAP: O FAILURE id 16 len 25 msg is "MD/DES compare
 failed"

Remove the existing username/password entry
using the command:
no username <username>
 where <username> matches the one in the
CHAP message

Configure the username and password using the
command:
username <username> password <password>
 The username should be the same as in the
CHAP message shown above. The password
should match the password on the remote
router.

Если узел обнаруживает сообщение сбоя на входе, это означает, что локальный маршрутизатор был не в состоянии аутентифицировать узел и отослал сообщение.

Следовательно, необходимо теперь устранить неполадки маршрутизатора, на котором указывает на сбой передачи данных.

Эти сообщения на локальном маршрутизаторе указывают на сбой передачи данных:

```
BR0:1 CHAP: O FAILURE id 10 len 26 msg is "Authentication failure"  
или
```

```
BR0:1 LCP: O TERMREQ [Open] id 22 len 4
```

Маршрутизатор использует схему No AAA или Only Local AAA

Если маршрутизатор не использует проверку подлинности на основе сервера, авторизацию, и бухгалтерский (AAA) система (Радиус или Tacsacs +), то маршрутизатор может использовать или AAA или локальный AAA. Проверьте, видите ли вы одно из следующих сообщений в выходных данных отладки:

Невозможно проверить ответ

<Username> имени пользователя, не найденный

```
BR0:1 CHAP: I RESPONSE id 18 len 33 from "maui-soho-03" ! -- Incoming CHAP response to our  
challenge. ! -- The username used in the response is maui-soho-03. BR0:1 CHAP: Unable to  
validate Response. Username maui-soho-03 not found ! -- The username supplied by the peer is not  
configured on the router. ! -- We assume the peer does not have permission to connect. BR0:1  
CHAP: O FAILURE id 18 len 26 msg is "Authentication failure" ! -- Outgoing CHAP failure message.  
! -- The peer will see this as an incoming failure. BR0:1 PPP: Phase is TERMINATING [0 sess, 0  
load]
```

Несовпадение имен пользователя может быть вызвано двумя причинами:

1. Одноранговый узел не подает имя пользователя, ожидаемое локальным маршрутизатором. Например, мы ожидали (и настроил), имя пользователя `routera`, но узел использовал имя `МаршрутизаторВ`. Вы можете или сконфигурировать имя пользователя и пароль, высланные точкой вызова, или поправить его, сообщив правильное имя пользователя.
2. Локальный маршрутизатор не имеет конфигурированного имени пользователя. Если имя пользователя, предоставленное узлом, совпадает, что ожидаемый локальный маршрутизатор, то настройте имя пользователя и пароль.

Данная проблема чаще всего возникает тогда, когда узел использует команду `ppp chap hostname` для настройки имени пользователя, отличного от имени узла маршрутизатора.

Используйте команду *<password>* пароля *<username>* имени пользователя, где *<username>* заменен именем пользователя в сообщении об ошибках выше.

<Username> имени пользователя, не найденный

Не удается выполнить аутентификацию для узла

```
BR0:1 CHAP: I CHALLENGE id 17 len 33 from "maui-soho-01" ! -- Incoming challenge from maui-soho-  
01. ! -- This router must look up the username specified ! -- in order to create the CHAP  
response. BR0:1 CHAP: Username maui-soho-01 not found ! -- The username (maui-soho-01) supplied  
by the peer is not configured locally. BR0:1 CHAP: Unable to authenticate for peer ! -- Since  
this router does not recognize the username ! -- it cannot create the outgoing CHAP RESPONSE.  
BR0:1 PPP: Phase is TERMINATING ! -- Authentication fails.
```

Несовпадение имен пользователя может быть вызвано двумя причинами:

1. Одноранговый узел не подает имя пользователя, ожидаемое локальным маршрутизатором. Например, мы ожидали (и настроил), имя пользователя `routera`. Однако узел использовал имя МаршрутизаторВ. Можно или настроить имя пользователя и пароль, передаваемое узлом, или обновить узел с корректным именем пользователя.
2. Локальный маршрутизатор не имеет конфигурированного имени пользователя. Если имя пользователя, предоставленное узлом, совпадает, что ожидаемый локальный маршрутизатор, то настройте имя пользователя и пароль.

[Данная проблема чаще всего возникает тогда, когда узел использует команду `ppp chap hostname` для настройки имени пользователя, отличного от имени узла маршрутизатора.](#)

Используйте команду `<password>` пароля `<username>` имени пользователя, где `<username>` заменен именем пользователя в сообщении об ошибках выше.

