

# Выходные данные команды "debug ppp negotiation"

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Стадии согласования PPP](#)

[Пакеты согласования PPP: описание](#)

[LCP, аутентификация и этап работы протокола NCP](#)

[Устранение проблем с Выходными данными debug ppp negotiation](#)

[Считайте Выходные данные debug ppp negotiation](#)

[Пример выходных данных команды debug ppp negotiation](#)

[Глоссарий и распространенные сообщения](#)

[Общие сведения](#)

[LCP](#)

[Authentication](#)

[NCP](#)

[Дополнительные сведения](#)

## **[Введение](#)**

В приложениях, использующих удаленный доступ, как правило, используется тип инкапсуляции PPP. PPP позволяет двум компьютерам на канале связи типа «точка-точка» согласовывать различные параметры аутентификации, сжатия, а также протоколы 3 уровня (L3), например IP. Сбой в согласовании PPP между двумя маршрутизаторами может привести к сбою подключения.

Команда `debug ppp negotiation` позволяет просматривать транзакции согласования PPP, определять проблему или этап, на котором возникла проблема, и разрабатывать решение. Однако считается обязательным понимать выходные данные команды `debug ppp negotiation`. В этом документе описан метод полноценного чтения выходных данных команды `debug ppp negotiation`.

## **[Предварительные условия](#)**

### **[Требования](#)**

Читатели должны выполнить следующие требования:

- PPP необходимо включить на интерфейсах обоих маршрутизаторов. **Выполните команду `encapsulation ppp` для выполнения этой задачи.**
- Выполните эту команду, чтобы включить на маршрутизаторе штамп времени в миллисекундах: `Router(config)# service timestamp debug datetime msec` Для получения дополнительной информации о командах отладки посмотрите [раздел Важные сведения о командах отладки](#).

**Примечание:** Согласование PPP между двумя узлами не может запуститься, пока низший уровень (ISDN, физический интерфейс, линия коммутируемого доступа, и так далее) под PPP не функционирует отлично. Например, если следует использовать PPP по каналу ISDN, необходимо включить все уровни ISDN, иначе протокол PPP не будет функционировать.

## 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 Технические рекомендации Cisco. Условные обозначения.](#)

## Стадии согласования PPP

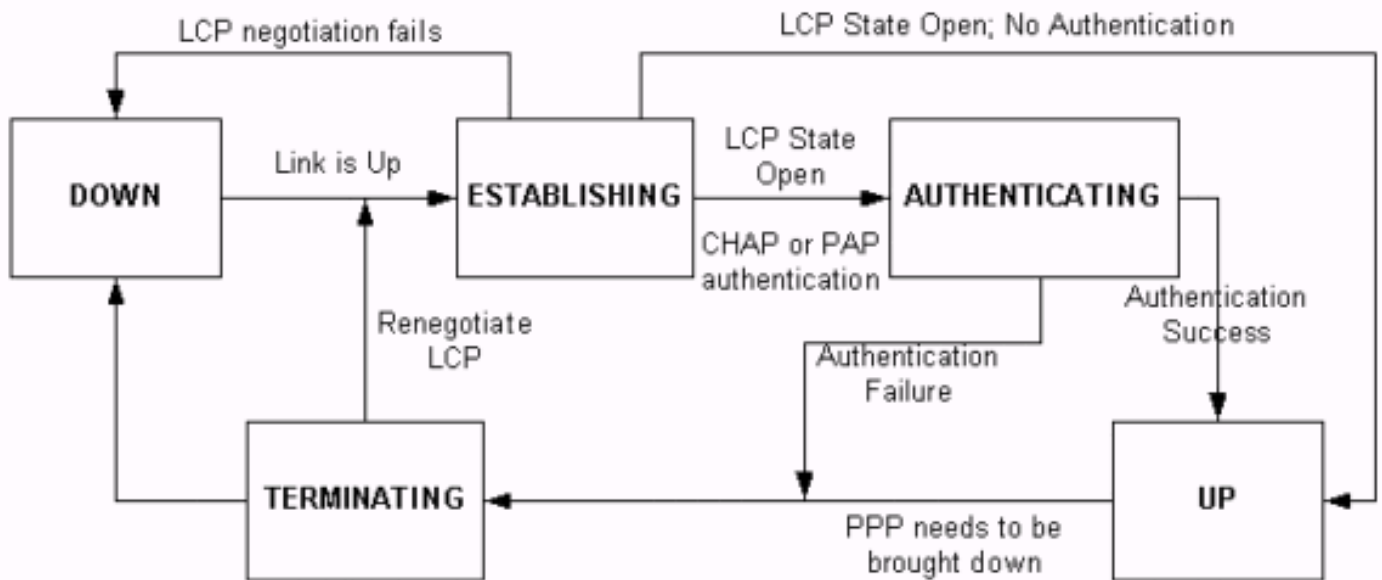
Согласование PPP на канале состоит из нескольких этапов, как показано в следующей таблице. В результате PPP либо начинает работать, либо нет.

