Guide
Ver 1.5

iGS03 Telnet Command

Scope of the Document

This document presents the telnet command set for iGS03 serials which includes the following variants:

1. IGS03M: The LTE model
2. IGS03W: The WiFi model
3. IGS03E: The Ethernet Model

PLEASE NOTE, MOST OF THE CHANGES MADE WILL ONLY BE EFFECTIVE AFTER REBOOT.

Command Syntax

Basic syntax

These commands have the format of “COMMAND” or “COMMAND ARG”.

The “COMMAND” without any argument means reading settings.

The “COMMAND ARG” format means setting ARG for this command setting.

Extended syntax

One of the extended formats is “ COMMAND INDEX ARG” for setting ARG to the given index.

Some action commands may have different arguments which are documented in the command description.

Connect to device

To use telnet command, the device must be connected first. You have to discover the IP address of the iGS03 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

System command set

Command	Description	Default
SYS INFO	Summary of device firmware version/MAC/IP information	
SYS DUMP	List of all device settings (Mainly for diagnostic and sending bug report)	
SYS NSLOOKUP <target host>	Query Internet name servers > SYS NSLOOKUP www.google.com	
SYS PING <target ip>	Send ICMP ECHO_REQUEST to network hosts > SYS PING 8.8.8.8	
SYS OTA <act> <arg>	This command is used for updating firmware. Config to fetch resource file: > SYS OTA RES https://url/res.bin Config to fetch application file: > SYS OTA APP https://url/app.bin To start OTA, the device will reboot to new firmware automatically. > SYS OTA START To start OTA and reset default, device will reboot to new firmware automatically and reset default settings. > SYS OTA START_RESET Since v1.0.6.0+, the “SYS OTA START” command will automatically check the latest firmware release. If a new firmware version is found, it will start upgrading.	
SYS WORKMODE <mode>	<mode> Config the system working mode: 0: TCP server mode 1: TCP client mode 2: HTTP client mode 3: MQTT client mode	0
SYS USERNAME <user>	<user> Username for login device	admin
SYS PASSWORD <pass>	<pass> Password for login device	admin
SYS CACHEFULLOPT <opt>	<opt> 0: Immediately send data if cache full 1: Discard new input data if cache full	0

SYS THROTTLE <en>	<en> 0: Disable throttling 1: Enable throttling Enable throttle to filter out duplicate MAC in cache. Also needs a request interval (REQINTVL) to make this function work.	0
SYS THROTTLE_MASK <mask> (v1.1.8.0+)	<mask> 0: Apply throttle to all reports BIT(0): 1 Excluding GPRP report BIT(1): 2: Excluding RSPR report BIT(3): 8 Excluding LRAD report BIT(4): 16 Excluding LRSR report BIT(5): 32 Excluding 1MAD report BIT(6): 64 Excluding 1MSR report BIT(9): 512: Excluding GPSR report If the bitmap is set, the corresponding report type will not apply to throttle logic.	0
SYS TIMESTAMP <opt>	<opt> 0: No timestamp 1: Append timestamp in second 2: Append timestamp in millisecond	0
SYS REQINTVL <interval>	<interval> in seconds 0: Upload data immediately > 0: Upload data in specific request interval timeout	0
SYS CTRLHOST <host>	<host> The control server the device will connect to and allow sending commands from the server. If not set, the device will not connect to the control server.	
SYS CTRLPORT <port>	<port> The control server listen port	
SYS AUTORESET <timeout>	<timeout> in minutes 0: Disable Set auto reboot in specific timeout	0
SYS HEARTBEAT <interval>	<interval> in minutes 0: Disable Send heartbeat report in specific interval	0
SYS HBRP_FMT <fmt>	<fmt> heartbeat payload format 0: Default 1: IP address in ASCII 2: IP address in HEX	0
SYS JSON_PREFIX <prefix>	<prefix> The prefix used in JSON format output	{"data": [
SYS JSON_SUFFIX <suffix>	<suffix>	]}

