MultiConnect® rCell API

Developer Guide

MultiTech Systems

MultiConnect® rCell API Developer Guide
Models: MTR-H5, MTR-H6, MTR-G3, MTR-EV3, MTR-C2 (Software Version 3.1.4)
S000576, Version 1.2

Revision History

Revision	Date	Author	Description
0.1	1/4/13	Jason Reiss	Initial Document
0.5	6/1/13	Sean Godinez	Updated Auto-Gen Scripts and Document Content
0.9	12/4/13	Jason Reiss	Updated document layout
1.0	1/15/14	Sean Godinez	Initial Release (3.0.9)
1.1	3/7/14	Sean Godinez	Updated (3.0.12)
1.2	2/23/15	Sean Godinez	Updated (3.1.4)

Contacting Multi-Tech

Knowledge Base
The Knowledge Base provides immediate access to support information and resolutions for all Multi-Tech products.
Visit `http://www.multitech.com/kb.go`.

Installation Resources
To download manuals, firmware, and software, visit `http://www.multitech.com/setup/product.go`.

Support Portal
To create an account and submit a support case directly to our technical support team, visit: `https://support.multitech.com`.

Technical Support
Business Hours: M-F, 9am to 5pm CST

Country	By Email	By Phone
Europe, Middle East, Africa:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	(800) 972-2439 or (763) 717-5863

World Headquarters
Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112
United States
Phone: 800-328-9717 or 763-785-3500
Fax: 763-785-9874

Warranty
To read the warranty statement for your product, please visit: `http://www.multitech.com/warranty.go`.

Contents

1 Introduction

The MultiConnect® rCell is a cellular router that uses a RESTful JSON API for managing configurations, polling statistics, and issuing commands. This document provides information on the design, patterns, and methods within the rCell API. The Appendix of this document has additional information for those unfamiliar with the REST architecture or JSON data format. For additional examples and use-cases, explore the JavaScript within the rCell website, specifically https://[rcell_ip]/js/api.js.

2 Requests

All API requests will be directed to the https://[rcell_ip]/api url. The majority of requests follow the same RESTful pattern. Following the api url will be a collection name or a command directive. For example, information on the current DHCP settings can be found in the DHCP collection at https://[rcell_ip]/api/dhcp. A full list of collections and commands can be found in section 4. For all examples in this document, the rCell's IP address is 192.168.2.1.

2.1 Making Requests

The RESTful interface allows users to retrieve data, add data, update data, and delete data using call methods: GET, POST, PUT and DELETE, respectively. These methods can be set in the HTTP header, or they can be set in the URI using the key: **method**. Using the URI parameter **method** is a useful way to execute RESTful requests through a web browser. Additional URI parameters can be found in section 2.9 URI Parameters.

All API requests return a JSON object. The JSON response will always contain the members **code** and **status**. The **status** member indicates a high-level result of the request and has two possible values: *success* and *fail*. The **code** member is an HTTP response code describing the outcome of the API result. For a full list of response code values, see section 3.2.2 Error Codes.

If an API call was successful, it may contain the member: **result**. This member contains data that was either requested or data that was generated as part of the API request. If an API call was unsuccessful, the JSON response will contain the member **error**. This member is a short description of the failure.

Example: Retrieving the current DHCP setting using the **method** URI parameter.

```
GET https://192.168.2.1/api/dhcp?method=GET

Status: HTTP/1.1 200 OK
{
  "code" : 200,
  "result" : {
    "defaultGateway" : "192.168.2.1",
    "domain" : "",
    "enabled" : true,
    "fixedAddresses" : [
      {
        "ip" : "192.168.2.15",
        "mac" : "00:1A:12:19:3F:60"
      }
    ],
    "leaseTime" : 86400,
    "leases" : [
      {
        "expiration" : 70359,
        "hostName" : "my-pc",
        "ip" : "192.168.2.103",
```

```
22          "mac" : "00:3a:83:10:24:DC"
23        }
24      ],
25      "maxLeases" : 200,
26      "options" : [ "dhcp-authoritative" ],
27      "rangeEnd" : "192.168.2.254",
28      "rangeStart" : "192.168.2.100",
29      "subnetAddress" : "192.168.2.0",
30      "subnetMask" : "255.255.255.0"
31    },
32    "status" : "success"
33  }
```

The API allows requests to path to specific elements or groups of embedded elements. For example, if a user only wanted to know if DHCP was enabled, they could make the request: https://[rcell_ip]/api/dhcp/enabled.

Example: Path to an element within the DHCP collection.

```
1  GET https://192.168.2.1/api/dhcp/enabled
2
3  Status: HTTP/1.1 200 OK
4  {
5    "code" : 200,
6    "result" : true,
7    "status" : "success"
8  }
```

Accessing objects within an array can be done using the index of the desired object in the path. Some collections support using an object's unique identifier in place of the object's index; generally, this unique identifier is a member called **name** or **guid**. For example, suppose an rCell was configured with a GRE tunnel named *MyGreTunnel*, and a user wanted to know the IP address of the remote end point of that tunnel. The user could make a RESTful GET request to https://[rcell_ip]/api/greTunnels/MyGreTunnel/remoteIp.

Example: Path to an element within an object in an array using the object's unique identifier.

```
1  GET https://192.168.2.1/api/greTunnels/MyGreTunnel/remoteIp
2
3  Status: HTTP/1.1 200 OK
4  {
5    "code" : 200,
6    "result" : "166.184.38.73",
7    "status" : "success"
8  }
```

2.2 Logging In

To use the API, a user must be authorized and have equal or greater privileges than the API call they are invoking. A user can login with valid credentials by passing their username and password to the login URL (`https://192.168.2.1/api/login`) either as URI parameters or within a JSON object. The following call will login the user *admin*, and return the session information including an authorized token. The API attempts to cache the token as a cookie in the user's web browser for authorizing future calls. As an alternative to using a browser cookie, this token can be passed as a URI parameter using the key: **token**. Additional URI parameters can be found in section 2.9 URI Parameters.

Example: Login using username 'admin' and password 'admin'.

```
1  GET https://192.168.2.1/api/login?username=admin&password=admin
2
3  Status: HTTP/1.1 200 OK
```

```
{
  "code" : 200,
  "result" : {
    "address" : "192.168.2.103",
    "permission" : "admin",
    "port" : "59486",
    "timestamp" : "2:58:40:389",
    "token" : "B7083A0B14C0F0BEFFBED89B99EFBC",
    "user" : "admin"
  },
  "status" : "success"
}
```

A token may timeout due to inactivity. The timeout configuration is in the rCell's Remote Access collection (`api/remoteAccess/timeoutSeconds`). There are two authorizers, one for website access and one for non-web browser usage, such as command line utilities like wget and curl. The same user can not be logged in through the same authorizer from more than one IP address. If a user is already logged in and attempts to login from another IP address, a conflict error will be returned. A user can logout from any IP address with the proper credentials.

2.3 Logging Out

The logout call requires that the caller has equal or greater permissions than the user they are logging out. If a user wants to logout, they can pass their authorized token in the following call:

Example:. `https://192.168.2.1/api/logout?token=ABCDEF1234567890ABCDEF12345678`

To logout another user (*guest*), a user with equal or greater permissions can use their token to authorize the call:

Example: `https://192.168.2.1/api/logout?logoutUser=guest&token=ABCDEF1234567890ABCDEF12345678`

Credentials can also be passed with the logout command to authorize the logout call of another user:

Example: `https://192.168.2.1/api/logout?username=admin&password=admin&logoutUser=guest`

2.4 Who Am I

At any point, a user can retrieve their session information using the following API call:

Example:

```
GET https://192.168.2.1/api/whoami

Status: HTTP/1.1 200 OK
{
  "code" : 200,
  "result" : {
    "address" : "192.168.2.103",
    "permission" : "admin",
    "port" : "59486",
    "timestamp" : "2:58:40:389",
    "token" : "B7083A0B14C0F0BEFFBED89B99EFBC",
    "user" : "admin"
  },
  "status" : "success"
}
```

2.5 Passing JSON Data

Data can be sent to the rCell by passing a JSON object in the body of the request content or by passing a JSON object in the URI parameter: **data**. As an example, the following request uses a RESTful PUT call to edit the current DHCP configurations by passing in a JSON object with the **enabled** member set to *false*

Example: To disable DHCP, send the following request:
`https://192.168.2.1/api/dhcp?data={"enabled":false}&method=PUT`

2.6 Saving Changes

A call to save (https://[rcell_ip]/command/save) will write current changes to the device settings. Commands are executed using RESTful POST requests. A full list of commands can be found in section 4.1 Commands.

