『monoコネクト』

管理者マニュアル

Ver.1.2

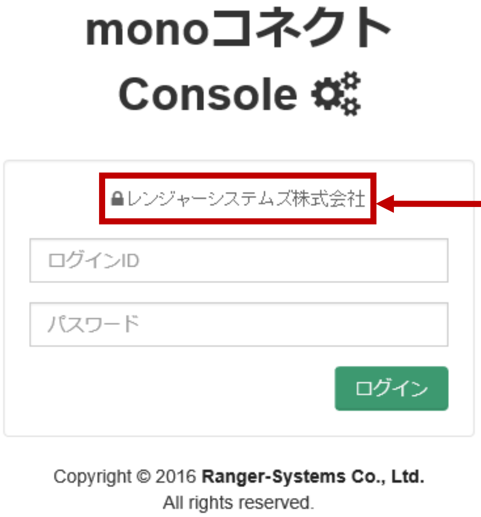
目次

改訂履歴

改訂日	版数	変更箇所	変更内容
2017/6/9	初版	-	-
2018/4/26	1.1	5-2.　iGS02 コマンド一覧	新規追加
2020/7/15	1.2	5-2．iGS01S コマンド一覧 5-3.　iGS02 コマンド一覧 5-4．iGS03 コマンド一覧 5-5．コマンド実行例	新規追加 項番修正

1. ログイン

弊社よりお伝えしている**「ログインURL」**より、**ログインID**と**パスワード**を入力し、ログインします。



monoコネクト
Console

レンジャーシステムズ株式会社

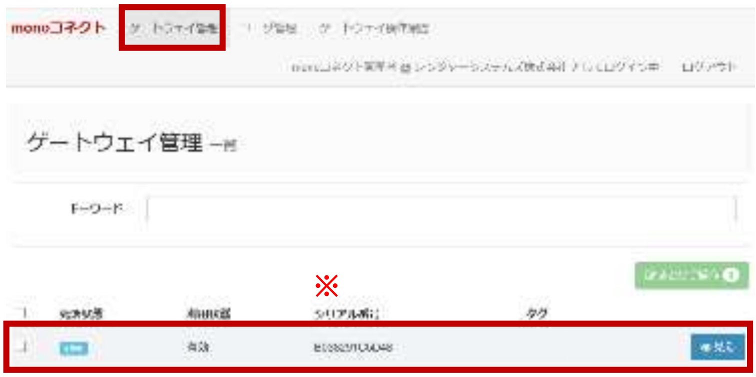
Copyright © 2016 **Ranger-Systems Co., Ltd.**
All rights reserved.

貴社名になっていることをご確認ください。

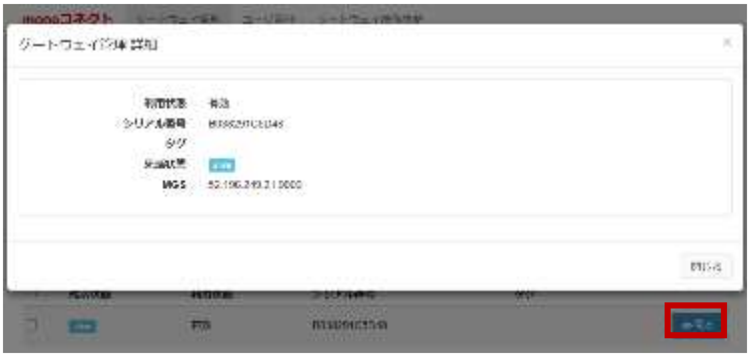
※ログインURL、ID、パスワードを忘れた場合は、弊社までご連絡ください。

2．ゲートウェイ管理

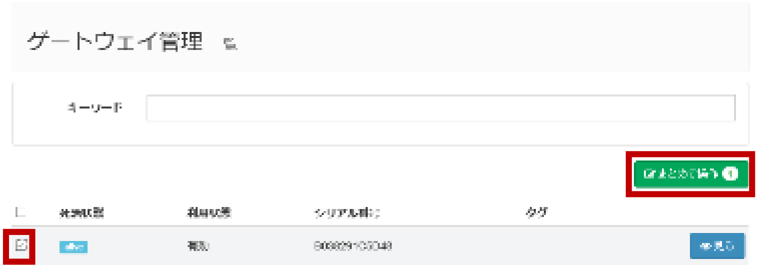
2-1．ご利用するゲートウェイを登録します。



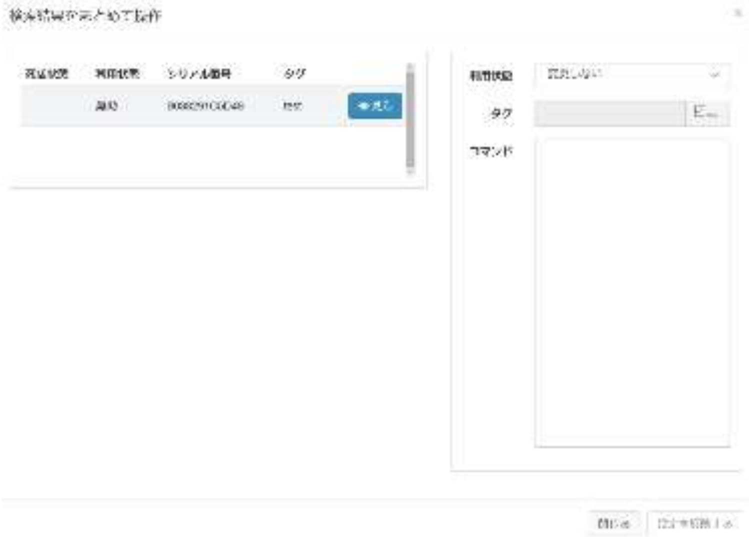
2-1-1.
「ゲートウェイ管理」を選択
登録されているゲートウェイの情報が表示されます。
※
「シリアル番号」の欄には、ゲートウェイのWiFi側MACアドレスが表示されます。



2-1-2.
「見る」を選択するとゲートウェイの詳細が確認できます。



2-1-3.
ゲートウェイごとのチェックボックスに☑を入れた後、「まとめて操作」を選択すると、ゲートウェイごとにコマンド設定などを実施することができます。

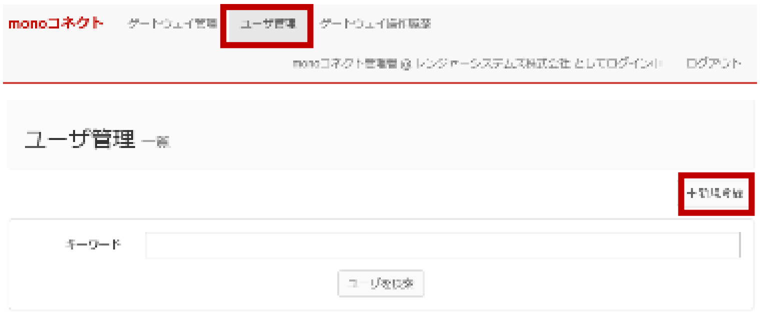


2-1-4.
画面左側に設定対象となるゲートウェイが表示されます。画面右側に「利用状態」、「タグ」、「コマンド」の設定画面が表示されます。

【利用状態】
ゲートウェイの有効・無効が設定できます。
無効にすると利用状態の変更が行われなくなります。
【タグ】
任意のタグが入力できます。
【コマンド】
巻末のコマンドリファレンスを参照ください。

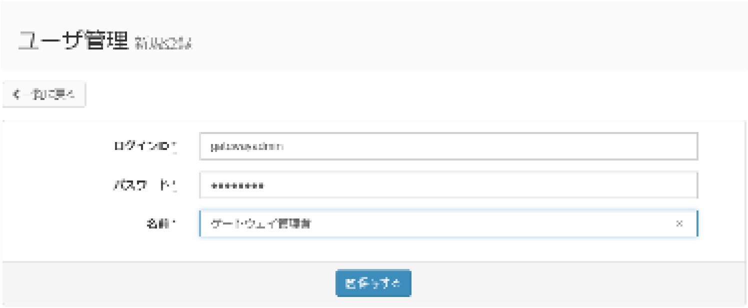
3. ユーザ管理

3-1. 管理画面へのユーザアカウントを登録します。



3-1-1.

「ユーザ管理」>「新規登録」を選択



ログインID * gatewayadmin

パスワード * *********

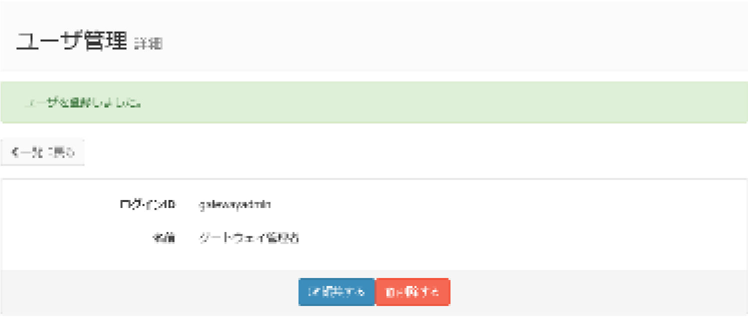
名前 * ゲートウェイ管理者

3-1-2.

【ログインID】
ログイン用IDを入力してください

【パスワード】
ログイン用パスワードを入力してください

【名前】
管理者の名前を入力してください。



ユーザを登録しました。

ログインID gatewayadmin

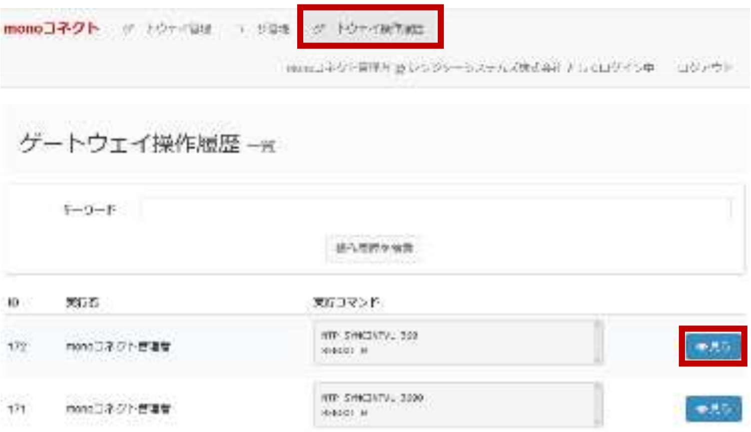
名前 ゲートウェイ管理者

3-1-3.

