

Manuel Utilisateur

BulletPlus

4G / LTE Ethernet Deux SIM / Sériel / USB Passerelle w / Wi-Fi

Document: BulletPlus.Operating Manual.v1.3.1.fr.pdf FW: v1.3.0 Build 1016

Juillet 2016



This document is an automated translation. Refer to the English manual for the original text.

Ce document est une traduction automatique. Reportez-vous au manuel en anglais pour le texte original.



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

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



Garantie

Microhard Systems Inc. garantit que chaque produit est exempt de défauts de matériaux et de fabrication pour une période d'un (1) an pour ses produits. La garantie commence à la date à laquelle le produit est expédié par la seule responsabilité et la responsabilité de Microhard Systems Inc. Microhard Systems Inc. en vertu de cette garantie est de réparer ou de remplacer tout produit qui est retourné à elle par l'Acheteur et qui Microhard Systems Inc. détermine ne sont pas conformes à la garantie. Produit retourné à Microhard Systems Inc. pour le service de garantie seront expédiés à Microhard Systems Inc. aux frais de l'acheteur et seront retournés à l'acheteur aux frais de Microhard Systems Inc.. En aucun cas, Microhard Systems Inc. est responsable en vertu de cette garantie pour tout défaut qui est causée par la négligence, l'abus ou de mauvais traitements d'un produit ou pour toute unité qui a été altéré ou modifié de quelque façon. La garantie de remplacement prend fin avec la garantie du produit.

BulletPlus

Limitations de la garantie

microhard

MICROHARD SYSTEMS INC. NE DONNE AUCUNE GARANTIE DE QUELQUE NATURE QU'ELLE SOIT, EXPRESSE OU IMPLIC-ITE, EN CE QUI CONCERNE LES MATÉRIELS, LES LOGICIELS ET / OU DES PRODUITS ET DÉCLINE TOUTE ET TOUTES CES GARANTIES, Y COMPRIS, MAIS SANS S'Y LIMITER, LA GARANTIE DE NON-CONTREFAÇON, IMPLICITE GARANTIES DE QUALITÉ MARCHANDE À UN USAGE PARTICULIER, TOUTE INTERRUPTION OU PERTE DU MATÉRIEL, DES LOGICIELS, ET / OU D'UN PRODUIT, TOUT RETARD DANS LA FOURNITURE DU MATÉRIEL, DES LOGICIELS, ET / OU D'UN PRODUIT , OU TOUT RETARD DANS LA FOURNITURE DU MATÉRIEL, DES LOGICIELS, ET / OU D'UN PRODUIT , OU TOUTE AUTRE GARANTIE. L'ACHETEUR DÉCLARE ET GARANTIT QUE MICROHARD SYSTEMS INC. N'A PAS FAIT DE TELLES GARANTIES À L'ACHETEUR OU SES AGENTS MICROHARD SYSTEMS INC. EXPRESS GARANTIE À L'ACHETEUR CONSTITUE MICROHARD SYSTEMS INC. RESPONSABILITÉ UNIQUE ET RECOURS UNIQUES DE L'ACHETEUR. SAUF AINSI FOURNIS, MICROHARD SYSTEMS INC. EXCLUT TOUTE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE DE QUALITÉ MAR-CHANDE OU D'ADAPTATION À UNE PROMESSE PARTICULIER.

Microhard SYSTEMS INC. PRODUITS NE SONT PAS conçus ou destinés à être utilisés dans toute VIE SUPPORT DISPOSITIF LIÉS OU SYSTÈME LIÉS FONCTIONS NI DANS LE CADRE DE TOUTE AUTRE SYSTÈME CRITIQUE ET SONT ACCORDES AUCUNE GARANTIE FONCTIONNEL. Indemnité

L'acheteur devra indemniser Microhard Systems Inc. et de ses administrateurs, dirigeants, employés, successeurs et ayants droit, y compris des filiales, des sociétés liées ou affiliées, doit être libéré de toute manière d'agir, causes d'action, responsabilité, pertes, dommages, poursuites, cotisations, sommes d'argent, les frais (y compris les frais juridiques), dommages-intérêts généraux, dommages spéciaux, y compris, sans limitation, les réclamations pour blessures corporelles, la mort ou des dommages matériels liés aux produits vendus aux termes des présentes, les coûts et les exigences de chaque et tout type et nature que ce soit à la loi.

EN AUCUN CAS microhard SYSTEMS INC. NE SERA RESPONSABLE DE DOMMAGES INDIRECTS, SPÉCIAUX, IN-DIRECTS, ACCESSOIRES, INTERRUPTION DES ACTIVITÉS, CATASTROPHIQUE, PUNITIFS OU AUTRES DOM-MAGES POUVANT ÊTRE prétendais ARISE EN RELATION AVEC LE MATÉRIEL, QUELLE QUE SOIT LA THÉORIE JURIDIQUE DERRIÈRE CES RECLAMATIONS, QUE CE SOIT DANS UN DÉLIT, UN CONTRAT OU EN AUCUN LOIS LÉGALES OU RÉGLEMENTAIRES, RÈGLES, RÈGLEMENTS, DIRIGEANTS OU ADMINISTRATIVES ORDRES OU DECLARATIONS APPLICABLES OU AUTREMENT, MÊME SI microhard SYSTEMS INC. A ÉTÉ AVERTI OU A AUTREMENT CONNAISSANCE DE LA POSSIBILITÉ DE TELS DOMMAGES ET PREND AUCUNE ACTION pour prévenir ou minimiser TELS DOMMAGES. DANS LE CAS QUELLES QUE SOIENT LES EXCLUSIONS DE GARANTIE ET TIENDRA DISPOSITIONS INOFFENSIVES INCLUSES CI-DESSUS microhard SYSTEMS INC. Est en quelque sorte TENUE RESPONSABLE DE TOUT DOMMAGE OU DE BLESSURES, LA RESPONSABILITÉ DE microhard SYSTEMS INC. POUR ANYDAMAGES NE DOIT PAS DEPASSER LE PROFIT RÉALISÉ PAR microhard SYSTEMS INC . SUR LA VENTE OU DISPOSITION DU MATÉRIEL AU CLIENT.

Droits de Propriété

L'Acheteur reconnaît que Microhard Systems Inc. a un droit de propriété et de droits de propriété intellectuelle dans le matériel, les logiciels et / ou produits. L'acheteur ne doit pas (i) retirer tout droit d'auteur, secret commercial, d'une marque ou une autre preuve de la propriété de Microhard Systems Inc. ou d'intérêt ou de confidentialité d'autres avis de propriété de propriété contenus sur, ou, du matériel, du logiciel ou des produits, (ii) reproduire ou modifier tout matériel, logiciel ou produits ou faire des copies de celui-ci, (iii) désassembler, désosser ou décompiler tout logiciel ou copier celui-ci, en tout ou en partie, (iv) vendre, transférer ou mettre à disposition à d'autres le matériel , logiciel, ou les produits ou la documentation de celui-ci ou toute copie de celui-ci, sauf en conformité avec le présent accord.



Informations Utilisateur (suite)

À propos de ce manuel

Il est supposé que les utilisateurs des produits décrits ici ont soit l'intégration du système ou de l'expérience de la conception, ainsi que la compréhension des principes de base de communications radio.

Tout au long de ce manuel, vous rencontrerez non seulement des illustrations (qui approfondit encore plus sur le texte d'accompagnement), mais aussi plusieurs symboles dont vous devez être attentif à:



Attention ou Avertissement

Habituellement déconseillées une action qui pourrait entraîner des conséquences indésirables ou nuisibles.



Point à retenir

Faits saillants une clé caractéristique, le point, ou l'étape qui est remarquable. Garder à l'esprit ces simplifiera ou d'améliorer l'utilisation de l'appareil.



Pointe

Une idée ou une suggestion pour améliorer l'efficacité ou à améliorer l'utilité.



Information

Les informations concernant une technologie ou d'un concept particulier.

This document is an automated translation. Refer to the English manual for the original text.

Ce document est une traduction automatique. Reportez-vous au manuel en anglais pour le texte original.



Informations Utilisateur (suite)

Regulatory Requirements / Exigences Réglementaires



To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna being used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

Pour satisfaire aux exigences de la FCC d'exposition RF pour les appareils mobiles de transmission, une distance de séparation de 23cm ou plus doit être maintenue entre l'antenne de cet appareil et les personnes au cours de fonctionnement du dispositif. Pour assurer le respect, les opérations de plus près que cette distance n'est pas recommandée. L'antenne utilisée pour ce transmetteur ne doit pas être co-localisés en conjonction avec toute autre antenne ou transmetteur.



MAXIMUM EIRP

ECC Regulations allow up to 36dBm Effective Isotropic Radiated Power (EIRP). Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain cannot exceed 36dBm.

Réglementation de la FCC permettra à 36dBm Puissance isotrope rayonnée équivalente (EIRP). Par conséquent, la somme de la puissance transmise (en dBm), la perte de câblage et le gain d'antenne ne peut pas dépasser 36dBm.



EQUIPMENT LABELING / ÉTIQUETAGE DE L'ÉQUIPEMENT This device has been modularly approved. The manufacturer, product name, and FCC and Industry Canada identifiers of this product must appear on the outside label of the end-user equipment.

Ce dispositif a été approuvé de façon modulaire. Le fabricant, le nom du produit, et la FCC et de l'Industrie du Canada identifiants de ce produit doit figurer sur l'étiquette à l'extérieur de l'équipement de l'utilisateur final.

SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE : BulletPlus (Contains):

FCCID: NS915PX2 IC: 3142A-15PX2

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

Please Note: These are only sample labels; different products contain different identifiers. The actual identifiers should be seen on your devices if applicable. S'il vous plaît noter: Ce sont des exemples d'étiquettes seulement; différents produits contiennent des identifiants différents. Les identifiants réels devrait être vu sur vos périphériques le cas échéant.



CSA Class 1 Division 2 Option

CSA Classe 1 Division 2 est disponible uniquement sur les unités particulièrement marquées

Si marqué cette Classe 1 Division 2 - alors ce produit est disponible pour une utilisation en Classe 1 Division 2 , dans les groupes indiqués sur le produit .

Dans un tel cas, la suivante doit être remplie:

L'émetteur-récepteur n'est pas acceptable comme une unité autonome pour une utilisation dans des endroits dangereux . L'émetteur-récepteur doit être monté dans un boîtier séparé , qui est approprié pour l'application envisagée. Montage des unités dans une enceinte approuvée qui est certifié pour les emplacements dangereux , ou est installé à l'intérieur des lignes directrices , conformément aux règles de la CSA et le code électrique local et le feu , assurera une installation sûre et conforme .

La ligne d'alimentation d'antenne , câble d'alimentation CC et le câble d'interface doivent être acheminés à travers le conduit en conformité avec le National Electrical Code .

Ne pas connecter ou déconnecter l'équipement que l'alimentation est coupée ou que la zone est connue pour être non dangereux.

Installation, l'exploitation et la maintenance de l'émetteur-récepteur doivent être en conformité avec le manuel d'installation de l'émetteur-récepteur , et le National Electrical Code .

Falsification ou le remplacement des composants non - usine peut nuire à l'utilisation sécuritaire de l'émetteur-récepteur dans des endroits dangereux, et peut annuler l'approbation.

Les adaptateurs muraux fournis avec les émetteurs-récepteurs sont PAS classe 1, division 2 ont approuvé , et par conséquent, doit être alimenté pour les unités à l'aide des connecteurs de type vis ou verrouillage fournies par Microhard Systems Inc. et une Division 2 source d'alimentation de classe 1 au sein de votre panneau.

Si vous n'êtes pas sûr de l'installation et de câblage des lignes directrices spécifiques pour la classe 1 Division 2 codes , communiquer avec la CSA International.



Historique des Révisions

Revision	La description	Initials	Date
1.0	Préliminaire. (Firmware v1.3.0-r1009-28)	PEH	Nov 2015
1.1	Mise à jour firmware v1.3.0-R1010. Ajouté la bande passante, Filtre Cloud, Web Filter, multi WAN, GRE. mises à jour Divers à des cap- tures d'écran et le formatage.	PEH	Dec 2015
1.2	Mise à jour firmware v1.3.0-r1012. corrections divers, ajoutés VRRP, mise à jour Utilisation des données, Paramètres transporteurs.	PEH	Apr 2016
1.3	Mise à jour firmware v1.3.0-R1014.	PEH	May 2016
1.3.1	Divers. corrections.	PEH	June 2016



Table des Matières

1.0	Ove	erview	10
	1.1	Caractéristiques de performance	10
	1.2	Caractéristiques	11
	-		
2.0	DÉI	MARRAGE RAPIDE	13
	2.1	Installation de la carte SIM	13
	2.2	Mise en route avec Cellular	13
3.0	Car	actéristiques matérielles	17
	3.1	BulletPlus	17
		3.1.1 BulletPlus Dessins mécaniques	18
		3.1.2 BulletPlus Support de fixation (en option)	19
		3.1.2 BulletPlus Connecteurs et indicateurs	20
		3.1.2.1 Avant & Haut	20
		5. I.Z.Z AITIERE EL IALEI AIE	21
<u>م ۸</u>		nfiguration	າາ
4.0		Intorfaco utilisatour Woh	22
	4.0	101 Logon fenêtre	22
	4.1	Svstème	23
		4.1.1 Résumé	24
		4.1.2 Paramètres	25
		Nom d'hôte	25
		Console Timeout	25
		Date / Heure	26
		Paramètres du serveur NTP	27
		4.1.3 Services	28
		FTP	28
		Telnet	28
		HIIP/HIIPS	28
		4.1.4 Keepalive	29
		4.1.5 Maintenance	31
		Páinitialisar	১। 21
		Sauvegarde et restauration Configurations	32
		4 1 6 Réinitialiser	33
	4.2	Réseau	34
		4.2.1 Résumé	34
		4.2.2 LAN	35
		LAN DHCP	37
		VLAN Configuration	39
		4.2.3 WAN	40
		4.2.4 DHCP (Liaison MAC)	42
		4.2.5 DDNS	43
		4.2.6 Routes	44
		4.2.7 VKKP (Virtual Router Redundancy Protocol)	46 47
		4.2.8 PORS (SWICH)	4/
		4.2.9 Bande passante (Controle Inrottling)	4ð 40
		4.2.10 Liste des periprieriques	49 50
		4.2.11 I little Oloud (Oonlehit / Fille de Securite)	50
		4.2.12 web riner (MAO / Reseau de lineage de contenu)	53
			55

10101

4

10

BulletPlus



Table des Matières

4.3	Carrier	. 5	6
	4.3.1 Statut	. 5	6
	4.3.2 Paramètres	. 5	7
	Double gestion des cartes	. 5	8
	APN	. 5	9
	4.3.3 SMS	. 6	1
	434 SMS Config	6	1
	SMS Commandes	6	1
	SMS Alertes	6	3
	135 L'utilisation de données	6	5
	4.0.0 L'utilisation des données	0. 6	0
		. U	0
4.4		0	3
	4.4.1 Statut	. 6	9
	4.4.2 Radio1	. [0
	Radio1 Configuration de Phy	. 7	0
	Virtual Interface Radio	. 7	3
	4.4.3 Hotspot	. 7	6
4.5	Pare-feu	. 8	0
	4.5.1 Résumé	. 8	0
	4.5.2 Général	. 8	1
	4.5.3 Port Forwarding	. 8	3
	4.5.4 MAC-IP List	8	5
	455 Rèales	8	7
	456 Pare-feu par défaut	8	9
46	VPN	q	ň
4.0	161 Pácumá	a	ň
	4.6.1 Resume	. ອ ດ	1
	4.0.2 Passelelle Galeway	. ອ ດ	I G
		. 9	0
		. 9	ð
		. 9	8
	OpenVPN Client	. 1	01
	4.6.4 GRE	. 1	03
	4.6.5 VPN Users	. 1	06
	4.6.6 Certificate Managment	. 1	07
4.7	Routeur	. 1	80
	4.7.1 RIPV2	. 1	80
	4.7.2 OSPF	. 1	09
4.8	Série	. 1	10
-	4.8.1 Résumé	. 1	10
	482 Paramètres	1	11
	LISB	1	11
	Données bauds	1	12
	ID Protocol Config	. 1 1	11
		. I 4	14
		. I 4	14
		. 1 4	14
	ICP Client/Serveur	. 1	15
	UDP Point à Point	. 1	15
	SMTP Client	. 1	15
	PPP	. 1	16
	GPS Transparent Mode	. 1	17
4.9	I/O	. 1	18
	4.9.1 Paramètres	. 1	18



Table des Matières

4.10) GPS	120
	4.10.1 Emplacement	120
	4.10.2 Paramètres	121
	4 10 3 Rapport	122
	4 10 4 GPSGate	124
	4.10.5 Epregistreur	127
	4.10.5 Enregistred	120
		123
1 1 1	4.10.7 TAIF	122
4.1		100
		133
	4.11.1.1 TCP Modpus	133
	4.11.1.2 Serial (COM) Modbus	135
	4.11.1.3 Modbus Data Map	136
	4.11.2 Rapport Netflow	137
	4.11.3 Moniteur local	138
	4.11.4 Rapport d'événement	140
	4.11.4.1 Configuration	140
	4.11.4.2 Structure du message	141
	4.11.4.2 Message Payload	142
	4.11.5 Websocket	143
4.12	? Diag	145
	4.12.1 Ping	145
	4.12.2 Traceroute	145
	4.12.3 [perf.	146
4.13	Admin	148
	4 13 1 Utilisateurs	148
	4 13 2 Authentification (RADIUS)	150
	4 13 3 NMS	151
	4.13.4 SNMP	155
	4.13.5 La découverte	150
	4.13.5 La déconnector	150
	4.13.6 Se deconnecter	159
	O a man and the stanfa a a	400
5.0 AI	Command Line Interface	160
5.1	AT Aperçu Commande	160
	5.1.1 Port Série	160
	5.1.2 Telnet	161
5.2	AT Commande Syntaxe	162
5.3	Commandes AT Supportées	163
Annexe	es	212
Ann	exe A: Interface série	212
Ann	exe B: IP-Passthrough Exemple	213
Ann	exe C: Port Forwarding Exemple.	215
Ann	exe D [.] VPN (Site à Site) Exemple	217
Δnn	exe F [.] Firewall Rules Exemple	219
Δnn	exe F: Port Forwarding w/IP-Passtbrough (Iperf)	221
	eve G: Dénannade	223 223
AIII	eve O. Deparinaye	223



1.0 Overview

Le BulletPlus est une haute performance cellulaire double Ethernet Passerelles / Serial / USB w / WiFi, équipé 3x ports Ethernet RJ45, capacité de double SIM, analogiques programmables 2x / O, Standalone GPS, 802.11b / g / n WiFi, et une RS232 port de communication série.

Le BulletPlus utilise l'infrastructure cellulaire pour fournir un accès réseau aux appareils avec ou sans fil partout la couverture cellulaire est pris en charge par un opérateur cellulaire. Le BulletPlus supporte les connexions 4G / LTE avec des vitesses fulgurantes rapides.

Fournir une fonctionnalité de pont Ethernet cellulaire fiable de service ainsi passerelle pour la plupart des types d'équipements qui utilisent une interface RS232, RJ45 ou WiFi, le Bullet-Plus peut être utilisé dans un illimitées types d'applications telles que:

- Backbone haut débit
- Surveillance vidéo IP

communications sans fil

- la migration de réseau Legacy / périphérique
- SCADA (automates, Modbus, Hart)
- Voice over IP (VoIP)

Faciliter les

inter-réseaux

1.1 Caractéristiques de performance

Principales caractéristiques de performance de la Bullet Plus incluent:

- Les vitesses de connexion rapides et fiables à 4G, 3G, LTE et HSPA Networks • (varie selon le modèle)
- 2x programmables entrées analogiques / numériques ou jusqu'à 8 sorties • numériques
- DMZ et Port Forwarding •
- 3x ports Ethernet 10/100 (WAN/2LAN) •
- GPS autonome (Reporting Serveur TCP / UDP / SMTP)
- Interface utilisateur via la console, telnet, navigateur web local
- Compatibilité avec pratiquement tous les automates, RTU et autres périphériques • série RS232.
- Local à distance du firmware sans fil extensible
- L'utilisateur du pare-feu configurable avec IP / MAC ACL
- IPSec VPN sécurisé et GRE Tunneling
- Industrial Température Note (-40°C à + 85°C)



1.0 Aperçu

1.2 Caractéristiques					
BulletPlus	BulletPlus				
Bandes supportées : (Amérique du Nord)	LTE FDD (Bandes 1-5,7,8,13,17,18,19,20) UMTS DC-HSPA+ (Bandes 1,2,4,5,8) GSM GPRS EDGE (Bandes 2,3,5,8) 3GPP Protocole Stack Release 9				
Bandes supportées : (China)	LTE FDD: Band 1, 3, 8, all bands with diversity LTE TDD: Band 39, 40, 41(38), all bands with diversity DC-HSPA+/HSPA+/HSPA/UMTS: Band 1, 5, 8, 9, all bands with diversity TD-SCDMA: Band 34, 39, all bands with diversity GSM/GPRS/EDGE: 1800 MHz/900 MHz				
Caractéristiques techniqu (Amérique du Nord)	ues: LTE: DL 100 Mbps, UL 50 Mbps HSPA+: DL 42 Mbps, UL 5.7 Mbps HSPA+: DL 21 Mbps, UL 5.7 Mbps WCDMA: DL/UL 384 kbps EDGE Class 33: DL/UL 236.8 kbps GPRS Class 33: DL/UL 85.6kbps				
Caractéristiques techniqu (Chine)	LTE FDD: UL 50Mbit/s, DL 150Mbit/s @20M BW cat4 LTE TDD: UL 10Mbit/s; DL 112Mbit/s @20M BW cat4 TD-SCDMA PS: UL 384 kbit/s; DL 384 kbit/s TD-HSPA+: UL 2.2 Mbit/s; DL 4.2 Mbit/s DC-HSPA+: UL 5.76 Mbit/s; DL 42 Mbit/s HSPA+: UL 5.76 Mbit/s; DL 21.6 Mbit/s WCDMA PS: UL 384 kbit/s; DL 384 kbit/s WCDMA CS: UL 64 kbit/s; DL 64 kbit/s EDGE: UL 236.8 kbit/s; DL 236.8 kbit/s GPRS: UL 85.6 kbit/s; DL 85.6 kbit/s				
Général					
Interface Série : Serial Bauds : USB*:	RS232, RS485, RS422 300bps to 921kbps USB 2.0				

Interface Serie :	RS232, RS485, RS422
Serial Bauds :	300bps to 921kbps
USB*:	USB 2.0
(*avenir)	USB Port Console
	USB vers série de routage des données
	USB to Ethernet Routage des données (NDIS)

 $\begin{array}{l} \textbf{Consommation de courant:} \\ (@12VDC) \end{array}$

Modèle	AVG (mA)	w/Wi-Fi (AP)
BulletPlus	120	170
BulletPlus + données série	142	180
BulletPlus + Ethernet	155	195
BulletPlus Apogée	230	305



1.0 Overview

Ethernet :	2 x LAN 10/100 BaseT, Auto - MDI/X, IEEE 802.3 1 x WAN 10/100 BaseT, Auto - MDI/X, IEEE 802.3
I/O :	2x programmables analogiques / Entrées numériques ou jusqu'à sorties numériques 2x 60 mA récepteur de courant sur drain ouvert
SIM Card :	Dual: 1.8 / 3.0V Standard / taille de 2FF
Caractéristiques PPP :	Connexion à la demande / temps d'inactivité
Protocoles réseau :	TCP, UDP, TCP/IP, TFTP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP, QoS
Management :	Local console série, Telnet, WebUI, SNMP, FTP & Mise à jour sans fil, l'authentification RADIUS, IPsec VLAN
Diagnostics :	Température, RSSI, diagnostic à distance
Tension d'entrée :	7-30 VDC
Power over Ethernet :	Passif PoE sur le port Ethernet (WAN)
GPS :	Sensibilité: - acquisition autonome: -145 dBm - Sensibilité de suivi: -158 dBm (50% des correctifs valides) Précision de la position: - Suivi L1, le code CA - 12 canaux - Max. taux de mise à jour 1 Hz Erreur calculée emplacement moins de 11,6 mètres 67% du temps, et à moins de 24.2 mètres à 95% du temps
Ecologique	
Tompóraturo do fonction	noment : $40^{\circ}E(40^{\circ}C)$ to $19E^{\circ}E(9E^{\circ}C)$

Température de fonctionnement : -40°F(-40°C) to 185°F(85°C)

Humidité : 5% to 95% non-condensing

Mécanique

Dimensions :	2.21" (56mm) X 3.85" (97mm) X 1.46" (37mm)				
Poids :	Environ. 245 grammes				
Connecteurs :	Antenne : CELL, DIV, GPS: SMA femelle ANT3: RP-SMA femelle				
	Données : DE-9 femelle (avant RS232) Ethernet : 2x RJ-45				
	Exigences d'antenne GPS:				
	- Gamme de fréquences: 1575,42 MHz (GPS L1 Band)				
	- Bande passante: +/- 2 MHz				
	- Total NF <2.5dB				
	- Impédance 50 ohm				
	 Amplification (Gain appliqué au connecteur RF): 19dB à 23dB 				
	- Tension d'alimentation 1.5V à 3.05V				
	 Consommation de courant - 20mA typique (100mA max) 				
	 Puissance antenne cellulaire Rejet + Isolation: 				
	- 824-915 MHz> 10dB				
	- 1710 - 1785 MHz> 19dB				
	- 1850 - 1980 MHz> 23dB				



Ce guide de démarrage rapide vous guidera à travers l'installation et processus requis pour accéder à la fenêtre de configuration de WebUI et d'établir une connexion sans fil de base à votre opérateur.

Notez que les unités arrivent de l'usine avec le réseau local paramètre configuré comme «statique» (adresse 192.168.168.1 IP, le masque de sous-réseau 255.255.255.0 et la passerelle 192.168.168.1), en mode serveur DHCP. (Ceci est pour l'adaptateur Ethernet LAN à l'arrière de l'unité de BulletPlus.)

2.1 Installation de la carte SIM

✓ Avant les BulletPlus peut être utilisé sur un réseau cellulaire d'une carte SIM valide pour votre transporteur sans fil doit être installé. Insérez la carte SIM dans la fente comme indiqué, la fente inférieure SIM est pour SIM1: (Les contacts doivent faire face vers le bas, et l'encoche vers la droite)

Emplacement pour carte SIM



2.2 Mise en route avec Cellular

✓ Connectez l'antenne aux prises d'ANTENNE applicables de la BulletPlus.



 Branchez le connecteur d'alimentation à l'adaptateur d'alimentation et mettre sous tension l'appareil, la LED CPU clignote pendant le démarrage, une fois allumé, passez à l'étape suivante.





Pour rétablir les paramètres par défaut, appuyez et maintenez le bouton CFG pendant 8 secondes avec le Bullet plus sous tension. La LED clignote rapidement et le modem redémarre avec les paramètres par défaut.

۶ ۱

Utilisez l'adaptateur secteur fourni ou NHS une source de puissance équivalente. L'appareil peut également être alimenté par PoE à l'aide d'un injecteur PoE MHS.



✓ Connecter un PC configuré pour DHCP directement à un port LAN du BulletPlus, à l'aide d'un câble Ethernet. Si le PC est configuré pour DHCP, il acquiert automatiquement une adresse IP à partir du BulletPlus.



Ouvrez une fenêtre de navigateur et entrez l'adresse IP 192.168.168.1 dans la barre \checkmark d'adresse.



Le Bullet Plus sera alors demander un nom d'utilisateur et mot de passe. Entrez les pa- \checkmark ramètres par défaut indiqués ci-dessous.

Authentication Required	La connexion pa	r défaut d'usine:
The server http://192.168.168.1:80 requires a username and password. The server says: WebUI.	Nom d'utilisat Mot de passe:	eur: admin admin
User Name: admin Password: *******	Comme la vers -R1014 vous d mot de passe vous vous con mière fois.	ion firmware v1.3.0 evrez changer le par défaut lorsque nectez pour la pre-
Log In Cancel		



Les paramètres réseau par défaut:

IP: 192.168.168.1 Subnet: 255.255.255.0 Passerelle: 192.168.168.1

ſ₩,	
211	
\ 'J	

La connexion par défaut:

Nom d'utilisateur: admin Subnet: admin

Il est toujours une bonne idée de changer le login admin par défaut pour la sécurité future.

١.



✓ Une fois connecté, la page Résumé du système sera affiché.

m Network Ca	rrier Wireless Fire	wall VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
ary Settings Se	rvices Keepalive Ma	intenance	Reboot							
em Information										
tem information										
Host Name	UserDevice		[Description			myE	Bulletplus	-GPS	
Product Name	Bulletplus-GPS		s	system Date	9		201	6-05-16	10:33:47	
Hardware Version	1.0		s	system Upti	me		48 (min		
Software Version	v1.3.0		E	Build Date			201	6-05-09		
Software Build	1014		E	Build Time			10:	49:51		
Temperature (°C)	46.9		5	Supply Volta	age (V)		12.	23		
rier Information										
Module Status	Enabled		1	MEI			867	2230200	82723 🛈	
Current APN	wrstat.bell.ca		1	MSI		302	302610012606734			
Connection Status	Connected		5	SIM Card			REA	READY		
Network	N/A		5	IM Number	r (ICCID)		893	0261020	301083239	
Home/Roaming	Home		F	Phone Num	ber		158	7432793	9	
Current Technology	WCDMA		C	Cell ID			793	20699		
Service Mode WCDMA		C	Channel Nu	mber		108	1087			
IP Address	184.151.220.2		R	SSI (dBm)			-55	dBmIl	Ī	
DNS	70.28.245.227		F	RSCP (dBm)			-63			
DIND	184.151.118.254		E	CNO (dB)			-8			

✓ Comme on le voit ci-dessus sous l'état de porteur, la carte SIM est installée, mais un APN n'a pas été spécifiée. Réglage de l'APN à l'auto (par défaut) peut fournir une connectivité réseau rapide, mais peut ne pas fonctionner avec certains transporteurs, ou avec le secteur privé APN de. Pour définir ou modifier l'APN, cliquez sur l'onglet Paramètres> Carrier et entrez l'APN fourni par votre opérateur dans le champ APN. Certains transporteurs peuvent également nécessiter un nom d'utilisateur et mot de passe.

ystem Network Carrier	Wireless Firew	all VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
atus Settings SMS SMSC	onfig DataUsag	e								
Carrier Configuration										
Conoral										
General										
Carrier status 0	Enable 🔻									
IP-Passthrough	Disable 🔻									
MTU Size(500~1500/Blank) ❶										
SIM Selection	Dual SIM Car	ds ▼								
Dual Cards Management										
Primary Slot 🕕	SIM Card-1 V	1								
SIM Card-1 (Bottom slot) Settings										
SIM Number(ICCID) 0	89302610203	010832398								
Data Roaming	Disable 🔻									
Carrier Operator	Auto	•								
Technologies Mode	AUTO	T								
APN	wrstat.bell.ca		1							
Advanced+										
Network+										
SIM Card-2 (Top slot) Settings										
SIM Number(ICCID)	N/A									
Data Roaming	Disable ▼									
Carrier Operator	Auto	•								
Technologies Mode	AUTO	•								
APN	wrstat.bell.ca		1							
Advanced+										
Network+										

 Une fois que l'APN et toute autre information requise est entré pour se connecter à votre opérateur, cliquez sur «Soumettre».

۶ ۳

Auto APN: Le Bullet Plus va tenter de détecter le transporteur basé sur la carte SIM installée et faire défiler une liste d'APNs couramment utilisées pour fournir une connectivité réseau rapide.



✓ Sur le Carrier> Onglet Etat, vérifiez qu'une adresse IP WAN a été attribué par votre opérateur. Il peut prendre quelques minutes, alors essayez de rafraîchir la page si l'adresse IP WAN ne montre pas tout de suite. L'état d'activité devrait également montrer «Connecté».

System Network Carrier	Firewall VPN	MultiWAN	Serial	USB	I/0	GPS	Applications	Admin
Status Settings SMS SMSC	onfig DataUsag	je						
Carrier Status								
Carrier Status - LN930	\frown							
Current APN	wrstat.bell.ca		0	Core Ter	nperatu	re(°C)	36	
Activity Status	Connected		1	MEI			35640606	0021903
Network	Bell	/	5	SIM PIN	(Card-1)		READY	
Home/Roaming	Home		5	SIM Num	ber (IC	CID)	89302610	203010832398
Service Mode	E-UTRAN		F	Phone N	umber		15874327	939
Service State	E-UTRAN		F	RSSI (dB	n)		الس. 90-	
Cell ID	28963586		F	RSRP/Q	(dBm/d	B)	-87 / -6	
LAC	11204		9	SINR (dB)		17	
Current Technology	LTE		(Connect	on Dur	ation	10 min 16	sec
Available Technology	LTE, UMTS, GSM		١	NAN IP /	Address	(184.151.2	20.2
Frequency Pand(MHz)			[DNS Serv	/er 1		70.28.245	.227
riequency ballu(MHZ)	DANU_LIE_4		[DNS Ser	/er 2		184.151.1	18.254

- ✓ Si vous avez défini une adresse IP statique sur votre PC, vous devrez peut-être ajouter les serveurs DNS indiqués dans le Menu Etat Transporteur à votre PC pour permettre l'accès à Internet.
- ✓ Félicitations à vous! Votre BulletPlus est correctement connecté à votre cellulaire Carrier.
- Pour accéder à des périphériques connectés à BulletPlus à distance, un ou plusieurs des éléments suivants doivent être configurés: IP-Passthrough, Port Forwarding, DMZ. Une autre option serait de mettre en place un VPN.
- ✓ Assurez-vous que tous les mots de passe par défaut sont modifiés pour limiter l'accès au modem. (Version firmware v1.3.0-R1014 exige que les valeurs par défaut des mots de passe sont modifiés lors de la connexion initiale).
- ✓ Pour les meilleures pratiques et de limiter les frais de données, il est essentiel de bien configurer le pare-feu. (Il est particulièrement important pour les adresses IP publique statique.)



Veiller à la valeur par défaut des mots de passe sont modifiés.



Mettre en place des règles de pare-feu appropriés pour bloquer les données entrantes indésirables.



3.1 BulletPlus

Le BulletPlus est une unité entièrement fermée prêt à être relié à des périphériques externes avec connecteurs standard tel que discuté ci-dessous. Un support de montage en option peut être commandé pour permettre aux BulletPlus d'être monté pour une installation fixe.



Image 3-1: BulletPlus

Les balles plus Hardware caractéristiques comprennent:

- Connecteurs standard pour:
- 3x ports 10/100 Ethernet (RJ45 1xWAN / 2xLAN)
- Port de données (RS232 / DB9)
- 4-Pin: MATE-N-LOK Type de connecteur pour Power / I / O 1/2
- Antenne cellulaire (Connexion SMA femelle Antenne x2)
- Antenne GPS (SMA femelle Raccordement de l'antenne)
- WiFi Antenna (RP-SMA femelle Raccordement de l'antenne)
- Statut / diagnostic de LED pour RSSI (x3), Tx, Rx, GPS, CPU
- Dual SIM (Mini-SIM (2FF)) Connecteurs de cartes
- CFG Bouton pour les opérations de récupération d'usine par défaut / du firmware
- Connecteur USB 2.0



3.1.1 Dessins Mécaniques



Dessin 3-1: BulletPlus Top Voir Dimensions



Dessin 3-2: BulletPlus Retour Voir Dimensions



Dessin 3-3: BulletPlus Side View Dimensions

Remarque: Toutes les unités de dimension: Millimeter







Dessin 3-4: BulletPlus Top Voir Dimensions (Montré avec amovible TS35 Rail DIN)



Dessin 3-5: Bullet plus des supports de montage Dimensions

Remarque: Toutes les unités de dimension: Millimeter



3.1.3 Connecteurs et Indicateurs

3.1.3.1 Avant & Haut

Sur le devant de la Bullet est le bouton CFG, port USB, Main, GPS et diversité, GPS et WIFI Connecteurs d'antenne et fente pour carte SIM. Le sommet de la Bullet sont les indicateurs d'état, RSSI, Tx, RX, GPS et PWR.



Dessin 3-6: Bullet Front & Top View

Le port USB est un développement futur d'être disponible dans les versions ultérieures du firmware.

CFG (Button) - Maintenez ce bouton pendant la mise sous tension de la Bullet va démarrer l'appareil en mode SYSTÈME DE RÉCUPÉRATION FICHIER FLASH. L'adresse IP par défaut pour la récupération du système (seulement - pas pour un accès normal à l'unité) est statique: 192.168.1.39. Maintenez pendant 1 seconde pour le mode de récupération de httpd, 5 secondes pour le mode de récupération de tftp, ou 10 secondes pour maître reset. Si le bouton est maintenu pendant plus de 15 secondes sur le bouton sera ignoré.

Si l'appareil a été mis sous tension pendant un certain temps (> 1 minute), en appuyant sur le bouton CFG pour ~ 10 secondes (appareil redémarre) se traduira par DÉFAUT USINE en cours de restauration, y compris l'adresse IP usine statique. Cette adresse IP est utilisable dans un navigateur Web pour accéder à l'interface utilisateur Web.

Recevoir Signal Strength Indicator (RSSI) - Comme les augmentations de force de signal reçu, en commencant par le plus à gauche, le nombre d'actifs RSSI LED augmente.

Tx (Rouge) / Rx (vert) LED - Les LED Tx / Rx indiquent porteuse du trafic (cellulaire).

IP: 192.168.168.1 Subnet: 255.255.255.0 Passerelle: 192.168.168.1

Les paramètres réseau par

défaut:

GPS - Indique que le module GPS autonome en option est synchronisée et est prêt à l'emploi.



LED PWR - Le voyant d'alimentation indique que l'alimentation a été appliquée au module. Le clignotement indique un processus de démarrage.



