Общие сведения и настройка аутентификации PPP CHAP

Содержание

Введение

Протокол аутентификации с косвенным согласованием (CHAP) (описан в RFC 1994) выполняет аутентификацию узла посредством трехэтапной процедуры согласования. Ниже перечисляются общие действия, выполняемые в рамках протокола CHAP:

1. После завершения этапа выполнения протокола LCP (Link Control Protocol) и согласования соединения обоих устройств по протоколу CHAP средством проверки подлинности посылается на одноранговый узел сообщение CHAP-вызова.
2. Одноранговым узлом посылается ответ со значением, рассчитанным с помощью однонаправленного хэширования (MD5 (Message Digest 5)).
3. Аутентификатор проверяет ответ на основе своего расчета ожидаемого значения хеша. Если значения совпадают, проверка подлинности считается успешной. В противном случае происходит разъединение подключения.

Этот метод проверки подлинности зависит от "тайны", известной только средству проверки подлинности и одноранговому узлу. Тайна не посылается по каналу. Хотя проверка подлинности является лишь односторонней, согласование по протоколу CHAP можно выполнить в обоих направлениях с помощью одной тайны, установленной для взаимной проверки подлинности.

Дополнительные сведения о преимуществах и недостатках CHAP см. в RFC 1994.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам:

- **Включение протокола PPP в интерфейсе с помощью команды encapsulation ppp.**
- **Выходные данные команды debug ppp negotiation.** Обратитесь к документу Общие сведения о выходных данных debug ppp negotiation для получения дополнительной информации.
- Возможность устранения неполадок, когда этап протокола LCP (Link Control Protocol) не находится в открытом состоянии. Это связано с тем, что этап проверки подлинности PPP не начинается, пока этап LCP не завершен и не находится в открытом состоянии. **Если команда debug ppp negotiation не указывает, что LCP открыт, необходимо устранить эту проблему, прежде чем продолжить работу.**

Примечание: В этом документе не говорится о протоколе MS-CHAP (версии 1 или 2). Для получения дополнительной информации о MS-CHAP обратитесь к Поддержке MS-CHAP и документам Версии 2 MSCHAP.

