

IP Protocol Config (Continued...)

VIP4G/VIP4Gb

SMS Transparent Mode: Serial data from the COM1 port can be send to one or multiple destinations via SMS text messaging. SMS messages received by the VIP4G can also be sent to the COM1 port.

Message Max Size	160		[1160]
Reply Timeout(s)	10		[165535] default: 10
Access Control	Anonymous	•	
Read SMS Control	Delete	•	
Example: +1403xxxxxx	¢ .		
Example: +1403xxxxxx Phone Number 1	+15878938644		
Example: +1403xxxxxx Phone Number 1 Phone Number 2	+15878938644		
Example: +1403xxxxxx Phone Number 1 Phone Number 2 Phone Number 3	+15878938644		
Example: +1403xxxxxx Phone Number 1 Phone Number 2 Phone Number 3 Phone Number 4	+15878938644		

Image 4-5-3: Comport > SMS Transparent Mode

- Message Max Size
 Enter the maximum message size. Once the number of characters has been reached the VIP4G will package the data up and send it as a SMS message to the number(s) specified.
 [1....160]. The character timeout can be used to send messages more frequently by detecting a pause in the incoming data.
 Default: 160
 - Reply Timeout(s)
 Enter a value for the Reply Timeout in seconds.
 Default: 10
 - Access Control By selecting Anonymous, the VIP4G will accept a SMS message from any number. If Control Phone List is selected, only messages from the numbers in the Access Control List will be accepted. Default: Anonymous
 - Read SMS Control Select Keep in SIM Card to save incoming SMS messages in the SIM card, select Delete to delete messages once they have been output to serial port. Default: Keep in SIM Card
- Access Control Phone List Messages can be sent to up to five (5) numbers, also, this list can be used to filter incoming SMS messages (See Access Control) Default: None



IP Protocol Config (Continued...)

GPS Transparent Mode: When in GPS Transparent Mode, GPS data is reported out the serial port at 1 second intervals. Sample output is shown below:



Image 4-5-4: Comport > GPS Transparent Mode



4.6 I/O

4.6.1 I/O > Status

The VIP4G has 4 status inputs, which can be used with various alarms and sensors for monitoring, telling the modem when certain events have occurred, such as an intrusion alarm on a door, a temperature threshold has been exceed, or a generator has failed, out of fuel. Also included are 4 outputs, that can be used to drive external relays to remotely control equipment and devices.

			/								_
	mi	crol	hard	SYSTE	MS II	NC.	1010	1011	27	01	01
System	Network	Carrier	Wireless	Comport	1/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Status 0	ОТРОТ	I/O Rules	Accelero	meter							
I/O Status	6										
INPUT STA	TUS										
INPUT	1		Open								
INPUT	2		Open								
INPUT	3		Open								
INPUT	4		Open								
OUTPUT S	TATUS										
OUTPU	T I		Open								
OUTPU	T 2		Close								
OUTPU	T 3		Open								
OUTPU	T 4		Close								

Image 4-6-1: I/O > Status

Input Status

The WebUI will display the current state of each input. The I/O pins are all normally open so an open status indicates that there is nothing connected to the input pins, or that an event has not occurred to trigger the input. The inputs have a small wetting current (Vin) used to detect a contact closure, and prevent false readings by any noise or intermittent signals, it has a threshold sensitivity of 1.8V.

Output Status

The WebUI will display the current state of each control output. Using the Output menu discussed in the next section, a user can remotely control the status of the output pins.



4.6.2 I/O > OUTPUT

Each of the 4 Outputs can be controlled separately, allowing a user to remotely trigger an event.

System Network	Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Status OUTPUT	I/O Rules	Accelero	meter							
OUTPUT Configurat	ion									
OUTPUT 1		Open Cl	ose							
OUTPUT 2		Open Cl	ose							
OUTPUT 3		Open Cl	ose							
OUTPUT 4		Open Cl	ose							

Image 4-6-2: I/O > OUTPUT

The output pins on the VIP4G can be used provide output signals, which can be used to drive an external relay to control an external device. Maximum recommended load for the Output Pin is 150mA @ 32 VDC (Vin)

4.6.3 I/O > I/O Rules

Custom rules can be applied to the I/O behavior, such as setting a output after a specified time, or an input or combination of inputs triggering output(s).

System Network Carrier	Wireless Compor	rt 1/0	GPS Fi	irewall	Router	VPN	MultiWAN	Tools
Status OUTPUT I/O Rules	Accelerometer							
I/O Rules								
I/O Rules Configuration								
I/O Port Rule Define	User Custom Rules 🔻							
RULE NAME	rule0							
I/O RULE MODE:	Use Timer Only	•						
	1	Seconds						
INPUT EVENT:								
INPUT 1	Open Close							
INPUT 2	Open Close							
INPUT 3	Open Oclose							
INPUT 4	Open Oclose							
ACTION TO OUTPUT:								
OUTPUT 1	● n/a [©] Open [©] Close							
OUTPUT 2	● n/a Open Close							
OUTPUT 3	● n/a ◎ Open ◎ Close							
OUTPUT 4	● n/a [©] Open [©] Close							
	Add To I/O RULE LIST							
I/O RULE LIST								
Name Rule Mode Expirat	tion Time Input1	Input2 In	put3 Inp	out4 Outp	outl Ou	tput2	Output3 O	utput4

Image 4-6-3: I/O > I/O Rules



I/O Port Rule Define

Values (selection)

Disable Default Rules

Custom Rules

Set the type of I/O rules to perform:

Disabled: Outputs have no logical connection to inputs.

Default Rules: Each input has a logical connection to each output as follows: Input 1 -> Output 1 Input 2 -> Output 2 Input 3 -> Output 3 Input 4 -> Output 4

Custom Rules:

User can make custom rules to trigger output states. Custom rules can contain any of the following I/O rules:

- A timer has finished counting down
- A input signal has changed state
- A combination of a input state and a timer.

	Rule Name
Each I/O rule must have a unique name. This is for reference purposes and	Values (characters)
	rule0

Define the parameters of the desired rule:

Use Timer Only: Once the programmed timer has expired, the defined output state will be triggered.

Use Input States Only: The VIP4G will set puts as defined based on input states.

Use Input States With Timer: A combination of inputs states and a timer would trigger an output action when the input state if changed for more than the specified time.

I/O Rule Mode

Values (selection)

Use Timer Only Use Input States Only Use Input States With Timer



4.6.4 I/O > Accelerometer

The VIP4G has a internal Accelerometer, which can be configured to report events to a remote host based on a specific physical activity.

System Network Carrie	er Wireless Compo	rt I/O GPS	Firewall	Router	VPN	MultiWAN	Tools
Status OUTPUT I/O Ru	es Accelerometer						
Accelerometer Report							
Report Configuration							
Accelerometer Report	Enable •						
Report Trigger Mode	Event •						
Interval Time(s)	120	[0~65535]					
Report Messsage	🗹 All 🔲 Impact 🗐 Activit	ty 🔲 Inactivity					
Report Format Type	TAIP •						
Remote IP	0.0.0.0	0.0.0.0					
Remote PORT	20100	[0 ~ 65535]					

Image 4-6-4: I/O > Accelerometer

	Accelerometer Report
Enable or disable reporting by the Accelerometer.	Values (selection)
	Disable Enable
	Report Trigger Mode
Select reporting on event, timer or both.	Values (selection)
	Event Timer Event OR Timer
	Interval
Set the time at which events will be reported if the timer feature is selected	Interval Values (seconds)
Set the time at which events will be reported if the timer feature is selected	Interval Values (seconds) 120
Set the time at which events will be reported if the timer feature is selected	Interval Values (seconds) 120 Report Message
Set the time at which events will be reported if the timer feature is selected Select the types of events that cause a report to be sent.	Interval Values (seconds) 120 Report Message Values (selection)



	Report Format Type
Select the format in which the report will be sent, TAIP or Text.	Values (selection)
	TAIP Text
	Remote IP
Enter the IP Address of the remote host. This is the address in	Values (IP Address)
which the reports will be sent via UDP packets.	0.0.0.0
	Remote PORT
Enter the UDP port number to send the reports.	Values (Port)
	20100



4.7 GPS

4.7.1 GPS > Location

Location Map

The location map shows the location on the VIP4G. The unit will attempt to get the GPS coordinates from the built in GPS receiver, and if unsuccessful, will use the Cell ID location reported by the Cellular Carrier.



Image 4-7-1: GPS > Location Map

When using standalone GPS the specific coordinates are shown as in the above screenshot. If the VIP4G is unable to locate GPS satellites, or if configured to use Embedded Carrier GPS, only the estimated location of the VIP4G is shown with a radius drawn on the map.



4.7.2 GPS > Settings

The VIP4G can be polled fro GPS data via GPSD standards and/or provide customizable reporting to up to 4 different hosts using UDP or Email Reporting.

GPS data can also be reported to the COM1 serial port. For more information, refer to the COM1 > IP Protocol Config > GPS Transparent Mode section.

System	Network	Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Location	Settings	Report	GpsGate	Recorder	Load	Record	TAIP				
GPS Servi Settings	ce Configura Option:	ation									
GPS S	tatus		Enable *								
CPS	Source		Standalone G	PS •							
TCP	Port		2947)	[0-65535]	(Default					
TCr	run.		2947)								

Image 4-7-2: GPS > Settings

	GPS Status
Enable or disable the GPS polling function of the VIP4G.	Values
	Disable / Enable
	GPS Source
Select the data source for GPS data.	Values
	Stand Alone GPS Embedded Carrier GPS
	TCP Port
Specify the TCP port on the VIP4G where the GPS service is running and	Values
Terriole systems can connect and poir for GFSD data.	2947



4.7.3 GPS > GPS Report

The VIP4G can provide customizable reporting to up to 4 hosts using UDP or Email Reporting.

System	Network	Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
ocation	Settings	Report	GpsGate	Recorder	Load	Recon	d TAIP				
GPS Repo	ort Configura	tion									
GPS Repo	ort No.1										
Repo	rt Define		UDP Report	•							
Time	e Interval		600	(5)						
Mes	sage 1		ALL NMEA	•							
Mes	sage 2		None								
Mes	sage 3		None	•							
Mes	sage 4		None								
Trig	ger Set		Only Timer								
Loca	I Streaming		Disable		•						
UDP	Remote IP		0.0.0								
UDP	Remote PORT		20175	[(~65535	1					
GPS Repo	ort No.2										
Repo	rt Define		Email Report								
Time	e Interval		600	(5)						
Mes	sage 1		ALL NMEA	۲							
Mes	sage 2		None	•							
Mes	sage 3		None								
Mes	sage 4		None	•							
Trig	ger Set		Only Timer								
Mail	Subject		GPSReportMe	essage2							
Mail	Server(IP/Nam	e)	smtp.gmail.co	m:465 ()	xx:port	1					
User	Name		@gmail.com								
Pass	word										
Auth	entication 0		None	•							
Mail	Recipient		host@	6	x@xx.x	x)					
GPS Repo	ort No.3										
Repo	rt Define		Disable	•							
GPS Repo	ort No.4										
Repo	rt Define		Disable	•							

Image 4-7-3: GPS > GPS Report

	Report Define
Enable UDP and/or Email or disable GPS Reporting. Up to 4 reports can	Values (selection)
	Disable UDP Report Email Report
	Time Interval
The interval timer specifies the frequency at which the GPS data is	Values (seconds)
reponed in seconds.	600



The Message field allows customization of up to 4 different GPS messages to be sent to the specified host. Values (None - Message is not used, no data will be sent None ALL - Sends all of the below GGA GGA - GPS Fix Data GSA GSA - Overall Satellite Data GSV GSV - Detailed Satellite Data RMC RMC - Recommended Min Data for GPS VTG VTG - Vector Track & Ground Speed Latitude/Log GPSGate - For use with GPSGate Tracking Software GPSGate	selection A ngitude JDP Protoc
NoneNoneNone-Message is not used, no data will be sentALL NME./ALL-Sends all of the belowGGAGGA-GPS Fix DataGSAGSA-Overall Satellite DataGSVGSV-Detailed Satellite DataRMCRMC-Recommended Min Data for GPSVTGVTG-Vector Track & Ground SpeedLatitude/LotGPSGate -For use with GPSGate Tracking SoftwareGPSGate	A Ingitude JDP Protoc
	Trigge
The trigger condition defines the conditions that must be met before a GPS Values (selection
trigger conditions must be met before an update is sent. The AND conditions be met before an update is sent. The Distance trigger Timer AND the Distance tr	r) Distance Distance
	Distance
The distance parameter allows the GPS data to only be sent when a Values (meters)
1000	
UDP Rem	ote IP /
This is the IP Address and port of the remote host in which the UDP Values (Address/F
0.0.0.0 / 20)175
	Mail Sub
If an Email report is chosen, the subject line of the Email can be defined Values (characte
1000	
	Mail Se
If an Email report is to be sent, the outgoing mail server must be defined, Values (Address:p
and the port number.	il.com:465
Sintegina	
Username	/ Passv
Some outgoing mail servers required username and password to prevent Values (e / Passv characte
Some outgoing mail servers required username and password to prevent an account being used for spam. Enter the login credentials here.	/ Passv characte / passwor
Some outgoing mail servers required username and password to prevent an account being used for spam. Enter the login credentials here.	e / Passv characte / passwor ail Recip
Some outgoing mail servers required username and password to prevent Values (Username and password to prevent Username Markov Some outgoing mail servers require a username and password to prevent Values (Username Markov Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some outgoing mail servers require a username and password to prevent Values (Username Some Outgoing mail servers require a username and password to prevent Values (Username Some Outgoing Markov Some Outgoi	e / Passv characte / passwor ail Recip characte



4.7.4 GPS > GpsGate

The VIP4G is compatible with *GpsGate - GPS Tracking Software*, which is a 3rd party mapping solution used for various GPS services including vehicle and asset tracking The VIP4G can communicate with GpsGate via Tracker Mode and TCP/IP. (UDP reporting can also send information to GpsGate, see the GPS > Report - UDP Reports)

System	Network	Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Location	Settings	Report	GpsGate	Recorder	Load	Record	і таір				
GpsGate	TrackerOne Co	onnection									
Tracker D	Device Setting										
Mode	Set		Enable Track	er Mode 🔹							
Serve	er Command Ch	annel	TCP and SMS	S •							
TCP	Alive Mode		_Ping Comma	and 🔻							
Alive	Time Interval		150	(s)						
Setu	p Phone Filter		Disable: Acce	ept All 🔻							
Moti	on Trigger		Enable Motion	Trigger T							
Send	IO Status		Disable	۲]						
When	n GPS Invalid, Se	nding Data	Not Use Last	Valid Position	•						

Image 4-7-4: GPS > GpsGate Tracker Mode

GpsGate - Tracker Mode

	Mode Set
Enable GpsGate Tracker Mode or TCP modes. In tracker mode The VIP4G	Values (selection)
connection is not available it will attempt to use SMS messaging.	Disable Enable Tracker Mode Enable TCP Send Mode
Serve	r Command Channel
By default VIP4G and GpsGate will use TCP and SMS to ensure	Values (seconds)
SMS communication only. Initial setup in Tracker mode must be via SMS.	TCP and SMS TCP Only SMS Only
TCP Alive Mode	/ Alive Time Interval
TCP alive mode will keep TCP connection alive if tracker is not enabled or the tracker interval is too long. The default is 150 seconds	Values (seconds)
	150



	Setup Phone Filter
A phone number filter can be applied to prevent SMS commands not	Values (selection)
intended for the VIP4G from being processed.	Disable: Accept All Enable Filter
	Motion Trigger
Use this parameter to enable or disable the motion trigger in the VIP4G.	Values (selection)
	Disable Enable Motion Trigger
	Send IO Status
When enabled, the VIP4G will send the current status of the Digital I/O	Values (selection)
	Disable Send Input Status Send Output Status Send Input&Output Status
When GPS I	nvalid, Sending Data

VIP4G/VIP4Gb

Not Use Last Valid Position Use Last Valid Position

GpsGate - TCP Mode

Mode Set	Enable TCP Send N	Node •
Server Address/IP	192.168.168.1	
Server Port	30175	
Server Interval	60	(s)
Motion Distance	100	(m)
Send IO Status	Disable	•

Image 4-7-5: GPS > GpsGate TCP Mode

	Mode
Enable GpsGate Tracker Mode or TCP modes. In TCP Mode the VIP4G	Values (selection)
SMS setup process. If the TCP connection is not available, the VIP4G will continue to try to connect every few seconds.	Disable Enable Tracker Mode Enable TCP Send Mode
	Server Address
Enter the IP Address of the server running the GpsGate application.	Values (IP Address
	192.168.168.1
	Server P
Enter the TCP Port of the server running the GpsGate application.	Values (Port)
	30175
	Server Inter
Define the interval at which the VIP4G will send data to the GpsGate	Values (seconds)
Server.	60
	Motion Distar
Set the motion threshold in which the VIP4G will be triggered to send	Values (meters)
IOCATION GATA.	100
	Send IO Stat
When enabled, the VIP4G will send the current status of the Digital I/O	Values (selection)
	Disable Send Input Status Send Output Status Send Input&Output Stat
When GPS	Invalid, Sending D
Specify what happens when the GPS data is invalid, either use the last valid position or do not use the last valid position.	Values (selection)

VIP4G/VIP4Gb

Not Use Last Valid Position Use Last Valid Position

4.7.5 GPS > Recorder

The VIP4G can be configured to record events based on time intervals, and/or an event trigger and store them in non-volatile memory. These events can then be viewed within the WebUI, on a map, or sent to a remote server in a number of different formats.

VIP4G/VIP4Gb

Location Settings Report	GpsGate	Recorder	Load Record	тар
GPS Recorder Service				
Current CPS Infomation				
current di 5 infontation				
Local Time:	Wed Mar 26	15:26:59 ME	DT 2014	
Satellites In View:	15			
Satellites tracked:	10			
Latitude:	51.142662,	N		
Longitude:	-114.07553	1,W		
Altitude:	1130.2			
Speed:	O(Km/h)			
Orientation:	0(Degree to	North)		
NMEA UTC Time:	26/03/201	4 21:26:59		
COC Descender Cambre				
Grs Recorder Setting				
Status	Enable GPS	Recorder •		
Record Feature Selections:	(Record iten	ns among 16,	000~36,000.)	
Time Interval	30	[30-	~65535](s)	
DI/DO Changed	Record	T		
Speed	Record	•		
Over Speed	120	[Mir	n 30](Km/h)	
Orientation	Record	T		
Orientation Changed	60	[5~	180](180:Disable)	
Carrier RSSI Level	Record	•		
Altitude	Record	•		

Image 4-7-6: GPS > GPS Recorder Service

	Status
Use the Status parameter to enable the GPS recording functionality of the VIP4G. The total number of records that can be recorded varies between	Values (selection)
16,000 and 36,000, depending on the number of GPS parameters that are recorded.	Disable Enable GPS Recorder
	Time Interval
Define the interval at which the VIP4G will record GPS data. If there is no	Values (seconds)
unit will wait until the next time valid information is received.	300
	DI/DO Changed
The VIP4G can detect and report the current GPS info when a digital input	Values (selection)
or output status changes, regardless of the time interval setting.	Record / Don't Record



	Speed
Select Record to include the current speed in the reported data.	Values (selection)
	Record / Don't Record
	Over Speed
Trigger a GPS record entry when the speed has exceeded the configured	Values (Km/hr)
theshold. A minimum of 30 Km/m is required.	120
	Orientation
Select Record to record the current orientation when a GPS entry is	Values (selection)
recorded. (Degree to North).	Record / Don't Record
	Orientation Changed
Record a GPS, regardless of the time interval, if the orientation of the unit	Orientation Changed Values (5 ~ 180)
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable)	Orientation Changed Values (5 ~ 180) 60
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable)	Orientation Changed Values (5 ~ 180) 60 Carrier RSSI Level
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable)	Orientation Changed Values (5 ~ 180) 60 Carrier RSSI Level Values (selection)
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable) Select Record to record the current 4G/Cellular RSSI level when a GPS entry is recorded. (-dB).	Orientation Changed Values (5 ~ 180) 60 Carrier RSSI Level Values (selection) Record / Don't Record
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable) Select Record to record the current 4G/Cellular RSSI level when a GPS entry is recorded. (-dB).	Orientation Changed Values (5 ~ 180) 60 Carrier RSSI Level Values (selection) Record / Don't Record Altitude
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable) Select Record to record the current 4G/Cellular RSSI level when a GPS entry is recorded. (-dB).	Orientation Changed Values (5 ~ 180) 60 Carrier RSSI Level Values (selection) Record / Don't Record Altitude Values (selection)

4.7.6 GPS > Load Record

Data that has been recorded and saved by the VIP4G can then be viewed or sent to a remote server in various formats. The data recorded can also be viewed directly by selecting "View Data" and the data can be traced on a map (internet access required), by selecting "Trace Map", or "Quick Trace". The screenshots below show the raw data that can be viewed and the Trace Map/Quick Trace output.