MD/DES Выдерживают сравнение Отказавший

```
BR0:1 CHAP: I RESPONSE id 16 len 33 from "maui-soho-03" BR0:1 CHAP: O FAILURE id 16 len 25 msg
is "MD/DES compare failed"
```

Эта ошибка произошла из-за несоответствия пароля. Это могло быть причиной двумя причинами:

1. Одноранговый узел не поддерживает пароль, ожидаемый локальным маршрутизатором. Например, мы ожидали (и настроил), *пароль letmein*, но узел использовал *пароль letmein*. Можно перенастроить имя пользователя и пароль, полученные от однорангового узла, или исправить имя пользователя для этого узла.
2. Локальный маршрутизатор не имеет правильно настроенного пароля. Если вы проверили, что пароль, предоставленный узлом, корректен, то реконфигурируйте локальный маршрутизатор.

Решение:

1. Удалите существующую запись имени пользователя и пароля с помощью этой команды:
`no username <username>` Где `<username>` заменен именем пользователя в сообщении об ошибках. В данном примере, который был бы `maui-soho-03`.
2. Настройте имя пользователя и пароль с помощью этой команды:
`username <username> password <password>` Имя пользователя должно совпасть с в сообщении CHAP, показанном выше. Пароль должен совпадать с паролем на удаленном маршрутизаторе.

[Поиск и устранение общих серверных проблем аутентификации, авторизации и учета](#)

4

This section has some simple AAA troubleshooting points.
It can be used to troubleshoot both CHAP and PAP authentication

Enable the following debugs:
debug aaa authentication
and
debug radius
or
debug tacacs

Note: For Radius (prior to 12.2XB) , the debug output will need to be decoded. Use the [Output Interpreter tool](#).
In the radius/tacacs debug output, check to see if you are receiving an Access-Accept from the server. For example:
*Mar 1 05:07:40.310: RADIUS: Received from id 4 172.22.53.201:1645, Access-Accept, len 50

Do you see an Access-Accept?

Yes

No

Check to see if you get a Sendauth failure, which happens only for Radius with two-way authentication. The following debug shows an example:

```
AAA/AUTHEN/START (776188141): port='BR0:1' list=""  
action=SENDAUTH service=PPP  
AAA/AUTHEN/START (776188141): using "default" list  
AAA/AUTHEN/START (776188141): Method=radius  
(radius)  
AAA/AUTHEN/SENDAUTH (776188141): missing  
password for maui-soho-03  
AAA/AUTHEN/SENDAUTH (776188141): Failed  
sendauthen for maui-soho-03  
AAA/AUTHEN (776188141): status = FAIL  
AAA/AUTHEN/START (776188141): no methods left to try  
AAA/AUTHEN (776188141): status = ERROR  
AAA/AUTHEN/START (776188141): failed to authenticate  
BR0:1 CHAP: Username maui-soho-03: lookup failure
```

Configure one-way authentication by configuring the command **ppp authentication chap callin** on the dialout side

Please perform the following general troubleshooting steps:

- 1) Check if you have connectivity with the AAA server (try to ping the AAA server from the local router)
- 2) Check if the AAA server is correctly specified using the radius-server host or tacacs-server host command
- 3) Check if the secret key used between the local router and the AAA server is correct (use the command radius-server key and tacacs-server key)
- 4) Check if the local router is correctly identified in the AAA server configuration
- 5) Check if the username and password that is used for authentication is correctly configured on the AAA server

For more information refer to the Radius/Security Technical Tips Page

If you see an Access-Accept and CHAP authentication still fails, then contact the Cisco TAC for further troubleshooting

Примечание: Данная документация не является средством устранения неисправностей AAA. Для получения дополнительной информации об устранении проблем AAA обратитесь к следующим ресурсам:

- [Операции AAA](#)
- [RADIUS](#)
- [TACACS](#)

Проблема: Аутентификация PAP работает для PPP, но сбояв MSCHAPV2

Вы не могли бы быть в состоянии аутентифицироваться на сервере ACS, потому что сервер ACS не получает запрос аутентификации, который заставляет сеанс отказывать. Это поведение наблюдается и зарегистрировано под идентификатором ошибки Cisco [CSCee04466 \(только зарегистрированные клиенты\)](#). Как обходной путь, используйте сервер RADIUS для сеансов PPP. Однако поддержите TACACS + сервер для административных целей на маршрутизаторе.

Дополнительные сведения

- [Выходные данные команды "debug ppp negotiation"](#)
- [Общие сведения и настройка аутентификации PPP CHAP](#)
- [Проверка подлинности PPP с использованием команд ppp chap hostname и ppp authentication chap callin](#)
- [Настройка и устранение неисправностей протокола аутентификации пароля PPP \(PAP\)](#)
- [Набор и поддержка технологии доступа](#)
- [Cisco Systems – техническая поддержка и документация](#)