Example: To save the current changes, send a request to:
`https://192.168.2.1/api/command/save?method=POST`

2.7 Selecting a Version of an API Call

As the rCell API evolves and new features are added, backwards compatibility can be maintained by setting the desired API version within the request. The API version can be set through the **version** URI parameter, or through the URL path by subscripting the version number with the letter 'v'. If a request has only one version, this value is ignored.

Example: To use version 1 of the API, all API requests would be made through https://[rcell_ip]/api/v1/[request_path] or https://[rcell_ip]/api/[request_path]?version=1. If a version is not specified, the request will be executed using the latest API version.

2.8 Element Descriptions

The API provides documentation on collections and elements through https://[rcell_ip]/api/help. For a description of an element or group of elements, use the path to retrieve the data and prepend **help** to the collection component. For example, if a user wanted information on the DHCP element **enabled** (https://[rcell_ip]/api/dhcp/enabled), they could submit a RESTful GET request to https://[rcell_ip]/api/help/dhcp/enabled.

Example: Retrieving a description of the DHCP member *enabled*.

```
GET https://192.168.2.1/api/help/dhcp/enabled

Status: HTTP/1.1 200 OK
{
  "code" : 200,
  "result" : {
    "dhcp_enabled" : "enable or disable DHCP server (default:true) : BOOL"
  },
  "status" : "success"
}
```

The API also provides a separate set of help descriptions that are used by the rCell website for context-sensitive help-on-hover content. The path to each description follows the menu and category embedding of the rCell website.

Example: Retrieving a more human-readable description of the DHCP member *enabled*.

```
GET https://192.168.2.1/api/help/Setup/DHCP/Settings/Enabled

Status: HTTP/1.1 200 OK
{
  "code" : 200,
  "result" : {
    "Setup_DHCP_Settings_Enabled" : "Check to use a DHCP server on network"
  },
  "status" : "success"
}
```

2.9 URI Parameters

URI parameters are reserved keys that are used to modify the functionality of API calls, override HTTP header values, and bundle multiple API requests together. Below is a list of available URI keys and descriptions of their functionality.

URI Key	Description

fields	Applies a RESTful action to multiple collections/elements. Each request path is separated by a comma. Requested data within a field is returned using the path by replacing '/' characters with '_' characters.
	Example:
	`GET https://192.168.2.1/api?fields=lan/ip,serial/client/enabled&method=GET`
	
	`Status: HTTP/1.1 200 OK`
	`{`
	`  "code" : 200,`
	`  "result" : {`
	`  "lan_ip" : "192.168.2.1",`
	`  "serial_client_enabled" : false`
	`  },`
	`  "status" : "success"`
	`}`

method	Allows passing RESTful action (GET, PUT, POST, & DELETE) in URI. This overrides the HTTP header method. See section 2.1
apply	Allows the request to be applied at the given timestamp without restarting. Currently, only **apply=now** is supported.
token	Authorized Login Token. This can be passed to authorize an API call. A token is returned upon a successful login. If a user is logged in, the whoami request will return the users current token. See section 2.2
inactivity	Allows requests to be made without bumping the user's token expiration date. This is useful for automated polling loops that still want to allow a user to timeout due to inactivity (**inactivity=true**)
session	Reserved for internal use. This member will be overwritten.
data	Allows passing a JSON Object in the URI.
default	This option will retrieve the factory defaults of a collection when using a RESTful GET request, and set a collection to its factory defaults when using a RESTful PUT request. (**default=true**)
version	Sets the API version to use during the request. See section 2.7
username	User's login name. Used for logging into the API. See section 2.2
password	User's login password. Used for logging into the API. See section 2.2
logoutUser	User to be logged out. Only used on `api/logout` request. See section 2.3

3 Responses

All API requests return a JSON object. The JSON response will always contain the members **code** and **status**. The **status** member indicates a high-level result of the request and has two possible values: *success* and *fail*. The **code** member is a HTTP response code describing the outcome of the API result. Certain actions or events in the API may result in a URL redirect, such as trying to access API methods when a user is not logged in. In these situations, the JSON response may contain the member **referrer**.

3.1 Success

In the event of a successful request a success message will be returned with the member **status** set to *success* and **code** set to 200. If data is sent in the response it will be found in the **result** field.

3.1.1 Success response format

```
Status: HTTP/1.1 200 OK
{
  "code": 200,
  "status": "success",
  "result": { [JSON Object or Array] }
}
```

3.2 Error

An error response will always contain the members: **code**, **status**, and **error**. If an error is encountered during a request, the API will halt processing and return an error message. This means that a request with multiple errors will receive a response containing error information on only the first error that the API finds during the processing of that request.

3.2.1 Error response format

```
Status: HTTP/1.1 [Error Code] [Error Message]
{
  "code": [Error Code],
  "status": "fail",
  "error": "[Error Message]"
}
```

3.2.2 Error Codes

Code	Error
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
408	Request Timeout
409	Conflict
500	Internal Server Error
501	Not Implemented

4 Commands and Collections

4.1 Commands

The API supports a set of special actions through the Command URL (`api/command`). To execute a command, the call method must be a POST request. A RESTful GET request will return an array of all of the commands.

Command	Description	Parameters
firmware_upgrade	Upgrades rCell firmware	upgrade file
legacy_sync	Synchronizes legacy configurations	
restart	Restarts rCell device	
revert	Reverts all changes since the last save	
save	Saves the current configurations	
ddns_update	Pushes DDNS information to the configured DDNS server	
download_config	Downloads the current configurations	
loglvl_debug	Sets the API's logging level to DEBUG	
loglvl_info	Sets the API's logging level to INFO	
loglvl_trace	Sets the API's logging level to TRACE	
loglvl_warning	Sets the API's logging level to WARNING	
ping	Send a set of ICMP pings to an address or url `{ "ip": [IP Address or URL], "interface": [ANY, LAN, WIFI, CELLULAR, ETHERNET ] }`	JSON Data
radio_activate	Attemtps to activate the on-board cellular radio (CDMA only)	JSON Data
radio_cmd	Send a string directly to the cellular radio `{ "at": [AT COMMAND], "timeout": [milliseconds] }`	JSON Data
remove_icon	Deletes user-supplied icon	
remove_image	Deletes user-supplied image	
remove_logo	Deletes user-supplied logo	
reset_bluetooth	Resets the Bluetooth hardware	
reset_modem	Resets the cellular radio hardware	
reset_wifi	Resets the WiFi hardware	
restore_defaults	Resets the rCell with User-Defined defaults if set, otherwise factory	
restore_factory	Resets the rCell with factory defaults	
clean_oem	Clears User-Defined default configurations returning factory default	
save_oem	Saves current configurations as factory/OEM defaults	
save_restart	Saves the current configurations and restarts the rCell	
telit_upgrade	Upgrades the Telit radio firmware	upgrade file
upload_config	Uploads and sets new configurations	configuration file
upload_icon	Uploads and sets new icon	icon file
upload_image	Uploads and sets new image	image file
upload_logo	Uploads and sets new logo	logo file

4.2 Collections

Collections are groups of related elements used to configure a service or capability. There are four main actions that can be performed on a collection: get, edit, add, and delete. These actions align with RESTful calls: GET, PUT, POST, and DELETE.