OVIP4G/VIP4Gb



Image 4-7-7: GPS > GPS Load Record



	Record Time Range
Check the boxes next to the records listed above that are to be sent to the	Values (selection)
	(no default)
S	Send Mode / Protocol
Specify the data format / protocol type for the data to be sent.	Values (selection)
	NMEA via UDP NMEA via TCP GpsGate via UDP GpsGate via TCP Plain Text via UDP Plain Text via TCP
	Server Address/IP
Enter the address or IP address of the remote server to which the data is to	Values (IP)
	nms.microhardcorp.com
	Server Port
Enter the UDP/TCP port number of the remote server to which the data is to be sent.	Values (Port)

30175



4.7.7 GPS > TAIP

The VIP4G has the ability to send GPS data in TAIP (Trimble ACSII Interface Protocol) format to up to 4 different TAIP servers. The following section describes the configuration parameters required to initialize TAIP reporting.

System	Network	Carrier	Wireless	Comport	1/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Location	Settings	Report	GpsGate	Recorder	Load	Record	TAIP				
TAIP Con	figuration										
Settings	No.1										
TAIP	service status		Enabled •								
Remo	te TAIP Server		0.0.0.0								
Socke	t Type		UDP .								
Remo	te TAIP Port		21000								
Messi	age Type		RPV ·								
Interv	al		5		(\$)						
Vehic	le ID		0000		4 alpha-r	numeric					
Settings	No.2										
TAIP	service status		Disabled *								
Settings	No.3										
TAIP	service status		Disabled •								
Settings	No.4										
TAIP	service status		Disabled •								

Image 4-7-8: GPS > TAIP

	TAIP service status
Enable or disable TAIP service on the VIP4G. The VIP4G can report TAIP to up to 4 different basts	Values (selection)
	Enable / Disable
	Remote TAIP Server
Enter the IP Address of the Remote TAIP Server.	Values (IP Address)
	0.0.0.0
	Socket Type
Select the socket type that is used by the Remote TAIP server. Select TCP or LIDP, this will define how the connection (TCP) or data is sent (LIDP) to	Socket Type Values (selection)
Select the socket type that is used by the Remote TAIP server. Select TCP or UDP, this will define how the connection (TCP) or data is sent (UDP) to the server.	Socket Type Values (selection) UDP / TCP
Select the socket type that is used by the Remote TAIP server. Select TCP or UDP, this will define how the connection (TCP) or data is sent (UDP) to the server.	Socket Type Values (selection) UDP / TCP Remote TAIP Port
Select the socket type that is used by the Remote TAIP server. Select TCP or UDP, this will define how the connection (TCP) or data is sent (UDP) to the server.	Socket Type Values (selection) UDP / TCP Remote TAIP Port Values (TCP/UDP)



	Message Type
Select between RPV and RLN message types.	Values (selection)
RPV - Position/Velocity RLN - Long Navigation Message	RPV / RLN
	Interval
Set the frequency at which TAIP messages are reported to the remote	Values (seconds)
	60
	Vehicle ID
Set the Vehicle ID using 4 alpha-numeric characters.	Values (chars)
	0000



4.8 Firewall

4.8.1 Firewall > Status

Firewall Status allows a user to see detailed information about how the firewall is operating. The All, Filter, Nat, Raw, and Mangle options can be used to view different aspects of the firewall.

Syste	m I	Netwo	ork Carrier	Wirel	ess	С	omport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Status	G	eneral	Rules Po	rt Forv	vardi	ing	MAC-	IP List	Rese	t				
Firew	all St	atus												
FILCW														
St	Status and Rules All V Check													
Targe	Target Filter													
Chair			CCEPT 0 analysis 0	(
chair	okte	(policy a	torget	bytes)	prot	ont	in	out		destination	ontions			
1	2753	188K	ACCEPT		all		*	*	0.0.0.0/0	0.0.0.0/0	state RELAT	ED.ESTABL	ISHED	
2	80	4158	ACCEPT		all		lo	ż	0.0.0/0	0.0.0/0				
3	72	3960	syn_flood		tcp		*	×	0.0.0.0/0	0.0.0.0/0	tcp flags:0)	(17/0x02		
4	2070	136K	input_rule		all		ż	*	0.0.0.0/0	0.0.0/0				
5	2070	136K	input		all		*	×	0.0.0.0/0	0.0.0.0/0				
Chair	FORW	ARD (pol	icy DROP 0 packets,	0 bytes)										
num	pkts	bytes	target		prot	opt	in	out	source	destination	options			
1	0	0	zone_wan3_MSSFIX		all		*	*	0.0.0.0/0	0.0.0/0				
2	0	0	zone_wan2_MSSFIX		all		ż	*	0.0.0.0/0	0.0.0/0				
3	0	0	zone_wan_MSSFIX		all	-	*	×	0.0.0.0/0	0.0.0/0				
4	0	0	ACCEPT		all		*	*	0.0.0.0/0	0.0.0/0	state RELAT	TED, ESTABL	ISHED	
5	0	0	forwarding_rule		all	-	*	*	0.0.0.0/0	0.0.0.0/0				
6	0	0	forward		all		*	×	0.0.0.0/0	0.0.0/0				
7	0	0	reject		all		*	*	0.0.0.0/0	0.0.0/0				
_														
Chair	OUTP	UT (polic	y ACCEPT 0 packets,	0 bytes)										
num	pets	Dytes 71.0K	target		prot	opt	in s	out	source	destination	options			
	2044	4159	ACCEPT		-11			- 1-	0.0.0.0/0	0.0.0.0/0	state RELA	IEU,ESTABL	ISHED	
-	75	15498	output rule		-11		*	*	0.0.0.0/0	0.0.0.0/0				
4	75	15498	output		all		ż	ż	0.0.0.0/0	0.0.0.0/0				
Chair	GRE_f	orward_c	hain (1 references)											
num	pkts	bytes	target		prot	opt	in	out	source	destination	options			
1	0	0	ACCEPT		all		tunnel_1	br-lan	0.0.0.0/0	0.0.0.0/0	state RELAT	ED, ESTABL	ISHED	
2	0	0	ACCEPT		all		br-lan	tunnel_1	0.0.0/0	0.0.0.0/0				
з	0	0	ACCEPT		all		tunnel_1	*	0.0.0.0/0	0.0.0.0/0				
Chair	GRE_i	nput_cha	in (1 references)											
num	pkts	bytes	target		prot	opt	in	out	source	destination	options			
1	0	0	ACCEPT		all		tunnel_1	ż	0.0.0.0/0	0.0.0.0/0				
2	0	0	ACCEPT		icm p		tunnel_1	*	0.0.0.0/0	0.0.0/0	icm p type ()		
3	0	0	ACCEPT		icm p		tunnel_1	*	0.0.0.0/0	0.0.0/0	icmp type 8	3		
4	0	0	ACCEPT		icm p		tunnel_1	*	0.0.0.0/0	0.0.0.0/0	icm p type 3	8		
5	0	0	zone_wan		all	-	tunnel_1	*	0.0.0.0/0	0.0.0/0				
6	0	0	ACCEPT		47		*	*	0.0.0.0/0	0.0.0.0/0				

Image 4-8-1: Firewall > Status

4.8.2 Firewall > General

The General Firewall settings allow users to enable or disable the firewall, and to decide which areas of the modem to protect. The Firewall can also be reset to factory defaults from this area of the WebUI.

010

VIP4G/VIP4Gb

In a cellular device such as this, it is highly recommended to configure the firewall to protect any devices connected to the modem, and to control data usage. This is especially important units set up with a public IP address as the modem is effectively on the public internet and is susceptible to a wide range of threats which may severely impact the data usage. This can be avoided by blocking all 4G/Cellular traffic and setting up specific rules to either open only used ports, or even restrict access to specific IP/networks.

System	Network C	arrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Status	General Rule	es Po	rt Forwardi	ng MAC-1	IP List	Rese	t				
Firewall	General										
Firewall	Mode Configuration	n									
Firev	wall Status		Enable •								
Firewall	General Configurat	ion									
WAN	Remote Managem	ent 0	Enable C	isable							
4G F	Remote Managemen	nt 😶	● Enable ◎ D	isable							
WAN	Request 0		Block Al	low							
4G F	Request 🕕		Block Al	ow							
LAN	to WAN Access Con	ntrol 0	Block Al	low							
LAN	to 4G Access Conti	rol 💿	Block Al	low							
Anti	-Spoof 🔍		🔍 Enable 🖲 🛙	isable							
Pack	et Normalization		🔍 Enable 🖲 🛛	bisable							



<u> </u>		Firewall Status
For best practices and to control data usage it is critical that the firewall be	When enabled, the firewall settings are in effect. When disabled, none of	Values
configured properly.	"open" to anyone.	Disable / Enable
all incoming 4G/Cellular traffic and create rules to	WAN	Remote Management
use ACL lists to limit incoming connections.	Allow remote management of the VIP4G on the WAN side using the WebUI on port 80(HTTP) and 443 (HTTPS). If disabled, the configuration can only	Values
	be accessed from the LAN (or 4G if enabled).	Enable / Disable
	4G	Remote Management
	Allow remote management of the VIP4G from the 4G side of using the WebLIL on port 80(HTTP) and 443 (HTTPS). If disabled, the configuration	Values
	can only be accessed from the LAN (or WAN if enabled).	Enable / Disable

have invalid flag combinations.

4.0 Configuration

		WAN Request
	When Blocked the VIP4G will block all requests from devices on the WAN	Values
When 4G is set to 'Allow' the modem is open to anyone, this is not recommended as it may impact data usage from unwanted sources.	configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the WAN Remote Management option.	Block / Allow
		4G Request
	When Blocked all requests from devices on the 4G (Wireless Carrier) side will be blocked, unless specified otherwise in the Access Rules, MAC List.	Values
	IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the 4G Remote Management option.	Block / Allow
impact data usage from unwanted sources.	LAN to	WAN Access Control
unwanted sources.	Allows or Blocks traffic from the LAN accessing the WAN unless specified otherwise using the Access Rules, MAC, and IP List configuration.	Values
		Block / Allow
	LAN	to 4G Access Control
	Allows or Blocks traffic from the LAN accessing the 4G connection unless specified otherwise using the Access Rules, MAC, and IP List	Values
	configuration.	Block / Allow
		Anti-Spoof
	The Anti-Spoof protection is to create some firewall rules assigned to the external interface (WAN & $4G(Cellular)$ of the firewall that examines the	Values
	source address of all packets crossing that interface coming from outside. If the address belongs to the internal network or the firewall itself, the packet is dropped.	Enable / Disable
		Packet Normalization
	Packet Normalization is the normalization of packets so there are no	Values
	scrub directive also reassembled fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that	Enable / Disable

VIP4G/VIP4Gb

4.8.3 Firewall > Rules

Once the firewall is turned on, rules configuration can be used to define specific rules on how local and remote devices access different ports and services. MAC List and IP List are used for general access, and are applied before rules are processed.

010

VIP4G/VIP4Gb

It is highly recommended to block as much traffic as possible from the modem, especially when using a public IP address. The best security would to be to allow traffic only from trusted IP addresses, and only the specific ports being used, and block everything else. Not configuring the firewall and the firewall rules correctly could result in unpredictable data charges from the cellular carrier.

System Networ	k Carrier	Wireless	Con	nport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Status General	Rules P	Port Forward	ing	MAC-II	P List	Rese	t				
Firewall Rules											
Firewall Rules Config	uration										
Rule Name	rule1										
ACTION	Accept •										
Source 🔍	None •										
Source IPs 🔍	192.168.0.0)	То	192.168	0.0						
Destination 0	None •										
Destination IPs	192.168.0.0)	То	192.168	0.0						
Destination Port	0										
Protocol	TCP ·										
Add Rule											
Firewall Rules Summ	ary										
Name Action	Src Src IP	From Src I	РТо	Dest	Dest IP	From	Dest IP T	o Des	tination Po	rt Pro	tocol

Image 4-8-3: Firewall > Rules

	Rule Name			
The rule name is used to identify the created rule. Each rule must have a	Values (10 Chars)			
unique name and up to to characters can be used.	characters			
	Action			
The Action is used to define how the rule handles the connection request.	Values (selection)			
ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.	ACCEPT DROP REJECT			
This is configured based on how the WAN/4G Request and LAN to WAN/4G Access Control are configured in the previous menus.				
	Source			
Select the zone which is to be the source of the data traffic. WAN applies to the WAN P 145 connection, and 4C refers to the connection to the	Values			
cellular carrier. The LAN refers to local connections on the VIP4G (Ethernet/WiFi).	LAN / 4G / WIFI / WAN None			



Refer to Appendix D for an example of how to set up a firewall to block all connections and then add access to only specific IP's and Ports.

<u>Appendix D: Firewall</u> <u>Example</u>

	Source IPs
Match incoming traffic from the specified source IP range. Boxes accept	Values (IP Address)
192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)	192.168.0.0 to 192.168.0.0
	Destination
Select the zone which is the intended destination of the data traffic. WAN	Values (selection)
to local connections on the VIP4G (Ethernet/WiFi)	LAN / 4G / WIFI / WAN None
	Destination IPs
Match incoming traffic from the specified destination IP range. Boxes	Values (IP Address)
to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)	192.168.0.0 to 192.168.0.0
	Destination Port
Match incoming traffic directed at the given destination port or port range.	Values (port)
(To specify a port range use a From:To (100:200) format)	0
	Protocol
The protocol field defines the transport protocol type controlled by the rule.	Values
	TCP UDP Both ICMP

VIP4G/VIP4Gb



4.8.4 Firewall > Port Forwarding

The VIP4G can be used to provide remote access to connected devices. To access these devices a user must define how incoming traffic is handled by the VIP4G. If all incoming traffic is intended for a specific connected device, DMZ could be used to simplify the process, as all incoming traffic can be directed towards a specific IP address.

VIP4G/VIP4Gb

In the case where there is multiple devices, or only specific ports need to be passed, Port forwarding is used to forward traffic coming in from the WAN (Cellular) to specific IP Addresses and Ports on the LAN. Port forwarding can be used in combination with other firewall features, but the Firewall must be enabled for Port forwarding to be in effect. If the WAN Request is blocked on the General Tab, additional rules and/ or IP Lists must be set up to allow the port forwarding traffic to pass through the firewall.

IP-Passthrough (Carrier > Settings) is another option for passing traffic through the VIP4G, in this case all traffic is passed to a single device connected to a RJ45 port on the VIP4G, The device must be set for DHCP or have the WAN IP set as its static IP, as the VIP4G assigns the WAN IP to the device, and the modem enters into a transparent mode, routing all traffic to the RJ45 port. This option bypasses all firewall features of the VIP4G, as well as all other features of the VIP4G such as COM, VPN, GPS etc.

System Network Car	rier Wireless (Comport I/O	GPS Firewall	Router	VPN	MultiWAN	Tools
Status General Rules	Port Forwarding	MAC-IP List	Reset				
Firewall Port Forwarding							
Notice							
Constrained by the off Stationed	110 (10	and the second second					
Port Forwarding Rules are	taken into consideratio	n after the General f	irewall				
rules must be created	wan and/or 40 cenula	r traffic is blocked, a	additional				
1. Add rules in the Rules c	onfiguration to open po	orts or allow IP addre	esses				
2. Create a IP/Mac List to a	allow desired connectio	ns.					
Firewall DMZ Configuration							
DMZ Mode	Disable •						
DMZ Source	4G •						
DMZ Server IP	192.168.100.100						
Exception TCP Port	0						
Exception UDP Port	0						
Firewall Port Forwarding Confi	auration						
Firewait Fort Forwarding Contr	guiation						
Name	forward1						
Source	4G 🔻						
Internal Server IP	192.168.2.1						
Internal Port	3000						
Protocol	TCP ·						
External Port	2000						
Add Port Forwarding							
Firewall Port Forwarding Summ	nary						
Number of Street	1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	hannel C. J.					
NAME SOURCE	internal IP						

Image 4-8-4: Firewall > Port Forwarding

	DMZ Mode
Enable or disable DMZ Mode. DMZ can be used to forward all traffic to a	Values (selection)
specific IP address (DIVIZ Server IP) on the LAN.	

Disable / Enable



If DMZ is enabled and an exception port for the WebUI is not specified, remote management will not be possible. The default port for remote management is TCP 80.



	DMZ Source
Select the source for the DMZ traffic, either 4G or from WAN.	Values (selection)
	4G / WAN
	DMZ Server II
Enter the IP address of the device on the LAN side of the VIP4G where all the traffic will be forwarded to	Values (IP Address)
	192.168.100.100
	Exception Por
Enter a exception port number that will NOT be forwarded to the DMZ	Values (Port #)
excluded to retain external control of the VIP4G.	443
	Nam
This is simply a field where a convenient reference or description is added to the rule. Each Forward must have a unique rule name and can use up to	Values (10 chars)
10 characters.	Forward
	Sourc
Select the source for the DMZ traffic, either 4G or from WAN.	Values (selection)
	4G / WAN
	Internal Server I
Enter the IP address of the intended internal (i.e. on LAN side of VIP4G)	Values (IP Address)
server. This is the IP address of the device you are forwarding trainc to.	192.168.2.1
	Internal Po
Target port number of internal server on the LAN IP entered above.	Values (Port #)
	3000
	Protoco
Select the type of transport protocol used. For example Telnet uses TCP,	Values (selection)
SNMF USES ODF, ElC.	TCP / UDP / Both
	External Po
Port number of incoming request (from 4G/WAN-side).	Values (Port #)
	2000

VIP4G/VIP4Gb

1010

0



If the firewall is set to block incoming traffic on the WAN and/or 4G interfaces, additional rules or IP/MAC lists must be configured to allow desired traffic access.



4.8.5 Firewall > MAC-IP List

MAC List configuration can be used to control which physical LAN devices can access the ports on the VIP4G, by restricting or allowing connections based on the MAC address. IP List configuration can be used to define who or what can access the VIP4G, by restricting or allowing connections based on the IP Address/Subnet.

MAC-IP List can be used alone or in combination with LAN to WAN/4G Access Control to provide secure access to the physical ports of the VIP4G.

System Network	Carrier	Wireless	Compor	t I/O	GPS	Firewall	Router	VPN	MultiWAN	Tools				
Status General	Rules Po	rt Forwardi	ng MAG	-IP List	Rese									
Firewall MAC/IP List	irewall MAC/IP List													
Firewall MAC List Cont	figuration													
Name		mac1												
Action		Accept •												
Mac Address		00:00:00:00:00	00:00											
Add Mac List														
Firewall IP List Configu	uration													
Name	ip1													
Action	Accept •													
Source 0	None •													
Source IPs 0	192.168.0.0		To 192	168.0.0										
Destination IPs 🕕	192.168.0.0		To 192	168.0.0										
Add IP List														
Firewall MAC List Sum	mary													
Name Acti	on Mad	Address												
Firewall IP List Summa	ry													
Name Acti	on Src	Src IP From		Src IP T	0	Dest IP F	rom		Dest IP To					

Image 4-8-5: Firewall > MAC-IP List

Firewall MAC List Configuration

	Rule Name		
The Rule Name field is required to give the rule a convenient name for	Values (10 chars)		
length.	MAC_List		
	MAC Addross		
	MAC AUDIESS		
Specify the MAC Address to be added to the list. Must be entered in the	Values (MAC Address)		

Firewall MAC List Configuration (Continued)			
	Action		
The Action is used to define how the rule handles the connection request.	Values (selection)		
ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.	ACCEPT DROP REJECT		
Firewall IP List Configuration			
	Rule Name		
The Rule Name field is required to give the rule a convenient name for	Values (10 chars)		
length.	IP_List		
	Action		
The Action is used to define how the rule handles the connection request.	Values (selection)		
ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.	ACCEPT / DROP / REJECT		
	Source		
Enter the specific zone that the IP List will apply to, 4G (Cellular), WAN,	Values (Selection)		
LAN (Ethernet, WIFI) or None (both).	LAN / WAN / / WIFI / 4G / NONE		
	Source Address		
Match incoming traffic from the specified source IP range. Boxes accept	Values (IP Address)		
192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)	192.168.0.0 to 192.168.0.0		
	Destination Address		
Match incoming traffic from the specified destination IP range. Boxes	Values (IP Address)		
to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)	192.168.0.0 to 192.168.0.0		

VIP4G/VIP4Gb



4.8.6 Firewall > Reset

To reset the firewall back to default settings and erase all rules, port forwards, and IP/MAC lists, use the reset button see below:



Image 4-8-6: Firewall > Reset to Defaults



4.9 Router

4.9.1 Router > RIPV2

The VIP4G is capable of providing and participating in RIPv2 (Routing Information Protocol v2), to exchange routing information from attached devices. Static routes can also be added in the Network > Routes menu.

System Network Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
RIPV2 OSPF									
Router Configuration									
RIPV2 Status	Enable •								
Authentication Type	MD5 V								
Authentication Port	WAN •								
MD5 Authentication Password	•••••								
RIPv2 Network Announcement Conf	guration								
Subnet Address / SubnetMask Leng	Subnet Address / SubnetMask Length								
/									
Add To Network List									
RIPv2 Network Announcement List									
Subnet Address		SubnetMask Le	ngth						

Image 4-9-1: Router > RIPv2

	RIPV2 Status		
Enable or disable RIPV2 routing on the VIP4G. If enabled the VIP4G will exchange routing information on the specified (interfaces) attached	Values (selection)		
networks.	Enable / Disable		
Authentication T	ype / Port / Password		

None MD5

RIPV2 Network Announcement Configuration

Each attached network that is to participate with the RIPV2 exchange must be specified here. Once added they participating networks are shown in the list.

