Содержание

Введение

Протокол соединения Point-to-Point Protocol (PPP) поддерживает два протокола проверки подлинности: Протоколы проверки пароля PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol). Оба указаны в RFC 1334 и поддерживаются на синхронных и асинхронных интерфейсах.

- Протокол аутентификации по паролю предоставляет простой способ установления идентификации на удаленном сайте при помощи двухэтапного установления связи. По окончании этапа установления связи PPP удаленный сайт несколько раз отправляет по каналу имя пользователя и пароль (в виде простого текста), пока не будет выполнена проверка подлинности либо прервано подключение.
- PAP – это не протокол безопасной проверки подлинности. Пароли передаются через ссылку в открытом тексте и нет никакой защиты от атак метода проб и ошибок или воспроизведения. Удаленный узел управляет частотой и распределением во времени попыток регистрации.

Для получения дополнительной информации об устранении проблем проверки подлинности PPP (использующий или PAP или CHAP), обратитесь к Устранению проблем PPP (CHAP или

PAP) Аутентификацию для завершенной, пошаговой блок-схемы для устранения проблем фазы аутентификации PPP. Для получения дополнительной информации об устранении проблем всех фаз PPP (LCP, Аутентификация, NCP), ссылаются на Блок-схему Устранения проблем PPP документа для завершенной блок-схемы для пошагового устранения проблем всех связанных фаз PPP и договорных параметров.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

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.

Общие сведения

CHAP, как полагают, более безопасен, потому что пароль пользователя никогда не передается через соединение. Для получения дополнительной информации о CHAP обратитесь к Проверке подлинности CHAP PPP Настройки и Пониманию.

Несмотря на некоторые недостатки, PAP можно использовать в следующих средах:

- Большая установленная база клиентских приложений, не поддерживающих протокол аутентификации CHAP
- Несовместимость между различными реализациями изготовителя CHAP
- Ситуации, когда для моделирования входа на удаленный хост должен быть доступен нешифрованный пароль

Сравнение односторонней и двусторонней аутентификации

Как и большинство типов аутентификации PAP поддерживает двунаправленную (двустороннюю) и однонаправленную (одностороннюю) аутентификацию. Однонаправленная проверка подлинности подразумевает, что только принимающая вызов сторона (NAS) проверяет подлинность удаленной стороны (клиента). Удаленный клиент не аутентифицирует сервер.

С двунаправленной аутентификацией, каждая сторона независимо отправляет запрос на аутентификацию (AUTH-REQ) и получает либо сообщение о подтверждении аутентификации (AUTH-ACK), либо сообщение о не подтверждении аутентификации (AUTH-NAK). Они могут быть замечены с командой debug ppp authenticaion. Пример этой команды

отладки на клиенте приведен ниже:

```
*Mar  6 19:18:53.322: BR0:1 PAP: O AUTH-REQ id 7 len 18 from "PAPUSER"! --- Outgoing PAP AUTH-REQ. We are sending out our username (PAPUSER)and password ! --- to the NAS. The NAS will verify that the username/password is correct. *Mar 6 19:18:53.441: BR0:1 PAP: I AUTH-ACK id 7 Len 5! --- Incoming AUTH-ACK. ! --- The NAS verified the username and password and responded with an AUTH-ACK. ! --- One-way authentication is complete at this point. *Mar 6 19:18:53.445: BR0:1 PAP: I AUTH-REQ id 1 Len 14 from "NAS"! --- Incoming AUTH-REQ from the NAS. This means we now verify the identity of the NAS.*Mar 6 19:18:53.453: BR0:1 PAP: Authenticating peer NAS! --- Performing a lookup for the username (NAS) and password.*Mar 6 19:18:53.457: BR0:1 PAP: O AUTH-ACK id 1 Len 5! --- Outgoing AUTH-ACK. ! --- We have verified the username/password of the NAS and responded with an AUTH-ACK. ! --- Two-way authentication is complete.
```

Аутентификация в вышеприведенном результате отладки была двусторонней. Однако, если ранее была настроена однонаправленная аутентификация, мы сможем увидеть лишь первые две отладочные строки.

