AP NOTE 001
Ver.1

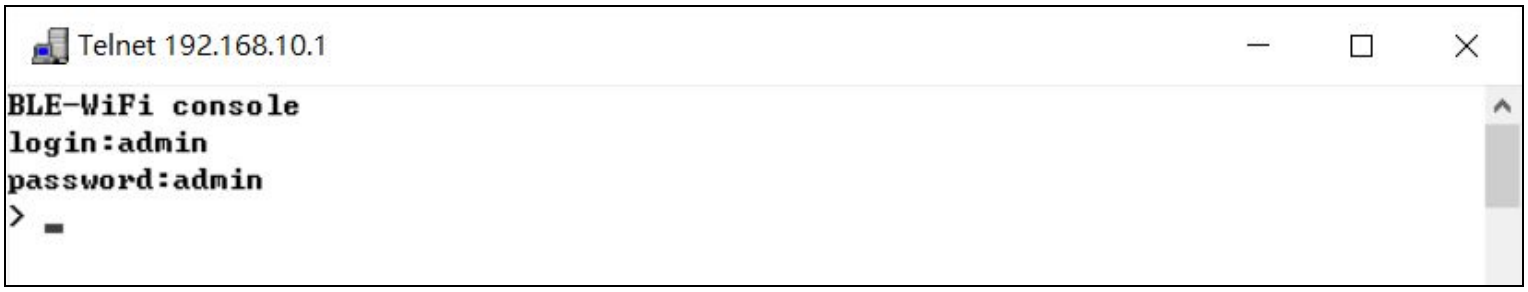
iGS01S Telnet Command

Description

To help user to configure iGS01S in some case that he can't get into webUI, the telnet command is developed. For mass configuration, telnet command is also recommended. PLEASE NOTE, ALL THE CHANGES MADE WILL ONLY BE EFFECTIVE AFTER REBOOT.

Connect

To use telnet command, the device must be connected first. You have to discover the IP address of the iGS01S first. Once you know the IP address, just use any telnet tool, you can telnet into the device. The login account and password is the same with the one you get into the webUI, it is "admin" in default. Below figure is the example



Command set

COMMAND	PROPERTY	VALUE	DEFAULT
WIFI	SCAN		
	MODE	0: AP mode 1: STA mode	0
	APSSID	The AP SSID	BLE-WIFI_XX_XX
	APSECT	The AP security type: OPEN WPA_AES WPA_TKIP WPA2_AES WPA2_TKIP	wpa2_aes
	APSECK	The AP security key	12345678
	APCHNL	The AP channel	6

	STASSID	STA SSID	
	STASECT	STA security type: OPEN WEP_OPEN WEP_SHARED WPA_AES WPA_TKIP WPA2_AES WPA2_TKIP WPA2_MIXED	
	STASECK	STA security key	
	STAWEPK	STA wep key	
DHCP	ENABLE	0: Disable 1: Enable	1
	IPADDR	Static IP setting	192.168.0.100
	NETMASK	Static netmask setting	255.255.255.0
	GATEWAY	Static gateway setting	192.168.0.255
	DNS	Static DNS setting	8.8.8.8
DHCPD	IPADDR	DHCP server IP	192.168.10.1
	NETMASK	DHCP server netmask	255.255.255.0
TCPSRV	PORT	M2M TCP server listen port	8080
TCPCLI	HOST	M2M TCP client target host	
	PORT	M2M TCP client target port	8080
HTTP	HOST	HTTP server host	
	PORT	HTTP server port	80
	URLPATH	URL path	
	USERNAME	Username for basic auth	
	PASSWORD	Password for basic auth	
	EXTRAHDR	Extra header field name	
	EXTRAVAL	Extra header field value	
	KEEPALIVE	Enable/disable http keepalive	1
	HTTPS	Force using https on non-standard port	0
MQTT	HOST	MQTT server host	
	PORT	MQTT server port	1883
	PUBTOPIC	MQTT Publish Topic	
	CLIENTID	MQTT client ID setting	
	USERNAME	MQTT username	