Используемые компоненты

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

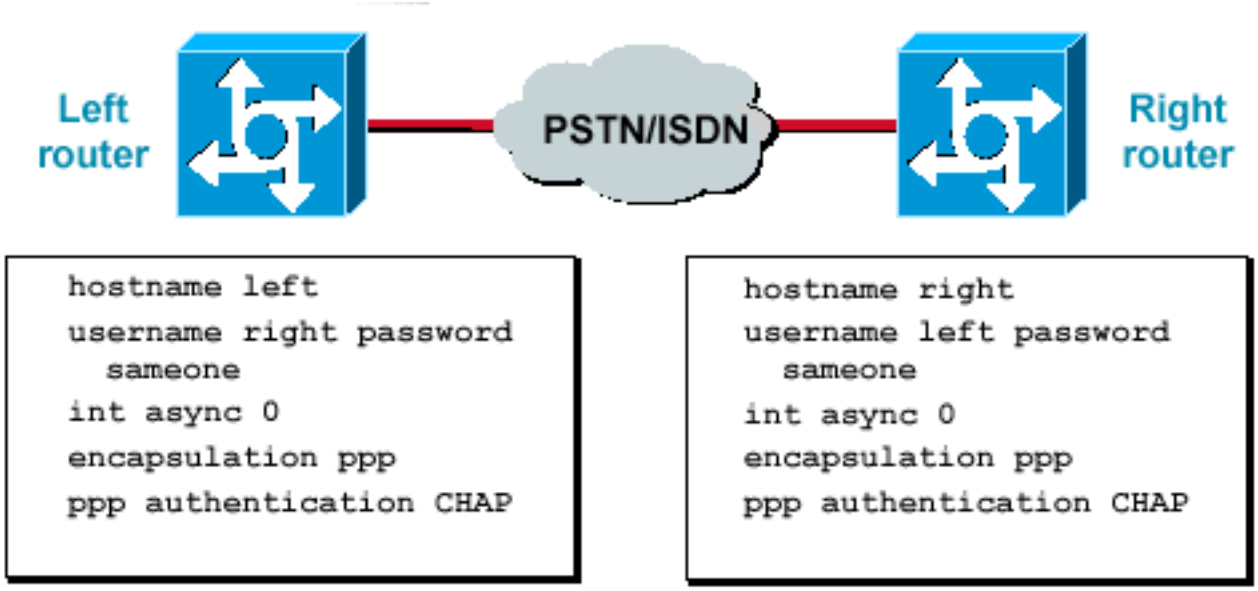
Условные обозначения

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

Настройте CHAP

Процедура настройки CHAP достаточно проста. Например, предположите, что у вас есть два маршрутизатора, левые и правые, связанные через сеть, как показано на рисунке 1.

Рисунок 1 Г Два маршрутизатора, Связанные Через Сеть



Чтобы настроить проверку подлинности по протоколу CHAP, выполните следующие действия:

1. **Выполните в интерфейсе команду encapsulation ppp.**
2. **Включите на обоих маршрутизаторах использование проверки подлинности по протоколу CHAP с помощью команды ppp authentication chap.**
3. Настройте имена пользователей и пароли. Для этого выполните команду *password password username username*, где *имя пользователя* является именем хоста узла. Убедитесь в следующем:Пароли на обоих концах одинаковы.Пароль и имя маршрутизатора полностью одинаковы, так как в них учитывается регистр знаков.**Примечание:** По умолчанию для аутентификации одноранговому узлу маршрутизатор использует собственное имя хоста. **Однако CHAP-имя пользователя можно изменить с помощью команды ppp chap hostname.** См. Проверку подлинности PPP Использование Команд ppp chap hostname и ppp authentication chap callin для получения дополнительной информации.

Односторонняя и двусторонняя проверка подлинности

CHAP определяется как метод односторонней проверки подлинности. Однако протокол CHAP используется в обоих направлениях для создания двухсторонней проверки подлинности. Следовательно, при использовании двустороннего протокола CHAP трехэтапное установление связи инициируется каждой стороной в отдельности.

В реализации компанией Cisco протокола CHAP вызываемая сторона должна по умолчанию проверить подлинность вызывающей стороны (если проверка подлинности не выключена полностью). Следовательно, односторонняя проверка подлинности, инициируемая вызываемой стороной, является минимально возможной проверкой подлинности. Однако вызывающая сторона также может проверить идентичность вызываемой стороны, и это приведет к двусторонней проверке подлинности.

Необходимость в односторонней проверке подлинности часто возникает при подключении к устройствам других компаний, отличных от Cisco.

Для односторонней проверки подлинности настройте на вызывающем маршрутизаторе

команду ppp authentication chap callin.

Таблица 1 показывает, когда настроить параметр вызова.

Таблица 1 Г , Когда Настроить Параметр вызова

Тип проверки подлинности	**Клиент (вызывающая сторона)**	**NAS (вызываемая сторона)**
Односторонняя (однонаправленная)	**ppp authentication chapcallin**	**ppp authentication chap**
Двусторонняя (двунаправленная)	**ppp authentication chap**	**ppp authentication chap**

Для получения дополнительной информации о том, как внедрить одностороннюю проверку подлинности, обратитесь к Проверке подлинности PPP Использование Команд ppp chap hostname и ppp authentication chap callin.

Команды и параметры конфигурации CHAP

Таблица 2 перечисляет команды CHAP и опции:

Таблица 2 Г Команды CHAP и Опции

Команда	**Описание**
аутентификация "PPP" {*парень	парень мс	ms-chap-v2	eap |pap*} *[вызов]*	Эта команда включает локальную проверку подлинности удаленного узла PPP с помощью заданного протокола.
ppp chap hostname username	С помощью этой команды определяется относящееся к интерфейсу имя узла CHAP. См. Проверку подлинности PPP Использование Команд ppp chap hostname и ppp authentication chap callin для получения дополнительной информации.
ppp chap password password	С помощью этой команды определяется относящийся к интерфейсу пароль CHAP.
вызов **ppp direction** *|*	С помощью этой команды принудительно устанавливается направление вызова. Данную команду используют, когда маршрутизатору не удается определить,

