AT Commands Interface for TCP/IP

Version : **For eDsoft-w302 v1.0 Doc rev 1.7**

Date : **Avr, 15th 2003 by F.D. eDevice**

Reference :

Level	Date	History of the evolution	
00.1	06/08/02	Creation	
001	19/11/02	Update and review	
01.3	03/03/03	Updated with new response codes	
01.4	07/03/03	Amendments after doc review.	
01.5	11/03/03	Amendments during acceptance test execution	
01.6	18/03/03	Added note for manual accptance of incoming call	
01.7	15/04/03	Minor page setting	

Contents

1 Introduction

1.1 Scope of this document

This document describes the AT parameters and command set available to configure and drive the TCP/IP stack and protocols available on Wavecom products.

TCP/IP features and protocols available:

- PPP
- GPRS
- ICMP
- DNS
- SMTP
- POP3
- FTP
- TCP socket

2 AT# PARAMETERS SET

2.1 ANSWERMODE

Target	Dialing features GSM
Definition	The TCP/IP stack can handle incoming calls in different ways. This parameter defines how the TCP/IP stack will behave when receiving an incoming call.
Legal values	0: (Ignore) ignores the incoming call. In this case, it is the responsibility of the host to accept/not accept the incoming call by issuing the AT#ACCEPT command. 1: (Automatic Answer) The TCP/IP stack goes off hook and accepts the incoming call. As described below, the calling number must match the one specified in the CALLSCREENNUM parameter. (The RINGCOUNT parameter must be > 0). 2: (Static Callback) The TCP/IP stack ignores the incoming call and then automatically dials (DIALN1 or DIALN2 determined by the DIALSELECT parameter) by issuing an AT#CONNECTIONSTART command. As described below, the calling number must match the one specified in the CALLSCREENNUM parameter. The RINGCOUNT parameter must be > 0. 3: (Dynamic Callback) The TCP/IP stack ignores the incoming call and then automatically dials the calling number by issuing an AT#CONNECTIONSTART command. For this feature, the CallerID service is mandatory. As described below, the calling number must match the one specified in the CALLSCREENNUM parameter. Ensure that the calling phone number is correctly provided by the network.
Legal values	Integer between 0 and 3 inclusive.
Default value	0
Note	The ANSWERMODE parameter must be configured in accordance with the ATS0 configuration for not interacting.

2.2 APNSERV

Target	GPRS feature
Definition	Access Point Name parameter coming from the GSM operator for providing GPRS access.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter

2.3 APNPW

Target	GPRS feature
Definition	Access Point Name password parameter coming with the APNUN from the GSM operator for providing GPRS access.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter

2.4 APNUN

Target	GPRS feature
Definition	Access Point Name Username parameter coming with the APNPW from the GSM operator for providing GPRS access.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter

2.5 BODY1 / BODY2 / BODY3

Target	SMTP / Email Sending features
Definition	These parameters store pre-defined message bodies. They allow the host application to send pre-defined e-mail combinations
Legal values	The body content has to be entered after the AT#BODY1(CR) command has been executed and the response message Ok_Info_WaitingForData is displayed. It has to be an alphanumeric ASCII text string up to 120 characters followed by the following character: 0x1A (ASCII) <SUB> Generated on a keyboard by CTRL+Z (depending on the keyboard configuration). Example for single line: AT#BODY1(CR) Text string (CTRL)+Z (ASCII 0x1A) Example for multi line: AT#BODY1(CR) Text string (CR)(LF) Text string (CR)(LF) (CTRL)+Z (ASCII 0x1A)
Default value	There is no default value for this parameter
Note	The total size of the email body must not exceed the 120 character limit.

2.6 CALLBACKTIMER

Target	Dialing features GSM
Definition	This parameter defines the number of seconds the TCP/IP stack will wait before an automatic call-back operation occurs after receiving an incoming call. It only applies when the ANSWERMODE parameter is set to an automatic call-back mode (value>1). This timer starts at the end of the ringing signal.
Legal values	Integer between 2 and 255 inclusive. This timer is set in seconds.
Default value	2

2.7 CALLSCREENNUM

Target	Dialing Specific features
Definition	When receiving an incoming call, the caller identification (Caller ID) service allows the TCP/IP stack to identify the phone number of the remote caller. This service is helpful in preventing unauthorized callers triggering actions on the TCP/IP stack. This parameter allows the user to filter the incoming calls when the ANSWERMODE parameter is set to an automatic mode (value>0). This filtering doesn't apply when the ANSWERMODE parameter is set to 0, in this case it is the host's responsibility to accept or reject the incoming call. If an incoming phone number is unauthorised, the TCP/IP stack will ignore it.
Legal values	0 (zero): No remote caller authorized. Value between "". * (all): No filtering is applied on incoming calls. All the remote phone numbers are authorized. This value must be set when wanting to receive incoming calls while the Caller ID service is not available. Value between "". Decimal phone number: Only the phone number configured here before is authorized for incoming calls. Value between "". Ensure that this value is exactly that of the CLI digit string of the incoming call (international format can be used).
Default value	0

2.8 CCREC1 / CCREC2 / CCREC3

Target	SMTP / Email Sending
Definition	The software can send e-mail messages to an additional recipient as a "carbon copy". This parameter contains the e-mail address of the additional recipient. This e-mail address will appear in the header of the e-mail sent by the TCP/IP stack software in the field ' Cc: '. For a given value n, the "CCRECn" parameter is directly associated with the "RECn" parameter.
Legal values	Alphanumeric ASCII text string between "". up to 120 characters. The address must be provided in literal format (for instance dev12345678@edevice.com).
Default value	There is no default value for this parameter

2.9 DIALN1

Target	Dialing features GSM
Definition	Primary dial-up phone number for call origination.
Legal values	Decimal phone numbers between "" (up to 64 characters)
Default value	There is no default value for this parameter