Команды для настройки

Обычная проверка подлинности PAP, описанная ниже, требует трех команд:

ppp authentication pap callin

Маршрутизатор, на котором будет настроена команда ppp authentication pap, будет использовать PAP для проверки подлинности другой стороны (одноранговового узла). Это означает, что другая сторона (равноправный узел) должна сообщить локальному устройству имя пользователя и пароль для проверки.

Параметр вызова говорит маршрутизатор, что команда ppp authentication pap callin настроена на, будет только аутентифицировать другую сторону во время входящего вызова. Для исходящего вызова это не будет аутентифицировать другую сторону. Это означает, что маршрутизатору, инициирующему вызов, не требуется запрос на аутентификацию (AUTH-REQ) с противоположной стороны

В следующей таблице показано, когда настраивать параметр callin:

Тип проверки подлинности	Клиент (вызывающая сторона)	NAS (вызываемая сторона)
Unidirectional	ppp authentication pap callin	ppp authentication pap
Bi-directional	ppp authentication pap	ppp authentication pap

username <имя пользователя> password <пароль>

Это имя пользователя и пароль, которые используются локальным маршрутизатором для аутентификации равноправного узла PPP. Когда одноранговый узел отправляет свое имя пользователя и пароль PAP, локальный маршрутизатор проверяет, настроены ли эти имя пользователя и пароль локально. Если существует полное совпадение, узел

аутентифицируется.

Примечание: Функция команды имени пользователя для PAP является другой, чем ее функция для CHAP. С CHAP эти имя пользователя и пароль используются для генерации ответа на запрос, но PAP использует их только для проверки верности входящих имени пользователя и пароля.

Для односторонней аутентификации достаточно применить эту команду на вызванном маршрутизаторе. Для двусторонней аутентификации эту команду нужно выполнить на обеих сторонах.

PPP pap sent-username <username> password <password>

Включает внешнюю аутентификацию PAP. Локальный маршрутизатор использует имя пользователя и пароль, заданное командой ppp pap sent-username для аутентификации себя на удаленном устройстве. **Другой маршрутизатор должен иметь тождественное имя пользователя/пароль, конфигурированный при помощи команды username, как описано выше.**

Если используется односторонняя проверка подлинности, эта команда будет необходима только на маршрутизаторе, инициирующим вызов. Для двусторонней аутентификации эта команда должна быть настроена на обоих сторонах.

Пример конфигурации

Следующие разделы конфигурации содержат необходимые команды PAP для сценария односторонней аутентификации.

Примечание: Показаны только соответствующие разделы конфигурации.

Настройка вызывающей стороны (клиента)

```
interface BRI0! --- BRI interface for the dialout. ip address negotiated encapsulation ppp! --- Use PPP encapsulation. This command is a required for PAP. dialer string 3785555 class 56k! --- Number to dial for the outgoing connection. dialer-group 1 isdn switch-type basic-ni isdn spid1 51299611110101 9961111 isdn spid2 51299622220101 9962222 ppp authentication pap callin! --- Use PAP authentication for incoming calls. ! --- The callin keyword has made this a one-way authentication scenario. ! --- This router (client) will not request that the peer (server) authenticate ! --- itself back to the client. ppp pap sent-username PAPUSER password 7 <deleted>! --- Permit outbound authentication of this router (client) to the peer. ! --- Send a PAP AUTH-REQ packet to the peer with the username PAPUSER and password. ! --- The peer must have the username PAPUSER and password configured on it.
```