Values (Subnet/Length))

(no default)



4.9.2 Router > OSPF

The VIP4G is also capable of providing and participating in OSPF (Open Shortest Path First), to exchange routing information from attached devices. Static routes can also be added in the Network > Routes menu.

m	icro	hard sy	STEM	S INC.	-	-		0	10	10101
System Network RIPV2 <mark>OSPF</mark>	Carrier	Wireless Firew	all VPN	Router	Serial	1/0 G	PS Apps	Diag	Admin	10110
Router Configuratio	n									
OSPF Status OSPF Network Annour	cement Confi	Enable v]							
Network Address / 1 Add	letwork Mask /	OSPF Area								
OSPF Network Annour	cement List									
Network Address		Network	Mask		OSPF Ar	22				

Image 4-9-2: Router > OSPF

	OSPF Status	
Enable or disable OSPF routing on the VIP4G. If enabled the VIP4G will exchange routing information on the specified (interfaces) attached	Values (selection)	
networks.	Enable / Disable	
OSPF Network Annour	ncement Configuration	

Each attached network that is to participate with the OSPF exchange must be specified here. Once added they participating networks are shown in the list.

Values (Subnet/Length))

(no default)



4.10 VPN

4.10.1 VPN > Summary

A Virtual Private Network (VPN) may be configured to enable a tunnel between the VIP4G and a remote network.. The VIP4G supports VPN IPsec Gateway to Gateway (site-to-site) tunneling, meaning you are using the VIP4G to connect a tunnel to network with VPN capabilities (Another VIP4G or VPN capable device). The VIP4G can also operate as a L2TP Server, allowing users to VPN into the unit from a remote PC, and a L2TP Client.

								_
1	micro	hard	SYSTEM	S INC.	1010101	101	01	01
System Net	work Carrie	er Wireless	Comport I	O GPS I	irewall Rout	er VPN	MultiWAN	Tools
Summary G	ateway To Ga	teway Clier	nt To Gateway	VPN Client	Access Certi	ficate Man	agement	
Summary								
Gateway To Ga	teway							
No. Name Add	Status Phase2 Enc/	'Auth/Grp Int	erface Local Group	Remote Group	Remote Gateway	RX/TX Bytes	Tunnei Test	Config.
L2TP Client To	Gateway							
No. Name	Status Interface	Local/Remote IP A	ddress Server	Gateway Sta	rt Time Duration	RX/TX Bytes	Tunnel Test	Config.
L2TP Server								
Status	Interface	Local IP	Client IP Range Start		Client IP Range	End	Cont	lig.
disable	WAN						Edit	
DISADIe	40						EOII	
L2TP Connectio	on List							
No. Rem	ote Address	L2TP IP	Address	Start Time	Duration	RX Btyes	TX Btye	5
VPN Client Acce	ess							
No. Add	Userna	me			Config.			

Image 4-10-1: VPN > Summary



4.9.2 VPN > Gateway To Gateway (Site-to-Site)

A Gateway to Gateway connection is used to create a tunnel between two VPN devices such as an VIP4G and another device (another VIP4G or Cisco VPN Router or another vendor...). The local and remote group settings will need to be configured below to mirror those set on the other VPN device.

System Network Carrier	Wireless Comport I/O GPS Firewall Router VPN MultiWAN Tools
Summary Gateway To Gate	way Client To Gateway VPN Client Access Certificate Management
Gateway To Gateway	
,	
Add a New Tunnel	
Tunnel Name	
Enable	8
Authentication	Preshared Key 🔹
Interface	WAN T
Local Group Setup	
Local Security Gateway Type	IP Only •
Interface IP Address	74.198.186.197
Next-hop Gateway IP	
Group Subnet Gateway	
Group Subnet IP/Mask - 1	/ 255.255.255.0
	Add Remove
Remote Group Setup	
Remote Security Gateway Type	IP Only
Gateway IP Address	
Next-hop Gateway IP	
Group Subnet IP/Mask - 1	/ 255.255.255.0
	Add Remove
IPSec Setup	
Aggressive Mode	
Phase1 Strict Mode:	
Phase 1 DH Group	modp1024 •
Phase 1 Encryption	3des 💌
Phase 1 Authentication	md5 🔻
Phase 1 SA Life Time(s)	28800
Perfect Forward Secrecy	
Phase 2 SA Type	ESP •
Phase2 Strict Mode:	8
Phase 2 DH Group	modp1024 🔻
Phase 2 Encryption	3des •
Phase 2 Authentication	md5 •
Phase 2 SA Life Time(s)	3600
Preshared Key	
DPD Delay(s)	32
DPD Timeout(s)	122
DPD Action	hold v

	tunnel1
Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created each requiring a unique name	Values (chars)
	Tunnel Name



Enable

Used to enable (checked) is disable (unchecked) the VPN tunnel.

Values (checkbox)

Enable (Checked)

VIP4G/VIP4Gb

Local Group Setup

Local Security Gateway Type Specify the method for identifying the router to establish the VPN tunnel. Values (selection) The Local Security Gateway is on this router; the Remote Security Gateway is on the other router. At least one of the routers must have either IP Only a static IP address or a dynamic IP with server id to make a connection. **IP + Server ID** Dynamic IP + Server ID IP Only: Choose this option if this router has a static WAN IP address. The WAN IP address appears automatically. For the Remote Security Gateway Type, an extra field appears. If you know the IP address of the remote VPN router, choose IP Address, and then enter the address. IP + Server ID: Choose this option if this router has a static WAN IP address and a server id. The WAN IP address appears automatically. For the Remote Security Gateway Type, an extra field appears. If you know the IP address of the remote VPN router, choose IP Address, and then enter the address. Dynamic IP + Server ID: Choose this option if this router has a dynamic IP address and a server id (available such as @microhard.vpn). Enter the server id to use for authentication. The server id can be used only for one tunnel connection. **Interface IP Address** Displays the IP address of the VIP4G, which is the local VPN Gateway. Values (IP Address) **Current IP Address** Server ID This option appears when the Local Security Gateway Type specifies that Values (IP Address) the Server ID is required for the connection. The Server ID must be in the format @name, where name can be anything. Both routers must know (no default) each others names to establish a connection. **Next-hop Gateway IP**

Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network. (no default)

Define the local network by specifying the local subnet. The local and Values (IP Address) remote routers must use different subnets.

(no default)

Group Subnet IP



	Group Subnet Mask
Specify the subnet mask of the local network address.	Values (IP Address)
	255.255.255.0
Gr	oup Subnet Gateway
Enter the Gateway for the local group network.	Values (IP Address)
	(no default)
Remote Group Setup	
Remote Se	ecurity Gateway Type
Specify the method for identifying the router to establish the VPN tunnel.	Values (selection)
Gateway is on the other router. At least one of the routers must have either a static IP address or a dynamic IP with server id to make a connection. (See Local Group Setup for details)	IP Only I P + Server ID Dynamic IP + Server ID
	Gateway IP Address
If the remote VPN router has a static IP address, enter the IP address of	Values (IP Address)
the remote vi n Galeway here.	(no default)
	Server ID
This option appears when the Remote Security Gateway Type specifies	Values (IP Address)
the format $@$ <u>name</u> , where name can be anything. Both routers must know each others names to establish a connection.	(no default)
	Next-hop Gateway IP
Next-hop Gateway means the next-hop gateway IP address for the local or	Values (IP Address)
remote gateway participant's connection to the public network.	(no default)
	Subnet IP Address
Define the remote network by specifying the local subnet.	Values (IP Address)
	(no default)
	Subnet Mask
Specify the subnet mask of the remote network address.	Values (IP Address)
	255.255.255.0

VIP4G/VIP4Gb


Phase 1 DH Group
Values (selection)
modp1024 modp1536 modp2048
Phase 1 Encryption
Values (selection)
3des aes aes128 aes256
ase 1 Authentication
Values (selection)
md5 sha1
Phase 1 SA Life Time
Values
28800
orward Secrecy (pfs)
Values (selection)
Disable / Enable
Phase 2 DH Group
Values (selection)
modp1024 modp1536 modp2048
Phase 2 Encryption
Values (selection)
3des
ads



Ph	ase 2 Authentication
Select value to match the Phase 1 Authentication used by the remote VPN	Values (selection)
	md5 sha1
	Phase 2 SA Life Time
	Phase 2 SA Life Time
Select value to match the values required by the remote VPN router.	Values
	3600
	Preshared Key
Set the Preshared Key required to authenticate with the remote VPN	Values (characters)
	password
	DPD Delay(s)
Dead Peer Detection is used to detect if there is a dead peer. Set the DPD	Values (seconds)
Delay (seconds), as required.	32
	DPD Timeout(s)
Set the DPD (Dead Peer Detection) Timeout (seconds), as required.	DPD Timeout(s) Values (seconds)
Set the DPD (Dead Peer Detection) Timeout (seconds), as required.	DPD Timeout(s) Values (seconds) 122
Set the DPD (Dead Peer Detection) Timeout (seconds), as required.	DPD Timeout(s) Values (seconds) 122 DPD Action
Set the DPD (Dead Peer Detection) Timeout (seconds), as required.	DPD Timeout(s) Values (seconds) 122 DPD Action Values (seconds)



4.10.3 VPN > Client To Gateway (L2TP Client)

The VIP4G can operate as a L2TP Client, allowing a VPN connection to be made with a L2TP Server.

ystem Network Carrier	Wireless Comport I/O GPS Firewall Router VPN MultiWAN Tools	
ımmary Gateway To Gate	way Client To Gateway VPN Client Access Certificate Management	
2TD Client		
21P Client		
Add a New Tunnel		
Tunnel Name		
Enable	8	
IPsec	8	
Interface	4G T	
Local Group Setup		
Local Security Cateway Type		
Interface IP Address	74 108 107	
Next-hon Gateway IP	74.180.100.187	
next hop outenay in		
Remote Group Setup		
Remote Security Gateway Type	IP + Server ID 🔻	
Gateway IP Address		
Server ID		
Next-hop Gateway IP		
Group Subnet IP		
Group Subnet Mask	255.255.255.0	
PPP Setup		
Idle time before hanging up	0 seconds [065535]	
PAP	Unencrypted Password	
CHAP	Challenge Handshake Authentication Protocol	
User Name		
Redial	2	
Redial attempts	3	
Time between redial attempts	15	
IPCor Sotup		
Circo ACA LOTD		
CISCO ASA L2TP		
Authentication	Preshared Key 🔻	
Pridse 1 SA Life Time(s)	43200	
Perfect Forward Secrecy		
Phase 2 SA Life Time(s)	10800	
Preshared Key		
DPD Delay(s)	5	
DPD Timeout(s)	30	
DPD Action	restart 🔻	
Advanced+		

Image 4-10-3: VPN > Client to Gateway

	Tunnel Name
Enter a name for the VPN Tunnel. Up to 16 different tunnels can be	Values (chars)
created, each requiring a unique name.	tunnel1
	Enable
Used to enable (checked) is disable (unchecked) the VPN tunnel.	Values (checkbox)
	Enable (Checked)



Loca	al Interface IP Address
his will show the WAN or 4G IP Address used for the L2TP Interface.	Values (IP Address)
	Current IP
Remot	te Gateway IP Address
Enter the IP Address of the Remote Gateway that you wish to establish a	Values (IP Address)
onnection with.	none
	Remote Server ID
Some servers require that you know the Server ID as well as the IP	Values
iddress. Enter the Server ID of the remote router here.	none
	Remote Subnet IP
n order to communicate with the devices on the other side of the tunnel, be VIP4G must know which data to pass through the tunnel, to do this	Values (IP Address)
enter the Remote Subnet network IP address here.	none
	Remote Subnet Mask
Inter the Remote Subnet Mask	Values (IP Address)
	none
Idle ti	ime before hanging up
Enter the Idle time (in seconds) to wait before giving up the PPP	Values (seconds)
connection. The default is 0, which means the time is infinite. (0-65535)	0
	Username
Enter the Username	Values (chars)
	0
	Preshared Key
be preshared key is required to connect to the L2TP Server.	Values (chars)

IPSec Setup - See previous sections for additional info.



4.10.4 VPN > VPN Client Access

For VPN L2TP Server operation, users will be required to provide a username and password. Use VPN Client Access to set up the required users.

	m	icro	hard	SYSTEM	AS I	NC.	1010	1010	01	01	01
System	Network	Carrier	Wireless	Comport	1/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Summary	y Gatewa	y To Gate	way Clien	t To Gatewa	y VI	PN Clie	nt Access	Certifica	ate Ma	nagement	
VPN Clie	nt Access										
User	name										
New	Password	vord									
-											
			Imag	ie 4-10-4: VF	PN >	VPN C	lient Acces	S			
										Usei	rname
Enter a u	username	for the us	er being se	et up.				V	alue	s (charac	ters)
											,
									N	lew Pas	sword
Enter a p	bassword f	for the use	e.					V	alue	s (charac	ters)
								Confi	irm N	lew Pas	sword

Enter the password again, the VIP4G will ensure that the password match. Values (IP Address)



4.10.5 VPN > Certificate Management

When using the VPN features of the VIP4G, it is possible to select X.509 for the Authentication Type. If that is the case, the VIP4G must use the required x.509 certificates in order to establish a secure tunnel between other devices. Certificate Management allows the user a place to manage these certificates.

											_
14	mi	crol	nard	SYSTE	MSI	NC.	10404	010	01	01	01
System N	etwork	Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Summary	Gateway	To Gatev	way Client	To Gatew	ay VI	PN Clie	nt Access	Certifica	ate Mar	nagement	
Certificate M	Manageme	nt									
X509 Root Co	ertificates										
No.			Name							Confi	ig.
Import Ce	rtificate:		Choose file	No file chose	n					Impo	ərt
X509 Cartific	ates										
x305 Certino	Lates										
No.	at fanta		Name Observe Ele	No fla chara						Confi	9.
import Ce	runcate.		Choose file	No file chose	n					impo	H.
X509 Private	Keys										
No.			Name							Confi	g.
Import Pri	ivate key:		Choose file	No file chose	en					Impo	ort
X509 Certific	cates Revoca	ation Lists									
No.			Name							Confi	g.
Import Ce	rtificate:		Choose file	No file chose	n					Impo	art

Image 4-10-5: VPN > Certificate Management



4.11 MultiWAN

4.11.1 MultiWAN > Status

The VIP4G is capable of having 2 WAN connections, one connected to the physical WAN port on the VIP4G and the Cellular WAN connection to the wireless carrier. The MultiWAN section allows a user to define how traffic uses these WAN's.

The main purpose of the MultiWan feature is to use one network for a primary connection, such as a local, wired ISP for broadband access, and if that connection fails or is offline, the VIP4G can automatically switch to an alternate network connection such as the 4G/Cellular connection.

The Status menu gives an overview of both WAN connections and their configuration. WAN group 1 is the wired WAN and WAN group 2 is the 4G/Cellular connection to a wireless carrier.

	icrol	ard	OVOTE	MGI	NC	-				010	101
111	iero.	naru	SISIE	WIS I	NC.	1010	1011	22	0	1001	20
System Network	Carrier	Wireless	Comport	1/0	GPS	Firewall	Router	VPN	MultiWAN	Tools	
Status Settings											
Multi WAN Status											
Multi WAN GROUP 1											
WAN Name					1	WAN					
IP Address						10.126.52.9					
Gateway						10.126.52.1					
DNS											
Status					3	ĸ					
Multi WAN GROUP 2											
WAN Name						4G [Primary]					
IP Address					3	74.198.186.1	97				
Gateway					0	74.198.186.1	97				
DNS						8. <mark>8.8.8 8.8.4</mark> .	4				
Status					1	JP					
								Sto	p Refreshing In	erval: 20 (in se	conds)

Image 4-10-1: MultiWAN > Status



4.10.2 MultiWAN > Settings

The following section describes the parameters required for MultiWan for failover purposes. The configuration for each interface in identical, so will only be described once.

System	Network	Carrier	Wireless	Comport	1/0	GPS	Firewall	Router	VPN	MultiWAN	Tools
Status	Settings										
Multi W	AN Configurat	tion									
Configu	ration										
Mult	i Wan status		Enable •								
Prim	ary Connection		4G •								
WAN Int	terface										
Heal	th Monitor Inter	rval	5 sec. 🔻								
Heal	th Monitor ICM	Host	8.8.8.8								
Heal	th Monitor ICMF	Timeout	3 sec. 🔻								
Atte	mpts Before WA	N Failover	3 •								
Atte	mpts Before WA	N Recovery	3 🔻								
Failo	over Traffic Dest	ination	4G 🔻								
4G Inter	face										
Heal	th Monitor Inter	val	5 sec. •								
Heal	th Monitor ICMP	PHost	8.8.8.8								
Heal	th Monitor ICMP	Timeout	3 sec. •								
Atte	mpts Before 4G	Failover	3 🔻								
Atte	mpts Before 4G	Recovery	3 •								
Failo	over Traffic Dest	ination	WAN •								

Image 4-10-2: MultiWAN > Settings

	Multi Wan status		
Enable or disable the MultiWan service on the VIP4G.	Values (selection)		
To use MultiWAN, the WAN (wired) must be configured as independent in the Network > WAN settings <u>and/or</u> the Wireless must be set to Client & bound to the WIFI interface.	Enable / Disable		
	Primary Connection		
Define which connection is the primary network/internet connection for the VIPAC. Normally this is the wired WAN connection to an ISP.	Values (selection)		
VIF 40. Normally this is the whet wan connection to an ISF.	WAN / 4G / WIFI		

	Health Monitor Interval
This is the frequency at which the VIP4G will send ICMP packets to the defined best to determine if the interface has failed	Values (selection)
	5,10,20,30,60,120(sec.) Disable
Hea	Ith Monitor ICMP Host
This is the IP Address or domain name of a valid reachable host that can	Values (Address)
	8.8.8.8
Health	Monitor ICMP Timeout
This is the amount of time the Health Monitor will wait for a response from the ICMP Heat	Values (selection)
	1, 2, 3 , 4, 5, 10 (seconds)
Attempt	s Before WAN Failover
This is the number of attempts the VIP4G will attempt to reach the IMCP	Values (selection)
host before going into failover and switching WAN interfaces.	1, 3 , 5, 10, 15, 20
Attempts	Before WAN Recovery
The VIP4G will continue to monitor the failed interface, even after failover	Values (selection)
before recovering the failed interface.	1, 3 , 5 , 10, 15, 20
Faile	over Traffic Destination
Select the interface to use once failover has occurred.	Values (selection)
	4G, WAN, Disable

VIP4G/VIP4Gb



4.12 Tools

4.12.1 Tools > Discovery

Network Discovery

The Network discovery tool allows the VIP4G to send a broadcast to all VIP4G/VIP Series units on the same network. Other units on the network will respond to the broadcast and report their MAC address, IP address (With a hyperlink to that units WebUI page), description, firmware version, operating mode, and the SSID (regardless of whether it was set to broadcast or not).

The discovery service can be a useful troubleshooting tool and can be used to quickly find and indentify other units on the network. It can be disabled from the Network > sdpServer menu.

7	mi	crol	hard	SYSTE	MSI	NC.	1010	1010	51		1	01	0101
System	Network	Carrier	Wireless	Comport	1/0	GPS	Firewall	Router	VPN	Mult	tiwan	Tools	
Discovery	Netflow	NMS Se	ttings E	vent Report	Mod	bus	Websocket	Site Su	rvey	Ping	Trace	Route	Traffic
Network	Discovery Discovery												
MAC	Address	IP	Address	Descrip	tion	Prod	uct Name	Firmwar	re Ver		Mode	SSID	
00:00 Start	F:92:00 B3:3B t discovery netw	<u>19</u> vork again	2.168.168.1	VIP4G-M	IKT	VIP4	G_WIFI_N	v1.1.6-r	1190-4		sta	MyNetwo	rk

Image 4-12-1: Tools > Discovery

To begin, click the *Start discovery network again* button, the VIP4G will send out a broadcast message, and will report back, by populating the network discovery screen as seen above. This will detect any VIP4G or Microhard enabled devices on the local broadcast domain, regardless of the IP address or subnet. Once devices are found, and if on a accessible subnet, the IP Address link can be used to automatically open a web browser WebUI session with that unit.



4.12.2 Tools > Netflow Report

The VIP4G can be configured to send Netflow reports to up to 3 remote systems. Netflow is a tool that collects and reports IP traffic information, allowing a user to analyze network traffic on a per interface basis to identity bandwidth issues and to understand data needs. Standard Netflow Filters can be applied to narrow down results and target specific data requirements.

mi	crohard sy	YSTEMS INC.	010101010	1010101
System Network	Carrier Wireless Co	omport I/O GPS Fire	wall Router VPN MultiWA	AN Tools
Discovery Netflow	NMS Settings Event	Report Modbus Webso	ocket Site Survey Ping Tr	aceRoute Traffic
Netflow Report Report Configuration No	.1			
Status Source Address Interface Remote IP Remote Port Filter expression Version Report Configuration No	Enable • 0.0.0.0 ALL • 0.0.0.0 2055 V5 •	default 0.0.0.0		
Status Report Configuration No Status	Disable V Jisable V			

Image 4-12-2: Tools > Netflow Report

	Status
Enable / Disable Netflow Reporting.	Values (selection)
	Disable / Enable
	Source Address
The Source Address is the IP Address, of which data is to be collected and	Values (IP Address)
addresses connected to the interface selected below.	0.0.0.0
	Interface
Select between WAN ,4G/Cellular and LAN interfaces, or capture data from all interfaces	Values (selection)
	LAN / WAN / 4G / ALL



	Remote IP	
The Remote IP is the IP Address of the NetFlow collector where the flow	Values (IP Address)	
	0.0.0.0	
	Remote Port	
Enter the Remote Port number.	Values (IP Address)	
	0	
	0 Filter expression	
Filter expression selects which packets will be captured. If no expression is given all packets will be captured. Otherwise, only packets for which	0 Filter expression Values (chars)	
Filter expression selects which packets will be captured. If no expression is given, all packets will be captured. Otherwise, only packets for which expression is `true' will be captured. Example: tcp&&port 80	0 Filter expression Values (chars) (no default)	

	Version
Select the Netflow version format to use. V1, 5 and 7 are supported.	Values (selection)
	V1 / V5 / V7



4.12.3 Tools > NMS Settings

The Microhard NMS is a no cost server based monitoring and management service offered by Microhard Systems Inc. Using NMS you can monitor online/offline units, retrieve usage data, perform backups and centralized upgrades, etc. The following section describes how to get started with NMS and how to configure the VIP4G to report to NMS.