2.10 DIALN2

Target	Dialing features GSM
Definition	Secondary dial-up phone number for call origination..
Legal values	Decimal phone numbers between "" (up to 64 characters)
Default value	There is no default value for this parameter

2.11 DIALSELECT

Target	Dialing features GSM
Definition	The value of this parameter determines the number to be used for an outgoing call attempt. It configures the TCP/IP stack software to use the primary dial-up number or the secondary dial-up number.
Legal values	Integer between 1 and 2 inclusive. 1: Use primary dial-up number 2: Use secondary dial-up number
Default value	1

2.12 DLEMODE

Target	Socket TCP
Definition	When using socket TCP, the attached host has the choice whether or not to code the ETX character.
Legal values	Integer between 0 and 1 inclusive. 0: When DLEMODE is set to 0, no specific process is needed on [ETX] characters. It means that it is not possible for a host to request an end of connection or to receive a clear indication of the end of a connection from the TCP/IP stack. 1: When DLEMODE is set to 1, the [ETX] character means a request or an indication of end of connection. As a consequence, [ETX] characters that belong to the payload data must be sent by the host on the serial port preceded by a DLE character. Similarly ETX characters received by the TCP/IP stack from the Internet are sent to the host through the serial port preceded by a DLE character
Default value	1

2.13 DNSSERV1

Target	Domain Name configuration
Definition	In order to translate the server names from literal format into IP addresses, the TCP/IP stack software implements the Domain Name System (DNS) protocol. The DNS Server IP address must be specified for use by the TCP/IP stack software.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "".
Default value	0.0.0.0

2.14 DNSSERV2

Target	Domain Name configuration
Definition	In order to translate the server names from literal format into IP addresses, the TCP/IP stack software implements the Domain Name System (DNS) protocol. The DNS Server IP address has to be specified for use by the TCP/IP stack software. This secondary DNS server is used in the case where the primary DNS server does not respond to a request.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "".
Default value	0.0.0.0

2.15 DOMAIN

Target	SMTP / Email Sending
Definition	When sending an e-mail message, the TCP/IP stack software must provide the SMTP server with the domain name of the sender. In some cases, this domain name may be different from the domain name included in the sender's e-mail address.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter

2.16 FTPGETFILENAME

Target	FTP
Definition	In order to download a file from the FTP server, the TCP/IP stack software must know the name of the relevant file.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter

2.17 FTPGETPATH

Target	FTP
Definition	In order for the TCP/IP stack software to get a file from the FTP server, the TCP/IP stack software must know the path of the relevant file. For example, it could be : /list
Legal values	Alpha-numeric ASCII text string between "" up to 120 characters.
Default value	.
Note	Depending on the FTP server, the value . can be used for getting a file from the root directory of the FTP server

2.18 FTPPORT

Target	FTP
Definition	To reach the FTP server, the TCP/IP stack software must know the control port of the FTP server used for file transfer.
Legal values	From 1 to 5 digits (each digit between 0 and 9 inclusive). Note that numbers above 65,535 are illegal as the port identification fields are 16 bits long in the TCP header. Value between "".
Default value	21
Note	This parameter should be changed only upon request of your network administrator. It depends on network infrastructure configuration including Firewalls, Proxy or specific TCP port translation settings.

2.19 FTPPUTFILENAME

Target	FTP
Definition	In order for the TCP/IP stack software to upload a file to the FTP server, the TCP/IP stack software must know the name of the relevant file.
Legal values	Alpha-numeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter.

2.20 FTPPUTPATH

Target	FTP
Definition	In order for the TCP/IP stack software to upload a file to the FTP server, the TCP/IP stack software must know the path of the relevant file. For example, it could be : /list
Legal values	Alpha-numeric ASCII text string between "" up to 120 characters.
Default value	.
Note	Depending on the FTP server, the value . can be used for putting a file into the root directory of the FTP server.

2.21 FTPPW

Target	FTP
Definition	Before transferring files from a specified FTP server, the TCP/IP stack software must open an FTP session using a valid FTP password.
Legal values	Alphanumeric ASCII text string between "" up to 64 characters
Default value	There is no default value for this parameter

2.22 FTPSERV

Target	FTP
Definition	FTP server address. To connect to an FTP server to download files, the TCP/IP stack software must know the address of the FTP server that is to be used.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "". Or alphanumeric ASCII text string between "" up to 120 characters if DNS is available
Default value	There is no default value for this parameter

2.23 FTPTYPE

Target	FTP
Definition	Before transferring files from a specified FTP server, the TCP/IP stack software must specify the type of data to be transferred within the FTP session.
Legal values	A or I character. A for FTP ASCII sessions I for FTP Binary sessions
Default value	I
Note	When this value is set to A, all the data sent by the TCP/IP stack to the FTP server is made of 7 bits characters (NVT-ASCII: the MSB is set to 0). As a consequence binary data containing 8 bits characters will be corrupted during the transfer if the FTPTYPE is set to A.

2.24 FTPUN

Target	FTP
Definition	Before transferring files from a specified FTP server, the TCP/IP stack software must open an FTP session using a valid FTP user name
Legal values	Alphanumeric ASCII text string between "" up to 64 characters.
Default value	There is no default value for this parameter

2.25 GPRSCID

Target	GPRS feature
Definition	PDP context identifier which specifies a particular PDP context definition. This parameter is local and may be used in other PDP context-related commands.
Legal values	Numeric between 1 and 4 inclusive
Default value	1

2.26 GPRSMODE

Target	GPRS feature
Definition	Configure the activation of the Wavecom software for switching between GSM or GPRS.
Legal values	Integer between 0 and 1 inclusive. 0: The Wavecom software is configured for a GSM connection attempt. 1: The Wavecom software is configured for a GPRS connection attempt
Default value	1

2.27 ISPUN

Target	PPP
Definition	User name of the ISP account. When communication is initiated and once the physical (modem) connection has been established with the ISP, the TCP/IP stack software must provide the ISP with the user name associated with the account to be used.
Legal values	Alpha-numeric ASCII text string between "" up to 64 characters
Default value	There is no default value for this parameter
Note	GSM only.