Carte SIM - Ce slot est utilisé pour installer la carte SIM (s) fournie par le transporteur cellulaire. Assurez-vous que la carte SIM est correctement in-

stallée en prêtant attention à la figure imprimée à côté de la fente de la carte SIM. La fente du bas est
 SIM1, le contact doit faire face vers le bas, et l'encoche doit être à droite.

Signal (dBm)	RSSI1	RSSI2	RSSI3		
(-85, 0]	sur	Sur	sur		
(-90, -85]	sur	sur	FLASH		
(-95, -90]	sur	sur	de		
(-100, -95]	sur	FLASH	de		
(-105, -100]	sur	de	de		
(-109, -105]	FLASH	de	de		
Autre	balayage	balayage	balayage		

Tableau 3-1: LED RSSI



3.1.3.2 Arrière et Vue latérale

Sur le côté de la Bullet est le port de données (RS232) et sur le dos sont la puissance et Ethernet (PoE) interfaces et 2x Programmable I / O.



Dessin 3-7: BulletPlus arrière et Vue latérale

Le **Port de données** (RS232 DCE) sur le côté de l'appareil est utilisé pour des appareils de terrain sur la base de données RS232 de série à 300 bps à 921kbps.

Les ports **Ethernet** (2LAN / WAN) sont 10/100 Mbps RJ-45 interfaces utilisées pour connecter des appareils de terrain sur la base des dispositifs Ethernet.

Programmable I / O Le Bullet dispose de 2 programmables / Entrées analogiques ou numériques 2 sorties numériques. Charge maximale recommandée pour la broche de sortie est 150mA @ 30 Vdc (Vin).

Vin + / Vin- est utilisée pour alimenter l'unité. La plage d'entrée de tension est 7-30 Vdc.

PoE- Le Bullet peut également être alimenté par PoE passif sur le port Ethernet (WAN), par l'intermédiaire d'un injecteur PoE.

	Ethernet RJ45 Nombre Pin									
La source Tension1234567						8				
9 - 30 Vdc	D	D	D	DC+	DC+	D	DC-	DC-		

Tableau 3-3: Connexions Ethernet PoE

Nom	Épingle	Direction		
DCD	1	0		
RXD	2	0		
TXD	3	Ι		
DTR	4	Ι		
SG	5			
DSR	6	0		
RTS	7	I		
CTS	8	0		
RING	9	0		

Tableau 3-2: Données RS232 Affectation des broches





Attention: L'utilisation d'un bloc d'alimentation qui ne fournit pas la tension appropriée peut endommager le modem



all Summary - IPn4Gii Admin ×				
← → C ♠ [] 192.168.16			Q 57 =	
System Network	Crohard Systems in Carrier Firewall VPN MultiWAN S	NC. Serial USB 1/0 GP	Location - BrivGii Admin ×	 ∞ • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • <!--</th-->
Summary Settings System Information System Information	Services Keepalive Maintenance Re	boot	microhard systems inc	Plications Admin
Host Name Product Name Hardware Version Software Version	IPn4Gii_MKT IPn4Gii Rev A v1.2.0 build 1036	Description System Date System Uptime Temperature('C)	Location Settings Report CpsCate Recorder Load Record TAIP Location Map Waiting for valid CPS data_cetting for carrier's recent/celline location: Last Center's Lastude \$1.138461, Longstede-114.067350, Radius:1331m (Updot: The Mor 31 14 51 42 2015	
Carrier Information Module Status Current APN Connection Status Network Home/Roaming Current Technology Frequency Ban(MH IP Address DNS Server 1 DNS Server 2 LAN Status MAC Address IP Address Subnet Mask USB Port Status	Databage - Priddi Ada X Databage - Priddi Ada X Databage - Priddi Ada X Databage - Ada X Veneroda X Venerod	ii/carrier-datausage.sh VSTEMS INC. VMURWAN Serial USB argo Secol To Zero: your carrier's aculation on your me		
MAC Address Local IP Address	Satus Enable Di Latt config Time Tale Mar 3 Monthly Over Linit None Monthly Data Units U Byles Period Start Day II Dally Over Linit None Dally Data Units U Byles	Intal Usage Monitor International and the second s	a compared to a	au 2015 Googe Term of Lin Propert a mig-ter Auto Reflecting Intervet Too I in seconds Verw With Rim Map 13-2014 Microhard Systems Inc. IPr4Gil
			Submit « Cancel «	

4.0 Interface Utilisateur Web



Les paramètres réseau par défaut:

IP: 192.168.168.1 Subnet: 255.255.255.0 Passerelle: 192.168.168.1 Image 4-0-1: WebUI

La configuration initiale d'un BulletPlus en utilisant l'utilisateur Web (navigateur) Interface (interface Web) méthode implique les étapes suivantes:

- configurer une adresse IP statique sur votre PC pour correspondre à la sous-réseau par défaut ou si votre PC est configuré pour DHCP, il suffit de connecter un PC à un port LAN du BulletPlus et il sera attribué une adresse IP automatiquement.
- connecter le port BulletPlus ETHERNET (LAN) pour PC carte réseau à l'aide d'un câble Ethernet
- alimenter le BulletPlus et attendre environ 60 secondes pour que le système pour charger
- ouvrir un navigateur Web et saisissez l'adresse IP par défaut d'usine (192.168.168.1) de l'unité:
- fenêtre d'ouverture de session apparaît; connecter à l'aide par défaut Nom d'utilisateur: admin Mot de passe: admin
- utiliser l'interface utilisateur du navigateur Web pour configurer les BulletPlus selon les besoins.
- reportez-vous à la section 2.0: Démarrage rapide pour des instructions étape par étape.

Dans cette section, tous les aspects de l'interface de navigateur Web, présentés menus et options de configuration disponibles seront discutées.



4.0.1 Logon fenêtre

En accédant avec succès le BulletPlus à l'aide d'un navigateur Web, la fenêtre d'ouverture de session apparaît.

Authentication Required	Authentication Required ×
The server http://192.168.168.1:80 requires a username and password. The server says: UserDevice.	The server http://192.168.168.1:80 requires a username and password. The server says: UserDevice.
User Name: admin Password:	User Name: admin Password: *****
Log In Cancel	Log In Cancel

Image 4-0-2: Logon Fenêtre

Le nom par défaut de l'utilisateur est: admin

Le mot de passe par défaut est: admin

Notez que le mot de passe est sensible à la casse. Il doit être changé (discuté plus loin dans cette section), mais une fois changé, si oublié, ne peut pas être récupéré.

Lorsque entré, le mot de passe apparaît comme «points», comme indiqué dans l'image ci-dessous. Ce format d'affichage interdit aux autres de visualiser le mot de passe.

La case à cocher "Mémoriser mon mot de passe» peut être sélectionné pour des raisons de commodité, il est toutefois recommandé de veiller à ce qu'il soit désactivé - en particulier une fois que l'unité est déployée sur le terrain - pour une raison principale: la sécurité.

Si le BulletPlus est restauré aux valeurs par défaut du mot de passe est également restauré le mot de passe par défaut d'origine.

De la version de firmware v1.3.0-R1014, il est nécessaire de changer le mot de passe lors de la connexion initiale, une fois que le mot de passe est modifié, il sera nécessaire de se connecter à l'unité une fois de plus avec le mot de passe mis à jour.



Pour plus de sécurité, ne pas laisser le navigateur Web de se rappeler le nom d'utilisateur ou mot de passe.



Il est conseillé de changer le mot de passe de connexion. Ne pas oublier le nouveau mot de passe car il ne peut pas être récupéré.



4.1 Système

Les principaux onglets de catégorie situés en haut de la barre de navigation séparent la configuration des BulletPlus en différents groupes basés sur la fonction. L'onglet Système contient le sous-menu de ce qui suit:

•	Résumé	-	Résumé de l'état de la radio entière, y compris les paramètres réseau, les informations de version, et l'état de connexion radio
•	Paramètres	-	Hostname, Paramètres journal système, System Time / Date
•	Services	-	Activer / Désactiver et configurer les numéros de port pour SSH, Telnet, HTTP et services HTTPS
•	Keep Alive	-	Configurer système garder en vie pour assurer un accès réseau / Internet.
•	Entretien	-	Mises à jour du firmware à distance, réinitialisés aux valeurs par défaut, sauvegarde de la configuration et de restauration.
•	Réinitialiser	-	Calendrier redémarrages redémarrer et / ou immédiatement le système.
			-

4.1.1 Système> Résumé

L'écran Résumé du système est affiché immédiatement après la connexion initiale, montrant un résumé et le statut de toutes les fonctions des BulletPlus dans un seul écran. Ces informations comprennent l'état du système, l'état de porteur, cellulaire et LAN / WAN informations sur le réseau, les informations de version, etc.

stem Network C	arrier Wireless	Firewall VP	N Router	Serial	I/0	GPS	Apps	Diag	Admin		
mmary Settings S	ervices Keepaliv	e Maintenanc	e Reboot								
vstem Information											
System Information											
Host Name	UserDevic	e		Description	1		my	Bulletplu	is-GPS		
Product Name	Bulletplus	-GPS		System Dat	e		20	16-05-16	5 11:18:27		
Hardware Version	1.0			System Up	time		1:3	3			
Software Version	v1.3.0			Build Date			20	16-05-09)		
Software Build	1014			Build Time			10	49:51			
Temperature (°C)	47.8			Supply Vol	tage (V)		12	.23			
Carrier Information											
Module Status	Enabled			IMEI			86	722302(082723 🕕		
Current APN	wrstat.bel	l.ca		IMSI			30	2610012	2606734		
Connection Status	Connected	i		SIM Card				ADY			
Network	N/A	N/A			r (ICCIE))	89	3026102	03010832398		
Home/Roaming	Home		Phone Nun	iber		15	15874327939				
Current Technology	WCDMA			Cell ID			79	79320699			
Service Mode	WCDMA			Channel Number				87			
IP Address	184.151.220.2			RSSI (dBm)				dBm	J.		
DNS	70.28.245	5.227		RSCP (dBm)			-64	-64			
DNS	184.151.1	18.254		ECNO (dB)			-12	2			
LAN Status											
MAC Address	00:0F:92:	02:95:38									
IP Address	192.168.1	68.1		Mode					static		
Subnet Mask	255.255.2	255.0		Gateway			N/	N/A			
WAN Status											
MAC Address	00:0F:92:	03:95:38									
IP Address	N/A			Mode			dh	ср			
Subnet Mask	N/A			Gateway			N/	A			
DNS1				DNS2							
Radio 1 Interface 1 Status											
General Status											
MAC Address	Mode	SSID	Freque	ncy Rand	Ra	dio Fred	wency	Secu	rity Mode		
00:0F:92:FE:01:26	Access Point	TESTSSID	2.4G N	lode	2	462 GH7	a circy	WPA	2 (PSK)		
Traffic Status			2.1.01						. ,		
Receive Rutes	Receive	Packate	Tra	smit Bytee			Tran	Transmit Backets			
ACCEIVE Bytes	Receive	Receive Packets		ansmit Bytes			ridi	Transmit Packets			

Image 4-1-1: Système Fenêtre Info



La page Résumé du système sera d'actualisation automatique, chaque fois que cela se produit une petite quantité de données est utilisé. Si l'affichage sur le réseau cellulaire de ces données pourrait ajouter jusqu'à une quantité importante sur une longue période de temps.



4.1.2 Système> Paramètres

Les paramètres du système

Les options disponibles dans le menu Paramètres système permettent la configuration du nom d'hôte, Description, paramètres du serveur Console Timeout et du journal système.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summar	y Settings	Services	Keepalive	e Mainter	nance	Reboot							
System	Settings												
System	Settings												
						_							
Hos	t Name		Bullet	Plus-MKT									
Des	cription		myBul	letplus-GPS									
Con	Console Timeout (s) 120		[30 ~ 65535] 0-Disable										
CFC	Reset to Defau	et to Default Button 💿 Enable 🔍 Disable			e								
Syst	System Log Server IP/Name 0.0.0.0			0.0.0.0-Dis	able								
Syst	em Log Server	Port	514			Default: 51	4						
Time Se	ettings												
Cur	rent Date(yyyy-i	mm-dd)	2016-	04-26									
Cur	rent Time(hh:m	m:ss)	11:40	:08									
Dat	e and Time Sett	ing Mode	O Loc	al Time 💽 N	TP								
Tim	ezone		Moun	tain Time		•							
POS	IX TZ String		MST7	MDT, M3.2.0, N	v111.1.0								
NTF	Server IP/Nam	e	pool.n	tp.org]							
NTF	Server Port		123]							
NTF	Client Interval	(seconds)	0			[0 ~ 65535	0-Disable						

Image 4-1-2: Paramètres système> Paramètres système

Hć	ote Nom / La description						
Le nom d'hôte est un identifiant pratique pour une unité de BulletPlus	Valeurs						
unités: une référence croisée commode pour l'adresse WAN / IP Carrier l'unité. Ce nom apparaît lorsque connecté à une session de telnet, ou lorsque	BulletPlus (varie)						
l'appareil signale dans Microhard système NMS.	jusqu'à 30 caractères						
La description fournit un champ supplémentaire pour les caractères de texte, mais ne sont pas affichées partout, mais dans ce domaine.							
	Console Timeout (s)						
Cette valeur détermine quand une connexion de la console (fait via le port	Valeurs						
	60 0-65535						
CFG Réinitialiser les paramètres par défaut Bouton							
Activé par défaut, lorsque le bouton CFG sur le devant de la BulletPlus est	Valeurs						

maintenue enfoncée pendant 10s pendant que l'appareil est mis sous tension, l'appareil se réinitialise et tous les paramètres seront réinitialisés aux valeurs par défaut. Lorsqu'il est désactivé, l'appareil sera réinitialisé, mais les paramètres ne sera pas écrasé.

Activer Désactiver



Systè	eme Syslog Server IP
Le BulletPlus peut signaler des événements au niveau du système à un	Valeurs
rapportés par le BulletPlus.	0.0.0.0
Port ser	veur Syslog système
Entrez le port d'écoute UDP du serveur Syslog. Le numéro de port par défaut est généralement 514, mais peut varier de serveur à serveur	Valeurs
deladi est generalement o 14, mais peut vaner de serveur a serveur.	514

Time Settings

Les BulletPlus peut être configuré pour utiliser une source de temps locale, gardant ainsi le temps luimême, ou il peut être configuré pour synchroniser la date et l'heure via un serveur NTP. Les options et les menus disponibles va changer en fonction de la valeur actuelle de la date et de l'heure Réglage du mode, comme on le voit ci-dessous.

Date and Time Setting Mode	🖲 Local Time 🔍 NTP
Date (yyyy.mm.dd)	2015.03.31
Time (hh:mm:ss)	14:54:44
Date and Time Setting Mode	
Date and Time Setting Mode	 Local Time INTP
Date and Time Setting Mode Timezone	O Local Time NTP Mountain Time ▼
Date and Time Setting Mode Timezone POSIX TZ String	Cocal Time NTP Mountain Time MST7MDT,M3.2.0,M11.1.0
Date and Time Setting Mode Timezone POSIX TZ String NTP Server IP/Name	O Local Time NTP Mountain Time MST7MDT,M3.2.0,M11.1.0 pool.ntp.org
Date and Time Setting Mode Timezone POSIX TZ String NTP Server IP/Name NTP Server Port	O Local Time NTP Mountain Time MST7MDT,M3.2.0,M11.1.0 pool.ntp.org 123

Image 4-1-3: Paramètres système> Paramètres du Temps

Date et heure Réglage du mode

Valeurs

Sélectionnez le mode Date et heure Réglage nécessaire. Si défini pour 'Utiliser l'heure locale "l'unité gardera son temps et ne pas essayer de se synchroniser avec un serveur de réseau. Si 'Date et heure Over Network Synchroniser' est sélectionné, un serveur NTP peut être défini.

Use Local Time Source Synchronize Date And Time Over Network

Date

La date peut être saisie dans ce domaine. Notez que la valeur saisie est perdue doit les BulletPlus perdre de la puissance pour une raison quelconque.

Valeurs

2015.04.01 (varies)



Network Time Protocol (NTP) peut être utilisé pour synchroniser l'heure et les systèmes de date ou de l'ordinateur avec un système centralisé, serveur référencé. Cela peut aider à assurer que tous les systèmes d'un réseau ont la même heure et la date.



	Temps		
Le temps peut être entré dans ce domaine. Notez que la valeur saisie est perdue doit les BulletPlus perdre de la puissance pour une raison	Valeurs		
quelconque.	11:27:28 (variable)		
	Fuseau horaire		
Si la connexion à un serveur de temps NTP, spécifier le fuseau horaire dans la liste déroulante	Valeurs		
	Défini par l'utilisateur (ou hors de date)		
	POSIX TZ Chaîne		
Cela affiche la chaîne POSIX TZ utilisée par l'unité telle que	Valeurs		
	(Variable)		
	Serveur NTP		
Entrez l'adresse IP ou le nom de domaine du serveur de temps NTP	Valeurs		
	pool.ntp.org		
	NTP Port		
Entrez l'adresse IP ou le nom de domaine du serveur de temps NTP	Valeurs		
Soundite.	123		
	NTP client Intervalle		
Par défaut, le modem ne synchronise l'heure et la date lors du	Valeurs		
synchroniser à intervalles réguliers. Ce processus consomme des	0		



4.1.3 Système> Services

Certains services dans les BulletPlus peuvent être désactivés ou activés soit pour des considérations de sécurité ou des considérations ressources / puissance. Les Activer / Désactiver les options sont appliquées après un redémarrage et prendront effet après chaque mise sous tension. Les fonctions de démarrage / redémarrage / arrêt s'appliquent uniquement à la session en cours et ne seront pas conservés après un cycle d'alimentation.

System Ne	etwork	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summary S	ettings	Services	Keepaliv	e Mainter	nance	Reboot							
Services													
Services Statu	us												
FTP	€Ena	able ODisab	le					Updat	е				
Telnet	Ena	able ODisab	le	Port 2	3			Updat	е				
SSH	Ena	able ODisab	le	Port 2	2			Updat	е				
Web UI	●HT	TP/HTTPS		S Port 8	0	HTTP/ 443	HTTPS	Updat	е				
Microhard	d Sh 🔍 Ena	able Disab	le					Updat	е				

Image 4-1-5: Système> Services

	FTP
Le service FTP peut être activée / désactivée à l'aide du menu des	Valeurs
récupération du micrologiciel.	Enable / Disable
	Telnet
Utilisation du service Telnet Activer / Désactiver la fonction, vous	Valeurs
port utilisé par le service Telnet peut également être modifié. La valeur par défaut est 23.	23
	SSH
Utilisation du service SSH Activer / Désactiver la fonction, vous	Valeurs
modem. Le port utilisé par le service SSH peut également être modifié. La valeur par défaut est 22.	22
	Web UI
Le port du serveur Web par défaut pour les outils de configuration	Valeurs
443 (HTTPS).	HTTP/HTTPS
Changer au besoin, mais gardez à l'esprit que si un port non standard est utilisé, il doit être spécifié dans un navigateur Internet pour accéder à l'unité. (Exemple: http://192.168.168.1:8080).	HTTPS
	Microhard Sh

Réservé à un usage interne.



4.1.4 Système> Keep Alive

L'onglet Keep Alive permet la configuration des caractéristiques de garder en vie des BulletPlus. Le BulletPlus peut vérifier l'activité sur l'interface sans fil, la CLI (Command Line Interface), l'interface utilisateur Web, et veiller à ce qu'ils fonctionnent comme prévu. Dans le cas où l'BulletPlus ne détecte pas d'activité sur une interface, il va redémarrer pour tenter de résoudre les problèmes qui ont pu se produire.

1.1												+01
mi	oro	bord	avan		ING						40	1010
1111		naru	SYST	EMS	INC.	101	010	310	57	0	01	0101
Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
y Settings	Services	Keepalive	Mainter	nance	Reboot							
e Configurati	on											
ration												
ration												
alive		Enab	le 🔹									
affic Check		Enab	le 🔻									
Activity		Disab	le 🔹									
b UI Activity		Disab	le •									
pe		ICMP	•									
st Name		8.8.8.0	3		Test							
epalive Interval	0	300			[60-60000]	(s)						
epalive Retry 0	Ĩ.	20			[10-200]							
	Network Settings e Configurati ation alive affic Check Activity b UI Activity be st Name epalive Interval epalive Retry •	Network Carrier Settings Services e Configuration alive affic Check Activity b UI Activity be st Name epalive Interval © epalive Retry ©	Initial Stress Network Carrier Wireless Settings Services Keepalive Settings Services Keepalive e Configuration Enab Enab alive Enab Enab ffic Check Enab Enab Activity Disat Disat b UI Activity Disat Enab st Name 8.8.8.1 Band epalive Interval 300 Band applive Retry 20 Content	Imicrohard system Network Carrier Wireless Firewall Settings Services Keepalive Mainten Settings Services Keepalive Mainten e Configuration Enable Activity Disable Pressure alive Enable Compare ICMP Settings b UI Activity Disable Pressure Setting Setting st Name 8.8.8.8 Setting Setting <th>Mitcrohard systems Network Carrier Wireless Firewall VPN Settings Services Keepalive Maintenance e Configuration Maintenance Maintenance alive Enable Activity Disable Maintenance b UI Activity Disable Maintenance Maintenance be Enable Enable Enable Maintenance st Name 8.8.8.8 agalive interval 300 agalive interval 20</th> <th>Mitcrohard systems inc. Network Carrier Wireless Firewall VPN Router Settings Services Keepalive Maintenance Reboot e Configuration Maintenance Reboot alive Enable • </th> <th>Mitcrohard systems inc. Network Carrier Wireless Firewall VPN Router Serial Settings Services Keepalive Maintenance Reboot e Configuration alive Enable • effic Check Enable • Activity Disable • b UI Activity Disable • se ICMP • st Name 8.8.8.8 Test epalive Interval • 300 [60-60000](s) palive Retry • 20 [10-200]</th> <th>Mitcrohard systems inc. Network Carrier Wireless Firewall VPN Router Serial I/O Settings Services Keepalive Maintenance Reboot I/O Settings Services Keepalive Maintenance Reboot I/O e Configuration Settings Enable • Ific Check Ific Chec</th> <th>Mireless Firewall VPN Router Serial I/O GPS Network Carrier Wireless Firewall VPN Router Serial I/O GPS Settings Services Keepalive Maintenance Reboot Image: Color of the serial series Maintenance Enable • Activity Disable • Set Name Serial series Set Name Series series Sepalive Interval • 300 [60-60000](s) Sepalive Retry • 20 [10-200]</th> <th>Mitcroblatic systems inc. Network Carrier Wireless Firewall VPN Router Serial I/O GPS Apps Settings Services Keepalive Maintenance Reboot Image: Color of the serial series Network serial series Enable • Activity Disable • Set series ICMP • Set series 300 Good series Good series Series 300 Series 20</th> <th>Mireless Firewall VPN Router Serial I/O GPS Apps Diag Network Carrier Wireless Firewall VPN Router Serial I/O GPS Apps Diag Settings Services Keepalive Maintenance Reboot I/O GPS Apps Diag e Configuration Maintenance Reboot I/O GPS Apps Diag ation alive Enable • Ific Check Enable • Ific Check Enable • Ific Check Ific Disable • Ific Check Ific Office • Ific Check Ific Office • Ifi</th> <th>Mitcipation Systems inc. Network Carrier Wireless Firewall VPN Router Serial I/O GPS Apps Diag Admin Settings Services Keepalive Maintenance Reboot Image: Color Structure Admin e Configuration Maintenance Reboot Image: Color Structure Image: Color Structur</th>	Mitcrohard systems Network Carrier Wireless Firewall VPN Settings Services Keepalive Maintenance e Configuration Maintenance Maintenance alive Enable Activity Disable Maintenance b UI Activity Disable Maintenance Maintenance be Enable Enable Enable Maintenance st Name 8.8.8.8 agalive interval 300 agalive interval 20	Mitcrohard systems inc. Network Carrier Wireless Firewall VPN Router Settings Services Keepalive Maintenance Reboot e Configuration Maintenance Reboot alive Enable •	Mitcrohard systems inc. Network Carrier Wireless Firewall VPN Router Serial Settings Services Keepalive Maintenance Reboot e Configuration alive Enable • effic Check Enable • Activity Disable • b UI Activity Disable • se ICMP • st Name 8.8.8.8 Test epalive Interval • 300 [60-60000](s) palive Retry • 20 [10-200]	Mitcrohard systems inc. Network Carrier Wireless Firewall VPN Router Serial I/O Settings Services Keepalive Maintenance Reboot I/O Settings Services Keepalive Maintenance Reboot I/O e Configuration Settings Enable • Ific Check Ific Chec	Mireless Firewall VPN Router Serial I/O GPS Network Carrier Wireless Firewall VPN Router Serial I/O GPS Settings Services Keepalive Maintenance Reboot Image: Color of the serial series Maintenance Enable • Activity Disable • Set Name Serial series Set Name Series series Sepalive Interval • 300 [60-60000](s) Sepalive Retry • 20 [10-200]	Mitcroblatic systems inc. Network Carrier Wireless Firewall VPN Router Serial I/O GPS Apps Settings Services Keepalive Maintenance Reboot Image: Color of the serial series Network serial series Enable • Activity Disable • Set series ICMP • Set series 300 Good series Good series Series 300 Series 20	Mireless Firewall VPN Router Serial I/O GPS Apps Diag Network Carrier Wireless Firewall VPN Router Serial I/O GPS Apps Diag Settings Services Keepalive Maintenance Reboot I/O GPS Apps Diag e Configuration Maintenance Reboot I/O GPS Apps Diag ation alive Enable • Ific Check Enable • Ific Check Enable • Ific Check Ific Disable • Ific Check Ific Office • Ific Check Ific Office • Ifi	Mitcipation Systems inc. Network Carrier Wireless Firewall VPN Router Serial I/O GPS Apps Diag Admin Settings Services Keepalive Maintenance Reboot Image: Color Structure Admin e Configuration Maintenance Reboot Image: Color Structure Image: Color Structur

Image 4-1-6: Carrier> Keep Alive

	Keep Alive		
Activer ou désactiver les fonctions keep alive du modem. Si elle est désactivée l'utilisateur peut configurer le Traffic Check séparément	Valeurs		
L'unité sera de surveiller le trafic sur l'interface cellulaire.	Activer / Désactiver		
	Traffic Check		
Surveille le trafic sur l'interface cellulaire ainsi que l'interface WAN si le	Valeurs		
réseau. Si le Bullet détecte qu'il n'y a pas d'activité sur les interfaces ci -dessus, il va tenter un ICMP, HTTP ou DNS Lookup tel que configuré ci-dessous pour déterminer si le service a été perdu.	Activer / Désactiver		
	Activitó CL		
	ACTIVITE CEI		
Surveiller l'activité des CLI. Si la console ne sont pas accessibles au sein de la période qui est spécifiée par Console. Timeout dans	Valeurs		
Surveiller l'activité des CLI. Si la console ne sont pas accessibles au sein de la période qui est spécifiée par Console Timeout dans Réglages système page Web, le modem envoie la demande de connexion.	Valeurs Activer / Désactiver		
Surveiller l'activité des CLI. Si la console ne sont pas accessibles au sein de la période qui est spécifiée par Console Timeout dans Réglages système page Web, le modem envoie la demande de connexion.	Valeurs Activer / Désactiver Web UI Activité		
Surveiller l'activité des CLI. Si la console ne sont pas accessibles au sein de la période qui est spécifiée par Console Timeout dans Réglages système page Web, le modem envoie la demande de connexion.	Valeurs Activer / Désactiver Web UI Activité Valeurs		



	гуре
Une fois que la connexion est perdue, le modem envoie une des	Valeurs
le modem ne parvient pas à obtenir la réponse, il sera ré-envoyer la demande dans les secondes spécifiées par Keepalive Interval ci- dessous:	ICMP HTTP DNS Lookup
ICMP: Envoyer une requête "ping" HTTP: Envoyer une demande "wget" à un serveur HTTP Recherche DNS: Envoyer une demande "de dslookup" à un serveur DNS	
	Nom d'hôte
Indiquez une adresse IP ou le domaine qui est utilisé pour tester la connexion du modem. Le modem envoie les demandes de connexion à l'hôte spécifié.	Valeurs
à l'hôte spécifié.	8.8.8.8
	Keepalive Interval
La valeur d'intervalle détermine la fréquence, ou combien de fois,	Valeurs
d'abord tenter de ré-initialiser le modèle cellulaire avant d'effectuer un redémarrage complet du système, donc l'intervalle peut être retardé jusqu'à 120 secondes)	300
	Keepalive Retry
Le Keepalive Retry est le nombre maximum d'échecs de connexion tels que "Host unreachable" l'unité tentera avant que l'appareil se	Valeurs
réinitialise pour tenter de corriger les problèmes de connexion. Le nombre par défaut est 20, et la valeur en cours de validité est de 10 à 200.	20



4.1.5 Système> Maintenance

Mise à jour du firmware

les mises à jour du firmware occasionnels peuvent être libérés par microhard Systems qui peuvent inclure des corrections et / ou de nouvelles fonctionnalités. Le firmware peut être mis à jour sans fil en utilisant l'interface utilisateur Web.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summary	/ Settings	Services	6 Keepaliv	e Mainter	nance	Reboot							
System M	laintenance												
Version	Information												
Pro	luct Name		Hardware Typ	e	Buil	d Version			Build	Date		Build Time	e
Bull	etplus-GPS		1.0		v1.3	3.0 build 10	14		2016	-05-09		10:49:51	
Firmwar	e Upgrade												
Erase	Current Confi	gurations	Keep	All Configura	ations	•							
Firm	ware Image		Cho	ose file No f	ile chose	en							
Upgr	ade		Upgr	ade Firmware)								
Reset to	Default Configu	urations											
Rese	t to Default Co	nfigurations	Rese	to Default	•	Keep Carrier	Settings						
Backup (Configurations												
Conf	iguration File N	lame	Micro	hardBulletplu	IS-GPS.c								
Back	up		Back	Backup Configurations									
Restore	Configurations												
Selec	t Configuratio	n File	Cho	ose file No f	ile chose	n							
Chec	k Configuratio	n File	Chec	k Configuratio	on File								

Image 4-1-7: Maintenance > Firmware Upgrade

Effacer la configuration actuelle

Cochez cette case pour effacer la configuration de l'unité BulletPlus au cours du processus de mise à niveau. Ce sera mise à niveau et retourner l'appareil aux valeurs par défaut, y compris les adresses et les mots de passe IP par défaut. Ne pas vérifier la boîte conservera tous les réglages lors d'une procédure de mise à niveau du micrologiciel.

Valeurs

incontrôlé

Firmware Image

Utilisez le bouton Parcourir pour rechercher le fichier du firmware fourni par Systems microhard. Sélectionnez "Upgrade Firmware" pour démarrer le processus de mise à niveau. Cela peut prendre plusieurs minutes. Valeurs

(Pas par défaut)

Réinitialiser

Le BulletPlus peut être remise aux valeurs par défaut en utilisant le Réinitialiser option sous Système> Maintenance> Réinitialiser. * Attention * - Tous les réglages seront perdus !!!



Sauvegarde et restauration de configuration

La configuration des BulletPlus peut être sauvegardé dans un fichier à tout moment en utilisant la fonction de configuration de sauvegarde. Le fichier peut-il être restauré à l'aide de la fonction de configuration de restauration. Il est toujours une bonne idée de sauvegarder les configurations en cas de remplacement de l'unité. Les fichiers de configuration ne peuvent pas être modifiés en mode hors connexion, ils sont utilisés strictement pour sauvegarder et restaurer des unités.

MicrohardBulletplus.config	
Backup Configuration	
	Backup Configuration
Choose file No file chose	Downloading Configuration File, please wait Right click to save MicrohardBulletplus config
Check Restore File	Right click to save <u>micronardballetplus.coming</u>
	MicrohardBulletplus.config Backup Configuration Choose file No file chose Check Restore File

Restore Configuration	
The configuration looks good	1
Config file Name	MicrohardBulletplus.config
Generated	Mon Nov 9 13:13:56 MST 2015
Vendor	2014-2015 Microhard Systems Inc.
Product	Bulletplus-PWii
Hardware Type	Rev A
Restore	Keep Carrier Settings
Restore	Excep Carrier Settings

Image 4-1-8: Maintenance > Reset to Default / Backup & Restore Configuration

Nommez cette configuration / Configuration de la sauvegarde

Utilisez ce champ pour nommer le fichier de configuration. L'extension .config sera automatiquement ajouté au fichier de configuration.

Restaurer le fichier de configuration / Vérifiez Restaurer le fichier / Restaurer

Utilisez le bouton "Parcourir" pour trouver le fichier de sauvegarde qui doit être restauré à l'unité. Utilisez le bouton 'Check Restore File' pour vérifier que le fichier est valide, puis l'option pour restaurer la configuration est affiché, comme on le voit ci-dessus.

La zone Paramètres transporteurs Gardez peut être sélectionné avant que le processus de restauration est démarré, si elle est sélectionnée, les BulletPlus conservera les réglages porteurs actuels et ne pas les écraser avec les paramètres contenus dans le fichier de sauvegarde.



4.1.6 Système> Reboot

Le BulletPlus peut être redémarré à distance en utilisant le menu Système> Reboot. Comme on le voit cidessous un bouton «Redémarrer maintenant» est fourni. Une fois pressé, l'unité redémarre immédiatement et commence sa procédure de démarrage. Le BulletPlus peut également être redémarré sur une base régulière par la mise en place d'un horaire quotidien / hebdomadaire / mensuel.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summary	Settings	Services	Keepalive	Mainter	nance	Reboot							
Reboot N	low												
Config So	cheduled Ret	boot											
Schedule	No.1												
Statu	5		Enabl	e 🔹									
Туре	e		Rebo	ot Daily 🔹									
Tim	е		01 🔻	: <mark>01 ▼</mark>									
Schedule	No.2												
Statu	s		Enabl	e •									
Туре	e		Rebo	ot Weekly 🔹									
Day	s 🕕		1,			(Example:1,	2,3)						
Tim	е		01 🔻	: 01 🔻									
Schedule	No.3												
Status	s		Enabl	e •									
Туре	e		Rebo	ot Monthly 🔻]								
Day	s 🕕		6,			(Example:1,	2,3)						
Tim	e		01 🔻	: 01 🔻									

Image 4-1-9: Système> Reboot

	Status
Utilisez cette option pour activer ou redémarrages scolarisés	Valeurs
l'intervalle défini ci-dessous.	Désactiver / Activer
	Туре
Horaire quotidien, hebdomadaire ou mensuel redémarrages. Mise en place d'un calendrier de redémarrage peut aider à garder le modem	Valeurs
relié au support cellulaire et empêcher physiquement le redémarrage du modem si situé à une destination distante.	Reboot Daily Reboot hebdomadaire Reboot mensuel
	Days / Time
Si elle est définie pour chaque semaine, les jours sont comptés à partir du dimanche au samedi (0-6), et si défini mensuellement les jours sont	Valeurs
comptés 1 à 31. jours multiples peuvent être spécifiées en séparant par une virgule ','.	1,
Réglez l'heure de la journée (24 heures d'horloge) pour lequel redémarrer l'appareil.	



4.2 Réseau

4.2.1 Réseau> Résumé

L'écran Synthèse réseau donne une vue d'ensemble des interfaces réseau actuellement configurés, y compris le type de connexion (statique / DHCP), adresse IP, masque de réseau, la passerelle par défaut, DNS et IPv4 table de routage.

tem Netw	ork Carri	ier Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Dia	g	Admin	
us LAN V	VAN DDN	S Routes VR	RP Ports	Bandv	vidth De	evice Lis	t Clou	ıd Filte	r Wel	bfilte	r M	lultiWAN	
twork Status													
AM Dave Status													
AN FOIL STALUS													
General Stat	us												
IP Address		Connect	tion Type		Subne	t Mask			MAC A	ddres	5		
192.168.16	8.1	static			255.2	55.255.0			00:0F:	92:02:	95:3	8	
Traffic Statu	s												
Receive byte	es	Receive	Receive packets			nsmit bytes			Tra	nsmit	pack	ets	
361.273KB		3492			373	.656KB			228	31			
IAN Port Status													
General Stat	us												
IP Address		Connect	tion Type		Subne	t Mask			MAC A	ddress			
N/A		dhcp			N/A				00:0F:9	92:03:	95:38	8	
Traffic Statu	s												
Receive byte	es	Receive	e packets		Tra	nsmit bytes			Tra	nsmit	pack	ets	
OB		0			OB				0				
G Port Status													
General Stat	us												
IP Address		Connect	ion Type		Subnet	Mask			MAC	Addres	55		
184.151.22	0.2	static			255.25	5.255.252		00:0F:92:FE:00:01					
Traffic Statu	s												
Receive byte	es	Receive	e packets		Tra	nsmit bytes		Transmit packets					
514.780KB		4840			1.12	21 MB			511	0			
efault Gateway													
Gateway		184	.151.220.1										
NC													
G													
DNS Server(s)	70.2	8.245.227										
		104	151.110.254										
v4 Routing Tab	le												
Destination	l.	Gateway		Subnet I	Mask		Flags	Met	tric	Ref	Use	Interface	
0.0.0.0		184.151.220.1		0.0.0.0			UG	0		0	0	(br-wan2)	
184.151.22	0.0	0.0.0.0		255.255	.255.252		U	0		0	0	(br-wan2)	
192.168.16	8.0	0.0.0		255.255	.255.0		U	0		0	0	(br-lan)	

lmage 4-2-1: Réseau> État du réseau



4.2.2 Réseau> LAN

Configuration Port LAN

Les BulletPlus propose 2 ports LAN qui peuvent être utilisés pour la connexion de périphériques sur un réseau local. Le port WAN peut aussi être comblé avec le LAN offrant ainsi jusqu'à 3 ports LAN. Par défaut, l'a une adresse IP statique attribuée, 192.168.168.1. En outre, par défaut, le LAN est en cours d'exécution d'un serveur DHCP pour fournir des adresses IP à des périphériques qui sont connectés au port LAN physique (s) (directement ou par l'intermédiaire d'un commutateur).

