enfora

Enable Information Anywhere

Application Note
GSM0000AN012

Network Transparency Configuration for PAD

Revision 1.01

Enfora, Inc.
www.enfora.com

Objective:

The intent of this document is to provide appropriate configuration settings for the Enabler-G modem when used on transparent and non-transparent GPRS networks. The Enabler platform is able to automate the appropriate requirements when using the PAD such that programmatic and/or manual intervention is not required.

Overview:

GPRS service providers have two distinct methods of negotiating with mobile devices in order for them to obtain an IP address. This construct is known as transparency. A network is either transparent or non-transparent in architecture. The transparency determines if the mobile platform is required to provide a username and password to successfully connect to the network. A transparent network will not require a username and password, whereas, a non-transparent network will.

Enfora has designed a Packet Assembler/Disassembler (PAD) interface to facilitate connections to platforms that do not have an IP stack. The PAD can be fully automated to provide a network connection upon power up. Please see *GSM0000AN011 - PAD Configuration and Use* for detailed information concerning the PAD.

If the PAD is being used on a non-transparent network, it needs to provide a username and password to properly connect. The module will need to provide the authentication protocol required along with the username and password parameters. The following command provides this capability:

The following command sets the negotiation type.

AT%CGPPP=**<pt>**

<pt>	**0 -** No authentication (ignore login + pwd) **1 -** PAP **2 -** CHAP **3 -** automatic authentication

The following command sets the authentication format and parameters.

AT%CGPCO=**<n>,”<authentication format>”,<cid>**

<n>

0 - Inputs specified in Hexadecimal
1 - Inputs specified in ASCII

<Authentication format>

Authentication format (**ASCII**)**,** **<username>**,**<password>** where

Username: Maximum 16 bytes ASCII string.
Password: Maximum 16 bytes ASCII string.

Authentication format(**Hexadecimal**): **Protocol Configuration Option** specified in Hex value; maximum size is equal to 256 bytes.

<cid>

0 – The new username, password, and protocol type is to be applied to all context Activation.
1 – Context ID zero.
2 – Context ID one.

Example:

ASCII format for all define contexts, username: johndoe, password: tornado.

AT%CGPCO=1,”johndoe,tornado”,0

The %CGPCO command parameters can be provided in both hexadecimal and ASCII formats. The command allows for the simultaneous use of two context activations and unique login parameters for each.

Please check with your network provider to determine the transparency type.

If the PAD is being used on a transparent network, it will function properly without having to be concerned with the username and password.

Revision History

Date	Rev	Author	Description
2/3/03	Draft	Matt Glover	Initial Draft.
9/16/03	1.01	Matt Glover	Removed authentication designation from authentication format string.