	PASSWORD	MQTT password	
	VERSION	0: mqtt-3.1 1: mqtt-3.1.1	1
	MQTTS	0: Disable 1: enable mqtts	0
	ROOTCA	0: No CA 1: AWS-IOT 2: Azure-IOT	0
	USECERT	0: Disable 1: Use cert/key	0
SYS	INFO	Show system firmware information	
	DUMP	Dump all settings	
	ECHO		
	WORKMODE	0: M2M server 1: M2M client 2: HTTP 3: MQTT	0
	USERNAME	System login username	admin
	PASSWORD	System login password	admin
	THROTTLE	Enable throttle to filter out duplicated MAC in cache. (apply to http only)	0
	REQINTVL	The send request interval, if 0 send request immediately. (apply to http only, need THROTTLE enable to work)	0
	FULLDROP	Drop input data if cache full before reaching request interval	0
	AUTORESET	reset timeout:HH MM (0: disable) valid range is 0 ~ 49 days	0
	BROADCAST	<interval(ms)> <timeout(ms)> <payload>	
	RSSITHR	0 ~ -127	-100
	GPRPWL	<mask> <pattern>	
	GPRPWL2	<mask> <pattern>	
	NSLOOKUP	DNS lookup for a given hostname	
	PING	Ping a given IP	
	HEARTBEAT	Send heartbeat report periodically	0
	ACTSCAN	0: Disable 1: Enable Will report RSRP if enabled.	0
	MSTIME	Enable timestamp in millisecond (when NTP	0

		enabled)	
	FORMATSEL	0: plain-text 1: json format	0
	BLEMACWL	BLE MAC whitelist (allow set 10 sets) <index> <mac> E.g. > SYS BLEMACWL 1 C5A369551012 To clear the setting: > SYS BLEMACWL 1 ""	
	STRICTMODE	Enable strictly error detection	0
	ACTIVEPING	Enable regularly ping GW to detect networking issue To ping GW per minute: > SYS ACTIVEPING 1	0
	OTA	Support fetching firmware via http for OTA: > SYS OTA FS <url_for_fs_image> <md5sum> > SYS OTA APP <url_for_app_image> <md5sum> > SYS OTA START	
NTP	ENABLE	Enable/disable NTP	0
	SERVER	NTP server	pool.ntp.org
	SYNCINTVL	Sync interval in seconds	86400 (1day)
REBOOT		0: reboot 1: reboot to default setting 2: reboot to OTA mode 3: reboot to WPS mode	
EXIT			

Examples

Join Access Point	
	WIFI MODE 1
	WIFI STASSID YOUR_AP
	WIFI STASECT wpa2_mixed
	WIFI STASECK 12345678
Set as M2M server	
	SYS WORKMODE 0
	TCPSRV 8080
Set as M2M client	
	SYS WORKMODE 1
	TCPCLI HOST 192.168.0.123

	TCPCLI PORT 8080
Set as HTTP client	
	SYS WORKMODE 2
	HTTP HOST test
	HTTP PORT 80
	HTTP URLPATH /api/test/endpoint
Set as MQTT client	
	SYS WORKMODE 3
	MQTT HOST iot.eclipse.org
	MQTT PORT 1883
	MQTT PUBTOPIC my/test/pub/topic

The following is an example to configure an iGS01(in default AP mode) as a HTTPS client connecting to a HTTPS server called “YOUR_HTTPS”.

WIFI STASSID YOUR_AP

WIFI STASECT wpa2_aes

WIFI STASECK your_ap_password

WIFI MODE 1

HTTP HOST YOUR_HTTPS

HTTP PORT 443

HTTP URLPATH /api/gwpost/igs01s_xx_xx

SYS WORKMODE 2

REBOOT

Revision History

DATE	REVISION	CHANGES
Apr 16, 2018	1	Initial release