Фаза	Описание
отключен	На этом этапе PPP отключен. Данное сообщение отображается после отключения канала и PPP: <code>*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN</code>
УСТАНОВЛЕНИЕ	Передача PPP будет продолжаться до момента получения уведомления о том, что физический уровень готов к использованию. Согласование LCP <sup>1</sup> происходит в этой фазе. <code>*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING</code>
АУТЕНТИФИКАЦИЯ	Если проверка подлинности PPP (CHAP <sup>2</sup> или PAP <sup>3</sup> ) желательна на ссылке, то переходы PPP к этой фазе. Помните, что аутентификация PPP не является обязательной. <code>*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING</code>
включен	После завершения аутентификации PPP переходит на этап UP. Согласование NCP <sup>4</sup> происходит в этой фазе. <code>*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP</code>
ЗАВЕРШЕНИЕ	На этом этапе PPP отключается. <code>*Mar 3 23:43:23.256: BR0:1 PPP: Phase is</code>

TERMINATING
-------------

1. LCP = протокол управления каналом
2. CHAP = протокол аутентификации по квитированию вызова
3. PAP = протокол аутентификации пароля
4. NCP = протокол управления сетью

На следующей схеме показаны этапы переходов PPP:



## Пакеты согласования PPP: описание

В этой таблице содержится описание пакетов согласования PPP, которые используются как при согласовании LCP, так и при согласовании NCP:

Пакет	Код	Описание
CONFREQ	Configure-Request	Чтобы открыть подключение к одноранговому участнику, устройство передает это сообщение вместе с параметрами и значениями конфигурации, поддержку которых отправитель требует от однорангового участника. Все параметры и значения согласовываются одновременно. Если одноранговый участник отвечает сообщением CONFREJ или CONFNAK, маршрутизатор отправляет еще одно сообщение CONFREQ с другим набором параметров или значений.
CONFREJ	Configure-Reject	Если какие-либо параметры конфигурации, полученные в

J		сообщении CONFREQ, являются недопустимыми или нераспознанными, маршрутизатор отвечает сообщением CONFREJ. Недопустимый параметр (из сообщения CONFREQ) включается в сообщение CONFREJ.
CONFNAK	Configure-NAK1	Если полученный параметр конфигурации определяется и считается допустимым, однако полученное значение не является допустимым, маршрутизатор передает сообщение CONFNAK. Маршрутизатор присоединяет этот параметр и значение, которое он может принять, к сообщению CONFNAK, так что одноранговый участник может включить этот параметр в следующее сообщение CONFREQ.
CONFACK	Configure-ACK2	Если все параметры в сообщении CONFREQ распознаны и все значения являются допустимыми, маршрутизатор передает сообщение CONFACK.
TERMREQ	Terminate-Request	Данное сообщение используется для инициации закрытия LCP.
TERMACK	Terminate-ACK	Это сообщение передается в ответ на сообщение TERMREQ.

1. NAK = отрицательное квитирование

2. ACK = подтверждает

**Примечание:** Каждый узел может передать CONFREQ с опцией или значением, которое это хочет, чтобы узел поддержал. Это может привести к тому, что параметры, согласованные в обоих направлениях, будут отличаться. Например, одна сторона может требовать аутентификации одноранговых участников, другая сторона — нет.