Collection	Type	Description
autoDialout	OBJECT	allow use of cellular modem directly from serial port
autoReboot	OBJECT	cause the device to automatically reboot
backOffTimers	OBJECT	carrier-defined backoff timings for PPP connections, SMS retries, and modem resets
bluetooth	OBJECT	allow a device to connect via Bluetooth
brand	OBJECT	customize icons, images and support information for rebranded rCell
certificate	OBJECT	secure public key certificate configurations
command	OBJECT	set of special actions to perform on the device (requires POST request)
ddns	OBJECT	dynamic domain name server update remote server when ip address changes
devices	ARRAY	list of saved devices
dhcp	OBJECT	DHCP settings
dns	OBJECT	dns forwarding feature
filters	ARRAY	array of firewall filters
gccp	OBJECT	settings for gccp application
gps	OBJECT	gps service settings
greTunnels	ARRAY	list of gre tunnels
ipPipes	ARRAY	list of configured IP Pipes
ipsecTunnels	ARRAY	array of IPsec tunnels
lan	OBJECT	lan interface settings
legacyDefaults	OBJECT	legacy default settings, do not modify
nat	ARRAY	list of NAT rules for advanced firewall settings
networks	ARRAY	array of networks to be used in setting filters and tunnels
ppp	OBJECT	PPP settings
remoteAccess	OBJECT	settings to configure remote access of device
remoteManagement	OBJECT	remote management settings
routes	ARRAY	list of static routes
serial	OBJECT	settings for serial port
sms	OBJECT	settings for sms
smtp	OBJECT	settings for smtp
sntp	OBJECT	settings for clock synchronization between computer systems
syslog	OBJECT	settings for syslog support
system	OBJECT	system attributes
users	ARRAY	users collection for authentication
waninfo	OBJECT	information on WAN interfaces
wanmngr	OBJECT	settings for WAN management
wifi	OBJECT	settings for wi-fi services

4.3 Collection Details

4.3.1 autoDialout

Description: allow use of cellular modem directly from serial port : OBJECT

Element	Type	Description
eia	BOOL	enable or disable EIA standard signal characteristics (default:false)
enabled	BOOL	enable or disable this feature (default:true)
inactivity	UINT	set inactivity timeout in seconds set to 0 to disable (default:0)
login	BOOL	enable or disable login requirement (default:true)
port	UINT	configure port to use when connecting to rCell (default:5000)
raw	BOOL	enable or disable raw mode (default:false)
tcpKeepaliveInterval	UINT	The interval between subsequential keepalive probes, regardless of what the connection has exchanged in the meantime (default:75)
tcpKeepaliveProbes	UINT	The number of unacknowledged probes to send before considering the connection dead and notifying the application layer (default:9)
tcpKeepaliveTime	UINT	The interval between the last data packet sent (simple ACKs are not considered data) and the first keepalive probe; after the connection is marked to need keepalive, this counter is not used any further (default:7200)

4.3.2 autoReboot

Description: cause the device to automatically reboot : OBJECT

Element	Type	Description
hour	UINT	based on the mode as either Hour of Day or Hours from Boot
mode	STRING	DISABLED, TIME, or TIMER (default: DISABLED)

4.3.3 backOffTimers

Description: carrier-defined backoff timings for PPP connections, SMS retries, and modem resets : OBJECT

Element	Type	Description
enabled	BOOL	enable or disable backOffTimers feature (default:true)
timers	ARRAY	list of BackOff Timers
carrierName	STRING	name of carrier
data	ARRAY	Data timings, interval between cellular connection attempts in seconds
dataReset	ARRAY	Data reset timings, interval between connection reset attempts in seconds
modemReset	ARRAY	Modem reset timings, interval between resetting the modem in seconds
readOnly	BOOL	read-only
sms	ARRAY	Sms timings, interval between attempts to send SMS in seconds

4.3.4 bluetooth

Description: allow a device to connect via Bluetooth : OBJECT

Element	Type	Description
device	OBJECT	bluetooth settings of connected device
address	STRING	mac address of bluetooth device
name	STRING	name of bluetooth device
devices	ARRAY	list of bluetooth devices found during last scan
address	STRING	mac address of device
name	STRING	label for device
enabled	BOOL	enable or disable bluetooth feature (default:false)
savedDevices	ARRAY	list of saved bluetooth devices
address	STRING	mac address of device
friendlyName	STRING	user defined name of device
name	STRING	scanned name of device

4.3.5 brand

Description: customize icons, images and support information for rebranded rCell : OBJECT

Element	Type	Description
address1	STRING	address of company for support contact
address2	STRING	address of company for support contact
city	STRING	city of company for support contact
companyName	STRING	company name for support contact
country	STRING	country of company for support contact
fax	STRING	fax number of company for support contact
icon	STRING	image file name for custom favicon in browser
image	STRING	image file name for custom image on support page
links	ARRAY	list of web links for customer support
label	STRING	label for hyperlink
text	STRING	text of hyperlink
url	STRING	url of hyperlink
logo	STRING	image file name for custom logo in header and on login page
phoneNumbers	ARRAY	list of phone numbers for customer support
label	STRING	phone number label
number	STRING	phone number
showOnDashboard	BOOL	enable or disable display of brand information on support page (default:false)
state	STRING	state or province of company for support contact
website	STRING	website of company for support contact
zipCode	STRING	zipCode of company for support contact

4.3.6 certificate

Description: secure public key certificate configurations : OBJECT

Element	Type	Description
create	ACTION	creates a new certificate
commonName	STRING	rCell IP address that you use to connect to rCell
country	STRING	two letter code for the country for which the certificate is valid
days	UINT	number of days that certificate is valid (default:365)
emailAddress	STRING	email address of the person reponsible for the rCell
locality	STRING	city or locality for which the certificate is valid
organization	STRING	organization name for which the certificate is valid
state	STRING	state or province for which the certificate is valid
details	OBJECT	current certificate information
credentials	STRING	certificate subject description
details	STRING	certificate details description
periodFrom	STRING	certificate start date
periodTo	STRING	certificate end date
upload	ACTION	uploades the new certificate (POST certificate file)

4.3.7 ddns

Description: dynamic domain name server update remote server when ip address changes : OBJECT

Element	Type	Description
authentication	OBJECT	authentication information
password	STRING	password for ddns account
username	STRING	username for ddns account
checkIp	OBJECT	configure remote server to connect to
enabled	BOOL	enable or disable check IP feature (default:true)
port	UINT	port on remote server (default:80)
server	STRING	domain name of remote server (default:'checkip.dyndns.org')
domain	STRING	registered domain name
enabled	BOOL	enable or disable DDNS feature (default:false)
port	UINT	servers port number (default:80)
retriesMax	UINT	maximum number of tries to connect before failing (default:5)
server	STRING	name of server with currently assigned IP address (default:'members.dyndns.org')
system	STRING	system registration type, DYNAMIC or CUSTOM (default:DYNAMIC)
updateInterval	UINT	number of days between forced update (default:28)

4.3.8 devices

Description: list of saved devices : ARRAY

Element	Type	Description
friendlyName	STRING	friendly name to associate with device
mac	STRING	mac address of device
name	STRING	name of device

4.3.9 dhcp

Description: DHCP settings : OBJECT

Element	Type	Description
defaultGateway	STRING	default gateway of network (default:'192.168.2.1')
domain	STRING	network domain name
enabled	BOOL	enable or disable DHCP server (default:true)
fixedAddresses	ARRAY	list of fixed addresses
ip	STRING	ip address to assign to client
mac	STRING	mac address of client
leaseTime	UINT	number of seconds leases are issued for (default:86400)
leases	ARRAY	current leases issued by DHCP server
maxLeases	UINT	maximum number of leases that can be issued (default:200)
options	ARRAY	an array of additional dhcp options
rangeEnd	STRING	end ip address of dhcp lease range (default:'192.168.2.254')
rangeStart	STRING	start ip address of dhcp lease range (default:'192.168.2.100')
subnetAddress	STRING	subnet of network (default:'192.168.2.0')
subnetMask	STRING	mask of network (default:'255.255.255.0')

4.3.10 dns

Description: dns forwarding feature : OBJECT

Element	Type	Description
enabled	BOOL	enable or disable dns server (default:true)
options	ARRAY	an array of additional dns options
primary	STRING	static ip address of primary dns server
secondary	STRING	static ip address of secondary dns server

4.3.11 filters

Description: array of firewall filters : ARRAY

Element	Type	Description
action	STRING	action of filter: ACCEPT, REJECT, LOG or DROP
description	STRING	filter description
direction	STRING	direction of traffic: INGRESS or EGRESS
dstIp	STRING	ip address of destination or 'ANY'
dstMask	UINT	network mask of destination (0-32)
dstPortEnd	STRING	end of destination port range or 'ANY'
dstPortStart	STRING	beginning of destination port range or 'ANY'
enabled	BOOL	enable or disable this filter
name	STRING	name of filter
protocol	STRING	filter protocol, TCP, UDP or TCP/UDP
srcIp	STRING	ip address of source or 'ANY'
srcMac	STRING	mac address of source
srcMask	UINT	network mask of source (0-32)
srcPortEnd	STRING	end of source port range or 'ANY'
srcPortStart	STRING	beginning of source port range or 'ANY'

4.3.12 gccp

Description: settings for gccp application : OBJECT

Element	Type	Description
enabled	BOOL	enable or disable gccp feature (default:false)
port	UINT	port to open on rCell for gccp connection (default:5000)