выноска / выделенный	является ли вызов входящим или исходящим (например, когда устанавливается встречно-параллельное подключение или подключение по выделенным линиям, а устройство обслуживания канала или устройство обслуживания данных (CSU/DSU), или адаптер терминала (TA, Terminal Adapter) ISDN настроены на набор номера).
ppp chap refuse [callin]	Этой командой отключается удаленная проверка подлинности одноранговым узлом (по умолчанию проверка подлинности включена). С помощью данной команды CHAP-проверка подлинности отключается для всех вызовов. Это означает, что все попытки, предпринимаемые одноранговым узлом по принудительной проверке подлинности пользователя с помощью CHAP, отвергаются. Параметр "callin" позволяет указать, что маршрутизатор отказывается отвечать на вызовы CHAP-проверки подлинности, получаемые от однорангового узла, но одноранговому узлу по-прежнему требуется отвечать на все CHAP-вызовы, посылаемые маршрутизатором.
ppp chap wait	Этой командой указывается, что вызывающая сторона должна выполнить проверку подлинности первой (по умолчанию настройка включена). Этой командой указывается, что маршрутизатором не проводится проверка подлинности для однорангового узла, запрашивающего CHAP-проверку подлинности до тех пор, пока этим узлом не будет выполнена собственная проверка подлинности для маршрутизатора.
значение **ppp max-bad-auth**	Этой командой задается допустимое число попыток проверки подлинности (значение по умолчанию равно 0). Данной командой интерфейс "точка-точка" настраивается на исключение сброса в исходное состояние сразу после ошибки проверки подлинности, а вместо этого разрешается заданное количество попыток проверки подлинности.
ppp chap splitnames	Этой скрытой командой разрешаются разные имена узлов для CHAP-вызова и CHAP-ответа (по умолчанию разрешение отключено).
ppp chap ignoreus	Этой скрытой командой игнорируются CHAP-вызовы с локальным именем (по умолчанию игнорирование включено).

Пример транзакции

На рисунках в этом разделе показана серия событий, которые происходят во время CHAP-проверки подлинности между двумя маршрутизаторами. **На них не показаны реальные сообщения, отображаемые в выходных данных команды debug ppp negotiation.** Для получения дополнительной информации обратитесь к Пониманию Выходных данных debug ppp negotiation.

Звонить

Рисунок 2 Г Вызов Входит

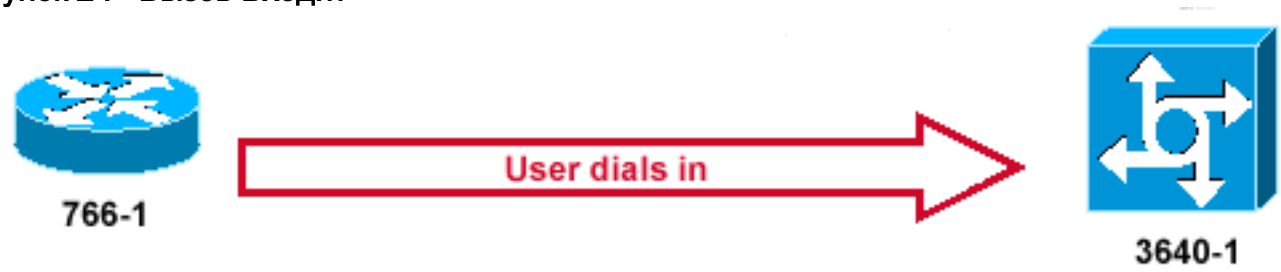


Рисунок 2 показывает эти шаги:

1. Вызов поступает в 3640-1. **Настраивается интерфейс входящих вызовов с помощью команды ppp authentication chap.**
2. LCP согласует CHAP и MD5. Для получения дополнительной информации о том, как определить это, обратитесь к Пониманию Выходных данных debug ppp negotiation.
3. Для данного вызова требуется CHAP-опрос из 3640-1 на вызывающий маршрутизатор.