続けて登録するには「一覧に戻る」を選択

4．ゲートウェイ操作履歴

4-1．ゲートウェイの操作履歴確認



monoコネクト　ゲートウェイ管理　タグ管理　ゲートウェイ操作履歴

monoコネクト管理者 @レンジャーシステムズ株式会社 としてログイン中　ログアウト

ゲートウェイ操作履歴 一覧

キーワード

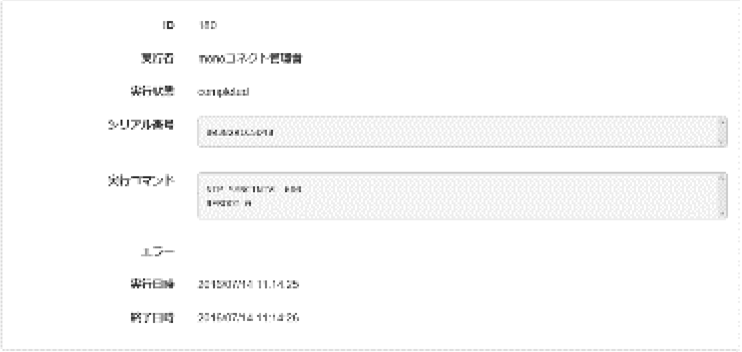
操作履歴を検索

ID	実行者	実行コマンド	
172	monoコネクト管理者	NTP SYNCINTVL 300 REBOOT 0	見る
171	monoコネクト管理者	NTP SYNCINTVL 3000 REBOOT 0	見る

4-1-1.

「ゲートウェイ操作履歴」を選択
「ゲートウェイ管理画面」で、今までに実行したコマンド履歴を確認することができます。
なお、「利用状態」、「タグ」の操作履歴は表示されません。

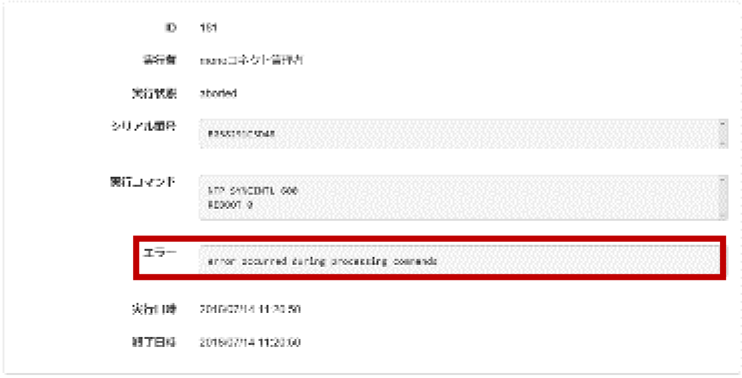
「見る」を選択すると、実行したコマンドの詳細を確認することができます。



ID	180
実行者	monoコネクト管理者
実行状態	completed
シリアル番号	[illegible]
実行コマンド	NTP SYNCINTVL 600 REBOOT 0
エラー	
実行日時	2016/07/14 11:14:25
終了日時	2016/07/14 11:14:26

4-1-2.

実行コマンドの詳細を表示させることができます。
正常にコマンドが実行された場合、「エラー」欄には何も表示されません。



ID	181
実行者	monoコネクト管理者
実行状態	aborted
シリアル番号	[illegible]
実行コマンド	NTP SYNCINTVL 600 REBOOT 0
エラー	error occurred during processing commands
実行日時	2016/07/14 11:20:50
終了日時	2016/07/14 11:20:00

4-1-3.

正常にコマンドが実行されなかった場合、左図の通り「エラー」欄にエラーが発生した旨、表示されます。

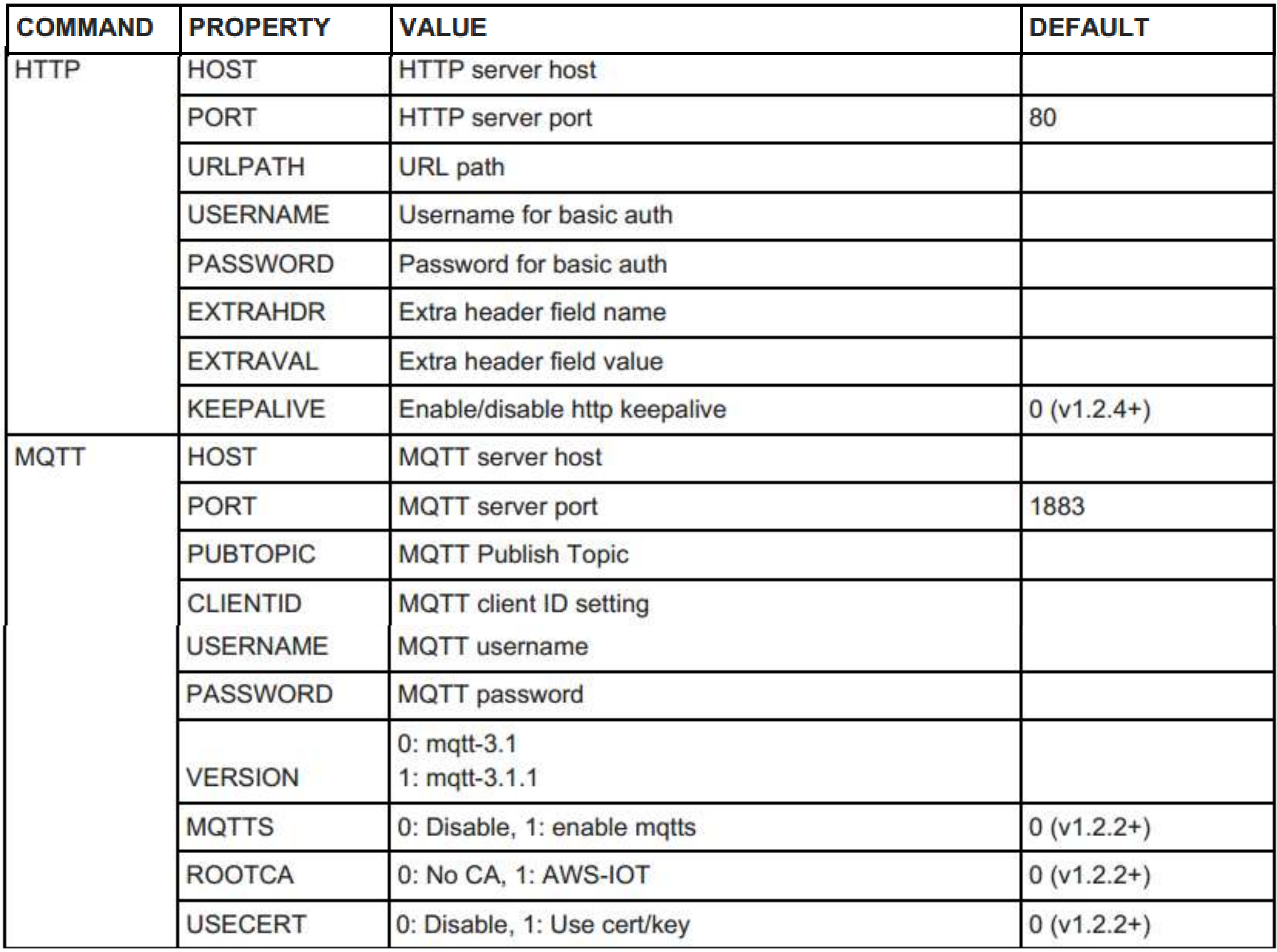
5．コマンドリファレンス

5-1．iGS01 コマンド一覧

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

5．コマンドリファレンス

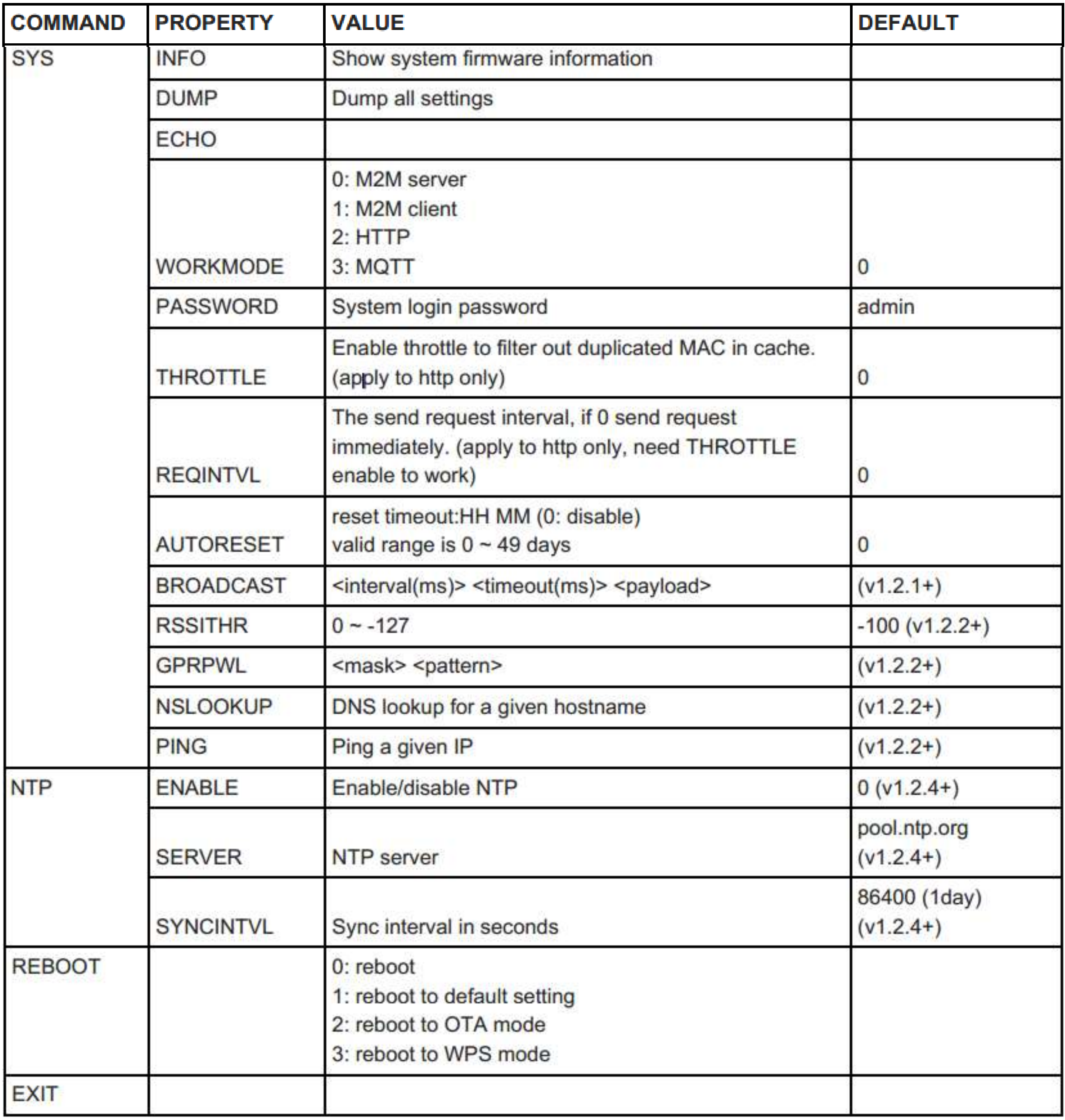
5-1．iGS01 コマンド一覧



COMMAND	PROPERTY	VALUE	DEFAULT
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	0 (v1.2.4+)
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	
	MQTTS	0: Disable, 1: enable mqtts	0 (v1.2.2+)
	ROOTCA	0: No CA, 1: AWS-IOT	0 (v1.2.2+)
	USECERT	0: Disable, 1: Use cert/key	0 (v1.2.2+)