System	Network	Carrier	Wireles	s Firewall	VPN	Router	Seria	I/0	GPS	Apps	Diag	Admi	n
Status	LAN WAN	DHCP E	DDNS RO	outes VRRI	P Ports	Bandwi	dth D	evice Li	st Clo	ud Filte	r Wel	ofilter	MultiWAN
Networ	Network LAN Configuration												
LAN In	terfaces Settings												
No	. Name	Static IP	Address		Prot	ocol	DHO	P Server		(Config		
1	lan	192.168.	.168.1		stati	c	On					Ed	it
Ac	ld												
VLAN Configuration VLAN Mode 802.1Q Port Isolation New VLAN 													

Image 4-2-2: Réseau> Configuration du réseau LAN

LAN Ajouter / Modifier Interface

Le BulletPlus a la capacité d'avoir plusieurs SSID pour la radio WiFi. Nouvelles interfaces peuvent être ajoutés pour SSID supplémentaires, et il dispose, le cas échéant, des sous-réseaux distincts pour chaque SSID. Par défaut toutes les interfaces supplémentaires ajoutées assignera automatiquement des adresses IP aux dispositifs de connexion via DHCP. Des interfaces supplémentaires ne peuvent être utilisés par WIFI supplémentaire (interfaces virtuelles) de SSID.

LAN Configuration							
Spanning Tree (STP)	Off •						
Connection Type	Static IP •						
IP Address	192.168.168.1						
Netmask	255.255.255.0						
DNS Mode	Manual 🔻						
Primary DNS							
Secondary DNS							

Image 4-2-3: Réseau> LAN Configuration Port





DHCP: Dynamic Host Configuration Protocol peut être utilisé par les périphériques en réseau (clients) pour obtenir des adresses de réseau uniques à partir d'un serveur DHCP.

Avantage:

Garantit des adresses IP uniques sont affectés, à partir d'un point central (serveur DHCP) dans un réseau.

Inconvénient:

L'adresse d'un dispositif particulier est pas «connu» et est également sujette à changement.

Les adresses statiques doivent être suivis (pour éviter l'utilisation en double), mais ils peuvent être affectés en permanence à un dispositif.



Au sein d'un réseau IP chaque appareil doit avoir sa propre adresse IP unique.



		Type de connexion
	Cette sélection détermine si les BulletPlus va obtenir une adresse IP	Valeurs
Les paramètres réseau par défaut:	statique sera entré. Si une adresse IP statique est choisi, les champs suivants doivent également être remplis.	DHCP Statique
IP: 192.168.168.1 Subnet: 255.255.255.0 Passerelle: 192.168.168.1		Adresse IP
	Si 'statique' Type de connexion est sélectionnée, une adresse IPv4	Valeurs
	est choisi ce champ ne sera pas apparaître et il sera rempli automatiquement à partir du serveur DHCP.	192.168.168.1
1.		Netmask
UN MASQUE SUBNET est un masque de bits qui sépare les parties réseau et hôte (périphérique) d'une adresse IP.	Si 'statique' Type de connexion est sélectionné, le masque de réseau doit être saisi pour le Réseau. Si "DHCP" est choisi ce champ ne sera	Valeurs
	pas apparaître et il sera rempli automatiquement à partir du serveur DHCP.	255.255.255.0
La partie «démasqué» laisse à disposition les informations nécessaires pour identifier les différents dispositifs sur le sous-réseau.		Mode DNS
	Si le type de connexion est réglé sur DHCP, vous pouvez utiliser Auto pour le mode de DNS et un serveur DNS sera automatiquement défini	Valeurs
C 22	Si le type de connexion est définie comme statique, les serveurs DNS peuvent être spécifiés manuellement.	Auto Manuel
5 m		imaira / DNS cacandaira
(57)	DNS pr	
Au sein d'un réseau IP,	Définissez le DNS primaire et alternatif (Domain Name Server) pour une utilisation par les périphériques sur le port LAN, si nécessaire.	Valeurs
chaque appareil doit avoir sa propre adresse IP unique.		Auto

Auto Manuel


DHCP LAN

Un BulletPlus peut être configuré pour fournir le protocole de contrôle dynamique de l'hôte (DHCP) service à tous attachés (soit filaire ou sans fil (WiFi) -connexe) périphériques. Par défaut, le service DHCP est activé, de sorte que les périphériques connectés aux ports LAN Ethernet physiques, ainsi que tous les périphériques qui sont connectés par WiFi sera attribué une adresse IP par le BulletPlus. Le service DHCP LAN est disponible pour chaque interface, et est situé dans les menus add / interface d'édition.

AN DHCP		
DHCP Server	Enable •	
Start 🔍	192.168.168.100	
Limit 🔍	150	
Lease Time (in minutes) 0	720	
Alternate Gateway		
Preferred DNS server		
Alternate DNS server		
WINS/NBNS Servers		
WINS/NBT Node Type	none 🔻	

Image 4-2-4: Réseau> Serveur DHCP

		Serveur DHCP
	L'option est utilisée pour activer ou désactiver le service DHCP pour les périphériques connectés au port (s) LAN	Valeurs
, utres		Enable / Disable
ır		Démarrer
e	Sélectionnez les adresses à partir des adresses IP DHCP assignable.	Valeurs
	configuration IP du réseau local, et ne peuvent pas être changé.	192.168.168.100
		Limite
	Définir le nombre maximum d'adresses IP qui peuvent être affectées	Valeurs
		150
		Durée du bail
	La durée du bail DHCP est la quantité de temps avant une nouvelle	Valeurs
	DHCP.	720
		Autre passerelle
	Spécifiez une autre passerelle pour les périphériques DHCP attribués	Valeurs
	si la passereire par deladi est de rie pas etre duilse.	(IP Address)



Avant d'activer ce service, vérifiez qu'il n'y a pas d'autres appareils - soit filaire (par exemple LAN) ou sans fil avec un service de serveur DHCP actif. (Le serveur délivre des informations d'adresse IP à la demande d'un client DHCP, qui reçoit les informations.)



2	
DNS: Domain Name Service est un service Internet qui traduit easily- rappeler les noms de domaine en adresses IP souvenaient pas si easily	•

0

Etant donné que l'Internet est basé sur les adresses IP, sans DNS, si l'on est entré le nom de domaine www.microhardcorp.com (par exemple) dans la ligne d'adresse d'un navigateur Web, le site "n'a pu être trouvée»).

H-noeud: hybride

	Serveur DNS préféré				
Indiquez une adresse de serveur DNS préféré à attribuer aux dispositifs DHCP	Valeurs				
	(Adresse IP)				
	Autre serveur DNS				
Indiquez l'adresse du serveur DNS alternatif à attribuer aux dispositifs	Valeurs				
	(Adresse IP)				
	WINS / NBNS Servers				
Saisissez l'adresse du service WINS / NBNS (NetBIOS) Server. Le	Valeurs				
semblable à un serveur DNS traduit les noms de domaine en adresses IP.	(Pas par défaut)				
WI	NS / Type de nœud NBT				
Sélectionnez la méthode utilisée pour résoudre les noms d'ordinateur	Valeurs				
a des adresses IP. Pour le nom des methodes de resolution sont disponibles: B-noeud: diffusion P-noeud: le point-à-point M-noeud: mixte / modifié	none b-node p-node m-node				

h-node

© Microhard 2016



VLAN Configuration

Le BulletPlus a la capacité d'ajouter plusieurs interfaces réseau, comme tel, il peut être souhaitable de segmenter ces différents sous-réseaux. Les BulletPlus fonctionnalités VLAN 802.1Q. 802.1Q VLAN utilise le marquage pour permettre la séparation des segments de réseau. Les ports peuvent appartenir à plusieurs VLANs. Un orifice d'ouverture du coffre peut être configuré pour communiquer avec un autre commutateur de réseau local virtuel en ajoutant tous les réseaux locaux virtuels configurés pour un port unique. Le VLAN1 natif est utilisé par défaut, il est important que tout commutateur VLAN connecté

/LAN Configuration		
VLAN Mode	802.1Q OPort Isolation	AND CONTRACTOR OF AND ADDRESS AND ADDRESS ADDR
New VLAN		
Name		
VLAN ID		
Port 1	Exclude	d v
Port 2	Exclude	d 🔻
Network	None	T
Add new VLAN		
802.1Q VLAN Summa	Ŷ	
VLAN name	VLAN ID Port 1	Port 2 Network Config

Image 4-2-5: Réseau> VLAN

		Nom VLAN
Les noms de VLAN peuvent être ajoutés pour aider à l'identification de	Valeurs	
VLAN (but, I, e ingeniene, comptabilite, etc.).	(no default)	
		VLAN ID
Lors de l'ajout d'un VLAN, vous devez sélectionner un ID de VLAN.	Valeurs	
Selectionnez entre z et 127 pour les 1D de VLAN valides.	2 (2-127)	
		Port 1 - 2
Attribuer port au VLAN actuel.	Valeurs	
Exclus: Ne fait pas partie du VLAN actuel Tagged: En 802.1Q VLAN cela affecte le courant vers le port, Untagged: Dans le port VLAN basé sur cette attribue un port au VLAN actuel.	Excluded Tagged Untagged	
		Réseau
Permet à l'utilisateur la possibilité d'attribuer des interfaces spécifiques	Valeurs	
un reseau de configuration à un vizien specifique. (ouz. 10)	Aucun LAN (interfaces résea supplémentaires	u)



4.2.3 Réseau> WAN

Configuration WAN

doivent également être remplis.

La configuration WAN se réfère à la connexion filaire WAN sur les BulletPlus. Le port WAN peut être utilisé pour connecter le Bullet Plus pour d'autres réseaux, l'Internet et / ou d'autres ressources du réseau.

Syster	n Ne	twork	Carrie	r Wire	eless F	irewall	VPN	Router	Ser	ial I/O	GPS	Apps	Diag	Admi	1
Status	LAN	WAN	DHCP	DDNS	Routes	5 VRRP	Ports	Bandwi	dth	Device Li	ist Clo	oud Filte	r Web	ofilter	MultiWAN
WAN	ort Co	nfigurati	ion												
Conf	guratior	I													
w	orking N	/lode 🕕			Indepe	ndent WAN	•								
WAN	Configu	ration													
C	onnectio	n Type			Static IF	Pv									
IP	Addres	s													
Su	ibnet Ma	ask													
D	efault G	ateway													
D	efault Ro	oute			Yes •										
D	NS Mode	9			Manua	- v									
Pr	imary D	NS													
Se	condary	/ DNS													

Image 4-2-6: Réseau> Configuration WAN

Mode de fonctionnement

Valeurs

Utilisez cette option pour régler la fonction du port RJ45 WAN physique. Si la valeur WAN indépendante, le port WAN physique fonctionne comme un port WAN standard. En variante, il peut être configuré de façon à ponter au LAN, et fonctionner en tant que deuxième port de réseau local ou même en tant que réseau local indépendant.

Independent WAN Bridged with LAN Port Independent LAN

Type de connexion

Cette sélection détermine si les BulletPlus va obtenir une adresse IP WAN à partir d'un serveur DHCP, ou si une adresse IP statique sera entré. Si une adresse IP statique est choisi, les champs suivants

DHCP Static

Adresse IP

Si 'statique' Type de connexion est sélectionnée, une adresse IPv4 valide pour le réseau utilisé doit être entré dans le champ. Si "DHCP" est choisi ce champ ne sera pas apparaître et il sera rempli automatiquement à partir du serveur DHCP.

Valeurs

(no default)

Netmask

Si 'statique' Type de connexion est sélectionné, le masque de réseau doit être saisi pour le Réseau. Si "DHCP" est choisi ce champ ne sera pas apparaître et il sera rempli automatiquement à partir du serveur DHCP.

Valeurs

(no default)



DHCP: Dynamic Host Configuration Protocol peut être utilisé par les périphériques en réseau (clients) pour obtenir des adresses de réseau uniques à partir d'un serveur DHCP.

Avantage:

Garanti des adresses IP uniques sont affectés, à partir d'un point central (serveur DHCP) dans un réseau.

Inconvénient: L'adresse d'un dispositif particulier est pas «connu» et est également sujette à changement.

Les adresses statiques doivent être suivis (pour éviter l'utilisation en double), mais ils peuvent être affectés en permanence à un dispositif.



	Passerelle par défa
Si le BulletPlus est intégré dans un réseau qui a une passerelle définie, puis, comme avec d'autres hôtes sur le réseau, l'adresse IP de	Valeurs
cette passerelle sera entré dans ce domaine. S'il y a un serveur DHCP sur le réseau, et le type de connexion (voir page précédente) est choisie pour être DHCP, le serveur DHCP remplir ce champ avec l'adresse de la passerelle appropriée.	(Pas par défaut)
	Route par défa
Le paramètre Route par défaut vous permet de définir cette interface	Valeurs
toutes les données envoyées à l'interface WAN si le réseau de destination est pas directement connecté (LAN, WIFI, etc.), et aucun autre itinéraire a été spécifié (4G). Dans les cas où le WAN est la connexion principale ce serait réglé sur Oui.	Non / Oui
	Mode D
Sélectionnez entre manuelle ou automatique pour le serveur (s) DNS	Valeurs
détecter automatiquement les serveurs DNS à utiliser, ce qui est normalement le cas lorsque le WAN est DHCP. Manuel requis les adresses DNS soient connus et sont entrés ci-dessous.	Manuel / Auto
	DNS prima
DNS (Domain Name Service) Les serveurs sont utilisés pour résoudre	Valeurs
connexion est définie pour DHCP le serveur DHCP remplira ce champ et l'ensemble de la valeur peut être vu sur la> page d'état du réseau. Pour ajouter des serveurs statiques supplémentaires, saisissez-les ici.	(Pas par défaut)
	DNS seconda
DNS (Domain Name Service) Les serveurs sont utilisés pour résoudre les noms de domaine en adresses IP. Si la valeur auto et le type de	Valeurs
connexion est définie pour DHCP le serveur DHCP remplira ce champ et l'ensemble de la valeur peut être vu sur la> page d'état du réseau. Pour ajouter des serveurs statigues supplémentaires, saisissez-les ici.	(Pas par défaut)



4.2.4 DHCP (MAC Binding)

Dans certaines applications, il est important que les dispositifs spécifiques ont toujours une adresse IP prédéterminée. Ce menu permet de MAC lier à une adresse IP Adresse, de sorte que chaque fois que le dispositif qui a l'adresse MAC spécifiée, sera toujours obtenir l'adresse IP sélectionnée à partir du service DHCP. Dans cette situation, tous attachés (filaire ou sans fil) appareils peuvent tous être configurés pour DHCP, mais toujours obtenir une adresse IP connue.

System	Net	work	Carrier	Wire	less I	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	1	
Status	LAN	WAN	DHCP	DDNS	Routes	5 VRRP	Ports	Bandwi	dth De	evice Li	st Cl	oud Filte	r Wel	ofilter I	MultiWAN	
DHCP	DHCP Configuration															
Static	Static IP addresses (for DHCP Server)															
Na	me															
MA	C Addre	ss														
IP /	Address															
Ad	d static I	Ρ														
Static Ad	dresses															
MAG	Address			IP Ad	idress			Name				NetStatus				
Active D	Active DHCP Leases															
MAG	Address			IP A	idress			Name				Expires in				
The	re are no k	nown DHC	P leases.													
R	elease /	All Re	fresh													

Image 4-2-7: Réseau> Adresse MAC Binding

	Nom		
Le champ de nom est utilisé pour donner au dispositif un nom	Valeurs		
	(Pas par défaut)		
	Adresse Mac		
Entrez dans l'adresse MAC de l'appareil à être lié à une adresse IP	Valeurs		
format: AB: CD: DF: 12: 34: D3. Il est pas sensible à la casse, mais les colons doivent être présents.	(Pas par défaut)		
	Adresse IP		
Entrez l'adresse IP à attribuer à l'appareil spécifié par l'adresse MAC	Valeurs		
0-403343.	(Pas par défaut)		
Adrossos statiquos			

Cette section affiche l'adresse IP et l'adresse MAC actuellement affectée par le service DCHP, qui sont liés par son adresse MAC. Aussi indiqué est le nom, et la capacité de supprimer la liaison en cliquant sur "Supprimer _____".

Contrats de location DHCP actifs

Cette section affiche les adresses IP actuellement affectées par le service DCHP. Aussi montré est le MAC Adresse, Nom et heure d'expiration du bail pour référence. Le bouton "Release All 'termine tous actifs loués et exige que tous les périphériques connectés à demander de nouvelles informations de réseau (IP / sous-réseau / etc)



4.2.5 Réseau> DDNS

Sauf si un transporteur émet une adresse IP statique, il peut être souhaitable d'utiliser un service DNS dynamique (DDNS) pour suivre les changements IP dynamiques et mettre à jour automatiquement les services DNS. Ceci permet l'utilisation d'un nom d'hôte résolvable constante pour les BulletPlus.

System	Net	work	Carrier	Wire	eless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admi	n
Status	LAN	WAN	DHCP	DDNS	Route	es VRRP	Ports	Bandwi	dth De	vice Li	st Clo	ud Filte	r Wel	ofilter	MultiWAN
DDNS Configuration															
Config	uration														
DD	NS stati	JS			Enab	le 🔻									
Net	work				Auto	•									
Per	iodic Up	odate			Disat	ole 🔹									
Ser	vice				chan	geip	•								
Use	r Name														
Pas	sword							Show Passw	/ord 📃						
Host							NSlookup]							

Image 4-2-8: Réseau > DDNS

		DDNS Status
Cette sélection permet l'utilisation d'un Dynamic Domain Name Server	Valeurs	
	Activer / Désa	activer
		Réseau
Si le Bullet Plus est utilise un WAN filaire (ISP), ainsi qu'un support cellulaire spécifique qui utilisera le service DNS	Valeurs	
	Auto / Carrier	/ WAN
		Service
Voici une liste des fournisseurs de services DNS dynamiques pris en	Valeurs	
les fournisseurs spécifiques pour plus d'informations.	changeip dyndns eurodyndns hn noip	ods ovh regfish tzo zoneedit
	Identifiant I	Mot de passe
Entrez un nom d'utilisateur et mot de passe pour le service DDNS	Valeurs	
selectionne d-dessus.	(aucun)	
		Hôte
Ceci est l'hôte ou le nom de domaine pour le Bullet plus attribué par le	Valeurs	
serveur (si configuré correctement)	(aucun)	



4.2.6 Réseau> Routes

Configuration des routes statiques

Il peut être souhaitable d'avoir des dispositifs sur différents sous-réseaux pour être en mesure de parler les uns aux autres. Ceci peut être accompli en spécifiant une route statique, dire la Bullet Plus où envoyer des données.

System	Net	twork	Carrier	Wire	less	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admi	n
Status	LAN	WAN	DHCP	DDNS	Route	es VRRP	Ports	Bandwi	dth D	evice Li	st Clo	oud Filte	r Wel	ofilter	MultiWAN
Static R	Static Routes Configuration														
Add St	atic Rou	ite													
Nar	me				route1										
Des	stinatio	n Subnet	0		192.1	68.168.0									
Net	tmask				255.2	55.255.0									
Gat	teway				192.1	68.168.1									
Met	tric				0										
Inte	erface				LAN		•								
Add	d Static	Route													
Static I	Route Si	ummary													
Na	me	De	estination			Netmask		Gatev	vay		Metric		Interface		

Image 4-2-9: Réseau> Routes

	Nom
Les itinéraires peuvent être des noms faciles à consulter, ou de décrire	Valeurs
	(no default)
	Destination
Entrez l'adresse IP du réseau pour la destination.	Valeurs
	(192.168.168.0)
	Passerelle
Spécifiez la passerelle utilisée pour atteindre le réseau spécifié ci-	Valeurs
uessus.	192.168.168.1
	Netmask
Entrez le masque pour le réseau de destination.	Valeurs
	255.255.255.0



Métrique

Dans certains cas, il peut y avoir de multiples voies pour atteindre une destination. La métrique peut être réglé pour donner des itinéraires certaine priorité, plus la métrique est, mieux la route. Plus houblon qu'il faut pour arriver à une destination, plus la métrique.

Interface

Définir l'interface de sortie. La destination est un dispositif sur le réseau local, LAN1 (Of port WAN physique est ponté comme indépendant LAN), 3G / 4G (cellulaire), USB ou le WAN?

Valeurs

Valeurs

255.255.255.0

LAN / LAN1 / WAN / Cell / USB None



4.2.7 Réseau > VRRP

Le BulletPlus lorsqu'il est associé à d'autres appareils compatibles VRRP (une autre BulletPlus ou appareils compatibles) peut fournir un accès Internet redondant pour les périphériques RL en utilisant VRRP (Virtual Router Redundancy Protocol) comme illustré ci-dessous. Si un périphérique connecté doit accéder à l'Internet, il utilisera selon routeur virtuel a la plus haute priorité, si ce dispositif ne sont pas disponibles le prochain routeur avec la plus haute priorité routeur le trafic.



In order to edit existing VRRP configurations, First change VRRP Status to Disable and then click Submit. After VRRP web-GUI refreshed, change VRRP Status to Enable, enter new settings and then click

Submit.

lmage 4-2-10: Réseau > VRRP

VRRP Status

Activer ou désactiver le service VRRP sur le BulletPlus. Pour modifier les paramètres du service VRRP doit être désactivé (puis soumis), puis réactivé.

Valeurs

Activer / Désactiver



	Virtuel Routeur IP
Ceci est l'adresse IP du routeur virtuel, cela doit être le même sur tous	Valeurs
ocal PC / périphérique connecté utiliserait comme sa passerelle par défaut.	192.168.220.211
	Virtuel Routeur ID
Ceci est l'ID de routeur. Chaque routeur / participant à VRRP doit avoir un ID de routeur pour les distinguer	Valeurs
	2
	Routeur Priorité
Ceci est la priorité du routeur. Ce numéro de attribué à chaque routeur	Valeurs
primaire. Plus l'ID est élevée, plus la priorité.	150

4.2.8 Réseau > Ports

Le Réseau> menu Ports peut être utilisé pour déterminer les caractéristiques des interfaces Ethernet physiques sur le BulletPlus. Comme on le voit ci-dessous le mode (Auto / Manuel), auto-négociation, Vitesse (10 / 100Mbit / s) et le Duplex (de moitié plein /) peuvent tous être configurés sur les BulletPlus.

	mi	icro	hard	even	FMS	INC		-			-	1	01
	1111	ICT O	mare	1 31311	LIVIS	INC.	10	1010	15	22	O	0	10
stem 🛛	Network	Carrier	Wireless	Firewall	VPN	Router	Seria	l 1/0	GPS	Apps	Diag	Adm	in
tus LA	N WAN	DHCP [DNS Rout	es VRRP	Ports	Bandwi	dth D	evice Li	st Clo	oud Filter	r Web	filter	MultiW
hernet Po	ort Configu	iration											
Port	Mode		Aut	o-Negotiation		Speed					Duplex		
WAN	Auto	Manual	• C	n Off		100	Mbit/s	10Mbit/s			Full) Half	
LAN1	Auto	Manual	• C	n Off		100	Mbit/s 🕬	10Mbit/s			Full) Half	
LAN2	Auto	Manual	® (n Off		100	Mbit/s	10Mbit/s			Full) Half	
thernet	Port Status												
Port	Lii	nked 🕕		Auto-Negotia	ation			Spe	eed		Du	olex	
WAN	no	0		on				10	Mb/s		Hal	f	
LAN1	ye	s		on				10	0Mb/s		Ful		
LAN2	nc)		on				10	Mb/s		Hal	f	

Image 4-2-11: Réseau > Ports



4.2.9 Réseau > Bande passante

Les BulletPlus Bouilloire limitation de bande passante, ce qui permet l'upload / download des connectés réseaux / utilisateurs des vitesses de données à être limitée à une valeur spécifiée. Réseau limitation de bande passante peut être mis en œuvre par chaque interface Ethernet physique comme on le voit dans l'image ci-dessous.

System	Net	twork	Carrie	r Wire	eless F	irewall	VPN	Router	Seria	l I/O	GPS	Apps	Diag	Admi	n
Status	LAN	WAN	DHCP	DDNS	Routes	5 VRRP	Ports	Bandwi	ith I)evice Li	st Clo	oud Filte	r Web	ofilter	MultiWAN
Bandwi	Bandwidth Throttling														
Rule Co	onfigura	tion													
Rule	e Name				rule1										
Net	work				LAN		• (One	rule per net	work)						
Upl	oad Bar	ndwidth I	Enable		Enable	le 🔍 Disabl	e								
Upl	oad Bar	ndwidth			10000	10000 kbps									
Dov	vnload	Bandwid	th Enable		Enable	le 🔍 Disabl	e								
Dov	vnload	Bandwid	th		30000		k	dps							
Add	l Rule														
Rule Li	st Sum n	nary													
Nai	me	Network	Uplo	ad Enable		Upload Limit		Download E	able		Download	l Limit	(Configure	

Image 4-2-12: Réseau > limitation de bande passante

	Nom de la règle			
Le nom de la règle est utilisé comme référence pour être en mesure d'aider à identifier quelle interface ou le réseau est attaché à l'interface	Valeurs			
réseau affectée.	rule1			
	Réseau			
Sélectionnez l'interface physique d'être affectées par la limitation de bande passante telle que définie ci-dessous	Valeurs			
	(Variable)			
Téléchargez la	bande passante Activer			
Activer ou désactiver ajout sur l'interface spécifiée. Cette empêche les	Valeurs			
des vidéos ou d'autres fichiers sur un serveur).	Activer / Désactiver			
Télécha	arger la bande passante			
Régler la limite de données (vitesse) pour le téléchargement de	Valeurs			
bande passante Activer.	10000			



Télécharger la bande passante Activer

Activer ou désactiver le téléchargement sur l'interface spécifiée. Cette empêche les données d'être téléchargé à partir d'un serveur. (À savoir le téléchargement de fichiers, navigation Internet, etc.).

Valeurs

Enable / Disable

Té	élécha	arger la bande passante
Régler la limite de données (vitesse) pour les téléchargement	ts de	Valeurs
passante de téléchargement Activer.	ande	30000

4.2.10 Réseau> Liste des périphériques

La liste des réseaux> Device affiche la table ARP actuelle pour les cartes réseau. L'adresse MAC et l'adresse IP sont présentés, les appareils affectés mais non seulement DHCP sont répertoriés dans la liste des périphériques, des appareils, même ceux affectés statiquement, qui sont connectés via l'interface de réseau local (RJ45) sont affichés, y compris ceux qui sont liés par un concentrateur ou passer.

2	ļ	mi	icro	oha	ırd	SYST	EMS	INC.	10	1010	270	57	0	10	0101
System	Net	work	Carrie	r Wire	less	Firewall	VPN	Router	Seria	I I/O	GPS	Apps	Diag	Admi	n
Status I	LAN	WAN	DHCP	DDNS	Rout	es VRRP	Ports	Bandwi	dth D	evice Li	st Clo	ud Filte	r Web	ofilter	MultiWAN
Network Select netwo	Network Device List Select Show MACs without IP networks: Show IPs without MAC Apply Filter Show some IPv6														
Net	Network MAC Address					I	IP Address			Sta	State		Ageir	ng Timei	1
Car	Carrier 4c:54:99:45:e5:d5			1	184.151.220.1			RE	REACHABLE			3.55			
LAN	LAN 00:50:b6:0f:63:34				1	192.168.168.212				DELAY 0.43					

Image 4-2-13: Réseau> Liste des périphériques



4.2.11 Réseau> Filtre Nuage

Le BulletPlus assure un filtrage de contenu basé sur Cloud et la sécurité en utilisant le service tiers par Open DNS. OpenDNS est un service qui offre des services DNS gratuits ou premium avec sécurité, protection phishing et facultatif, filtrage de contenu avancé. Pour commencer à utiliser OpenDNS un compte doit d'abord être créé avec OpenDNS en visitant leur site web.

System Network	Carrier Win	eless Firewall	VPN Ro	outer Seria	1/0 0	GPS Apps	Diag Admin		
Status LAN WAN D	HCP DDNS	Routes VRRP	Ports Ba	andwidth D	evice List	Cloud Filter	Webfilter M	lultiWAN	
Cloud Based Filtering/	ecurity					-			
cioud based i mering/	county								
Configuration									
OnonDNS									
by									
OpenDNS Cloud Filter	r	Enable 🔹							
Status		Service needs to b	e configured						
Disable Bypassing Op	enDNS 🛈								
User Name		OpendnsUsernam	e	_					
Password		OpendnsPasswor	d Sho	w Secret 🗹					
						Stop F	Refreshing Interva	l: 20 (in seconds)	
		Image	4-2-14: Rés	seau> Nuage	Filtrage				
						Filtre	OpenDN		
						THUC	ореньн	o nuuge	
Activer ou désactiv	ver le filtrag	e OpenDNS n	uage et s	sécurité ba	sée.	Valeur	s		
						Activer /	Désactiver	,	
				Dá	oootiv			ntournor	
				De	Sacin	ver Oper		ntoumer	
Si activé tous les	clients c	onnectés à tr	avers le	BulletPlus	seront	Valour	'e		
contraints d'utilise	r OpenDN	IS et est sou	imis à to	oute filtrad	e et la	valeur	3		
sécurité des conte	nus, pour e	empêcher le co	ontournen	nent.		Activer /	Désactiver	,	
	•					,,			
								Statut	
Lorsque le filtre Clo	oud est act	ivé, ce statut s	era rafra	îchie toute:	s les 30	Valeur	s		
secondes, indiqua	nt l'état Op	enDNS. Pour (OpenDNS	S d'être act	if, l'état				
doit être vert et affi	cher "Coni	Activer /	Désactiver	,					
						ldentifi	ant Mot o	de passe	
Entroy lo nom duit	iliaataur at	mot do passa	nourle	cometo Or					
Entre∠ le nom d'ut	cui a átá spácifiá lors de l'inscription et la configuration du sonvico								
qui a ete specifie iors de l'inscription et la configuration du service.							Décestion		



4.2.12 Réseau> Web Filter

Le BulletPlus peut fournir le filtrage de contenu complet, limitant l'accès à des sites Web spécifiques et d'autres contenus. Par adresse MAC, l'BulletPlus permet au contenu d'être filtrer indépendamment de l'adresse IP attribuée. Le filtrage peut également être appliqué sur un réseau entier, ce qui limite l'accès à tout appareil connecté.

em	Network	Carrier	Wireless Fire	wall VPN Route	Serial 1/0	GPS Apps	Diag Admin				
ıs L	AN WAN	DHCP D	DNS Routes V	RRP Ports Bandy	vidth Device L	ist Cloud Filte	er Webfilter MultiV				
filter											
neral S	Setting										
Webfi	lter Status 🔍		Enable •								
Filter	HTTPS										
MAC	address Webfil	ter Default Se	tting 🛡								
	Mac Address C	0:00:00:00:00:0	0:00 Default	Action Allow • Add N	AC Webfilter Defaul	t Rule					
MAC	Address Webfil	lter Default Li	st								
Mac Address Default Action											
MAC	Webfilter Rules	;									
	Name		Mac Address 🛈	Domain/URL/IP 🛈	Action 🛈	Rule Priority 🕕	Enabled 🛈				
	mac1		00:00:00:00:00:00	.company.com	Deny 🔻	50	Enabled •				
	Add MAC W	/ebfilter Rule									
+Sho	w Summary										
Netwo	ork Webfilter D	efault Setting	0								
		,									
LA	M dependent I A	N	Allow •								
Inc	dependent LA	IN	Allow ¥								
Netwo	ork Webfilter R	ule									
	Name		Network 🕕	Domain/URL/IP 🕕	Action 🔍 Ru	e Priority 🕕	Enabled 0				
			LAN	 .company.com 	Deny 🔻 50		Enabled •				
	net1										
	net1 Add Networ	k Webfilter Ru	ule								
+Sho	net1 Add Networ	k Webfilter Ri	ule								

Image 4-2-15: Réseau> Filtrage Web



Activer / Désactiver



MAC Adresse Web Filter Réglage par défaut

Le réglage par défaut peut être utilisé pour les adresses MAC où toutes les adresses peuvent être autorisés (Autoriser) à quelques exceptions près, ou lorsque toutes les adresses sont bloc (Deny), à quelques exceptions près. Après une règle par défaut a été appliqué, des exceptions peuvent être ajoutés par l'ajout de règles WebFilter MAC.

Valeurs

00:00:00:00:00:00 Allow

MAC Règles de filtrage Web

00: 00: 00: 00: 00: 00

Company.com

Valeurs

Mac1

Nier 50

Activée

Ajouter des règles MAC WebFilter pour appliquer le filtrage. Si une règle par défaut a été ajouté ces règles peuvent être utilisés pour spécifier des exceptions. Règles WebFilter MAC peuvent également être appliquées pour limiter l'accès à un seul ou quelques sites Web en ajoutant simplement la à la liste MAC Webfilter sans utiliser une règle par défaut.

Nom: Ajouter un nom pour le MAC Web règle de filtrage.

Adresse MAC: Entrée de l'adresse MAC d'appliquer la règle à. Entrée de l'adresse MAC d'appliquer la règle à.

Domaine / URL / IP: Entrez le nom de domaine ous URL de l'Accès de Contrôle de site de verser, à savoir www.company.com. Versez le l'assureur domaine complet is bloqué, le domaine le Entrez, plus inclusif, à savoir .company.com bloquera www.company.com et images.company.com et videos.company.com. Sinon, vous can UTILISER Une adresse ous l'adresse IP gamme écrite en notation CIDR, à savoir 8.8.8.0/24.

Action: Spécifiez si la règle Permet d'accéder ou de refuser l'accès à l'adresse indiquée. Règle Priorité: La priorité de la règle est utilisée pour déterminer l'ordre des règles sont évaluées. règles de priorité plus élevées (plus grand nombre) sont évaluées en premier et la première pour correspondre a son action assignée prise. "

Activé: Activer ou désactiver la règle MAC Webfilter.

MAC Adresse Web Filter Réglage par défaut

Lorsqu'un réseau est défini sur Autoriser (Blacklist), il permettra d'accéder à tous les sites non bloqués dans les règles de filtrage. Sélection Deny (Whitelist) ne permettra l'accès à des sites Web avec une action Autoriser dans les règles de filtrage, tous les autres sites seront bloqués.

Valeurs

Autoriser / Refuser

Ajouter des règles WebFilter réseau pour autoriser ou refuser l'accès au contenu spécifié. Les règles de réseau fonctionnent avec les paramètres par défaut WebFilter réseau.

Nom: Ajouter un nom pour la règle MAC Webfilter. **Réseau:** Sélectionnez le réseau local pour lequel la règle est applicable.

Domaine/URL/IP: Voir la description dans les règles de filtrage MAC ci-dessus.

Action: Voir la description dans les règles de filtrage MAC ci-dessus. Règle Priorité: Voir la description dans les règles de filtrage MAC cidessus.

Activé: Activer ou désactiver la règle Webfilter réseau.

MAC Règles de filtrage Web

Valeurs

net1 LAN Company.com Nier 50 Activée



4.2.13 Réseau > MultiWAN

MultiWAN est utilisé pour gérer la connexion de données utilisée par les BulletPlus. Dans les cas où un WAN filaire (ISP) est disponible, il est généralement utilisé pour la connexion primaire des données est généralement moins cher (illimité) que d'une connexion cellulaire. Le BulletPlus peut fournir des services de basculement automatique, la commutation de la connexion (ou route par défaut) utilisé pour les données externes.

System	Netv	vork	Carrie	r Wire	eless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admi	n		
Status I		WAN	DHCP	DDNS	Route	s VRRP	Ports	Bandwi	dth De	vice Li	st Clo	ud Filte	r Wel	ofilter	Mult	iWAN	
MultiWA	N Stati	us/Cor	nfiguratio	on													
Setting (Options																
Mult		nabla	8		Ench												
Prin	mary WA				Local		t WAN .	1									
Sec	ond WA	N			WIFL	Client	•]									
Thi	rd WAN				Carri	er Network/4	G T]									
Hea	alth Mor	nitor Int	terval 🕕		20	20 [3~1000](seconds)											
Swi	itch Not	tificatio	m		Disat	le		•									
Inde	penden	t WAN	Settings														
Ту	pe				ICMP	•											
					8.8.8	8.8.8.8 Test											
Hos	st Name	U			4.2.2.	1											
امط	lvanced.				208.6	(.222.222											
Pin	a Mode				Sec	uentially 🔘	Simultan	Pously									
ICM	IP Time	out			3	dentiality of		'1~1000](se	conds)								
Atte	empts B	Before F	ailover 🕕	6	3 •		,		,								
Atte	empts B	Before R	ecovery (D													
Rec	overy Ir	mmedia	te Mode		Disat												
Wai	it Before	e Recov	ery		60		[[1~1000](se	conds)								
WIFI	Client S	Setting	s		(Servi	e is disable	d. <u>Enable</u>	Here)									
Ту	pe				ICMP	•											
					8.8.8	3		Test									
Hos	st Name	•			4.2.2.	1											
	lyancod				208.6	7.222.222											
Carri	ior Note	+ Nork / A	C Setting	e													
Tvi	ne ne		o setung.	,	ICMP	-											
.,,					888			Test									
Hos	Host Name 0			4.2.2.	1		1000										
					208.6	7.222.222											
Ad	lvanced-	+															

Image 4-2-16: Réseau> MultiWAN

MultiWAN Activer

Activer ou désactiver le service MultiWAN sur les BulletPlus. Pour utiliser MultiWAN, le WAN (par câble) doit être configuré comme indépendant dans le Réseau> WAN paramètres et / ou sans fil doit être réglé au client et lié à l'interface WIFI.