To get started with NMS, browse to the Microhard NMS website, <u>mms.microhardcorp.com</u>, click on the register button in the top right corner to register for a Domain (profile), and set up a Domain Administrator Account.

G II Microhard Systems Inc. [CA]	https://nms.micronardcorp.co	m/wiicronardNM5/login.s	eam 🖓
ops 💯 microhardcorp.com 💆 Microhard Dev Site 💈	Microhard Support 👜 OET FC	CID Search 📋 Webmail LOGIN	MantisBT 🥩 Constant Contact : L
ohard NMS:			Register 1
E			
111			
V			
IMICIOITATU SYSTEMS INC.	Louis		
	engin		
	Email Address:		
	Passwordt		
		1	
	Forgot your password?	1.000	
		Login	
			Consulate Directory Contactory Inc. 2014 All Distance Rese
			a cohluffu uncentra al
			100 100
C n Microhard Systems Inc. [CA]	https://nms.microhardcorp.co 22 Microhard Support 🛛 😫 OET FC	m/MicrohardNMS/registr CID Search 🗋 Webmail LOGIN	ration.seam 🖓
C fi AMicrohard Systems Inc. [CA] P Microhard Corp.com 2 Microhard Dev Site anard MMS:	https://nms.microhardcorp.co 쩐 Microhard Support (由 OET FC	m/MicrohardNMS/registr CID Search 📋 Webmail LOGIN	ation.seam 🖧
C fi Microhard Systems Inc. [CA]	https://nms.microhardcorp.co 22 Microhard Support 👜 OET FC	m/MicrohardNMS/registr CID Search 🕐 Webmail LOGIN	ation.seam 🖧 I 🐊 MantisBT 🎯 Constant Contact : L Register i
C M Microhard Systems Inc. [CA] pr Ø microhardcorp.com Ø Microhard Dev Site shard MMS: ister for Domain and Domain Administrator Account	https://nms.microhardcorp.co ፴ Microhard Support (國 OET FC	m/MicrohardNMS/registr CID Search 🗋 Webmail LOGN	ation.seam 😭
C fi A Microhard Systems Inc. [CA] ps. 22 microhard corp.com 22 Microhard Dev Site standard MMS: isister for Domain and Bomain Administrator Account omain	nttps://nms.microhardcorp.co 辺 Microhard Support 、	m/MicrohardNMS/registr C ID Search 🕜 Webmail LOGIN	ationsearri 🖓
C A Microhard Systems Inc. [CA] ps. Microhard cop.com Microhard Dev Site shard MMS: ister for Domain and Bomain Administrator Account omain Choose your domain name*	https://nms.microhardcorp.co	m/MicrohardNMS/registr	ationsearri 🟠
C Microhard Systems Inc. [CA]	ittps://nms.microhardcorp.co 蓝 Microhard Support (論) OET FC	m/MicrohardNMS/registr CID Search D Webmail LOGIN	ation.seam
C f Microhard Systems Inc. [CA] psp microhardcorp.com 27 Microhard Dev Site shard NMS: inster for Domain and Demain Administrator Account Omain Choose your domain name * Create a password for your domain*	ittps://nms.microhardcorp.co 涩 Microhard Support 一般 OET FC	m/MicrohardNMS/registr CID Search D Webmail LOGIN	ation.seam Constant Contact: L Register / The Domain Rame and Domain Passnoor The Domain Rame and Passnoor The Domain
C Microhard Systems Inc. [CA] pr. microhardcorp.com 20 Microhard Dev Site stand dMS: inter for Domain and Bomain Administrator Account omain Choese your demain name Create a password for your domain Confirm your domain password	ittps://nms.microhardcorp.co 逻 Microhard Support 曲 OET FC	m/AforohardNMS/registr CID Serich () Webmail LOGN () value a required () value a required	ation.seam Contact: Lu: Mentist Contact: Lu: Prepiater / Prepiater / • The Bornain Name and Domain Pasework will be the createrial used in the modern NU configuration. • The Bornain Name and Domain Pasework between the second se
C fi Microhard Systems Inc. [CA] :	ttps://nms.microhardcorp.co	m/AlcrohardNMS/registr CID Serch _ Webmail LOGN @ value a regard @ value a regard	Altion.seam Kentisil Centaret Contact: Lu: Register
C fi Microhard Systems Inc. [CA] i pp: 22 microhardcorp.com 22 Microhard Dev Site 2 whard MMS: uister for Domain and Domain Administrator Account tomain Choose your domain name * Confirm your domain name * Confirm your domain password * Please enter the address of your organization *	ttps://nms.microhardcorp.co	m/AforohardNMS/registr CID Serich () Webmail LOGN () value a report () value a report () value a report ()	Alfon-Seam Alfon-Seam Americal Constant Contact: L.:. Register Americal America
C fi Microhard Systems Inc. [CA] i pp: 2 microhardcorp.com 2 Microhard Dev Site 2 whard MMS: patter for Domain and Domain Administrator Account Comain Choose your domain name " Croate a password for your domain" Confirm your domain password " Please enter the name of your organization" Please enter the hone number of your organization"	ittps://nms.microhardcorp.co 涩 Microhard Support 一段 OET FC	m/AlicrohardNMS/registr CID Serrch () Webmail LOGN () value a reparted () value a reparted	Alfon-Seam MetrisBT Constant Contact : L.: MetrisBT Constant Contact : L.: The Domain Hame and Domain Password and to provide the modern top of the angle. The short threaden top organization/departmentingen accordingly. (In the angle. The short for search in the forders top organization/departmentingen accordingly. (In the angle. The forder the the Bomain Hame bein your email is stoc2/you can, passes us your email is stoc2/you can, passes us your email is stoc2/you can, passes us
C A Microhard Systems Inc. [CA] pro 22 microhardcorp.com 22 Microhard Dev Sie 2 phand MMS: pister for Domain and Domain Administrator Account comain Choese pure domain name * Create a pueseword for your domain * Continn your domain puesword * Piease enter the name of your organization * Piease enter the address of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization * Piease enter the phone number of your organization *	ttps://mms.microhardcorp.co	m/AlcrohardNMS/registr CID Serch Webmail LOOM	Alton-Seam Constant Contact: Lu: Register Register Register Register Register Re
C	ttps://mms.microhardcorp.co	m/AforohardINMS/registr CID Serich () Webmail LOGN () value a required () value a required () value a required	Altonuseam Constant Contact : Lu: Register • • • The Dorsain Rame and Domain Password • • The Dorsain Rame and Domain Password • • • • • • • • • • • • • • • • • •
C	ttps://nms.microhardcorp.co	m/AficrohardNMS/registr CID Serich () Webmail LOGN () value a repared () value a repared	Attention Register Image: State of the
Chase enter the phone number of your organization Rease enter the address of your organization	ttps://mms.microhardcorp.co	m/AforohardNMS/registr CID Search (Webmail LOOM CID Search (Webmail LOOM)	Attornseam Constant Contact: Lu Register Constant Contact: Lu Register Contact and Contact: Lu Register Contact and Contact: Lu Register Contact and Contact: Lu Contact and Contact: Lu Register Contact and Contact: Lu Contact and Contact: Lu Contact and Contact: Lu Contact and Contact And Contact: Lu Contact and Contact And Contact And Contact Contact And Contact
C Microhard Systems Inc. [CA] Microhard Systems Inc. [CA] Microhard Bev Sine Mic	ttps://mms.microhardcorp.co	m/AforohardINMS/registr CID Serech () Webmail LOOM () value a required () value a required	Attornise Attornise Constant Contact: Lu Register Contact Contact: Lu Register Contact Contact: Lu Register Contact Contact: Lu Contact Contact: Lu Register Contact Contact: Lu Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact
C	ttps://mms.microhardcorp.co	m/AforohardINMS/registr CID Serich () Webmail LOGIN () value a regard () value a regard () value a regard ()	Attention Constant Contact: Lu Register Constant Contact: Lu Register Contact Contact: Lu Register Contact Contact: Lu Contact Contact: Lu Register Contact Contact: Lu Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contact Contac
C	Nttps://mms.microhardcorp.co	m/AficrohardNMS/registr CID Search () Webmail LOGN () value a resurse () value a resurse	Attornseam Constant Contact: Lu Register The Domain Rame and Contact: Register The Domain Rame and Rame Rame Rame Rame The Domain Rame and Rame Rame Rame The Domain Rame Rame Rame Rame The Domain Administrator Account (semal address and password) will be your Domain The Domain Administrator Account The Domain Rame Rame The Domain Administrator Account The Domain Rame Rame The Domain Rame Rame The Domain Rame Rame The Domain Rame Rame The Domain Rame The Domain Rame Rame
C Microhard Systems Inc. [CA] Microhard Systems Inc. [CA] Microhard Bey Size Microhard Microhard Bey Size Microhard Bey Size Microhard Bey Size Microhard Bey Size Microhard	ttps://mms.microhardcorp.co	m/AforohardNMS/registr CID Search Webmail LOOM	Atomicsom Constant Context : Li Register Constant Context : Li Register Constant Context : Li Register Constant Rame and Domain Password Constant Rame and Domain Password Constant Rame and Domain Rame and Constant Rame and Constant Rame and Domain Rame and Constant Rame Ram
C	ttps://mms.microhardcorp.co	m/AfronhardINMS/registr CID Serich Webmail LOGM	Alton.seam Alton.seam Annotation and a seam of a seam
C C	Image: Same as provery small address	m/AficrohardNMS/registr CID Search () Webmail LOGN	Alton.seam Mentiol Constant Contact: Li Register Register Register Register Register Register Register Register Register Reg
C Microhard Systems Inc. [CA] Microhard Systems Inc. [CA] Microhard Bey Size Microhard Microhard Bey Size Microhard Mic	ttps://mms.microhardcorp.cc	m/AforohardINMS/registr CID Search : Webmail LOOM	Altonisam
C	ttps://mms.microhardcorp.cc	m/AfronhardINMS/registr CID Serech Webmail LOGM	Alton.seam Mention Contact Contact Contact: Lu: Register Contact Contact Contact: Lu: Provide Contact: Lu: Provide Cont
C	Same as prinsey small address KOP KUMK	m/AfcrohardINMS/registr CID Serich Webmail LOGIN	Alton.seam Mentiol Constant Contact: Lu: Register Register Register Register Register Register Register Register Register Register Register Register Register Regis
C Microhard Systems Inc. [CA] Microhard Systems Inc. [CA] pape Z microhardcorp.com Z Microhard Dev Sin Z microhard Miss microhard Miss microhard Administrator Account Comain Choese spaceword for your domain * Content your domain password * Please enter the address of your organization * Please enter your if ist name * Please enter your if ist name * Please enter your add address * (as login and address * your cell phone number Please enter the characters from the above image * Please enter the characters from the above image * Please enter the characters from the above image *	ttps://mms.microhardcorp.cc Microhard Support ∰ OET - FC	m/AforohardNMS/registr CID Search : Webmail LOOM	Altonization A
C Microhard Systems Inc. [CA] Microhard Systems Inc. [CA] pape Z microhardcop.com Zi Microhard Dev Sine Z hand MMS: pape Z microhardcop.com Zi Microhard Dev Sine Z hand MMS: Commain Administrator Account Contens your domain passwort Please enter the name of your organization Please enter the address of your organization Please enter the phone number of your organization Please enter the phone number of your organization Please enter the phone number of your organization Please enter your first name Please enter your inst name Please enter	Same as primary anal address	m/AfronhardINMS/registr CID Serech Webmail LOGM	Altonization A
C A Microhard Systems Inc. [CA] + proceeding microhardcop.com Microhard Dev Sine Sahard MMS: provide microhardcop.com Microhard Dev Sine Sahard MMS: provide microhardcop.com Microhard Dev Sine Sahard MMS: Create a password for your organization Tease enter the address of your organization Tease enter the phone number of your organization Tease enter the phone number of your organization Tease enter your first name Please enter your and address tagoent enter your address Your cell phone number Please enter the characters from the above image Lagree the Tama and Confilment ".	Same as primary amail address Same as primary amail address Same as primary amail address	m/AfronhardINMS/registr CID Search Webmail LOGM	Altonisam

Image 4-12-3: NMS Registration

Domain Name: A logical management zone for 3G or 4G devices will report to on NMS, the logged data is separated from any other users that are using NMS. The Domain Name is required in every 3G or 4G device for it to report to right zone. Under this user domain, one can create and manage sub-domain. The sub-domain can only be created by the domain administrator, NOT by the NMS subscription page.

010

VIP4G/VIP4Gb

Domain Password: This password is used to prevent misuse of the domain. This needs to be entered into each 3G or 4G device for it to report to right zone.

Email Address: The email address entered here will be the login username. During the registration stage, a confirmation email will be sent by the NMS system for verification and confirmation to activate your account.

Once confirmed, this account will be the administrator of the domain. The administrator can manage subdomain and user accounts that belong to this domain.

Once NMS has been configured, each VIP4G must be configured to report into NMS.

System	Network	Carrier	Wireless	Comport	I/0	GPS	Firewall	Router	VPN	Mult	iWAN	Tools	
Discovery	Netflow	NMS Se	ttings E	vent Report	Modbu	us W	ebsocket	Site Su	rvey	Ping	Trace	Route	Traffic
NMS Con	figuration		Table of the shade		2221								
Defai	lit Settings		Edit with def	ault configurati	ion								
System S	etting												
NMS :	Server/IP		nms.microha	rdcorp.com	Login NMS	<u>IS</u>							
Doma	ain Name		mytech										
Doma	ain Password		•••••		Min 5 char	racters							
Confi	rm Password		•••••		J								
NMS Rep	ort Setting												
Carri	er Location		Enable Upda	te Over Network	k 🔻								
Repo	rt Status		Enable NMS	Report •									
	0007		20200		[0 ~ 65535	5]							
Kem	IOLE POKI		(default:202	00)									
Inter	rval Time(s)		120		0~65535	5]							
Info	rmation Selection	on	Available Ite	ms:									
Ethe	rnet		O Disable 🖲	Enable									
Carr	ier		O Disable	Enable									
Radi	io:		Disable •	Enable									
Com	E		O Disable 🖲	Enable									
DI/D	:00		O Disable @	Enable									
GRE	tunnel_1		Disable	Enable									
Webclien	t Setting												
Statu	5		Enable •										
Serve	r Type		HTTPS •										
Serve	r Port		9998										
User	Name		admin		1								
Passw	ord		•••••										
Interv	al		5		(minutes)								

Image 4-12-4: NMS Settings

Network Management System (NMS) Configuration			
	Default Settings		
The default Settings link will reset the configuration form to the default factor to be submitted before any changes will occur.	ry values. The form still needs		
	NMS Server/IP		
The default server address for NMS is nms.microhardcorp.com. The NMS	Values (IP/Name)		
	nms.microhardcorp.com		
Dom	ain Name / Password		
This is the domain name and password that was registered on the NMS	Values (chars)		
	default		
NMS Report Setting			
	Carrier Location		
Enable or Disable location estimation via carrier connection. When	Values (chars)		
from the internet.	Disable/Enable		
	Report Status		
Enable or Disable UDP reporting of data to the NMS system.	Values (chars)		
	Enable NMS Report Disable NMS Report		
	Remote Port		
This is the port to which the UDP packets are sent, and the NMS system is	Values (UDP Port#)		
is 20200.	20200		
	Interval(s)		
The Interval defines how often data is reported to NMS. The more often	Values (seconds)		
user's data plan. (0 to 65535 seconds)	300		

VIP4G/VIP4Gb

li li	nformation Selection
The VIP4G can report information about the different interfaces it has. By default the VIP4G is set to send information about the Carrier, such as usage and RSSI. Statistical and usage data on the Radio (WiFi), Ethernet and Serial interfaces can also be reported. The more that is reported, the more data that is sent to the NMS system, be aware of data plan constraints and related costs.	Values (check boxes) Ethernet Carrier Radio COM DI / DO
Webclient Setting	
	Status
The Web Service can be enabled or disabled. This service is used to remotely control the VIP4G. It can be used to schedule reboots, firmware upgrade and backup tasks, etc.	Values (chars) Disable/Enable
	Server Type
Select between HTTPS (secure), or HTTP server type.	Values (chars) HTTPS/ HTTP
	Server Port
This is the port where the service is installed and listening. This port should be open on any installed firewalls.	Values (Port#) 9998
U	sername / Password
This is the username and password used to authenticate the unit.	Values (seconds) admin/admin
	Interval
The Interval defines how often the VIP4G checks with the NMS System to determine if there are any tasks to be completed. Carrier data will be consumed every time the device probes the NMS system.	Values (min) 60

VIP4G/VIP4Gb



4.12.4 Tools > Event Report

4.12.4.1 Event Report > Configuration

Event Reporting allows the VIP4G to send periodic updates via UDP packets. These packets are customizable and can be sent to up to 3 different hosts, and at a programmable interval. The event packet can report information about the modem such as the hardware/ software versions, core temperature, supply voltage, etc; carrier info such as signal strength (RSSI), phone number, RF Band; or about the WAN such as if the assigned IP Address changes. All events are reported in binary.

System Network	Carrier Wireless Comport	I/O GPS I	irewall Router	VPN Multiv	VAN Tools
Discovery Netflow	NMS Settings Event Report	Modbus We	bsocket Site Su	rvey Ping T	raceRoute Traffic
Event Report					
Benert Configuration No. 1					
Report Configuration No.1					
Event Type	Modem_Event •				
Remote IP	0.0.0.0	0.0.0.0			
Remote PORT	20200	[0 ~ 65535]			
Interval Time(s)	600	[0~65535]			
Message Info Type	Modem • None • No	one 🔻			
Report Configuration No.2					
Event Type	SDP_Event •				
Remote IP	0.0.0.0	0.0.0			
Remote PORT	20200	[0~65535]			
Interval Time(s)	600	[0 ~ 65535]			
Report Configuration No.3					
Event Type	Management •				
Remote IP	0.0.0.0	0.0.0			
Remote PORT	20200	[0 ~ 65535]			
Interval Time(s)	600	[0~65535]			
Interface Selection					
Ethernet	Disable Senable				
Carrier:	Disable Disable				
Radio:	Disable Disable				
Com:	Disable Enable				
DI/DO:	Disable Disable				
CRE: tunnel_1	Disable Disable				

Image 4-12-5: Tools > Event Report

Event Type

This box allows the selection of the type of event to be reported. The default is disabled. If Modem_Event is selected, additional options appear to the right and allow for customization of the event reported via Messages. If Management is selected, additional check boxes appear below to select the interfaces to report to the Microhard NMS system.

Modem_Event SDP_Event Management

Values (selection)



	Remote IP
Enter the IP Address of a reachable host to send the UDP packets	Values (IP Address)
	0.0.0.0
	Remote Port
Specify the UDP port number of the Remote IP Address.	Values (Port #)
*Default Port Numbers for Microhard NMS (20100 for modem events, 20200 for Management)	20200
	Interval Time(s)
This is the interval time in seconds, that the VIP4G will send the configured	Values (seconds)
ODF message to the Remote if and Fort specified.	600
	Message Info Type
When Modem_Event is selected, up to three different payloads can be selected.	Values (seconds)
	Modem Carrier WAN

VIP4G/VIP4Gb

4.12.4.2 Event Report > Message Structure

Modem_event message structure

- fixed header (fixed size 20 bytes)
- Modem ID (uint64_t (8 bytes))
- Message type mask (uint8_t(1 byte))
- reserved
- packet length (uint16_t(2 bytes))

Note: packet length = length of fixed header + length of message payload.

Message type mask

Modem info -	2 bits
	00 no
	01 yes (0x1)
Carrier info -	2 bits
	00 no
	01 yes (0x4)
WAN Info -	2 bits
	00 no
	01 yes (0x10)

sdp_event message structure

- spd_cmd (1 byte(0x01))
- content length (1 byte)
- spd_package same as spd response inquiry package format



4.12.4.3 Event Report > Message Payload

Modem info:

Content length Modem name Hardware version Software version Core temperature Supply voltage		2 BYTES (UINT16_T) STRING (1-30 bytes) STRING (1-30 bytes) STRING (1-30 bytes) STRING (1-30 bytes) STRING (1-30 bytes)
Carrier info:		
Content length RSSI RF Band Service type Channel number SIM card number	- - - -	2 BYTES (UINT16_T) 1 BYTE (UINT8_T) 2 BYTES (UINT16_T) STRING (1-30 Bytes) STRING (1-30 Bytes) STRING (1-30 Bytes)

WAN Info:

Phone number

Content length	-	2 BYTES (UINT16_T)
IP address	-	4 BYTES (UINT32_T)
DNS1	-	4 BYTES (UINT32_T)
DNS2	-	4 BYTES (UINT32_T)

Message Order:

Messages will be ordered by message type number.