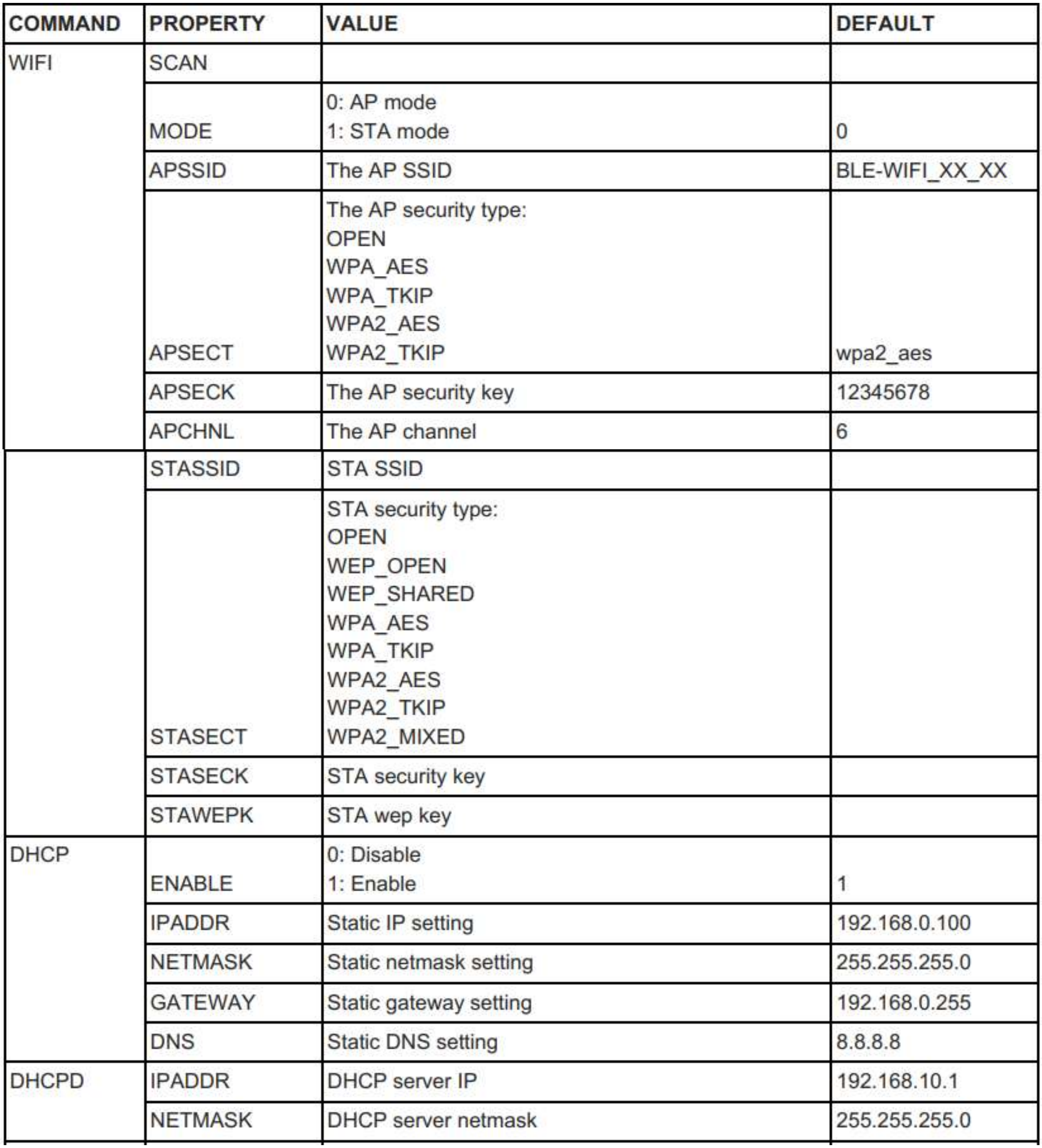
5. コマンドリファレンス

5-1. iGS01 コマンド一覧

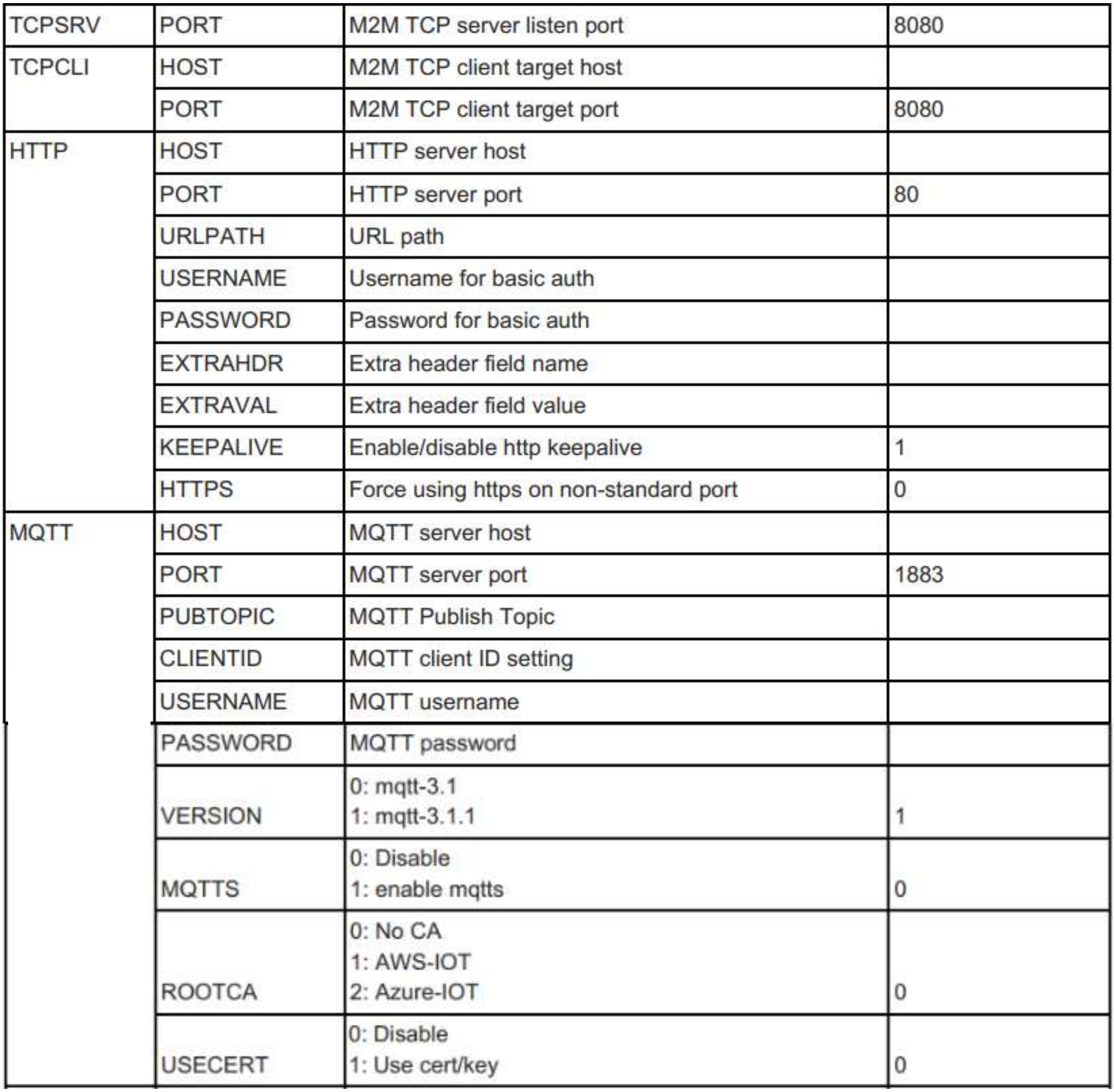


COMMAND	PROPERTY	VALUE	DEFAULT
SYS	INFO	Show system firmware information	
	DUMP	Dump all settings	
	ECHO		
	WORKMODE	0: M2M server 1: M2M client 2: HTTP 3: MQTT	0
	PASSWORD	System login password	admin
	THROTTLE	Enable throttle to filter out duplicated MAC in cache. (apply to http only)	0
	REQINTVL	The send request interval, if 0 send request immediately. (apply to http only, need THROTTLE enable to work)	0
	AUTORESET	reset timeout:HH MM (0: disable) valid range is 0 ~ 49 days	0
	BROADCAST	<interval(ms)> <timeout(ms)> <payload>	(v1.2.1+)
	RSSITHR	0 ~ -127	-100 (v1.2.2+)
	GPRPWL	<mask> <pattern>	(v1.2.2+)
	NSLOOKUP	DNS lookup for a given hostname	(v1.2.2+)
	PING	Ping a given IP	(v1.2.2+)
NTP	ENABLE	Enable/disable NTP	0 (v1.2.4+)
	SERVER	NTP server	pool.ntp.org (v1.2.4+)
	SYNCINTVL	Sync interval in seconds	86400 (1day) (v1.2.4+)
REBOOT		0: reboot 1: reboot to default setting 2: reboot to OTA mode 3: reboot to WPS mode	
EXIT			