	The suffix used in JSON format output	
SYS CLIENT_CERT	The client certificate To fetch certificate file from a http server: > SYS CLIENT_CERT GET http://xxx.xxx.xxx/cert.pem	
SYS CLIENT_KEY	The client key To fetch key file from a http server: > SYS CLIENT_KEY GET http://xxx.xxx.xxx/cert.pem	
SYS SERVER_CERT	The server certificate To fetch certificate file from a http server: > SYS SERVER_CERT GET http://xxx.xxx.xxx/ca.pem	
SYS LOCK <en>	<en> 0: Unlock 1: Disable local network configuration interface Once lock is set, it requires reset default to re-configure the device.	0
SYS ECHO <arg>	<arg> Send back <arg>	
SYS SYSLOG	Show runtime errors for diagnostics	

BLE command set

Command	Description	Default
BLE PHYMODE <mode>	<mode> 1: LE 1M PHY 2: LE Coded PHY	1
BLE ACTSCAN <en>	<en> 0: Disable active scan 1: Enable active scan If ACTSCAN is set: In LE 1M PHY mode, will receive a scan response “$RSPR” report. In LE Coded PHY mode, will receive a long range scan response “$LRSR” report.	0
BLE RSSITHR <threshold>	<threshold> (0 ~ -127) BLE RSSI threshold	-100
BLE MAXRSSITHR <max_threshold>	<max_threshold> (0 ~ -127) BLE Maximum RSSI threshold	0

(v2.0.0+)		
BLE TYPEMASK <mask>	<mask> BLE report type mask BIT(0): GPRP BIT(1): RSPR BIT(3): LRAD BIT(4): LRSR BIT(5): 1MAD BIT(6): 1MSR If the bitmap is set, the corresponding report type will be filtered out.	0
BLE MACWL <idx> <mac>	BLE MAC whitelist <idx> 1 ~ 10 <mac> The beacon BLE MAC To set MAC F83B3148264D as first whitelist: > BLE MACWL 1 F83B3148264D To clear index 1 of mac whitelist: > BLE MACWL 1 ""	
BLE PAYLOADWL <idx> <pattern>	BLE payload whitelist <idx> 1 ~ 6 <pattern> The BLE payload pattern to match To set payload whitelist for index 1: > BLE PAYLOADWL 1 02010612XXXX0080BC260100 Note, the XXXX means don't care about fields. To clear payload whitelist for index 1: > BLE PAYLOADWL 1 ""	
BLE CMASK <mask> (v1.0.6.0+ & BT_FW: v1.0.2+)	<mask> If the corresponding bit is set, it means mask the channel accordingly. BIT(0): ch37 BIT(1): ch38 BIT(2): ch39 i.e. > BLE CMASK 0 // Default, enable all > BLE CMASK 3 // ch39 only (disable 37,38) > BLE CMASK 5 // ch38 only (disable 37,39) > BLE CMASK 6 // ch37 only (disable 38,39)	0

DHCP command set

Command	Description	Default
DHCP ENABLE <en>	<en> Enable DHCP client 0: Disable DHCP 1: Enable DHCP The user needs to config IPADDR/NETMASK/GATEWAY/DNS settings if DHCP is disabled.	1
DHCP IPADDR <ip>	<ip> The static IP address when DHCP is disabled	
DHCP NETMASK <nm>	<nm> The netmask IP when DHCP is disabled	
DHCP GATEWAY <gw>	<gw> The gateway IP when DHCP is disabled	
DHCP DNS1 <dns>	<dns> The primary DNS server when DHCP is disabled	
DHCP DNS2 <dns>	<dns> The secondary DNS server when DHCP is disabled	

DHCPD command set

Command	Description	Default
DHCPD IPADDR <ip>	<ip> The IP address when device is running ad dhcp server in AP mode	192.168.10.1
DHCPD NETMASK <nm>	<nm> The netmask when device is running ad dhcp server in AP mode	255.255.255.0