## [LCP, аутентификация и этап работы протокола NCP](#)

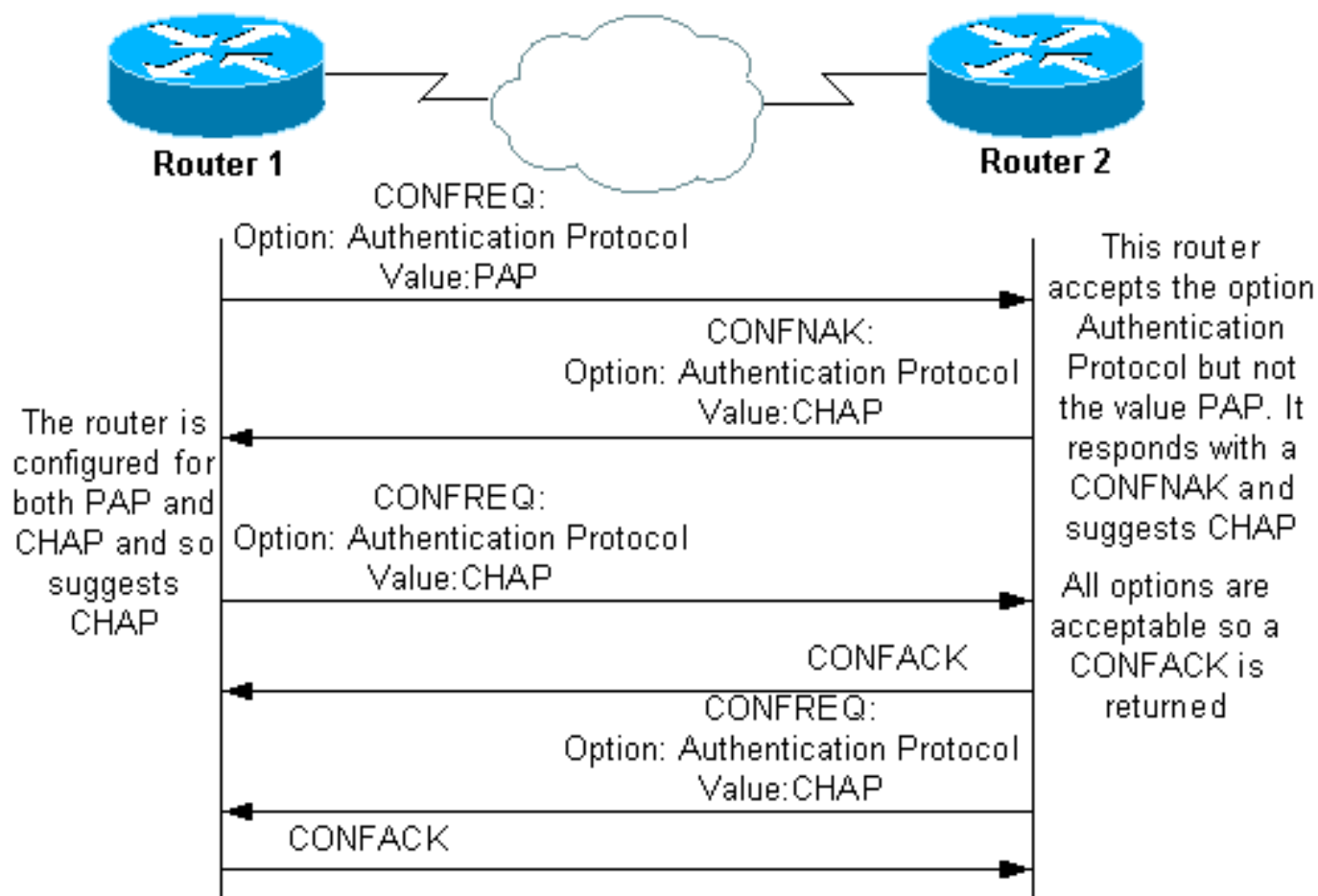
В некоторых фазах PPP, описанных ранее, PPP также входит в определенные этапы, такие как согласование LCP, аутентификация и согласование NCP. Для получения дополнительной информации обратитесь к [RFC 1548](#) и [RFC 1661](#).

### [LCP \(обязательный этап\)](#)

LCP – это этап, на котором согласуются параметры, которые необходимы для создания, настройки и проверки подключения по каналу передачи данных. Открытое состояние LCP

означает успешное завершение LCP, в то время как закрытое состояние LCP означает сбой на этапе LCP.

На следующей схеме приведена концепция установления связи LCP:



При согласовании LCP также используется параметр, называемый MagicNumber, который используется для определения, является ли канал связи возвратной петлей. Случайная строка отправляется по каналу, и если возвращается то же значение, то маршрутизатор определяет, что канал является возвратной петлей.

### [Аутентификация \(Дополнительная фаза по умолчанию\)](#)

На этом этапе выполняется аутентификация с помощью протокола аутентификации (CHAP или PAP), согласованного на этапе LCP. Для дополнительных сведений PAP обратитесь к [Настройке и Протоколу аутентификации Пароля PPP Устранения проблем \(PAP\)](#).

Для дополнительных сведений CHAP обратитесь к [Проверке подлинности CHAP PPP Настройки и Пониманию](#).

**Примечание:** Аутентификация является дополнительной, и PPP только вводит этот этап, если это должно аутентифицироваться.

### [NCP \(обязательный этап\)](#)

Этот этап используется для подключения и настройки других протоколов сетевого уровня. Наиболее распространенным согласуемым протоколом третьего уровня является IP.

Маршрутизаторы обмениваются сообщениями протокола управления IP (IPCP) для согласования параметров, применимых к протоколу (в этом случае — IP).

[RFC 1332](#) говорит, что IPCP выполняет согласование о двух опциях: сжатие и назначение IP-адресов. Однако протокол IPCP также используется для передачи сетевых данных, таких как основные и резервные серверы WINS и DNS.

Согласование происходит при использовании Сообщений CONF, как описано в [Пакетах согласования PPP](#): раздел [Описания](#) этого документа.