Проблема

Рисунок 3 Г Пакет запроса вызова CHAP Создан

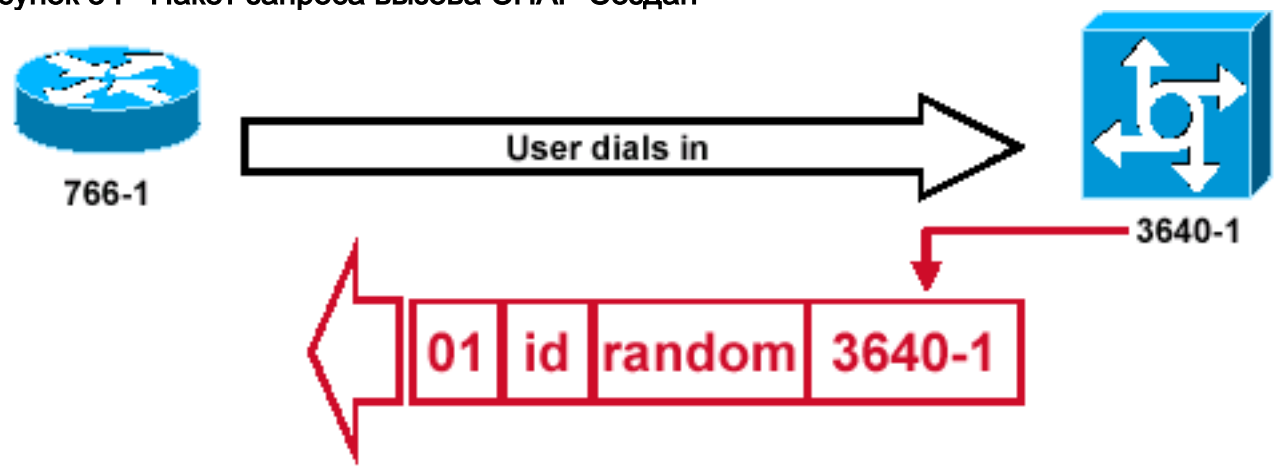


Рисунок 3 иллюстрирует эти шаги в Аутентификацию CHAP между этими двумя маршрутизаторами:

1. Пакет CHAP-вызова создается со следующими характеристиками:01 = идентификатор типа пакета CHAP-вызова.ID = порядковый номер, определяющий CHAP-вызов.random = псевдослучайное число, генерируемое маршрутизатором.3640-1 = имя проверки подлинности отправителя CHAP-вызова.

2. Код и случайные значения хранятся в вызываемом маршрутизаторе.
3. Пакет CHAP-вызова отправляется на вызывающий маршрутизатор. Ведется список ожидающих выполнения CHAP-вызовов.