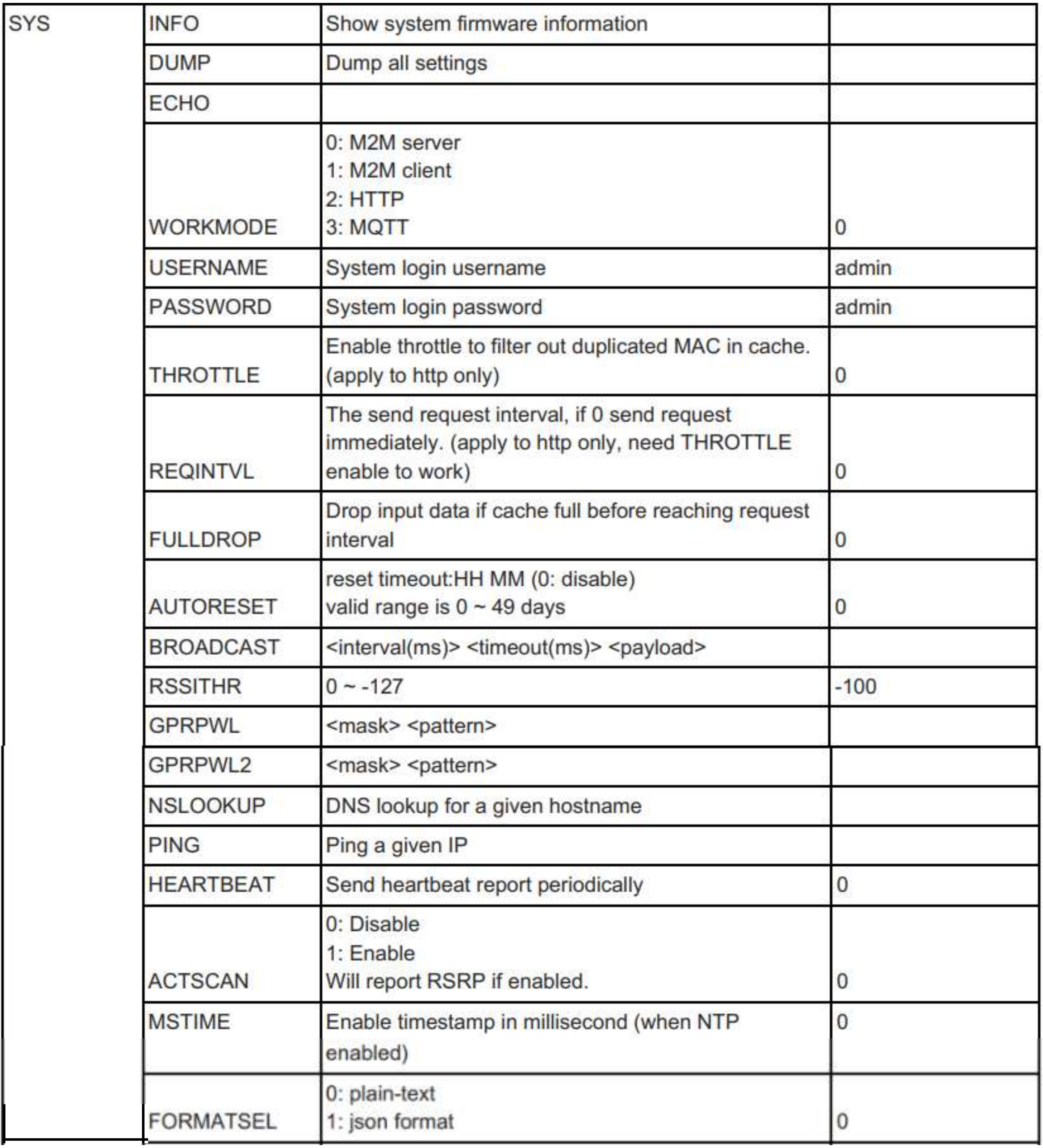
5-2. iGS01S コマンド一覧



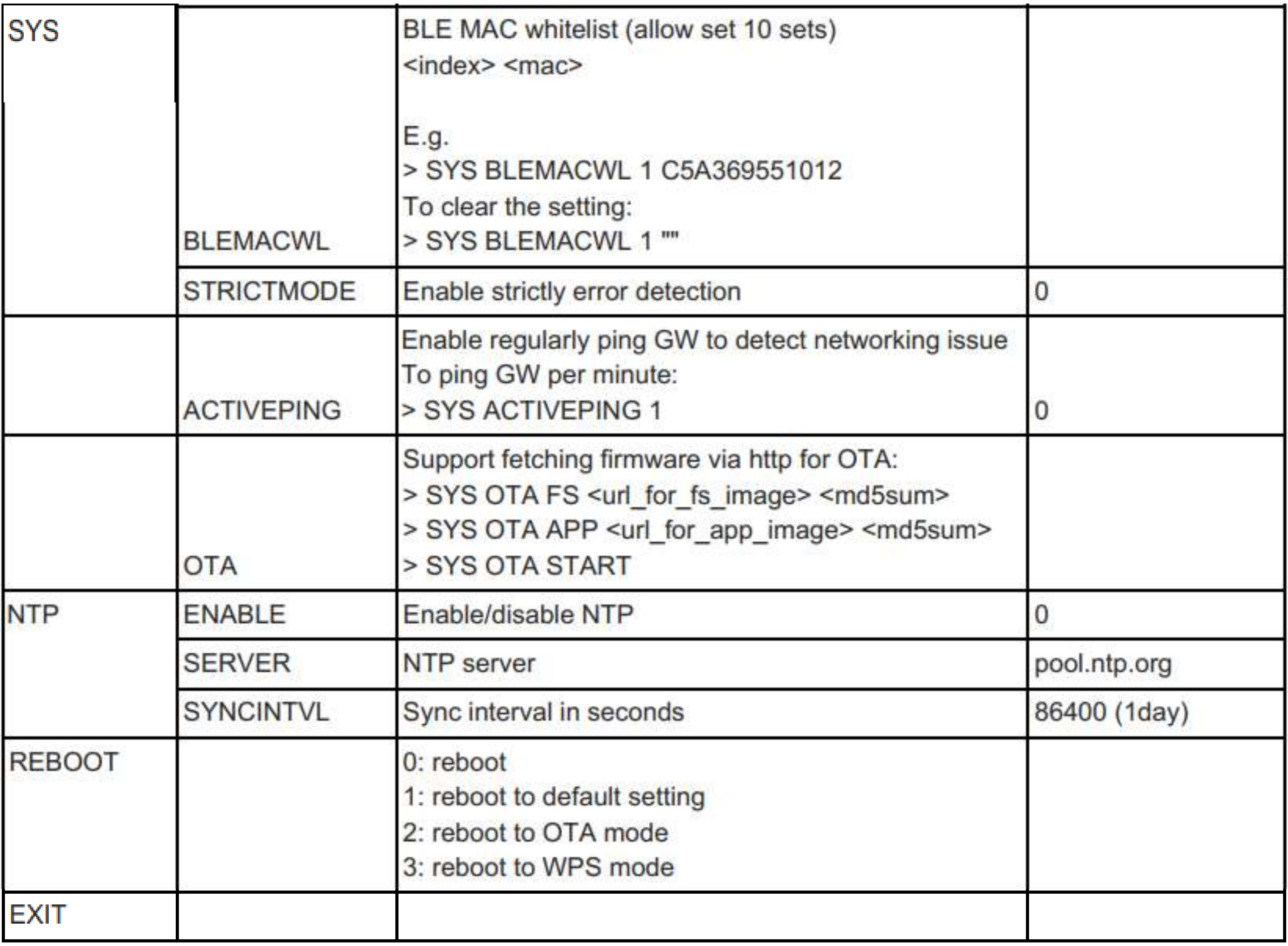
COMMAND	PROPERTY	VALUE	DEFAULT
WIFI	SCAN		
	MODE	0: AP mode 1: STA mode	0
	APSSID	The AP SSID	BLE-WIFI_XX_XX
	APSECT	The AP security type: OPEN WPA_AES WPA_TKIP WPA2_AES WPA2_TKIP	wpa2_aes
	APSECK	The AP security key	12345678
	APCHNL	The AP channel	6
	STASSID	STA SSID	
	STASECT	STA security type: OPEN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



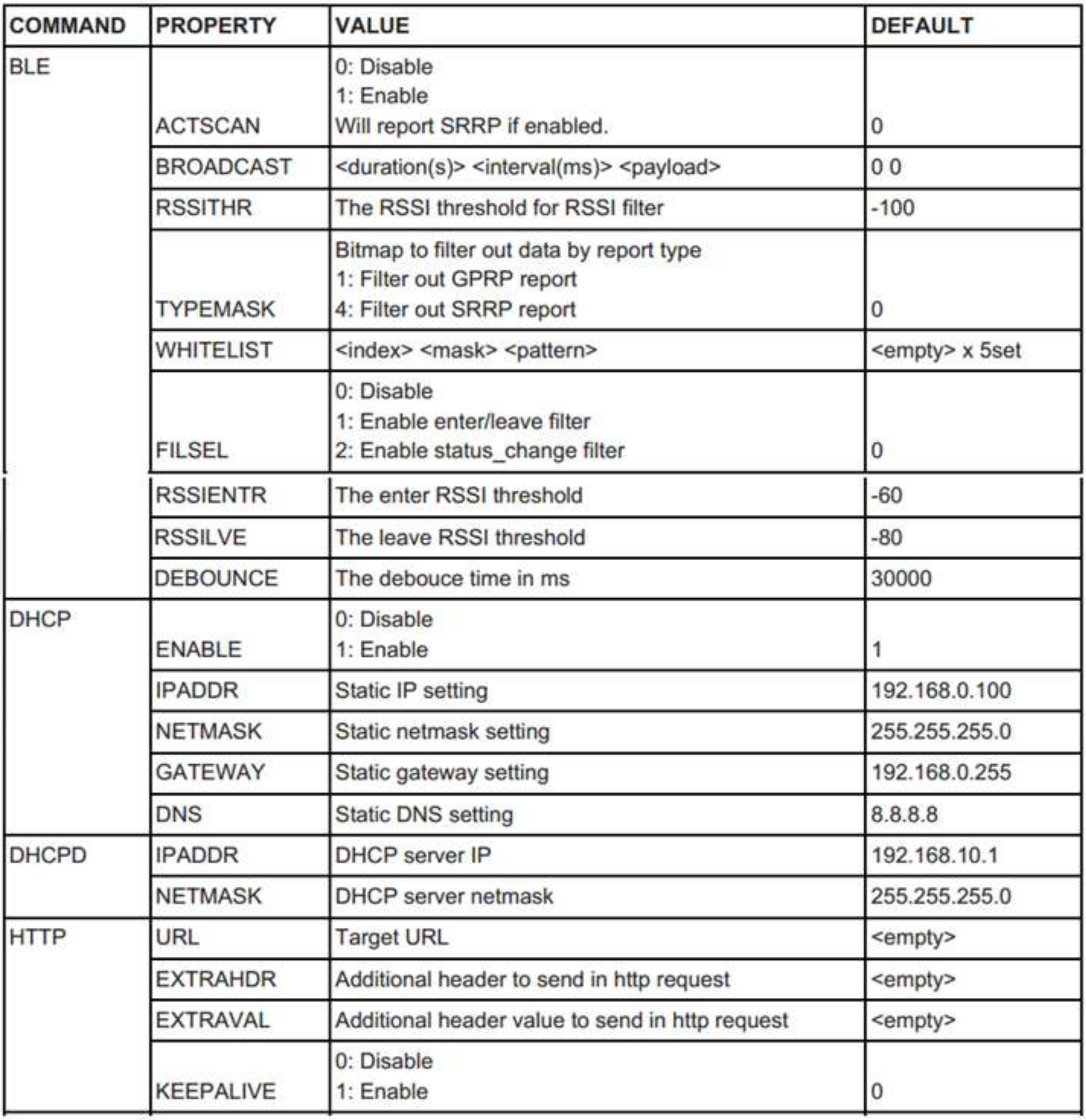
SYS	INFO	Show system firmware information	
	DUMP	Dump all settings	
	ECHO		
	WORKMODE	0: M2M server 1: M2M client 2: HTTP 3: MQTT	0
	USERNAME	System login username	admin
	PASSWORD	System login password	admin
	THROTTLE	Enable throttle to filter out duplicated MAC in cache. (apply to http only)	0
	REQINTVL	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 enabled)	0
	FORMATSEL	0: plain-text 1: json format	0