## [Устранение проблем с Выходными данными debug ppp negotiation](#)

При просмотре выходных данных команды `debug ppp negotiation` в целях устранения неполадок руководствуйтесь следующими инструкциями:

1. **Определите переходы на следующие этапы в выходных данных команды debug.** Определите этап, на котором было выполнено подключение, то есть UP или AUTHENTICATING. Это поможет определить, на каком этапе произошел сбой подключения. Для получения дополнительной информации о фазах посмотрите раздел [Этапов согласования PPP](#).
2. **Определив этап, на которой произошел сбой, найдите сообщения, которые указывают на успешное выполнение LCP, аутентификации или NCP:** Состояние LCP должно быть открытым. Можно также просмотреть последние входящие и исходящие сообщения CONFACK, чтобы проверить, согласованы ли требуемые параметры. Аутентификация должна быть успешной. Если использовать двухстороннюю аутентификацию, то каждая транзакция должна завершиться успешно. Для получения дополнительной информации об устранении проблем сбоев проверки подлинности PPP обратитесь к [Устранению проблем PPP \(CHAP или PAP\) Аутентификацию](#). Состояние IPCP должно быть открытым. Убедитесь, что адресация верна и маршрут к одноранговому участнику установлен.

## [Считайте Выходные данные debug ppp negotiation](#)

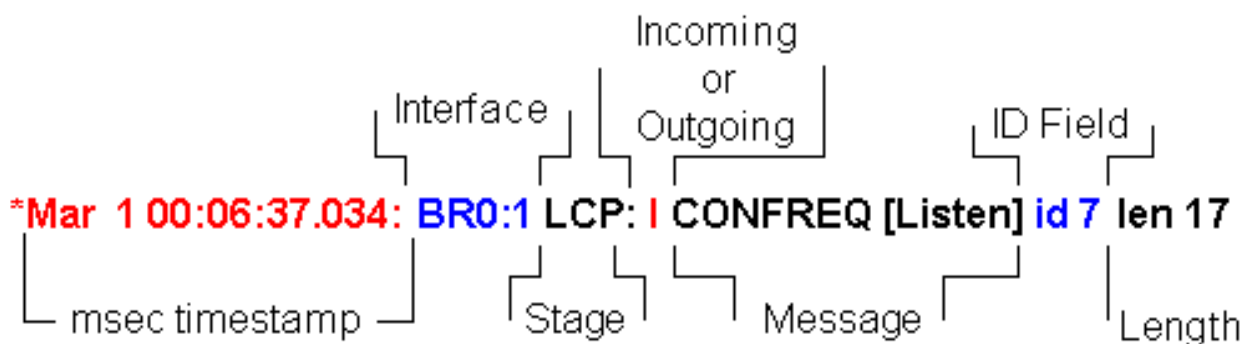
Большинство строк в выходных данных команды `debug ppp negotiation` характеризуются следующими факторами:

1. **Штамп времени в Ъ”** Шапмы времени в миллисекундах полезны. Посмотрите раздел [Предварительных условий](#) этого документа для получения дополнительной информации.
2. **Когда соединения отладки используют множественные соединения, или когда переходы подключения через несколько интерфейсов, интерфейс и Номер интерфейса** — Это поле полезно. Например, определенные подключения (такие как многоканальные вызовы) управляются сначала физическим интерфейсом, однако затем управление берет на себя интерфейс номеронабирателя или интерфейс виртуального доступа.
3. **Тип сообщения PPP** — Это поле указывает, является ли линия общим PPP, LCP, CHAP, PAP или сообщением IPCP.

4. **Направление сообщения** — **я** указывает на входящий пакет, и **О** указывает на исходящий пакет. Это поле может использоваться для определения, было ли сообщение создано или получено маршрутизатором.
5. **Сообщение** — Это поле включает конкретную транзакцию под согласованием.
6. **ID** — Это поле используется, чтобы совпасть и координировать сообщения запроса к соответствующим ответным сообщениям. Можно использовать это поле для сопоставления ответа со входящим сообщением. Этот параметр особенно полезен, если входящее сообщение и ответ на него находятся слишком далеко друг от друга в выходных данных отладки.
7. **Длина** Длина поля определяет длину информационного поля. Это поле не имеет значения при общем устранении неполадок.