Valeurs

Activer / Désactiver



	Primaire WAN
Définir quelle connexion est la connexion réseau primaire / Internet	Valeurs
un FAI.	WAN / Carrier / WIFI Client
	Deuxième WAN
Sélectionnez le WAN connexion est la connexion secondaire. En cas	Valeurs
alternative. En général, ce sera la connexion cellulaire.	WAN / 4G / WIFI
	Troisième WAN
La connexion sur la puce Plus peut être configuré en tant que client et	Valeurs
utilise en tant que connexion de données pour acceder a internet.	WAN / 4G / WIFI / Désactiver
S	anté Moniteur Intervalle
Ceci est la fréquence à laquelle le BulletPlus envoie des paquets	Valeurs
TOMP à mole denni pour déleminer si milenace est en panne.	20
Com	mutateur de notification
Il est possible pour le BulletPlus pour envoyer une notification lorsque	Valeurs
données par une autre interface.	De / Email / SMS / Deux
Paramètres de basculement (Mêmes paramètres pour WAN, V	VIFI Client et transporteurs)
	Туре

Sélectionnez le type de détection de basculement à utiliser. Par défaut ICMP est utilisé pour la commande ping une adresse (s) spécifiée, une recherche DNS peut également être sélectionné.

Nom d'hôte

Jusqu'à trois (3) adresses accessibles peuvent être spécifiées pour	Valeurs	
moniteur Intervalle de santé.	8.8.8.8	
Un bouton de test est prévu pour assurer cette adresse accessible ont été saisies et qu'il n'y a pas d'erreurs.	208.67.222.222	

Avancée + (Seulement montré si elle est sélectionnée)



	Ping Mode						
Le mode Ping permet aux hôtes sélectionnés être épinglées	Valeurs						
affiché lorsque le mode de basculement est réglé sur ICMP.	3						
	ICMP temps libre						
Ceci est la quantité de temps le Health Monitor attendra une réponse de l'hôte ICMP (lorsque le type est configuré comme ICMP)	Valeurs						
de mote reme (iorsque le type est coningure comme reme).	3						
Les tentatives Avant Failover							
Ceci est le nombre de tentatives de la Bullet Plus va tenter d'atteindre l'hôte ICMP avant d'entrer dans le basculement et la commutation des	Valeurs						
interfaces WAN.	1, 3 , 5, 10, 15, 20						
Les tentative	es de récupération Avant						
Le BulletPlus continuera de surveiller l'interface a échoué, même	Valeurs						
réussies nécessaires avant de récupérer l'interface défaillante.	1, 2, 5 , 10, 15, 20						
Mode immédi	at de récupération / Wait						
Une fois la connexion préférée est de nouveau considéré comme disponible, il peut être spécifié à attendre une quantité de temps	Valeurs						

configurable avant de rétablir la connexion.

Désactiver / Activer



4.3 Carrier

4.3.1 Carrier > Statut

La fenêtre porteuse d'état fournit des informations aperçu complet lié à la partie cellulaire porteuse des BulletPlus. Une variété d'informations peuvent être trouvées ici, comme état d'activité, Réseau (nom du transporteur sans fil connecté), Type de données de service (WCDMA / HSPA / HSPA + / LTE, etc), la bande de fréquence, numéro de téléphone, etc.

7	mic	rohar	d syst	EMS INC.	101040	101	0101	0101
System	Network Ca	rrier Wireles	s Firewall	VPN Router	Serial I/O	GPS Apps	Diag Admin	0.10
Status S	ettings SMS	SMSConfig D	ataUsage					
Carrier St	atus							
Carrier St	tatus - LN930							
Curr	ent APN	wrstat.	ell.ca		Core Temperature	e(°C) 4	6	
Activ	ity Status	Connec	ted		IMEI	3	56406060882064	
Netw	vork	Bell			SIM PIN (Card-1)	R	EADY	
Hom	e/Roaming	Home			SIM Number (ICCI	D) 8	9302610203010832398	
Servi	ice Mode	E-UTRA	N		Phone Number	1	5874327939	
Servi	ice State	E-UTRA	N		RSSI (dBm)	-6	53II	
Cell	ID	289636	56		RSRP/Q (dBm/dB)	-8	35 / -8	
LAC		11204			SINR (dB)	1	5	
Curr	ent Technology	LTE			Connection Durat	ion 1	8 min 24 sec	
Avai	lable Technology	LTE,UM	TS,GSM		WAN IP Address	1	84.151.220.2	
Dawa	/F		TC C		DNS Server 1	7	0.28.245.227	
Bano	/Frequency(MHz) BAND_L	IE_D		DNS Server 2	1	84.151.118.254	
Received	Packet Statistics			Transmit	ted Packet Statistics	5		
Rece	ive bytes	43.083	(B		Transmit bytes	3	21.756KB	
Rece	ive packets	273			Transmit packets	3	35	
Rece	ive errors	0			Transmit errors	0		
Drop	packets	0			Drop packets	0		
						Stop	p Refreshing Interval: 20	(in seconds)
					Convri	nht @ 2014-201	5 Microbard Systems Inc	Bulletolus

Image 4-3-1: Carrier > Statut

Toutes les statistiques paramètres affichés ne sont pas applicables.

Les octets et les paquets reçus et transmis indiquent le montant respectif de données qui a été déplacé à travers la radio.

Les chiffres d'erreur reflètent ceux qui ont eu lieu sur la liaison sans fil.



4.3.2 Carrier > Paramètres

Les paramètres dans le menu de configuration porteuse doit être entrée correctement; ils sont la condition de base requise par votre fournisseur de téléphonie cellulaire pour la connectivité réseau. Le BulletPlus peut prendre en charge deux cartes SIM, comme décrit ci-dessous soit fente peut être définie comme la fente primaire et si un problème de connectivité se produit, l'appareil peut être configuré pour passer automatiquement à la carte SIM de remplacement.

microh	ard systems into
micron	ard systems inc.
stem Network Carrier W	ireless Firewall VPN Router Serial I/O GPS Apps Diag Admi
itus Settings SMS SMSConf	ig DataUsage
arrier Configuration	
General	
Carrier status 0	Enable •
IP-Passthrough	Disable •
MTU Size(500~1500/Blank) 🐠	
SIM Selection	Dual SIM Cards •
Dual Cards Management	
Primary Slot 🔍	SIM Card-1 V
SIM Card-1 (Bottom slot) Settings	
SIM Number(ICCID)	89302610203010832398
Data Roaming	Disable •
Carrier Operator	Auto 🔻
Technologies Mode	AUTO •
APN	wrstat.bell.ca
Advanced+	
Network+	

Image 4-3-2: Carrier > Paramètres

	Statut Carrier
Statut du transporteur est utilisé pour activer ou désactiver la connexion au Cellular Carrier Par défaut cette option est activée	Valeurs
connexion au Cenulai Camer. Par delaut, cette option est activee.	Activer / Désactiver
	MTU Taille
Permet à un utilisateur de spécifier la taille MTU pour les applications	Valeurs
système déterminera la meilleure valeur.	(blanc)



IP pass-through permet l'adresse IP WAN à attribuer à l'appareil connecté aux ports LAN ou WAN. Dans ce mode, la Buillet est la	Valeurs
plupart du temps transparent et transmet tout le trafic sur le périphérique connecté au port Ethernet sélectionné, sauf que la liste ci -dessous:	Désactiver Ethernet (RL) WAN
-Le port de WebUI (Port par défaut: TCP 80), ce port est retenu pour la gestion à distance de la Bullet. Ce port peut être changé à un autre port dans le cadre du système> Services Menu. -Le SNMP Port d'écoute (Port par défaut: UDP 161). -Règles de redirection de port. Le BulletPlus avant d'autres services de modem interne (Iperf etc) en utilisant X.X.X.1 pour une adresse IP interne.	
L'adresse IP virtuelle est configurable pour permettre l'accès à l'unité sur le connecteur LAN / WAN une fois IP-Passthrough a été activée.	
Les pare-feu / règles doivent être configurés pour autoriser le	
trafic, tout le trafic porteur entrant est bloqué par défaut.	
trafic, tout le trafic porteur entrant est bloqué par défaut.	Sélectio
Le BulletPlus prend en charge un ou deux cartes SIM à installer. Par	Sélectio Valeurs
Le BulletPlus prend en charge un ou deux cartes SIM à installer. Par défaut, le principal SIM est le top SIM, et l'unité tentera de se connecter en utilisant SIM1 d'abord, puis si elle ne parvient pas à se connecter, ou perd la connexion à un support valide, il tentera alors SIM2.	Sélectio Valeurs Deux cartes SIM Card-1 SIM Only Card-2 SIM Only

Par défaut, le SIM primaire est la carte SIM installée dans la fente SIM1 sur l'unité. La carte SIM installée dans la fente primaire sera le transporteur cellulaire dans lequel le BulletPlus tentera d'établir une connexion avec. Cela peut être modifié ici.

Fente Primaire

Card-1 SIM Only Card-2 SIM Only

Valeurs

Carte SIM-1 Paramètres

Itinérance des données

Valeurs

Activer / Désactiver

Cette fonction permet la désactivation ou activer l'itinérance des données. Lorsque l'itinérance de données est activée, le modem sera autorisé à utiliser des données lorsqu'il est en état d'itinérance. Il est recommandé de ne pas autoriser l'itinérance à moins que les plans de données appropriées sont en place.



Dans certains cas, un utilisateur peut vouloir verrouiller sur un certain support. Il y a quatre options au choix: Auto, SIM basée, Manuel et fixe.

- Auto permet à l'appareil de choisir le support automatiquement. l'itinérance des données est autorisée.
- SIM base ne permet l'unité de connexion au réseau indiqué par la carte SIM utilisée dans l'appareil.
- Manuel numérise pour les transporteurs disponibles et permettre à un utilisateur de choisir parmi les transporteurs disponibles. Il faut 2 à 3 minutes pour compléter un balayage.

Sélectionnez les types valides de connexions Carrier autorisées. Par

exemple, si réglé sur auto la BulletPlus se connecter à tout type de données. Si la valeur WCDMA uniquement, le BulletPlus ne permettre

la connexion aux technologies WCDMA liées, et ne pas laisser

L'APN est requise par chaque transporteur afin de se connecter à leurs

réseaux. L'APN définit le type de réseau auquel la puce est connectée et le type de service. La plupart des transporteurs ont plus d'un APN, généralement

beaucoup, en fonction des types de services offerts.

l'appareil pour se connecter à moindre technologies (plus lent).

 Fixe permet à un utilisateur d'entrer le code de support (numérique) directement, puis l'appareil ne se connecter à ce transporteur.

Opérateur Carrier

Valeurs

Auto Sur la base de la carte SIM Manuel Fixé

Mode Technologies

Valeurs

AUTO WCDMA, LTE, GSM GSM seulement WCDMA seulement LTE seulement WCDMA, GSM LTE,WCDMA WCDMA, LTE LTE, GSM

Nom APN Access Point

Valeurs

auto

Auto APN (par défaut) peut permettre à l'unité de se connecter rapidement à un transporteur, en parcourant une liste prédéterminée de APNs communs. Auto APN ne fonctionnera pas pour APNs privées ou pour tous les transporteurs.

Avancée+

	SIM Pin
e Pin SIM est nécessaire pour certains transporteurs internationaux.	Valeurs
Si elle est fournie et requise par l'operateur cellulaire, entrez le code PIN SIM ici.	(none)
	Authentification
Définit le type d'authentification requis pour négocier avec les pairs.	Valeurs
CHAP - Challenge Handshake Authentication Protocol. Seulement requis si le transporteur a besoin d'un nom d'utilisateur et mot de passe.	AUTO PAP CHAP No Auth



	Nom d'utilisat
Un nom d'utilisateur peut être nécessaire pour l'authentification à un	Valeurs
adresses IP attribuées dynamiquement à partir du support sans fil. Varie par le transporteur.	Transporteur / pairs dépendan
	Mot de pa
Entrez le mot de passe pour le nom d'utilisateur ci-dessus. Ne peut	Valeurs
	Transporteur / pairs dépendan
Réseau+	
	Adress
Dans certains cas, l'adresse IP statique doit être entré dans ce domaine si elle est affectée par un opérateur sans fil. Dans la plupart	Valeurs
des cas, l'IP sera lu à partir de la carte SIM et de ce champ doit être laissé à la valeur par défaut.	(blanc)
Adresse IP Ut	tilisation à distance [
Si elle est activée Bullet avec l'utilisation du serveur DNS comme	Valeurs
specifie automatiquement par le fournisseur de services.	Activer / Désactiver
	Route par dé
Utilisez cette interface comme route par défaut pour tout le trafic	Valeurs
Sontant, Saur mulcation dans le Reseau de lablez Roules.	Oui / Non
	DNS-Passthro
Lorsqu'elle est activée DNS-Passthrough transmettra les informations	Valeurs
	Activer / Désactiver

Carte SIM-2 Paramètres

Paramètres de carte-2 SIM sont identiques à celle de la carte SIM-1, reportez-vous à la section précédente pour obtenir des informations sur la façon de configurer la carte-2 SIM.



4.3.3 Carrier > SMS

SMS Historique des commandes

Le menu SMS permet à un utilisateur d'afficher le SMS Historique des commandes et afficher les messages SMS sur la carte SIM.

Syste	m Netwo	rk Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Statu	s Settings	SMS SMS	Config Dat	aUsage									
SMS	Command H	istory											
Fro	n	Send Time		Content	:	Resu	t						
+14	+14036129217 15/11/09,17:43:55-20 MSC#REBOOT Run:reboot @Mon Nov 9 15:44:07 2015												
SM	SMS Untreated In SIM Card												
No.	From	Time		Cor	ntent								
1	+140361292	17 15/09/23,	15:07:04-16	Thi	s is also	a test. <u>Delet</u>	te						
2	+140361292	17 15/09/23,	15:13:08-16	08-16 Phone reply test 1. Delete									
3	3 +14036129217 15/09/23,15:15:33-16 Phone to laptop test 2. Delete												
4	4 +14036129217 15/09/23,15:24:28-16 Phone to laptop test 3. Delete												
5	+140361292	17 15/09/23,	15:25:48-16	:48-16 Phone to laptop 4 <u>Delete</u>									
6	6 +14036129217 15/09/23,15:35:01-16 At+mwlieo=1 OK Delete												
				De	lete All Al	bove SMS							

Image 4-3-3: SMS > SMS Historique des commandes

4.3.4 Carrier > SMS Config

Les messages SMS peuvent être utilisés pour redémarrer à distance ou d'événements dans les BulletPlus trigger. alertes SMS peuvent être mis en place pour obtenir des messages SMS en fonction des événements du système tels que l'itinérance statut, RSSI, Ethernet Link Status ou IO Status.

Commande SMS System

System Network Carrier Wir	eless Firewall \	VPN Router	Serial	I/0	GPS	Apps	Diag	Admin	
Status Settings SMS SMSConfig	DataUsage								
SMS Configuration									
System SMS Command:									
Status	Enable SMS Comma	and 🔻							
Set Phone Filter	Enable Phone Filter	•							
Valid Phone Numbers:									
Phone No.1									
Phone No.2									
Phone No.3									
Phone No.4									
Phone No.5									
Phone No.6									
System SMS Alert:									
Status	Disable SMS Alert	T							

Image 4-3-4: SMS > SMS Configuration



Statut

Cette option permet à un utilisateur d'activer ou de désactiver l'utilisation du SMS suivant les commandes pour redémarrer ou déclencher des événements dans le Bullet Plus:

Valeurs

Activer / Désactiver

MSC#REBOOT redémarrer le système MSC#NMS Envoyer NMS UDP Rapport MSC#WEB Envoyer web client enquête MSC#MIOP1 ouvrir I/O sortie1 MSC#MIOP2 ouvrir I/O sortie2 MSC#MIOC1 ouvrir I/O sortie1 MSC#MIOC2 ouvrir I/O sortie2 MSC#EURD0événement déclencheur rapport0MSC#EURD1événement déclencheur rapport1MSC#EURD2événement déclencheur rapport2MSC#EURD3événement déclencheur rapport3MSC#GPSR0gâchette gps rapport0MSC#GPSR1gâchette gps rapport1MSC#GPSR2gâchette gps rapport2MSC#GPSR3gâchette gps rapport3

Définir le filtre de téléphone

Si elle est activée, le Bullet Plus sera seulement accepter et commandes en provenance des numéros de téléphone dans la liste des filtres de téléphone exécuter. Jusqu'à 6 numéros peuvent être ajoutés.

Activer / Désactiver

Valeurs



Alertes SMS Système

ystem SMS Alert:		
Status	Enable SMS Alert 🔻	
Received Phone Numbers:		
Phone No.1	0	
Phone No.2	0	
Phone No.3	0	
Phone No.4	0	
Phone No.5	0	
Phone No.6	0	
Alert Condition Settings:		
Time Interval(s)	300	[5~65535]
Device Alias	UserDevice	[Max 30 characters]
RSSI Check	Enable RSSI Check	
Low Threshold(dBm):	-99	Default: -99
Carrier Network	Enable Roaming Chec	k 🔻
Home/Roaming Status:	Changed	•
LAN Ethernet Port	Enable Ethernet Check	•
Link Status:	Changed	•
IO Status	Disable IO Check	•
	View Alert SMS Record	

Image 4-3-6: SMS > SMS Alertes

	Statut		
Activer alertes SMS. IF alertes SMS activés seront envoyés lorsque	Valeurs		
téléphone indiqués.	Activer / Désactiver		
Nun	néros de téléphone reçus		
Alertes SMS peuvent être envoyés à jusqu'à 6 numéros de téléphone différents qui sont énumérés ici	Valeurs		
	(Pas par défaut)		
	Intervalles de temps		
Alertes SMS, lorsqu'il est actif, seront envoyés à la fréquence définie	Valeurs		
	300		
	Dispositif Alias		
l'alias de l'appareil est un texte qui est envoyé avec le message SMS	Valeurs		
source de l'alerte SMS.	UserDevice		



	Vérifier RSS		
Activer ou désactiver les alertes RSS.	Valeurs		
	Désactiver vérification RSSI contrôle Enabled RSSI		
	Low Threshold (dBm		
Réglez le seuil de RSSI alertes. Lorsque la puissance du signal tombe	Valeurs		
au-dessous de ce seuil, une alerte sera envoye au numero (s) spécifié.	-99		
	Réseau de l'opérateu		
Activer ou désactiver les alertes SMS pour l'état d'itinérance.	Valeurs		
	Désactiver l'itinérance Vérifier Activer l'itinérance Vérifier		
	Accueil / État Itinéranc		
The BulletPlus ne peut pas envoyer des alertes en fonction de l'état	Valeurs		
et il est important de savoir quand un dispositif a commencé l'itinérance.	En Roaming Modification ou En itinérance Changé en itinérance		
	Etherne		
Activer ou désactiver les alertes SMS pour l'état de la liaison Ethernet	Valeurs		
	contrôle Ethernet Désactiver Activer contrôle Ethernet		
	Ethernet Link Statu		
L'état de la liaison Ethernet du LAN (RJ45) peut être utilisé pour	Valeurs		
problème avec le périphérique connecté.	Modifié En aucun-link Modification ou sans lien Changé en no-link		
	I/O Statu		
Alertes SMS peuvent être envoyés sur la base des changements	Valeurs		
	Désactiver IO Vérifier Activer: ENTREE Changed Activer: Sortie Changed Activer: entrée ou de sortie changé.		



4.3.5 Carrier > L'utilisation de données

L'outil d'utilisation de données sur les BulletPlus permet aux utilisateurs de surveiller la quantité de données cellulaires consommées. Puisque les appareils cellulaires sont généralement facturés en fonction de la quantité de données utilisées, les alertes peuvent être déclenchées par la mise en jour et les limites / ou mensuelles. Les notifications peuvent être envoyées par SMS ou e-mail, permettant une alerte précoce en cas de limites configurables sont sur le point d'être dépassé. Les données d'utilisation rapportés par l'utilisation des données du moniteur peuvent ne pas correspondre aux données communiquées par le transporteur, mais il donne aux utilisateurs une idée de la bande passante consommée par les BulletPlus.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Status	Settings SI	MS SMSC	Config Data	aUsage								
Data Us	age Monitor											
	-											
Data Us	age Statistic											
Toda	ay's Usage:		2.08	MB								
Yest	erday's Usage:		0 Byt	es								
Curr	ent Monthly Us	age:	3.68	MB								
Last	Monthly Usage	e:	154.0	08 MB								
Tota	l Odometer:		1.61	GB More								
Atte	ntion:Data usa	ge statistic i	s not exact sar	me to your ca	rrier's ca	culation on	your mont	hly bill				
with	different syste	ms.										
Data Us	age Monitor											
Stat	us		Enal	ole Data Usag	e Monito)r 🔻						
Las	t Config Time		Thu J	un 20 12:02:	47 MDT	2013						
Las	t Reset Time		2016	-05-09 10:49	:51 <u>Rese</u>	t Now						
Mon	thly Over Limi	t	Sen	d Notice SMS		·						
Мо	nthly Data Unit	s	M By	/tes 🔻								
Dat	ta Limit		500			[1~65535]						
Per	iod Start Day		1			[1~31](day o	of month)					
Ade	ditional Notice	0				[10~500](%)						
Ade	ditional Notice	2 🕕				[10~500](%)						
Pho	one Number 0		+140	3								
Dail	y Over Limit		Sen	d Notice Emai	l •	•						
Dai	ly Data Units		M By	/tes 🔻								
Dat	ta Limit		50			[1~65535]						
Ma	il Subject		Daily	Data Usage I	Notice							
Ma	il Server(IP/Nar	ne)	smtp	gmail.com:46	5	(xxx:port)						
Use	er Name		@gm	ail.com								
Pas	sword		•••									
Aut	thentication 🕕		Non	e	•							
Ma	il Recipient		host	0		(xx@xx.xx)						

Image 4-3-7: Carrier > L'utilisation de données

<u>Statut</u>

Si elle est activée Bullet Plus va suivre la quantité de données cellulaires consommées. Si elle est désactivée, les données ne sont pas enregistrées, même dans l'affichage de l'utilisation des données actuelles.

Valeurs

Désactiver Activer



Mensuel/Daily Limiter

Sélectionnez la méthode de notification utilisée pour envoyer des alertes lorsque les seuils quotidiens ou mensuels sont dépassés. Si aucun est sélectionné, les notifications ne seront pas envoyés, mais l'utilisation de données seront enregistrées à des fins de référence.

Aucun

Valeurs

Envoyer avis SMS Envoyer avis Email Les deux SMS & Email

Monthly Over Limit	Send Notice SMS	T
Monthly Data Units	M Bytes •	
Data Limit	500	[1~65535]
Period Start Day	1	[1~31](day of month)
Additional Notice1 0		[10~500](%)
Additional Notice2 0		[10~500](%)
Phone Number	+1403	

Image 4-3-9: Utilisation de données > SMS Config

Unité mensuelle / D	onnées quotidienne		
Sélectionner l'unité de données à utiliser pour la surveillance de l'utilisation des données	Valeurs		
	Bytes / K Bytes / M Bytes G Bytes		
	Limite des donnée		
Sélectionner la limite de données du jour ou par mois, utilisé en liaison avec l'unité de données est le champ précédent. Si vous souhaitez définir	Valeurs		
la limite à 250 Mo, sélectionnez M Octets pour l'unité de données, et 250 pour la limite de données.	500		
	Période Jour Débi		
Pour le suivi mensuel, sélectionnez le jour où les cycles de facturation / de données commence. Ce jour chaque mois, le BulletPlus va réinitialiser les	Valeurs		
numéros de moniteur d'utilisation des données.	1 (Day of Month)		
Avis	supplémentaires 1		
Jusqu'à deux (2) autres avis peuvent être envoyés sur la base d'un	Valeurs		
	(blanc)		
1	Numéro de téléphor		
Si SMS est sélectionné comme méthode de notification, entrez le numéro	Valeurs		
de données dépasse les limites configurées			



Daily Over Limit	Send Notice Email
Daily Data Units	M Bytes •
Data Limit	50 [1~65535]
Mail Subject	Daily Data Usage Notice
Mail Server(IP/Name)	smtp.gmail.com:465 (xxx:port)
User Name	@gmail.com
Password	***
Authentication 💿	None •
Mail Recipient	host@ (xx@xx.xx)

Image 4-3-10: Utilisation des données> Email Config

	Mail Sujet
Si Email est sélectionné comme méthode de notification, entrez la ligne d'objet du courriel désiré pour l'e-mail de notification envoyé lorsque tous	Valeurs
les jours et / ou des limites mensuelles d'utilisation sont dépassées.	Daily/Monthly Utilisation des données
N	/lail Server (IP / Nom)
Si Email est sélectionné comme méthode de notification, entrez les détails du serveur SMTP pour le compte utilisé pour envoyer les notifications par e	Valeurs
-mail. Domaine ou adresse IP avec le port associé comme indiqué.	smtp.gmail.com:465
	Nom d'utilisateur
Si Email est sélectionné comme méthode de notification, entrez le nom d'utilisateur du compte de messagerie utilisé pour envoyer des e-mails.	Valeurs
	@gmail.com
	Mot de passe
Si Email est sélectionné comme méthode de notification, entrez le mot de passe du compte de messagerie utilisé pour envoyer des e-mails la	Valeurs
plupart des serveurs de messagerie nécessitent une authentification sur les e-mails sortants.	***
	Authentification
Si Email est sélectionné comme méthode de notification, entrez le mot de passe du compte de messagerie utilisé pour envoyer des e-mails. La	Authentification Valeurs
Si Email est sélectionné comme méthode de notification, entrez le mot de passe du compte de messagerie utilisé pour envoyer des e-mails. La plupart des serveurs de messagerie nécessitent une authentification sur les e-mails sortants.	Authentification Valeurs Aucun SSL/TLS STARTTLS SSL/TLS + STARTTLS
Si Email est sélectionné comme méthode de notification, entrez le mot de passe du compte de messagerie utilisé pour envoyer des e-mails. La plupart des serveurs de messagerie nécessitent une authentification sur les e-mails sortants.	Authentification Valeurs Aucun SSL/TLS STARTTLS SSL/TLS + STARTTLS SSL/TLS + STARTTLS
Si Email est sélectionné comme méthode de notification, entrez le mot de passe du compte de messagerie utilisé pour envoyer des e-mails. La plupart des serveurs de messagerie nécessitent une authentification sur les e-mails sortants. De Entrez l'adresse e-mail de la liste individuelle ou de distribution pour envoyer la notification par courrier électronique.	Authentification Valeurs Aucun SSL/TLS STARTTLS SSL/TLS + STARTTLS stinataire du courrier Valeurs

host@



Histoire d'utilisation des données

Le BulletPlus fournit un podomètre qui montre l'ensemble des données utilisées par les BulletPlus. Vous pouvez également cliquer sur le lien Plus pour obtenir un résumé de l'histoire de l'utilisation des données comme on le voit ci-dessous.

System Net	work	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Status Settin	igs Sl	NS SMSC	Config Da	taUsage									
Data Usago O	domoto												
Data Usage U	uomete												
Total Odomete	r: 3.69 M	В											
Last 6 Mon	ths Rec	ords											
2015-06	1	N/A											
2015-07	1	N/A											
2015-08	1	N/A											
2015-09	1	N/A											
2015-10	1	N/A											
2015-11	2.15	MB											
Last 15 day	E Rocou	de											
2015 10 26	ys Recoi	N/A											
2013-10-20	,	IN/A											
2015-10-27		N/A											
2013-10-20	, ,	IN/A											
2015-10-25	,	N/A											
2015-10-30	,	N/A											
2015-10-31		N/A											
2015-11-01		N/A											
2015-11-02		N/A											
2015-11-03		N/A											
2015-11-04		N/A											
2015-11-05	570	.32 KB											
2015-11-06	; 10	KB											
2015-11-07	,	N/A											
2015-11-08	3	N/A											
2015-11-09	617	.50 KB											
Attention:M	leasured	by local mo	onitor and tir	ne zone for ref	erence.	Your carrier'	s data usag	ge					
accounting	on your	monthly bil	ll may differ.										

Image 4-3-11: Utilisation de données > Utilisation des données du compteur kilométrique



4.4 Wireless (WiFi)

4.4.1 Wireless > Statut

La fenêtre d'état donne un résumé de tous les paramètres de la radio ou sans fil liées et les connexions.

La section générale d'état indique l'adresse MAC sans fil de la radio actuelle, le mode de fonctionnement (Access Point, Client), le SSID utilisé, les informations de canal de fréquence et le type de sécurité utilisé.

État du trafic montre des statistiques sur les données transmises et reçues.

Le BulletPlus renseigne sur toutes les connexions sans fil dans la section Informations sur la connexion. L'adresse MAC sans fil, Noise Floor, Rapport signal sur bruit (SNR), la force du signal (RSSI), la transmission et de réception de la qualité de connexion client (CcQ), TX et RX débits de données, et une représentation graphique du niveau de signal ou de la qualité.

	mi	icroha	rd sy	ST	EMS	INC.	404	0404	01	01	01	0101 1010
Svste	m Network	Carrier Wire	ess Fire	wall	VPN	Router	Serial	1/0 G	PS ADDS	Diag Ad	min	10
Statu	s Radio1 Hot	Spot										
Wirel	less Interfaces											
Pad	in 1 Interface 1 Stat											
Kuu	io i internace i stat	us										
	General Status											
	MAC Address	Mode	SSIE)		Frequen	icy Band	Radio I	Frequency	Security mo	ode	
	00:0F:92:FE:00:8F	Access Point	Bull	etPlus_	MKT	2.4G Mo	ode	2.462	GHz	WPA2(PSK)		
	Traffic Status											
	Receive bytes	R	eceive packet	ts		Trans	smit bytes		Tra	insmit packets		
	173.101KB	1	192			1.254MB			1549			
	Connection Info											
	IP Address	MAC Address	Noise Floor (dBm)	SNR (dB)	RSSI (dBm)	TX CCQ (%)	RX CCQ (%)	TX Rate	RX Rate	Signal Level		
	192.168.168.215	D0:22:BE:B9:30:6B	-94	49	-45	92	100	72.2 MBit/s	72.2 MBit/s	i	100%	
										Stop Refr	eshing Inte	erval: 20(s)
								Copyright (2014-201	5 Microhard Sys	stems Inc.	Bulletplus

Image 4-4-1: Wireless > Statut



4.4.2 Wireless > Radio1

Radio1 Phy Configuration

bruit et plus courts potentiels de distance.

La partie supérieure de la configuration sans fil permet la configuration du module radio physique. Vous pouvez allumer la radio ou hors tension, et sélectionnez la bande passante du canal et la fréquence comme on le voit ci-dessous.

System Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Status Radio1 Hot	Spot											
Wireless Configuration												
Radio1 Phy Configuratio	on											
Radio		On	○ Off									
Mode		802.	11NG 🔹									
High Throughput	t Mode	HT2	v 0									
Advanced Capabi	ilities	🔲 Sh	DW									
Channel-Frequency		11 -	2.462 GHz 🔻	7								
Tx Power		20 d	bm 🔻									
Wireless Distance		100			(m)							
RTS Thr (256~2346)	I OF	F									
Fragment Thr (256~	-2346)	🗹 OF	F									
CCA Power Thr (4~1	127)	28										
Add Virtual Interfac	e											

Image 4-4-2: Wireless > Radio Configuration

Radio Cette option est utilisée pour activer le module radio ou désactiver. Si Valeurs désactivé les connexions sans fil ne peuvent pas être faites. La valeur par défaut est activé. Allumé / éteint Mode Le mode définit les standard sans fil à utiliser pour le réseau sans fil. Valeurs Le BulletPlus soutient 802.11 / b / g / n modes comme on le voit ici. Sélectionnez le mode d'exploitation approprié dans la liste. 802.11B SEULEMENT 802.11BG Les options ci-dessous dépendent et varient du mode de 802.11NG fonctionnement choisi ici. Bande passante du canal Apparaît seulement lors de l'utilisation des modes 802.11b ou b / g. Valeurs largeurs de bande inférieures de canal peuvent fournir une plus grande portée et être moins sensibles au bruit, mais au compromis 20MHz Taux normal des débits de données. bande passante du canal supérieur peut fournir des taux plus élevés de données, mais sera plus sensible au



	Mode Haute Throughput
Sélectionnez HT20 pour un canal de 20MHz, ou HT40 pour un MHz	Valeurs
adjacents et + et désigné pour utiliser le plus élevé ou plus bas des canaux adjacents.	HT20 HT40- HT40+

Fonctionnalités avancées (visible uniquement si la case est cochée)

MPDU Aggregation (Activer / Désactiver) - Permet des trames de données multiples à être envoyés dans un bloc de transmission unique, permettant de reconnaître ou de réémettre si des erreurs se produisent.

GI Short (Activer / Désactiver) - GI (intervalle de garde) est le temps d'attente du récepteur pour toute réflexion RF pour régler avant que les données d'échantillonnage. Activation d'un court GI (400ns) peut augmenter le débit, mais peut également augmenter le taux d'erreur dans certaines installations.

Capacités HT Info - TX-STBC RX-STBC1 DSSS_CCK-40 AMSDU maximum (octets) - 3839 AMPDU maximum (octets) - 65535

Le réglage Channel-Freq permet de configurer le canal pour fonctionner sur, auto peut être choisi lorsque l'appareil choisit automatiquement un canal pour fonctionner. Si un lien ne peut être établi, il va essayer un autre canal.

Channel-Freq

Valeurs

Auto Canal 01: 2.412 GHz Canal 02: 2.417 GHz Canal 03: 2.422 GHz Canal 04: 2.427 GHz Canal 05: 2.432 GHz Canal 06: 2.437 GHz Canal 07: 2.442 GHz Canal 08: 2.447 GHz Canal 09: 2.452 GHz Channel 10: 2.457 GHz Canal 11: 2.462 GHz

Puissance TX

Ce paramètre établit le niveau de puissance d'émission qui sera présenté aux connecteurs d'antenne à l'arrière des BulletPlus. Sauf si nécessaire, la puissance Tx doit être réglé pas pour le maximum, mais plutôt pour la valeur minimale nécessaire pour maintenir une marge d'évanouissement du système adéquat.

11 dBm	21 dBm
12 dBm	22 dBm
13 dBm	23 dBm
14 dBm	24 dBm
15 dBm	25 dBm
16 dBm	26 dBm
17 dBm	27 dBm
18 dBm	28 dBm
19 dBm	29 dBm
20 dBm	30 dBm

Valeurs



Se reporter à la FCC (ou autrement applicable) des règlements pour déterminer, et ne fonctionne pas au-delà, la puissance de sortie de l'émetteur admissible maximum et puissance isotrope rayonnée équivalente (PIRE).



	Distance sans fil
Le paramètre sans fil Distance permet à un utilisateur de régler la distance prévue le signal WiFi a bassin de voyager. Le volour par	Valeurs
défaut est de 100 m, de sorte que le BulletPlus supposera que le signal peut avoir besoin de se déplacer jusqu'à 100m il fixe donc diverses temporisations internes pour tenir compte de ce temps de Voyage. Des distances plus longues, il faudra un réglage plus élevé, et les distances plus courtes peuvent mieux performer si le réglage est réduit.	100
	RTS Thr (256 ~ 2346)
Une fois la taille du paquet défini RTS de seuil est atteint, le système	Valeurs
d'améliorer la bande passante, tandis qu'un plus petit seuil RTS aidera le système à récupérer des interférences ou des collisions causées par des obstructions.	Allumé / éteint
Fra	agment Thr (256 ~ 2346)
Le seuil de fragmentation permet au système de modifier la taille maximale des paquets RE L'augmentation de la taille des paquets RE	Valeurs
réduit la nécessité de briser les paquets en fragments plus petits. Augmenter légèrement le seuil de fragmentation peut améliorer les performances si un taux d'erreur de paquet est connu.	Allumé / éteint
CCA	A Puissance Le (4 ~ 127)
L'évaluation Clear Channel utilise détection de porteuse et détection de l'énergie afin de déterminer si un canal / médium est disponible	Valeurs
pour la transmission. Changer le seuil aura un impact sur la façon dont le BulletPlus Wifi détermine la disponibilité des canaux.	28


Radio 1 Interface Virtuelle

La partie inférieure de la configuration sans fil fournit pour la configuration du mode de fonctionnement de l'interface sans fil, la puissance TX, informations réseau sans fil, sans fil Encryption. Le BulletPlus peut supporter plusieurs interfaces virtuelles. Ces interfaces fournissent différents SSID pour les différents utilisateurs, et peuvent également être affectés à des sous-réseaux distincts (Interfaces Réseau) pour empêcher les groupes d'interagir.

Network	LAN 🔻
Mode	Access Point 🔻
TX bitrate	Auto 🔻
ESSID Broadcast	On Off
AP Isolation	○ On ● Off
WMM	On Off <u>WMM Configuration</u>
SSID	BulletPlus_MKT
Encryption Type	WPA2 (PSK)
WPA PSK	
Show password	

Image 4-4-3: Wireless > Radio Configuration

	Réseau
Choisissez entre RL ou WAN pour l'interface virtuelle. Si les interfaces	Valeurs
le nom de l'interface apparaîtra également ici.	RL WAN Etc (Interfaces supplémentaires)
	Mode
Point d'accès - Un point d'accès peut fournir une connexion de	Valeurs
répéteurs, ou d'autres dispositifs sans fil pris en charge, tels que les ordinateurs portables, etc.	Point d'accès Client
Si plus de 1 Interface virtuelle (plus de 1 SSID) a été défini, le BulletPlus ne peut fonctionner comme un point d'accès, et sera verrouillé dans ce mode.	Repetiteur
Gare / Client - Une station peut maintenir une connexion sans fil, à savoi	r à un point d'accès.

Repeater - Un répéteur peut être connecté à un point d'accès pour étendre la portée et de fournir une connexion de données sans fil à de nombreux clients, tels que les stations.



TX bitrate

Ce paramètre détermine la vitesse à laquelle les données doivent être transférées sans fil. La valeur par défaut est «Auto» et, dans cette configuration, l'appareil transfère les données à la vitesse la plus élevée possible en tenant compte de la force de recevoir de signal (RSSI). Définition d'une valeur spécifique du taux de transmission a l'avantage de «prévisibilité» de ce taux, mais si le RSSI descend en dessous du niveau minimum requis pour soutenir ce rythme, les communications échouera.