Ответ

Рисунок 4 Г Получение и Обработка MD5 Пакета вызова от Узла

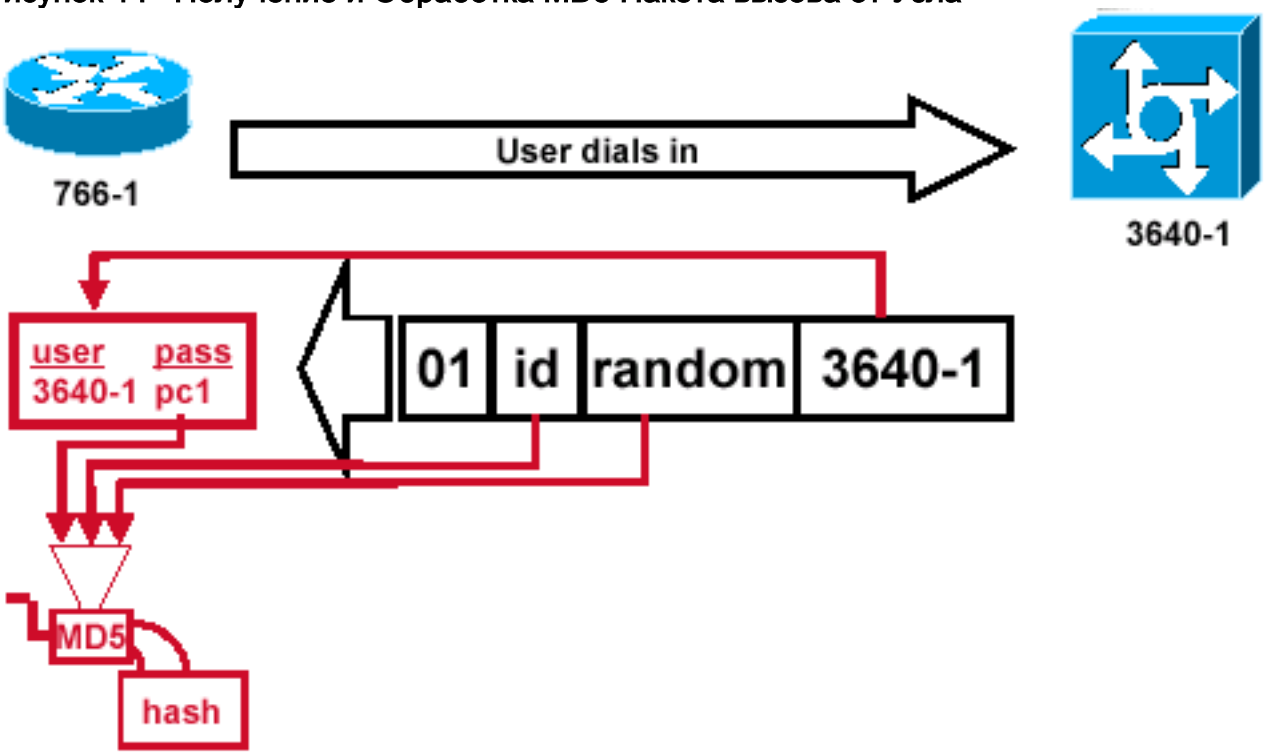


Рисунок 4 иллюстрирует, как пакет вызова получен от узла и обработанный (MD5). Маршрутизатором обрабатывается входящий пакет CHAP-вызова следующим способом:

1. Значение ID подается в мастер создания хэширования MD5.
2. Значение random подается в мастер создания хэширования MD5.
3. Имя 3640-1 используется для поиска пароля. Маршрутизатором ищется запись, соответствующая имени пользователя в CHAP-вызове. В этом примере ищется:`username 3640-1 password pc1`
4. Пароль подается в мастер создания хэширования MD5.Результатом этих действий является MD5-хэшированный CHAP-вызов, который отсылается обратно в CHAP-ответе.

Отклик (продолжение)

Рисунок 5 Г Пакет ответа CHAP, переданный к Средству проверки подлинности, Создан.