2.28 ISPPW

Target	PPP
Definition	Password for the ISP account. When communication is initiated and once the physical (modem) connection has been established with the ISP, the TCP/IP stack software must provide the ISP with the password associated with the account to be used.
Legal values	Alpha-numeric ASCII text string between "" up to 64 characters
Default value	There is no default value for this parameter
Note	GSM only.

2.29 PHYTIMEOUT

Target	General configuration (GSM)
Definition	Used by the TCP/IP stack software in order to terminate connections to the telephone line when a long period elapses without activity. "Without activity" is defined as a period when no data is transferred between the Internet and the TCP/IP stack software or between the TCP/IP stack software and the attached equipment. This timer prevents the GSM call from being connected indefinitely for any reason.
Legal values	Integer between 1 and 255 inclusive. This timer is set in minutes.
Default value	15
Note	When the inactivity timer expires, the Wavecom product ends the communication. Error message #CME ERROR: 35862 is displayed. (See section ' Response messages and error codes'.)

2.30 POP3HEADERMODE

Target	POP3 / Email Retrieving
Definition	When receiving an email message, the TCP/IP stack can be configured to send or not to send the POP3 header over the serial port. The POP3 header contains the From, Cc and Subject fields.
Legal values	Integer between 0 and 1 inclusive. 0: the email header will not be sent over the serial port while retrieving 1: the email header will be sent over the serial port while retrieving
Default value	1

2.31 POP3PORT

Target	POP3 / Email Retrieving
Definition	To reach the POP3 server, the TCP/IP stack software must know the port of the POP3 server used for the email retrieving.
Legal values	From 1 to 5 digits (each digit between 0 and 9 inclusive). Note that numbers above 65,535 are illegal as the port identification fields are 16 bits long in the TCP header. Value between "".
Default value	110
Note	This parameter should be changed only upon request of your network administrator. It depends on network infrastructure configuration including Firewalls, Proxy or specific TCP port translation settings.

2.32 POP3PW

Target	POP3 / Email Retrieving
Definition	Password for POP3 account. To retrieve e-mail messages sent to a specified e-mail address, the TCP/IP stack software must know the POP3 password that has been set for that e-mail account.
Legal values	Alphanumeric ASCII text string between "" up to 64 characters.
Default value	There is no default value for this parameter

2.33 POP3SERV

Target	POP3 / Email Retrieving
Definition	To retrieve e-mail messages, the TCP/IP stack software must know the address of the POP3 server that is to be used. The POP3 server must be the one where the specified e-mail account is hosted (which is not necessarily maintained by the local ISP).
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "". Or alphanumeric ASCII text string between "" up to 120 characters if DNS is available.
Default value	There is no default value for this parameter

2.34 POP3UN

Target	POP3 / Email Retrieving
Definition	User name for POP3 account. To retrieve e-mail messages sent to a specified e-mail address, the TCP/IP stack software must know the POP3 user name that has been set for that e-mail account.
Legal values	Alphanumeric ASCII text string between "" up to 64 characters.
Default value	There is no default value for this parameter

2.35 PPPMODE

Target	PPP
Definition	The TCP/IP stack can manage the access layer through different ways. This parameter selects the behavior the TCP/IP stack must run once the physical layer successfully established.
Legal values	Integer between 0 and 4 inclusive. 0: (Modem) the TCP/IP stack behaves as a standard modem. The data is sent/received to/from a remote standard modem in a point-to-point connection. No IP/PPP stack is running. 1: (Standard PPP) the TCP/IP stack behaves as a PPP client for outgoing calls and as a PPP server for incoming calls. 2: (Reverse PPP) the TCP/IP stack behaves as a PPP server for outgoing calls and as a PPP client for incoming calls. 3: (PPP client only) the TCP/IP stack always behaves as a PPP client for both outgoing and incoming calls. 4: (PPP server only) the TCP/IP stack always behaves as a PPP server for both outgoing and incoming calls.
Default value	1
Note	GSM only

2.36 PPPMYIP

Target	PPP
Definition	When the TCP/IP stack behaves as a PPP server (according to the PPPMODE parameter setting), it is in charge of the IP address attribution mechanism. Once the PPP authentication is successfully achieved, the remote PPP peer asks the TCP/IP stack for an IP address. The related PPP layer, called IPCP, then suggests an IP address to the peer that has been previously stored in the TCP/IP stack parameters. If the remote accepts this address, the IP link is then established. This parameter defines the IP address to be attributed to the TCP/IP stack when the PPP Server mode is running.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "".
Default value	0.0.0.0
Note	GSM only.

2.37 PPPPEERIP

Target	PPP
Definition	When the TCP/IP stack behaves as a PPP server (according to the PPPMODE parameter setting), it is in charge of the IP address attribution mechanism. Once the PPP authentication successfully achieved, the remote PPP peer asks the TCP/IP stack for an IP address. The related PPP layer, called IPCP, then suggests an IP address to the peer that has been previously stored in the TCP/IP stack parameters. If the remote accepts this address, the IP link is then established. This parameter defines the IP address to be attributed to the remote PPP peer when the PPP Server mode is running.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "".
Default value	0.0.0.0
Note	GSM only.

2.38 PPPSERVPW

Target	PPP
Definition	When the TCP/IP stack behaves as a PPP server (according to the PPPMODE parameter setting), it checks the remote PPP client login/password before granting access to the server. This parameter defines the password that must be specified by the remote PPP client.
Legal values	Alpha-numeric ASCII text string up to 64 characters between "".
Default value	There is no default value for this parameter
Note	GSM only.