NTP command set

Command	Description	Default
NTP ENABLE <en>	<en> Enable NTP sync 0: Disable 1: Enable	1
NTP SERVER <srv>	<srv> NTP server	pool.ntp.org
NTP SYNCINTVL <interval>	<interval> NTP sync interval in seconds	86400

HTTP command set

Command	Description	Default
HTTP URL <url>	<url> The URL for uploading data	
HTTP HDR <hdr>	<hdr> The additional http header to send	
HTTP HDRVAL <val>	<val> The additional http header value to send	
HTTP FORMAT <fmt>	<fmt> 0: plain-text 1: JSON 2: Decoded JSON (v1.1.0.0+)	0
HTTP KEEPALIVE <en>	<en> 0: Disable http keepalive 1: Enable http keepalive	1
HTTP ROOTCA <ca>	<ca> 0: NONE 1: AWS-IoT 2: AZURE-IoT	0

	3: Google-IoT 4: User uploaded CA	
HTTP USECERT <en>	<en> 0: Disable loading certificate 1: Enable loading certificate	

MQTT command set

Command	Description	Default
MQTT HOST <host>	<host> The MQTT broker host	
MQTT PORT <port>	<port> The MQTT broker listen port	
MQTT USERNAME <user>	<user> Username to be used for authenticating with the broker	
MQTT PASSWORD <pass>	<pass> Password to be used for authenticating with the broker	
MQTT CLIENTID <id>	<id> The id to use for this client. If not given, the system will generate a random id.	
MQTT PUBTOPIC <topic>	<topic> Mqtt publish topic	
MQTT TLS <tls>	<tls> 0: Disable TLS 1: Enable TLS	0
MQTT ROOTCA <ca>	<ca> 0: NONE 1: AWS-IoT 2: AZURE-IoT 3: Google-IoT 4: User uploaded CA	0
MQTT USECERT <en>	<en> 0: Disable 1: Enable	
MQTT FORMAT <fmt>	<fmt> 0: Plain-text 1: JSON 2: Decoded JSON (v1.1.0.0+)	

MQTT KEEPALIVE <sec>	<sec> MQTT keep alive time interval in seconds.	120
MQTT QOS <qos>	<qos> 0: QoS 0 1: QoS 1 2: QoS 2	0
MQTT VERSION <ver>	<ver> 0: MQTT-3.1 1: MQTT-3.1.1	1
MQTT BULKMODE <en> (v1.0.6.0+)	<en> Support publish multiple entries with one publish request 0: Disable 1: Enable	

TCPCLI command set

Command	Description	Default
TCPCLI HOST <host>	<host> TCP client target host	
TCPCLI PORT <port>	<port> TCP client target port	8080

TCPSRV command set

Command	Description	Default
TCPSRV PORT <port>	<port> TCP server listen port	8080

WiFi command set

Command	Description	Default
WIFI SCAN	Scan nearby AP	
WIFI DISABLE	0: Enable wifi 1: Disable wifi	0

	(Only available for iGS03M)	
WIFI MODE <mode>	<mode> 1: STA mode 2: AP mode	2
WIFI AP_SSID <ssid>	<ssid> The SSID when device is running in AP mode	
WIFI AP_PASSWORD <pwd>	<pwd> The AP password when device is running in AP mode	12345678
WIFI AP_CHANNEL <ch>	<ch> The AP channel	6
WIFI AP_AUTHMODE <auth>	<auth> The AP authenticate mode 0: Open 2: WPA_PSK 3: WPA2_PSK 4: WPA_WPA2_PSK	3
WIFI STA_SSID <ssid>	<ssid> The target AP SSID when device is running in STA mode	
WIFI STA_PASSWORD <pwd>	<pwd> The target AP password when device is running in STA mode	
WIFI STA_AUTHMODE <auth>	<auth> The target AP authenticate mode 0: Open 1: WEP 2: WPA_PSK 3: WPA2_PSK 4: WPA_WPA2_PSK 5: WPA2_ENTERPRISE 6: WPA3_PSK 7: WPA2_WPA3_PSK	
WIFI EAP_TYPE <type>	<type> 0: EAP-TLS 1: EAP-PEAP (PEAP-MSCHAPv2 only) 2: EAP-TTLS (TTLS-MSCHAPv2 only)	
WIFI EAP_ID <id>	<id> EAP identity	anonymous
WIFI EAP_USERNAME <user>	<user> The username used by EAP-PEAP / EAP-TTLS.	
WIFI EAP_PASSWORD <pass>	<pass> The password used by EAP-PEAP/ EAP-TTLS.	
WIFI WPA2_ENT_CA	The WPA2 CA certificate	