4.3.13 gps

Description: gps service settings : OBJECT

Element	Type	Description
client	OBJECT	settings for gps client
enabled	BOOL	enable or disable gps client (default:false)
password	STRING	password to use when connecting to remote server
port	UINT	port to connect on remote server (default:5445)
protocol	STRING	protocol to when making connection, UDP or TCP (default:TCP)
remoteHost	STRING	ip address of remote server (default:'192.168.2.3')
nmea	OBJECT	specify what nmea sentences to send and how often to send them
gga	BOOL	global positioning system fix data (default:true)
gll	BOOL	geographic position, latitude/longitude (default:true)
gsa	BOOL	GPS DOP and active satellites (default:true)
gsv	BOOL	GPS Satellites in view (default:true)
id	STRING	optional id to attach to messages
idPrefix	STRING	optional prefix to attach to messages
interval	UINT	interval in seconds to send gps information (default:10)
rmc	BOOL	recommended minimum specific GPS/Transit data (default:true)
vtg	BOOL	track made good and ground speed (default:true)
server		settings for gps server
dumpSerialPort	BOOL	output gps information to serial port (default:false)
enabled	BOOL	enable or disable gps server on rCell (default:false)
password	STRING	password needed for client to connect to server
port	UINT	port to for server to listen on (default:5445)

4.3.14 greTunnels

Description: list of gre tunnels : ARRAY

Element	Type	Description
description	STRING	description for gre tunnel
enabled	BOOL	enable or disable this tunnel
name	STRING	name of tunnel
remoteIP	STRING	remote ip of tunnel
routes	ARRAY	list or tunnel routes
ip	STRING	ip address of route
mask	STRING	network mask of route (0-32)
ttl	UINT	time to live (0-255)

4.3.15 ipPipes

Description: list of configured IP Pipes : ARRAY

Element	Type	Description
activation	STRING	signal to start connection
description	STRING	summary of the pipe
enabled	BOOL	enable or disable this pipe
ip	STRING	ip address of the remote end of the pipe
mode	STRING	determines whether local end point is a client or server or both
name	STRING	label of the pipe
port	UINT	port number of the remote end point when in CLIENT mode, or listening port when in SERVER mode
protocol	STRING	the internet protocol to use (UDP, TCP or SSL/TLS)
secondaryIp	STRING	ip address of the second server to try if a connection can not be made to the first. Requires CLIENT mode
secondaryPort	STRING	port of the second server to try if a connection can not be made to the first. Requires CLIENT mode
sequence	STRING	the character or stream of characters that signal the pipe to terminate. Requires termination mode to be SEQUENCE
source	STRING	the source defines the local device to convert data to and from ip communication
termination	STRING	the mode for terminating the pipe
timeoutSeconds	UINT	the amount of seconds of inactivity allowed before the pipe will close. Requires termination mode to be TIMEOUT
type	STRING	the type of pipe. currently only serial-to-ip and bluetooth-to-ip are supported

4.3.16 ipsecTunnels

Description: array of IPsec tunnels : ARRAY

Element	Type	Description
aggressiveMode	BOOL	[OPTIONAL] whether to allow a less secure mode that exchanges identification in plain text
authMethod	STRING	how the two security gateways should authenticate each other
compression	BOOL	whether IPComp compression of content is proposed on the connection
description	STRING	a note about the tunnel
enabled	BOOL	enable or disable this tunnel
encryptMethod	STRING	IKE encryption/authentication algorithm to be used for phase 1 and phase 2 of the connection
ikelife	UINT	how long the keying channel of a connection should last before being renegotiated (hours)
keylife	UINT	how long a particular instance of a connection should last, from successful negotiation to expiry (hours)
localId	STRING	how the local participant should be identified for authentication
name	STRING	label of tunnel
natTraversal	BOOL	[OPTIONAL] whether to accept or offer to support NAT workaround for IPsec
perfectForwardSecrecy	BOOL	whether Perfect Forward Secrecy of keys is desired on the connection's keying channel
phase1	STRING	[OPTIONAL] specific algorithms to use for phase 1. Format: cipher-hash;group. Example: aes128-sha1;modp1024
phase2	STRING	[OPTIONAL] specific algorithms to use for phase 2. Format: cipher-hash;group. Example: aes128-sha1;modp1024
psk	STRING	pre-shared key
remoteId	STRING	how the remote participant should be identified for authentication
remoteNetwork	STRING	saved network of remote end of tunnel
remoteNetworkIp	STRING	network at the remote end of tunnel
remoteNetworkMask	UINT	network mask at the remote end of tunnel
remoteWanIp	STRING	public ip of remote end of tunnel
retries	UINT	number of attempts that should be made to negotiate a connection, or a replacement for one, before giving up
type	STRING	type of ipsec tunnel: Internet Key Exchange is currently the only type supported
uid	BOOL	whether or not tunnel end points should be identified for authentication

4.3.17 lan

Description: lan interface settings : OBJECT

Element	Type	Description
gateway	STRING	default gateway (default:192.168.2.1)
ip	STRING	ip address (default:192.168.2.1)
mask	STRING	subnet mask (default:255.255.255.0)

4.3.18 legacyDefaults

Description: legacy default settings, do not modify : OBJECT

Element	Type	Description

4.3.19 nat

Description: list of NAT rules for advanced firewall settings : ARRAY

Element	Type	Description
description	STRING	description of rule
direction	STRING	direction of rule, INGRESS or EGRESS
enabled	BOOL	enable or disable rule (default:true)
guid	STRING	rule guid
lanIp	STRING	LAN ip address of rule
lanPortEnd	STRING	LAN end port range of rule
lanPortStart	STRING	LAN beginning port range of rule
name	STRING	name of rule
protocol	STRING	TCP, UDP or TCP/UDP
type	STRING	SNAT or DNAT
wanIp	STRING	WAN ip address of rule or 'ANY'
wanPortEnd	STRING	WAN end port range or 'ANY'
wanPortStart	STRING	WAN beginning port range or 'ANY'

4.3.20 networks

Description: array of networks to be used in setting filters and tunnels : ARRAY

Element	Type	Description
ip	STRING	ip address of network
mask	UINT	network mask (0-32)
name	STRING	name of network
type	STRING	type of network, STATIC or DYNAMIC, configured networks should be set as DYNAMIC

4.3.21 ppp

Description: PPP settings : OBJECT

Element	Type	Description
authentication	OBJECT	PPP authentication settings
password	STRING	password of ppp account
type	STRING	type of authentication to use when connecting to ppp, PAP, CHAP or PAP-CHAP (default:'PAP-CHAP')
username	STRING	username of ppp account
connectTimeout	UINT	time in seconds to wait for a connection while in receive mode (default:90)
dialOnDemand	BOOL	enable or disable dial on demand : (default:false)
diversity	BOOL	enable or disable antenna diversity (default:true)
enabled	BOOL	enable or disable ppp connection (default:false)
idleTimeout	UINT	timeout in seconds before connection is considered idle and disconnected (default:180)
keepAlive	OBJECT	PPP keep alive settings
dataRecv	OBJECT	keep ppp connection alive as long as data is being received
enabled	BOOL	enable or disable data receive monitor (default:false)
window	UINT	time in minutes (default:0)
enabled	OBJECT	enable or disable keep alive feature
hostname	STRING	host to connect to
icmpCount	UINT	number of pings to send (default:4)
pingInterval	UINT	interval in seconds to send pings (default:60)
tcpPort	UINT	port on host to connect to (default:0)
type	STRING	method to use for keep alive, ICMP or TCP (default:ICMP)
maxRetries	UINT	maximum number of retries to attempt before failing (default:0)
modem	OBJECT	modem settings
apnString	STRING	apn connection string from service provider
baudRate	UINT	baud rate of modem (default:115200)
commands	ARRAY	list of at commands to send to modem after successfully connecting
connectString	STRING	string to send modem on successful connection (default:'CONNECT')
dialNumber	STRING	number for modem to dial for connection (default:'*99***1#')
dialPrefix	STRING	prefix to add to number (default:'ATDT')
initStrings	ARRAY	list of init strings to send to modem (default:['AT+CSQ'])
simPin	STRING	pin used to unlock sim for use
nat	BOOL	enable or disable nat feature (default:true)
powerOnInitString	STRING	string to send to radio on boot up
wakeUpOnCall	OBJECT	wake-up on call settings
ackString	STRING	string used to acknowledge (to the delivering SMSC) the receipt of an SMS
callerIds	OBJECT	list of valid caller ids for wake-up
action	STRING	action to perform on wake-up
text	STRING	text of wake-up SMS message or caller-id value
type	STRING	type of call: CALLER or SMS
delay	UINT	seconds to wait after call before reconnecting (default:10)
enabled	BOOL	enable or disable wake-up on call (default:false)
fromLan	BOOL	enable or disable wake-up on lan activity (default:false)
initStrings	ARRAY	list of cellular radio AT init strings
onCallerId	BOOL	enable or disable wake-up on caller id (default:false)
onRing	BOOL	enable or disable wake-up on ring (default:false)
onSms	BOOL	enable or disable wake-up on sms (default:false)