Конфигурация приемной стороны (сервера)

```
username PAPUSER password 0 cisco! --- Username PAPUSER is the same as the one sent by the client. ! --- Upon receiving the AUTH-REQ packet from the client, we will verify that the ! --- username and password match the one configured here.interface Serial0:23! --- This is the D-channel for the PRI on the access server receiving the call. ip unnumbered Ethernet0 no ip directed-broadcast encapsulation ppp! --- Use PPP encapsulation. This command is a required for PAP. dialer-group 1 isdn switch-type primary-ni isdn incoming-voice modem peer default ip address pool default fair-queue 64 256 0 ppp authentication pap! --- Use PAP authentication for incoming calls. ! --- This router (server) will request that the peer authenticate itself to us. ! --- Note: the callin option is not used as this router is not initiating the call.
```

Отладка результатов

Для устранения неполадки PPP PAP используются команды debug ppp negotiation и debug ppp authentication. Существует две главных проблемы, которых необходимо остерегаться:

1. Согласовали ли обе стороны, что способом аутентификации является PAP?
2. Если так, проходит ли успешно аутентификация PAP?

См. отладки ниже для получения информации о том, как должным образом ответить на эти вопросы. Кроме того, см. Понимание Выходных данных debug ppp negotiation для пояснения всех других линий отладки с их относительным значением во время других фаз PPP, включая проверку подлинности PPP. Этот документ полезен в быстром определении причины сбоев согласования PPP. Для получения дополнительной информации об устранении проблем проверки подлинности PPP (использующий или PAP или CHAP), обратитесь к Устранению проблем PPP (CHAP или PAP) Аутентификацию для завершенной, пошаговой блок-схемы для устранения проблем фазы аутентификации PPP.

Отладка вызывающей стороны (клиента) для успешной односторонней проверки подлинности PAP

```
maui-soho-01#show debugPPP:  PPP authentication debugging is on  PPP protocol negotiation
debugging is onmaui-soho-01#ping 172.22.53.144Type escape sequence to abort.Sending 5, 100-byte
ICMP Echos to 172.22.53.144, timeout is 2 seconds:*Mar  6 21:33:26.412: %LINK-3-UPDOWN:
Interface BRI0:1, changed state to up*Mar  6 21:33:26.432: BR0:1 PPP: Treating connection as a
callout*Mar  6 21:33:26.436: BR0:1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load]*Mar
6 21:33:26.440: BR0:1 PPP: No remote authentication for call-out! --- The client will not
authenticate the server for an outgoing call. ! --- Remember this is a one-way authentication
example. *Mar 6 21:33:26.444: BR0:1 LCP: O CONFREQ [Closed] id 82 Len 10*Mar  6 21:33:26.448:
BR0:1 LCP:    MagicNumber 0x2F1A7C63 (0x05062F1A7C63)! --- Outgoing CONFREQ (CONFigure-REQuest).
! --- Notice that we do not specify an authentication method, ! --- since only the peer will
authenticate us. *Mar 6 21:33:26.475: BR0:1 LCP: I CONFREQ [REQsent] id 13 Len 14*Mar  6
21:33:26.479: BR0:1 LCP:    AuthProto PAP (0x0304C023)! --- Incoming LCP CONFREQ (Configure-
Request) indicating that ! --- the peer(server) wishes to use PAP. *Mar 6 21:33:26.483: BR0:1
LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B)*Mar 6 21:33:26.491: BR0:1 LCP: O CONFACK [REQsent]
id 13 Len 14*Mar  6 21:33:26.495: BR0:1 LCP:    AuthProto PAP (0x0304C023)! --- This shows the
outgoing LCP CONFACK (CONFigure-ACKnowledge) indicating that ! --- the client can do PAP.*Mar 6
21:33:26.499: BR0:1 LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B)*Mar 6 21:33:26.511: BR0:1 LCP:
I CONFACK [ACKsent] id 82 Len 10*Mar 6 21:33:26.515: BR0:1 LCP: MagicNumber 0x2F1A7C63
(0x05062F1.A7C63)*Mar 6 21:33:26.519: BR0:1 LCP: State is Open! --- This shows LCP negotiation
is complete.*Mar 6 21:33:26.523: BR0:1 PPP: Phase is AUTHENTICATING, by the peer [0 sess, 0
load]! --- The PAP authentication (by the peer) begins.*Mar 6 21:33:26.531: BR0:1 PAP: O AUTH-
REQ id 20 Len 18 from "PAPUSER"! --- The client sends out a PAP AUTH-REQ with username PAPUSER.
! --- This username is configured with the ppp pap sent-username command. *Mar 6 21:33:26.555:
BR0:1 PAP: I AUTH-ACK id 20 Len 5! --- The Peer responds with a PPP AUTH-ACK, indicating that !
--- it has successfully authenticated the client.
```