	To fetch CA certificate file from a http server: > WIFI WPA2_ENT_CA GET http://xxx.xxx.xxx/ca.pem	
WIFI WPA2_ENT_CERT	The WPA2 user certificate (For EAP-TLS) To fetch certificate file from a http server: > WIFI WPA2_ENT_CERT GET http://xxx.xxx.xxx/cert.pem	
WIFI WPA2_ENT_KEY	The WPA2 private key (For EAP-TLS) To fetch private key file from a http server: > WIFI WPA2_ENT_KEY GET http://xxx.xxx.xxx/key.pem	

LTE command set (IGS03M)

Command	Description	Default
LTE INFO	Summary of LTE module information	
LTE LOG	LTE AT commands log	
LTE APN <apn>	<apn> LTE APN setting	internet.iot
LTE AUTHTYPE <auth>	<auth> 0: NONE 1: PAP 2: CHAP	0
LTE USERNAME <user>	<user> username	
LTE PASSWORD <pass>	<pass> password	
LTE DNS1 <dns>	<dns> The primary DNS (If not set, use the DNS provided by peer)	
LTE DNS2 <dns>	<dns> The secondary DNS (If not set, use the DNS provided by peer)	

GNSS command set (IGS03M)

Command	Description	Default
GNSS INFO	Summary of current position information	

GNSS NMEA	NMEA information	
GNSS STATS	NMEA statistics	
GNSS ENABLE <en>	<en> 0: Disable 1: Enable	0
GNSS FIXCOUNT <count>	<count> Number of attempts for positioning. 0 indicates continuous positioning. Non-zero values indicate the actual number of attempts for positioning.	0
GNSS FIXRATE <rate>	<rate> Unit: s. the interval time between the first and second time positioning.	1
GNSS RPTRATE <rate>	<rate> Unit: s. the report interval time.	600
GNSS FIXMAXTIME <time>	<time> Unit: s. The maximum positioning time. which indicate the response time of GNSS receiver while measuring the GNSS pseudo range, and the upper time limit of GNSS satellite searching. It also includes the time for demodulating the ephemeris data and calculating the position.	240
GNSS FIXMAXDIST <dist>	<dist> Unit: m. Accuracy threshold of positioning.	50

Misc commands

Command	Description	Default
REBOOT <opt>	Make device reboot <opt> DEFAULT: Reboot to default settings WPS: Reboot to start WPS enrollee	
EXIT	Exit the telnet session	

Command Return Result code

Return Result	Description	
0	Success	
1	Insufficient arguments	

2	Invalid argument	
3	Unknown command	
4	Execution error	
5	Command not supported	
6	Out of memory	
7	Forbidden	

Revision History

DATE	REVISION	CHANGES
Apr 15, 2020	1	Initial release
Nov 17, 2020	1.1	Add SYS SYSLOG command Add 1MAD, 1MSR for BLE TYPEMASK command
Apr 14, 2021	1.2	Add MQTT BULKMODE command Add BLE CMASK command Update SYS OTA START command
Dec 8, 2021	1.3	Add new json format for HTTP & MQTT
May 24, 2023	1.4	Add SYS THROTTLE_MASK command
Jun 19, 2025	1.5	Add BLE MAXRSSITHR command