**Примечание:** Поля 4 - 7 могут не появиться во всех сообщениях PPP, в зависимости от цели сообщения.

**Примечание:** Данный пример иллюстрирует поля:



## Пример выходных данных команды debug ppp negotiation

Ниже приведено выходные данные команды debug ppp negotiation с примечаниями:

```
maui-soho-01#debug ppp negotiation PPP protocol negotiation debugging is on maui-soho-01# *Mar 1
00:06:36.645: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up !--- The Physical Layer (BRI
Interface) is up. Only now can PPP !--- negotiation begin. *Mar 1 00:06:36.661: BR0:1 PPP:
Treating connection as a callin *Mar 1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive
Open [0 sess, 0 load] !--- The PPP Phase is ESTABLISHING. LCP negotiation now occurs. *Mar 1
00:06:36.669: BR0:1 LCP: State is Listen *Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7
len 17 !--- This is the incoming CONFREQ. The ID field is 7. *Mar 1 00:06:37.038: BR0:1 LCP:
AuthProto PAP (0x0304C023) *Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D
(0x0506507A214D) *Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300) !--- The peer has
requested: !--- Option: Authentication Protocol, Value: PAP !--- Option: MagicNumber (This is
used to detect loopbacks and is always sent.) !--- Option: Callback, Value: 0 (This is for PPP
Callback; MS Callback uses 6.) *Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15 !-
-- This is an outgoing CONFREQ, with parameters for the peer to implement. !--- Note that the ID
Field is 4, so this is not related to the previous !--- CONFREQ message. *Mar 1 00:06:37.058:
BR0:1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1
(0x05061081E7E1) !--- This router requests: !--- Option: Authentication Protocol, Value: CHAP !-
-- Option: MagicNumber (This is used to detect loopbacks and is always sent.) *Mar 1
00:06:37.066: BR0:1 LCP: O CONFREQ [Listen] id 7 len 7 !--- This is an outgoing CONFREQ for
message with Field ID 7. !--- This is the response to the CONFREQ received first. *Mar 1
00:06:37.070: BR0:1 LCP: Callback 0 (0x0D0300) !--- The option that this router rejects is
Callback. !--- If the router wanted to do MS Callback rather than PPP Callback, it !--- would
have sent a CONFNAK message instead. *Mar 1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4
len 15 !--- This is an incoming CONFACK for a message with Field ID 4. *Mar 1 00:06:37.102:
BR0:1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 00:06:37.106: BR0:1 LCP: MagicNumber 0x1081E7E1
```



(0x05061081E7E1) !--- The peer can support all requested parameters. \*Mar 1 00:06:37.114: BR0:1 LCP: I CONFREQ [ACKrcvd] id 8 len 14 !--- This is an incoming CONFREQ message; the ID field is 8. !--- This is a new CONFREQ message from the peer in response to the CONFREQ id:7. \*Mar 1 00:06:37.117: BR0:1 LCP: AuthProto PAP (0x0304C023) \*Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D) !--- The peer has requested: !--- Option: Authentication Protocol, Value: PAP !--- Option: MagicNumber (This is used to detect loopbacks and is always sent.) \*Mar 1 00:06:37.125: BR0:1 LCP: O CONFNAK [ACKrcvd] id 8 len 9 !--- This is an outgoing CONFNAK for a message with Field ID 8. \*Mar 1 00:06:37.129: BR0:1 LCP: AuthProto CHAP (0x0305C22305) !--- This router recognizes the option Authentication Protocol, !--- but does not accept the value PAP. In the CONFNAK message, !--- it suggests CHAP instead. \*Mar 1 00:06:37.165: BR0:1 LCP: I CONFREQ [ACKrcvd] id 9 len 15 !--- This is an incoming CONFREQ message with Field ID 9. \*Mar 1 00:06:37.169: BR0:1 LCP: AuthProto CHAP (0x0305C22305) \*Mar 1 00:06:37.173: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D) !--- CHAP authentication is requested. \*Mar 1 00:06:37.177: BR0:1 LCP: O CONFACK [ACKrcvd] id 9 len 15 !--- This is an outgoing CONFACK for a message with Field ID 9. \*Mar 1 00:06:37.181: BR0:1 LCP: AuthProto CHAP (0x0305C22305) \*Mar 1 00:06:37.185: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D) \*Mar 1 00:06:37.189: BR0:1 LCP: State is Open !--- This indicates that the LCP state is Open. \*Mar 1 00:06:37.193: BR0:1 PPP: Phase is AUTHENTICATING, by both [0 sess, 0 load] !--- The PPP Phase is AUTHENTICATING. PPP Authentication occurs now. !--- Two-way authentication is now performed (indicated by the both keyword). \*Mar 1 00:06:37.201: BR0:1 CHAP: O CHALLENGE id 4 len 33 from "maui-soho-01" !--- This is the outgoing CHAP Challenge. !--- In LCP the routers had agreed upon CHAP as the authentication protocol. \*Mar 1 00:06:37.225: BR0:1 CHAP: I CHALLENGE id 3 len 33 from "maui-soho-03" !--- This is an incoming Challenge message from the peer. \*Mar 1 00:06:37.229: BR0:1 CHAP: Waiting for peer to authenticate first \*Mar 1 00:06:37.237: BR0:1 CHAP: I RESPONSE id 4 len 33 from "maui-soho-03" !--- This is an incoming response from the peer. \*Mar 1 00:06:37.244: BR0:1 CHAP: O SUCCESS id 4 len 4 !--- This router has successfully authenticated the peer. \*Mar 1 00:06:37.248: BR0:1 CHAP: Processing saved Challenge, id 3 \*Mar 1 00:06:37.260: BR0:1 CHAP: O RESPONSE id 3 len 33 from "maui-soho-01" \*Mar 1 00:06:37.292: BR0:1 CHAP: I SUCCESS id 3 len 4 !--- This is an incoming Success message. Each side has !--- successfully authenticated the other. \*Mar 1 00:06:37.296: BR0:1 PPP: Phase is UP [0 sess, 0 load] !--- The PPP status is now UP. NCP (IPCP) negotiation begins. \*Mar 1 00:06:37.304: BR0:1 IPCP: O CONFREQ [Closed] id 4 len 10 \*Mar 1 00:06:37.308: BR0:1 IPCP: Address 172.22.1.1 (0x0306AC160101) !--- This is an outgoing CONFREQ message. It indicates that !--- the local machine address is 172.22.1.1. \*Mar 1 00:06:37.312: BR0:1 CDPCP: O CONFREQ [Closed] id 4 len 4 \*Mar 1 00:06:37.320: BR0:1 CDPCP: I CONFREQ [REQsent] id 4 len 4 \*Mar 1 00:06:37.324: BR0:1 CDPCP: O CONFACK [REQsent] id 4 len 4 !--- These messages are for CDP Control Protocol (CDPCP). \*Mar 1 00:06:37.332: BR0:1 IPCP: I CONFREQ [REQsent] id 4 len 10 \*Mar 1 00:06:37.336: BR0:1 IPCP: Address 172.22.1.2 (0x0306AC160102) !--- This is an incoming CONFREQ message that indicates that the peer !--- address is 172.22.1.2. An address of 0.0.0.0 indicates that the peer !--- does not have an address and requests the local router to provide it !--- with an address in IPCP negotiation. \*Mar 1 00:06:37.344: BR0:1 IPCP: O CONFACK [REQsent] id 4 len 10 \*Mar 1 00:06:37.348: BR0:1 IPCP: Address 172.22.1.2 (0x0306AC160102) \*Mar 1 00:06:37.356: BR0:1 IPCP: I CONFACK [ACKsent] id 4 len 10 \*Mar 1 00:06:37.360: BR0:1 IPCP: Address 172.22.1.1 (0x0306AC160101) \*Mar 1 00:06:37.363: BR0:1 IPCP: State is Open !--- The IPCP state is Open. Note that in the IPCP negotiation, each side !--- accepted the IP address of the peer, and one was assigned to the peer. \*Mar 1 00:06:37.371: BR0:1 CDPCP: I CONFACK [ACKsent] id 4 len 4 \*Mar 1 00:06:37.375: BR0:1 CDPCP: State is Open !--- This indicates that the CDPCP state is Open. \*Mar 1 00:06:37.387: BR0 IPCP: Install route to 172.22.1.2 !--- A route to the peer is installed. \*Mar 1 00:06:38.288: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up \*Mar 1 00:06:42.609: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to maui-soho-03