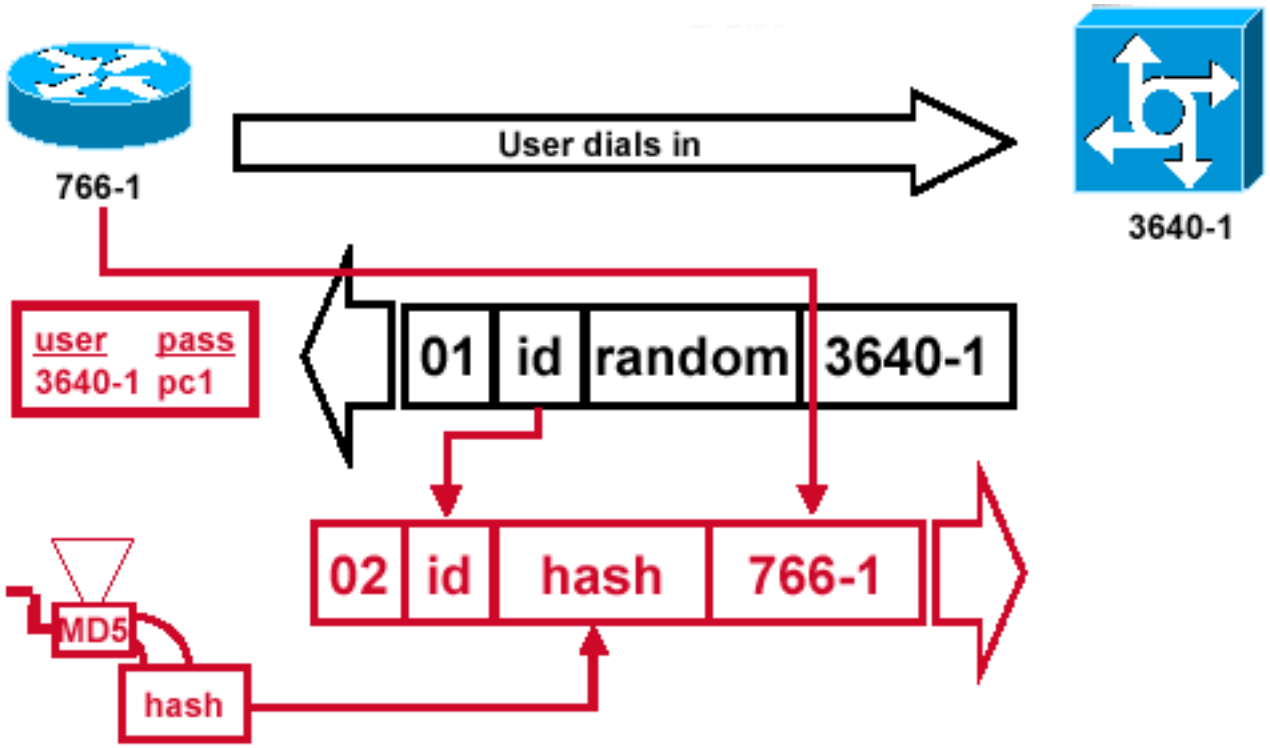


Рисунок 5 иллюстрирует, как создан пакет ответа CHAP, переданный к средству проверки подлинности. На этом рисунке показаны следующие шаги:

1. Пакет ответа собирается из следующих компонентов:02 = идентификатор типа пакета CHAP-ответа.ID = копируется из пакета CHAP-вызова.hash = выходные данные из мастера создания хэширования MD5 (хэшированные сведения из пакета CHAP-вызова).766-1 = имя проверки подлинности данного устройства. Это необходимо для узла к поиску, запись имени пользователя и пароля должна была проверить идентичность (это объяснено более подробно в Сверять разделе CHAP).
2. Затем пакет ответа отправляется отправителю CHAP-вызова.

Проверьте CHAP

В этом разделе даются рекомендации по проверке конфигурации.

