

После ввода AT-команды *ATD\*99\*\*\*1#* ответ вида *CONNECT* свидетельствует о готовности GSM-модуля к началу обмена PPP-пакетами.

Отметим, что оригинальные сообщения в данных примерах содержат дополнительные экранирующие символы, наличие или отсутствие которых в пакетах PPP зависит от соответствующей опции LCP. Для упрощения восприятия приведенные примеры очищены от экранирующих символов, что является распространенной практикой при анализе PPP-пакетов.

## 1. PPP Link Control Protocol (LCP)

Фаза LCP служит для конфигурирования параметров соединения: максимального размера принимаемого пакета (Maximum-Receive-Unit, MRU), используемого протокола аутентификации, наличия или отсутствия сжатия полей заголовков PPP-пакетов и некоторых других.

Пакет LCP содержит следующие поля:

Code	Identifier	Length	Data
1 байт	1 байт	2 байта	0...N байт

Поле Code определяет тип сообщения, наиболее часто используемые типы:

01 - Configure-Request – запрос опций

02 - Configure-Ack – подтверждение запроса

03 - Configure-Nak – отклонение запроса с предложением собственных опций

04 - Configure-Reject – отклонение запроса с перечислением неприемлемых опций

Другие допустимые типы сообщений LCP можно найти в документах [3] и [4].

Поле Identifier содержит идентификатор сообщения, служащий для связывания между собой запроса и ответа.

Поле Length определяет длину LCP-пакета, включая поля Code, Identifier, Length и Data. Значение поля Length не должно превышать величину MRU.

Поле Data содержит данные, формат которых определяется полем Code.

С более подробным описанием полей пакетов LCP можно ознакомиться в [3].

В случае использования GSM-модулей на этапе LCP необходимо согласовывать параметры (опции) соединения для каждого из двух направлений передачи в отдельности. Рассмотрим конкретный пример обмена данными в фазе LCP между GSM-модулем и управляющим микроконтроллером (MCU).

1.1 GSM-модуль запрашивает опции соединения:

7E FF 03 C0 21 01 01 00 12 02 06 00 0A 00 00 03 04 C0 23 07 02 08 02 55 83 7E

C0 21 - протокол LCP

01 – запрос (Configure-Request)

01 – идентификатор сообщения

00 12 – длина пакета LCP

02 06 00 0A 00 00 - Async-Control-Character-Map

03 04 C0 23 – протокол аутентификации PAP

07 02 – компрессия поля протокола (Protocol-Field-Compression)

08 02 – компрессия полей адреса и управления (Address-and-Control-Field-Compression)

55 83 – контрольная сумма

1.2 MCU параллельно запрашивает опции соединения для обратного направления (в данном случае опции по умолчанию):

7E FF 03 C0 21 01 02 00 04 B5 5A 7E

C0 21 - протокол LCP

01 – запрос (Configure-Request)

02 – идентификатор сообщения

00 04 - длина пакета LCP (поле данных LCP отсутствует, опции по умолчанию)

B5 5A – контрольная сумма

1.3 GSM-модуль подтверждает запрошенные MCU опции соединения:

7E FF 03 C0 21 02 02 00 04 78 7F 7E

C0 21 - протокол LCP

02 – подтверждение запроса (Configure-Ack)

02 – идентификатор сообщения

00 04 - длина пакета LCP (поле данных LCP отсутствует, опции по умолчанию)  
78 7F – контрольная сумма

1.4 MCU отклоняет запрос модуля с идентификатором 01 и указывает неприемлемые опции:

7E FF 03 C0 21 04 01 00 0E 02 06 00 0A 00 00 07 02 08 02 74 50 7E

C0 21 - протокол LCP  
04 – отклонение запроса с перечислением неприемлемых опций (Configure-Reject)  
01 – идентификатор сообщения  
00 0E - длина пакета LCP  
02 06 00 0A 00 00 - Async-Control-Character-Map  
07 02 – компрессия поля протокола (Protocol-Field-Compression)  
08 02 – компрессия полей адреса и управления (Address-and-Control-Field-Compression)  
74 50 – контрольная сумма

1.5 GSM-модуль посылает новый запрос с учетом отклоненных опций:

7E FF 03 C0 21 01 02 00 08 03 04 C0 23 23 EB 7E

C0 21 - протокол LCP  
01 – запрос (Configure-Request)  
02 – идентификатор сообщения  
00 08 – длина пакета LCP  
03 04 C0 23 – протокол аутентификации PAP  
23 EB – контрольная сумма пакета

1.6 MCU подтверждает принятый от GSM-модуля запрос:

7E FF 03 C0 21 02 02 00 08 03 04 C0 23 F3 61 7E

C0 21 - протокол LCP  
02 – подтверждение запроса (Configure-Ack)  
02 – идентификатор сообщения  
00 08 - длина пакета LCP  
03 04 C0 23 – протокол аутентификации PAP  
F3 61 – контрольная сумма

После согласования опций соединения в обоих направлениях фаза LCP считается завершенной, можно переходить к следующему этапу - аутентификации.