## Глоссарий и распространенные сообщения

### Общие сведения

#### CONFREQ (Configure-Request):

Когда более низкий уровень становится доступным (Up), отправляется сообщение CONFREQ для запуска этапа PPP (этап LCP). Оно используется на этапах LCP и NCP как попытка настройки подключения. Чтобы открыть подключение к одноранговому участнику,



устройство передает это сообщение вместе с параметрами и значениями конфигурации, поддержку которых отправитель требует от однорангового участника. Все параметры и значения согласовываются одновременно. Если одноранговый участник отвечает сообщением CONFREJ или CONFNAK, маршрутизатор отправляет еще одно сообщение CONFREQ с другим набором параметров или значений.

### CONFACK (Настраивают - Подтверждает):

Если все параметры в сообщении CONFREQ распознаны и все значения являются допустимыми, маршрутизатор передает сообщение CONFACK.

### CONFREJ (настраивают отклонение):

Если какой-либо параметр конфигурации, полученный в сообщении CONFREQ, является недопустимым или не распознается, маршрутизатор отвечает сообщением CONFREJ. Недопустимый параметр (из сообщения CONFREQ) включается в сообщение CONFREJ.

### CONFNAK (настраивают отрицательное квитирование):

Если полученный параметр конфигурации определяется и считается допустимым, однако полученное значение не является допустимым, маршрутизатор передает сообщение CONFNAK. Маршрутизатор присоединяет этот параметр и значение, которое он может принять, к сообщению CONFNAK, так что одноранговый участник может включить этот параметр в следующее сообщение CONFREQ.

### ECHOREQ (запрос эха) и ECHOREP (эхо - ответ):

PPP использует сообщения keeralive, чтобы поддерживать целостность подключения. Эти сообщения являются фреймом ECHOREQ, который отправляется удаленному одноранговому участнику PPP, а этот участник должен ответить фреймом ECHOREP при получении фрейма ECHOREQ. Если маршрутизатор пропускает пять фреймов ECHOREP (значение по умолчанию), то канал считается отключенным, и протокол PPP отключается.

### TERMREQ (Запрос на прерывание):

Этот фрейм указывает на то, что одноранговый участник PPP, отправивший этот фрейм, прерывает PPP-подключение.

### TERMAK (Оповещение о завершении):

Это сообщение передается в ответ на сообщение TERMREQ. Это приводит к отключению PPP-подключения.