Рисунок 6 Г Процессы Претендента Ответный пакет

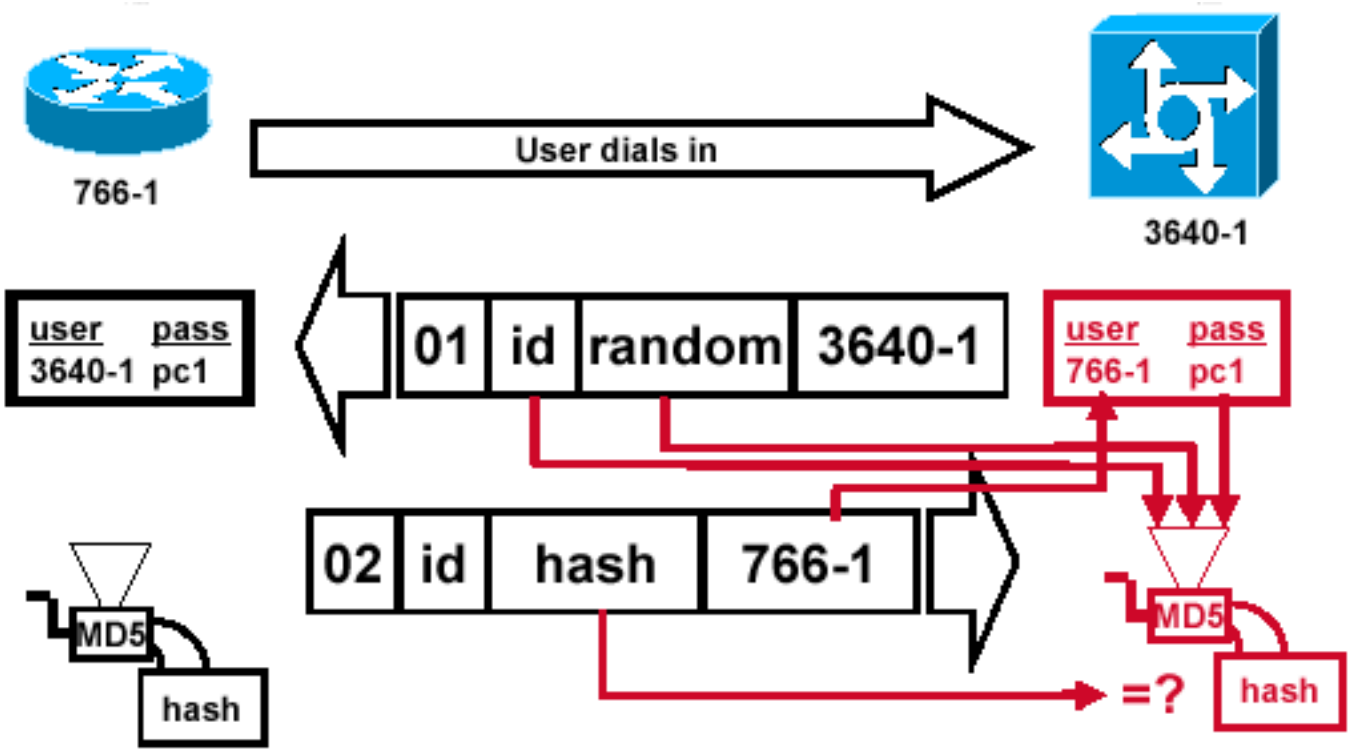


Рисунок 6 показывает, как претендент обрабатывает ответный пакет. Здесь приведены действия, выполняемые при обработке пакета ответа CHAP (на средстве проверки подлинности):

1. Значение ID используется для нахождения пакета исходного CHAP-вызова.
2. Значение ID подается в мастер создания хэширования MD5.
3. Исходное случайное значение запроса подается в генератор хеша MD5.
4. Имя 766-1 используется для поиска пароля в одном из следующих источников:Локальная база данных имен пользователей и паролей.Сервер RADIUS или TACACS+.
5. Пароль подается в мастер создания хэширования MD5.
6. Затем значение хэш-функции, получаемое в пакете ответа, сравнивается с расчетным значением хэш-функции MD5. Проверка подлинности CHAP завершается успешно, если расчетное и полученное значения хеша - равны.

Результат

Рисунок 7 Г Сообщение об успешном завершении Передается Вызывающему маршрутизатору