2.39 PPPSERVUN

Target	PPP
Definition	When the TCP/IP stack behaves as a PPP server (according to the PPPMODE parameter), it checks the remote PPP client login/password before granting access. This parameter defines the username that must be specified by the remote PPP client.
Legal values	Alpha-numeric ASCII text string between "" up to 64 characters
Default value	there is no default value for this parameter
Note	GSM only

2.40 REC1 / REC2 / REC3

Target	SMTP / Email Sending
Definition	To send e-mail messages, the TCP/IP stack software must know the e-mail address of the recipient. This e-mail address will appear in the header of the e-mail sent by the TCP/IP stack software, in the field ` To: `.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters. The address must be provided in literal format (for instance dev12345678@wavecom.com).
Default value	There is no default value for this parameter

2.41 REDIALCOUNT

Target	Dialing features GSM
Definition	Indicates how many unsuccessful connection attempts the TCP/IP stack software will make before terminating the connection attempt activity.
Legal values	Integer between 0 and 14, inclusive. If the value is set to 0, the TCP/IP stack software will not make any call retry.
Default value	5

2.42 REDIALDELAY

Target	Dialing features GSM
Definition	It controls how much of delay (in seconds), if any, will be between each call retry.
Legal values	Integer between 5 and 14 inclusive. If this parameter is configured to zero, the TCP/IP stack software will attempt another connection immediately after terminating the previous unsuccessful attempt.
Default value	5

2.43 RINGCOUNT

Target	Dialing features GSM
Definition	This parameter defines the number of rings that will be counted before an automatic operation occurs when receiving an incoming call. This parameter only applies when the ANSWERMODE parameter is set to an automatic mode (value>0). To use this feature with the ANSWERMODE parameter (value >0), the RINGCOUNT value must also be >0.
Legal values	Integer between 0 and 15 inclusive.
Default value	0
Note	The RINGCOUNT parameter must be configured in accordance with the ATS0 configuration to prevent conflicting interaction with the two features.

2.44 SENDERADDR

Target	SMTP / Email Sending
Definition	To send e-mails, the TCP/IP stack software must know the e-mail address of the sender. The "sender" is the email identification of the hardware platform itself or the optional attached equipment. This e-mail address will appear in the header of the e-mail sent by the TCP/IP stack software, in the field ' From: '.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters. The address must be provided in literal format (for instance dev12345678@wavecom.com).
Default value	There is no default value for this parameter

2.45 SENDERNAME

Target	SMTP / Email Sending features
Definition	The sender's literal name (different from the SENDERADDR parameter, which is the sender's email address). This parameter will appear in the header of the e-mail sent by the TCP/IP stack software, in the field: 'From: '.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters. The address must be provided in literal format (for instance "machine 245").
Default value	There is no default value for this parameter

2.46 SMTPPORT

Target	SMTP / Email Sending
Definition	To reach the SMTP server, the TCP/IP stack software must know the port of the SMTP server used for the email sending.
Legal values	From 1 to 5 digits (each digit between 0 and 9 inclusive). Note that numbers above 65,535 are illegal as the port identification fields are 16 bits long in the TCP header.
Default value	25
Note	This parameter should be changed only upon request of your network administrator. It depends on network infrastructure configuration including Firewalls, Proxy or specific TCP port translation settings.

2.47 SMTPPW

Target	SMTP / Email Sending
Definition	To send email messages, some SMTP servers are using an authentication process. In these cases, the TCP/IP stack software will provide the SMTP password (associated to the SMTP user name) for the email sending process.
Legal values	Alphanumeric ASCII text string between "" up to 64 characters.
Default value	There is no default value for this parameter

2.48 SMTPSERV

Target	SMTP / Email Sending
Definition	To send e-mail messages the TCP/IP stack software must know the address of the SMTP server that is to be used. In most cases, the local ISP maintains the SMTP server.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "". Or alphanumeric ASCII text string between "" up to 120 characters if DNS is available.
Default value	There is no default value for this parameter

2.49 SMTPUN

Target	SMTP / Email Sending
Definition	To send email messages, some SMTP servers use an authentication process. In these cases, the TCP/IP stack software will provide the SMTP user name (associated with a SMTP password) for the email sending process.
Legal values	Alphanumeric ASCII text string between "" up to 64 characters.
Default value	There is no default value for this parameter

2.50 SUBJ1 / SUBJ2 / SUBJ3

Target	SMTP / Email Sending
Definition	These parameters contain the pre-defined subject text that will be used by the TCP/IP stack to compose the e-mail header.
Legal values	Alphanumeric ASCII text string between "" up to 120 characters.
Default value	There is no default value for this parameter

2.51 TCPPORT

Target	Socket TCP
Definition	For opening a socket: To exchange data over TCP, the TCP/IP stack software must know the port of the remote peer used for the TCP session. For a listening socket: Defines the number of the port to be opened in listen mode.
Legal values	From 1 to 5 digits (each digit between 0 and 9 inclusive). Note that numbers above 65,535 are illegal as the port identification fields are 16 bits long in the TCP header.
Default value	0
Note	This parameter should be configured on advice from your network administrator. It depends on network infrastructure configuration including Firewalls, Proxy or specific TCP port translation settings.