## ЗАВЕРШЕНИЕ

Это сообщение указывает на отключение PPP-подключения. Подключение LCP или NCP может отключиться по следующим причинам:

- административное закрытие (только LCP).

- когда нижний уровень прекращает обслуживание (канал модемного подключения, ISDN и так далее).
- при неудаче согласования.
- при обнаружении возвратной петли.

## LCP

### ACCM (таблица символов асинхронного управления):

Это один из параметров, согласованных на этапе LCP, в фрейме CONFREQ. ACCM задает последовательность символов выхода. ACCM заставляет порт игнорировать указанные символы управления в потоке данных. Если маршрутизатор на другом конце подключения не поддерживает согласование ACCM, порт принудительно использует FFFFFFFF. В этом случае выполните команду:

```
ppp accm match 000a000
```

### ACFC (Адрес и сжатие контрольного поля):

ACFC — это параметр LCP, которые позволяет конечным точкам эффективно обмениваться сообщениями.

### AuthProto (протокол аутентификации):

AuthProto — это тип протокола аутентификации, согласованный в фрейме CONFREQ между одноранговыми участниками PPP-подключения для использования на этапе аутентификации. Если аутентификация PPP не настроена, выходные данные не отображаются в согласованных параметрах фрейма CONFREQ. Возможные значения — CHAP или PAP.

### Обратный вызов "#":

Это сообщение указывает, что согласуется параметр обратного вызова. Номер после синтаксиса обратного вызова указывает, согласование какого параметра обратного вызова выполняется. Номер 0 — это обычный обратный вызов PPP, а номер 6 указывает на использование параметра обратного вызова Microsoft (который автоматически доступен в ПО Cisco IOS® версии 11.3(2)T и выше).

### CHAP (протокол аутентификации по квитированию вызова):

Это сообщение указывает, что согласованным протоколом аутентификации является CHAP.

### EndpointDisc (различитель оконечная точки):

Это параметр LCP, используемый для идентификации узла PPP на многоканальном соединении PPP. Для получения дополнительной информации обратитесь к [Критериям для Именования Пакетов протокола PPP](#).

## LCP: Состояние Открыто

Это сообщение указывает на то, что согласование LCP было успешно завершено.

### [LQM \(мониторинг качества канала\)](#)

Мониторинг качества канала LQM доступен на всех последовательных интерфейсах, на которых работает PPP. LQM отслеживает качества канала и отключает канал, если качество снижается ниже указанного процентного соотношения. Процентное соотношение вычисляется для входящего и исходящего направлений. Качество на исходящем направлении вычисляется путем сравнения общего количества отправленных пакетов и байтов с общим количеством пакетов и байтов, полученных одноранговым участником. Качество на входящем направлении вычисляется путем сравнения общего количества полученных пакетов и байтов с общим количеством пакетов и байтов, отправленных одноранговым участником.

При работе LQM отчеты LQR отправляются через интервал keepalive. Отчеты LQR отправляются вместо пакетов keepalive. Все входящие пакеты keepalive получают допустимый ответ. Если функция LQM не настроена, сообщения keepalive отправляются через интервал keepalive, а все входящие отчеты LQR получают ответ в виде LQR.

### [MagicNumber](#)

Поддержка Magic Number доступна на всех последовательных интерфейсах. При использовании PPP всегда производится попытка согласовать параметр Magic Numbers, который используется для определения сетей с возвратной петлей. Случайная строка отправляется по каналу, и если возвращается то же значение, то маршрутизатор определяет, что канал является возвратной петлей.

Ссылка могла бы или не могла бы быть приведена в нерабочее состояние после с закольцовыванием обнаружения; это зависит от использования [команды down-when-looped](#).

### [PAP \(протокол аутентификации пароля\)](#)

Это сообщение указывает, что согласуемым протоколом аутентификации, который будет использоваться одноранговыми участниками PPP, является PAP. Для получения дополнительной информации о PAP обратитесь к [Настройке и Протоколу аутентификации Пароля PPP Устранения проблем \(PAP\)](#).

### [PFC \(сжатие поля протокола\)](#)

Этот параметр включает сжатие для полей протокола (on или off).

### [MRRU \(Max получают восстановленный модуль\)](#)

Это параметр LCP, согласованный при настройке LCP для PPP Multilink. Он определяет максимальное количество байтов, из которого может состоять фрейм. Если MRRU не согласовывается на этапе LCP, протокол Multilink PPP (MPPP) может не работать на канале.

### [MRU \(максимальный размер принимаемого блока данных\)](#)

MRU — это параметр LCP, который согласовывается в фрейме CONFREQ для

согласования размера обмениваемых пакетов.

## Authentication

### AUTH-REQ (запрос аутентификации)

Этот фрейм передается с локального однорангового участника PPP (на котором включена аутентификация) на удаленного однорангового участника. В нем запрашивается отправка удаленным участником допустимого имени пользователя и пароля для аутентификации PPP-подключения. Этот фрейм используется только для PAP.