Отладка вызываемой стороны (сервера) для успешной односторонней проверки подлинности PAP

```
maui-nas-06#show debugPPP:  PPP authentication debugging is on  PPP protocol negotiation
debugging is onmaui-nas-06#*Jan  3 14:07:57.872: %LINK-3-UPDOWN: Interface Serial0:4, changed
state to up*Jan  3 14:07:57.876: Se0:4 PPP: Treating connection as a callin! --- Since the
connection is incoming, we will authenticate the client.*Jan 3 14:07:57.876: Se0:4 PPP: Phase is
ESTABLISHING, Passive Open*Jan 3 14:07:57.876: Se0:4 LCP: State is Listen*Jan 3 14:07:58.120:
Se0:4 LCP: I CONFREQ [Listen] id 83 Len 10*Jan 3 14:07:58.120: Se0:4 LCP: MagicNumber 0x2F319828
(0x05062F319828)*Jan 3 14:07:58.124: Se0:4 LCP: O CONFREQ [Listen] id 13 Len 14*Jan  3
14:07:58.124: Se0:4 LCP:    AuthProto PAP (0x0304C023)! --- Outgoing CONFREQ (Configure-Request)
! --- use PAP for the peer authentication.*Jan 3 14:07:58.124: Se0:4 LCP: MagicNumber 0x3DD5D5B9
```

```
(0x05063DD5D5B9)*Jan 3 14:07:58.124: Se0:4 LCP: O CONFACK [Listen] id 83 Len 10*Jan 3
14:07:58.124: Se0:4 LCP: MagicNumber 0x2F319828 (0x05062F319828)*Jan 3 14:07:58.172: Se0:4 LCP:
I CONFACK [ACKsent] id 13 Len 14*Jan  3 14:07:58.172: Se0:4 LCP:    AuthProto PAP (0x0304C023)! --- This shows the incoming LCP CONFACK (Configure-Acknowledge) indicating that ! --- the client can do PAP.*Jan 3 14:07:58.172: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9)*Jan 3
14:07:58.172: Se0:4 LCP: State is Open*Jan 3 14:07:58.172: Se0:4 PPP: Phase is AUTHENTICATING,
by this end! --- The PAP authentication (by this side) begins.*Jan 3 14:07:58.204: Se0:4 PAP: I
AUTH-REQ id 21 Len 18 from "PAPUSER"! --- Incoming AUTH-REQ from the peer. This means we must now verify ! --- the identity of the peer.*Jan 3 14:07:58.204: Se0:4 PPP: Phase is
FORWARDING*Jan 3 14:07:58.204: Se0:4 PPP: Phase is AUTHENTICATING*Jan 3 14:07:58.204: Se0:4 PAP:
Authenticating peer PAPUSER! --- Performing a lookup for the username (PAPUSER) and password.*Jan 3 14:07:58.208: Se0:4 PAP: O AUTH-ACK id 21 Len 5! --- This shows the outgoing AUTH-ACK. ! --- We have verified the username and password and responded with an AUTH-ACK. ! --- One-way authentication is complete.
```

Устранение неполадок PAP

При устранении неполадок PAP следует ответить на вопросы, приведенные в разделе выходных данных отладки:

1. Согласовали ли обе стороны, что способом аутентификации является PAP?
2. Если так, проходит ли успешно аутентификация PAP?

Для получения дополнительной информации об устранении проблем проверки подлинности PPP (использующий или PAP или CHAP), обратитесь к Устранению проблем PPP (CHAP или PAP) Аутентификацию для завершенной, пошаговой блок-схемы для устранения проблем фазы аутентификации PPP.