2.52 TCPSERV

Target	Socket TCP
Definition	For opening a socket: To exchange data over TCP, the TCP/IP stack software must know the address of the remote TCP server (or host) that is to be used. For a listening socket: Used to apply filtering of incoming TCP requests from a remote destination IP address. Only requests from the configured IP address will be allowed to connect to the Wavecom module.
Legal values	32-bit number in dotted-decimal notation (i.e. xxx.xxx.xxx.xxx) between "". Or alphanumeric ASCII text string between "" up to 120 characters if DNS is integrated.
Default value	There is no default value for this parameter

3 AT# COMMANDS SET

3.1 AT#ACCEPT

Target	Dialing features GSM	
Definition	This command directs the TCP/IP stack to answer an incoming call. When the TCP/IP stack receives an incoming call, it sends over the serial port the "RING" messages. Depending on the value of the ANSWERMODE parameter the TCP/IP stack may answer automatically or not. If ANSWERMODE is set to 0, it is the host that is responsible for answering the incoming call. Once the physical layer is up, the TCP/IP stack runs the applicable protocol as specified in the PPPMODE parameter. The AT#CONNECTIONSTOP command ends the connection by going on hook.	
Return codes	<digit sequence>	*DIALN1 or DIALN2 depending on DIALSELECT*
	CONNECT <rate>	*Modem speed negotiated between both side.* *If the TCP/IP stack is configured for modem only operation (PPPMODE parameter) there are no further return codes.*
	xx.xx.xx.xx	*IP address attributed to the TCP/IP stack*
	Ok_Info_Ppp	*As soon as the TCP/IP stack software displays this message it is ready to receive commands, PPP protocol is running.*
Error codes	#CME ERROR: <value>	*The PPP negotiation has failed (check ISPUN, ISPPW and PPPMODE and the configuration of the PPP peer)* (See section ' Response messages and error codes'.)
	NO CARRIER	*The modem handshaking process with the remote host is interrupted or unsuccessful.*
Note	If an incoming call answer attempt is made at the same time that the call is being answered automatically by the module (in the case where the answermode parameter is >0), there is the possibility that the message #CME ERROR 49153 will be displayed. This is due to an attempt to answer the incoming call twice, once automatically and once manually. This error message display is expected behaviour and the module will continue to handle the incoming call.	

3.2 AT#CONNECTIONSTART

Target	Dialing features GSM / GPRS feature	
Definition	This command directs the TCP/IP stack to originate an outgoing call. Upon receiving this command, the TCP/IP stack attempts to complete a connection session according to the GPRSMODE parameter, selecting the GSM or GPRS mode. - In GSM mode, the TCP/IP stack will dial the number according to the Dial Option parameter (DIALN1 or DIALN2 depending on DIALSELECT). If an error occurs, the TCP/IP stack automatically re-attempts the call origination attempt, according to the REDIALCOUNT parameter. Once the physical layer is up, the TCP/IP stack runs the applicable protocol as specified in the PPPMODE parameter. - In GPRS mode, the TCP/IP stack will establish a GPRS session with the APN using APNUN, APNPW, GPRSCID parameter. Once the GPRS link is up, the product is connected to the Internet. The AT#CONNECTIONSTOP command closes the GSM or GPRS connection session.	
Return codes in GSM mode.	DIALING	*The phone line is available*
	<digit sequence>	*DIALN1 or DIALN2 depending on DIALSELECT*
	CONNECT <rate>	*Modem speed negotiated between both side.* *If the TCP/IP stack is configured for modem only operation (PPPMODE parameter) there is no more return codes*
	xx.xx.xx.xx	*IP address attributed to the TCP/IP stack*
	Ok_Info_Ppp	*As soon as the TCP/IP stack software displays this message it is ready to receive commands, PPP protocol is running.*
Error codes in GSM mode	BUSY	*A busy signal is detected on the remote site.* *TCP/IP stack waits for REDIALDELAY seconds and then dials again. This re-dialing will continue until connection success or until the number of call retries defined in parameter REDIALCOUNT has been reached.*
	NO ANSWER	*There is no response from the remote site.* *TCP/IP stack waits for REDIALDELAY seconds and then dials again. This re-dialing will continue until connection success or until the number of call retries defined in parameter REDIALCOUNT has been reached.*
	NO CARRIER	*The modem handshaking process with the remote host is interrupted or unsuccessful.* *TCP/IP stack waits REDIALDELAY seconds and then dials again. This re-dialing will continue until connection success or until the number of call retries defined in parameter REDIALCOUNT has been reached.*
	#CME ERROR : 37120 #CME ERROR : 37121 #CME ERROR : 28980 #CME ERROR : 28981	*The PPP negotiation has failed (check ISPUN, ISPPW and PPPMODE)* (See section ' Response messages and error codes'.)

	#CME ERROR: 35865	*The product is not registered on the network*
	#CME ERROR: 35840	*The product is already running (Host is connected).*
Return codes in GPRS mode	xx.xx.xx.xx	*IP address attributed to the TCP/IP stack*
	Ok_Info_GprsActivation	*GPRS session established and product connected to the Internet*
Error codes in GPRS mode	#CME ERROR: 35866	*All connection attempts will return this message if the GPRS session can not be established*
	#CME ERROR: 35865	*The product is not registered on the network*
	#CME ERROR: 35868	*Aborted GPRS connection, check APN parameters.*

3.3 AT#CONNECTIONSTOP

Target	Dialing features GSM / GPRS connection.
Definition	This command directs the TCP/IP stack to end a PSTN or GSM communication previously established with a connection origination attempt command.
Return codes	OK *The connection session is now ended.*

3.4 AT#DISPLAYIP

Target	General features (GSM and GPRS).	
Definition	This command allows the attached host to view the attributed IP addresses. This command should be issued only once the module as successfully connected to the TCP/IP network.	
GSM mode return messages	MY IP: *x.x.x.x*	*IP address attributed to the TCP/IP stack*
	PEER IP: *x.x.x.x*	*IP address attributed to the PPP peer*
GPRS mode return messages	MY IP: *x.x.x.x*	*IP address attributed to the TCP/IP stack*
	Gateway IP: *x.x.x.x*	*IP address attributed to the PPP peer*
Error codes	#CME ERROR: 35867	*no IP addresses have been attributed: no active connection or PPP/IPCP negotiation not yet completed*