4.3.22 remoteAccess

Description: settings to configure remote access of device : OBJECT

Element	Type	Description
bruteForcePrevention	OBJECT	settings to configure login attempt throttling
enabled	BOOL	enable device to throttle username and password combination attempts (default:false)
failAttempts	UINT	set the number of consecutive failures before locking out an account (default:3)
lockoutSeconds	UINT	set the amount of seconds that a user account will be locked out (default:300)
dosAttackPrevention	OBJECT	settings to configure new connection throttling
enabled	BOOL	enable device to throttle number of new connection attempts to device (default:false)
limitBurst	UINT	set the upper limit of new connections allowed per minute (default:100)
limitPerMinute	UINT	set the average number of new connections allowed per minute (default:60)
http	OBJECT	settings to configure HTTP access to device
enabled	BOOL	(default:true)
lan	BOOL	enable HTTP access for LAN traffic (default:true)
port	UINT	set HTTP port (default:80)
redirectToHttps	BOOL	redirect request for HTTP port to HTTPS port (default:true)
wan	BOOL	enable HTTP access for WAN traffic (default:false)
https	OBJECT	settings to configure HTTPS access to device
enabled	BOOL	(default:true)
lan	BOOL	enable HTTPS access for LAN traffic (default:true)
port	UINT	set port for rcell configuration website (default:443)
wan	BOOL	enable HTTPS access for WAN traffic (default:false)
icmp	OBJECT	settings to configure ICMP access to device
enabled	BOOL	enable any response to icmp traffic (default:true)
respondToLan	BOOL	respond to lan icmp traffic (default:true)
respondToWan	BOOL	responsd to wan icmp traffic (default:false)
pingLimit	OBJECT	settings to configure ICMP throttling
enabled	BOOL	enable device to throttle number of icmp packets allowed to device (default:false)
limitBurst	UINT	set the upper limit of icmp packets allowed per second (default:30)
limitPerSecond	UINT	set the average number of new connections allowed per second (default:10)
privateWan	BOOL	drop packets with private source addresses coming from public wan interfaces, i.e. spoofed packets (default:false)
ssh	OBJECT	settings to configure SSH access to device
enabled	BOOL	enable ssh access to the device (default:true)
lan	BOOL	allow ssh access from lan (default:true)
port	UINT	set the port for ssh access to the device (default:22)
wan	BOOL	allow ssh access from wan (default:false)
timeoutSeconds	UINT	(default:300)

4.3.23 remoteManagement

Description: remote management settings : OBJECT

Element	Type	Description
accountKey	STRING	account key registered to user by device management platform
allowConfigurationUpgrade	BOOL	allow configuration upgrades to be managed through device management platform (default:true)
allowFirmwareUpgrade	BOOL	allow firmware upgrades to be managed through device management platform (default:true)
enabled	BOOL	enable the device to be managed by a remote management platform (default:false)
gpsDataInterval	UINT	set the gps push interval in seconds (default:43200)
queryServerInterval	UINT	set the check-in interval in seconds (default:43200)
serverName	STRING	remote management platform's url or IP address (default:ds.multitech.com)
serverPort	UINT	remote management platform's IP port (default:5798)
sslEnabled	BOOL	enable traffic encryption (default:true)
syncWithDialOnDemand	BOOL	only allow the device to contact the remote management platform when the cellular link is already up (default:false)

4.3.24 routes

Description: list of static routes : ARRAY

Element	Type	Description
gateway	STRING	default gateway of route
ip	STRING	ip address of route
mask	UINT	network mask of route (0-32)
name	STRING	name of route

4.3.25 serial

Description: settings for serial port : OBJECT

Element	Type	Description
baudRate	UINT	(default:115200)
dataBits	UINT	(default:8)
flowControl	STRING	RTS-CTS or NONE (default:NONE)
modbus	BOOL	enable or disable modbus (default:false)
parity	STRING	ODD, EVEN or NONE (default:NONE)
stopBits	UINT	(default:1)
type	STRING	if device support flexible serial port: RS-232, RS-422, or RS-485 (default:RS-232)

4.3.26 sms

Description: settings for sms : OBJECT

Element	Type	Description
enabled	BOOL	enable or disable SMS service (default:true)
inbox		a list of received SMS messages
outbox		a list of sent SMS messages
receivedLimit	UINT	number of received SMS to keep. Set it to 0 if you do not want to keep SMS. Maximum is 1000, (default:1000)
resendLimit	UINT	the number of times that the modem retries sending the failed SMS message. Set it to 0 if you do not want to resend failed SMS messages. Maximum is 10. (default:3)
sentLimit	UINT	number of sent SMS to keep. Set it to 0 if you do not want to keep SMS. Maximum is 1000, (default:1000)

4.3.27 smtp

Description: settings for smtp : OBJECT

Element	Type	Description
enabled	BOOL	Enable SMTP to allow your router to send email messages (default:false)
maxNumberOfEntries	STRING	Specify the number of mail log entries to keep for completed emails in router. Minimum number is 10, maximum is 1000
password	STRING	SMTP password
serverAddress	STRING	Address of SMTP server
serverPort	STRING	SMTP server's port number
sourceEmailAddress	STRING	Multi-Connect rCell Email address. The provided address will be displayed as the From address in the sent email
username	STRING	SMTP username

4.3.28 sntp

Description: settings for clock synchronization between computer systems : OBJECT

Element	Type	Description
enabled	BOOL	enable or disable SNTP client (default:false)
pollingTime	UINT	frequency in minutes to poll current time (default:120) [0-1440]
server	STRING	ip address or domian name of server
timeZone	STRING	zoneinfo file path to use as timezone : (default:UTC)

4.3.29 syslog

Description: settings for syslog support : OBJECT

Element	Type	Description
cellDataHistory	UINT	The number of days to keep cellular history in router.
enabled	BOOL	enable or disable syslog daemon (default:false)
ethDataHistory	UINT	The number of days to keep ethernet history in router.
ipAddress	STRING	ip address of syslog server
logLevel	UINT	level of debug output to log, 20(warning), 30(info), 50(debug), 60(trace) or 100(maximum) (default:30)
outputToFile	BOOL	enable or disable syslog output to file (default:false)
saveDataLimit	UINT	Data limit in Mb to update the statistics.
saveTimeout	UINT	Timeout in seconds to update the statistics.
wifiDataHistory	UINT	The number of days to keep wifi history in router.