Две стороны не достигают согласования при использовании протокола аутентификации PAP

В определенной конфигурации можно увидеть, что две стороны не согласуются по PAP из-за протокола аутентификации или наоборот согласуются в CHAP (при PAP). Для устранения неполадок выполните следующие действия:

1. Убедитесь, что на принимающем вызов маршрутизаторе используется одна из следующих команд аутентификации`ppp authentication pap` or `ppp authentication pap chap` or `ppp authentication chap pap`
2. Убедитесь, что в настройках вызывающего маршрутизатора есть строка ppp authentication pap callin.
3. Проверьте, что вызывающая сторона имеет правильно сконфигурированный пароль для команды ppp pap sent-username username password, где имя пользователя и пароль соответствуют значениям, указанным на приемном маршрутизаторе.
4. Настройте команду ppp chap refuse в режиме конфигурации интерфейса на вызывающем маршрутизаторе.Маршрутизаторы Cisco, по умолчанию, примут CHAP как протокол аутентификации. В ситуации, где клиент хочет сделать PAP, но сервер доступа может сделать PAP или CHAP (настроенный pap аутентификации ppp chap), **команда ppp chap refuse** может использоваться, чтобы вынудить клиента принять PAP как протокол аутентификации.`maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse`

Проверка подлинности PAP не выполнена

Если эти две стороны договариваются о PAP как о протоколе аутентификации, но сбои PAP

- подключения, это наиболее вероятно проблема имени пользователя/пароля.

1. *Проверьте, что вызывающая сторона имеет правильно сконфигурированный пароль для команды ppp pap sent-username username password, где имя пользователя и пароль соответствуют значениям, указанным на приемном маршрутизаторе.*
2. *В случае двусторонней аутентификации проверьте, правильно ли настроена команда ppp pap sent-username имя_пользователя password пароль на принимающей стороне: имя пользователя и пароль должны соответствовать настройкам вызывающего маршрутизатора.Если при проведении двусторонней аутентификации на принимающем маршрутизаторе отсутствовала команда ppp pap sent-username username password password и PPP-клиент требует от сервера принудительного проведения удаленной аутентификации, то результаты выполнения команды debug ppp negotiation (или debug ppp authentication) будут указывать на следующее*`maui-soho-01(config)#`**`interface BRI 0`**`maui-soho-01(config-if)#`**`ppp chap refuse`**Это сообщение об ошибках является сигналом о проблеме с конфигурацией, а не обязательно о нарушении безопасности.
3. 3. Проверьте, что имя пользователя и пароль, совпадает с тем, настроенным в *имени и пароль пользователя для команды ppp pap sent-username password* на узле.Если они не совпадают, вы видите это сообщение:`*Jan  3 17:18:57.559: Se0:3 PAP: I AUTH-REQ id 25 Len 18 from "PAPUSER"*Jan  3 17:18:57.559: Se0:3 PPP: Phase is FORWARDING*Jan  3 17:18:57.559: Se0:3 PPP: Phase is AUTHENTICATING*Jan  3 17:18:57.559: Se0:3 PAP: Authenticating peer PAPUSER*Jan  3 17:18:57.559: Se0:3 PAP: `**`O AUTH-NAK`**` id 25 Len 32 msg is `**`"Password validation failure"`*`! --- This is an outgoing AUTH-NAK. This means that the mismatch occurred ! --- on this router. Verify that the username and password configured locally is ! --- identical to that on the peer.`*

Дополнительные сведения

- Настройка аутентификации
- Контрольная схема устранения неполадок PPP
- Устранение неисправностей аутентификации PPP (CHAP или PAP)
- Выходные данные команды "debug ppp negotiation"
- Проверка подлинности PPP с использованием команд ppp chap hostname и ppp authentication chap callin
- Технология удаленного доступа: Обзоры и объяснения
- Cisco Systems – техническая поддержка и документация