3.5 AT#FTPGET

Target	FTP	
Definition	This command, sent by the attached host, directs the TCP/IP stack to connect to the specified FTP server and to retrieve the specified file from this server. Once the operation is completed, the TCP/IP stack closes the FTP connection. Once an IP link is established, the attached host can retrieve a file from a FTP server at any time (except when the TCP/IP stack software is already in a process using TCP resources). This command is similar to a GET operation (with an automatic connect/disconnect) issued by a standard FTP client on a PC. The TCP/IP stack handles the whole 'FTP get' process by itself.	
Return codes	Ok_Info_DataBegin	*The server is ready to send data to the TCP/IP stack. For the attached host, it notifies the switch from command to data mode.*
	Data	*The data transmitted from the FTP server to the TCP/IP stack is sent over the serial port.*
	<ETX>	*Once the file transfer has finished, the TCP/IP stack sends an ETX character over the serial port to notify the attached host of the end of file transfer : switches from data to command mode*
	OK	*The FTP process was successfully completed.*
	#CME ERROR: 38027	*The address of the FTP server has not been resolved by the secondary DNS server.* *The TCP/IP stack is not able to reach the primary or secondary DNS servers or a wrong FTP server address has been filled in.*
Error codes	#CME ERROR: <value>	*The connection to the FTP server failed.* *(See section ' Response messages and error codes.)* *If an error occurs once the data transfer started, it is preceded by an ETX character*
Note	Each <ETX> character present in the payload data of the FTP flow will be coded by the TCP/IP stack on the serial port as <DLE><ETX>. Each <DLE> character will be coded as <DLE><DLE>. The attached host must then decode the FTP flow to remove these escape characters.	

3.6 AT#FTPPUT

Target	FTP	
Definition	This command sent by the attached host directs the TCP/IP stack to connect to the specified FTP server and to upload the data received on the serial port to the specified file on this server. Once the operation completed, the TCP/IP stack closes the FTP connection. Once an IP link is established, the attached host can send a file to a FTP server at any time (except when the TCP/IP stack software is already in a process using TCP resources). This command is similar to a PUT operation (with an automatic connect/disconnect) issued by a standard FTP client on a PC. The TCP/IP stack handles the global FTP put process by itself	
Return codes	Ok_WaitingForData	*TCP/IP stack is ready to send data from the serial port to the remote FTP server.* *TCP/IP stack then immediately transfers all the data sent by the attached host to the remote FTP server.* ***To notify the TCP/IP stack that all data has been sent, the attached host must send the <ETX> character***
	<ETX>	*Notification from the host for end of data : switches from data mode to command mode*
	OK	*The FTP process was successfully completed.*
	#CME ERROR: 38027	*The address of the FTP server has not been resolved by the secondary DNS server.* *TCP/IP stack is not able to reach the primary or secondary DNS servers or a wrong FTP server address has been filled in.*
Error codes	#CME ERROR: <value>	*The connection to the FTP server failed.* *(See section ' Response messages and error codes'.)* *If an error occurs once the data transfer started, it is preceded by an ETX character*
Note	The TCP/IP stack will only interpret an <ETX> character as the end of the file to be transferred if it's not preceded by a <DLE> character. As a consequence the attached host must send <ETX> characters preceded by <DLE> characters and it must also code <DLE> characters as <DLE><DLE>.	

3.7 AT#GETMAIL

Target	POP3 / Email retrieving	
Definition	This command allows the attached host to direct the TCP/IP stack to retrieve the first mail present in the POP3 server list. Once an IP link is established, the attached host can retrieve an email message at any time (except when the TCP/IP stack software is already in a process using TCP resources). This command is similar to a "check email box" feature issued by a standard messaging client on a PC.	
Return codes	Ok_Info_Mail	*This message is issued when one email message is located in the specified POP3 mailbox.* *Depending on the POP3HEADERMODE parameter, the TCP/IP stack sends the email header over the serial port to the attached host.* *The (CR)(LF)(.)(CR)(LF) sequence finally indicates the end of the email body.*
	Ok_Info_NoMail	*There is no email to retrieve in the POP3 mailbox*
Error codes	#CME ERROR: 38027	*The address of the POP3 server has not been resolved by the secondary DNS server.* *TCP/IP stack is not able to reach the primary and secondary DNS servers or a wrong POP3 server address has been filled in.*
	#CME ERROR: <value>	*An error has occurred during the communication with the remote POP3 server. It may also happen during the data transfer after the MAIL message. In this case it is preceded by a (CR)(LF)(.)(CR)(LF) sequence.* *This error can be due to one of the following reason:* • *the DNS servers are not able to resolve the POP3 server address* • *the POP3 server is temporarily out of service* • *the authentication (POP3UN, POP3PW) is not valid* *(See section ' Response messages and error codes'.)*