	802.11 b/g	802.11n (HT20/HT40)
	Auto 1 Mbps (802.11b,g) 2 Mbps (802.11b,g) 5.5 Mbps (802.11b,g) 11 Mbps (802.11b,g) 6 Mbps (802.11g) 9 Mbps (802.11g) 12 Mbps (802.11g) 18 Mbps (802.11g) 24 Mbps (802.11g) 36 Mbps (802.11g) 48 Mbps (802.11g) 54 Mbps (802.11g)	Auto mcs-0 (7.2/15) Mbps mcs-1 (14.4/30.0) Mbps mcs-2 (21.7/45.0) Mbps mcs-3 (28.9/60.0) Mbps mcs-4 (43.3/90.0) Mbps mcs-5 (57.8/120.0) Mbps mcs-6 (65.0/135.0) Mbps mcs-7 (72.2/150.0) Mbps
		ESSID Broadcast
La désactivatio	n de la diffusion SSID permet de sécuriser le résea	au Valeurs
d'autres de «vo	ion de la diffusion du SSID (nom du reseau) perme ir» le réseau sans fil et peut-être tenter de 'rejoind	re' elle. On / Off
		AP Isolation
Lorsque Isolem	ent AP est activé dispositifs sans fil connectés à c	e SSID Valeurs
Lorsque Isolem ne sera pas el d'autres termes nombreux clier clients en ne pe	ent AP est activé dispositifs sans fil connectés à c n mesure de communiquer les uns avec les autr s, si l'BulletPlus est utilisé comme un point chaud p nts sans fil, AP Isolation assurerait la sécurité p ermettant pas l'accès à un autre appareil sans fil.	ve SSID res. En pour de nour les Valeurs On / Off
Lorsque Isolem ne sera pas el d'autres termes nombreux clier clients en ne pe	ent AP est activé dispositifs sans fil connectés à c n mesure de communiquer les uns avec les aut s, si l'BulletPlus est utilisé comme un point chaud p nts sans fil, AP Isolation assurerait la sécurité p ermettant pas l'accès à un autre appareil sans fil.	ve SSID res. En pour de our les On / Off WMM
Lorsque Isolerr ne sera pas e d'autres termes nombreux clier clients en ne pe	ient AP est activé dispositifs sans fil connectés à c n mesure de communiquer les uns avec les aut s, si l'BulletPlus est utilisé comme un point chaud p nts sans fil, AP Isolation assurerait la sécurité p ermettant pas l'accès à un autre appareil sans fil.	ve SSID res. En pour de our les On / Off WMM alité de Valeurs
Lorsque Isolerr ne sera pas en d'autres termes nombreux clier clients en ne po WiFi Multimed service sur un en fonction du	ent AP est activé dispositifs sans fil connectés à c n mesure de communiquer les uns avec les aut s, si l'BulletPlus est utilisé comme un point chaud p nts sans fil, AP Isolation assurerait la sécurité p ermettant pas l'accès à un autre appareil sans fil. ia (WMM) est une fonction qui améliore la qua réseau en donnant la priorité des paquets de de type de données. (Vidéo, voix, Best Effort, Fond)	ve SSID res. En pour de our les On / Off WMM alité de onnées . On / Off On / Off
Lorsque Isolerr ne sera pas el d'autres termes nombreux clier clients en ne pe WiFi Multimed service sur un en fonction du	ia (WMM) est une fonction qui améliore la qua réseau en donnant la priorité des paquets de données. (Vidéo, voix, Best Effort, Fond)	ve SSID res. En pour de our les On / Off WMM alité de onnées . On / Off On / Off
Lorsque Isolerr ne sera pas et d'autres termes nombreux clier clients en ne pe WiFi Multimed service sur un en fonction du WMM Configuration Control Status	tent AP est activé dispositifs sans fil connectés à c n mesure de communiquer les uns avec les aut s, si l'BulletPlus est utilisé comme un point chaud p nts sans fil, AP Isolation assurerait la sécurité p ermettant pas l'accès à un autre appareil sans fil. ia (WMM) est une fonction qui améliore la qua réseau en donnant la priorité des paquets de de type de données. (Vidéo, voix, Best Effort, Fond).	ve SSID res. En pour de our les On / Off WMM alité de onnées . On / Off On / Off

3

2

Video

Voice

default: 3 4

default: 2 3

default: 4

default: 3

2

2

default: 2 94

default: 2 47

default: 94 0

default: 47 0

default: 0

default: 0

101010101 microhard **BulletPlus** 1010101

4.0 Configuration

		SSID
-	Tous les dispositifs de connexion aux BulletPlus dans un réseau	Valeurs
SSID: Service Set Identifier. Le «nom» d'un réseau sans fil. Dans un réseau sans fil ouvert, le SSID est diffusé;	unique est non seulement un élément de sécurité pour un réseau particulier, mais permet également d'autres réseaux - avec leur propre adresse de réseau unique - à opérer dans la même zone, sans la possibilité d'échange de données indésirables entre les réseaux.	BulletPlus
dans un système fermé non. Le SSID doit être connue par un client potentiel pour qu'il		Type de chiffrement
soit en mesure d'accéder au réseau sans fil.	Les types de chiffrement définit le type de sécurité utilisé pour	Valeurs
-	connaître le mot de passe / mot de passe / clé correcte.	Désactiver
Modifiez la valeur par défaut	Les options de sécurité dépendent du type de version. Cette section décrit toutes les options disponibles. versions d'exportation peuvent ne pas avoir tous disponibles en option pour répondre aux exigences réglementaires définies les politiques gouvernementales.	WPA (PSK) WPA2 (PSK) WPA Enterprise (RADIUS) WPA2 Enterprise (RADIUS) WPA+WPA2 Enterprise(RADIUS)
quelque chose d'unique pour votre réseau. Pour ce faire,		WPA PSK
pour une mesure supplémentaire de sécurité et de différencier votre réseau à	Ceci est le mot de passe ou une clé pré-partagée qui est requise par	Valeurs
partir d'autres pouvant se trouver à proximité.	fortement recommandé d'avoir toujours un mot de passe défini, et a changé à partir de la valeur par défaut.	0123456789
		Montrer le mot de passe
	Cochez cette case pour afficher le mot de passe actuellement configuré pour WPA / WPA2 passphrase	Valeurs
		incontrôlé
		Adresse IP RADIUS
	Si vous utilisez Enterprise (RADIUS) cryptage, entrez l'adresse IP du	Valeurs
		(Pas par défaut)
		RADIUS Port
	Si vous utilisez Enterprise (RADIUS) cryptage, entrez le numéro de port du serveur d'authentification RADIUS ici.	Valeurs
		(Pas par défaut)
		RADIUS Server Key

Ceci est le mot de passe ou une clé pré-partagée qui est requise par un appareil pour se connecter à l'interface sans fil du BulletPlus. Il est fortement recommandé d'avoir toujours un mot de passe défini, et a changé à partir de la valeur par défaut.

Valeurs

0123456789



4.4.3 Wireless > HotSpot

La configuration sans fil Hotspot est utilisé pour fournir des services hotspot public et il est nécessaire d'utiliser un service d'authentification serveur ou basé sur le Web pour vérifier les utilisateurs, fournir des conditions d'utilisation ou d'autres informations.

	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
us Radio1 HotSpot											
tspot Configuration											
otspot Generic Configuration											
Hotspot Mode 🛛 🕘	Sim	ole Internal 🔹	1								
Hotspot Location Name	micro	hard									
	<cen< td=""><th>ter>Terms o</th><td>f Use<!--</td--><td>center></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td></cen<>	ter>Terms o	f Use </td <td>center></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	center>							
Terms of Use Text 0											
							1.				
	www.	paypal.com	www.pay	oalobjects	.com						
Sites Allowed	www.	notspotsyst	em.com	customer.no	otspotsys	tem.com					
							11				
otspot Network Configuration											
otspot Network Configuration											
otspot Network Configuration Hotspot Network	LAN	•									
otspot Network Configuration Hotspot Network Network IP Addr	LAN 192.1	▼ 168.182.0									
Hotspot Network Configuration Hotspot Network Network IP Addr Network Netmask	LAN 192. 255.2	▼ 168.182.0 255.255.0									
Hotspot Network Configuration Hotspot Network Network IP Addr Network Netmask DNS Domain	LAN 192. 255.2 key.c	• 168.182.0 255.255.0 hillispot.info									
Hotspot Network Configuration Hotspot Network Network IP Addr Network Netmask DNS Domain Primary DNS	LAN 192. 255.2 key.c 208.6	(((
Hotspot Network Configuration Hotspot Network Network IP Addr Network Netmask DNS Domain Primary DNS Secondary DNS	LAN 192. 255.2 key.c 208.6 208.6	 I68.182.0 255.255.0 hillispot.info 57.222.222 57.220.220 									
Hotspot Network Configuration Hotspot Network Network IP Addr Network Netmask DNS Domain Primary DNS Secondary DNS DHCP Start	LAN 192.1 255.2 208.6 208.6 3	 168.182.0 255.255.0 hillispot.info 37.222.222 37.220.220 									
Hotspot Network Configuration Hotspot Network Network IP Addr Network Netmask DNS Domain Primary DNS Secondary DNS DHCP Start DHCP End	LAN 192. 255.3 (key.c 208.6 3 250	168.182.0 255.255.0 hillispot.info 67.222.222 87.220.220									

Image 4-4-4: Wireless > Configuration Réseau Hotspot

Hotspot Mode Utilisez cette option pour activer ou désactiver le service d'authentification Valeurs hotspot. Il y a trois options différentes pour le mode Hotspot: Désactiver Simple interne - Afficher les termes d'un texte simple basé sur l'utilisation ou de interne simple la déclaration aux utilisateurs connectés. simple externe Simple externe - Afficher une page externe RADIUS / UAM RADIUS / UAM - Utiliser un service d'authentification 3ème Partie pour authentifier et / ou inviter les utilisateurs à accepter les conditions de service. **UAM URL de connexion** Si le mode Hotspot, RADIUS / UAM est choisi, spécifiez le hotspot Valeurs URL donnée par votre fournisseur de services. L'adresse de l'UAM Server, le portail d'authentification. https:// customer.hotspotsystem.com/ customer/hotspotlogin.php **UAM Secret**

Si le mode Hotspot, RADIUS / UAM est choisi, cela est un mot de passe secret entre l'URL de redirection et Hotspot donnée par le fournisseur de hotspot.

Valeurs

hotsys123

© Microhard 2016



Configuration Réseau Hotspot

	Hotspot Réseau
Ce champ est utilisé pour spécifier quel configuré réseau est lié au hotspot, réseaux sous peuvent être créés dans le menu Réseau>	Valeurs
LAN, qui sont dédiées aux dispositifs hotspot.	Varies
* Le service DHCP pour le réseau utilisé doit être désactivé que toutes les affectations d'adresses IP seront prises par le fournisseur de services de hotspot. *	
	Réseau Adresse IP
Indiquez l'adresse IP de l'application Hotspot. Tous les clients hotspot	Valeurs
recevioni une adresse il dans le meme reseau que le noispoi.	192.168.182.0
	Netmask Réseau
Spécifiez le Netmask de l'application Hotspot. Tous les clients hotspot	Valeurs
recevioni une adresse in dans le meme reseau que le noispoi.	255.255.255.0
	DNS Domain
Indiquez vos fournisseurs de services de domaine Server 1er DNS.	Valeurs
	Key.chillispot.info
	DNS primaire
Spécifiez le serveur DNS primaire pour être utilisé par les	Valeurs
	208.67.222.222
	DNS secondaire
Spécifiez le serveur DNS secondaire à utiliser par les appareils connectés au réseau Hotspot	Valeurs
	208.67.222.220
	DHCP Démarrer
Lorsque les périphériques se connectent au Bullet plus Wifi et Hotspot	Valeurs
sélectionnez la plage de départ ici.	3
	DHCP Fin
Lorsque les périphériques se connectent au Bullet plus Wifi et Hotspot	Valeurs
sélectionnez la plage de fin ici.	250



Hotspot Radius Configuration

Hotspot Radius Configuration					
Radius NAS ID	microhard_1				
Radius Server 1	radius.hotspotsystem.com				
Radius Server 2	radius2.hotspotsystem.com				
Radius Auth Port	1812				
Radius Acct Port	1813				
Radius Secret	hotsys123	Show Secret 🗹			
Radius CoA UDP Port	3799				
Radius Session Timeout	3600	Secs (0=Disabled)			
Radius Idle Timeout	900	Secs (0=Disabled)			

Image 4-4-5: Wireless > Hotspot Radius Configuration

	Radius NAS ID
Ceci est le nom de RADIUS de votre Hotspot comme donné par votre	Valeurs
ioumisseur de services notspot.	Microhard_1
	Radius Server 1
Comme attribué par le fournisseur de services de Hotspot, le nom ou	Valeurs
	radius.hotspotsystem.com
	Radius Server 2
Comme attribué par le fournisseur de services de Hotspot, le nom ou	Valeurs
Taulesse IF de l'autre serveur NADIOS.	radius2.hotspotsystem.com
	Radius Auth Port
Le numéro Radius Authentication Port. La valeur par défaut est 1812.	Radius Auth Port Valeurs
Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot.	Radius Auth Port Valeurs 1812
Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot.	Radius Auth Port Valeurs 1812 Radius Acct Port
Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot. Le numéro de compte Radius Port. La valeur par défaut est 1813.	Radius Auth Port Valeurs 1812 Radius Acct Port Valeurs
Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot. Le numéro de compte Radius Port. La valeur par défaut est 1813. Cela est fourni par votre fournisseur de services de Hotspot.	Radius Auth PortValeurs1812Radius Acct PortValeurs1813
Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot. Le numéro de compte Radius Port. La valeur par défaut est 1813. Cela est fourni par votre fournisseur de services de Hotspot.	Radius Auth PortValeurs1812Radius Acct PortValeurs1813Radius Secret
Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot. Le numéro de compte Radius Port. La valeur par défaut est 1813. Cela est fourni par votre fournisseur de services de Hotspot.	Radius Auth PortValeurs1812Radius Acct PortValeurs1813Radius SecretValeurs



	Radius CoA UDP Port							
Spécifiez le rayon CoA UDP Port ici. Ces informations sont fournies	Valeurs							
par le lournisseur de service de hotspot.	3799							
Radius expiration de la sessio								
Spécifiez le rayon Session Timeout. En quelques secondes, 0 =	Valeurs							
	3600							
	Radius Délai d'inactivité							
Spécifiez le délai d'inactivité Radius. En quelques secondes, 0 =	Valeurs							
	900							



4.5 Pare-feu

4.5.1 Pare-feu > Résumé

Le résumé du pare-feu permet à un utilisateur de voir des informations détaillées sur la façon dont le parefeu fonctionne. Le Tout, Filtre, Nat, Raw, et les options Mangle peuvent être utilisés pour afficher les différents aspects du pare-feu.

Syste	em I	Netwo	ork Carrier	Wireless	5	Firewa	all Vi	PN Ro	uter S	erial	I/0	GPS	Apps	Diag	Admin	
Sumr	nary	Gene	eral Port For	warding	M	AC-IP	List I	Rules	Firewall	Defa	ılt					
Fire	vall St	atus														
The	an si	atus		_												
	Status	and Ru	les	A	ll	•	Check									
Tar	get Filter															
Cha		T (malia	ACCEPT 0 and the	0 (
Cha	a okto	huter	ACCEPT 0 packets,	o bytes)		in			destination							
1	16785	1130K	delegate input	all		*	*	0000/0	0.0.0.0/0	· option						
			benegate_mpor						0.0.0.0,0							
Cha	in FORW	VARD (p	licy DROP 0 packets	s, 0 bytes)												
nun	n pkts	bytes	target	prot	opt	in	out	source	destination	1 option	15					
1	10076	4928K	delegate_forward	all	2	*	*	0.0.0.0/0	0.0.0.0/0							
Cha	in OUTF	UT (poli	icy ACCEPT 0 packet	s, 0 bytes)												
nun	n pkts	bytes	target	prot	opt	in	out	source	destination	n option	15					
1	16571	1645K	delegate_output	all		*	*	0.0.0.0/0	0.0.0/0							
Cha	in deleg	ate_forv	vard (1 references)													
nun	n pkts	bytes	target	prot	opt	in	out	source	destination	n option	15					
1	10076	4928K	forwarding_rule	all		*	*	0.0.0.0/0	0.0.0.0/0	/ ^k use	r chain fo	r forwardin	ig */			
2	9656	4898K	ACCEPT	all	-	*	*	0.0.0.0/0	0.0.0.0/0	ctstate	RELATED	ESTABLISH	HED			
3	420	30630	zone_lan_forward	all	-	br-lan	*	0.0.0.0/0	0.0.0.0/0							
4	0	0	zone_wan_forward	all	-	br-wan	*	0.0.0.0/0	0.0.0.0/0							
5	0	0	zone_wan2_forward	all	-	br-wan2	*	0.0.0.0/0	0.0.0.0/0							
6	0	0	reject	all	-	*	*	0.0.0.0/0	0.0.0.0/0							
Cha	in deleg	jate_inpi	ut (1 references)													
nun	n pkts	bytes	target	prot	opt	in	out	source	destination	n option	15					
1	11850	689K	ACCEPT	all	-	lo	*	0.0.0.0/0	0.0.0.0/0							
2	4935	441K	input_rule	all		*	*	0.0.0.0/0	0.0.0.0/0	/ ^k use	r chain fo	r input */				
3	3902	371K	ACCEPT	all	-	*	*	0.0.0.0/0	0.0.0.0/0	ctstate	RELATED	ESTABLISH	HED			
4	110	5668	syn_flood	tcp	-	*	*	0.0.0.0/0	0.0.0.0/0	tcp fla	gs:0x17/(0×02				
5	864	63478	zone_lan_input	all	-	br-lan	*	0.0.0.0/0	0.0.0.0/0							
6	51	1632	zone_wan_input	all	-	br-wan	*	0.0.0.0/0	0.0.0.0/0							
7	118	4918	zone_wan2_input	all	-	br-wan2		0.0.0.0/0	0.0.0.0/0							
~																
Cha	in deleg	jate_out	put (1 references)						dention							
nun	n pkts	bytes	target	prot	opt		out	source	destination	1 option	15					
2	4723	059K	ACCEPT	all	-		*	0.0.0.0/0	0.0.0.0/0	14	a shair a f	and an a star				
2	4/21	956K	output_rule	all	-		-	0.0.0.0/0	0.0.0/0	/* use	n chain fo	FOUTPUT */				
2	2/21	092K		all			heles	0.0.0.0/0	0.0.0.0/0	ctstate	RELATED	,car ABLISH	100			
*	0	0	zone_ian_output	-11			bruces	0.0.0.0/0	0.0.0.0/0							
2	922	63140	zone_wan_output	a/		*	bruces?	0.0.0.0/0	0.0.0.0/0							
•	922	05140	zone_wanz_output	an		-	pr-wan2	0.0.0.0/0	0.0.0.0/0							

Image 4-5-1: Pare-feu > Statut



4.5.2 Pare-feu > Général

Les paramètres de pare-feu général permettent aux utilisateurs d'activer ou de désactiver le pare-feu, et de décider quelles zones du modem pour protéger. Le pare-feu peut également être réinitialisé aux valeurs par défaut de cette zone de la WebUI.

Dans un dispositif cellulaire tel que cela, il est fortement recommandé de configurer le pare-feu pour protéger tous les périphériques connectés au modem, et de contrôler l'utilisation des données. Ceci est particulièrement important avec les unités mises en place avec une adresse IP publique que le modem est effectivement sur l'Internet public et est sensible à un large éventail de menaces qui peuvent gravement influer sur l'utilisation des données. Ceci peut être évité en bloquant tout le trafic cellulaire et la mise en place des règles spécifiques, soit les ports utilisés uniquement ouverts, ou même restreindre l'accès aux IP / réseaux spécifiques.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	1/0	GPS	Apps	Diag	Admin	
Summary	General	Port For	warding M	IAC-IP List	Rules	Firewa	ll Defaul	lt					
Firewall	General												
Firewall	General Configu	uration											
WAN	Remote Mana	gement 🖲	Er	able 🔍 Disabl	e								
Carri	er Remote Mar	nagement 🔍	🔍 🖲 Er	able 🔍 Disabl	e								
WAN	Request 🕕		B	ock 🔍 Allow									
Carri	er Request 0		🖲 Bl	ock 🔍 Allow									
LAN 1	to WAN Access	Control 🖲	O Bl	ock 🖲 Allow									
LAN 1	LAN to Carrier Access Control 👀 🛛 💿 Block 👁 Allow												
Anti-	Spoof 🕕		🔘 Er	able 🖲 Disabl	e								
Packe	et Normalizatio	on 🕕	Er	iable 🖲 Disabl	e								

Image 4-5-2: Pare-feu > Général

le ;	Ges	tion à distance WAN					
creer rir des / ou	Autoriser la gestion à distance des BulletPlus sur le côté WAN en utilisant le Web sur le port 80 (HTTP), et 443 (HTTPS), Si elle est désactivée, la configuration ne	Valeurs					
ur ns	peut être accessible à partir du réseau local (ou cellulaire si elle est activée).	Activer / Désactiver					
	Gestion à distan	ce des transporteurs					
	Autoriser la gestion à distance du BulletPlus du côté cellulaire de l'utilisation de Valeurs						
	désactivée, la configuration ne peut être accessible à partir du réseau local (ou WAN si activé).	Activer / Désactiver					
		Demande WAN					
lé sur m est est pas	Lorsque bloqué les BulletPlus va bloquer toutes les demandes des périphériques sur le WAN, sauf indication contraire dans les règles, les configurations de liste Liste	Valeurs					
lle peut nées à	MAC, IP les accès. L'accès aux ports 80 (HTTP) et 443 (HTTPS si activé), est toujours disponible à moins handicapés dans l'option de gestion à distance WAN.	Bloquer / Autoriser					
on		Demande Carrier					
	Lorsque bloqué toutes les demandes provenant d'appareils sur le côté cellulaire	Valeurs					
	d'accès, liste MAC, les configurations de la liste IP. L'accès aux ports 80 (HTTP) et 443 (HTTPS si activé), est toujours disponible à moins handicapés dans l'option de gestion à distance 4G.	Bloquer / Autoriser					



Pour les meilleures pratiques et de contrôler l'utilisation des données, il est essentiel que le parefeu est configuré correctement.

Il est recommandé de bloquer tout le trafic cellulaire entrant et créer des règles pour ouvrir des ports spécifiques et / ou utiliser ACL liste pour limiter les connexions entrantes.



Lorsque demande transporteur est réglé sur "Autoriser" le modem est ouvert à tous, ce n'est pas recommandée car elle peut avoir un impact de l'utilisation des données à partir de sources non désirées.



	LAN to WAN Access Cont
Autorise ou bloque le trafic du réseau local d'accéder au WAN, sau	If Valeurs
Liste IP.	Bloquer / Autoriser
LAN A	Access Control Transport
Autorise ou bloque le trafic du réseau local accéder à la connexion	Valeurs
d'accès, MAC et IP Liste.	Bloquer / Autoriser
	Anti-Sp
La protection anti-Spoof est de créer des règles de pare-feu attribu	és à Valeurs
la source de tous les paquets qui traversent cette interface provena l'extérieur. Si l'adresse appartient au réseau interne ou le pare-feu	ant de Activer / Désactiver lui-

Normalization Packet est la normalisation des paquets donc il n'y a aucune ambiguïté dans l'interprétation par la destination finale du paquet. La directive scrub également remonté des paquets fragmentés, la protection de certains systèmes d'exploitation de certaines formes d'attaque, et laisse tomber les paquets TCP qui ont des combinaisons de drapeaux invalides.

Valeurs

Activer / Désactiver



4.5.3 Pare-feu > Port Forwarding

Les BulletPlus peuvent être utilisées pour fournir un accès à distance aux périphériques connectés. Pour accéder à ces dispositifs un utilisateur doit définir comment le trafic entrant est géré par les BulletPlus. Si tout le trafic entrant est destiné à un périphérique connecté spécifique, DMZ pourrait être utilisé pour simplifier le processus, comme tout le trafic entrant peut être dirigé vers une adresse IP spécifique.

Dans le cas où il y a plusieurs périphériques, ou seulement des ports spécifiques doivent être transmis, redirection de port est utilisé pour transférer le trafic venant de la WAN (cellulaire) à des adresses IP spécifiques et des ports sur le réseau local. La redirection de port peut être utilisé en combinaison avec d'autres fonctions de pare-feu, mais le pare-feu doit être activé pour le transfert Port d'être en vigueur. Si la demande WAN est bloqué sur l'onglet Général, des règles supplémentaires et / ou des listes de propriété intellectuelle doivent être mis en place pour permettre le trafic de redirection de port pour passer à travers le pare-feu.

IP-Passthrough (Carrier> Paramètres) est une autre option pour faire passer le trafic à travers le BulletPlus, dans ce cas, tout le trafic est passé à un seul appareil connecté au port RJ45 du BulletPlus, Le dispositif doit être réglé pour DHCP, que les ayants droit de BulletPlus l'IP WAN à l'appareil, et le modem entre en mode transparent, routage tout le trafic sur le port RJ45. Cette option contourne toutes les fonctionnalités de pare-feu de la BulletPlus, ainsi que toutes les autres caractéristiques de l'BulletPlus tels que COM, VPN, GPS, etc.

deration after the Genera additional rules must be open ports or allow IP add nnections.	al firewall setting: created: dresses.	s are applied. If													
deration after the Genera additional rules must be open ports or allow IP add inections.	al firewall setting: created: dresses.	s are applied. If													
additional rules must be open ports or allow IP add mections.	created: dresses.														
open ports or allow IP add	dresses.														
nections.															
				2. Create a IP/Mac List to allow desired connections.											
		irewall DMZ Configuration													
isable 🔻															
2.168.100.100															
isable 🔻															
2.168.200.100															
rward1															
arrier 🔻															
2.168.2.1															
00															
CP 🔻															
000															
	22.168.100.100 iisable ▼ 22.168.200.100 isarrier ▼ 32.168.2.1 300 CP ▼ 300	22.168.100.100 iisable ▼ 22.168.200.100 isarrier ▼ 32.168.2.1 300 CP ▼ 300	22.168.100.100 iisable ▼ 22.168.200.100 isarrier ▼ 32.168.2.1 300 CP ▼ 300	12.168.100.100 13.168.200.100 12.168.200.100 13.168.2.1 100 CP ▼ 100											

Image 4-5-3: Pare-feu > Port Forwarding



Si DMZ est activée et un port d'exception pour le WebUI est pas spécifié, la gestion à distance ne sera pas possible. Le port par défaut pour la gestion à distance est TCP 80.



	DMZ Mode
Activer ou désactiver le mode DMZ. DMZ peut être utilisé pour transférer	Valeurs
	Désactiver / Activer
	DMZ Server IP
Entrez l'adresse IP de l'appareil sur le côté LAN du BulletPlus où tout le	Valeurs
	192.168.100.100
	Exception Port
Entrez un numéro de port d'exception qui ne seront pas transmises à l'adresse IP du serveur DMZ. Habituellement, une configuration ou d'un port de gestion à distance	Valeurs
qui est exclu de conserver le contrôle externe de la BulletPlus.	0

Pare-feu Configuration du port Forwarding

	Nom
Ceci est tout simplement un domaine où on ajoute une référence commode	Valeurs
unique et peut utiliser jusqu'à 10 caractères.	Forward
	La source
Sélectionnez la source pour le trafic, soit de la 3G / cellulaire ou à partir du	Valeurs
	Carrier / WAN
	Internal Server IP
Entrez l'adresse IP de l'interne destiné (i.p. sur le côté LAN de Bullet Plus)	Valeurs
vers.	192.168.2.1
	Port Interne
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus.	Port Interne Valeurs
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus.	Port Interne Valeurs 3000
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus.	Port Interne Valeurs 3000 Protocole
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus. Sélectionnez le type de protocole de transport utilisé. Par exemple Telnet	Port Interne Valeurs 3000 Protocole Valeurs
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus. Sélectionnez le type de protocole de transport utilisé. Par exemple Telnet utilise le protocole TCP, SNMP utilise UDP, etc.	Port Interne Valeurs 3000 Protocole Valeurs TCP / UDP / Both
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus. Sélectionnez le type de protocole de transport utilisé. Par exemple Telnet utilise le protocole TCP, SNMP utilise UDP, etc.	Port Interne Valeurs 3000 Protocole Valeurs TCP / UDP / Both
Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus. Sélectionnez le type de protocole de transport utilisé. Par exemple Telnet utilise le protocole TCP, SNMP utilise UDP, etc. Numéro de port de la demande entrante (de 4G / WAN côté).	Port Interne Valeurs 3000 Protocole Valeurs TCP / UDP / Both Port Externe Valeurs



Si le pare-feu est configuré pour bloquer le trafic entrant sur le réseau étendu et / ou interfaces Carrier, des règles supplémentaires ou des listes IP / MAC doivent être configurés pour permettre l'accès du trafic désiré.



4.5.4 Pare-feu> Liste MAC-IP

Configuration Liste MAC peut être utilisée pour contrôler les périphériques physiques LAN peuvent accéder aux ports sur le BulletPlus, en restreignant ou en permettant des connexions basées sur l'adresse MAC. configuration de la liste IP peut être utilisée pour définir qui ou ce qui peut accéder aux BulletPlus, en restreignant ou en permettant des connexions basées sur l'adresse IP / sous-réseau.

MAC-IP Liste peut être utilisé seul ou en combinaison avec LAN WAN / 4G de contrôle d'accès pour fournir un accès sécurisé aux ports physiques des BulletPlus.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Summary	y General	Port For	warding	MAC-IP List	Rules	Firewa	ll Defaul	t				
Firewall	MAC/IP List											
Firewall	MAC List Confi	guration										
Name	e											
Actio	n		Ac	cept 🔻								
Mac	Address		00:	00:00:00:00:00								
Add I	Mac List											
Firewall IP List Configuration												
Name	e	ip1										
Actio	n	Acc	ept 🔻									
Source	ce 🕕	WA	N V									
Source	ce IP / Prefix 🔇	0.0.0	.0	/								
Add I	IP List											
Firewall	MAC List Sumn	iary										
Nam	e Actio	n So	urce		1	Mac Address						
Firewall	IP List Summar	У										
Nam	e Actio	n Sro	:	Src IP				Pre	efix			

Image 4-5-5: Pare-feu > Liste MAC-IP

Pare-feu Configuration Liste MAC

	Nom de la règle
Le champ Nom de la règle est tenu de donner la règle un nom commode	Valeurs
caractères.	MAC_List
	Adresse Mac
Indiquez l'adresse MAC à ajouter à la liste. Doit être entré dans le format	Adresse Mac Valeurs



Pare-feu Configuration Liste MAC (Suite)

	Action			
L'action est utilisée pour définir comment la règle gère la demande de connexion	Valeurs			
ACCEPTER permettra une connexion, alors que REJETER (erreur) et DROP (tranquillement abandonné), refusera les connexions.	ACCEPTEZ LAISSEZ TOMBER REJETER			
Pare-feu Configuration Liste IP				
	Nom de la règle			
Le champ Nom de la règle est tenu de donner la règle un nom commode	Valeurs			
caractères.	IP_List			
	Action			
L'action est utilisée pour définir comment la règle gère la demande de	Valeurs			
(erreur) et DROP (tranquillement abandonné), refusera les connexions.	ACCEPTER / DROP / REJET			
	La source			
Entrez la zone spécifique que la Liste IP s'appliquera, Cellular, LAN, WAN	Valeurs			
ou none (les deux).	LAN/LAN1/WAN/Cell/USB NONE			
	Source IP Address			
Faites correspondre le trafic entrant de la gamme IP source spécifiée.	Valeurs			
par exemple: 192.168.1.0 à 192.168.1.255 représente toutes les adresses IP dans le réseau 192.168.1.0/24. (Mettez même IP dans les deux boîtes	192.168.0.0			

pour une seule partie IP.)



4.5.5 Pare-feu > Règles

Une fois que le pare-feu est activé, la configuration des règles peut être utilisé pour définir des règles spécifiques sur la façon dont les périphériques locaux et distants accéder à différents ports et services. Liste MAC et la liste IP sont utilisés pour l'accès général, et sont appliquées avant les règles sont traitées.

Il est fortement recommandé de bloquer le trafic autant que possible à partir du modem, en particulier lors de l'utilisation d'une adresse IP publique. La meilleure sécurité serait d'être pour autoriser le trafic uniquement à partir des adresses IP de confiance, et seuls les ports spécifiques utilisés, et de bloquer tout le reste. Pas la configuration du pare-feu et les règles de pare-feu pourraient bien entraîner des frais de données imprévisibles du support cellulaire.

System	Network	Carrier	Wireles	5 Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin		
Summary	/ General	Port For	warding	MAC-IP List	Rules	Firewa	ll Defaul	t						
Firewall	irewall Rules													
Firewall	Rules Configur	ation												
Rule I	Name	rule	1											
ACTIO	ON	Ac	cept 🔻											
Sourc	ce 🕕	No	ne 🔻											
Sourc	ce IPs 🕕	۲	P range 🦷	🛛 Subnet / prefi	х									
		0.0	0.0	To		0.0.0	.0							
Desti	nation 🕕	No	ne 🔻											
Desti	nation IPs 0	۲	P range 🦷 🤇	🛛 Subnet / prefi	х									
		0.0	0.0	То		0.0.0	.0							
Desti	nation Port 0	0												
Proto	col	TC	P V											
Add F	Rule													
Firewall	Rules Summary	/												
Name	e Action S	Src Src IP Fro	m Src	IP To /Prefix	Dest	Dest IP Fro	m D	est IP To	/P	refix D	est Port	Protocol		

Image 4-5-6: Pare-feu > Règles

	Nom de la règle
Le nom de la règle est utilisée pour identifier la règle créée. Chaque règle	Valeurs
doit avoir un nom unique et jusqu'à 10 caracteres peut être duilse.	personnages
	Action
L'action est utilisée pour définir comment la règle gère la demande de	Valeurs
ACCEPTER permettra une connexion, alors que REJETER (erreur) et DROP (tranquillement abandonné), refusera les connexions. Ceci est configuré en fonction de la façon dont la demande WAN / LAN Carrier et de contrôle d'accès WAN / Transporteur sont configurés dans les menus précédents.	ACCEPTEZ LAISSEZ TOMBER REJETER
	La source
Sélectionner la zone qui doit être la source du trafic de données. Le LAN / LAN1 fait référence aux connexions locales sur le BulletPlus.	Valeurs

LAN/LAN1/WAN/Transporteur Aucun



Reportez-vous à l'Annexe D pour un exemple de la façon de mettre en place un parefeu pour bloquer toutes les connexions, puis ajoutez l'accès aux adresses IP et des ports seulement spécifiques.

Annexe D: Exemple de parefeu



	Source IPs
Faites correspondre le trafic entrant de la gamme IP source spécifiée.	Valeurs
par exemple: 192.168.1.0 à 192.168.1.255 représente toutes les adresses IP dans le réseau 192.168.1.0/24. (Mettez même IP dans les deux boîtes pour une seule partie IP.)	192.168.0.0 à 192.168.0.0
	Destination
Sélectionnez la zone qui est la destination prévue du trafic de données.	Valeurs
local, LAN1, USB se réfère aux connexions locales sur les BulletPlus.	LAN/LAN1/cellules/WAN/ USB
	IP de destination
Faites correspondre le trafic entrant de la gamme IP de destination	Valeurs
réseau, par exemple: 192.168.1.0 à 192.168.1.255 représente toutes les adresses IP dans le réseau 192.168.1.0/24. (Mettez même IP dans les deux boîtes pour une seule partie IP.)	192.168.0.0 à 192.168.0.0
L	e port de destination.
Faites correspondre le trafic entrant dirigé vers le port de destination ou	Valeurs
(100: 200) format)	0
	Protocole
Le champ de protocole définit le type de protocole de transport contrôlé par	Valeurs
	TCP UDP Tous les deux ICMP



4.5.6 Pare-feu > Pare-feu par défaut

L'option par défaut du pare-feu permet à un utilisateur de revenir réglage retour aux valeurs par défaut du pare-feu du modem sans avoir à réinitialiser l'ensemble du modem.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Summary	General	Port Forv	warding	MAC-IP List	Rules	Firewa	ll Defau	lt				
Firewall I	Default											
Notice												
Firew	all Default is a	vailable nov	v. Please foll	ow the steps:								
1. Cli	ck the followir	ng button.										
2. Wa	it couples of s	econds.										
Eirewall	Default											
2. Wa	ck the followir it couples of s Default	econds.										



4.6 VPN

4.6.1 VPN > Résumé

Un réseau privé virtuel (VPN) peut être configuré pour permettre à un tunnel entre le BulletPlus et un réseau distant. Le BulletPlus prend en charge VPN passerelle IPsec Gateway (site à site) tunnel, ce qui signifie que vous utilisez les BulletPlus pour créer un tunnel à un réseau avec des capacités de VPN (autre BulletPlus ou VPN dispositif capable). Le BulletPlus peut également fonctionner comme un serveur L2TP, permettant aux utilisateurs de VPN dans l'unité à partir d'un PC à distance, et un client L2TP.