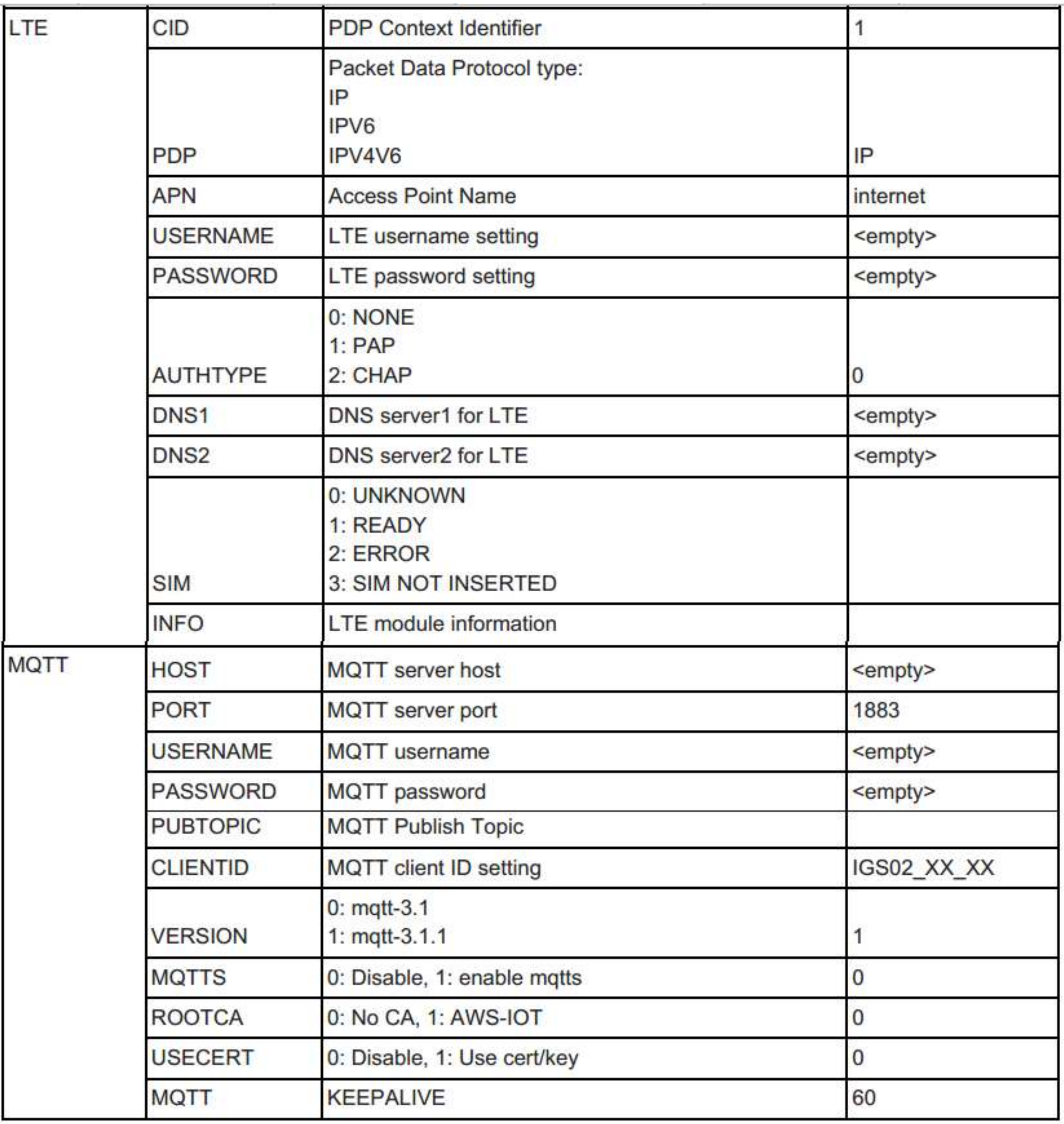
SYS	BLEMACWL	BLE MAC whitelist (allow set 10 sets) <index> <mac> E.g. > SYS BLEMACWL 1 C5A369551012 To clear the setting: > SYS BLEMACWL 1 ""	
	STRICTMODE	Enable strictly error detection	0
	ACTIVEPING	Enable regularly ping GW to detect networking issue To ping GW per minute: > SYS ACTIVEPING 1	0
	OTA	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			

5．コマンドリファレンス

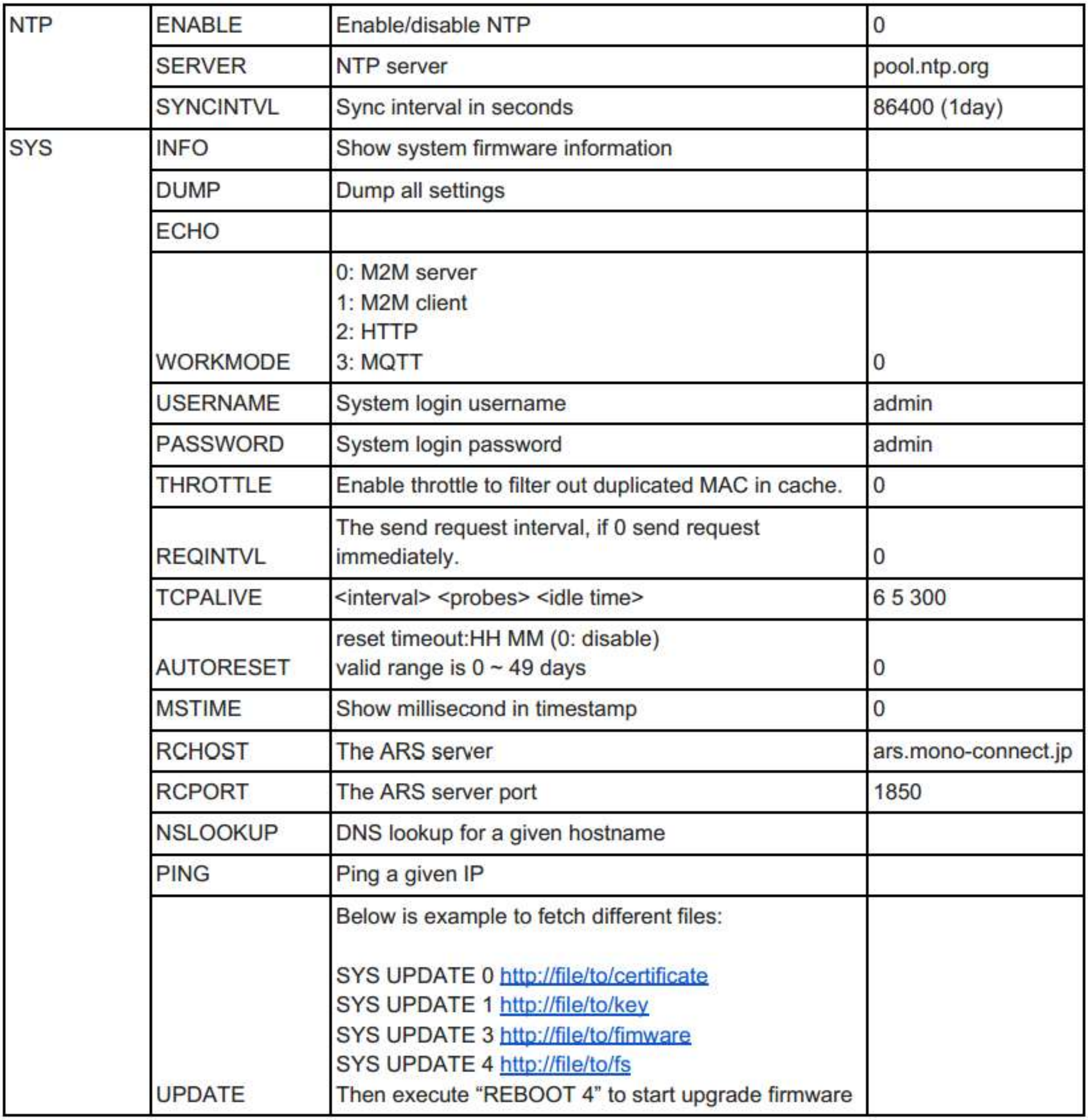
5-3．iGS02 コマンド一覧



COMMAND	PROPERTY	VALUE	DEFAULT
BLE	ACTSCAN	0: Disable 1: Enable Will report SRRP if enabled.	0
	BROADCAST	<duration(s)> <interval(ms)> <payload>	0 0
	RSSITHR	The RSSI threshold for RSSI filter	-100
	TYPEMASK	Bitmap to filter out data by report type 1: Filter out GPRP report 4: Filter out SRRP report	0
	WHITELIST	<index> <mask> <pattern>	<empty> x 5set
	FILSEL	0: Disable 1: Enable enter/leave filter 2: Enable status_change filter	0
	RSSIENTR	The enter RSSI threshold	-60
	RSSILVE	The leave RSSI threshold	-80
	DEBOUNCE	The debouce time in ms	30000
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
HTTP	URL	Target URL	<empty>
	EXTRAHDR	Additional header to send in http request	<empty>
	EXTRAVAL	Additional header value to send in http request	<empty>
	KEEPALIVE	0: Disable 1: Enable	0