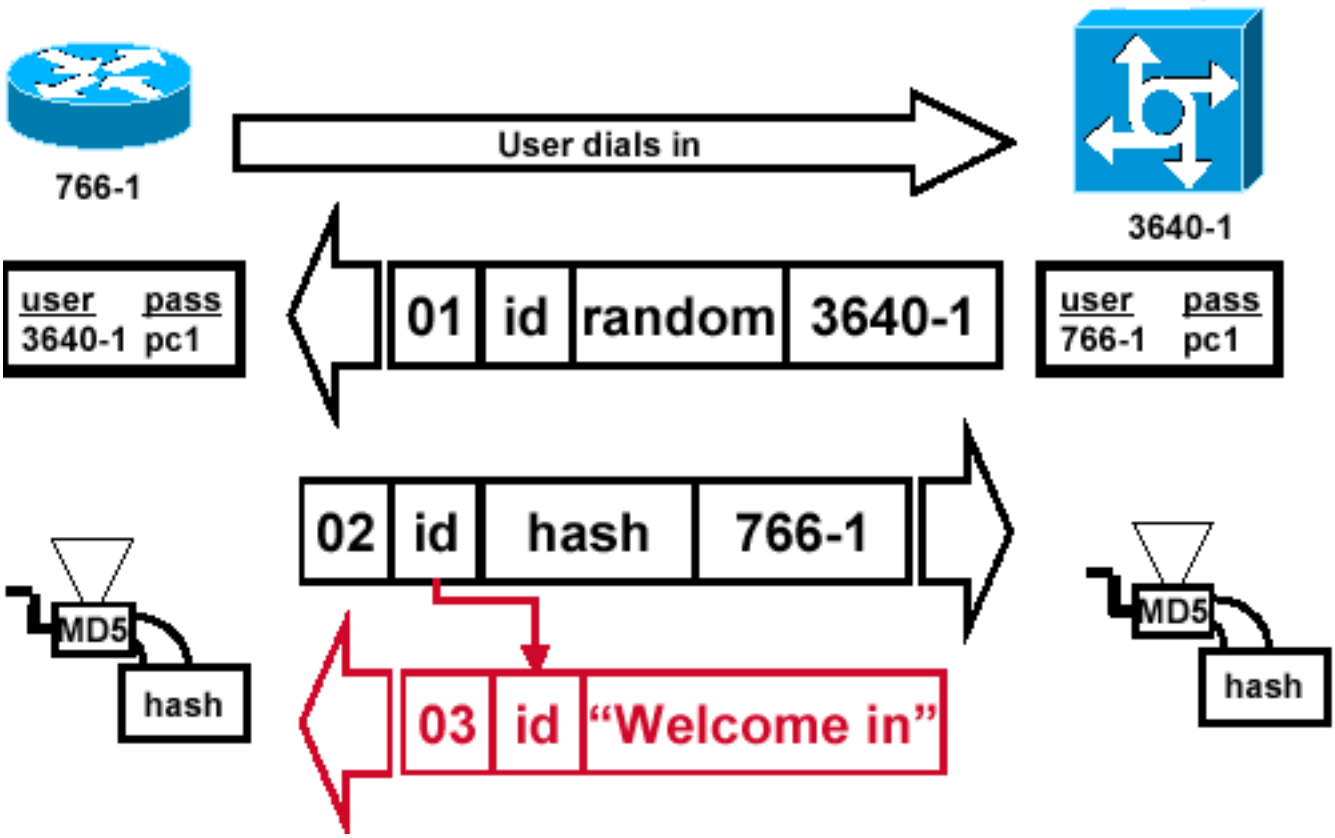


Рисунок 7 иллюстрирует сообщение об успешном завершении, передаваемое вызывающему маршрутизатору. Отправка включает следующие этапы:

1. Если проверка подлинности выполнена успешно, создается пакет успеха CHAP из следующих компонентов:03 = тип CHAP-сообщения об успешном выполнении.ID = копируется из пакета ответа.â Приветствие inâ является просто текстовым сообщением, которое предоставляет объяснение, доступное пользователю.
2. Если проверка подлинности завершается неудачей, создается пакет неудачи CHAP из следующих компонентов:04 = тип CHAP-сообщения о неудаче выполнения.ID = копируется из пакета ответа.â Аутентификация failureâ или другое текстовое сообщение, которое предоставляет объяснение, доступное пользователю.
3. Затем на вызывающий маршрутизатор отправляется пакет успешной или неуспешной проверки подлинности.**Примечание:** Этот пример показывает одностороннюю аутентификацию. В двусторонней проверке подлинности весь этот процесс повторяется. Однако исходный CHAP-вызов инициируется вызывающим маршрутизатором.

CHAP устранения неполадок

См. Устранение проблем Проверки подлинности PPP для получения информации о том, как решить проблемы.

Дополнительные сведения

- Выходные данные команды "debug ppp negotiation"
- Устранение проблем проверки подлинности PPP

- Проверка подлинности PPP с использованием команд ppp chap hostname и ppp authentication chap callin
- Страницы поддержки технологии доступа
- Техническая поддержка - Cisco Systems