Sys	tem	Net	work	Carrier	Wire	less Fi	rewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin			
Sun	nmary	y Ga	ateway	y To Gate	way	L2TP Clie	nt Op	enVPN	GRE \	/PN User	s Cer	tificate	s					
Su	Summary																	
G	Gateway To Gateway																	
	No. Name Status Phase2 Enc/Auth/Grp Interface Local Group Remote Group Remote Gateway RX/TX Bytes										Tunnal	nfia						
	Add		Status	Thasez EncyA	any orp	interna	Ce Lucai	oroup	Kelliote oro	up Kellio	ie Galewa	y io	UTA Bytes	Tunner		ing.		
		,																
L	2TP Cli	ent																
	No.	Name	Status	Interface I	.ocal/Ren	note IP Addre	is	Server G	ateway	Start Time	Duratio	n RX/1	X Bytes	Tunnel T	est Co	nfig.		
	Add	J																
L	2TP Ser	ver																
	Statu	15	Inter	face	Local IP	Cli	ent IP Rang	e Start	Client IP Range End						Config.			
	disab	ole	WAN												Edit			
	disab	ole	4C												Edit			
		nnectiv	on List															
	No	Periote Address				12TP IP Address				Start Time Duration			RX Rives TX Rives					
	140.	Ken		53			633		Start Time	-	Duration		KA BLYES		A BLYES			
G	RE Tun	nels Li	ist															
	lo. Nam	ne Stat	tus Multi	icast ARP TI	'L IPsec	Local Tunnel	IP Loca	l Gateway	Local Sub	onet Remot	e Gateway	Rem	ote Subnet	RX/TX	Bytes Tu	nnel Test	Config.	
Į	Add																	
	2TD Her																	
	No. Add	i		Usernan	ne						Config.							
		,																
C	penVP	N User:	s															
	No.			Usernan	ne						Config.							
	Add																	

Image 4-6-1: VPN > Résumé



4.6.2 VPN > Gateway To passerelle (site à site)

Une passerelle à passerelle connexion est utilisée pour créer un tunnel entre deux dispositifs de VPN comme un BulletPlus et un autre appareil (un autre BulletPlus ou routeur VPN Cisco ou un autre fournisseur ...). Les paramètres de groupe locaux et distants devront être configuré ci-dessous pour refléter celles qui figurent sur l'autre appareil VPN.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summary	y Gateway	/ To Gate	way L2TP	Client Op	enVPN	I GRE V	/PN User	s Cer	tificate	as			
Cateway	To Cateway					_							
Oatemay	TO Gateway												
Add a N	ew Tunnel												
Tunr	nel Name												
Enab	ole 🕕												
Auth	entication		Pre	shared Key 🖲)								
Inter	face		4G	•									
Local Gr	roup Setup												
Loca	I Security Cate	way Type		ha ha		1							
Inter	face IP Addres	s and type	104	151 220 2		J							
Next	-hon Gateway	IP	104.	101.220.2									
Grou	in Subnet Gate	wav											
Grou	p Subnet IP/M	lask - 1			/ 25	5.255.255.0	2						
			Add	Remove									
Remote	Crown Setun												
Rem	ote Security Ga	ateway Type	IP (Only	•	J							
Gate	way IP Addres	s											
Next	-nop Gateway	IP Inclui 1			1/05								
Grou	ID SUDNET IP/M	lask - T	Add	Pamawa	/ 25	9.299.299.0							
			Aud	Remove									
IPSec Se	tup												
Aggr	ressive Mode												
Phas	e1 Strict Mode	e											
Phas	e 1 DH Group		mod	ip1024 •									
Phas	e 1 Encryption	1	3de	s *									
Phas	e 1 Authentica	ation	md8	5 •									
Phas	e 1 SA Life Tin	ne(s)	288	00									
Perfe	ect Forward Se	crecy											
Phas	e 2 SA Type		ESF	•									
Phas	e2 Strict Mode	e:											
Phas	e 2 DH Group		mod	ip1024 🔻									
Phas	e 2 Encryption	1	3de	s T									
Phas	e 2 Authentica	ation	md8	5 •									
Phas	e 2 SA Life Tin	ne(s)	360)				_					
Presi	nared Key					Show Presi	nared Key 🛛						
DPD	Delay(s)		32										
DPD	I Imeout(s) U		122										
DPD	Action		hok	•									

Image 4-6-2: VPN > Passerelle Gateway

Tunnel Nom

Entrez un nom pour le tunnel VPN. Jusqu'à 16 tunnels différents peuvent être créés, chacun nécessitant un nom unique.

Valeurs

tunnel1



Activer

Utilisé pour activer (cocher) est désactivée (non cochée) le tunnel VPN.

Enable (Checked)

Valeurs

Local Group Setup

Local Security Gateway Type Spécifiez la méthode d'identification du routeur pour établir le tunnel VPN. Valeurs La passerelle de sécurité locale est sur ce routeur; Security Gateway à distance est de l'autre routeur. Au moins l'un des routeurs doit avoir soit IP Only une adresse IP statique ou une adresse IP dynamique avec l'id de serveur **IP + Server ID** pour établir une connexion. Dynamic IP + Server ID IP uniquement: Choisissez cette option si ce routeur dispose d'une adresse IP WAN statique. L'adresse IP WAN apparaît automatiquement. Pour le type de passerelle de sécurité à distance, un champ supplémentaire apparaît. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez l'adresse IP, puis entrez l'adresse. IP ID + Serveur: Choisissez cette option si ce routeur dispose d'une adresse IP statique WAN et un identifiant de serveur. L'adresse IP WAN apparaît automatiquement. Pour le type de passerelle de sécurité à distance, un champ supplémentaire apparaît. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez l'adresse IP, puis entrez l'adresse. Dynamic IP + Serveur ID: Choisissez cette option si ce routeur dispose d'une adresse IP dynamique et un identifiant de serveur (disponible tel que @ microhard.vpn). Entrez l'identifiant du serveur à utiliser pour l'authentification. L'identifiant du serveur peut être utilisé que pour une seule connexion tunnel. Adresse IP Interface Affiche l'adresse IP de la Bullet Plus, qui est la passerelle VPN locale. Valeurs Adresse IP actuelle Server ID Cette option apparaît lorsque le type de passerelle de sécurité locale Valeurs précise que l'ID Server est requis pour la connexion. L'ID Server doit être dans le format @name, où nom peut être quelque chose. Les deux (Pas par défaut) routeurs doivent connaître les uns les autres noms pour établir une connexion. Next-hop passerelle IF Next-hop passerelle signifie que l'adresse IP de nouvelle passerelle-hop Valeurs pour la connexion du participant de la passerelle locale ou à distance au réseau public. (Pas par défaut) **Groupe Subnet IP** Définir le réseau local en spécifiant le sous-réseau local. Les routeurs Valeurs locaux et distants doivent utiliser différents sous-réseaux. (Pas par défaut)



	Groupe Subnet Mask
Spécifiez le masque de sous-réseau de l'adresse du réseau local.	Valeurs
	255.255.255.0
Groupe so	ous-réseau Passerelle
Entrez la porte d'entrée pour le réseau de groupe local.	Valeurs
	(Pas par défaut)
Configuration des groupes à distance	
Télécommande T	ype Security Gateway
Spécifiez la méthode d'identification du routeur pour établir le tunnel VPN. La passerelle de sécurité locale est sur ce routeur: Security Gateway à	Valeurs
distance est de l'autre routeur. Au moins l'un des routeurs doit avoir soit une adresse IP statique ou une adresse IP dynamique avec l'id de serveur pour établir une connexion. (Voir Configuration de groupe local pour plus de détails)	IP seulement IP + serveur ID Dynamic IP + serveur ID
Adres	se IP de la passerelle
Si le routeur VPN distant possède une adresse IP statique, entrez	Valeurs
i auresse in de la passerelle vnin a distance ici.	(Pas par défaut)
	Server ID
Cette option apparaît lorsque le type de passerelle de sécurité à distance indique que l'ID Server est requis pour la connexion. L'ID Server doit être	Valeurs
dans le format @name, où nom peut être quelque chose. Les deux routeurs doivent connaître les uns les autres noms pour établir une connexion.	(Pas par défaut)
Ν	lext-hop passerelle IP
Next-hop passerelle signifie que l'adresse IP de nouvelle passerelle-hop	Valeurs
réseau public.	(Pas par défaut)
	Subnet Adresse IP
Définir le réseau distant en spécifiant le sous-réseau local.	Valeurs
	(Pas par défaut)
	Subnet Mask
Spécifiez le masque de sous-réseau de l'adresse de réseau à distance.	Valeurs
	255.255.255.0



Configuration IPsec

	Phase 1 DH Group
Sélectionner la valeur pour correspondre aux valeurs requises par le	Valeurs
	modp1024 modp1536 modp2048
	Phase 1 Encryption
Sélectionner la valeur pour correspondre à la phase 1 type de cryptage utilisé par le routeur VPN distant.	Valeurs
	3des aes aes128 aes256
Ph	ase 1 Authentication
Sélectionner la valeur pour correspondre à la Phase d'Authentification 1	Valeurs
utilisee par le fouteur VFN distant.	md5 sha1
F	Phase 1 SA Life Time
Sélectionner la valeur pour correspondre aux valeurs requises par le	Valeurs
	28800
Perfect F	orward Secrecy (pfs)
Sélectionner la valeur pour correspondre aux valeurs requises par le routeur VPN distant	Valeurs
	Désactiver / Activer
	Phase 2 DH Groupe
Sélectionner la valeur pour correspondre aux valeurs requises par le	Valeurs
	modp1024 modp1536 modp2048
Ph	
	ase 2 Le chiffrement
Sélectionner la valeur pour correspondre à la phase 1 type de cryptage	Valeurs
Sélectionner la valeur pour correspondre à la phase 1 type de cryptage utilisé par le routeur VPN distant.	Valeurs



Aut	hentification Phase 2
Sélectionner la valeur pour correspondre à la Phase d'Authentification 1	Valeurs
	md5 sha1
	Phase 2 SA Life Time
Sélectionner la valeur pour correspondre aux valeurs requises par le	Valeurs
	3600
	Clé Pré-Partagée
Réglez le Shared Key Pré requis pour l'authentification avec le routeur	Valeurs
VEN UStant.	password
	Retards DPD
Dead Peer Detection est utilisé pour détecter s'il y a un pair mort. Réglez le	Valeurs
DE D'Elai (secondes), selon les desolits.	32
	DPD temps libre(s)
Réglez le DPD (de Dead Peer Detection) Délai (secondes), selon les	Valeurs
	122
	DPD Action
Réglez le DPDaction, détenir ou clair, selon les besoins.	Valeurs
	Hold Clear



4.6.3 VPN > L2TP Client

Le BulletPlus peut fonctionner comme un client L2TP, permettant une connexion VPN à effectuer avec un serveur L2TP.

mary Gateway To Gateway	L2TP Client OpenVPN GRE VPN Users Certificates	_
TP Client		
dd a New Tunnel		
Tunnel Name		
Enable 0	8	
IPsec	8	
Interface	4G T	
ocal Group Setup		
Local Security Gateway Type	IP Only	
Interface IP Address	184.151.220.2	
Next-hop Gateway IP		
emote Group Setup		
Remote Security Gateway Type	IP + Server ID T	
Gateway IP Address		
Server ID		
Next-hop Gateway IP		
Group Subnet IP		
Group Subnet Mask	255.255.255.0	
PP Setup		
Idle time before hanging up	0 [065535](s)	
PAP	Unencrypted Password	
CHAP	Challenge Handshake Authentication Protocol	
User Name	•	
Redial	2	
Redial attempts	3	
Time between redial attempts	15 (5)	
Sec Setup		
Authentication	Preshared Key V	
Phase 1 SA Life Time(s)	28800	
Perfect Forward Secrecy		
Phase 2 SA Life Time(s)	3600	
Preshared Key	Show Preshared Key	
DPD Delay(s) 💿	32	
DPD Timeout(s) 💿	122	
DPD Action	clear *	

Image 4-6-3: VPN > Client to Gateway

	Tunnel Nom
Entrez un nom pour le tunnel VPN. Jusqu'à 16 tunnels différents peuvent	Valeurs
ette crees, chacun necessitant un nom unique.	tunnel1
	Activer
Utilisé pour activer (cocher) est désactivée (non cochée) le tunnel VPN.	Valeurs
	Activer (Vérifié)



	Adresse IP Interface
Cela permet d'afficher le courant BulletPlus WAN (cellulaire) Adresse IP.	Valeurs
	Current IP
Adresse distar	te IP de la passerelle
Entrez l'adresse IP de la passerelle à distance que vous souhaitez établir	Valeurs
ine connexion avec.	none
	ID de serveur distant
Certains serveurs exigent que vous connaissez l'ID du serveur, ainsi que	Valeurs
adresse IP. Entrez I ID du serveur du fouleur distant ici.	none
	IP Subnet à distance
Afin de communiquer avec les dispositifs de l'autre côté du tunnel, le	Valeurs
aire entrer l'adresse IP du réseau de sous-réseau à distance ici.	none
Masque de so	ous-réseau à distance
Saisissez le masque de sous-réseau à distance.	Valeurs
	none
Temps d'inactivité	é avant de raccrocher
Coisisson la tampa d'inactivité (an assandas) à attendus svent	
Saisissez le temps d'inactivité (en secondes) à attendre avant	Valeurs
d'abandonner la connexion PPP. La valeur par défaut est 0, ce qui signifie que le temps est infini. (0-65535)	Valeurs 0
d'abandonner la connexion PPP. La valeur par défaut est 0, ce qui signifie que le temps est infini. (0-65535)	Valeurs 0 Nom d'utilisateur
Entrez le nom d'utilisateur.	Valeurs 0 Nom d'utilisateur Valeurs
Entrez le nom d'utilisateur.	Valeurs 0 Nom d'utilisateur Valeurs 0
Entrez le nom d'utilisateur.	Valeurs 0 Nom d'utilisateur Valeurs 0 Clé Pré-Partagée
La valeur par défaut est 0, ce qui signifie que le temps est infini. (0-65535)	Valeurs 0 Nom d'utilisateur Valeurs 0 Clé Pré-Partagée Valeurs

IPSec Configuration - Voir les sections précédentes pour plus d'infos.



4.6.4 Réseau> OpenVPN

OpenVPN serveur

Le Bullet Plus prend en charge OpenVPN et peut être configuré comme un serveur ou un client. Cette section décrit la configuration d'un serveur OpenVPN.

nary Gateway To Gateway	L2TP Client Ope	enVPN	GRE V	PN Users	6 Cer	tificate	s	
a\/PN								
enVPN Setup								
Open∨PN Mode	Server •							
enVPN Server Setup								
Server Bridge Mode								
Port	1194	[1194]					
Tunnel Protocol	UDP •							
MSSFIX/Fragment size	1370	[1370]					
Root Certificate	ca.crt	[ca.crt]					
Public Server Certificate	server.crt	[server.crt]					
Private Server Key	server.key	[server.key]					
TLS Auth Key		[ta.key]					
Diffie hellman parameter	DH2048 •							
User/Password Authentication								
Server Virtual Subnet / Netmask	10.8.0.0	/ 255	.255.255.0					
Push DNS to Client	NO 🔻							
Client Isolation	Yes •							
Keep Alive Ping Interval(seconds)	10	[10]					
Keep Alive Ping Period(seconds)	120	[at least twi	e of Interv	al]			
Cipher	BF-CBC •							
Use LZO Compression	Disable •							
enVPN Server Network Settings								
Subnets to push								
back to Clients:								
Subnet # 1, IP / Netmask		/						
	Add Remove							
Client Subnets to add								
to the Server's routing table:								
Common Name of Client #1								
Client's Subnet JP / Netmask								

Image 4-6-4: VPN > OpenVPN Serveur

	OpenVPN Mode
Activer / Désactiver le mode OpenVPN en sélectionnant le mode d'opérer	Valeurs
demandes de connexion entrantes des clients OpenVPN.	Client / Serveur / Désactiver
	Port
Le port TCP / UDP que le serveur est à l'écoute. Par défaut est 1194	Valeurs
	1194



	Protocole de tunnel
Sélectionnez le protocole de tunnel à utiliser. Les options sont TCP et	Valeurs
ODP, la valeur par dellaut est ODP.	TCP / UDP
MSSFI	X / taille de Fragment
Le maximum résultant UDP envoyer la taille des paquets après la Open/VPN a entièrement encapsulé données. Les paquets qui dénassent	Valeurs
la valeur maximale seront fragmentés.	1370
	Root Certificate
Le fichier racine de certificat (fichier CA) que tout le serveur et les clients	Valeurs
	ca.crt
Certifi	cat de serveur public
Le certificat de serveur public qui est le fichier de certificat qui réside	Valeurs
	server.crt
	Key Private Server
La clé de serveur privé, qui ne devrait pas être divulguée.	Valeurs
	server.key
	server.key TLS Auth Key
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire	server.key TLS Auth Key Valeurs
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS.	server.key TLS Auth Key Valeurs (Pas par défaut)
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN.	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs (Pas par défaut)
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN.	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs (Pas par défaut) fie paramètre hellman
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN. Diff Sélectionnez entre 1024 et 2048 bit clés bits Diffie Hellman pour la sécurité	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs (Pas par défaut) fie paramètre hellman Valeurs
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN. Diff Sélectionnez entre 1024 et 2048 bit clés bits Diffie Hellman pour la sécurité.	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs (Pas par défaut) fie paramètre hellman Valeurs DH2048 / DH1024
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN. Diff Sélectionnez entre 1024 et 2048 bit clés bits Diffie Hellman pour la sécurité.	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs (Pas par défaut) fie paramètre hellman Valeurs DH2048 / DH1024 Subnet / Subnet Mask
Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS. Authentification utilis Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN. Diff Sélectionnez entre 1024 et 2048 bit clés bits Diffie Hellman pour la sécurité. Serveur virtuel S Le sous-réseau et sous-réseau masque que le serveur va créer pour attribuer l'adresse à lui-même et les clients	server.key TLS Auth Key Valeurs (Pas par défaut) sateur / mot de passe Valeurs (Pas par défaut) fie paramètre hellman Valeurs DH2048 / DH1024 Subnet / Subnet Mask Valeurs



Pc	oussez DNS au client
Si elle est activée (Auto), le serveur va pousser ses informations de serveur DNS pour le client. Manuel permet à l'information de DNS pour	Valeurs
être saisie manuellement.	NO / Auto / Manuel
	Client Isolation
Lorsque certains oui, les clients ne verront pas les uns des autres. Sélectionnez non il permettra des clients différents pour être en mesure de	Valeurs
«voir» les uns des autres. Par défaut, les clients ne verront le serveur.	Non / Oui
Kee	ep Alive Ping Interval
La directive vie keep provoque des messages de ping-like à envoyer avant	Valeurs
descendu. Par défaut 10 secondes.	10
Kee	p Alive Ping Période
Par défaut 120 secondes. Ping toutes les 10 secondes, on suppose que	Valeurs
deuxième période de 120 fois. (Doit être au moins deux fois l'intervalle spécifié ci-dessus)	120
	Chiffrer
Sélectionnez un algorithme de chiffrement cryptographique. Doit être le même sur le serveur et le client.	Valeurs
	DES-CBC RC2-CBC DES-EDE-CBC DES-EDE3-CBC DESX-CBC BF-CBC RC2-40-CBC CAST5-CBC RC2-64-CBC AES-128-CBC AES-128-CBC AES-256-CBC SEED-CBC
Utilis	er LZO Compression
Activer / Désactiver la compression LZO sur le lien VPN. Lempel-Ziv- Oberhumer (LZO) est un algorithme de compression sans perte de	Valeurs
données.	Activer / Désactiver
OpenVPN Param	ètres réseau serveur
OpenVPN supporte plusieurs sous-réseaux derrière serveur / client. Alors que la connexion von peut atteindre le sous-réseau derrière. Chaque sous-	Valeurs
réseau doit être spécifié pour les données peuvent être acheminés correctement.	(Pas par défaut)



OpenVPN Client

Le Bullet Plus prend en charge OpenVPN et peut être configuré comme un serveur ou un client. Cette section décrit la configuration d'un client OpenVPN.

Systen	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin		
Summa	ry Gateway	/ To Gatev	vay L2TP	Client Op	enVPN	GRE V	PN User	s Cer	tificate	25				
OpenV	PN													
Open	/PN Setup													
Open∨PN Mode			Clie	nt 🔻										
Open	/PN Client Setup													
Cli	ent Bridge Mode													
Tu	nnel Protocol		UDF	UDP •										
MS	SFIX/Fragment s	ize	1370	1370 [1370]										
Se	ver1 IP : Port			: 1194										
			Add	Remove										
Ro	ot Certificate		ca.cr	ca.crt [ca.crt]										
Cli	ent Certificate		clien	client.crt [client.crt]										
Cli	ent Key		clien	t.key		[client.key]								
TL	S Auth Key					[ta.key]								
Us	er/Password Aut	hentication												
Ke	ep Alive Ping Int	erval(second	s)	[10]										
Ke	Keep Alive Ping Period(seconds)			[at least twice of Interval]										
Cij	oher		BF-0	BF-CBC •										
Us	e LZO Compress	ion	Disa	ble •										

Image 4-6-4: VPN > OpenVPN Client

	OpenVPN Mode
Activer / Désactiver le mode OpenVPN en sélectionnant le mode d'opérer	Valeurs
demandes de connexion entrantes des clients OpenVPN.	Client / Serveur / Désactiver
	Client Bridge Mode
Cochez la case pour activer le mode Client Bridge.	Valeurs
	(Décochée)
	Pseudowire Mode
Lorsque le mode Client Bridge est sélectionné l'option pour activer le	Valeurs
	(Décochée)
	Protocole de tunnel
Sélectionnez le protocole de tunnel à utiliser. Les options sont TCP et	Valeurs
	TCP / UDP



MS	SFI	(/ taille d	de Fragmo
Le maximum résultant UDP envoyer la taille des paquets après	la	Valeurs	
la valeur maximale seront fragmentés.	1370		
		Serv	eur IP / P
L'adresse IP et le port TCP / UDP qui se trouve le serveur. Ceci e	est	Valeurs	
serveur est en cours d'exécution.	ie	(Pas par dé	efaut)
		Roc	ot Certific
Le fichier racine de certificat (fichier CA) que tout le serveur et les clie	nts	Valeurs	
doivent avoir en commun.		ca.crt	
		Cer	tificat cli
Le certificat client qui est le fichier de certificat qui réside uniquement su	r le	Valeurs	
client.		client.crt	
			Client k
La clé du client privé, qui ne devrait pas être divulguée.		Valeurs	
		client.key	
		TI	_S Auth K
Le serveur et chaque client doit disposer d'une copie de cette clé pour fa	aire	Valeurs	
Taumentification TES.		(Pas par de	éfaut)
			Cipl
Sélectionnez un algorithme de chiffrement cryptographique. Doit être	Val	eurs	
ie meme sur le serveur et le client.	DES RC2 DES DES DES BF-0	-CBC -CBC -EDE-CBC -EDE3-CBC :X-CBC CBC	RC2-40-CBC CAST5-CBC RC2-64-CBC AES-128-CB AES-192-CB AES-256-CB SEED-CBC
U1	tilis	er LZO <u>C</u>	omp <u>res</u> si
Activer / Désactiver la compression LZO sur le lien VPN. Lempel-Z	Ziv-	Valeurs	

données.

Activer / Désactiver



4.6.4 VPN > GRE

GRE Configuration

Le BulletPlus soutient GRE (Generic Routing Encapsulation) Tunneling qui peuvent encapsuler une grande variété de protocoles de couche réseau non pris en charge par VPN traditionnel. Cela permet à des paquets IP de voyager d'un côté d'un tunnel GRE à l'autre sans être analysé ou traité comme des paquets IP.

System Netwo	rk Car	rrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summary Gate	way To (Gatew	ay L2TP	Client O	penVPN	GRE V	'PN User	s Cer	tificate	es			
Add a New Tunne	1												
Name													
Enable 0													
Multicast													
TTL													
MTU													
Key													
ARP													
NAT													
Interface			4G	•									
Local Setup													
Gateway IP Add	iress												
Tunnel IP Addr	ess 🕕												
Netmask													
Subnet IP Addr	ess												
Subnet Mask													
Remote Setup													
Gateway IP Add	iress												
Subnet IP Addr	ess												
Subnet Mask													
IPsec Setup													
Enable 🕕			None	9	•								

Image 4-6-5: VPN > Modifier / Ajouter GRE Tunnel

		Nom
Chaque tunnel GRE doit avoir un nom unique. Jusqu'à 10 tunnels GRE	Valeurs	
sont pris en charge par la puce Plus.	gre	
		Activer
Activer / Désactiver le Tunnel GRE.	Valeurs	

Désactiver / Activer



	Multicast			
Activer / Désactiver le support multicast via le tunnel GRE.	Valeurs			
	Désactiver / Activer			
	TTL			
Réglez le TTL (Time-to-live) la valeur pour les paquets qui traversent le	Valeurs			
	1 - 255			
	Clé			
Entrez une clé est nécessaire, la clé doit être le même pour chaque	Valeurs			
	(Pas par défaut)			
	ARP			
Activer / Désactiver ARP (Address Resolution Protocol) support sur le	Valeurs			
	Désactiver / Activer			
Configuration locale				

La configuration locale se réfère à la partie locale du tunnel GRE, par opposition à l'extrémité distante.

Adress	se IP de la passerelle			
Ceci est l'adresse IP WAN des BulletPlus, ce champ doit être rempli avec	Valeurs			
Taulesse if actuelle WAIN.	(Variable)			
	Tunnel Adresse IP			
Ceci est l'adresse IP du tunnel local.	Valeurs			
	(Variable)			
	Netmask			
Entrez le masque de sous-réseau de l'adresse IP du tunnel local.	Valeurs			
	(Variable)			
	Subnet Adresse IP			
Entrez l'adresse de sous-réseau pour le réseau local.	Valeurs			
	(Variable)			



	Subnet Mask
Le masque de sous-réseau pour le réseau / sous-réseau local.	Valeurs
	(Variable)

Configuration à distance

La configuration à distance indique les BulletPlus sur l'extrémité éloignée, l'adresse IP pour créer le tunnel, et le sous-réseau qui est accessible sur le côté opposé du tunnel.

Adress	e IP de la passerelle
Entrez l'adresse IP WAN du Bullet Plus ou autre GRE dispositif pris en	Valeurs
charge dans lequel un tunnel doit etre cree avec à l'extremite eloignee.	(Variable)
	Subnet Adresse IP
L'est de l'adresse IP du réseau distant, sur le côté opposé du tunnel GRE.	Valeurs
	(Variable)
	Subnet Mask
Le est le masque de sous-réseau pour le réseau à distance / sous-réseau.	Valeurs
	(Variable)

IPsec Setup

Reportez-vous à la configuration IPsec dans la section du site VPN au site du manuel pour plus d'informations.



4.6.5 VPN > VPN Utilisateurs

Pour VPN L2TP ou opération OpenVPN, les utilisateurs seront tenus de fournir un nom d'utilisateur et mot de passe. Utilisez le menu Utilisateurs VPN pour configurer les utilisateurs requis.

System	Network	Carrier	Win	eless	Firew	/all	VPN	Route	r	Serial	I/0	GPS	Apps	Diag	Admin
Summary	/ Gateway	To Gate	way	L2TP	Client	Ор	enVPN	GRE	VP	N User	s Cer	tificate	15		
VPN User	rs														
New L2T	P user name/pa	assword													
L2TP	Username														
L2TP	New Password	ł		(5-64 characters,no space)											
L2TP	Confirm New	Password													
New Ope	nVPN user nam	e/password													
Open	VPN Username	e													
OpenVPN New Password				(5-64 characters,no space)											
Open	VPN Confirm I	New Passwo	rd												

Image 4-6-6: VPN > Accès Client VPN

	Nom d'utilisateur
Entrez un nom d'utilisateur pour l'utilisateur en cours d'installation.	Valeurs
	(Pas par défaut)
Ν	louveau mot de passe
Entrez un mot de passe pour l'utilisation.	Valeurs
	(Pas par défaut)
Confirmer le n	ouveau mot de passe
Entrez à nouveau le mot de passe, les BulletPlus veillera à ce que le match	Valeurs
de moi de passe.	(Pas par défaut)



4.6.6 VPN > Gestion des certificats

Lorsque vous utilisez les fonctionnalités VPN du BulletPlus, il est possible de sélectionner X.509 pour le type d'authentification. Si tel est le cas, les BulletPlus doivent utiliser les certificats x.509 nécessaires afin d'établir un tunnel sécurisé entre d'autres appareils. Gestion des certificats permet à l'utilisateur une place pour gérer ces certificats.

	11						getter de la constante						
	m	icro	hard	SVST	FMS	INC					0	10	1
			marc	5151	LIVIS	INC.	101	010	210	21	0	01	0
System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summar	y Gateway	To Gate	way L2TP	Client Op	enVPN	GRE \	/PN User	s Cer	tificate	25			
Certifica	ates												
X509 R	oot Certificates												
No.			Name									Config.	
Imp	ort Certificate:		Choose file	Choose file No file chosen									
X509 C	ertificates												
No.	ant Cantification		Name	No filo chos								Config.	
imp	ont Certificate:		Choose life		Sell							import	
X509 P	rivate Keys												
No.			Name									Config.	
Imp	ort Private key:		Choose file	No file cho	sen							Import	
X509 C	ertificates Revoc	ation Lists											
No.			Name									Config.	
Imp	ort Certificate:		Choose file	No file chos	sen							Import	

Image 4-6-7: VPN > Gestion des certificats



4.7 Routeur

4.7.1 Routeur > RIPV2

Le BulletPlus est capable de fournir et de participer à RIPv2 (Routing Information Protocol v2), pour échanger des informations de routage des périphériques connectés. Les routes statiques peuvent également être ajoutés dans le menu> Routes Réseau.

System Network Carrier Wired RIPV2 OSPF	rd systems inc. Serial VPN Router Serial I/O GPS Apps Diag Admin
Router Configuration	
RIPV2 Status Authentication Type Authentication Port MD5 Authentication Password RIPv2 Network Announcement Configuratio	Enable T MD5 T WAN T
Subnet Address / SubnetMask Length Address / SubnetMask Length Add To Network List RIPv2 Network Announcement List	
Subnet Address	SubnetMask Length

Image 4-7-1: Routeur > RIPv2

	RIPV2 Status
Activer ou désactiver RIPV2 routage sur les BulletPlus. Si activé le BulletPlus échangera des informations de routage sur les interfaces spécifiées () réseaux connectés.	Valeurs
	Activer / Désactiver
Type d'authentification / Port / Mot de passe	
Activer l'authentification MD5 sur le protocole RIPV2. Sélectionnez également le port utilisé pour RIPV2, et le mot de passe requis.	Valeurs
	Aucun MD5
Configuration Annonce RIPV2 Réseau	
Chaque réseau ci-joint qui est de participer à l'échange RIPV2 doit être spécifié ici. Une fois les réseaux ajoutées qu'ils participants apparaissent dans la liste.	Valeurs
	(Pas nar défaut)

(Pas par défaut)


4.7.2 Router > OSPF

Le BulletPlus est également capable de fournir et de participer à OSPF (Open Shortest Path First), pour échanger des informations de routage des périphériques connectés. Les routes statiques peuvent également être ajoutés dans le menu> Routes Réseau.

micro	hard systems	INC.		010	10101
System Network Carrier	Wireless Firewall VPN	Router Serial I/0	O GPS Apps	Diag Admin	10110
Router Configuration					
OSPF Status OSPF Network Announcement Conf	Enable T				
Network Address / Network Mask	OSPF Area				
OSPF Network Announcement List					
Network Address	Network Mask	OSPF Area			

Image 4-7-2: Router > OSPF

	OSPF Status
Activer ou désactiver le routage OSPF sur les BulletPlus. Si activé le	Valeurs
spécifiées () réseaux connectés.	Activer / Désactiver
Configuration /	Annonce OSPF Réseau
Chaque réseau ci-joint qui est de participer à l'échange OSPF doit être	Valeurs

Chaque réseau ci-joint qui est de participer à l'échange OSPF doit être spécifié ici. Une fois les réseaux ajoutées qu'ils participants apparaissent dans la liste.

(Pas par défaut)

© Microhard 2016



4.8 Serial

4.8.1 Serial> Statut

La série> menu Etat présente un résumé du Port de données série RS232 situé sur le côté des BulletPlus, le port utilise un connecteur DB-9 standard. Si les convertisseurs USB-série sont connectés, ils seront également apparaître comme de nouveaux onglets répertoriés comme des périphériques USB. A ce moment le BulletPlus ne supporte que certains appareils utilisant FTDI générique ou pilote Prolific USB-to-Serial.

La fenêtre Résumé affiche un certain nombre d'éléments d'état qui aident à visualiser l'opération, les statistiques et le dépannage de l'interface RS232 ou USB port série.

Situation Générale

- Ports USB (série) Listes disponibles RS232 ou disponibles Port.
- Port Status Indique si le port a été activé dans la configuration.
- Vitesse La vitesse de transmission de courant utilisé pour l'interface avec l'appareil connecté.
- Connecter As Le type de protocole IP Config est affiché ici (TCP, UDP, SMTP, PPP, etc.)
- · Connecter Status Indique s'il y a des connexions actuelles / si le port est actif.
- Recevoir Octets Affiche le total des octets reçus par le modem dans la session en cours.
- Recevoir Packets Affiche le total des paquets reçus dans la session en cours.
- Transmettre Octets Affiche le nombre total d'octets transmis par le modem dans la session en cours.
- Transmit Packets Affiche le total des paquets transmis dans la session en cours.

1	m	icro	hard s	YSTEMS	INC.	1010	101	01	0	1010	101 010 101
System	Network	Carrier	Wireless Fir	ewall VPN	Router	Serial	I/O GP	S Apps	Diag	Admin	
Status S	Settings U	SB0									
Serial Po	rt Status										
Port	Status	Baud Rate	Connect As	Conn Statu	ect R s b	eceive ytes	Receive packets	Transn bytes	nit	Transmit packets	
RS232	Enable	115200	TCP Server	Active	e (1) 1	2.58 KB	432	90 B		90	
USBO	Enable	115200	TCP Server	Active	e (1) 1	.21 KB	44	0 B Stop F	Refreshing	0 Interval: 20 (in s	seconds)

Image 4-8-1: Serial > Statut



4.8.2 Serial > Paramètres

Cette option de menu permet de configurer le serveur de périphérique série pour le port de communication série. données de l'appareil de série peuvent être introduits dans le réseau IP via TCP, UDP, ou multicast; il peut également quitter le réseau BulletPlus sur un autre port série BulletPlus. L'interface RS232 entièrement sélectionnée prend en charge une liaison matérielle.

Le BulletPlus est équipé de 2 modes de communication série comme décrit ci-dessous:

- Données Le port principal de données RS232 pour terminaux. Ce port prend en charge complète handshaking.
- Console Le mode par défaut pour ce port doit être configuré en tant que port de la console et est utilisé pour le diagnostic et la configuration à l'aide d'un ensemble de commandes AT. (115200/8 / N / 1)

USB

Le BulletPlus prend en charge l'utilisation de l'USB-to-Serial convertisseurs et de nouveaux onglets pour la configuration USB apparaîtra une fois un convertisseur a été connecté au port USB du BulletPlus. A cette époque, seuls les pilotes spécifiques FTDI et Prolific génériques sont pris en charge.

Bien que le BulletPlus peut être connecté à un concentrateur USB et de plusieurs ports USB peut être utilisé en tant que ports série supplémentaires, ce n'est pas pratique que chaque fois qu'un appareil est connecté (ou le BulletPlus redémarrage) il est attribué un numéro de port et il est actuellement pas un moyen fiable pour assurer ce port sera le même à chaque fois.

Les ports USB prennent en charge TCP / UDP paramètres de base du port série sont traitées pour le port série RS232.

microha	rds	YSTE	EMS	INC.	-			-	0	10
		-	-	-	101	010	10	1.1	~	01
System Network Carrier Wire	less Fir	rewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Status Settings USB0										
Serial Port Configuration										
Port Configuration										
Port status	Data	,								
Data Baud Rate	115200 🔻]								
Data Format	8N1 ▼									
Data Mode	Seamles	ss 🖲 Trar	nsparent							
Character Timeout	24]						
Maximum Packet Size	256]						
No-Connection Data 🛈	Oisable	Enable	e							
MODBUS TCP Status	Oisable	Enable	e							
IP Protocol Config	TCP Serv	er		•						
TCP Configuration										
Server Mode	Monitor	r 🔍 Pollin	g							
Polling Timeout (seconds)	10]						
Local Listening port	20002]						
Incoming Connection Timeout(second	300]						

Image 4-8-2: Serial > Configuration des paramètres



		Port Status
Sélectionnez l'état de fonctionnement du port série. Le port est	Valeurs	
	Désactivé /	Activer
	D	onnées bauds
La vitesse de transmission de série est la vitesse à laquelle le modem est de communiquer avec le périphérique asynchrone local connecté.	Valeurs 921600 460800 230400 115200 57600 38400 28800 19200 14400	9600 7200 4800 3600 2400 1200 600 300

例

Remarque: La plupart des ordinateurs ne prennent pas facilement les communications série supérieures à 115200 bps. Ce paramètre détermine le format des données sur le port série. La valeur par défaut est de 8 bits de données, pas de parité et 1 bit d'arrêt.

FO	rma	it ae	nnees

Valeurs

8N1 / 8E1 / 8O1

Contrôle de flux

Le contrôle de flux peut être utilisé pour améliorer la fiabilité des communications de données série, en particulier à des vitesses de transmission plus élevés. Si le périphérique connecté ne supporte pas une liaison matérielle, laissez ce paramètre à la valeur par défaut de 'None'. Lorsque CTS Framing est sélectionné, le BulletPlus utilise le signal CTS à la porte les données de sortie sur le port série.



Le contrôle de flux logiciel (XON / XOFF) ne sont pas pris en charge.



Aucun Matériel CTS Framing

Valeurs

Dessin 4A: Données CTS Sortie Encadrement

	Pure-données de retard
Voir le dessin ci-dessus 4A.	Valeurs
	100
	Post-données Délai
√oir le dessin ci-dessus 4A.	Valeurs
	100



Mode de données

Ce paramètre définit la série cadrage de données de sortie. En mode transparent (par défaut), les données reçues sont sorties rapidement des BulletPlus.

Valeurs

Seamless / Transparent

Lorsqu'il est réglé sur Seamless, le serveur de port série va ajouter un écart entre les trames de données pour se conformer au protocole MODBUS par exemple. Voir «Caractère Timeout» ci-dessous pour des informations connexes.