4.3.30 system

Description: system attributes : OBJECT

Element	Type	Description
capabilities	OBJECT	hardware capabilites
adc	BOOL	true if device supports analog inputs, otherwise false
bluetooth	BOOL	true if device supports bluetooth, otherwise false
din	BOOL	true if device supports digital inputs, otherwise false
dout	BOOL	true if device supports digital outputs, otherwise false
externalSerialPort	BOOL	true if device supports external serial port, otherwise false
flexibleSerialPort	BOOL	true if device supports flexible serial port, otherwise false
gps	BOOL	true if device supports gps, otherwise false
wifi	BOOL	true if device supports wifi, otherwise false
cmdtty	STRING	tty device to access used to issue at commands to radio
date	STRING	current system date
datetime	STRING	current system date and time
dbDirty	BOOL	true if is database in dirty state
defaultDeviceName	STRING	default name of device
deviceId	STRING	device id
deviceName	STRING	configured name of device
firmware	STRING	firmware version
firmwareDate	STRING	firmware built date
firstTimeSetup	BOOL	true if this is first run of device or has been reset to defaults
hardwareVersion	STRING	hardware version of device
imei	STRING	international mobile station equipment identity
imsi	STRING	international mobile subscriber identity
macAddress	STRING	mac address of ethernet port
macBluetooth	STRING	mac address of bluetooth module
macWifi	STRING	mac address of wifi module
memory	OBJECT	current memory stats
mode	STRING	system level mode of rcell (default:ROUTER)
oemId	STRING	configurable device id
permission	STRING	authorization level of the current user
ppptty	STRING	tty device used by ppp to make connections
productId	STRING	product id
radio	OBJECT	radio model number and type
carrier	STRING	current carrier providing cellular connectivity
code	STRING	radio model code number, H5, H6, EV3, C2, G3, LAT1, VW2 or LEU1
type	STRING	type of radio, GSM or CMDA
restartNeeded	BOOL	true if settings have been changed and a restart is needed to reflect those changes in services
time	STRING	current system time of device
uptime	STRING	time unit has been running
user	STRING	current logged in user
vendorId	STRING	Multi-Tech Systems
webTitle	STRING	configurable title to display in browser

4.3.31 users

Description: users collection for authentication : ARRAY

Element	Type	Description
name	STRING	name of user
password	STRING	current password (only used on password change)
newPassword	STRING	new password (only used on password change)
permission	STRING	permission level : ADMIN, USER, GUEST

4.3.32 waninfo

Description: information on WAN interfaces : OBJECT

Element	Type	Description
wans	ARRAY	list of WANs
available	BOOL	indicates whether or not the WAN is available
enabled	BOOL	indicates whether or not the WAN is enabled
gateway	STRING	gateway used by WAN
interface	STRING	network interface
ip	STRING	the ip address assigned to this interface
name	STRING	name of WAN
subnet	STRING	subnet of network
type	STRING	type of WAN

4.3.33 wanmngr

Description: settings for WAN management : OBJECT

Element	Type	Description
mode	STRING	WAN manager mode (default:'FAILOVER')
wans	ARRAY	WANs settings
interface	STRING	network interface
monitor	OBJECT	failover settings
active	OBJECT	active detection mode settings
hostname	STRING	host to connect to (default:'www.google.com')
icmpCount	UINT	number of pings to send. Minimum is 1, maximum is 200 (default:10)
tcpPort	UINT	port on host to connect to (default:80)
type	STRING	method to use for availability detection, ICMP or TCP (default:'ICMP')
checkInterval	UINT	set the failover check interval in seconds (default:300)
mode	STRING	set the failover availability detection mode (default:'ACTIVE')
priority	UINT	set the priority for WAN
weight	UINT	weight value is used for load balancing mode only

4.3.34 wifi

Description: settings for wi-fi services : OBJECT

Element	Type	Description
ap	OBJECT	wi-fi access point settings
beaconInterval	UINT	time in msec between beacon frames (default:100)
channel	STRING	wireless channel to use. Valid entries are 1-14 depending on country code or AUTO (default:AUTO)
countryCode	STRING	two character operating country code
dtimInterval	UINT	frames between delivery traffic indication messages for buffered multicast/broadcast data (default:1)
enabled	BOOL	enable or disable the wifi access point (default:false)
maxClients	UINT	Maximum number of clients to allow on the Access Point at any given time (default: 8)
networkMode	STRING	access point radio mode of operation. Valid entries are b, n, bg or bgn (default:bgn)
rtsThreshold	UINT	request to send threshold (default:2347)
security	OBJECT	wi-fi access point security settings
algorithm	STRING	algorithm to use with WPA modes. Valid entries are TKIP, AES or TKIP+AES (default:TKIP+AES)
mode	STRING	security mode for access point. Valid entries are NONE, WEP, WPA-PSK or WPA2-PSK (default:NONE)
psk	STRING	pre-shared key for client authentication
ssid	STRING	network SSID, may only contain alpha-numeric characters and symbols not including ?, ", $, [, \,] and + characters
client	OBJECT	wi-fi client settings
enabled	BOOL	enable or disable the wifi client (default:false)
mode	STRING	use the wifi interface as a WAN or LAN (default:WAN)
savedNetworks	ARRAY	list of network wi-fi client will use to find a connection
enabled	BOOL	enable or disable saved network when trying to connect
name	STRING	name of network
security	OBJECT	wi-fi client security settings
algorithm	STRING	algorithm to use with WPA modes. Valid entries are TKIP, AES or TKIP+AES (default:TKIP+AES)
mode	STRING	security mode (default:NONE)
password	STRING	password used to connect to network
psk	STRING	pre-shared key to connect to network
username	STRING	username used to connect to network
ssid	STRING	ssid of network
wpaConfig	OBJECT	settings gathered from wi-fi scan
networks	ARRAY	list of networks from last wifi scan

5 Statistics

The API supports collecting dynamic system data through its Statistics URL. This data is read-only. Every call actively collects the latest data associated with the selected stats element. For a list of pollable options, use a GET request on https://[rcell_ip]/api/stats.

Statistic Group	Description
bluetooth	Bluetooth statistics
dns	Current DNS servers
eth	Current Ethernet state
ethHistory	Ethernet statistics history
ethTotal	Ethernet statistics summary
gps	GPS NMEA and statistics
gre	GRE Tunnel statistics
ipsec	IPsec Interface statistics
lan	Local Area Network statistics
modbus	Modbus statistics
ppp	PPP statistics
pppHistory	PPP statistics history
pppTotal	PPP statistics summary
serial	Serial port statistics
service	Various service status
wlan	WiFi statistics
wlanHistory	WiFi statistics history
wlanTotal	WiFi statistics summary

Example Collecting latest PPP statistics:

```
GET https://192.168.2.1/api/stats/ppp

Status: HTTP/1.1 200 OK
{
  "code" : 200,
  "result" : {
   "areaCode" : "7D0E",
   "dnsServers" : [ "222.88.33.23" ],
   "ip" : "142.133.12.40",
   "link" : "PPP Link is up",
   "localIp" : "142.133.12.40",
   "mtu" : "1550",
   "number" : "14831268306",
   "remoteIp" : "192.168.202.0",
   "roaming" : false,
   "rssi" : "10",
   "rx" : {
     "bytes" : "102542",
     "dropped" : "0",
     "errors" : "0",
     "frame" : "0",
     "overruns" : "0",
     "packets" : "797"
   },
   "tower" : "2802",
   "tx" : {
     "bytes" : "44841",
     "carrier" : "0",
     "collisions" : "0",
     "dropped" : "0",
     "errors" : "0",
     "overruns" : "0",
```

```
33      "packets" : "648",
34      "queueLength" : "3 "
35    },
36    "uptime" : 104603
37   },
38   "status" : "success"
39 }
```

5.1 dns

Description: current dns server ip addresses : ARRAY

Element	Type	Description
dhcpLease	ARRAY	array of dns servers issued to dhcp clients with lease
servers	ARRAY	array of dns servers available for domain name resolution

5.2 ethHistory

Description: daily statistics on ethernet interface traffic : ARRAY

Element	Type	Description
date	UINT	time stamp (in seconds)
todayRx	UINT	number of received bytes for a day
todayTx	UINT	number of transmitted bytes for a day

5.3 ethTotal

Description: total and today statistics on the ethernet interface traffic : OBJECT

Element	Type	Description
todayRx	UINT	number of received bytes for today
todayTx	UINT	number of transmitted bytes for today
totalRx	UINT	number of received bytes for the stored period
totalTx	UINT	number of transmitted bytes for the stored period

5.4 gps

Description: statistics and positional information of gps device : OBJECT

Element	Type	Description
alt	STRING	altitude
data	ARRAY	a list of NMEA data strings containing latest gps information
fix	STRING	fix quality (0=Invalid, 1=GPS fix, 2 = DGPS fix)
lat	STRING	latitude coordinate
lng	STRING	longitude coordinate
sats	STRING	number of satelites
time	STRING	time

5.5 gre

Description: statistics on gre tunnels (keys are tunnel names) : OBJECT

Element	Type	Description
tunnel	OBJECT	statistics on ipsec lan interface transmitted bytes
localIp	STRING	the ip address assigned to this interface
mode	STRING	tunnel mode
remoteIp	STRING	the ip address of the remote end of this tunnel
rx	OBJECT	statistics on gre tunnel received bytes
Mcasts	UINT	number of multicast packets received
bytes	UINT	number of received bytes
csumErrors	UINT	number of packets dropped because of checksum failures
errors	UINT	number of received byte errors
outOfSequence	UINT	number of packets dropped because they arrived out of sequence
packets	UINT	number of received packets
ttl	STRING	time to live (specified in seconds or inherited)
tx	OBJECT	statistics on gre tunnel transmitted bytes
bytes	UINT	number of transmitted bytes
deadLoop	UINT	number of packets which were not transmitted because the tunnel is looped back to itself
errors	UINT	number of transmitted errors
noBuffs	UINT	number of packets which were not transmitted because the kernel failed to allocate a buffer
noRoute	UINT	number of packets which were not transmitted because there is no IP route to the remote endpoint
packets	UINT	number of transmitted packets