### AUTH-ACK (аутентификация подтверждают).

Данный фрейм отправляется с аутентифицированного однорангового участника PPP на аутентифицируемого однорангового участника PPP. Этот фрейм содержит корректное имя пользователя и пароль. Фрейм используется только при использовании PAP для аутентификации PPP-подключения.

### AUTH-NAK или СБОЙ

Этот фрейм отправляется с аутентифицируемого однорангового участника PPP при сбое аутентификации на аутентифицируемом участнике PPP.

## ПРОБЛЕМА

Это фрейм CHAP-вызова, который отправляется с аутентифицируемого однорангового участника PPP на аутентифицированного участника PPP. Фрейм CHAP-вызова состоит из идентификатора, случайного числа и имени хоста локального сервера связи или имени пользователя на удаленном устройстве. Фрейм используется только при использовании CHAP для аутентификации PPP-подключения.

## Ответ

Данный фрейм является CHAP-ответом, который отправляется с аутентифицированного однорангового участника PPP на аутентифицируемого однорангового участника PPP.

Обязательный ответ состоит из двух частей:

- Выходные данные хэша MD5 общего секретного ключа.
- Имя хоста удаленного устройства или имя пользователя на удаленном устройстве.

Фрейм используется только при использовании CHAP для аутентификации PPP-подключения.

## NCP

### Адрес a.b. cD

- Данное значение в исходящем сообщении CONFREQ означает IP-адрес, выбранный

для использования локальным маршрутизатором. Если этот адрес равен 0.0.0.0, локальный компьютер запрашивает участника о предоставлении IP-адреса, который можно использовать.

- Данное значение во входящем сообщении CONFREQ означает IP-адрес, выбранный для использования одноранговым участником. Если этот адрес равен 0.0.0.0, одноранговый участник запрашивает локальный компьютер о предоставлении IP-адреса, который можно использовать.
- В исходящем сообщении CONFNAK это значение указывает IP-адрес, который одноранговый узел должен использовать вместо адреса, предложенного этому узлу в сообщении CONFREQ.
- Данное значение во входящем сообщении CONFNAK означает IP-адрес, который должен использовать локальный компьютер вместо предложенного в предыдущем сообщении CONFNAK.
- В исходящем сообщении CONFACK это значение указывает, что IP-адрес, запрашиваемый одноранговым участником, разрешен локальным компьютером.
- Во входящем сообщении CONFACK это значение указывает, что IP-адрес, запрашиваемый локальным компьютером, разрешен локальным компьютером.

### [CCP \(протокол управления сжатием\)](#)

Это сообщение указывает, что протокол сжатия согласовывается обоими одноранговыми участниками PPP. В ПО Cisco IOS поддерживаются следующие протоколы сжатия для PPP-подключения:

- MS-Point-to-Point Compression (MS-PPC)
- накопитель
- средство прогнозирования

### [CDPCP \(протокол обнаружения Cisco протокол управления\)](#)

Это сообщение указывает, что согласование CDP происходит на этапе NCP. **Чтобы отключить CDP на маршрутизаторе, выполните команду по `cdp run`.**

### [CODEREJ \(отклонение кода\)](#)

Пакет CODEREJ отправляется при получении неопознанного пакета от удаленного однорангового участника PPP.

### [Установите маршрут к a.b. cD](#)

После завершения маршрутизатором согласования IPCP (этап NCP для протокола IP L3) данный IP-адрес удаленного участника PPP должен быть прописан в таблице маршрутизации вместе с допустимым маршрутом. **Если это сообщение не отображается, убедитесь, что не выполнялась команда по `peer neighbor-route`.**

### [IPCP \(IP Control Protocol\)](#)

Это значение указывает, что IP — это согласуемый сетевой уровень на этапе NCP.

## Состояние IPCP Открыто

Это сообщение указывает, что согласование IPCP (этап NCP для протокола IP L3) завершено успешно.

## PROTREJ (отклонение протокола)

Одноранговый участник PPP при получении пакета PPP с неизвестным протоколом в соответствующем поле использует сообщение PROTREJ для указания того, что другой участник попытался использовать неподдерживаемый протокол. Если устройство PPP получает сообщение PROTREJ, оно должно как можно быстрее приостановить отправку пакетов, относящихся к указанному протоколу.

## Дополнительные сведения

- [Настройка и устранение неисправностей протокола аутентификации пароля PPP \(PAP\)](#)
- [Проверка подлинности PPP с использованием команд `ppp chap hostname` и `ppp authentication chap callin`](#)
- [Общие сведения и настройка аутентификации PPP CHAP](#)
- [Устранение неисправностей аутентификации PPP \(CHAP или PAP\)](#)
- [Страницы поддержки технологии коммутации](#)
- [Техническая поддержка - Cisco Systems](#)