Timeout de caractères

Valeurs

24

En mode continu (voir Mode de données décrit à la page précédente), ce paramètre détermine quand le serveur série examinera les données entrantes récemment reçues comme étant prêt à transmettre. Conformément à la norme MODBUS, les cadres seront marqués comme «mauvais» si l'écart de temps entre les images est supérieure à 1,5 caractères, mais inférieure à la valeur du délai d'attente de caractères.

Le serveur série utilise également ce paramètre pour déterminer l'intervalle de temps entre les images insérées. Il est mesuré en «personnages» et liée à la vitesse de transmission.

Exemple: Si la vitesse de transmission est 9600 bps, il faut environ 1ms pour déplacer un personnage. Avec le délai d'attente de caractères réglé sur 4, le délai d'attente est de 4ms. Lorsque le temps calculé est inférieur à 3.5ms, le serveur de série sera réglé le délai d'attente de caractères à une valeur minimale de 3.5ms.

Si la vitesse de transmission est supérieure à 19200 bps, le délai minimal de caractères est réglé en interne sur 750us (microsecondes).

	Packet Taille maximale
Définit la taille de la mémoire tampon que le serveur série utilisera	Valeurs
que les critères de délai d'attente de caractères a été atteint, ou le tampon est plein, il en paquet la trame reçue et la transmet.	1024
	Pas de connexion-Data
Lorsqu'elle est activée les données continueront à le tampon reçu sur	Valeurs
Lorsqu'il est désactivé, les BulletPlus sera ignorer toutes les données reçues sur le port série de données lorsque la synchronisation radio est perdu.	Désactiver / Activer
	MODBUS TCP Status
Cette option activer ou désactiver les fonctions MODBUS de	Valeurs
decodage el d'encodage.	Désactiver / Activer
MODE	BUS TCP Protection Key
Clé de chiffrement MODBUS utilisée pour la fonction d'état MODBUS	Valeurs
	1034



IP Protocol Config

Ce paramètre détermine quel protocole le serveur série utilisera pour transmettre des données de port série sur le réseau BulletPlus.

Le protocole sélectionné dans le champ de protocole IP Config déterminera quelles options de configuration apparaissent dans le reste du menu Configuration RS232. TCP client Serveur TCP TCP Client / Serveur UDP Point-to-Point client SMTP PPP Mode transparent GPS

Valeurs

TCP Client: Lorsque TCP Client est sélectionné et les données sont reçues sur son port série, l'BulletPlus prend l'initiative de trouver et de se connecter à un serveur TCP distant. La session TCP se termine par cette même unité lorsque la session d'échange de données est terminée et que le délai de connexion a expiré. Si une connexion TCP ne peut être établie, les données de port série est mis au rebut.

• Serveur distant Adresse

Adresse IP d'un serveur TCP qui est prêt à accepter des données du port série via une connexion TCP. Par exemple, le serveur peut résider sur un serveur de réseau local. Par défaut: 0.0.0.0

Port de serveur distant

Un port TCP du serveur distant qui écoute, en attente d'une requête de connexion de session provenant du client TCP. Une fois que la session est établie, les données du port série est communiquée à partir du client au serveur. Par défaut: 20001

• Sortant Délai de connexion

Ce paramètre détermine quand le Bullet Plus va mettre fin à la connexion TCP si la connexion est dans un état de repos (à savoir pas de trafic de données sur le port série). Valeur par défaut: 60 (secondes)

Serveur TCP: Dans ce mode, la série BulletPlus ne sera pas lancer une session, au contraire, il attendra un client pour demander une session de celui-ci (il est d'être le serveur-it 'sert' un client). L'unité «écouter» sur un port TCP spécifique. Si une session est établie, les données iront à partir du client vers le serveur, et, si elle est présente, à partir du serveur vers le client. Si une session est pas établie, les données série côté client et côté serveur de données série, le cas échéant, seront rejetées.

• Port d'écoute locale

Le port TCP lequel le serveur écoute. Il permet une connexion TCP doit être créé par un client TCP pour transporter des données du port série. Par défaut: 20001

Incoming Délai de connexion

Créé lorsque le serveur TCP mettra fin à la connexion TCP est la connexion est dans un état inactif.

Par défaut: 300 (secondes)



UDP: User Datagram Protocol ne fournit pas d'informations de séquençage pour les paquets envoyés ni établir une «connexion» («handshake») et est donc le plus adapté à communiquer petits paquets de données.



TCP: Transmission Control Protocol contrairement à UDP fournit des informations de séquençage et est orienté connexion; un protocole plus fiable, en particulier lorsque de grandes quantités de données sont communiquées.

Nécessite plus de bande passante que UDP.

microhard

IP Protocol Config (a continué...)

BulletPlus

TCP Client / Serveur: Dans ce mode, le BulletPlus sera un client TCP combiné et le serveur, ce qui signifie qu'il peut à la fois initier et servir connexion TCP (session) des demandes. Reportez-vous aux descriptions des clients et TCP Serveur TCP et les paramètres décrits précédemment que toutes les informations, combinées, est applicable à ce mode.

UDP Point-to-Point: Dans cette configuration, le BulletPlus envoie des données en série à un point spécifiquement défini, en utilisant des paquets UDP. Ce même BulletPlus acceptera des paquets UDP à partir de ce même point.

Adresse IP distante

Adresse IP du périphérique distant auquel les paquets UDP sont envoyés lorsque les données reçues au port série. Par défaut: 0.0.0.0

Port à distance

Port UDP du dispositif distant mentionné ci-dessus. Par défaut: 20001

• Port d'écoute

Port UDP qui la série IP écoute (moniteurs). les paquets UDP reçus sur ce port sont transmis au port série de l'appareil. Par défaut: 20001

Client SMTP: Si le BulletPlus a accès à Internet, ce protocole peut être utilisé pour envoyer les données reçues sur le port série (COM1), dans un format sélectionnable (voir mode de transfert (ci-dessous)), à un destinataire e-mail. Tant le serveur SMTP et le destinataire e-mail doit être «accessible» pour sa fonction à la fonction.

Mail Sujet

Entrez un (e-mail intitulé) adapté 'objet du courriel. Par défaut: COM1 message

Mail Server (IP / Nom)

Adresse IP ou 'Nom' de SMTP (messagerie) Server. Par défaut: 0.0.00

• Destinataire du courrier

Une adresse e-mail valide pour le destinataire prévu, est entré dans le format approprié. Par défaut: accueil @

• Message Max Taille

La taille maximale pour le message électronique. Par défaut: 1024

• Timeout (s)

Combien de temps l'unité attendra pour recueillir des données à partir du port série avant d'envoyer un message e-mail; les données seront envoyées immédiatement après avoir atteint un message Taille max. Valeur par défaut: 10

• Mode de transfert

Sélectionnez la façon dont les données reçues sur COM1 doit être envoyé à l'adresse e-mail. Les options sont: Texte, fichier joint, Code Hex. Par défaut: Texte

Un UDP ou TCP port est une application de point final. L'adresse IP identifie le périphérique et, comme une extension de l'adresse IP, le port essentiellement «airs fins» où les données doivent aller «dans le dispositif.

Veillez à choisir un numéro de port qui est pas prédéterminé d'être associé à un autre type d'application, par exemple HTTP utilise le port 80.

La multidiffusion est une

transmission un-à-un grand nombre de données sur un réseau IP. Il est une méthode efficace pour transmettre les mêmes données vers plusieurs destinataires. Les bénéficiaires doivent me membres du groupe de multidiffusion spécifique.



TTL: Time to Live est le nombre de sauts qu'un paquet peut voyager avant d'être jetés.

Dans le contexte de multidiffusion, d'une valeur TTL de 1 limite la plage du paquet sur le même sousréseau.



IP Protocol Config (a continué...)

PPP: COM1 peut être configuré comme un serveur PPP pour une connexion série avec un PC ou un autre périphérique. Le PC connecté pourrait alors utiliser une série dédiée (WindowsXP - dialup / modem) de type connexion PPP pour accéder aux ressources du réseau des BulletPlus. Remarque: la console (si elle est configurée en tant que port de données) ne prend pas en charge ce mode.

PPP Mode

Peut être réglé pour Active ou passive. Si elle est définie pour Active, le serveur PPP initiera la connexion PPP avec un client PPP. Le serveur enverra périodiquement des demandes de liaison suivant le protocole PPP. Si la valeur passive, le serveur PPP ne sera pas lancer la connexion PPP avec le client PPP. Le serveur va attendre passivement le client pour lancer la connexion. Par défaut: Passif

• Chaîne prévue

Quand un client (PC ou périphérique) initie une session PPP avec le modem, c'est la chaîne handshaking qui devrait, afin de permettre une connexion. En général, cela doe pas besoin d'être changé.

Par défaut: CLIENT

• Chaîne de réponse

Ceci est la chaîne handshaking qui sera envoyé par le modem une fois que la chaîne attendue est reçue. En général, cela n'a pas besoin d'être changé. Par défaut: CLIENT SERVEUR

• PPP LCP Echo Nombre de défaillance

Le serveur PPP présumera l'homologue d'être mort si les LCP echo-requêtes sont envoyées sans recevoir de LCP echo-réponse valide. Si cela se produit, le serveur PPP mettra fin à la connexion. L'utilisation de cette option nécessite une valeur non nulle pour le paramètre LCP Echo Interval. Cette option peut être utilisée pour activer le serveur PPP de mettre fin après la connexion physique a été rompu (par exemple, le modem a raccroché). Par défaut: 0

• PPP Echo LCP Intervalle

Le serveur PPP envoie une trame de requête d'écho LCP à l'homologue tous les 'n' secondes. Normalement, le pairs devrait répondre à l'écho-demande en envoyant un écho-réponse. Cette option peut être utilisée avec l'option LCP-echo-failure pour détecter que le pair est plus connecté. Par défaut: 0

• PPP IP locale

Entrez l'adresse IP locale PPP, l'adresse IP du COM0 Port IPn4G. Par défaut: 192.168.0.1

PPP Host IP

Entrez l'adresse IP de l'hôte PPP ici. Ceci est l'adresse IP du PC ou le périphérique connecté.

Par défaut: 192.168.0.99

• PPP Idle Timeout(s)

Il est le délai d'attente pour la destruction de la connexion ppp quand il n'y a pas de trafic de données dans l'intervalle de temps. Quand il y a des données à venir, une nouvelle connexion ppp sera créé. Valeur par défaut: 30



SMTP: Simple Mail Transport Protocol est un protocole utilisé pour transférer le courrier à travers un réseau IP.



IP Protocol Config (a continué...)

GPS Mode transparent: En mode Transparent GPS, les données GPS est signalé sur le port série à 1 seconde d'intervalle. Exemple de sortie est illustré ci-dessous:

File Edit View Call Transfer Help	
The Fac Tick Tay Turket Teb	
\$GPVTG,,T,,M,,N,,K*4E \$GPGSV,1,1,00*79 \$GPGGA,,0,,*66 \$GPRMC,,V,,,N*53 \$GPGSA,A,1,,*1E \$GPVTG,,T,,M,,N,,K*4E \$GPGSV,1,1,00*79 \$GPGGA,,0,,*66 \$GPRMC,,V,,N*53 \$GPGSA,A,1,,N*53	
Connected 0:08:02 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo	

Image 4-8-3: Serial > Mode transparent GPS



4.9 I/O

4.9.1 I/O > Paramètres

Le BulletPlus a 8 l programmable / S, qui peut être utilisé avec différentes alarmes et des capteurs pour la surveillance, indiquant le modem lorsque certains événements ont eu lieu, comme une alarme d'intrusion sur une porte, etc. Tout le E / S peut également être programmé pour fonctionner comme une sortie, qui peut être utilisé pour piloter un relais externe pour contrôler à distance des équipements et appareils. Les broches d'E / S sont disponibles sur le connecteur de retour partagé avec la puissance d'entrée (1 et 2).

Le statut de l'E / S peut être lu, et dans le cas des sorties, peut être utilisé dans le WebUI. Les alertes peuvent être configuré pour envoyer des messages SMS si des changements d'E / S d'état, ainsi, les messages de contrôle SMS peuvent être envoyés à l'appareil pour déclencher des événements. SNMP et / ou Modbus peuvent être utilisés pour interroger le statut, ou définir des contrôles. Voir les sections appropriées du manuel pour plus d'informations.

7	m	icro	hard	SYSTEM	S INC.	10101	010	1	0	10	10 101 01010 10101
System	Network	Carrier	Wireless	Firewall VP	N Router	Serial I	O GPS	Apps	Diag	Admin	
Settings											
Settings											
Nam	e	Mode	• (Output Control							
I/01		O Inp	ut 🖲 Output	Open Oclosed	se						
1/02		Inp	ut 🔍 Output								
status											
Name		Mod	de	Statu	s	Mete	er(V)				
I/O1		Inpu	ut	High		2.77					
1/02		Inpu	ut	High		2.81					
Refresh								Stop I	Refreshing] Interval: 2	0 (in seconds)

Image 4-9-1: I/O Paramètres

Paramètres

Le menu Paramètres est utilisé pour configurer un I / O soit comme une entrée ou une sortie. Si elle est configurée en tant que sortie, l'utilisateur peut également définir la sortie comme ouvert ou fermé. La broche de sortie sur le BulletPlus peut être utilisée pour fournir des signaux de sortie qui peuvent être utilisés pour commander un relais externe pour commander un dispositif externe. Voir le tableau 4-9-1 pour les spécifications I / O.

Statut

La section d'état affiche l'état et de mesure tension (mètre) de tout IOs configurées comme entrées. Le WebUI affiche également l'état actuel de chaque sortie de contrôle.



Nom	La description	Paramètre	Min.	Тур.	Max	Unités
I/O 1 - 2 (Contribution)	plage de basse tension de grille d'entrée	VIL	-0.5	0	1.2	V
	gamme de haute tension de l'Etat d'entrée	VIH	1.5	3.3	30	V
	courant de fuite d'entrée (3,3 VDC IN)	IIN		58		μA
	Source d'entrée d'application Pin comprend une résistance	on typique est u ce de 56KΩ inte	n contact o erne tirer ju	de commu usqu'à 3,3	tation à se VDC.	ec au sol.
I/O 1 - 2 (Sortie)	Ouvrir lecteur de drain à la masse	ldc		100	110	mA
	Tension maximale en circuit ouvert appliquée	Voc		3.3	30	V
	Une application typique est	de conduire un	e bobine o	de relais à	la masse.	

Table 4-9-1: Spécifications numérique I / O



4.10 GPS

4.10.1 GPS > Emplacement

Une carte

La carte de localisation indique l'emplacement sur les BulletPlus. L'unité va tenter d'obtenir les coordonnées GPS du récepteur intégré GPS, et en cas d'échec, utilisera l'emplacement Cell ID rapporté par le Cellular Carrier.



Image 4-10-1: GPS > Une carte

Les cartes peuvent être consultés soit avec Bing ou Google Maps en utilisant l'option située en bas, coin juste à côté de l'option de rafraîchissement.

Si l'appareil avait un signal GPS (module GPS activé et l'antenne ci-joint), il présentera les coordonnées GPS spécifiques du modem, sinon seules les coordonnées estimées déclarées par le transporteur.



4.10.2 GPS > Paramètres

Les BulletPlus peuvent être interrogés pour les données GPS via les normes DSGP et / ou fournir des rapports personnalisables à un maximum de 4 hôtes différents en utilisant UDP ou de rapports par email. GPS est une fonctionnalité optionnelle de l'BulletPlus, et doit être spécifié au moment de la commande et préparé en usine. Si l'écran ci-dessous ne sont pas disponibles sur votre appareil, vous ne disposez pas d'un modèle de GPS activé.

	1							_				-
	m	icro	hard	1 SYST	EMS	INC.	101	010	10	1	0	10
System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Location	Settings	Report	GpsGate	Recorder	Load R	ecord T	AIP					
GPS Servi	ice Configur	ation										
Settings	Option:											
GPS S	Status		Ena	ble 🔻								
GPS	Source		Sta	ndalone GPS	T							
ТСР	Port		294	7		[0-65535] (Default 29	47)				
GPS	Online Assist	ance 0	Ena	ble 🔻								

Image 4-10-2: GPS > Paramètres

	Statut GPS	
Activer ou désactiver la fonction d'interrogation du GPS des BulletPlus.	Valeurs	
	Désactiver / Activer	
	GPS Source	
Le BulletPlus contient un module GPS autonome intégré dans l'unité. Pour utiliser les fonctions GPS de l'BulletPlus une antenne doit être connecté à	Valeurs	
l'antenne GPS Port.	GPS autonome GPS Module cellulaire	
	TCP Port	
Snácifiaz la nort TCP sur la BullatPlus où la sarvica CPS est en cours		
d'avécution et les systèmes distants neuvent se connecter et interroger des	Valeurs	
d'exécution et les systèmes distants peuvent se connecter et interroger des données GPS.	Valeurs 2947	
d'exécution et les systèmes distants peuvent se connecter et interroger des données GPS.	Valeurs 2947 stance en ligne GPS	
d'exécution et les systèmes distants peuvent se connecter et interroger des données GPS. Assi Lorsque les permis BulletPlus utilisera l'Internet pour télécharger un fichier au démarrage avec des informations sur son emplacement pour aider à	Valeurs 2947 stance en ligne GPS Valeurs	



4.10.3 GPS > Rapport

Le BulletPlus peut fournir des rapports personnalisables à un maximum de 4 hôtes utilisant UDP ou de rapports par email.

ystem Network C	arrier Wireless Fi	ewall VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
ocation Settings Re	eport GpsGate Rec	order Load F	Record T	AIP						
CPS Roport Configurati	0.0									
or o Report Configurati	01									
GPS Report No.1										
Report Define	UDP Re	ort 🔻								
Time Interval	600		(s)							
Message 1	ALL NM	A 🔹								
Message 2	None	•								
Message 3	None	•								
Message 4	None	•								
Trigger Set 0	Only Tim	er 🔻								
Local Streaming	Disable		•							
UDP Remote IP	0.0.0.0]							
UDP Remote PORT	20175		[0~65535]							
GPS Report No.2										
Report Define	Email Re	port 🔻								
Time Interval	600		(s)							
Message 1	ALL NM	A 🔹	-							
Message 2	None	•	1							
Message 3	None	•								
Message 4	None	•								
Trigger Set 0	Only Tim	er 🔻								
Mail Subject	GPSRep	rtMessage2]							
Mail Server(IP/Name)	smtp.gma	il.com:465	(xxx:port)							
User Name	@gmail.c	om]							
Password	•••]							
Authentication 0	None	•]							
Mail Recipient	host@		(xx@xx.xx)							
GPS Report No.3										
Report Define	Disable	T								
GPS Report No.4										
Report Define	Disable	T								

Image 4-10-3: GPS > Rapport GPS

	Signaler Définir
Activer UDP et / ou e-mail ou de rapports GPS désactiver. Jusqu'à 4 rapports peuvent être configurés et configuré indépendamment	Valeurs
	Désactiver Rapport UDP Email Rapport
	Intervalle de temps
Le compteur d'intervalle indique la fréquence à laquelle les données du	Valeurs
	600



	Message 1-4
Le champ du message permet de personnaliser jusqu'à 4 messages GPS différents pour être envoyées à l'hôte spécifié	Valeurs
Aucun - Le message est pas utilisé, aucune donnée ne sera envoyé ALL - Envoie tous les ci-dessous GGA - Données GPS Fix GSA - Données global par satellite GSV - Données détaillées par satellite RMC - Recommandé Données Min pour GPS VTG - Vector Track & Ground Speed GPSGate - Pour une utilisation avec GPSGate Tracking Software	Aucun ALL NMEA GGA GSA GSV RMC VTG Latitude Longitude GPSGate protocole UDP
Dé	clencheur est choisi
La condition de déclenchement définit les conditions qui doivent être remplies avant	Valeurs
les conditions de déclenchement à distance être remplies avant une mise à jour est envoyé. La condition ET, exige que le temporisateur de répétition et les conditions de déclenchement à distance être remplies avant une mise à jour est envoyé.	Seulement Minuteur Minuteur ET Distance Temps ou la distance
	Distance Set
Le paramètre de distance permet aux données GPS à seulement être	Valeurs
rapport.	1000
UDI	P IP à distance / Port
Ceci est l'adresse IP et le port de l'hôte distant dans lequel les paquets	Valeurs
ODF doivent ette envoyes.	0.0.0.0 / 20175
	Mail Sujet
Si un rapport d'Email est choisi, la ligne d'objet de l'e-mail peut être définie	Valeurs
ICI.	1000
	Serveur de courrier
Si un rapport d'email doit être envoyé, le serveur de courrier sortant doit être défini et le numére de port	Valeurs
	smtp.gmail.com:465
lder	ntifiant Mot de passe
Certains serveurs de messagerie sortants requis nom d'utilisateur et mot	Valeurs
informations de connexion ici.	Identifiant Mot de passe
Des	stinataire du courrier
Certains serveurs de messagerie sortants nécessitent un nom d'utilisateur	Valeurs
informations de connexion ici.	host@email.com



4.10.4 GPS > GpsGate

Le BulletPlus est compatible avec GpsGate - GPS Tracking Software, qui est une troisième solution de cartographie du parti utilisé pour divers services GPS, y compris véhicule et suivi Le BulletPlus peut communiquer avec GpsGate via le mode Tracker et TCP / IP actif. (Reporting UDP peut également envoyer des informations à GpsGate, voir le GPS> Rapport - Rapports UDP)

	1											10101
	m	icro	hard	l syst	EMS	INC.	101	10101	10	0	10	01010
System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/O GPS	6 Apps	Diag	Admin	
Location	Settings	Report	GpsGate	Recorder	Load R	lecord T	AIP					
GpsGate	TrackerOne	Connecti	on									
Tracker	Device Setting											
Mode	e Set		Ena	ble Tracker N	lode	•						
Serv	er Command	Channel	TCF	and SMS 🔻		- 1						
TCP	Alive Mode		_Pir	ng Command	•							
Aliv	e Time Interva	l	150			(s)						
Setu	p Phone Filter		Disa	able: Accept A	All V							
Mot	ion Trigger		Ena	ble Motion Tr	igger 🔻							
Sen	d IO Status		Disa	able		•						
Whe	en CPS Invalid,	Sending Da	ata Not	Use Last Val	d Positio	n 🔻						

Image 4-10-4: GPS > GpsGate Tracker Mode

Mode Tracker GpsGate

	Mode Set
Activer GpsGate mode Tracker ou modes TCP. En mode tracker Le logiciel	Valeurs
sont pas disponibles, il va tenter d'utiliser la messagerie SMS.	Désactiver Activer le mode Piste Activer TCP Envoyer mode
Serve	ur Commande Canal
Par défaut BulletPlus et GpsGate utilisera TCP et SMS pour assurer la	Valeurs
protocole TCP ou le SMS uniquement la communication. La configuration initiale en mode Tracker doit être via SMS.	TCP et SMS TCP seulement SMS seulement
Mode TCP Vivant / Vivan	t Intervalle de temps
Le mode vie TCP gardera connexion TCP vivant si traqueur est pas activé ou l'intervalle de suivi est trop long. La valeur par défaut est de 150	Valeurs
secondes.	150

150

© Microhard 2016



Un filtre de numéro de téléphone peut être utilisé pour empêcher les commandes SMS non destinées au BulletPlus d'âtre traitée	Valeurs		
	Désactiver: Accepter Toutes Activer le filtre		
	Mouvement Trigger		
Utilisez ce paramètre pour activer ou désactiver la détection de mouvement dans les BulletPlus	Valeurs		
	Désactiver Activer Mouvement Trigger		
	Envoyer IO Status		
Lorsqu'elle est activée, les BulletPlus va envoyer l'état actuel des entrées	Valeurs		
	Désactiver Envoyer Input Status Envoyer Etat de sortie Envoyer Entrée et sortie Etat		
Lorsque le GPS non valide	e, Envoi de données		

Spécifiez ce qui se passe lorsque les données GPS est invalide, soit utiliser la dernière position valide ou ne pas utiliser la dernière position valide.

Valeurs

Non Utilisez Dernière position valide Utilisez Dernière position valide

GpsGate - TCP Mode

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Location	Settings	Report	GpsGate I	Recorder	Load R	ecord T	AIP					
GpsGate	TrackerOne	e Connectio	on									
Tracker	Device Setting											
Mode	e Set		Ena	ble TCP Send	Mode 🔻	•						
Serv	er Address/IP	,	0.0.0	.0								
Serv	er Port		3017	5								
Serv	er Interval		60			(s)						
Mot	ion Distance		100			(m)						
Sen	d IO Status		Disa	ble		¥						
Whe	en GPS Invalid,	, Sending Da	ata Not	Use Last Vali	d Position	l ▼						

Image 4-10-5: GPS > GpsGate TCP Mode



	Mode Set
Activer GpsGate mode Tracker ou modes TCP. En mode TCP l'BulletPlus établit une connexion avec le serveur GpsGate directement sans le	Valeurs
processus d'installation de SMS. Si la connexion TCP ne sont pas disponibles, l'BulletPlus continuera d'essayer de se connecter toutes les quelques secondes.	Désactiver Activer le mode Piste Activer TCP Envoyer mode
Adi	resse du serveur / IP
Entrez l'adresse IP du serveur exécutant l'application GpsGate.	Valeurs
	0.0.0.0
	Port de serveur
Entrez le port TCP du serveur exécutant l'application GpsGate.	Valeurs
	30175
	Intervalle de serveur
Définir l'intervalle auquel le BulletPlus va envoyer des données au	Valeurs
	60
Ν	Nouvement Distance
Régler le seuil de mouvement dans lequel le BulletPlus sera déclenchée	Valeurs
	100
	Envoyer IO Status
Lorsqu'elle est activée, les BulletPlus va envoyer l'état actuel des entrées	Valeurs
	Désactiver Envoyer Input Status Envoyer Etat de sortie Envoyer Entrée et sortie Etat

Lorsque le GPS non valide, Envoi de données

Spécifiez ce qui se passe lorsque les données GPS est invalide, soit utiliser la dernière position valide ou ne pas utiliser la dernière position valide.

Valeurs

Non Utilisez Dernière position valide Utilisez Dernière position valide



4.10.5 GPS > Enregistreur

Les BulletPlus peut être configuré pour enregistrer des événements basés sur des intervalles de temps et / ou un déclencheur d'événements et de les stocker dans une mémoire non volatile. Ces événements peuvent être visualisées dans le WebUI, sur une carte, ou envoyés à un serveur distant dans un certain nombre de formats différents.

Recorder Service	
rrent GPS Infomation	
Local Time:	Wed Mar 26 15:26:59 MDT 2014
Satellites In View:	15
Satellites tracked:	10
Latitude:	51.142662,N
Longitude:	-114.075531,W
Altitude:	1130.2
Speed:	O(Km/h)
Orientation:	O(Degree to North)
NMEA UTC Time:	26/03/2014 21:26:59
S Recorder Setting	
Status	Enable GPS Recorder 🔻
Status Record Feature Selections:	Enable GPS Recorder (Record items among 16,000~36,000.)
Status Record Feature Selections: Time Interval	Enable GPS Recorder ▼ (Record items among 16,000~36,000.) 30 [30~65535](s)
Status Record Feature Selections: Time Interval DI/DO Changed	Enable GPS Recorder (Record items among 16,000~36,000.) 30 [30~65535](s) Record
Status Record Feature Selections: Time Interval DI/DO Changed Speed	Enable GPS Recorder (Record items among 16,000~36,000.) 30 [30~65535](s) Record Record
Status Record Feature Selections: Time Interval DI/DO Changed Speed Over Speed	Enable GPS Recorder (Record items among 16,000~36,000.) 30 [30~65535](s) Record [Record [Min 30](Km/h)
Status Record Feature Selections: Time Interval DI/DO Changed Speed Over Speed Orientation	Enable GPS Recorder (Record items among 16,000~36,000.) 30 [30~65535](s) Record 120 [Min 30](Km/h) Record
Status Record Feature Selections: Time Interval DI/DO Changed Speed Over Speed Orientation Orientation Changed	Enable GPS Recorder ▼ (Record items among 16,000~36,000.) 30 [30~65535](s) Record ▼ 120 [Min 30](Km/h) Record ▼ 60 [5~180](180:Disable)
Status Record Feature Selections: Time Interval DI/DO Changed Speed Over Speed Orientation Orientation Changed Carrier RSSI Level	Enable GPS Recorder (Record items among 16,000~36,000.) 30 [30~65535](s) Record Record 120 [Min 30](Km/h) Record 60 [5~180](180:Disable) Record

Image 4-10-6: GPS > GPS service Enregistreur

Statu

Valeurs

Utilisez le paramètre d'état pour activer la fonctionnalité d'enregistrement GPS des BulletPlus. Le nombre total d'enregistrements qui peuvent être enregistrées varie entre 16.000 et 36.000, en fonction du nombre de paramètres GPS qui sont enregistrés.

Désactiver Activer Enregistreur GPS

	Intervalle de temps
Définir l'intervalle auquel le BulletPlus enregistrera les données GPS. S'il	Valeurs
de satellites connectés), l'unité attendra jusqu'à ce que la prochaine fois que l'information valide est reçu.	300

DI/DO changé

Les BulletPlus peut détecter et signaler les informations GPS actuelle quand un changement d'entrée ou de l'état de sortie numériques, quel que soit le réglage de l'intervalle de temps.

<u>Valeurs</u>

Record / Will not Record



	La vitesse		
Sélectionnez Enregistrer pour inclure la vitesse actuelle dans les données	Valeurs		
	Record / aucun enregistrement		
	Plus de vitesse		
Déclencher une entrée d'enregistrement GPS lorsque la vitesse a dépassé	Valeurs		
le seur configure. On minimum de 30 Min/ in est fiècessaire.	120		
	Orientation		
Sélectionner le registre pour enregistrer l'orientation courante lorsqu'une	Valeurs		
entree GFS est enregistree. (Degre Nord).	Record / aucun enregistrement		
	Orientation Change		
Enregistrer un GPS, quel que soit l'intervalle de temps, si l'orientation des changemente unitaires (5 \approx 180: 180 = Désectiver)	Valeurs		
changements unitaries. (5 ~ 100. 100 – Desactiver)	60		
Trans	sporteur Niveau RSSI		
Sélectionnez Enregistrer pour enregistrer le niveau 3G / cellulaire RSSI	Valeurs		
courant lorsqu'une entree GPS est enregistree. (-dB).	Record / aucun enregistrement		
	Altitude		
Sélectionnez Enregistrer pour enregistrer l'altitude actuelle lorsqu'une	Valeurs		
entree GPS est enregistree (metres).			



4.10.6 GPS > Fiche de charge

Les données qui ont été enregistrées et sauvegardées par le BulletPlus peuvent ensuite être consultés ou envoyés à un serveur distant dans divers formats. Les données enregistrées peuvent également être consultés directement en sélectionnant «Voir les données» et les données peuvent être tracées sur une carte (accès Internet requis), en sélectionnant "Trace carte", ou "Trace rapide". Les captures d'écran cidessous montrent les données brutes qui peuvent être consultés et Trace Carte / sortie Trace rapide.



Image 4-10-7: GPS > GPS Record charge



	Record Time Range
Cochez les cases à côté des dossiers énumérés ci-dessus qui doivent être	Valeurs
envoyees au serveur.	(Pas par défaut)
Envo	yer Mode / Protocole
Spécifiez le type format de données / protocole pour les données à	Valeurs
envoyer.	NMEA via UDP NMEA via TCP GpsGate via UDP GpsGate via TCP Texte brut via UDP Texte brut via TCP
Ad	resse du serveur / IP
Saisissez l'adresse ou l'adresse IP du serveur distant sur lequel les	Valeurs
donnees doivent etre envoyees.	nms.microhardcorp.com
	Port de serveur
Entrer le numéro de port UDP / TCP du serveur distant vers lequel les données doivent être envoyées	Valeurs
	30175



4.10.7 GPS > TAIP

Le BulletPlus a la capacité d'envoyer des données GPS dans TAIP (Interface Protocol Trimble ASCII) pour jusqu'à 4 serveurs TAIP différents. La section suivante décrit les paramètres de configuration requis pour initialiser les rapports TAIP.

System Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Location Settings	Report	GpsGate F	Recorder	Load R	lecord T	AIP						
TAIP Configuration												
Settings No.1												
TAIP service statu	s	Ena	bled v									
Remote TAIP Serve	er	0.0.0	.0									
Socket Type		UDF	• ▼									
Remote TAIP Port		2100	0									
Message Type		RPV	/ 🔻									
Interval		5			(s)							
Vehicle ID		0000			4 Alphanur	neric chara	cters					
Settings No.2												
TAIP service statu	s	Disa	bled v									
Settings No.3												
TAIP service statu	s	Disa	ibled v									
Settings No.4												
TAIP service statu	s	Disa	ibled v									

Image 4-10-8: GPS > TAIP

	TAIP état du service
Activer ou désactiver le service TAIP sur le modem. L'unité peut rapporter	Valeurs
TAP à un maximum de 4 notes differents.	Activer / Désactiver
Télécon	nmande TAIP serveur
Entrez l'adresse IP du serveur distant TAIP.	Valeurs
	0.0.0.0
	Type de socket
Sélectionnez le type de socket qui est utilisé par le serveur TAIP à	Valeurs
(TCP), ou les données sont envoyées (UDP) au serveur.	UDP / TCP
	Port IP à distance
Entrez le numéro de port TCP ou UDP utilisé sur le serveur TAIP à	Valeurs
	UDP / TCP



	Type de message
Sélectionnez entre RPV et types de messages RLN.	Valeurs
RPV - Position / Velocity RLN - Message long Navigation	RPV / RLN
	Intervalle
Réglez la fréquence à laquelle des messages de type sont signalés au	Valeurs
60 secondes.	60
	ID du véhicule
Définissez l'ID du véhicule à l'aide de 4 caractères alphanumériques.	Valeurs
	0000



4.11 Apps

4.11.1 Apps > Modbus

4.11.1.1 Modbus > TCP Modbus

Les BulletPlus peut être configuré pour fonctionner comme un réseau TCP / IP ou série (COM) esclave Modbus et répondre aux demandes Modbus et signaler diverses informations comme indiqué dans les données cartographiques.

System	Network	Carrie	r Wireless	Firewall	VPN Router	Serial	I/O GPS	Apps	Diag	Admin
Modbus	Netflow Re	eport l	ocalMonitor	Event Rep	ort Websocke	it				
Modbus										
Modbus	Slave Device C	onfig:								
Statu	us		Enat	le Service 🔻]					
TCP	Mode Status		Enat	le TCP Conne	ction Service 🔻					
Por	t		502		[1 ~ 65535]					
Act	tive Timeout(s)		30		[0 ~ 65535]					
Slav	ve ID		1		[1 ~ 255]					
Coi	ls Address Off	set	0		[0 ~ 65535]					
Inp	ut Address Off	set	0		[0 ~ 65535]					
Reg	gister Address	Offset	0		[0 ~ 65535]					
Mas	ster IP Filter Se	t	Disa	ble IP Filter 🔻]					
Seria	al Mode Status	5	Enat	le Serial ASCI	I Mode 🔹 🔻					
Bau	id Rate		1920	0 🔻						
Dat	ta Format		8N1	T						
Cha	aracter Timeou	t(s)	5		[0 ~ 65535]					
Slav	ve ID		1		[1 ~ 255]					
Coi	ls Address Off	set	0		[0 ~ 65535]					
Inp	ut Address Off	set	0		[0 ~ 65535]					
Reg	gister Address	Offset	0		[0 ~ 65535]					
			<u>View</u>	Data Map						
				lmage 4-1	1-1: Apps > Mod	bus				
										Ctotut

Désactiver ou activer le service Modbus sur le BulletPlus.

0

Valeurs

service Désactiver Activer le service

TCP Mode Statut

Désactiver ou activer la fonction de connexion Modbus TCP sur les BulletPlus.

Valeurs

Désactiver Activer



	Port		
Spécifiez le port dans lequel le service Modbus TCP est d'écouter et	Valeurs		
repondre aux sondages.	502		
	Active Timeout(s)		
Définir le délai d'attente actif en quelques secondes			
	Valeurs		
	30		
	Slave ID		
Chaque dispositif esclave Modbus doit avoir une adresse unique, ou l'ID de	Valeurs		
l'esclave. Entrez cette valeur ici comme requis par le système hote Modbus.	1		
	Coile Address Offect		
	Colls Address Offset		
Entrez le décalage tel que requis par le Maître Adresse Bobines.	Valeurs		
	0		
	Input Address Offset		
Entrez le décalage tel que requis par le maître Adresse d'entrée.	Valeurs		
	0		
Red	gister Address Offset		
Entrez le décalage tel que requis par le maître Adresse d'entrée.	Valeurs		
	U		
	Master IP Filter Set		
Il est possible d'accepter uniquement les connexions à partir Modbus	Valeurs		
maître et de spécifier les adresses IP dans les champs prévus.	Désactiver / Activer		



4.11.1.2 Modbus > COM (Série) Modbus

Le BulletPlus peut également participer à la série en fonction Modbus, pour configurer et afficher les paramètres Modbus série, le port COM1 doit d'abord être désactivé dans le menu Comport> Paramètres. Seuls les paramètres qui sont différentes de Modbus TCP seront discutés.

COM Mode Status	Enable COM ASCII	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 4-11-2: Apps > Modbus Configuration série

COM Mode Statut

Bauds

Désactiver pour sélectionner le mode de série (COM) pour le service Modbus. En mode RTU, la communication est au format binaire et en mode ASCII, la communication est au format ASCII.