For example,

If message type mask = 0x15, the eurd package will be equipped by header+modem information+carrier information+wanip information.

STRING (1-30 Bytes)

010

VIP4G/VIP4Gb

If message type mask = 0x4, the eurd package will be equipped by header+carrier information.

If message type mask = 0x11, the eurd package will be equipped by header+modem infomation+wanip infomation.



4.12.5 Tools > Modbus

4.12.5.1 Modbus > TCP Modbus

The VIP4G can be configured to operate as a TCP/IP or Serial (COM) Modbus slave and respond to Modbus requests and report various information as shown in the Data Map.

todbus todbus Slave Device Config: Status Ena Port 502 Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 COM Mode Status Ena	ible Service	ce • 1 ~ 65535] 0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 0.0.0] 0.0.0.0] 0.0.0.0]			
Modbus Slave Device Config: Status Ena TCP Mode Status Ena Port 502 Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.00 COM Mode Status Ena Data Mode RS2	ible Service	ce • 1 ~ 65535] 0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 0 0 0 0] 0 0 0 0]			
Status Ena TCP Mode Status Ena Port 502 Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.00	able Service	ce • 1 ~ 65535] 0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 0 0.0.0] 0.0.0.0] 0.0.0.0]			
Status Ena TCP Mode Status Ena Port 502 Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.00	Ible Service Ible TCP Connection Service Ible TCP Connection Service Ible IP Filter Ible Ible Ible Ible Ible Ible Ible Ible	ce • 1 ~ 65535] 0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 0 0 0 0] 0 0 0 0]			
TCP Mode Status Ena Port 502 Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0	IDE TCP Connection Servi IDE IDE IDE IDE IDE IDE IDE IDE IDE IDE	ce • 1 ~ 65535] 0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 . 0.0.0] 0.0.0.0] 0.0.0.0]			
Port 502 Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0	I I I I I I I I I I I I I I I I I I I	1 ~ 65535] 0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 0.0.0] 0.0.0.0] 0.0.0.0]			
Active Timeout(s) 30 Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0	[1]]]]]]]]]]]]]]]]]]]	0 ~ 65535] 1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 0.0.0] 0.0.0.0] 0.0.0.0] 0.0.0.0]			
Slave ID 1 Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0	I I I I I I I I I I I I I I I I I I I	1 ~ 255] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0 0 0 0 0] 0 0 0 0]			
Coils Address Offset 0 Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0	1000 100 100 100 100 100 100 100 100 10	0 ~ 65535] 0 ~ 65535] 0 ~ 65535] 0.0.0.0] 0.0.0.0] 0.0.0.0] 0.0.0.0]			
Input Address Offset 0 Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 COM Mode Status Ena Data Mode RS3	10 10 10 10 10 10 10 10 10 10 10 10 10 1	0 ~ 65535] 0 ~ 65535] 0.0.0.0] 0.0.0.0] 0.0.0.0]			
Register Address Offset 0 Master IP Filter Set Ena Accept Master IP1 0.0.0	10.0 [1 0.0 [1 0.0 [1 0.0 [1 0.0 [1 0.0 [1 0.0 [1	0 ~ 65535] 0.0.0.0] 0.0.0.0] 0.0.0.0]			
Master IP Filter Set Ena Accept Master IP1 0.0.0 COM Mode Status Ena Data Mode RS2	ible IP Filter	0.0.0.0] 0.0.0.0] 0.0.0.0]			
Accept Master IP1 0.0.0 COM Mode Status Ena Data Mode RS2	0.0 [t 0.0 [t 0.0 [t 0.0 [t	0.0.0.0] 0.0.0.0] 0.0.0.0]			
Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 COM Mode Status Ena Data Mode RS2	0.0 [r 0.0 [r 0.0 [r	0.0.0.0]			
Accept Master IP1 0.0.0 Accept Master IP1 0.0.0 COM Mode Status Ena Data Mode RS2	0.0 (r 0.0 (r	[0.0.0.0			
Accept Master IP1 0.0.0 COM Mode Status Ena Data Mode RS2	0.0	10 0 0			
COM Mode Status Ena Data Mode RS2		0.0.0.01			
Data Mode RS2	ble COM ASCII Mode	•			
	232 •				
Baud Rate 192	• 00				
Data Format 8N1	•				
Character Timeout(s) 5	[0 ~ 65535]			
Slave ID 1)t	1 ~ 255]			
Coils Address Offset 0	l	0~65535]			
Input Address Offset 0	Į.	0~65535]			
Register Address Offset 0	Į.	0~65535]			

	Status
Disable or enable the Modbus service on the VIP4G.	Values (selection)
	Disable Service Enable Service
	TCP Mode Status
Disable or enable the Modbus TCP Connection Service on the VIP4G.	Values (selection)
	Disable Enable



	Port
Specify the Port in which the Modbus TCP service is to listen and respond	Values (Port #)
to poils.	502
	Active Timeout(s)
Define the active timeout in seconds.	Values (seconds)
	30
	Slave ID
Each Modbus slave device must have a unique address, or Slave ID. Enter	Values (value)
this value here as required by the would should should system.	1
	Coils Address Offset
Enter the Coils Address offset as required by the Master.	Values (value)
	0
	Input Address Offset
Enter the Input Address offset as required by the Master.	Values (value)
	0
Reg	gister Address Offset
Enter the Register Address offset as required by the Master.	Values (value)
	0
	Master IP Filter Set
It is possible to only accept connections from specific Modbus Master IP's,	Values (selection)
in the fields provided.	Disable / Enable

4.12.5.2 Modbus > COM (Serial) Modbus

The VIP4G can also participate in serial based Modbus, to configure and view the serial Modbus settings, the COM1 port must first be disabled in the *Comport > Settings* menu. Only the settings that are different from TCP Modbus will be discussed.

VIP4G/VIP4Gb

COM Mode Status	Enable COM A	SCIL	Mode 👻
Data Mode	RS232 -		
Baud Rate	19200 -		
Data Format	8N1	•	
Character Timeout(s)	5		[0 ~ 65535]
Slave ID	1		[1 ~ 255]
Coils Address Offset	0		[0 ~ 65535]
Input Address Offset	0		[0 ~ 65535]
Register Address Offset	0		[0 ~ 65535]

Image 4-12-7: Tools > Modbus Serial Configuration

		CC	M Mode	e Status		
Disable to select the Serial (COM) mode for the Modbus servic mode communication is in binary format and in ASC	ce. In RTU	Values (selection)				
communication is in ASCII format.	Disable Enable COM ASCII Mode Enable COM RTU Mode					
			Dat	ta Mode		
Determines which (rear of unit) serial interface shall be used to	connect to	Values (selection)				
COM1. When an interface other than RS232 is selected, the DE be inactive.	RS23 RS48 RS42	2 5 2				
			Ba	ud Rate		
The serial baud rate is the rate at which the modem is to	Values	(select	ion (bps)))		
	921600 460800 230400 115200	57600 38400 28800 19200	14400 9600 7200 4800	3600 2400 1200 600 300		
			Data	Format		
This setting determines the format of the data on the serial port. The default is 8 data bits. No parity, and 1 Stop bit.		Valu	es (selec	tion)		
		8N1 8N2 8E1	8O1 7 7N1 7 7N2 7 7	E1 O1 E2 O2		

Supported F	unction Codes:		Registers			
1Read Coils		16 Dite				
2Read Inpu	uts		TOBILS	Hex Format	Definition	
3Read Reg	3Read Registers		Address			
5Write Sing	gle Coil		0	0x0000	Modem Model Type	
6Write Sing	gle Register		1	0x0001	Build Version	
Data Address	s = Offset + Basi	c Address	2	0x0002	Modem ID Highest 2 Bytes	
Dit Address	Hav Format	Definition	3	0x0003	Modem ID Higher 2 Bytes	
DIL Aduress	nex Format	OUTPUT 1		0×0004	Modern ID Lewer 2 Pytes	
1	0x0001	OUTPUT 2	4	0x0004	Modern ID Lower 2 Bytes	
2	0x0002	OUTPUT 3	5	0x0005	Modem ID Lowest 2 Bytes	
3	0x0003	OUTPUT 4	6	0x0006	RSSI(dbm)	
9	0x0009	COM2 Status	8	0x0008	Core Temperature(C)	
12	0x000c	LAN/eth0 Status	9	0x0009	Carrier Received Bytes(MB)	
13	0x000d	WAN/eth1 Status	10	0x000a	Carrier Transmitted Bytes(MB)	
16	0x0010	Carrier Status	11	0×000b	CPS Altitude(m)	
18	0x0012	Wifi Status	10	0.0000	OPS Latitude (III)	
22	0x0016	GPS Status	12	0x000c	GPS Latitude High 2 Bytes	
23	0x0017	Location Over Network	13	0x000d	Latitude Low 2 Bytes(x1000000)	
24	0x0018	Event UDP Report 1	14	0x000e	GPS Longitude High 2 Bytes	
25	0x0019	Event UDP Report 2	15	0x000f	Longitude Low 2 Bytes(x1000000)	
26	0x001a	Event UDP Report 3	18	0x0012	COM2 Baud Rate(/100)(bps)	
27	0x001b	NMS Report	10	0×0012	COM2 Data Format	
28	0x001c	Sizewall Status	19	0,0015		
40	0x0078	SVSTEM Paboot	Caculation:	Real Latitude = (s	igned integer)[High 2 Bytes + Low 2 Byte	
40	0X0028	STSTEM REDUCT	Modem Mo	odel Types:		
Input Bits:			Type ID	Definition		
Bit Address	Hex Format	Definition	0	Unknow		
0	0x0000	INPUT 1	6	IPn3G		
1	0x0001	INPUT 2	7	VIP4G		
2	0x0002	INPUT 3		IPe 4C		
3	0x0003	INPUT 4	°	161140		

VIP4G/VIP4Gb

4.12.5.3 I	Modbus >	Modbus	Data	Map
------------	----------	--------	------	-----

-	D C III
ype ID	Definition
)	Unknow
1	8N1
2	8N2
3	8E1
1	801
i.	7N1
5	7N2
7	7E1
3	701
Э	7E2
10	702

Image 4-12-8: Tools > Modbus Data Map

4.12.6 Tools > Websocket

The Websocket service is a feature of HTML5.0 or later. Web Socket is designed to be implemented in web browsers and web servers to allow XML scripts to access the HTML web service with a TCP socket connection.

10

VIP4G/VIP4Gb

It is mainly used for two purposes:

- refreshing page information without refreshing the entire page to reduce network stream.
- to integrate internet applications with xml to get required information in real time.

Currently we provide four types of information as configured:

- GPS Coordinate Information
- GPS NMEA Data
- Carrier Information
- Comport Data

System Network Carrier	Wireless Comport	I/O GF	S Firewall	Router	VPN	MultiV	WAN Tools	
Discovery Netflow NMS S	ettings Event Repor	t Modbus	Websocket	Site Su	rvey	Ping 1	TraceRoute	Traffic
Web Socket Service								
Online Connected Data								
Browser Type: Chrome 47 Win	dows							
Status	Enable Web Socket Service	e 🔻						
Web Socket Port(default:7681)	7681	[100-65535]						
Data Fresh Interval(seconds)	10	[2-65535]						
Connect Password		(Blank for Dis	able)					
Max Keep Time(minutes)	60	(0:keep alive)						
GPS Coordinate	Disable Disable							
GPS NMEA Data	Disable Disable							
Carrier Information	Disable Enable							
Comport Data	Disabled (Please enable)	comport top se	erver.)					

Image 4-12-9: Tools > Web Socket Service

	Status
Enable or disable the web socket service in the VIP4G.	Values (selection)
	Enable / Disable
	Web Socket Port
Enter the desired web socket TCP port number. The default is 7681, and	Values (TCP port)
	7681

	Data Fresh Intervals
Enter in the time at which data is to be refreshed. The default is 10	Values (seconds)
seconds, the valid range is 2 to 65555 seconds.	10
	Connect Password
For added security a password can be required to connect to the web	Values
socket service. To disable, leave this field blank. The default is disabled.	(blank)
	Max Keep Time
This field determines how long the web socket is open once started/	Values (minutes)
continue to run indefinitely.	60
	GPS Coordinate
If enabled the VIP4G will report GPS coordinate data to the websocket.	Values (selection)
	Disable / Enable
	GPS NMEA Data
If enabled the VIP4G will report GPS NMEA data to the websocket.	Values (selection)
	Disable / Enable
	Carrier Information
If enabled the VIP4G will report carrier information to the websocket.	Values (selection)
	Disable / Enable
	Comport Data
If enabled, and the COM1 port is configured for TCP Server, the comport data will be reported to the web socket	Values (selection)
	Disable / Enable

VIP4G/VIP4Gb



4.12.7 Tools > Site Survey

Wireless Survey

The Wireless Survey feature will scan the available wireless channels for any other 802.11 wireless networks in proximity to the VIP4G. The Survey will display the Channel number the other networks are operating on, the MAC address, Encryption Type, Frequency and general signal level and quality information. This can be useful for finding available networks, or troubleshooting connection and sensitivity problems. If there are other networks operating on the same frequency, or a channel close to the one chosen, it can then be decided to try to use another channel.

eless Surve	ey								
e: Your WL	AN traffic will b	be interrupted during this	brief period.						
Start the	scan again								
lio1 <mark>Surv</mark> ey	Results								
Channel	SSID	MACDDR	Encryption	Frequency	RSSI	SNR	Noise	Signal Level	
1	PWII173001	00:0F:92 FE:00:C3	WPA/WPA2/PS	K 2.412GHz	-56 dBm	39 dB	-86 dBm	100%	
1	VIP4C679b	04 F0:21:0E:12:E5	WPA/WPA2/PS	K 2.412GHz	-60 dBm	35 dB	-90 dBm	100%	
1	SHAW-2EFB57	74:85:2A:42:6A:58	WPA/WPA2/PS	K 2.412GHz	-69 dBm	26 dB	-90 dBm	BÓN	
1	PWiilan3	00:0F:92:FF:FF:FF	WPA/WPA2/PS	K 2.412GHz	-50 dBm	45 d8	-86 dBm	100%	
1	Bob Marley	20 C9 D0 18 E0 28	WPA/WPA2/PS	K 2.412GHz	-73 dBm	22 dB	-90 dBm	73%	
1	PWiimicro	00.0F.92.FE.01 85	WPA/WPA2/PS	K 2.412GHz	-49 dBm	46 dB	-90 dBm	100%	
1	SHAW-EE9253	F8:08:8E:A6:DD:F9	WPA/WPA2/PS	K 2.412GHz	-70 dBm	25 dB	-90 dBm	83X	
1	SHAW-9D170F	8C:7F:3B.86:85:69	WPA/WPA2/PS	K 2.412GHz	-72 dBm	23 dB	-90 dBm	76%	
1		00.0F 92 FE 00 C8	WPA/WPA2/PS	K 2.412CHz	-48 dBm	47 dB	-86 dBm	100%	
1	ASUS-WIFI	38-2C-4A-A1:44-E0	WPA/WPA2/PS	K 2.412GHz	-49 dBm	46 dB	-89 dBm	100%	
1	VIP4Gddd	04:F0:21:12:36:C6	wpa/wpa2/ps	K 2.412GHz	-57 dBm	38 dB	-86 dBm	100%	
3	PWii-interface1	00:0F:92 FE:01:11	WPA/WPA2/PS	K 2.422GHz	-35 dBm	60 dB	-91 dBm	100%	

Image 4-12-10: Tools > Site Survey



4.12.8 Tools > Ping

Network Tools Ping

The Network Tools Ping feature provides a tool to test network connectivity from within the VIP4G unit. A user can use the Ping command by entering the IP address or host name of a destination device in the Ping Host Name field, use Count for the number of ping messages to send, and the Packet Size to modify the size of the packets sent.

mici	rohard syst	TEMS INC. 1000000000000000000000000000000000000
System Network Ca	rrier Wireless Comp	port I/O GPS Firewall Router VPN MultiWAN Tools
Discovery Netflow N	MS Settings Event Rep	port Modbus Websocket Site Survey Ping TraceRoute Traffic
Network Tools Ping		
Ping Network Utilities		
Ping Host Name	google.com	
Ping Count	4	
Ping Size	56	Ping Stop Clear
Please wait for output of "p 64 bytes from 216.58.216.2 64 bytes from 216.58.216.2 64 bytes from 216.58.216.2 64 bytes from 216.58.216.2 google.com ping statistic 4 packets transmitted, 4 pac round-trip min/avg/max = 1	nig -c + -s 50 google.com P 38: seq=0 ttl=55 time=154.46; 38: seq=1 ttl=55 time=151.088; 38: seq=2 ttl=55 time=164.823; cs kets received, 0% packet loss 50.651/253.007/545.462 ms	9 ms 59 ms 51 ms 52 ms 51 ms 52 ms 51 ms 52 ms

Image 4-12-11: Tools > Ping



4.12.9 Tools > TraceRoute

Network TraceRoute

The **Trace Route** command can be used to provide connectivity data by providing information about the number of hops, routers and the path taken to reach a particular destination.

miero	ohard syste	EMS INC.	10101	10101	010	10101 01010 10101 10110
System Network Carrie	er Wireless Compor	t I/O GPS	Firewall	Router VPN	MultiWAN To	pols
Discovery Netflow NMS	Settings Event Repo	rt Modbus	Websocket	Site Survey	Ping TraceRou	ite Traffic
Network TraceRoute						
TraceRoute Network Utilities						
	google.com	Run TraceRoute	e			
Tracerout Host Name	Stop TraceRoute Clear R	lesult	_			
raceroute to google. com (216. 1 74.198.28.241 (74.198.28.24 2 172.25.120.81 (172.25.120.8 3 10.118.20.2 (10.118.20.2) 14 4 24.153.3.89 (24.153.3.89) 14 5 69.63 248 233 (69.63 248.23 6 24.156.144.178 (24.156.144. 7 72.14.216.189 (72.14.216.18 8 209.85.143.154 (209.85.143. 9 216.239.51.227 (216.239.51. 10 ord31s22-in-f238.1e100.net	ate geogre.com 58.216.238, 30 hops max, 38 41) 295.632 ms 153.751 ms 12 11) 137.937 ms 135.732 ms 14 12.024 ms 138.831 ms 10.118, 18.720 ms 147.533 ms 134.08; 3) 140.875 ms 131.570 ms 40 178) 149.587 ms 149.724 ms 19) 412.341 ms 150.967 ms 13 154) 140.693 ms 150.108 ms 227) 156.449 ms 157.032 ms t (216.58.216.238) 148.525 m	byte packets 8.278 ms 1.889 ms 23.14 (10.118.23. 2 ms 0.302 ms 145.533 ms 8.560 ms 156.675 ms 152.194 ms \$ 147.815 ms 141.	14) 139.393 m 196 ms	5		
			Cop	oyright © 2012 Mid	crohard Systems Inc.	VIP4G_WIFI_N

Image 4-12-12: Tools > TraceRoute



4.12.10 Tools > Traffic

The Traffic menu shows a graphical display of the LAN traffic by day and month. It can be used to determine when there are high and low periods of LAN traffic over a period of time.