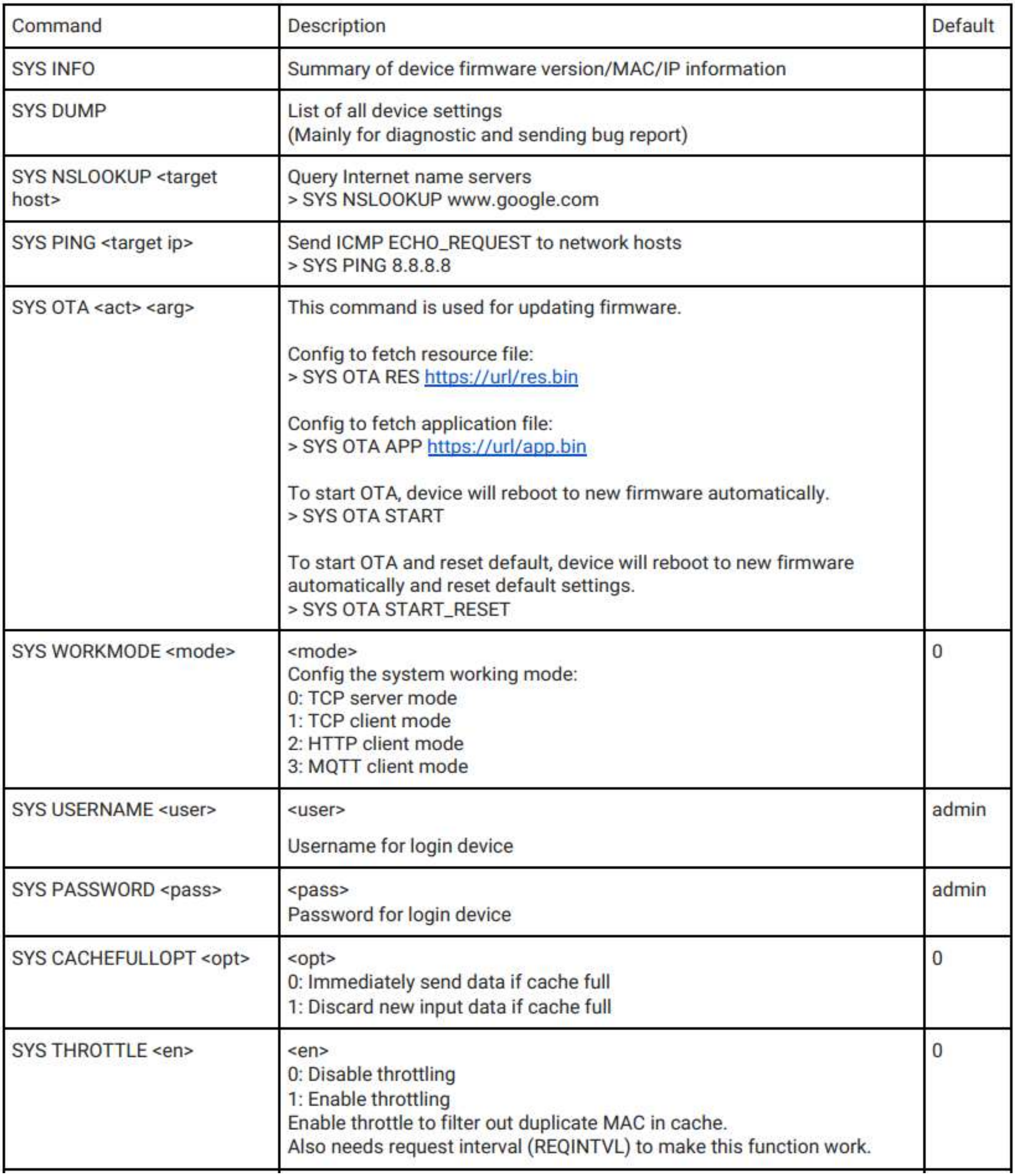


LTE	CID	PDP Context Identifier	1
	PDP	Packet Data Protocol type: IP IPV6 IPV4V6	IP
	APN	Access Point Name	internet
	USERNAME	LTE username setting	<empty>
	PASSWORD	LTE password setting	<empty>
	AUTHTYPE	0: NONE 1: PAP 2: CHAP	0
	DNS1	DNS server1 for LTE	<empty>
	DNS2	DNS server2 for LTE	<empty>
	SIM	0: UNKNOWN 1: READY 2: ERROR 3: SIM NOT INSERTED	
	INFO	LTE module information	
MQTT	HOST	MQTT server host	<empty>
	PORT	MQTT server port	1883
	USERNAME	MQTT username	<empty>
	PASSWORD	MQTT password	<empty>
	PUBTOPIC	MQTT Publish Topic	
	CLIENTID	MQTT client ID setting	IGS02_XX_XX
	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	0
	USECERT	0: Disable, 1: Use cert/key	0
	MQTT	KEEPALIVE	60



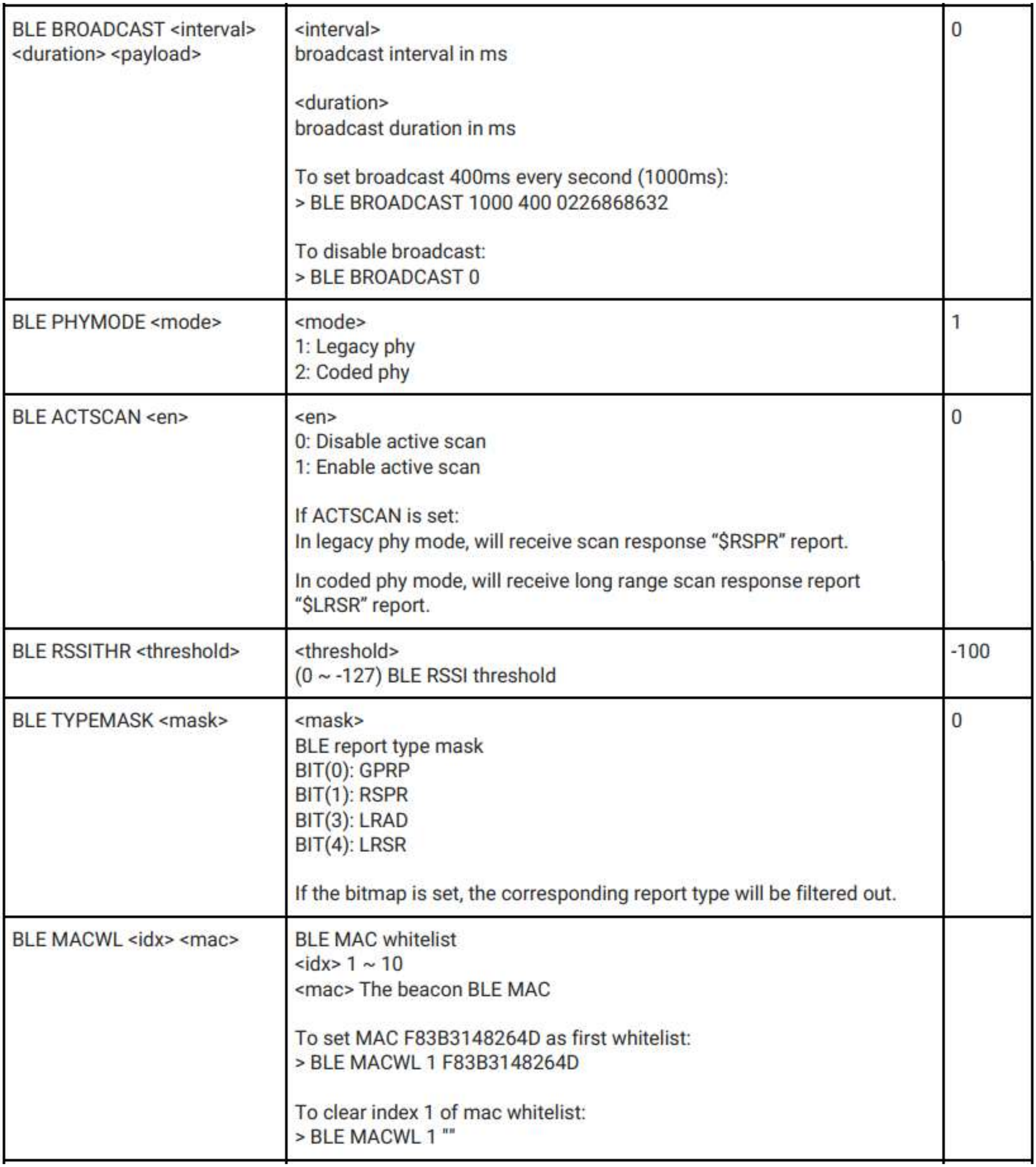
NTP	ENABLE	Enable/disable NTP	0
	SERVER	NTP server	pool.ntp.org
	SYNCINTVL	Sync interval in seconds	86400 (1day)
SYS	INFO	Show system firmware information	
	DUMP	Dump all settings	
	ECHO		
	WORKMODE	0: M2M server 1: M2M client 2: HTTP 3: MQTT	0
	USERNAME	System login username	admin
	PASSWORD	System login password	admin
	THROTTLE	Enable throttle to filter out duplicated MAC in cache.	0
	REQINTVL	The send request interval, if 0 send request immediately.	0
	TCPALIVE	<interval> <probes> <idle time>	6 5 300
	AUTORESET	reset timeout:HH MM (0: disable) valid range is 0 ~ 49 days	0
	MSTIME	Show millisecond in timestamp	0
	RCHOST	The ARS server	ars.mono-connect.jp
	RCPORT	The ARS server port	1850
	NSLOOKUP	DNS lookup for a given hostname	
	PING	Ping a given IP	
	UPDATE	Below is example to fetch different files: SYS UPDATE 0 http://file/to/certificate SYS UPDATE 1 http://file/to/key SYS UPDATE 3 http://file/to/fimware SYS UPDATE 4 http://file/to/fs Then execute “REBOOT 4” to start upgrade firmware	

TCPSRV	PORT	M2M TCP server listen port	8080
TCPCLI	HOST	M2M TCP client target host	
	PORT	M2M TCP client target port	8080
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	
REBOOT		0: reboot 1: reboot to default setting 2: reboot to OTA mode 3: reboot to WPS mode 4: reboot to upgrade firmware if firmware is ready	
EXIT			