5.6 ipsec

Description: statistics on ipsec interfaces : OBJECT

Element	Type	Description
ipsec0	OBJECT	statistics on ipsec lan interface
ip	STRING	the ip address assigned to this interface
mtu	STRING	maximum transmission unit in bytes
rx	OBJECT	statistics on ipsec lan interface received bytes
bytes	STRING	number of received bytes
dropped	STRING	number of received byte drops
errors	STRING	number of received byte errors
frame	STRING	number of received frames
overruns	STRING	number of received overruns
packets	STRING	number of received packets
tx	OBJECT	statistics on ipsec lan interface transmitted bytes
bytes	STRING	number of transmitted bytes
carrier	STRING	number of transmitted carriers
collisions	STRING	number of transmitted collisions
dropped	STRING	number of transmitted drops
errors	STRING	number of transmitted errors
overruns	STRING	number of transmitted overruns
packets	STRING	number of transmitted packets
queueLength	STRING	number of packets that can be queued for transmission
ipsec1	OBJECT	statistics on ipsec wan interface
ip	STRING	the ip address assigned to this interface
mtu	STRING	maximum transmission unit in bytes
rx	OBJECT	statistics on ipsec lan interface received bytes
bytes	STRING	number of received bytes
dropped	STRING	number of received byte drops
errors	STRING	number of received byte errors
frame	STRING	number of received frames
overruns	STRING	number of received overruns
packets	STRING	number of received packets
tx	OBJECT	statistics on ipsec lan interface transmitted bytes
bytes	STRING	number of transmitted bytes
carrier	STRING	number of transmitted carriers
collisions	STRING	number of transmitted collisions
dropped	STRING	number of transmitted drops
errors	STRING	number of transmitted errors
overruns	STRING	number of transmitted overruns
packets	STRING	number of transmitted packets
queueLength	STRING	number of packets that can be queued for transmission

5.7 lan

Description: statistics on local area network : OBJECT

Element	Type	Description
ip	STRING	the ip address assigned to this interface
mtu	STRING	maximum transmission unit in bytes
rx	OBJECT	statistics on local area network received bytes
bytes	STRING	number of received bytes
dropped	STRING	number of received byte drops
errors	STRING	number of received byte errors
frame	STRING	number of received frames
overruns	STRING	number of received overruns
packets	STRING	number of received packets
tx	OBJECT	statistics on local area network transmitted bytes
bytes	STRING	number of transmitted bytes
carrier	STRING	number of transmitted carriers
collisions	STRING	number of transmitted collisions
dropped	STRING	number of transmitted drops
errors	STRING	number of transmitted errors
overruns	STRING	number of transmitted overruns
packets	STRING	number of transmitted packets
queueLength	STRING	number of packets that can be queued for transmission

5.8 modbus

Description: statistics on modbus passthrough pipe : ARRAY

Element	Type	Description
id	UINT	identification of device on bus
rx	UINT	number of bytes received by device
status	STRING	status of device
time	UINT	seconds since last activity
tx	UINT	number of bytes transmitted by device

5.9 ppp

Description: statistics on ppp interface : OBJECT

Element	Type	Description
areaCode	STRING	identification code of area
dnsServers	ARRAY	an array of strings representing ip addresses of DNS servers
ip	STRING	the ip address assigned to this interface
link	STRING	status of the link
localIp	STRING	the ip address assigned to this interface
mtu	STRING	maximum transmission unit in bytes
number	STRING	cellular phone number
remoteIp	STRING	the externally facing ip address of this interface
roaming	BOOL	indicates whether or not this connection is considered roaming
rssi	STRING	a value representing signal strength [0-31]
rx	OBJECT	statistics on ppp interface received bytes
bytes	STRING	number of received bytes
dropped	STRING	number of received byte drops
errors	STRING	number of received byte errors
frame	STRING	number of received frames
overruns	STRING	number of received overruns
packets	STRING	number of received packets
tower	STRING	tower identification number
tx	OBJECT	statistics on ppp interface transmitted bytes
bytes	STRING	number of transmitted bytes
carrier	STRING	number of transmitted carriers
collisions	STRING	number of transmitted collisions
dropped	STRING	number of transmitted drops
errors	STRING	number of transmitted errors
overruns	STRING	number of transmitted overruns
packets	STRING	number of transmitted packets
queueLength	STRING	number of packets that can be queued for transmission
uptime	UINT	number of minutes connection has been established

5.10 pppHistory

Description: daily statistics on ppp interface traffic : ARRAY

Element	Type	Description
date	UINT	time stamp (in seconds)
todayRx	UINT	number of received bytes for a day
todayTx	UINT	number of transmitted bytes for a day

5.11 pppTotal

Description: total and today statistics on the ppp interface traffic : OBJECT

Element	Type	Description
todayRx	UINT	number of received bytes for today
todayTx	UINT	number of transmitted bytes for today
totalRx	UINT	number of received bytes for the stored period
totalTx	UINT	number of transmitted bytes for the stored period

5.12 radio

Description: statistics and information about the cellular radio : OBJECT

Element	Type	Description
carrier	STRING	cellular service provider (home network)
channel	STRING	ARFCN or UARFCN Assigned Radio Channel
cid	STRING	Cellular ID in HEX
code	STRING	MTS short model code [H5, H6, G3]
datetime	STRING	tower's date, time, and timezone. format MM/DD/YY HH:MM:SS GMT
debug	OBJECT	detailed information about the radio's current status (information may vary between radio types)
abnd	STRING	Active Band
bler	STRING	Block Error Rate (percentage)
drx	STRING	Discontinuous reception cycle length (ms)
ecio	STRING	Active Ec/Io (chip energy per total wideband power in dBm)
mm	STRING	Mobility Management State
nom	STRING	Network Operator Mode
psc	STRING	Primary Synchronization Code
rr	STRING	Radio Resource State
rscp	STRING	Active RSCP (Received Signal Code Power in dBm)
sd	STRING	Service Domain
txpwr	STRING	Transmit Power
firmware	STRING	radio firmware version
hardware	STRING	radio hardware revision
iccid	STRING	Integrated Circuit Card Identifier (Not available for CMDA)
imsi	STRING	International Mobile Subscriber Identity (Not Available on CDMA)
lac	STRING	Location Area Code in HEX
manufacturer	STRING	radio manufacturer
mcc	STRING	Mobile Country Code
mdn	STRING	Mobile Directory Number
meid	STRING	Mobile Equipment Identifier (CDMA Only)
mipProfile	OBJECT	Mobile IP configuration (CDMA Only)
enabled	BOOL	Indicates if this profile is active or not
homeAddress	STRING	Home Address
id	UINT	MIP Profile ID
mnAaaSpi	STRING	Mobile Node Authentication, Authorization, and Accounting Server Security Parameter Index
mnAaaSs	BOOL	Whether or not the Mobile Node Authentication, Authorization, and Accounting Server Shared Secret has been set
mnHaSpi	STRING	Mobile Node Home Agent Security Server Parameter Index
mnHaSs	BOOL	Whether or not theMobile Node Home Agent Shared Secret has been set
nai	STRING	Network Access Identifier
primaryHa	STRING	Primary Home Agent
revTun	BOOL	Reverse Tunneling Enabled
secondaryHa	STRING	Secondary Home Agent
mnc	STRING	Mobile Network (Operator) Code
model	STRING	radio model [HE910-D, HE910-EUD, GE910, DE910, CE910, ...]
msid	STRING	Mobil Station ID aka MIN aka MSIN
network	STRING	current cellular service provider (Not available for CDMA)
provisioned	BOOL	Whether or not the radio has been activated with a data account (CDMA only)
rac	STRING	Routing Area Code in HEX
roaming	BOOL	indicates whether or not using Home Network
rssi	UINT	Received Signal Strength Indication
rssidBm	STRING	Received Signal Strength Indication in dBm
service	STRING	service connection type [GPRS, EGPRS, WCDMA, HSDPA]
type	STRING	radio technology category [GSM, CDMA, LTE]