	HELWOIK	Carrier	Wireless	s Compoi	t I/0	GPS Fire	ewall Ro	outer VP	N Multi	IWAN Too	ls
scovery	Netflow	NMS Se	ttings E	vent Repo	rt Modb	us Webs	ocket S	ite Survey	Ping	TraceRout	a Traff
nstat - Ne	etwork Tra	ffic Monitor	tool								
raffic of I	Interface bi	r-lan									
br-Lan					12-46-45 16122	br-lan	/ bourlu	_	_	_	12/16/15 16
rx 1 tx 4 = 5 0.08	today 150 KiB 420 KiB 570 KiB kbit/s	tx = 0.	12/14/15 0 KIB 0 KIB 0 KIB 00 kbit/s	a. rx tx	11 time 150 KiB 420 KiB 520 KiB	1					
br-lan /	rx tx 0.00 / daily	Dec '15 150 KiB 420 KiB 570 KiB 570 KiB kbit/s		sin =	0/0 H10 ce 12/14/15 rx ■ tx A / Tome Totrob 12/16/15 16127	br-lan	10 19 29 21 2 / top 10	2 25 00 01 02 03	94 85 86 87	08 09 10 11 12 1	0 14 15 16 at 2 Table 15 12/16/15 16
br-lan / day 12/14/15	rx tx claily rx o KiB	Dec '15 150 KIB 420 KIB 570 KIB kbit/s	total o KiB	avg. rate	070 mib ce 12/14/15 rx ■ tx 4 × here terrete 12/16/15 16127 ■ rx ■ tx	br-lan	18 19 20 21 2 / top 10 ay rx	: 25 #0 #1 #2 #1 tx data available	04 05 06 07 tota	ee ee ie ii ii ii ii 1 avg. rat	2 14 15 16 et < Tooms Too 12/10/15 16 e
br-lan / day 12/14/15 12/16/15 estinated	rx = 0.00 / daily rx 100 K18 150 K18	Dec '15 150 KiB 420 KiB 570 KiB kbit/s tx 0 KiB 420 KiB	total o KiB 570 KiB	avg. rate 0.00 kbit/s 0.08 kbit/s	010 KID ce 12/14/15 rx tx A / Them Tableb 12/16/15 16:27	br-lan	10 10 20 21 2 / top 10 ay rx no	t 25 00 01 02 00 tx data available	04 05 06 07 tota	ee ee ie ii ii ii ii 	3 14 15 16 1 2/16/15 16 2/16/15 16 e
br-lan / day 12/14/15 12/16/15 estimated	rx tx = 0.00 / daily rx 0 K18 150 K18 	Dec '15 150 KiB 420 KiB 570 KiB hbit/s tx tx 420 KiB 420 KiB 	total o KiB 570 KiB	avg. rate 0.00 kbit/s 0.08 kbit/s	Co 12/14/15 rx E tx A / Team Teleph 12/16/15 16127 rx E tx A / Team Teleph tx	br1an	10 19 29 21 2 / top 10 ay rx no / monthly	t 23 00 01 02 07 tx data available	94 85 86 97 tota	ee ee ie ii ii ii 1 avg. rat	2 14 15 16 12/18/15 16 2 12/18/15 16 2 12/18/15 16
br-lan / day 12/14/15 12/16/15 estimated	rx tx = 0.00 / daily rx 150 Ki8 150 Ki8	Dec '15 150 ki8 420 ki8 hbit/s tx 0 Ki8 420 ki8 	total o KiB 570 KiB	avg. rate 0.00 kbit/s	c 12/14/15 rx tx A < Turner Turneb 12/14/15 rx tx A < Turner Turneb A < Turner Turneb	br-lan	10 10 20 21 2 / top 10 ay rx no / monthly rx	tx tx tx tx	94 eS eS e7 total	00 00 10 11 12 1 	2 14 15 16 41 - Come Tax 12/16/15 16 6 12/16/15 16 12/16/15 16

Image 4-12-13: Tools > Traffic



5.1 AT Command Overview

AT Commands can be issued to configure and manage the VIP4G, serial port (Serial), or by TCP/IP (telnet).

5.1.1 Serial Port

To connect and access the AT Command interface on the VIP4G, a physical connection must be made on the RS232 DB9 serial port labeled 'Serial'. A terminal emulation program (Hyperterminal, Tera Term, ProComm, Putty etc) can then be used to communicate with the VIP4G.

COM14 Properties		? ×	Default Settings:
Port Settings			Baud rate: 115200
Bits per second	115200	•	Data bits: 8
<u>D</u> ata bits	8	•	Parity: None
Parity	None	•]	Stop Bits: 1
Stop bits	1	•]	
Eow control	None	•	Flow Control: None
	1	Sestore Defaults	
	OK Canc	el Apply	

Image 5-1: Serial Port Settings

Once communication is established, a login is required to access the AT Command interface, once logged in, the AT Command Line Interface menu is displayed. Type "?" or Help to list the menu commands.

Phy Edda Marco Coll. Transfer Mida	
Ene Zolt Ziew Zell Trauzler Helb	
L 🖷 🗧 X ≈ B B'	
VIP46 login: admin Password:	Î
Entering character mode Escape character is '^l'.	
Command Line Interface VIP2>	E
VIP2> help	
Press Tab to fill in the rest of the Commands	
Commands available:	
help Show available commands	
history Show a list of previously run commands	
info system system information	
status diagnostic ping send ping to destination	
status diagnostic traceroute the connection route	
status connection Snow connection	
status notwork Show notwork status	
status network Show network status	
status network Show network status system logout Logout Command line Interface system reboot Reboot Command line interface	

Image 5-2: AT Command Window

Default Settings:

VIP4G login: admin

Password: admin



5.1.2 Telnet (TCP/IP)

Telnet can be used to access the AT Command interface of the VIP4G. The default port is TCP Port 23. A telnet session can be made to the unit using any Telnet application (Windows Telnet, Tera Term, ProComm etc). Once communication is established, a login is required to continue.



Image 5-3: Establishing a Telnet Session

A session can be made to the WAN IP Address (if allowed in the firewall settings) for remote configuration, or to the local RJ45 interface (default IP: 192.168.168.1).

Once a session is established a login is required to continue. As seen in the Serial port setup, the default login is **admin**, and the password is **admin**. Once verified, the AT Command Line Interface menu is shown and AT Commands can now be issued. (Type "?" or Help to list the commands)

Administrator: C:\Windows\s	ystem32\cmd.exe	
VIP4G login: admin Password: Entering character mod Escape character is '^	e]'.	•
Command Line Interface UIP2>		
help	Show available commands	
history	Show a list of previously run commands	
info	System info	
status	Display the system status	
system	Setting system configurations	
wifi	Set or Get wifi config	
lte	Set or Get lte config	
exit	Logout Command line Interface	
network	Set_or Get network config	
AT	AI Echo OK	
AT+TEST	AI Echo IESI	
ATH	Show a list of previously run AT commands	
HIL	List all available HI commands	
HI&R	Read modem active profile to editable profile	
	Display modem active profile	
	Enable configurations you have been entered	-
HI +MREB	Keboot the modem	

Image 5-4: Telnet AT Command Session



5.2 AT Command Syntax

The follow syntax is used when issuing AT Commands on the VIP4G

- All commands start with the AT characters and end with the <Enter> key
- Microhard Specific Commands start with +M
- Help will list top level commands (ATL will list ALL available AT Commands)
- To query syntax of a command: AT+<command name>=?
- Syntax for commands that are used only to query a setting: AT<command_name>
- Syntax for commands that can be used to query and set values:
 - AT<command_name>=parameter1,parameter2,... (Sets Values) AT<command_name>? (Queries the setting)

Query Syntax:

AT+MLEIP=? <Enter> +MLEIP: Command Syntax:AT+MLEIP=<IP Address>,<Netmask>,<Gateway> OK

Setting a value:

AT+MLEIP=192.168.0.1,255.255.255.0,192.168.0.1 <Enter> OK

Query a setting:

AT+MLEIP? <Enter> +MLEIP: "192.168.0.1", "255.255.255.0", "192.168.0.1" OK

A screen capture of the above commands entered into a unit is shown below:

```
Telnet 192.168.111.1
```

Image 5-5: Telnet AT Command Syntax

Once AT commands are entered, the changes are immediate.

ATO or ATA Exits the AT Command Line Interface.



	<i></i>
Description	Command Syntax
Echo OK.	AT <enter></enter>
Example	
Input: AT <enter> Response: OK</enter>	
	AT+TES
Description	Command Syntax
Echo TEST	AT+TEST <enter></enter>
Example	
Input: AT+TEST <enter> Response: AT ECHO TEST: :0</enter>	
	FA
Description	Command Syntax
Show a list of previously run commands.	ATH <enter></enter>
Example	
Input: ATH <enter> Response: AT Command history: 1. ATH 2. ATL 3. ATH</enter>	
	AT&
Description	Command Syntax
Read modem profile to editable profile. (Reserved)	AT&R <enter></enter>
Example	
Input: AT&R <enter> Response:</enter>	



		AT&
Description	Command Syntax	
Read modem active profile.	AT&V <enter></enter>	
Example		
Input: AT&V <enter> Response: &V: hostname:VIP4G timezone:MST7MDT,M3.2.0,M11.1.0 systemmode:gateway time mode:sync OK</enter>		
		AT&V
Description	Command Syntax	
Reserved.	AT&W <enter></enter>	
Example		
Input: AT&W <enter> Response: OK</enter>		
		AT+MRE
Description	Command Syntax	
Reboots the modem.	AT+MREB <enter></enter>	
Example		
Input:		

AT+MREB <enter> Response: OK. Rebooting...



	AT
Description	Command Syntax
Quit. Exits AT Command session and returns you to login prompt.	ATA <enter></enter>
Example	
Input: ATA <enter> Response: OK</enter>	
IPn3G Login:	
IPn3G Login:	AT
IPn3G Login: Description	AT Command Syntax
IPn3G Login: Description Quit. Exits AT Command session and returns you to login prompt.	AT Command Syntax ATO <enter></enter>
IPn3G Login: Description Quit. Exits AT Command session and returns you to login prompt. Example	AT Command Syntax ATO <enter></enter>

AT+CMGS

Description

Send SMS message. To send message CTRL+Z must be entered, to exit, ESC.

Command Syntax

AT+CMGS=<Phone Number><CR> text is entered <CTRL+Z/ESC>

Example

Input: AT+CMGS=4035553776 <enter>

4035553776 Test <ctrl+z>

Response: OK



AT+CMGR

Description

This command allows the application to read stored messages. The messages are read from the SIM card memory.

Command Syntax

AT+CMGR=<index>

Example

Input: AT+CMGR=<index><enter>

Response:

+CMGR: <stat>,<oa>,,<dt> <data> OK

Parameters:

<index> Index in SIM card storage of the message <stat> Status of Message in Memory (Text Mode) "REC UNREAD" Received unread messages "REC READ" Received read messages <oa> Originator Address String type <dt> Discharge Time String format: "yy/MM/dd,hh:mm:ss±zz" (year [00-99]/ month [01-12]/Day [01-31], Hour:Min:Second and TimeZone [quarters of an hour]) <data> SMS User Data in Text Mode String type

AT+CMGL

Description

This command allows the application to read stored messages by indicating the type of the message to read. The messages are read from the SIM card memory.

Command Syntax

AT+CMGL=<status> Status:

Olalus.

- 0 Lists all unread messages1 Lists all read messages
- 1 Lists all read messag
- 4 Lists all messages

Example

Input: AT+CMGL=1 <enter>

Response:

AT+CMGL=1 +CMGL: 0,"REC READ","+14035553776",,"2013/10/04,11:12:27-06" Test Message 1 +CMGL: 1,"REC READ","+14035553776",,"2013/10/04,11:12:53-06" Test Message 2 +CMGL: 2,"REC READ","+14035553776",,"2013/10/04,11:13:06-06" Another test message!
microhard systems INC.

Description

This command handles deletion of a single message from memory location <index>, or multiple messages according to <delflag>.

Example

Input: AT+CMGD=0,4 <enter>

Response: index=0 dflag=4

ΟK

Description

Modem Record Information

Example

Input: AT+GMR <enter> **Response:** +GMR: Hardware Version:v1.0.0 Software Version:v1.1.0 build 1060 Copyright: 2012 Microhard Systems Inc. System Time: Mon Dec 2 16:03:51 2013 OK

Command Syntax

AT+CMGD=<index>,<delflag>

- delflag: 0 - Deletes the message specified in <index>
- 1 Deletes all read messages
- 4 Deletes all messages

Command Syntax

AT+GMR <enter>

AT+GMI

Command Syntax

AT+GMI=<enter>

Example

Description

Input: AT+GMI<enter>

Response:

+GMI: 2012 Microhard Systems Inc. ΟK

Get Manufacturer Identification



AT+GMR

AT+CMGD

VIP4G/VIP4Gb 010



		AT+CNUM
Description	Command Syntax	
Check modem's phone number.	AT+CNUM <enter></enter>	
Example		
Input: AT+CNUM <enter> Response: +CNUM: "+15875558645" OK</enter>		
		AT+CIMI
Description	Command Syntax	
Check modem's IMEI and IMSI numbers.	AT+CIMI <enter></enter>	
Example		
Input: AT+CIMI <enter> Response: +CIMI: IMEI:012773002108403, IMSI:30272040698 OK</enter>	2933	
		AT+CCID
Description	Command Syntax	
Check modem's SIM card number.	AT+CCID= <enter></enter>	
Example		

Input: AT+CCID<enter> Response: +CCID: 89302720401025355531 OK



AT+MSYSI

Description

System Summary Information

Command Syntax

AT+MSYSI <enter>

Example

Input: AT+MSYSI <enter> **Response:** Carrier: Carrier: IMEI:012773002113114 SIMID:89302720401025355531 IMSI:302720406982933 Phone Num: +15878938645 Status: CONNECTED Network: ROGERS RSSI:WCDMA RSSI: 70 Temperature:51 degC Ethernet Port: MAC:00:0F:92:00:B3:3B IP:192.168.168.1 MASK:255.255.255.0 Wan MAC:00:0F:92:01:B3:3B Wan IP:0.0.0.0 Wan MASK:0.0.0.0 System: Device:VIP4G_MKT Product:VIP4G_WIFI_N Image:VIP4G Hardware:v2.0.0 Software:v1.1.6 build 1184-14

Copyright: 2012 Microhard Systems Inc. Time: Thu Jun 18 13:25:34 2015

AT+MMNAME

Description

Modem Name / Radio Description. 30 chars.

Example

Input: (To set value) AT+MMNAME=VIP4G_CLGY<enter> Response: OK

Input: (To retrieve value) AT+MMNAME=?<enter> Response: +MMNAME: VIP4G_CLGY OK

Command Syntax

AT+MMNAME=<modem_name>



AT+MLEIP

Description

Set the IP Address, Netmask, and Gateway for the local Ethernet interface.

Command Syntax

AT+MLEIP=<IPAddress>, <Netmask>, <Gateway>

Example

Input:

AT+MLEIP=192.168.168.1,255.255.255.0,192.168.168.1 <enter>
Response:
OK

AT+MDHCP

Description

Enable/Disable the DHCP server running of the local Ethernet interface.

Command Syntax

AT+MDHCP=<action>

- 0 Disable
- 1 Enable

Example

Input: AT+MDHCP=1 <enter> Response: OK

AT+MDHCPA

Description

Command Syntax

Define the Starting and Ending IP Address (range) assignable by DHCP on the local Ethernet interface.

AT+MDHCPA=<Start IP>, <End IP>

Example

Input: AT+MDHCPA=192.168.168.100,192.168.168.200 <enter> Response: OK



	AT+MEMAC
Description	Command Syntax
Retrieve the MAC Address of the local Ethernet interface.	AT+MEMAC <enter></enter>
Example	
Input: AT+MEMAC <enter> Response: +MEMAC: "00:0F:92:00:40:9A" OK</enter>	
	AT+MSIP
Description	Command Syntax
Set LAN static IP	AT+MSIP= <static address="" ip=""> <enter></enter></static>
Example	
Input: AT+MSIP=192.168.168.1 <enter> Response: +MSIP: setting and restarting network OK</enter>	
	AT+MSCT
Description	Command Syntax
Set LAN Connection Type.	AT+MSCT= <mode> Mode: 0 DHCP 1 Static IP</mode>

Example

Input: AT+MSCT=1 <enter> Response: OK



AT+MNTP

Description

Enable and define a NTP server.

Command Syntax

AT+MNTP=<status>,<NTP server> Status: 0 Disable

1 Enable

Example

Input: AT+MNTP=1,pool.ntp.org<enter> Response: OK

AT+MPIPP

Description

Enable/Disable IP-Passthrough

Command Syntax

AT+MPIPP=<Mode> Mode: 0 Disable 1 Ethernet

Example

Input: AT+MPIPP=1 <enter> Response: OK

AT+MCNTO

Description

Sets the timeout value for the serial and telnet consoles. Once expired, user will be return to login prompt.

Command Syntax

AT+MCNTO=<Timeout_s> 0 - Disabled

0 - 65535 (seconds)

Example

Input: AT+MCNTO=300 <enter> Response: OK



AT+MRTF

Description

Reset the modem to the factory default settings stored in non-volatile (NV) memory. Unit will reboot with default settings.

Command Syntax

AT+MRTF <action> Action: 0 pre-set action

- 1 confirm action
- OK

Example

Input: AT+MRTF=1 <enter> Response: OK

AT+MTWT

Description

Enable/Disable the Wireless Traffic Timeout. Unit will reset if it does not see any traffic from the carrier for the amount of time defined.

Command Syntax

AT+MTWT=<Mode>[,<Interval_s>,<Reboot Time Limit_s>] Mode: 0 Disable 1 Enable Reboot Time Limit:300-60000

Example

Input: AT+MTWT=1,1,300 <enter> Response: OK

AT+MSCMD

Description

Enable/Disable the Wireless Traffic Timeout. Unit will reset if it does not see any traffic from the carrier for the amount of time defined.

Example

Input: AT+MSCMD=1,1,403556767,4057890909<enter> Response: OK

Command Syntax

AT+MSCMD=<Mode>[,<Filter Mode>[,<Phone No.1>[,...,<Phone No.6>]]] Mode: 0 Disable 1 Enable SMS Command Filter Mode:

- 0 Disable
- 1 Enable Phone Filter
- ÖK



AT+MDISS

Description

Configure discovery mode service used by VIP4G and utilities such as "IP Discovery".

Command Syntax

AT+MDISS=<Mode>

- Mode: 0 Disable
- 0 Disable1 Discoverable

Example

Input: AT+MDISS=1 <enter> Response: OK

AT+MPWD

Description

Used to set or change the ADMIN password for the VIP4G.

Command Syntax

AT+MPWD=<New password>,<confirm password> password: at least 5 characters

Example

Input: AT+MPWD=admin,admin<enter> Response: OK

AT+MIKACE

Description

Enable or Disable IMCP ICMP keep-alive check.

Command Syntax

AT+MIKACE=<Mode> Mode:

0 Disable

1

Enable

Example

Input: AT+MIKACE=1<enter> Response: OK



AT+MIKAC

Description

Set ICMP Keep-alive check parameters.

Command Syntax

AT+MIKAC=<host name>, <interval in seconds>, <count>

Example

Input: AT+MIKAC=www.google.com,600,10<enter> Response: OK

AT+MDDNSE

Description

Enable/Disable DDNS.

Command Syntax

AT+MDDNSE=<Mode>

- Mode:
- 0 Disable
- 1 Enable

Example

Input: AT+MDDNSE=0<enter> Response: OK

AT+MDDNS

Description

Select DDNS service provider, and login credentials as required for DDNS services.

Command Syntax

AT+MDDNS=<service type>,<host>,<user name>,<password>

service type:

- 0 changeip
- 1 dyndns
- 2 eurodyndns
- 3 hn
- 4 noip
- 5 ods
- 6 ovh
- 7 regfish
- 8 tzo
- 9 zoneedit

Example

Input: AT+MDDNS=0,user.dydns.org,user,password <enter> Response: OK



Description

Example

AT+MEURD1 AT+MEURD2 AT+MEURD3 **Command Syntax** Define Event Report UDP Report No.1/2/3. AT+MEURD1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Ti me_s>] Mode: 0 Disable 1 Moden Event Report 2 SDP Event Report AT+MIKAC=www.google.com,600,10<enter> 3 Management Report

AT+MNMSR

Command Syntax

Enable NMS Report

1

AT+MNMSR=<Mode>[,<Remote Port>,<Interval Time_s>] Mode: Disable 0

Example

Description

Define NMS Report.

Input: AT+MNMSR=1,20200,300<enter> **Response:** 0K

> AT+MGPSR1 AT+MGPSR2 AT+MGPSR3 AT+MGPSR4

Description

Define GPS Report No.1/2/3/4.

Example

Input:

AT+MGPSR1=1,192.168.168.25,20175,600 <enter> Response: ΟK

Command Syntax

AT+MGPSR1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Ti me s>l Mode: Disable 0 1

Enable UDP Report

Input: **Response:** OK

AT+MCTPS

Description

Enable/Disable the Comport serial port. This port is located on the front of the VIP4G and is labelled as the SERIAL port. It is disabled by default allowing it to be used for Console/AT Commands. If enabled it can be used for data.

Command Syntax

VIP4G/VIP4Gb

AT+MCTPS=<Mode>

Mode: 0 Disable

010

1 Enable

Example

Input:

AT+MCTPS=0<enter> Response: OK

Description

Set Comport baud rate.

AT+MCTBR

Command Syntax

AT+MCTBR=<Baud Rate>

Baud Rate: 0 300

1 600

2 1200

3 2400

4 3600 5 4800

6 7200

7 9600

8 14400

9 19200 10 28800

11 38400

12 57600 13 115200

Example

Input: AT+MCTBR=13<enter> Response: OK



AT+MCTDF

Description	Command Syntax		
Set Comport data format	AT+MCTDF= <data format=""> Data Format: 0 8N1</data>		
Example	2 8E1		
Input: AT+MCTDF=0 <enter> Response: OK</enter>	3 801 4 7N1 5 7N2 6 7E1 7 701 8 7E2 9 702		
	AT+MCTDM		
Description	Command Syntax		
Set Comport data mode.	AT+MCTDM= <data mode=""> Data Mode: 0 Seamless 1 Transparent</data>		

Example

Input: AT+MCTDM=1<enter> Response: ΟK

AT+MCTCT

Description

Set Comport character timeout.

Example

Input: AT+MCTCT=0<enter> **Response:** ΟK

Command Syntax

AT+MCTCT=<timeout_s>



AT+MCTMPS

AT+MCTP

Description

Set comport maximum packet size.

Example

Input: AT+MCTMPS=1024<enter> **Response:** ΟK

Description

Set Comport port priority.

Command Syntax

Command Syntax

AT+MCTMPS=<size>

AT+MCTP=<Mode>

- Mode:
- 0 Normal Medium
- 1 High
- 2

Example

Input: AT+MCTP=0<enter> **Response:** ΟK

AT+MCTNCDI

Description

Enable/Disable Comport port no-connection data intake.

Command Syntax

AT+MCTNCDI=<Mode>

- Mode: 0
 - Disable
- Enable 1

Example

Input: AT+MCTNCDI=1<enter> **Response:** OK



AT+MCTMTC

Description

Set Comport modbus TCP configuration.