3.8 AT#LTCPSTART

Target	socket TCP	
Definition	This command, sent by the attached host, directs the TCP/IP stack to open a listening TCP connection on the specified TCP port. Once an IP link is established, the attached host can open a listening TCP socket at any time (except when the TCP/IP stack software is already in a process using TCP resources). The TCP connection will be active upon reception of a TCP connection request sent by a remote allowed TCP peer (TCPSERV) on the appropriate TCP port (TCPPORT). **Once opened, this TCP connection may be closed by the remote TCP peer or by the attached host which sends an ETX character on the serial port (depending on the DLEMODE parameter).**	
Return codes	Ok_Info_WaitingForData	*This message signals that an allowed remote TCP peer has opened the TCP socket. The TCP connection is now opened.* *All the data from the attached host / remote TCP server is then immediately transferred by the TCP/IP stack to the remote TCP server / attached host.*
	Ok_Info_SocketClosed OK	*The TCP socket is closed*
Error codes	#CME ERROR: <value>	*An error has occurred during the TCP connection. This connection is being closed.* *If this error occurs once the TCP connection opened, it is preceded by an ETX character* *(See section ' Response messages and error codes'.)*
Note	- This command can be aborted before an incoming TCP request has been received by issuing the LTCPSTOP command on the serial port. - Depending on the DLEMODE value, the attached host may close this TCP connection by sending an ETX character. - If the DLEMODE parameter is set to 1, the TCP/IP stack will only interpret an <ETX> character as a close request if a <DLE> character does not precede it. As a consequence the attached host must send <ETX> characters preceded by <DLE> characters and it must also code <DLE> characters in <DLE><DLE>. Similarly, each <ETX> character present in the payload data of the TCP frame will be coded by the TCP/IP stack on the serial port as <DLE><ETX>. Each <DLE> character will be coded as <DLE><DLE>. The attached host must then decode the TCP socket flow to remove these escape characters. - If the DLEMODE parameter is set to 0, the host cannot close the TCP connection. - If the remote TCP server closes the connection, the TCP/IP stack sends an ETX character on the serial port.	

3.9 AT#LTCPSTOP

Target	Socket TCP features
Definition	This command directs the TCP/IP stack to close a TCP listening mode (previously launched by the AT#LTCPSTART command.
Return codes	OK *The local listening port is closed in the TCP/IP stack*

3.10 AT#OTCP

Target	socket TCP	
Definition	This command sent by the attached host directs the TCP/IP stack to open a TCP connection to the specified TCP server. Once an IP link is established, the attached host can open a TCP connection at any time (except when the TCP/IP stack software is already in a process using TCP resources). This TCP connection may be closed by the remote TCP server or by the attached host via sending an ETX character on the serial port (**depending on the DLEMODE parameter**).	
Return codes	Ok_Info_WaitingForData	*This message signals that the TCP socket has been opened.* *All the data from the attached host / remote TCP server is then immediately transferred by the TCP/IP stack to the remote TCP server / attached host.*
	Ok_Info_SocketClosed OK	*The TCP socket is closed*
Error codes	#CME ERROR: 38027	*The address of the FTP server has not been resolved by the secondary DNS server.* *TCP/IP stack is not able to reach the primary and secondary DNS servers or a wrong FTP server address has been filled in.*
	#CME ERROR: <value>	*An error has occurred during the TCP connection. This connection is being closed.* *If this error occurs once the TCP connection opened, it is preceded by an ETX character* *(See section ' Response messages and error codes'.)*
Note	- Depending on the DLEMODE value, the attached host may close this TCP connection by sending an ETX character. - If the DLEMODE parameter is set to 1, the TCP/IP stack will only interpret an <ETX> character as a close request if a <DLE> character does not precede it. As a consequence the attached host must send <ETX> characters preceded by <DLE> characters and it must also code <DLE> characters in <DLE><DLE>. Similarly, each <ETX> character present in the payload data of the TCP frame will be coded by the TCP/IP stack on the serial port as <DLE><ETX>. Each <DLE> character will be coded as <DLE><DLE>. The attached host must then decode the TCP socket flow to remove these escape characters. - If the DLEMODE parameter is set to 0, the host cannot close the TCP connection. - If the remote TCP server closes the connection, the TCP/IP stack sends an ETX	

	character on the serial port.

3.11 AT#PUTMAIL

Target	SMTP / Email Sending	
Definition	This command allows the attached host to send an email message containing body text passed to the TCP/IP stack over the serial port. Once an IP link is established, the attached host can send an email message at any time (except when the TCP/IP stack software is already in a process using TCP resources). The header of this email is built using the REC1, CCREC1 and SUBJ1 parameters. This command is similar to a "send email" operation issued by a standard messaging client on a PC.	
Return codes	Ok_Info_WaitingForData	*A SMTP session has been successfully opened with the remote SMTP server.* *Once the TCP/IP stack has displayed this message, all the data received on the serial port is sent within the email body.* ***The (CR)(LF)(.)(CR)(LF) sequence sent by the attached host indicates the TCP/IP stack the end of the email body.***
	OK	*The mail has been successfully sent*
Error codes	#CME ERROR: 38027	*The address of the SMTP server has not been resolved by the secondary DNS server.* *TCP/IP stack is not able to reach the primary or secondary DNS servers or a wrong SMTP server address has been filled in.*
	#CME ERROR: <value>	*An error has occurred during the communication with the remote SMTP server. It may also happen during the data transfer (after the OK message).* *This error can be due to one of the following reason:* • *the DNS servers are not able to resolve the SMTP server address* • *the SMTP server is temporarily out of service* • *the authentication (SMTPUN, SMTPPW) is not valid* • *an email address specified in REC1 or CCREC1 is not valid* • *there has been an inactivity period of 50 seconds on the serial port* *(See section ' Response messages and error codes'.)*

3.12 AT#SENDMAIL1 / AT#SENDMAIL2 / AT#SENDMAIL3

Target	SMTP / Email Sending	
Definition	This command sends one of the 3 pre-defined email combinations. Once an IP link is established, the attached host can direct the TCP/IP stack to send an email message at any time (except when the TCP/IP stack software is already in a process using TCP resources). The header of this email is built using the REC1/2/3, CCREC1/2/3 and SUBJ1/2/3 parameters while the body is filled in the BODY1/2/3 parameter. This command is similar to a "send email" operation issued by a standard messaging client on a PC.	
Return codes	OK	*The mail has been successfully sent*
Error codes	#CME ERROR: 38027	*The address of the SMTP server has not been resolved by the secondary DNS server.* *TCP/IP stack is not able to reach the primary or secondary DNS servers or a wrong SMTP server address has been filled in.*
	#CME ERROR: <value>	*An error has occurred during the communication with the remote SMTP server. It may also happen during the data transfer (after the OK message).* *This error can be due to one of the following reason:* • *the DNS servers are not able to resolve the SMTP server address* • *the SMTP server is temporarily out of service* • *the authentication (SMTPUN, SMTPPW) is not valid* • *an email address specified in REC1 or CCREC1 is not valid* *(See section ' Response messages and error codes'.)*