5.13 serial

Description: statistics on serial interface : OBJECT

Element	Type	Description
dcd	STRING	status of dcd
rx	UINT	number of bytes received on serial interface
tx	UINT	number of bytes transmitted on serial interface

5.14 service

Description: status on various services : OBJECT

Element	Type	Description
ddns	OBJECT	status on ddns services
enabled	BOOL	indicates whether or not service is employed
status	STRING	status of ddns
dialOnDemand	OBJECT	status on dial-on-demand services
enabled	BOOL	indicates whether or not service is employed
status	STRING	status of dial-on-demand
keepAlive	OBJECT	status on keep-alive services
enabled	BOOL	indicates whether or not service is employed
status	STRING	status of keep-alive
sntp	OBJECT	status on sntp services
enabled	BOOL	indicates whether or not service is employed
status	STRING	status of sntp

5.15 status

Description: a list of important system events : ARRAY

Element	Type	Description
guid	STRING	unique traceable identifier of the event source
msg	STRING	the message describing the event
timestamp	STRING	the time when the event occured (UTC)
type	STRING	the event classification [INFO, WARNING, ERROR]

5.16 wlan

Description: statistics on wlan interface : OBJECT

Element	Type	Description
channels	ARRAY	array of available channels
countryCode	STRING	code used to assign wifi hardware to use country's authorized frequencies
ip	STRING	the ip address assigned to this interface
link	STRING	status of the wifi link
mtu	STRING	maximum transmission unit in bytes
rx	OBJECT	statistics on wifi interface received bytes
bytes	STRING	number of received bytes
dropped	STRING	number of received byte drops
errors	STRING	number of received byte errors
frame	STRING	number of received frames
overruns	STRING	number of received overruns
packets	STRING	number of received packets
tx	OBJECT	statistics on wifi interface transmitted bytes
bytes	STRING	number of transmitted bytes
carrier	STRING	number of transmitted carriers
collisions	STRING	number of transmitted collisions
dropped	STRING	number of transmitted drops
errors	STRING	number of transmitted errors
overruns	STRING	number of transmitted overruns
packets	STRING	number of transmitted packets
queueLength	STRING	number of packets that can be queued for transmission

5.17 wlanHistory

Description: daily statistics on wlan interface traffic : ARRAY

Element	Type	Description
date	UINT	time stamp (in seconds)
todayRx	UINT	number of received bytes for a day
todayTx	UINT	number of transmitted bytes for a day

5.18 wlanTotal

Description: total and today statistics on the wlan interface traffic : OBJECT

Element	Type	Description
todayRx	UINT	number of received bytes for today
todayTx	UINT	number of transmitted bytes for today
totalRx	UINT	number of received bytes for the stored period
totalTx	UINT	number of transmitted bytes for the stored period

6 Appendix

6.1 REST Architecture

A REST (Representational State Transfer) architecture is a style for interacting with distributed systems and is commonly used in websites. There are four methods to REST: POST, GET, PUT, and DELETE. These actions expose the four basic functions of persistent storage: Create, Read, Update, and Delete (CRUD). The responses to these RESTful actions can be returned in various formats. A RESTful JSON API responds to REST requests with JSON.

6.2 JSON Data

JSON (JavaScript Object Notation) is a text-based human-readable data interchange that represents simple data structures and associative arrays.

6.3 Examples

6.3.1 Using Curl to log in

```
curl -k "https://192.168.2.1/api/login?username=admin&password=admin"
```

Curl result:

```
{
   "code" : 200,
   "result" : {
      "address" : "192.168.2.103",
      "permission" : "admin",
      "port" : "52222",
      "timestamp" : "14:30:5:957",
      "token" : "2442CB0CB60B2EE9F5A35DF5ED8C33",
      "user" : "admin"
   },
   "status" : "success"
}
```

Verbose Curl result:

```
* About to connect() to 192.168.2.1 port 443 (#0)
*   Trying 192.168.2.1... connected
* successfully set certificate verify locations:
*   CAfile: none
  CApath: /etc/ssl/certs
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using ECDHE-RSA-AES256-SHA
* Server certificate:
*    subject: C=US; ST=Minnesota; L=Minneapolis; CN=rcell.example.com
*    start date: 2013-05-01 16:31:06 GMT
```

```
*     expire date: 2014-05-01 16:31:06 GMT
*     issuer: C=US; ST=Minnesota; L=Minneapolis; CN=rcell.example.com
*     SSL certificate verify result: self signed certificate (18), continuing anyway.
> GET /api/login?username=admin&password=admin HTTP/1.1
> User-Agent: curl/7.22.0 (x86_64-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4
    libidn/1.23 librtmp/2.3
> Host: 192.168.2.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Set-Cookie: token=5810A57DF87328951FF1901027A09A74; Max-Age=300; Path=/; Secure
< Cache-Control: no-cache
< Content-type: application/json
< Transfer-Encoding: chunked
< Date: Wed, 15 Jan 2014 14:56:09 GMT
< Server: rcell
<
{
   "code" : 200,
   "result" : {
      "address" : "192.168.2.103",
      "permission" : "admin",
      "port" : "43516",
      "timestamp" : "14:56:9:363",
      "token" : "5810A57DF87328951FF1901027A09A74",
      "user" : "admin"
   },
   "status" : "success"
}
* Connection #0 to host 192.168.2.1 left intact
* Closing connection #0
* SSLv3, TLS alert, Client hello (1):
```

6.3.2 Using Curl to enable PPP

```
curl -k -X PUT -H "Content-Type: application/json" -d '{
 "enabled" : true,
}' https://192.168.2.1/api/ppp?token=2442CB0CB60B2EE9F5A35DF5ED8C33
```

Curl result:

```
{
   "code" : 200,
   "status" : "success"
}
```

6.3.3 Using Curl to add a firewall DNAT rule

```
curl -k -X POST -H "Content-Type: application/json" -d '{
 "description" : "",
 "direction" : "INGRESS",
 "enabled" : true,
 "guid" : "FTP-SERVER-DNAT",
 "lanIp" : "192.168.2.103",
 "lanPortEnd" : 21,
 "lanPortStart" : 20,
 "name" : "FTP-SERVER",
 "protocol" : "TCP",
 "type" : "DNAT",
 "wanIp" : "ANY",
 "wanMask" : 32,
 "wanPortEnd" : "21",
 "wanPortStart" : "20"
}' https://192.168.2.1/api/nat?token=2442CB0CB60B2EE9F5A35DF5ED8C33
```

Curl result:

```
{
   "code" : 200,
   "status" : "success"
}
```

6.3.4 Using Curl to add a firewall filter rule

```
curl -k -X POST -H "Content-Type: application/json" -d '{
 "action" : "ACCEPT",
 "description" : "",
 "direction" : "INGRESS",
 "dstIp" : "192.168.2.103",
 "dstMask" : 32,
 "dstNetwork" : "",
 "dstPortEnd" : 21,
 "dstPortStart" : 20,
 "enabled": true,
 "name" : "FTP-SERVER",
 "protocol" : "TCP",
 "srcIp" : "ANY",
 "srcMask" : 32,
 "srcMac" : "",
 "srcNetwork" : "",
 "srcPortEnd" : "ANY",
 "srcPortStart" : "ANY"
}' https://192.168.2.1/api/filters?token=2442CB0CB60B2EE9F5A35DF5ED8C33
```

Curl result:

```
{
   "code" : 200,
   "status" : "success"
}
```

6.3.5 Using Curl to delete a firewall filter rule by name

```
curl -k -X DELETE
"https://192.168.2.1/api/filters/FTP-SERVER?token=2442CB0CB60B2EE9F5A35DF5ED8C33
```

Curl result:

```
{
   "code" : 200,
   "status" : "success"
}
```

6.3.6 Using Curl to delete a firewall filter rule by index

```
curl -k -X DELETE
"https://192.168.2.1/api/filters/0?token=2442CB0CB60B2EE9F5A35DF5ED8C33
```

Curl result:

```
{
   "code" : 200,
   "status" : "success"
}
```

6.3.7 Using Curl to save current configurations and reboot

```
curl -k -X POST -d ""
"https://192.168.2.1/api/command/save_restart?token=2442CB0CB60B2EE9F5A35DF5ED8C33"
```

Curl result:

```
{
   "code" : 200,
   "status" : "success"
}
```