Command Syntax

AT+MCTMTC=<Status>, <Protection status>, <Protection Key> Status and Protection Status:

- 0 Disable
- Enable 1

Example

Input: AT+MCTMTC=0,0,1234<enter> **Response:** ΟK

AT+MCTIPM

Description

Set the Comport serial port IP Protocol Mode.

Example

Input: AT+MCTIPM=1<enter> **Response:** OK

Command Syntax

AT+MCTIPM=<Mode> Mode:

- TCP Client
- 0 **TCP** Server 1
- **TCP Client/Server**
- 2 3 UDP Point to Point
- 4 UDP Point to Multipoint(P)
- 5 UDP Point to Multipoint(MP)
- UDP Multipoint to Multipoint 6
- SMTP Client 7
- 9 SMS Transparent Mode
- 11 GPS Transparent Mode

AT+MCTTC

Description

Set Comport TCP Client parameters when IP Protocol Mode is set to TCP Client.

Command Syntax

AT+MCTTC=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>

Example

Input: AT+MCTTC=0.0.0.0.20002.60<enter> **Response:** 0K



AT+MCTTS

Description

Set COM2 TCP Server parameters when IP Protocol Mode is set to TCP Server.

Example

Input: AT+MCTTS=0,100,20002,300<enter> Response: OK

Command Syntax

AT+MCTTS=<Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s> Polling Mode: 0 Monitor

1 Multi-polling

AT+MCTTCS

Description

Set COM2 TCP Client/Server parameters when IP Protocol is set to TCP Client/Server mode.

Example

Input: AT+MCTCS=0.0.0.0,20002,60,0,100,20002,300<ent er> Response: OK

Command Syntax

AT+MCTTCS=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>, <Polling Mode>, <Polling timeout_s>,<Local Listener Port>, <Connection timeout_s> Polling Mode: 0 Monitor

1 Multi-polling

AT+MCTUPP

Description

Set COM2 UDP Point-to-Point parameters when IP Protocol is set to UDP Point-to-Point mode.

Command Syntax

AT+MCTUPP=<Remote Server IP>, <Remote Server Port>, <Liste ner Port>, <UDP timeout_s>

Example

Input: AT+MCTUPP=0.0.0.0,20002,20002,10<enter> Response: OK



Description

Module Input Status.

Example

Input: AT+MIS <enter> Response: +MIS: available input status INPUT 1: 0 open OK

AT+MOS

AT+MIS

Description

Module Output Status.

Example

Input: AT+MOS=0 <enter> Response: +MOS: available output status OUTPUT 1: 0 open OK

Input:

AT+MOS=1,1,1 <enter> Response: OK

Command Syntax

Command Syntax

AT+MIS

AT+MOS=<Mode>[,<Setting No.>,<Status>] Mode:

0 All Output Status
1 Output Setting
Setting No.: 1, 2, 3, 4(if output available)

- Status:
- 0 open
- 1 close



			AT
Description		Command Syntax	
Lists all availabl	e AT Commands.	ATL <enter></enter>	
Example			
ATL <enter></enter>			
AT Commands av	ailable:		
AT	AT Echo OK		
AI+IESI	AI Echo IESI	- de	
ATH	Show a list of previously run A1 comma	nas	
AIL	List all available AT commands		
ATAK	Reserved		
AT&V AT \$1.1/	Display modern active profile		
	Reserved Report the modern		
ATICMES			
	Read SMS with changing status		
	List SMSs with changing status		
	Delete SMSs		
AT+GMR	Modem Record Information		
AT+GMI	Get Manufacturer Identification		
AT+CNUM	Check Modem's Phone Number		
AT+CIMI	Check Modem's IMEI and IMSI		
AT+CCID	Check Modem's SIM Card Number		
AT+MSYSI	System summary information		
AT+MMNAME	Modem Name Setting		
AT+MLEIP	Set the IP address of the modem LAN E	thernet interface	
AT+MDHCP	Enable or disable DHCP server running	on the Ethernet interface	
AT+MDHCPA	Set the range of IP addresses to be ass	igned by the DHCP server	
AT+MEMAC	Query the MAC address of local Etherne	et interface	
AT+MSIP	Set LAN static IP		
AT+MSCT	Set LAN Connection Type		
AT+MNTP	Define NTP server		
AT+MPIPP	Enable or disable IP-Passthrough		
	Set console timeout		
	Reset the modern to the factory default	settings from non-volatile (NV) memory	
	Enable of disable trainc watchdog timer		
	Set discovery service used by the mode		
	Set password	111	
AT+MIKACE	Enable or disable ICMP keen-alive cher	k	
	Set ICMP keep-alive check	ĸ	
AT+MDDNSF	Enable or disable DDNS		
AT+MDDNS	Set DDNS		
AT+MEURD1	Define Event UDP Report No.1		
AT+MEURD2	Define Event UDP Report No.2		
AT+MEURD3	Define Event UDP Report No.3		
AT+MNMSR	Define NMS Report		
AT+MGPSR1	Define GPS Report No.1		
AT+MGPSR2	Define GPS Report No.2		
AT+MGPSR3	Define GPS Report No.3		
AT MODEDA	Define GPS Report No 4		



VIP4G/VIP4Gb

5.0 AT Command Line Interface

AT+MCTPS	Enable or disable com port
AT+MCTBR	Set com port baud rate
AT+MCTDF	Set com port data format
AT+MCTDM	Set com port data mode
AT+MCTCT	Set com port character timeout
AT+MCTMPS	Set com port maximum packet size
AT+MCTP	Set com port priority
AT+MCTNCDI	Enable or disable com port no-connection data intake
AT+MCTMTC	Set com port modbus tcp configuration
AT+MCTIPM	Set com port IP protocol mode
AT+MCTTC	Set com port tcp client configuration when IP protocol mode be set to TCP Client
AT+MCTTS	Set com port tcp server configuration when IP protocol mode be set to TCP Server
AT+MCTTCS	Set com port tcp client/server configuration when IP protocol mode be set to TCP Client/Server
AT+MCTUPP	Set com port UDP point to point configuration when IP protocol mode be set to UDP point to point
AT+MIS	Module Input status
AT+MOS	Module Output status and setting

010

Appendix A: Serial Interface

Module (DCE) 1	Host (Signal DCD →	e.g. PC) (DTE) IN	Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE, informing the DTE that a carrier is present). The interface conforms to standard RS-232 signals, so direct connection
2 3 4 5	$\begin{array}{ccc} & & & \\ \leftarrow & TX \\ \leftarrow & DTR \\ & & \\ & & SG \end{array}$	OUT OUT	to a host PC (for example) is accommodated.
6 7	DSR \rightarrow \leftarrow RTS	IN OUT	
8	CTS \rightarrow	IN	The signals in the asynchronous serial interface are described below:

OVIP4G/VIP4Gb

- **DCD** *Data Carrier Detect* Output from Module When asserted (TTL low), DCD informs the DTE that a communications link has been established with another MHX 920A.
- **RX** *Receive Data* Output from Module Signals transferred from the MHX 920A are received by the DTE via RX.
- TX Transmit Data Input to Module Signals are transmitted from the DTE via TX to the MHX 920A.
- **DTR** Data Terminal Ready Input to Module Asserted (TTL low) by the DTE to inform the module that it is alive and ready for communications.
- **SG** Signal Ground Provides a ground reference for all signals transmitted by both DTE and DCE.
- **DSR** Data Set Ready Output from Module Asserted (TTL low) by the DCE to inform the DTE that it is alive and ready for communications. DSR is the module's equivalent of the DTR signal.
- **RTS** *Request to Send* Input to Module A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.
- **CTS** *Clear to Send* Output from Module A "handshaking" signal which is asserted by the DCE (TTL low) when it has enabled communications and transmission from the DTE can commence. When hardware handshaking is used, the CTS signal indicates to the host that the DCE can receive data.
- Notes: It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

"DCE" and "module" are often synonymous since a module is typically a DCE device. "DTE" is, in most applications, a device such as a host PC.



Appendix B: IP-Passthrough Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the VIP4G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, a common application of the VIP4G is to access connected devices remotely. In order to do this, the VIP4G must be told how to deal with incoming traffic, where to send it to. To accomplish this there are three options :

- IP-Passthrough
- Port Forwarding
- DMZ (a type of Port Forwarding)

In this section we will talk about IP-Passthrough and how to configure the VIP4G and the connected device/PC to work with IP-Passthrough. IP-Passthrough means that the VIP4G is transparent, and all outside (WAN) traffic is simply sent directly to a single device connected to one of the physical LAN RJ-45 ports on the VIP4G (With exception of port 80, which is retained for remote configuration (configurable). Also, any traffic that is sent to the RJ45 port is sent directly out the WAN port and is not processed by the VIP4G.

IP-Passthrough is ideal for applications where only a single device is connected to the VIP4G, and other features of the VIP4G are not required. When in passthrough mode, most features of the VIP4G are bypassed, this includes the serial ports, the GPS features, VPN, the Firewall, and much more. The advantage of IP-Passthrough is that the configuration is very simple.

In the example below we have a VIP4G connected to a PC (PC2). The application requires that PC1 be able to access several services on PC2. Using Port Forwarding this would require a new rule created for each port, and some applications or services may require several ports so this would require several rules, and the rules may be different for each installation, making future maintenance difficult. For IP-Passthrough, PC1 only needs to know the Public Static IP Address of the VIP4G, the VIP4G would then automatically assign, via DHCP, the WAN IP to the attached PC2, creating a transparent connection.



Step 1

Log into the VIP4G (Refer to Quick Start), and ensure that DHCP is enabled on the Network > LAN page.

N DHCP		
DHCP	Enable -	
Start	192.168.168.100	
Limit	150	
Lease Time (in minutes)	720	

VIP4G/VIP4Gb

Step 2

Since PC2 requires port 80 to be used as its Web server port, port 80 cannot be used on the VIP4G, by default it retains this port for remote configuration. To change the port used by the VIP4G, navigate to the **System > Settings** page as seen below. For this example we are going to change it to port 8080. When changing port numbers on the VIP4G, it is recommended to reboot the unit before continuing, remember the new WebUI port is now 8080 when you log back into the VIP4G. (e.g. 192.168.168.1:8080).

HTTP Port	8080
HTTP SSL	Off -



Appendix B: IP-Passthrough Example (Page 2 of 2)

Step 3

Now IP-Passthrough can be enabled on the VIP4G. Under the Carrier > Settings tab, IP-Passthrough can be found. To enable this feature, select "Ethernet" from the drop down box. Once the changes are applied, whichever device is physically connected to the LAN RJ45 port, will dynamically be assigned the WAN IP Address. In this example, this would be 74.198.186.193.

The default IP address of 192.168.168.1 on the LAN is no longer available, but it is still possible to access and configure the VIP4G on the LAN side, by using the X.X.X.1 IP Address, where the first 3 octets of the WAN IP are used in place of the X's. (e.g. 74.198.186.1, and remember the HTTP port in this example was changed to 8080).

System	Network	Carrier	Wireless Co
Status	Settings	Keepalive	Traffic Watch
Carrier	Configurati	on	
Config	uration		
Car	rier status		Enable •
IP-Passthrough		Disable -	
DN	S-Passthrough	1	Disable
			Ethernet

Network Connection Details

VIP4G/VIP4Gb



Close

Step 4

Attach the remote device or PC to the RJ45 port of the VIP4G. The end device has to be set up for DHCP to get an IP address from the VIP4G (Or it needs the carrier IP set as a static IP). In the test/example setup we can verify this by looking at the current IP address. In the screenshot to the right we can see that the Laptop connected to the VIP4G has a IP Address of 74.198.186.193, which is the IP address assign by the cellular carrier for the modem.

Step 5 (Optional)

IP-Passthrough operation can also be verified in the VIP4G. Once IP-Passthrough is enabled you can access the VIP4G WebUI by one of the following methods:

- Remotely on the WAN side (usually the internet), using the WAN • IP, and the port specified for HTTP operation (or, if enabled, by using the HTTPS (443) ports), in this example with would be 74.198.186.193:8080.
- On the LAN side, by entering in the first 3 octets of the WAN IP and .1 for the fourth, so in our example 74.198.186.1:8080.

	Connection Duration	1 min 43 sec
WAN IP Address it should look something like shown in the	WAN IP Address	74.198.186.193 on LAN
image to the right, 74.198.186.193 on LAN.	DNS Server 1	64.71.255.198

Step 6

The last step is to verify the remote device can be accessed. In this example a PC is connected to the RJ45 port of the VIP4G. On this PC a simple apache web server is running to illustrate a functioning system. On a remote PC, enter the WAN IP Address of the VIP4G into a web browser. As seen below, when the IP Address of the VIP4G is entered, the data is passed through to the attached PC. The screen shot below shows that our test setup was successful.

C	4.198-186.193 合 v C
ľ	is the Web Server Running on the Microhard Laptop.
1	ou can read this, it means that the IP-Passthrough or Port Forwarding exercise works!



Appendix C: Port Forwarding Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the VIP4G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the VIP4G is to access connected devices remotely. In order to do this, the VIP4G must be told how to deal with incoming traffic, where to send it to. To accomplish this there are three options :

O10VIP4G/VIP4Gb

- IP-Passthrough
- Port Forwarding
- DMZ (a type of Port Forwarding)

In the previous section we illustrated how to use and setup IP-Passthrough. In this section we will talk about port forwarding. Port forwarding is ideal when there are multiple devices connected to the VIP4G, or if other features of the VIP4G are required (Serial Ports, Firewall, GPS, etc). In port forwarding, the VIP4G looks at each incoming Ethernet packet on the WAN and by using the destination port number, determines where it will send the data on the private LAN. The VIP4G does this with each and every incoming packet.

DMZ (a form of port forwarding) is useful for situations where there are multiple devices connected to the VIP4G, but all incoming traffic is destined for a single device. It is also popular to use DMZ in cases where a single device is connected but several ports are forwarded and other features of the VIP4G are required, since in passthrough mode all of these features are lost.

Consider the following example. A user has a remote location that has several devices that need to be accessed remotely. The User at PC1 can only see the VIP4G directly using the public static IP assigned by the wireless carrier, but not the devices behind it. In this case the VIP4G is acting a gateway between the Cellular Network and the Local Area Network of its connected devices. Using port forwarding we can map the way that data passes through the VIP4G.



Appendix C: Port Forwarding Example (Page 2 of 2)

Step 2

Determine which external ports (WAN) are mapped to which internal IP Addresses and Ports (LAN). It is important to understand which port, accessible on the outside, is connected or mapped to which devices on the inside. For this example we are going to use the following ports, in this case it is purely arbitrary which ports are assigned, some systems may be configurable, other systems may require specific ports to be used.

Description	WAN IP	External Port	Internal IP	Internal Port
VIP4G WebUI	74.198.186.193	80	192.168.168.1	80
PC2 Web Server	74.198.186.193	8080	192.168.168.20	80
PLC Web Server	74.198.186.193	8081	192.168.168.30	80
PLC Modbus	74.198.186.193	10502	192.168.168.30	502
Camera Web Server	74.198.186.193	8082	192.168.168.40	80

Notice that to the outside user, the IP Address for every device is the same, only the port number changes, but on the LAN, each external port is mapped to an internal device and port number. Also notice that the port number used for the configuration GUI for all the devices on the LAN is the same, this is fine because they are located on different IP addresses, and the different external ports mapped by the VIP4G (80, 8080, 8081, 8082), will send the data to the intended destination.

Step 3

Create a rule for each of the lines above. A rules does not need to be created for the first line, as that was listed simply to show that the external port 80 was already used, by default, by the VIP4G itself. To create port forwarding rules, Navigate to the *Firewall* > *Port Forwarding* menu. When creating rules, each rules requires a unique name, this is only for reference and can be anything desired by the user. Click on the "Add Port Forwarding" button to add each rule to the VIP4G.

Once all rules have been added, the VIP4G configuration should look something like what is illustrated in the screen shot to the right. Be sure to **"Submit"** the Port Forwarding list to the VIP4G.

For best results, reboot the VIP4G.

ternal Server IP 192.168.168.2 ternal Port 80 otocol Both •	Name	PLC_WS
ternal Server IP 192.168.168.2 ternal Port 80 otocol Both • sternal Port 8080	Source	4G 👻
ternal Port 80 otocol Both • eternal Port 8080	nternal Server IP	192.168.168.20
otocol Both	nternal Port	80
sternal Port 8080	Protocol	Both 👻
	External Port	8080

VIP4G/VIP4Gb

irewall Port For	warding	Sum	mary			
Name	Source		Internal IP	Internal Port	Protocol	External Port
PC2_WS	4G		192,168,168,20	80	Both •	8080
PLC,W5	4G	٠	192.168.168.30	80	Both •	8081
PLC_Modbus	4G	٠	192.168.168.30	502	Both •	10502
Camera	4G	•	192,168,168,40	80	Both -	8082

Step 4

Configure the static addresses on all attached devices. Port forwarding required that all the attached devices have static IP addresses, this ensure that the port forwarding rules are always correct, as changing IP addresses on the attached devices would render the configured rules useless and the system will not work.

Step 5

Test the system. The devices connected to the VIP4G should be accessible remotely. To access the devices:

For the Web Server on the PC, use a browser to connect to 74.198.186:193:8080, in this case the same webserver is running as in the IP-Passthrough example, so the result should be as follows:

Firelox Children http://74.198.186.193.8080/	+	Continuenting in	particular in programmers	
(3 74.198.186.193:8080				<u>☆</u> ▼C
This is the Web Server	r Running on the	Microhard La	aptop.	
If you can read this, it	means that the I	P-Passthrough	or Port Forward	ing exercise works!

To access the other devices/services: For the PLC Web Server: 74.198.186.193:8081, for the Camera 74.198.186.193:8082, and for the Modbus on the PLC telnet to 74.198.186.193:10502 etc.



Appendix D: Firewall Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the VIP4G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the VIP4G is to access connected devices remotely. Security plays an important role in M2M deployments as in most cases the modem is publically available on the internet. Limiting access to the VIP4G is paramount for a secure deployment. The firewall features of the VIP4G allow a user to limit access to the VIP4G and the devices connected to it by the following means

- Customizable Rules
- MAC and/or IP List
- ACL (Access Control List) or Blacklist using the above tools.

Consider the following example. An VIP4G is deployed at a remote site to collect data from an end device such as a PLC or RTU connected to the serial DATA port (Port 20001 on the WAN. It is required that only a specific host (Host A) have access to the deployed VIP4G and attached device, including the remote management features.



Step 1

Log into the VIP4G (Refer to Quick Start). Navigate to the Firewall > General tab as shown below and ensure that the Firewall is turned on by enabling the *Firewall Status*. Next block all WAN traffic by setting the *4G Request* to Block, and disable *4G Remote Management*. Be sure to Apply the settings. At this point it should be impossible to access the VIP4G remotely through its cellular connection.

System	Network Carrier	Wireless Comp	ort 1/0	GPS	Firewall	VPN	MultiWAN	Tools
Status	General Rules Port	t Forwarding M/	AC-1P List	Reset				
Firewal	I General							
Fire	wall Status	Enable *						
Firewa	I General Configuration							
WA	N Remote Management O	CENABLE * Disable						
4G	Remote Management 🔍	🛛 Enable 🖲 Disable						
WA	N Request 🔍	Block O Allow						
4G	Request 🔍	Block Allow						
LAN	to WAN Access Control 0	Block Allow						
LAN	to 4G Access Control 0	Block Allow						
Ant	i-Spoof 🔍	🗇 Enable 🖲 Disable						
Pac	ket Normalization 0	CEnable Disable						



Appendix D: Firewall Example (Page 2 of 2)

Step 2

Under the Rules tab we need to create two new rules. A rule to enable Host A access to the Remote Management Port (TCP Port 80), and another to access the device attached the to serial port (WAN TCP Port 20001).