3.13 AT#VALL

Target	General configuration
Definition	This command directs the TCP/IP stack to display all of the AT# parameters, together with the software version information and date of generation. The parameters are listed by blocks of categories which are separated by a <CR><LF><CR><LF> sequence.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.14 AT#VDNS

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the DNS servers configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.15 AT#VFTP

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the FTP client configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.16 AT#VGPRS

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the GPRS configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.17 AT#VMAIL1 / AT#VMAIL2 / AT#VMAIL3

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the email combinations configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.18 AT#VPHY

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the physical layer configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.19 AT#VPOP3

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the email retriever configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.20 AT#VPPP

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the PPP layer configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.21 AT#VSMTP

Target	General configuration
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the email sender configuration.
Return code	#Mnemonic: Value *List of parameters with their associated value.* OK

3.22 AT#VSTATE

Target	General configuration	
Definition	This command directs the TCP/IP stack to display the current status of the Wavecom product.	
Return code	#STATE: "IDLE" OK	*Idle state.*
	#STATE: "DIALING" OK	*Originating an outgoing call attempt. (Not yet connected).*
	#STATE: "AUTHENTICATING" OK	*Connection not yet PPP negotiated.*
	#STATE: "CONNECTED" OK	*Internet connection established. (An IP address has been attributed to the TCP/IP stack).*
	#NO SERVICE OK	*No radio network connection made.*
	#STATE: "DISCONNECTING" OK	*In the process of disconnecting from the current communication session.*

3.23 AT#VTCP

Target	General configuration	
Definition	This command directs the TCP/IP stack to display all the AT# parameters related to the TCP socket configuration.	
Return code	#Mnemonic: Value	*List of parameters with their associated value.*
	OK	

3.24 AT#VVERSION

Target	General configuration	
Definition	This command directs the TCP/IP stack to display the software version	
Return code	#VERSION: "<Version name> <Binary file size in bytes> <Date and time of software generation>"	*Version Reference*
	OK	

4 Response messages and error codes.

List of the possible response codes and messages in both numeric and verbose format.

Numeric	Verbose	Description
Standard AT messages		
0	OK	Operation or command success
3	NO CARRIER	No physical layer connection
7	BUSY	Destination busy
8	NO ANSWER	No answer from destination
4	ERROR	Operation or command unsuccessful
2	RING	Incoming call indication
10	CONNECT 300	Physical layer connected at 300 baud
11	CONNECT 1200	Physical layer connected at 1200 baud
12	CONNECT 1200/75	Physical layer connected at 1200/75 baud
13	CONNECT 2400	Physical layer connected at 2400 baud
14	CONNECT 4800	Physical layer connected at 4800 baud
15	CONNECT 9600	Physical layer connected at 9600 baud
16	CONNECT 14400	Physical layer connected at 14400 baud
Information messages		
1025	Ok_Info_DataBegin	Start of data
1028	Ok_Info_WaitingForData	Send data
3074	Ok_Info_SocketClosed	Socket connection closed successfully
3072	Ok_Info_NoMail	No mail to retrieve on server
3073	Ok_Info_Mail	Mail ready to be retrieved on server
3077	Ok_Info_Ppp	PPP connection successful
3086	Ok_Info_GprsActivation	GPRS connection successful

List of the possible response codes with description.

Error codes	
Numeric	Description
34817	Bad command : Unknown command
34819	Bad command : Syntax error
34824	Bad command : EEPROM write failed
34881	Bad command : Command to long

34882	Bad command : Bad command argument value
35840	Physical layer : Modem is already running
35862	Physical layer : Timeout, no activity on network connection
35865	Physical layer : Module is not attached to the network
35866	Physical layer : Invalid event during activation process
35867	Physical layer : Physical layer connection is currently not active
35868	Physical layer : GPRS connection aborted
35869	Physical layer : Invalid incoming call type
35870	Physical layer : Incoming call CLI not provided
36872	SmartStack internal error : internal resource unavailable.
36929	SmartStack : Bad parameter configuration attempt
37120	SmartStack : PPP negotiation failed (client configuration)
37121	SmartStack : PPP negotiation failed (server configuration)
37122	SmartStack : Another internal application is already running
37952	Distant : TCP session closed (TCP Context cancelled)
37964	Distant : No response from server
37966	Distant : TCP session closed by peer (FIN received from peer)
38016	Distant : Open session attempt failed
38017	Distant : Data send attempt failed
38018	Distant : Close session attempt failed
38022	Distant : Change Directory attempt failed
38023	Distant : File deletion attempt failed
38024	Distant : Data retrieve attempt failed
38025	Distant : Email retrieve attempt failed
38026	Distant : Email header receive failed
38027	Distant : No answer from DNS servers or the domain name resolution could not be completed by the server.
38028	Distant : Sender email address rejected by server
38029	Distant : Recipient email address rejected by server
38030	Distant : CC Recipient email address rejected by server
38031	Distant : Email body send request rejected by server
38080	Distant : Username rejected by server
38081	Distant : Password rejected by server
38980	SmartStack : PPP timeout (client configuration)
38981	SmartStack : PPP timeout (server configuration)
49153	Internal error : Open data flow request failed
49154	Internal error : Close data flow request failed
49155	Internal error : Open GPRS session request failed
49156	Internal error : GPRS authentication failed
49157	Internal error : GPRS get IPCP information request failed
49158	Internal error : Open flow confirmation not received
34817	Bad command : Unknown command
34819	Bad command : Syntax error