## 2. PPP Authentication

Рассмотрим обмен пакетами между MCU и GSM-модулем на примере использования в фазе аутентификации протокола Password Authentication Protocol (PAP). Формат пакета PAP аналогичен формату пакетов LCP, поле Code может содержать следующие значения:

01 - Authenticate-Request – запрос аутентификации  
02 - Authenticate-Ack – подтверждение аутентификации  
03 - Authenticate-Nak – отклонение запроса аутентификации

В данном конкретном примере при аутентификации используется имя пользователя avan и пароль - avan.

2.1 MCU отправляет запрос аутентификации PAP:

7E FF 03 C0 23 01 01 00 0C 04 61 76 61 6E 04 61 76 61 6E 17 08 7E

C0 23 - протокол PAP  
01 – запрос (Authenticate-Request)  
01 – идентификатор сообщения  
00 0C – длина пакета PAP  
04 61 76 61 6E 04 61 76 61 6E – пользователь – avan, пароль - avan  
17 08 – контрольная сумма

2.2 GSM-модуль подтверждает принятый запрос:

7E FF 03 C0 23 02 01 00 05 00 8B 3B 7E

C0 23 - протокол PAP  
02 – подтверждение запроса (Authenticate-Ack)  
01 – идентификатор сообщения  
00 05 - длина пакета PAP  
00 – поле данных имеет нулевую длину  
8B 3B – контрольная сумма

## 3. PPP Network Control Protocol (NCP)

Наиболее часто используемым в фазе NCP протоколом является Internet Protocol Control Protocol (IPCP). Формат пакета IPCP аналогичен формату пакета LCP. Рассмотрим конкретный пример обмена пакетами IPCP между MCU и GSM-модулем .

3.1 После завершения фазы аутентификации GSM-модуль отправляет запрос IPCP нулевой длины:

7E FF 03 80 21 01 01 00 04 00 B7 7E

80 21 - протокол IPCP

01 – запрос (Configure-Request)

01 – идентификатор сообщения

00 04 - длина пакета IPCP (поле данных IPCP отсутствует)

00 B7 – контрольная сумма

3.2 MCU отправляет модулю свой запрос IPCP, содержащий IP-адрес 0.0.0.0:

7E FF 03 80 21 01 05 00 0A 03 06 00 00 00 00 F6 17 7E

80 21 - протокол IPCP

01 – запрос (Configure-Request)

05 – идентификатор сообщения

00 0A - длина пакета IPCP

03 06 00 00 00 00 – нулевой IP-адрес

00 B7 – контрольная сумма

3.3 MCU также отправляет подтверждение запроса, принятого от GSM-модуля :

7E FF 03 80 21 02 01 00 04 CD 92 7E

80 21 - протокол IPCP

02 – подтверждение запроса (Configure-Ack)

01 – идентификатор сообщения

00 04 - длина пакета IPCP (поле данных IPCP отсутствует)

CD 92 – контрольная сумма

3.4 GSM-модуль отклоняет запрос, принятый от MCU, предлагая другой IP-адрес:

7E FF 03 80 21 03 05 00 0A 03 06 64 6A BB AF BC 51 7E

80 21 – протокол IPCP

03 – отклонение запроса и предложение собственных опций (Configure-Nak)

05 – идентификатор сообщения

00 0A – длина пакета IPCP

03 06 64 6A BB AF – IP-адрес 100.106.187.175

BC 51 – контрольная сумма

3.5 MCU формирует новый запрос, содержащий IP-адрес, предложенный модулем:

7E FF 03 80 21 01 06 00 0A 03 06 64 6A BB AF F5 DF 7E

80 21 – протокол IPCP

01 – запрос (Configure-Request)

06 – идентификатор сообщения

00 0A – длина пакета IPCP

03 06 64 6A BB AF – IP-адрес 100.106.187.175

F5 DF – контрольная сумма

3.6 GSM-модуля подтверждает принятый запрос:

7E FF 03 80 21 02 06 00 0A 03 06 64 6A BB AF 9C AB 7E

80 21 – протокол IPCP

02 – подтверждение запроса (Configure-Ack)

06 – идентификатор сообщения

00 0A – длина пакета IPCP

03 06 64 6A BB AF – IP-адрес 100.106.187.175

9C AB – контрольная сумма

После получения управляющим устройством подтверждения, содержащего IP-адрес, соединение PPP считается установленным.