Rule 1

Rule

		Carri	ier Wirele	55 00	mport	1/0	GPS	
Status (General	Rules	Port Forwa	rding	MAC-IP	List	Reset	
Firewall	Rules							
Firewall	Rules Confi	guration						
Pula	Namo	Dem	Mat					
ACTI	ON	Ken						
Sour		ACC	ept •					
Sour		40	74 46 496	Ta	40	4 74 40	400	
Sour		104.	71,40.120	10	10	4.71.40	.126	
Dest	ination •	4G	•					
Desti	ination IPs	0.0.0	J.U	10	25	5.255.2	55.255	
Desti	ination Port	80						
Proto	bcol	TCF	•					
Add	Rule							
							_	
System	Network	Carrie	r Wireless	Comp	ort I/() GP	S	in
System Status G	Network General F	Carrie tules	r Wireless Port Forward	Comp ling M	ort I/(AC-IP Lis) GP st Re	IS F	ir
System Status G Firewall F Firewall Rule b	Network General R Rules Rules Config	Carrie Rules	r Wireless Port Forward	Comp ling M	ort I/(D GP st Re	eset	ir
System Status C Firewall F Firewall I Rule N ACTIO	Network General R Rules Rules Config Vame	Carrie Rules uration Device	r Wireless Port Forward	Comp ling M	ort I/(D GP st Re	PS F	ir
System Status C Firewall F Firewall f Rule N ACTIO Source	Network General F Rules Rules Config Name	Carrie Rules uration Device Accep 4G	r Wireless Port Forward	Comp ling M	ort I/(D GP st Re	S F	īr
System Status C Firewall F Firewall F Rule N ACTIC Source Source	Network Seneral F Rules Rules Config Name N :e 0 :e IPS 0	Carrie Rules uration Device Accep 4G 184.71	r Wireless Port Forward pt V 4.46.126	Comp ling M	AC-IP Lis) GP st Re	'S F	ir
System Status C Firewall F Firewall R Rule N ACTIO Source Source Destii	Network Seneral R Rules Rules Config Name N ie O ie IPS O nation O	Carrie Rules uration Device Accep 4G 184.71 4G	r Wireless Port Forward pt V 1.46.126	Comp ling M	AC-IP Lis	5 GP st Re	IS F	
System Status C Firewall F Firewall R Rule N ACTIO Source Source Destii Destii	Network General R Rules Config Name N :e O :e IPS O nation O nation IPS O	Carrie Rules uration Device Accep 4G 184.71 4G 0.0.0.0	r Wireless Port Forward pt • 1.46.126 •	Comp ling M	ort I/(AC-IP Lis 184.7'	5. 255. 25	55 F	
System Status C Firewall F Firewall R Rule N ACTIO Source Source Destii Destii Destii	Network Seneral F Rules Rules Config Name NN :e O :e IPS O nation O nation IPS O nation Port O	Carrie Rules (uration Device 4G 184.71 4G 0.0.0.0	r Wireless Port Forward b b t 1.46.126 y	Comp ling M To	ort 1/4 AC-IP Lis 184.7 255.25	5 GP		
System Status C Firewall F Firewall R Rule N ACTIO Sourc Sourc Destin Destin Destin Proto	Network General F Rules Rules Config Name N :e O :e IPs O nation Prot O col	Carrie Rules Uration Device 4G 184.71 4G 0.0.0.0 20001 TCP	r Wireless Port Forward t V 1.46.126 V	Comp ling M To	ort 1/4 AC-IP Lis [184.7] [255.24	5. 255 25	55 F	

After each rule is created be sure to click the **ADD Rule** button, once both rules are created select the **Submit** button to write the rules to the VIP4G. The Firewall Rules Summary should look like what is shown below.

Name	Action	Src	Src IP From	Src IP To	Dest	Dest IP From	Dest IP To	Destination Port	Protocol
Rem_Mgt	Accept	WAN	▼ 184.71.46.126	184.71.46.126	WAN	• 0.0.0.0	255.255.255.255	80	
Device	Accept -	WAN	184,71,46,126	184,71,46,126	WAN	- 0.0.0.0	255 255 255 255	20001	TCP -

Step 3

Test the connections. The VIP4G should only allow connections to the port specified from the Host A. An alternate means to limit connections to the VIP4G to a specific IP would have been to use the MAC-IP List Tool. By using Rules, we can not only limit specific IP's, but we can also specify ports that can be used by an allowed IP address.



Appendix E: VPN Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the VIP4G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the VIP4G is to access connected devices remotely. In addition to Port Forwarding and IP-Passthrough, the VIP4G has several VPN capabilities, creating a tunnel between two sites, allowing remote devices to be accessed directly.

VIP4G/VIP4Gb

VPN allows multiple devices to be connected to the VIP4G without the need to individually map ports to each device. Complete access to remote devices is available when using a VPN tunnel. A VPN tunnel can be created by using two VIP4G devices, each with a public IP address. At least one of the modems require a static IP address. VPN tunnels can also be created using the VIP4G to existing VPN capable devices, such as Cisco or Firebox.

Example: VIP4G to VIP4G (Site-to-Site)



Step 1

Log into each of the VIP4Gs (Refer to Quick Start), and ensure that the Firewall is enabled. This can be found under Firewall > General. Also ensure that either WAN Request is set to Allow, which allows traffic to come in from the WAN, or that sufficient Rules or IP lists have been setup to allow specific traffic to pass through the VIP4G. Once that is complete, remember to "Apply" the changes.

Step 2

Configure the LAN IP and subnet for each VIP4G. The subnets must be different and cannot overlap.

Site A		Site B	
System Network Car	rrier Wireless	System Network Ca	arrier Wireless
Status <mark>LAN</mark> Routes GR	RE SNMP sdpS	Status LAN Routes G	RE SNMP sdpS
Network LAN Configuration	i)	Network LAN Configuratio	n
LAN Configuration		LAN Configuration	
Spanning Tree (STP)	On 💌	Spanning Tree (STP)	On 👻
Connection Type	Static IP 💌	Connection Type	Static IP 💌
IP Address	192.168.100.1	IP Address	192.168.10.1
Netmask	255.255.255.0	Netmask	255.255.255.0
Default Gateway	192.168.100.1	Default Gateway	192.168.10.1
LAN DNS Servers		LAN DNS Servers	
DNS Server 1		DNS Server 1	
DNS Server 2		DNS Server 2	
LAN DHCP		LAN DHCP	
DHCP Server	Enable 💌	DHCP Server	Enable 💌
Start	192.168.100.100	Start	192.168.10.100
Limit	150	Limit	150
Lease Time (in minutes)	2	Lease Time (in minutes)	2



Appendix E: VPN Example (Page 2 of 2)

Step 3

Add a VPN Gateway to Gateway tunnel on each VIP4G.

Summary Gate	eway To Gateway	Client To Gate	eway VPN Clie	ent Access Certifica	ate Management	
Summary						
Gateway To Gate	ewav					
Galeway TO Gale	eway	21 201020 1		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	1000200100 020	W12 (7 12 12)

VIP4G/VIP4Gb

1001



Step 4

Submit changes to both units. It should be possible to ping and reach devices on either end of the VPN tunnel if both devices have been configured correctly and have network connectivity.



Appendix F: GRE Example

The following pages outline the different GRE configurations available for the VIP4G. This may be useful in determining which fields are populated by showing a working example. Three different setups are shown: General GRE (without IPsec), GRE over IPsec (Transport Mode) and GRE over IPsec (Tunnel Mode).



Appendix F Image 1: Network Configuration Example Topology

Prerequisites:

- 1. Firewall > General > WAN Request Allow (Not Recommened), <u>OR</u> add a specific firewall rules (Recommened)
- 2. Add a route on PC-1: ip route add 192.168.169.0/24 via 192.168.168.1 dev eth0 Add a route on PC-2: ip route add 192.168.168.0/24 via 192.168.169.1 dev eth0

Status LAN WIFI Rou	utes GRE PIM-SM SNMP s	Statūs LAN WIFI Routes	GRE PIM-SM SNMP
Add a New Tunnel		Add a New Tunnel	
Name	gretest-23472	Name	gretest-21836
Enable	1	Enable	
Multicast	X	Multicast	
Πι	255	TTL	255
Kev	12345	Key	12345
ARP	1	ARP	
NAT	<u> </u>	NAT	\checkmark
Local Setup	_	Local Setup	
Gateway IP Address	184.151.234.72	Gateway IP Address	184.151.218.36
Tunnel IP Address	10.0.1.1	Tunnel IP Address	10.0.2.1
Netmask	255.255.255.0	Netmask	255.255.255.0
Subnet IP Address	192.168.168.0	Subnet IP Address	192.168.169.0
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Remote Setup	r	Remote Setup	
Gateway IP Address	184.151.218.36	Gateway IP Address	184.151.234.72
Subnet IP Address	192.168.169.0	Subnet IP Address	192.168.168.0
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
IPsec Setup	-	IPsec Setup	
Enable	None 🔻	Enable	None 🔻

Appendix F: GRE Example

Example 2: GRE over IPsec (Transport Mode)

dd a New Tunnel		Add a New Tunnel	
Name	gratect_23/72	Name	gretest-21836
Foable	gretest-20472	Enable	✓
Multicast	✓	Multicast	v
TTI	255	TTL	255
Kev	12345	Key	12345
	12345	ARP	✓
NAT		NAT	<u> </u>
Incal Setup		Local Setup	0
	101 151 001 70	Gateway IP Address	184 151 218 36
Gateway IP Address	184.151.234.72		10 0 2 1
Tunnei IP Address	10.0.1.1	Netmask	255 255 255 0
Netmask	255.255.255.0	Subnet IP Address	192 168 169 0
Subnet IP Address	192.168.168.0	Subnet Mack	255 255 255 0
Subnet Mask	255.255.255.0	Bemote Setup	255.255.255.0
Remote Setup		Remote Setup	
Gateway IP Address	184.151.218.36	Gateway IP Address	184.151.234.72
Subnet IP Address	192.168.190.0	Subnet IP Address	192.168.168.0
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Psec Setup		IPsec Setup	
Enable	GRE over IPsec 🔻	Enable	GRE over IPsec 🔻
Tunnel Mode	Transport 🔻	Tunnel Mode	Transport 🔻
Aggressive Mode		Aggressive Mode	
Local Security Gateway Type	IP Only 🔻	Local Security Gateway Type	IP Only 🔻
Local Gateway IP	184.151.234.72	Local Gateway IP	184.151.218.36
Local Next-hop Gateway IP	184.151.234.72	Local Next-hop Gateway IP	184.151.218.36
Local Subnet IP	192.168.168.0	Local Subnet IP	192.168.169.0
Local Subnet Mask	255.255.255.0	Local Subnet Mask	255.255.255.0
Local Subnet Gateway	192.168.168.1	Local Subnet Gateway	192.168.169.1
Remote Security Gateway Type	IP Only	Remote Security Gateway Type	IP Only 🔻
Remote Gateway IP	184.151.218.36	Remote Gateway IP	184.151.234.72
Remote Next-hop Gateway IP	184.151.218.36	Remote Next-hop Gateway IP	184.151.234.72
Remote Subnet IP	192.168.169.0	Remote Subnet IP	192.168.168.0
Remote Subnet Mask	255.255.255.0	Remote Subnet Mask	255.255.255.0
Phase1 Strict Mode:		Phase1 Strict Mode:	
Phase 1 DH Group	modp1024 🔻	Phase 1 DH Group	modp1024 V
Phase 1 Encryption	3des 🔻	Phase 1 Encryption	3des 🔻
Phase 1 Authentication	md5 🔻	Phase 1 Authentication	md5 🔻
Phase 1 SA Life Time(s)	3600	Phase 1 SA Life Time(s)	3600
Perfect Forward Secrecy		Perfect Forward Secrecy	
Phase2 Strict Mode:		Phase2 Strict Mode:	
Phase 2 DH Group	modp1024 V	Phase 2 DH Group	modp1024 V
Phase 2 Encryption	3des 🔻	Phase 2 Encryption	3des 🔻
Phase 2 Authentication	md5 🔻	Phase 2 Authentication	md5 🔻
Phase 2 SA Life Time(s)	28800	Phase 2 SA Life Time(s)	28800
	20000		
Preshared Key	•••••	Preshared Key	•••••
Preshared Key DPD Delay(s)	32	Preshared Key DPD Delay(s)	•••••• 32
Preshared Key DPD Delay(s) DPD Timeout(s)	32 122	Preshared Key DPD Delay(s) DPD Timeout(s)	32 122

010

VIP4G/VIP4Gb

microhard systems INC.

Example 3: GRE over IPsec (Tunnel Mode)

Appendix F: GRE Example

Add a New Tunnel gretest-23472 Name Enable ≤ Multicast \checkmark 255 ΠL Key 12345 ARP \checkmark NAT 1 Local Setup 172.16.1.1 Gateway IP Address Tunnel IP Address 10.0.1.1 Netmask 255.255.255.0 Subnet IP Address 192.168.168.0 Subnet Mask 255.255.255.0 Remote Setup 172.16.2.1 Gateway IP Address Subnet IP Address 192.168.169.0 255.255.255.0 Subnet Mask IPsec Setup Enable GRE over IPsec 🔻 Tunnel Mode Tunnel T Aggressive Mode Local Security Gateway Type IP Only • 184.151.234.72 Local Gateway IP 184.151.234.72 Local Next-hop Gateway IP Local Subnet IP 172.16.1.1 Local Subnet Mask 255.255.255.255 Local Subnet Gateway 172.16.1.1 Remote Security Gateway Type IP Only v 184.151.218.36 Remote Gateway IP Remote Next-hop Gateway IP 184.151.218.36 Remote Subnet IP 172.16.2.1 Remote Subnet Mask 255.255.255.255 Phase1 Strict Mode: Phase 1 DH Group modp1024 🔻 Phase 1 Encryption 3des v Phase 1 Authentication md5 🔻 Phase 1 SA Life Time(s) 3600 Perfect Forward Secrecy Phase2 Strict Mode: Phase 2 DH Group modp1024 🔻 Phase 2 Encryption 3des . Phase 2 Authentication md5 🔻 Phase 2 SA Life Time(s) 28800 Preshared Key • 32 DPD Delay(s) DPD Timeout(s) 122 DPD Action hold 🔻

Add a New Tunnel	
Name	gretest-21836
Enable	
Multicast	
TTL	255
Key	12345
ARP	
NAT	\checkmark
Local Setup	
Gateway IP Address	172.16.2.1
Tunnel IP Address	10.0.2.1
Netmask	255.255.255.0
Subnet IP Address	192.168.169.0
Subnet Mask	255.255.255.0
Remote Setup	
Gateway IP Address	1/2.16.1.1
Subnet IP Address	192.168.168.0
Subnet Mask	255.255.255.0
IPsec Setup	
Enable	GRE over IPsec 🔻
Tunnel Mode	Tunnel 🔻
Aggressive Mode	
Local Security Gateway Type	IP Only 🔹
Local Gateway IP	184.151.218.36
Local Next-hop Gateway IP	184.151.218.36
Local Subnet IP	172.16.2.1
Local Subnet Mask	255.255.255.255
Local Subnet Gateway	172.16.2.1
Remote Security Gateway Type	IP Only
Remote Gateway IP	184.151.234.72
Remote Next-hop Gateway IP	184.151.234.72
Remote Subnet IP	172.16.1.1
Remote Subnet Mask	255.255.255.255
Phase1 Strict Mode:	
Phase 1 DH Group	modp1024 🔻
Phase 1 Encryption	3des 🔻
Phase 1 Authentication	md5 🔻
Phase 1 SA Life Time(s)	3600
Perfect Forward Secrecy	
Phase2 Strict Mode:	
Phase 2 DH Group	modp1024 🔻
Phase 2 Encryption	3des 🔻
Phase 2 Authentication	md5 🔻
Phase 2 SA Life Time(s)	28800
Preshared Key	•••••
DPD Delay(s)	32
DPD Timeout(s)	122
DPD Action	hold 🔻

O10VIP4G/VIP4Gb



Appendix G: Firmware Recovery Procedure

In event that your unit becomes unresponsive it may be required to perform a firmware recovery procedure outlined below:

VIP4G/VIP4Gb

- 1. Download and save firmware file in a local folder, for example C:\;
- 2. Separate the PC from the network and set IP to static:

192.168.1.1 255.255.255.0

- 3. Connect PC Ethernet port to the Ethernet port of the modem to be recovered
- 4. Start a ping on the PC

C:\>ping 192.168.1.39 -t Pinging 192.168.1.39 with 32 bytes of data: Request timed out. Request timed out.

- 5. Power cycle modem while pressing and holding CFG(Config) button;
- 6. Release the CFG button when ping responded:

C:\>ping 192.168.1.39 -t Pinging 192.168.1.39 with 32 bytes of data: Request timed out. Request timed out. Reply from 192.168.1.39: bytes=32 time<1ms TTL=128 Reply from 192.168.1.39: bytes=32 time<1ms TTL=128

Note, If ping responds as shown above, then you can probably recover the unit, please proceed. Otherwise, send the unit back for RMA.

7. Now use TFTP to push firmware file into the corrupted unit:

For example, on Windows XP using following command line:

tftp -i 192.168.1.39 put VIPn4G-v1_1_0-r1084-14.bin (or the file saved).

8. Wait until above command to successfully transfered the image, similar message should show

Transfer successful: xxxxxx bytes in 5 seconds, nnnnnn bytes/s, note the number might change for different firmware file

Note, if you see message above, the unit will re-flash itself and reboot, otherwise call for help or send back for RMA.

9. Wait for the unit to recover and reboot.



Appendix H: Troubleshooting (FAQ)

Below is a number of the common support questions that are asked about the VIP4G. The purpose of the section is to provide answers and/or direction on how to solve common problems with the VIP4G.

010

VIP4G/VIP4Gb

Question: Why can't I connect to the internet/network?

Answer: To connect to the internet a SIM card issued by the Wireless Carrier must be installed and the APN programmed into the Carrier Configuration of the VIP4G. For instructions of how to log into the VIP4G refer to the Quick Start.

Question: What is the default IP Address of the VIP4G?

Answer: The default IP address for the LAN is 192.168.168.1.

Question: What is the default login for the VIP4G?

Answer: The default username is *admin*, the default password is *admin*.

Question: What information do I need to get from my wireless carrier to set up the VIP4G?

Answer: The APN is required to configure the VIP4G to communicate with a wireless carrier. Some carriers also require a username and password. The APN, username and password are only available from your wireless carrier.

Newer units may support an AUTO APN feature, which will attempt to determine the APN from a preconfigured list of carriers and commonly used APN's. This is designed to provide quick network connectivity, but will not work with private APN's. Success with AUTO APN will vary by carrier.

Question: How do I reset my modem to factory default settings?

Answer: If you are logged into the VIP4G navigate to the System > Maintenance Tab. If you cannot log in, power on the VIP4G and wait until the status LED in on solid (not flashing). Press and hold the CONFIG button until the unit reboots (about 8-10 seconds).

Question: I can connect the Carrier, but I can't access the Internet/WAN/network from a connected PC?

Answer: Ensure that you have DHCP enabled or manually set up a valid IP, Subnet, Gateway and DNS set on the local device.

Question: I connected a device to the serial port of the VIP4G and nothing happens?

Answer: In addition to the basic serial port settings, the IP Protocol Config has to be configured. Refer to the Comport Configuration pages for a description of the different options.



Appendix H: Troubleshooting

Question: How do I access the devices behind the modem remotely?

Answer: To access devices behind the VIP4G remotely, several methods can be used:

<u>A. IP Passthrough</u> - The VIP4G is transparent and the connected device can be access directly. Refer to The IP-Passthrough Appendix for a detailed example of how this may be deployed. <u>B. Port Forwarding/DMZ</u> - Individual external WAN ports are mapped to internal LAN IP's and Ports. See the Port-Forwarding Appendix for a detailed example. <u>C. VPN</u> - A tunnel can be created and full access to remote devices can be obtained. Required

VIP4G/VIP4Gb

the use of multiple modems or VPN routers. See the VPN Appendix on an example of how to set up a VPN.

Question: I have set up firewall rules and/or port forwarding rules but they do not work?

Answer: Ensure that the Firewall is *Enabled*. Even port forwarding requires that the firewall feature is enabled. If the WAN/4G request is blocked (recommended), additional rules will need to be created for any external request.

Question: I have Internet/4G access but I cannot ping the device remotely?

Answer: Ensure that the 4G/WAN request is enabled in the Firewall settings, or create a Firewall rule to allow ping messages.

Question: I'm using IP-Passthrough but the serial ports won't work?

Answer: When using IP-Passthrough, the WAN IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. As a result serials port will not work. The only port not being passed through is the remote management port (default port 80), which can be changed in the security settings.

Question: I'm using IP-Passthrough but the modem won't take my Firewall settings?

Answer: When using IP-Passthrough, the 4G IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. As a result the firewall settings have no effect on the unit, and is automatically disabled.

Question: I cannot get IP-Passthrough to work?

Answer: When using IP-Passthrough, the 4G IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. In order for IP-Passthrough to work, the connected local device *must* have DHCP enabled, or the 4G IP set as a static IP in the end device.



Appendix H: Troubleshooting

Question: Why does my modem reset every 10 minutes (or other time)?

Answer: There are a number of processes in the VIP4G that ensure that the unit is communicating at all times, and if a problem is detected will reboot the modem to attempt to resolve any issues:

1. Traffic Watchdog - Detects if there is any Wireless Traffic between the VIP4G and the Cellular Carrier. Will reboot modem when timer expires unless there is traffic. Carrier > Traffic Watchdog.

VIP4G/VIP4Gb

 Keepalive - Attempts to contact a configured host on a defined basis. Will reboot modem if host is unreachable. Enabled by default to attempt to ping 8.8.8.8. May need to disable on private networks, or provide a reachable address to check. Access via Carrier > Keepalive.
 Local Device Monitor - The VIP4G will monitor a local device, if that device is not present the VIP4G may reboot. Network > LocalMonitor.

Question: How do I set up VPN?

Answer: Refer to the VPN Appendix for an example.

Question: Why is the data usage on my modem so high?

Answer: Although it is impossible to answer that question without more detailed information about your modem, and the devices/application you are using, there are a number of things to keep in mind:

1. Always setup and configure a Firewall on the modem, this is especially important if the modem is using a publically accessible IP address.

2. Always change the default user/passwords.

3. Turn off any services that are not needed, such as GPS, Comports, SNMP, SSH, anything not being used specifically in your application.

4. Use the Data Usage alerts to keep informed of daily and monthly data usage of the modem to avoid surprises once the data bill arrives.



microhard systems inc.

VIP4G/VIP4Gb

1010

150 Country Hills Landing NW Calgary, Alberta Canada T3K 5P3

> Phone: (403) 248-0028 Fax: (403) 248-2762 www.microhardcorp.com