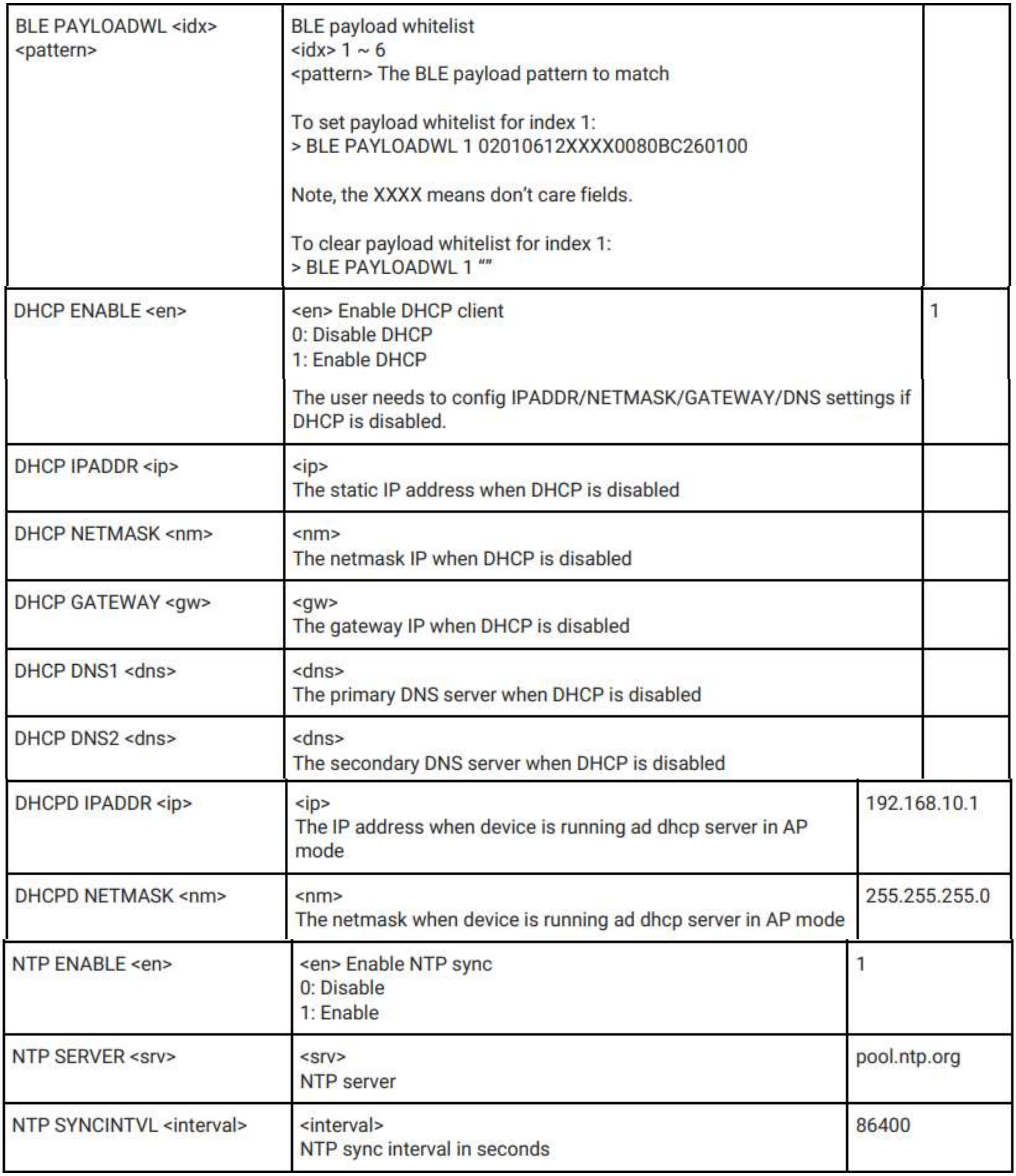


Command	Description	Default
SYS INFO	Summary of device firmware version/MAC/IP information	
SYS DUMP	List of all device settings (Mainly for diagnostic and sending bug report)	
SYS NSLOOKUP <target host>	Query Internet name servers > SYS NSLOOKUP www.google.com	
SYS PING <target ip>	Send ICMP ECHO_REQUEST 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, 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	
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 request interval (REQINTVL) to make this function work.	0

SYS TIMESTAMP <opt>	<opt> 0: No timestamp 1: Append timestamp in second 2: Append timestamp in milisecond	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 server. If not set, 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 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 ke 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, requires reset default to re-configure device.	0
SYS ECHO <arg>	<arg> Send back <arg>	

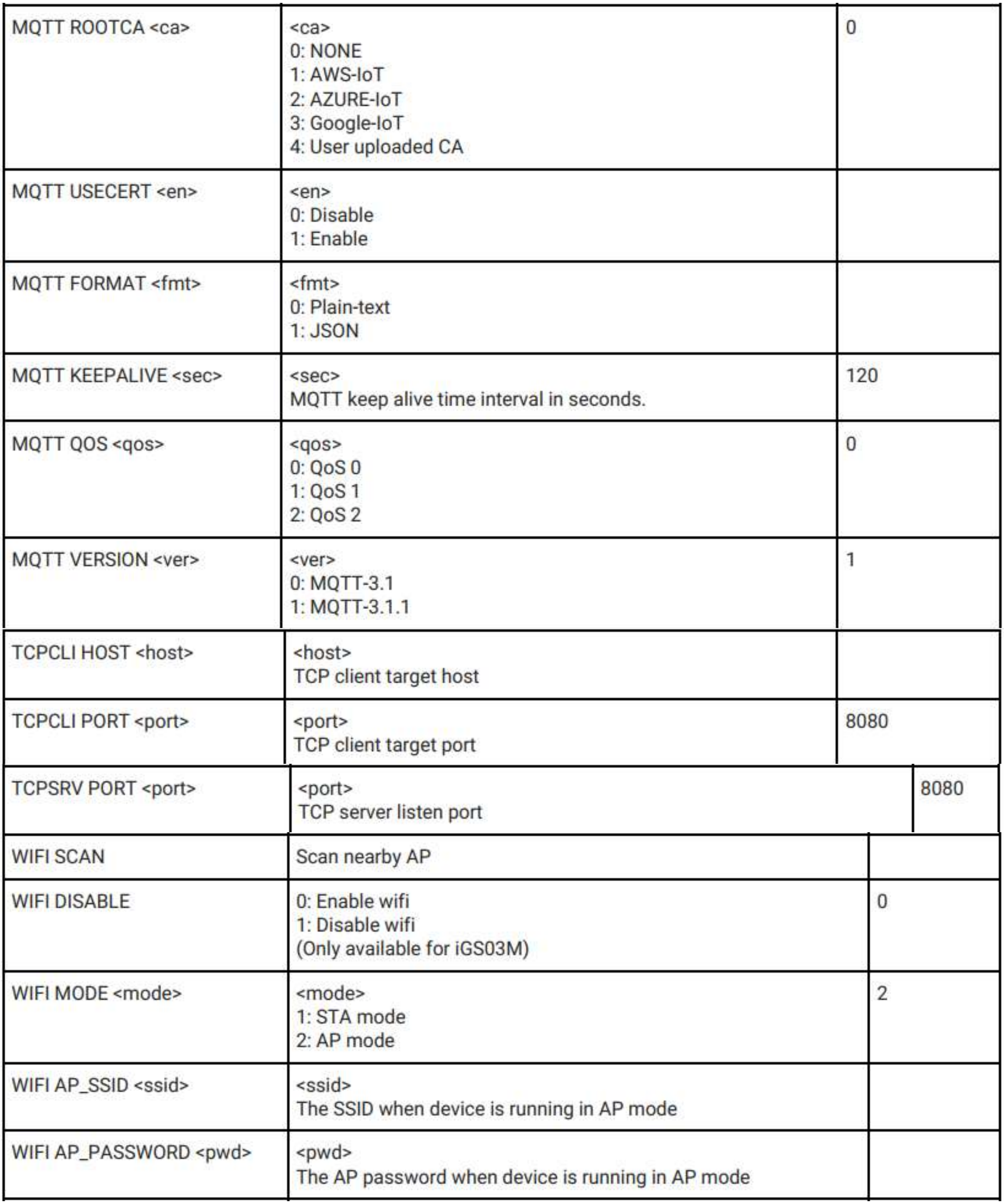


BLE BROADCAST <interval> <duration> <payload>	<interval> broadcast interval in ms <duration> broadcast duration in ms To set broadcast 400ms every second (1000ms): > BLE BROADCAST 1000 400 0226868632 To disable broadcast: > BLE BROADCAST 0	0
BLE PHYMODE <mode>	<mode> 1: Legacy phy 2: Coded phy	1
BLE ACTSCAN <en>	<en> 0: Disable active scan 1: Enable active scan If ACTSCAN is set: In legacy phy mode, will receive scan response “$RSPR” report. In coded phy mode, will receive long range scan response report “$LRSR” report.	0
BLE RSSITHR <threshold>	<threshold> (0 ~ -127) BLE RSSI threshold	-100
BLE TYPEMASK <mask>	<mask> BLE report type mask BIT(0): GPRP BIT(1): RSPR BIT(3): LRAD BIT(4): LRSR 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 fields. To clear payload whitelist for index 1: > BLE PAYLOADWL 1 “”	
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 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 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 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	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 3: Google-IoT 4: User uploaded CA	0
HTTP USECERT <en>	<en> 0: Disable loading certificate 1: Enable loading certificate	
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, system will generate a random id.	
MQTT PUBTOPIC <topic>	<topic> Mqtt publish topic	
MQTT TLS <tls>	<tls> 0: Disable TLS 1: Enable TLS	0

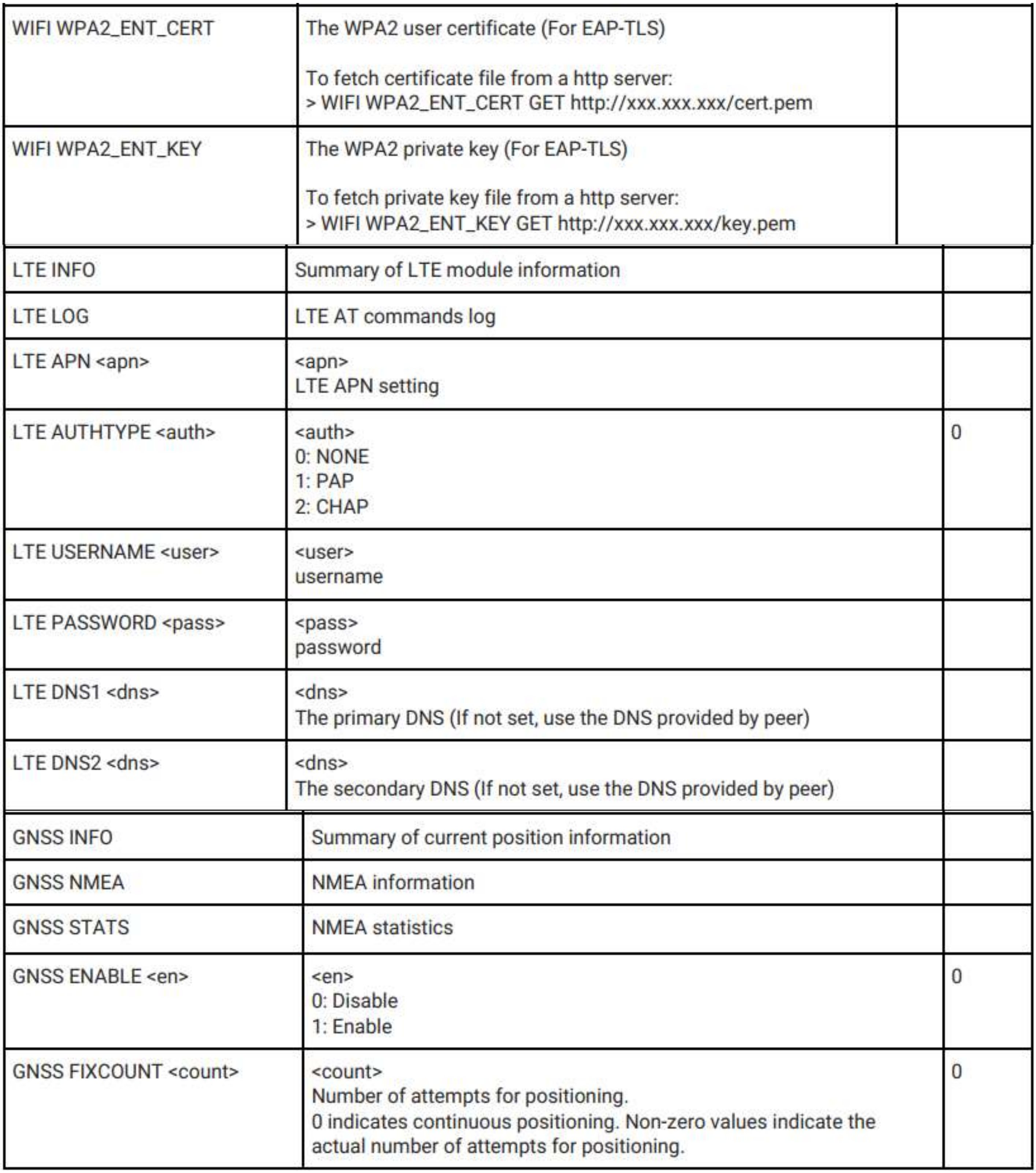


MQTT ROOTCA <ca>	<ca> 0: NONE 1: AWS-IoT 2: AZURE-IoT 3: Google-IoT 4: User uploaded CA	0
MQTT USECERT <en>	<en> 0: Disable 1: Enable	
MQTT FORMAT <fmt>	<fmt> 0: Plain-text 1: JSON	
MQTT KEEPALIVE <sec>	<sec> MQTT keep alive time interval in seconds.	120
MQTT QOS <qos>	<qos> 0: QoS 0 1: QoS 1 2: QoS 2	0
MQTT VERSION <ver>	<ver> 0: MQTT-3.1 1: MQTT-3.1.1	1
TCPCLI HOST <host>	<host> TCP client target host	
TCPCLI PORT <port>	<port> TCP client target port	8080
TCPSRV PORT <port>	<port> TCP server listen port	8080
WIFI SCAN	Scan nearby AP	
WIFI DISABLE	0: Enable wifi 1: Disable wifi (Only available for iGS03M)	0
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	

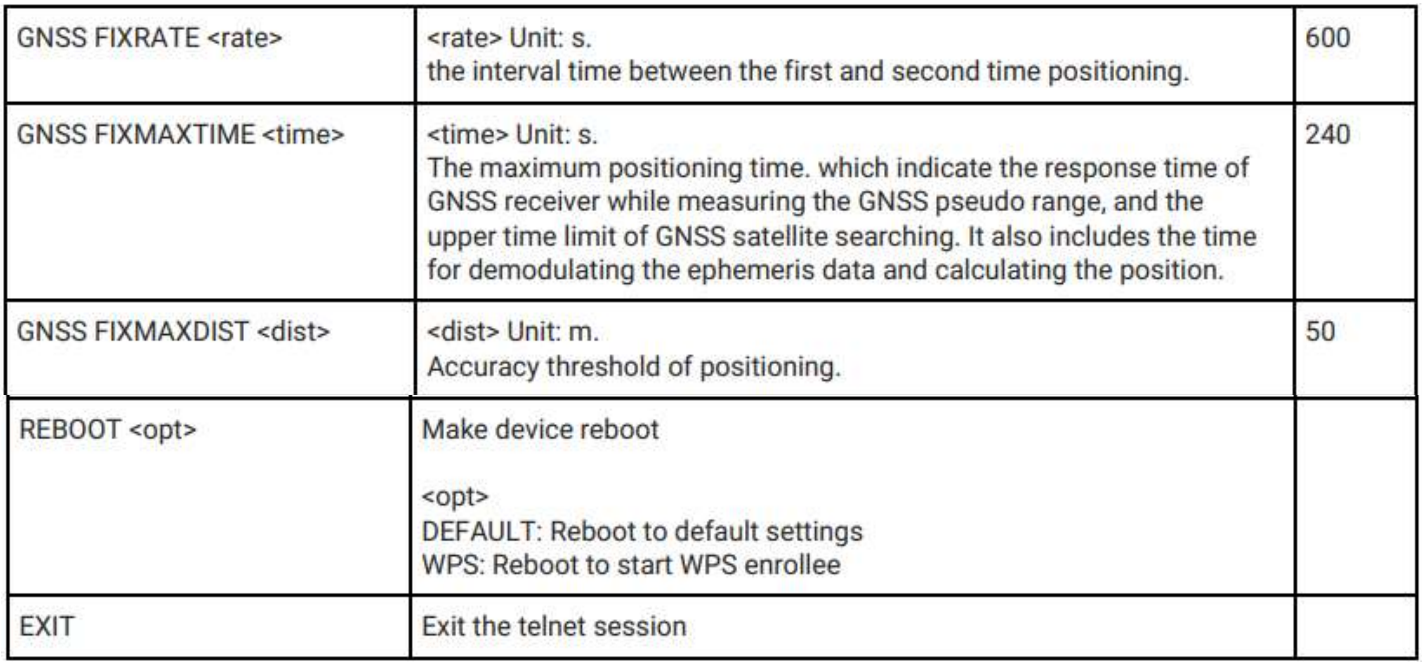
WIFI AP_CHANNEL <ch>	<ch> The AP channel	
WIFI AP_AUTHMODE <auth>	<auth> The AP authenticate mode 0: Open 2: WPA_PSK 3: WPA2_PSK 4: WPA_WPA2_PSK	
WIFI STA_SSID <ssid>	<ssid> The target AP SSID when device is running in STA mode	
WIFI STA_PASSWORD <pwd>	<pwd> The target AP password when device is running 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	

5．コマンドリファレンス

5-4．iGS03 コマンド一覧

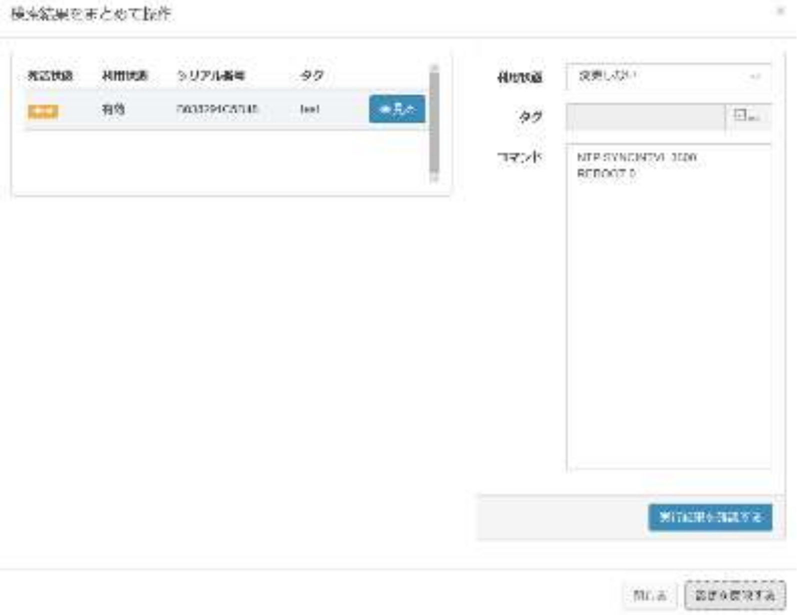


WIFI WPA2_ENT_CERT	The WPA2 user certificate (For EAP-TLS) To fetch certificate file from a http server: > WIFI WPA2_ENT_CERT GET http://xxx.xxx.xxx/cert.pem	
WIFI WPA2_ENT_KEY	The WPA2 private key (For EAP-TLS) To fetch private key file from a http server: > WIFI WPA2_ENT_KEY GET http://xxx.xxx.xxx/key.pem	
LTE INFO	Summary of LTE module information	
LTE LOG	LTE AT commands log	
LTE APN <apn>	<apn> LTE APN setting	
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 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.	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
REBOOT <opt>	Make device reboot <opt> DEFAULT: Reboot to default settings WPS: Reboot to start WPS enrollee	
EXIT	Exit the telnet session	

5-4. コマンド実行例



検索結果をまとめて操作

死活状態	利用状態	シリアル番号	タグ
[illegible]	有効	[illegible]	test

利用状態: 変更しない

タグ:

コマンド:

```
NTP SYNCINTVL 3600
REBOOT 0
```

5-2-1.

「コマンド」欄に実行するコマンドを入力します。「設定を反映する」を選択すると、ゲートウェイに対してコマンドが実行されます。
その後、「実行結果を確認する」が表示されますので、これを選択すると、「ゲートウェイ操作履歴」画面に遷移し、詳細を確認することができます。

左記の例では、以下のコマンドを実行しています。
・NTPサーバとの同期間隔を3600秒に設定。
・ゲートウェイの再起動を実行。

再起動(REBOOT)を行うことで設定が反映されます。　※一部のコマンドを除く

6. お問合わせ先

ご不明の点、ご相談は下記までお気軽にご連絡ください。

お問合せ先

レンジャーシステムズ株式会社
『IoT事業部』担当まで

TEL : 03-6257-1850
FAX : 03-6257-1855
E-Mail : mono-support@ranger-systems.co.jp