Valeurs

Désactiver Activer le mode ASCII COM Activer le mode COM RTU

La vitesse de transmission de série est la vitesse à laquelle le	Valeurs	(bps)
connecté.	921600	57600

	- (/			
921600 460800 230400 115200	57600 38400 28800 19200	14400 9600 7200 4800	3600 2400 1200 600	
110200	10200	1000	000	

	Format de données
Ce paramètre détermine le format des données sur le port série.	Valeurs
La valeur par defaut est de 6 bits de données, pas de partie et 1 bit d'arret.	8N1 / 8E1 / 8O1



4.10.1.3	Modbus	>	Modbus	Data	Мар
----------	--------	---	--------	------	-----

Modbus Dat	ta Map		Registers:		
Supported I	Function Codes:		16 Bits Address	Hex Format	Definition
2Read Inp	uts		0	0x0000	Modem Model Type
3Read Rec	aisters		1	0x0001	Build Version
5Write Sin	gle Coil		2	0x0002	Modem ID Highest 2 Bytes
6Write Sin	gle Register		3	0x0003	Modem ID Higher 2 Bytes
Data Addres	s = Offset + Basic	Address	4	0x0004	Modem ID Lower 2 Bytes
Coil Bits (O	utput(if config) a	and Internal Status):	5	0x0005	Modem ID Lowest 2 Bytes
Bit Address	Hex Format	Definition	6	0x0006	RSSI(dbm)
0	0x0000	OUTPUT 1	7	0x0007	VDC(x100)(V)
1	0x0001	OUTPUT 2	8	0x0008	Core Temperature(C)
9	0x0009	Serial Status	9	0x0009	Carrier Received Bytes(MB)
12	0x000c	LAN/eth0 Status(Read)	10	0x000a	Carrier Transmitted Bytes(MB)
13	0x000d	WAN/eth1 Status(Read)	11	0x000b	GPS Altitude(m)
16	0x0010	Carrier Status	12	0x000c	GPS Latitude High 2 Bytes
18	0x0012	Wifi Status	13	0x000d	Latitude Low 2 Bytes(x1000000)
22	0x0016	GPS Status	14	0x000e	GPS Longitude High 2 Bytes
23	0x0017	Location Over Network	15	0x000f	Longitude Low 2 Bytes(x1000000)
24	0x0018	Event UDP Report 1	18	0x0012	Serial Baud Rate(/100)(bps)
25	0x0019	Event UDP Report 2	19	0x0013	Serial Data Format
26	0x001a	Event UDP Report 3	Caculation:	Real Latitude = (si	gned integer)[High 2 Bytes + Low 2 Bytes] / 1
27	0x001b	NMS Report	Modem Mo	odel Types:	
28	0x001c	Web Client Service	Type ID	Definition	
32	0x0020	Carrier Connection(Read)	0	Unknow	
40	0x0028	SYSTEM Reboot	6	IPn3G	
			7	VIP4G	
Input Bits:(i	f config)		8	IPn4G	
Bit Address	Hex Format	Definition	9	IPn3Gii	
0	0x0000	INPUT 1	10	IPn4Gii	
1	0x0001	INPUT 2	11	PWii/BulletPlus	
1					

com bata	ormat Demitto
Type ID	Definition
0	Unknow
1	8N1
2	8N2
3	8E1
4	801
5	7N1
6	7N2
7	7E1
8	701
9	7E2
10	702

Image 4-11-3: Apps > Modbus Data Map



4.11.2 Apps > Rapport Netflow

Les BulletPlus peut être configuré pour envoyer des Netflow relève jusqu'à 3 systèmes distants. Netflow est un outil qui collecte et rapporte des informations sur le trafic IP, permettant à un utilisateur d'analyser le trafic réseau sur une base par interface aux problèmes de bande passante d'identité et de comprendre les besoins de données. Filtres Netflow standard peuvent être appliquées pour affiner la recherche et de cibler les besoins de données spécifiques.

System I	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Modbus N	letflow Re	port Lo	calMonitor	Event Rep	oort V	Nebsocke	t					
Netflow Re	Netflow Report											
Report Cor	Report Configuration No.1											
Status	Status Enable 🔻											
Source	e Address		0.0.0	.0	Default 0.0.0.0							
Interfa	Interface		ALL	ALL 🔻								
Remo	te IP		0.0.0	0.0.0.0								
Remo	te Port		2055	2055		[0 ~ 65535]						
Filter	expression]						
Versio	on		V5	∨5 ▼								
Report Cor	nfiguration N	o.2										
Status	Status			Disable V								
Report Cor	Report Configuration No.3											
Status	Status			ble 🔻								

Image 4-11-4: Apps > Rapport Netflow

	Status		
Activer / Désactiver Netflow Reporting.	Valeurs		
	Désactiver / Activer		
	Source Address		
La Source Adresse est l'adresse IP, dont les données doivent être	Valeurs		
communiquer des informations sur toutes les adresses connectés à l'interface sélectionnée ci-dessous.	0.0.0.0		
	Interface		
Sélectionnez entre LAN, WAN et transporteurs interfaces, ou des données	Valeurs		
de capture de toutes les internaces.	LAN / WAN / Carrier / Al I		



	IP à distance		
La distance IP est l'adresse IP du collecteur NetFlow où les rapports de flux sont envoyées.	Valeurs		
	0.0.0.0		
	Port à distance		
Entrez le numéro de port à distance.	Valeurs		
	0		
	Expression de filtre		
Expression de filtre sélectionne les paquets qui seront capturés. Si aucune	Valeurs		
paquets dont l'expression est `vrai 'sera capturé. Exemple: tcp&&port 80	(Pas par défaut)		

Le manuel "tcpdump", disponible sur Internet fournit une syntaxe d'expression détaillée.



4.11.3 Apps > Moniteur local

Le Moniteur de périphérique local permet aux BulletPlus pour surveiller un dispositif local connecté localement au port Ethernet ou le réseau connecté localement. Si le BulletPlus ne peut pas détecter l'IP spécifiée ou DHCP attribué IP, l'unité va redémarrer le service DHCP, et éventuellement redémarrer le modem pour tenter de rétablir la connexion.

Local Device Monitor							
Enable Local Device Monitor 🔻							
[5~65535](s)							
[30~65535](s)							

Image 4-11-5: Apps > Moniteur local

	Statu		
Activer ou désactiver le service de surveillance de périphérique local.	Valeurs		
	Désactiver / Activer		
	IP Mod		
Sélectionnez le mode IP. En sélectionnant une adresse IP fixe, le service	Valeurs		
automatique est sélectionné, le BulletPlus va détecter et surveiller DHCP adresse IP attribuée.	Fixed IP locale Détection automatique IP		
Lo	cale IP Configuratio		
Ce champ est affiché uniquement si IP fixe local est sélectionné pour le	Valeurs		
mode IP. Entrez le adresse IP statique à surveiller dans ce domaine.	0.0.0.0		
	Statut Timeou		
Le délai d'attente d'état est le temps maximum que le BulletPlus attendra	Valeurs		
pour détecter le dispositif surveillé. A ce moment le BulletPlus va redémarrer le service DHCP. (5-65535 secondes)	10		
Α	ttente DHCP Timeou		
Ce champ définit la quantité de temps le BulletPlus attendra pour détecter	Valeurs		
la diapasitif curveillé quant qu'il radémarra la madam (20,65525 accorder)			



4.11.4 Applications > Rapport d'événement

4.11.4.1 Rapport d'événement> Configuration

Rapports de l'événement permet aux BulletPlus d'envoyer des mises à jour périodiques via des paquets UDP. Ces paquets sont personnalisables et peuvent être envoyés à jusqu'à 3 hôtes différents, et à un intervalle programmable. Le paquet d'événement peut communiquer des informations sur le modem comme les versions matérielles / logicielles, la température centrale, tension d'alimentation, etc; info support tel que la force du signal (RSSI), numéro de téléphone, RF Band; ou sur le WAN, comme si les changements d'adresse IP attribuées. Tous les événements sont rapportés en binaire.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	1/0	GPS	Apps	Diag	Admin	
Modbus	Netflow Re	eport Lo	calMonitor	Event Re	port \	Nebsocke	t						
Event Re	Event Report												
Report (Configuration N	10.1											
Even	Event Type		Mod	em_Event 🔻]								
Ren	note IP		0.0.0	.0		0.0.0.0							
Ren	note PORT		2020	0		[0 ~ 65535]							
Inte	erval Time(s)		600			[0 ~ 65535]							
Inte	erface Selection	n											
M	odem:		Dis	sable 🔍 Enab	le								
Ca	arrier:		Dis	sable 🔍 Enab	le								
W	AN:		Dis	sable 🔍 Enab	le								
Report (Configuration N	10.2											
Even	nt Type		SDP	_Event •]								
Ren	note IP		0.0.0	.0		0.0.0.0							
Ren	note PORT		2020	20200 [0 ~ 65535]									
Inte	erval Time(s)		600			[0 ~ 65535]							
Report (Configuration N	10.3											
Even	nt Type		Man	agement 🔻]								
Ren	Remote IP		0.0.0	.0		0.0.0.0							
Ren	Remote PORT		2020	0		[0 ~ 65535]							
Interval Time(s)		600			[0 ~ 65535]								
Interface Selection													
Eth	Ethernet:		Dis	Disable Enable E									
Carrier:		O Dis	O Disable Enable										
Radio:		Dis	Isable Disable Disable										
Com:		Dis	sable 🔍 Enab	le									

Image 4-11-6: Apps > Rapport d'événement

Type d'événement

Valeurs

Cette boîte permet de sélectionner le type d'événement à signaler. La valeur par défaut est désactivé. Si Modem_event est sélectionné, des options supplémentaires apparaissent à droite et permettent la personnalisation de l'événement rapporté par l'intermédiaire de messages. Si la gestion est sélectionnée, les cases à cocher supplémentaires apparaissent ci-dessous pour sélectionner les interfaces pour signaler au système Microhard NMS.

Modem événement SDP Event La gestion

	IP à dista
Entrez l'adresse IP d'un hôte accessible pour envoyer les paquets UDP.	Valeurs

0.0.0.0

nce



	Port à distance
Indiquez le numéro de port UDP de l'adresse IP distante.	Valeurs
* Numéros de port par défaut pour Microhard NMS (20100 pour les événements de modem, 20200 pour la gestion)	20200
	Intervalle Times
Ceci est l'intervalle de temps en secondes, que les BulletPlus enverra le	Valeurs
message ODF configure pour HF à distance et le poir specifie.	600
	Message Info Type
Quand Modem_Event est sélectionné, jusqu'à trois charges utiles	Valeurs
	Modem Carrier WAN

4.11.4.2 Rapport d'événement > Message Structure

Modem_event structure de message

- Tête fixe (taille fixe 20 octets)
- Modem ID (uint64_t (8 octets))
- Message de masque de type (uint8_t (1 octet))
- réservé
- Longueur de paquet (uint16_t (2 octets))

Remarque: la longueur du paquet = longueur de tête fixe + longueur de charge utile du message.

Message type mask

Modem info -	2 bits
	00 non
	01 oui (0x1)
Carrier info -	2 bits
	00 non
	01 oui (0x4)
WAN Info -	2 bits
	00 non
	01 oui (0x10)

sdp_event structure de message

- spd_cmd (1 byte(0x01))
- longueur contenu (1 byte)
- spd_package même que le format de paquet de demande de réponse spd



4.11.4.3 Event Report > Message Payload

Modem info:

Longueur du contenu	-	2 BYTES (UINT16_T)
Nom du modem	-	STRING (1-30 bytes)
Version du matériel	-	STRING (1-30 bytes)
Une version de logiciel	-	STRING (1-30 bytes)
La température centrale	-	STRING (1-30 bytes)
Tension d'alimentation	-	STRING (1-30 bytes)
Adresse IP locale	-	4 BYTES (UINT32_T)
Masque IP locale	-	4 BYTES (UINT32_T)

Carrier info:

Longueur du contenu	-	2 BYTES (UINT16 T)
RSŠI	-	1 BYTE (ÙINT8_T)
RF Band	-	2 BYTES (UINT16_T)
3G_Network	-	STRING (1-30 Bytes)
Type de service	-	STRING (1-30 Bytes)
Le numéro de canal	-	STRING (1-30 Bytes)
Numéro de carte SIM	-	STRING (1-30 Bytes)
Numéro de téléphone	-	STRING (1-30 Bytes)

WAN Info:

Longueur du contenu	-	2 BYTES (UINT16_T)
Adresse IP	-	4 BYTES (UINT32_T)
DNS1	-	4 BYTES (UINT32_T)
DNS2	-	4 BYTES (UINT32_T)

Message Demande:

Les messages seront classés par numéro de type de message.

Par exemple,

Si le type de message masque = 0x15, le package EURD sera équipé de la tête + modem informations + informations de support + wanip d'information.

Si le type de message masque = 0x4, le package EURD sera équipé de la tête + support d'informations.

Si le type de message masque = 0x11, le package EURD sera équipé de la tête + modem infomation + wanip infomation.

```
un message queue fixe
longueur du contenu --- 2 BYTES (uint16_t)
nom du produit --- STRING (1-64 octets)
nom de l'image --- STRING (1-64 octets)
nom de domaine --- STRING (1-64 octets)
domaine mot de passe --- STRING (32 octets) // cryptage MD5
liste des modules --- 5 BYTES // radio, ethernet, transporteur, usb, com
```



4.11.5 Applications > Websocket

Le service de Websocket est une caractéristique de HTML5.0 ou plus tard. Socket Web est conçu pour être mis en œuvre dans les navigateurs Web et les serveurs Web pour permettre aux scripts XML d'accéder au service Web HTML avec une connexion de socket TCP.

Il est principalement utilisé pour deux raisons:

- Informations de rafraîchissement de la page sans rafraîchir la page entière pour réduire flux réseau.
- Pour intégrer des applications Internet avec xml pour obtenir des informations requises en temps réel.

Actuellement, nous fournissons quatre types d'informations selon la configuration:

- Coordonner GPS Informations
- GPS NMEA données
- · Renseignements sur le transporteur
- Comport données

Syste	m Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Modb	us Netflow R	Report L	ocalMonitor	Event Re	port	Websocke	t						
Web	Socket Service												
Onl	ne Connected Dat	a											
E	rowser Type: C	hrome 46 W	/indows										
Sett	ing												
9	tatus		Ena	ble Web Sock	et Serv	ice 🔻							
	Web Socket Port	(default:768	1) 7681			[100-65535]						
	Data Fresh Inter	al(seconds)	10			[2-65535]							
	Connect Passwo	rd				(Blank for D	isable)						
	Max Keep Time(minutes)	60			(0:keep alive	e)						
	GPS Coordinate		Di	sable 🔍 Enab	le								
	GPS NMEA Data		Di	sable 🔍 Enab	le								
	Carrier Informat	on	Di	sable 🔍 Enab	le								
	Comport Data		Di	sabled (Please	e enable	e comport top	o server.)						

Image 4-11-7: Applications > Service Websocket

	Statut
Activer ou désactiver le service websocket dans le modem.	Valeurs
	Activer / Désactiver
	Web Socket Port
Entrez le socket web numéro de port TCP souhaité. La valeur par défaut	Valeurs
est 7001, et la plage value est 100-00000.	7681



Intervalle	es données Actualise					
Entrez dans l'heure à laquelle les données doivent être actualisées. La valeur par défaut est de 10 secondes, la plage valide est de 2 à 65535 secondes.	Valeurs 10					
Se connecter Mot de pas						
Pour plus de sécurité un mot de passe peut être nécessaire pour se connecter au service de prise Web. Pour désactiver, laisser ce champ vide. La valeur par défaut est désactivé.	Valeurs (non)					
	Max Keep Tim					
Ce champ détermine la durée de la prise de web est ouvert une fois	Valeurs					
zéro signifie que le service de continuer à fonctionner indéfiniment.	60					
	Coordonner GP					
Si elle est activée, le modem rapport GPS données de coordonnées à	Valeurs					
	Désactiver / Activer					
	GPS NMEA donnée					
Si elle est activée, le modem rapport des données NMEA GPS au	Valeurs					
websockel.	Désactiver / Activer					
Renseignemer	nts sur le transporte					
Si elle est activée, le modem rapport des informations de support à	Valeurs					
I WEDSOCKEL	Désactiver / Activer					
	Comport donnée					
Si elle est activée, et le port RS232 est configuré pour TCP Server, les	Valeurs					
données de Compon seront communiques à la prise web.	Désactiver / Activer					


4.12 Diag

4.12.1 Outils de réseau Ping

La fonctionnalité Outils de réseau Ping fournit un outil pour tester la connectivité réseau à partir de l'unité. Un utilisateur peut utiliser la commande Ping en entrant l'adresse IP ou le nom d'hôte d'un dispositif de destination dans le champ Nom d'hôte Ping, utilisez le comte pour le nombre de messages de ping à envoyer, et la taille des paquets pour modifier la taille des paquets envoyés.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Ping Tr	aceroute I	perf											
Network	k Tools												
Ping													
Ping	Host Name		www	.google.com									
Ping	Count		4			(0 = contin	uous)						
Ping	Size		56										
			Star	t Stop Clea	ar								
Please PTMG www	wait for out;	out of "pin (184 150 1	ng -c 4 -s 56	www.google.	.com"								
17:01:3	35.274455 9	sending icm	ip request	aaca byees									
64 byte	es from 184.19	50.182.162:	seq=0 ttl=5	2 time=59.50	57 ms								
17:01:3	36.275146 9	sending icm	np request										
64 byte	es from 184.15	50.182.162:	seq=1 ttl=5	2 time=58.49	95 ms								
1/:01::	37.275895 9	sending icm	p request	2 +ima-07 0	00 mc								
17:01:3	38.276516 9	sending icm	n request	2 CINC-57.02	20 115								
64 byte	es from 184.15	50.182.162:	seq=3 ttl=5	2 time=57.12	25 ms								
www	v.google.com u	oing statis	tics										
A packs	te topoemitte	d 4 packs	to possived	0% packet	locc								

Image 4-12-1: Diag > Ping

4.12.2 Outils de réseau Traceroute

La fonction Traceroute peut être utilisé pour fournir des données de connectivité en fournissant des informations sur le nombre de sauts, les routeurs et le chemin pris pour atteindre une destination particulière.

Syste	m Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin
Ping	Traceroute I	iperf										
Netw	ork Tools											
Trac	eroute											
Т	raceroute Host Na	ame	www Star	.google.com t Stop Clea	r							
Begi	n traceroute te eroute to www.go	st at oogle.com (184.150.182.	148), 30 hop	s max.	38 byte pa	ckets					
1 2	172.25.16.188 (172.25.16.181 (172.25.16.1 172.25.16.1	88) 44.836 81) 29.466	ms 25.650 m ms 34.896 m	ns 41.5 ns 39.7	65 ms '90 ms						
3	172.25.21.10 (1 172.25.20.14 (1	72.25.21.10	 39.559 ms 41.093 ms 	37.380 ms 33.617 ms	30.009	ms						
6	1/2.25.16.2 (1/. 204.101.4.153 ()	2.25.16.2) 204.101.4.1 a bundle-et	48.142 ms 153) 39.673 m ther5 net bel	38.288 ms 3 ms 35.513 m 1 ca (64.230	9.545 m 15 123. 118 14	15 796 ms 10) 49 282	ms 51 2	32 ms	39 705	nc		
8	tcore4-calgary6	8_tengige0- pos11-1-0.	0-0-9.net.be	11.ca (64.23 (64.230.77.2	0.77.13 0.77.3	4) 59.447 .743 ms 5	ms core4	4-calga 39.330	ry68_ge	5-1-0.net	.bell.ca	a (64.230.77.2
1			/ <i>CA</i>	220 122 220		40 I	- 4	450	-			

Image 4-12-2: Diag > Traceroute



4.12.3 lperf

Le BulletPlus dispose d'un Iperf serveur / client intégré à utiliser pour mesurer et analyser le débit de paquets TCP / UDP et / ou des BulletPlus. Iperf est un utilitaire 3ème partie qui peut être chargé sur un PC pour mesurer les performances du réseau. Pour plus d'informations sur Iperf, s'il vous plaît visitez le site Web Iperf.

Les BulletPlus peut être configuré pour fonctionner comme un serveur, à l'écoute pour une connexion entrante d'un autre appareil (avec Iperf), ou un PC exécutant un client Iperf. Si la valeur client Iperf, l'BulletPlus va se connecter ou envoyer des paquets à un serveur Iperf spécifié.

Systen	n Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Ping 1	raceroute I	perf											
Throu	ghput Testing												
lperf	Configuration												
Ip Se Pr TC S	erf Mode rver Status otocol 2P Window Size 2P Maximum Segr ave Server Setting	ment Size	Serv En TCP 128K 0	er ▼ able ⊛ Disab ▼	le	(0 for defau (0 for defau	lt 85.3KBy lt)	rte)					
lperf	Configuration												
lp Pr Rv D Tr Rv Rv Rv	verf Mode rotocol emote Server IP A uration(seconds) CP Window Size CP Maximum Seg eport Format Save & Run Test]	ddress ment Size	Clie TCF 192. 5 1281 0 Mbi	nt v v v 168.168.100 (ts v]] (0 for defai] (0 for defai	ılt 85.3KB ılt)	yte)					

Image 4-12-3: Diag > Iperf

	Iperf Mode
Sélectionnez entre un serveur lperf (écoute pour les connexions entrantes)	Valeurs
et le client (etablit une connexion avec un serveur)	Serveur / Client
	Serveur Status
Si le mode Iperf pour régler sur le serveur, ce serveur Statut permet à un	Valeurs
utilisateur u activer ou desactiver le serveur.	Activer / Désactiver
	Protocol
SelSélectionner le type de paquets à envoyer à tester le débit. les paquets	Valeurs
pour le handshaking qui se produit, alors que UDP est un, le meilleur effort de protocole orienté.	TCP / UDP



	TCP Window Size
Définissez la taille de la fenêtre TCP pour le Iperf Client / Serveur. La	Valeurs
0.	0
ТСР Ма	ximum Segment Size
Définissez la taille TCP Max Segment pour le Iperf Client / Serveur. Mettre	Valeurs
a o pour les parametres recommandes.	0
Se	rveur distant Adresse
En mode client, sélectionnez le serveur Iperf en saisissant son adresse IP	Valeurs
	192.168.168.100
	Durée
En mode client, sélectionnez la durée de l'essai (en secondes). La valeur	Valeurs
par defaut est 5.	5
	Format du rapport
Sélectionnez le format pour afficher les numéros de bande passante dans les formats pris en charge sont les suivants:	Valeurs
'Kbits' = Kbits/sec 'Kbytes' = KBytes/sec 'Mbits' = Mbits/sec 'M'bytes = MBytes/sec	Kbits Mbits Kbytes Mbytes



4.13 Admin

4.13.1 Admin > Utilisateurs

Changement de mot de passe

Le menu changer le mot de passe permet le mot de passe de l'utilisateur 'admin' à modifier. Le nom d'utilisateur 'admin' ne peut pas être supprimé, mais les utilisateurs supplémentaires peuvent être définis et supprimé comme requis comme on le voit dans le menu Utilisateurs ci-dessous.

System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Users /	Authenticati	on NMS	SNMP Di	scovery L	ogout								
Access	Control												
Passwo	rd Change (It wi	ll take effect	immediately af	ter press "chai	nge passv	vd" button)							
Use	r Name : admin	I											
New	v Password :					(min 5 char	acters)						
Con	firm Password:					Change Pa	sswd						
Add Us	er (It will take ef	fect immedia	ately after press	"Add User" bi	utton)								
User	rname :					(5-32 chara	cters)						
Pass	sword					(5-32 chara	cters)						
Con	firm Password												
Use	r Type 🕕		Enc	d Customer O	nly								
Syst	tem		Hide	Submenu 🔹									
Net	work		Hide	Submenu 🔹									
Carr	rier		Hide	Submenu 🔹									
Wire	eless		Hide	Submenu 🔹									
Fire	wall		Hide	Submenu 🔹									
VPN	I		Hide	Submenu 🔹									
Rou	ter		Hide	Submenu 🔹									
Seri	al		Hide	Submenu 🔹									
I/O			Hide	Submenu 🔹									
GPS			Hide	Submenu 🔹									
App	S		Hide	Submenu 🔹									
Diag	9		Hide	Submenu 🔹									
Adn	nin		Hide	Submenu 🔹									
Add	User		Add	User									
Users S	ummary												
Nou	users defined.												

Image 4-13-1: Utilisateurs > Mot de passe Changer

	Nouveau mot de passe
Entrez un nouveau mot de passe pour l'utilisateur 'admin'. Il doit être	Valeurs
'admin'.	admin
Col	nfirmez le mot de passe
Le mot de passe exact doit être entré pour confirmer le changement	Valeurs
rejetées.	admin



Ajouter des utilisateurs

Différents utilisateurs peuvent être configurés avec un accès personnalisé à l'interface utilisateur Web. Chaque menu ou onglet de l'interface utilisateur Web peuvent être désactivés sur une base par utilisateur comme on le voit ci-dessous.

d User (It will take effect imme	diately after press "Add User" button)	System	Show Submenu V
		Settings	Disable •
Username :		(5-3 Services	Disable V
Password		(5) Maintenance	Disable •
rassworu		Reboot	Disable 🔻
Confirm Password		Network	Show Submenu 🔻
User Type 🕕	End Customer Only	Status	Disable 🔻
Svetem	Hido Submonu -	LAN	Disable V
system	Hide Submenu +	DDNS	Disable V
Network	Hide Submenu 🔻	Routes	Disable V
Carrier	Hide Submenu 🔻	Ports	Disable 🔻
Miroloso	Llide Submenu -	DeviceList	Disable 🔻
wireless	Hide Submenu 🔻	Carrier	Show Submenu 🔻
Firewall	Hide Submenu 🔻	Status	Disable V
VPN	Hide Submenu 🔻	SMS	Disable V
Router	Llido Submonu -	SMSConfig	Disable 🔻
Kouter	Hide Submenu 🔻	DataUsage	Disable 🔻
Serial	Hide Submenu 🔻	Wireless	Show Submenu 🔻
/0	Hide Submenu 🔻	Status	Disable V
CRE	Hido Submonu -	HotSpot	Disable V
5	Hide Submenu 🔻	Firewall	Show Submenu
Apps	Hide Submenu 🔻	Summary	Disable 🔻
Diag	Hide Submenu 🔻	General	Disable 🔻
Admin	Hide Submenu	PortForwarding	Disable V
Admin	Hide Submenu V	Rules	Disable V
Add User	Add User	FirewallDefault	Disable •
		VPN	Hide Submenu 🔻
		Router	Hide Submenu 🔻
		Serial	Hide Submenu 🔻
		1/0	Hide Submenu V
		Anns	Hide Submenu
		Diag	Hide Submenu
		Admin	Hide Submenu
		Add User	Add User

Image 4-13-2: Contrôle d'accès> Utilisateurs

Nom d'utilisateur

Entrez le nom d'utilisateur souhaité. caractère et un maximum de 32 caractères minimum ou 5. Les modifications ne prendront effet que

(Pas par défaut) Min 5 caractères Max 32 caractères

Mot de passe Confirmer mot de passe

Les mots de passe doivent être un minimum de 5 caractères. Le mot de passe doit être ré-entré exactement dans la zone Confirmer le mot de passe ainsi.

lorsque le système a été redémarré.

Valeurs

(Pas par défaut) min 5 caractères

Type d'utilisateur

Les utilisateurs peuvent être spécifiés comme un «utilisateur final», dans ce cas, seul un accès limité au modem (résumé et wifi SSID / mot de passe).

Valeurs

incontrôlé



4.13.2 Admin > Authentification

Il existe deux méthodes par lesquelles un utilisateur peut être authentifié pour accéder aux BulletPlus:

Locale •

> Utilisation de l'administration ou la mise à niveau d'accès et mots de passe associés l'authentification est effectuée «localement» dans le BulletPlus et

RADIUS&Locale .

> L'authentification RADIUS (en utilisant un nom d'utilisateur spécifique et un mot de passe fourni par votre RADIUS Server Administrator) - cette authentification se ferait «à distance» par un serveur RADIUS; si cette authentification échoue, procéder à l'authentification locale comme ci-dessus.

User	System	n Network	Carrier	Wireles	s Firewa	II VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
9	Users	Authenticati	on NMS	SNMP	Discovery	Logout								
vent être	Authe	ntication Conf	iguration											
lications	Au	thentication Serv	/er:	0	Local 💽 Loca	&RADIUS								
	Re	mote Server IP A	ddress	0	.0.0.0									
est	Re	mote Server IP P	ort	1	812		[Default: 18	312]						
ie les rectes.	Sh	ared Secret		n	osecret									

Image 4-13-3: Configuration de l'authentification

Se	rve	ur d'authentification
Sélectionnez le mode d'authentification: Local (par défaut) ou RADIU	IS	Valeurs
tentée FIRST; en cas d'échec, l'authentification locale peut être tentée.		Locale Local&RADIUS
Ser	veu	r distant Adresse
Dans ce domaine, l'adresse IP du serveur RADIUS doit être saisi	si	Valeurs
		RADIUS valide adresse du serveur
		0.0.0.0
		RADIUS Seci
Si le mode d'autorisation a été défini sur RADIUS Local, RADIUS obtenir	le	Valeurs
entrez dans ce champ.	CL	nosecret



Authentication Dial Ir Service. Un protocole d'authentification, d'autorisation et de comptabilité qui peuv utilisés dans des app d'accès au réseau.

Un serveur RADIUS utilisé pour vérifier qu informations sont co

on

Ρ



4.13.3 Admin > NMS Paramètres

Le Microhard NMS est un service de surveillance et de gestion de serveur basé sans frais offert par Microhard Systems Inc. Utilisation de NMS vous pouvez contrôler en ligne / unités hors ligne, récupérer des données d'utilisation, effectuer des sauvegardes et des mises à niveau centralisées, etc. La section suivante décrit comment démarrer avec NMS et comment configurer le BulletPlus de faire rapport au NMS.

Pour commencer avec NMS, accédez au site Microhard NMS, nms.microhardcorp.com, cliquez sur le bouton d'enregistrement dans le coin supérieur droit d'enregistrer pour un domaine (profil), et mettre en place un compte administrateur de domaine.

Microhard NMS ×	the in The state in the local division of th	And Description of Concession, Name
- C A Microbard Systems	Inc. [CA] https://pms.microhardcorp.com/MicrohardNMS	login seam2cid=2:5
	inc. [CA] https://infis.micronardcorp.com/inicronardivide	
Apps 🌌 microhardcorp.com 🌌 Microhard	I Dev Site 🏼 Microhard Support 💼 OET FCC ID Search 📄 Webn	nail LOGIN 🛛 🔐 MantisBT
rohard NMS:		Register Log
6		
111		
microhard system	SINC	
inter a biolem	Levie L	
	Login	
	Email Address:	
	Password:	
	Forgot your password?	
	Login	
	© Copyright Microhard	Systems Inc. 2014. All Rights Reserve
Microhard NMS ×	the in a monorhand of the other and the	
	really the interview of the base	
→ C f Microhard Systems	Inc. [CA] https://nms.microhardcorp.com/MicrohardNMS	/registration.sea Q 53
Apps 🌌 microhardcorp.com 🌌 Microhard	I Dev Site 🏼 Microhard Support 📾 OET FCC ID Search 📄 Webn	nail LOGIN 🔗 MantisBT
rohard NMS:		Register Lo
rohard NMS:		Register Lo
rohard NMS: gister for Domain and Domain Administrator Account		Register Lo
rohard NMS: gister for Domain and Domain Administrator Accour Domain	a a a a a a a a a a a a a a a a a a a	Register Lo
rohard HMS: gister for Domain and Domain Administrator Accour Domain	at	Register Lo
rohard NMS: gister for Domain and Domain Administrator Accour Domain Choose your domain name *	nt	Register Lo
rohard NN S: gister for Domain and Domain Administrator Accoun Domain Choose your domain name *	at	Register Lo • The Domain Name and Domain Password will be the
rohard NMS: gister for Domain and Domain Administrator Accour Domain Choose your domain name * Create a password for your domain *	N	Register Lo • The Domain Name and Domain Password will be the ordenaia used in the moders's
rohard NMS: gister for Domain Administrator Accour Domain Choose your domain name* Create a password for your domain* Confirm your domain password*	A	Register Lo • The Domain Name and Domain Password will be the own of the second second second second MAS configuration • The Domain Name should
rohard NMS: gister for Domain and Domain Administrator Accour Domain Choose your domain name " Create a password for your domain" Confirm your domain password" Please enter for mane of your organization "		Register Lo • The Domain Hame and Domain Password will be the ordential used in the moderni NIS configuration. • The Domain Hame should represent your
robard NMS: gister for Domain and Domain Administrator Accour Domain Choose your domain name* Create a password for your domain* Contimy your domain password* Please enter the name of your organization*		Register Lo The Domain Hame and Domain Password will be the orderatil used the modern NMS configuration. Tha Domain These mould present your accordingly, for seample
rohard NM 5: gister for Domain and Domain Administrator Accour Domain Choose your domain name* Create a password for your domain* Contim your domain password* Please enter the adres of your organization* Please enter the addres of your organization*	N	Register Lo Register Lo The Domain Name and Domain Password will be the ordertrail use in the modern's NMS configuration the second se
robard NM 5: gister for Domain and Domain Administrator Accour Domain Choose your domain name * Create a password for your domain * Contim your domain password* Please enter the name of your organization* Please enter the address of your organization* Please enter the phone number of your organization*	N	Register Lo
rohard NM 5: gister for Domain and Domain Administrator Accound Domain Choose your domain name * Create a password for your domain* Confirm your domain password* Please enter the name of your organization* Please enter the address of your organization* Please enter the phone number of your organization*	Nt	Register Le - The Domain Name and Domain Password will be the Domain Password will be the State of the State of the Net Comparison State of the State of the comparison of the State of the state of the State of the Comparison of the State of the Domain Name State of the State of the Domain Name State of the State o
rohard NM 5: gister for Domain and Domain Administrator Accour Domain Choose your domain name * Create a password for your domain* Confirm your domain password* Please enter hane of your organization* Please enter the address of your organization* Please enter the phone number of your organization	N	The Domain Hame and Domain Password will be the neederalia used in the moderation and the program of the second second represent your operated on the second second second second accessing in fore moderation and accessing in the second second second accessing in the second second second second second accessing in the second second second second second accessing in the second second second second second second second accessing in the second second second second second second second second accessing in the second second second second second second second second accessing in the second secon
robard NMS: gister for Domain and Domain Administrator Accour Domain Choose your domain name* Create a password for your domain* Contimy your domain password* Please enter the name of your organization* Please enter the phone number of your organization*	x	Register Le The Domain Name and Domain Password will be the orderarial used in the modern NMS configuration. The Domain Takes mould proceeding of the modern Modern
robard NM 5: gister for Domain and Domain Administrator Accour Domain Choose your domain name * Create a password for your domain* Confirm your domain password* Please enter mane of your organization* Please enter the address of your organization* Please enter the phone number of your organizati	N N	Register 2 Register 2 Register 2 The Domain Rame and Domain Password will be the orderating used in them domain The Domain Rame should represent your orgenization depending on teol In a recommended has the Dynamic depending on teol In a recommended has the Dynamic depending on teol Somain the addition come on teol Somain teology come, please use typic of the system Domain ten(m)
spister for Domain and Domain Administrator Account Domain Choose your domain name " Create a password for your domain " Confirm your domain password" Please enter the name of your organization" Please enter the phone number of your organization Please enter the phone number of your organization Domain Administrator Account	Nt	Register 2 to Compare the second se
orbard NMS: gister for Domain and Domain Administrator Account Domain Choose your domain name* Create a password for your domain* Confirm your domain password* Please enter the name of your organization* Please enter the dafess of your organization* Please enter the phone number of your organization*	N	Register Lo
orbard NM 5: gister for Domain and Domain Administrator Account Choose your domain name* Create a password for your domain* Confirm your domain password* Please enter the name of your organization* Please enter the address of your organization* Please enter the phone number of your organization* Please enter your first name*	N	Register 2 of The Domain Hame and Domain Password will be the neederalia used in the modern regressing your opanization/department/region acodoraginy (from endi- moderade that the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of body and the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as provide part of the domain the Domain Hame be the same as Domain Hame be the same as provide part of the domain the domain the Domain Hame be the same as Domain Hame be the sam
orbard NM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name* Create a password for your domain* Confirm your domain password* 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 your first name* Please enter your first name*	N	Register Lo
orbard NM 5: gister for Domain and Domain Administrator Account Choose your domain name* Create a password for your domain* Confirm your domain password* 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 first name* Please enter your last name*	N	Register Lo The Domain Hame and Domain Password will be the orderatil action in module represent your orgenization/tagentment/region module(action) The Domain Hame houd represent your orgenization/tagentment/region module(action) the recommendation the pomain Hame Series the pomain Hame
orbard NM 5: gister for Domain and Domain Administrator Accour Domain Choose your domain name* Create a password for your domain* Confirm your domain password* Please enter heame of your organization* Please enter headoress of your organization* Please enter headoress of your organization* Please enter headoress of your organization* Please enter your first name* Please enter your first name* Please enter your first name* Please enter your enail address* (a login and activation username)	Image: Control of the second secon	Register 2 of The Domain Hame and Domain Pasaword will be the oredential used in the modern Not Domain Pasaword will be the oredential used in the modern in the Domain the mould organization the accommode that the Domain Hame be the same as your opposition domain (ag if your email is absolgne con, based on the account of the same be Domain Hame be the same as your opposition domain (ag if your email is absolgne con, based on the account of the same be Domain Hame be the same as your opposition domain (ag if your email is absolgne con, based on the account of the same be the account email is absolgne and based of the same bit organization domain (age) You will be account be two. } You will be account be two. } You will be account be two. } You will be account and the mane and account of the same mane and account domain the mane and account email is account of the same and account of the same account of the same and account of the same account
robard MM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name * Create a password for your domain* Confirm your domain password* 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 first name* Please enter your first name* Please enter your first name* Please enter your first name* (as login and activation username) Create a password*	N	Register 2 to Register 2 to The Domain Hame and Domain Password will be the node crisit access in the solution The Domain Password will be the represent your organization inspectments The Domain Hame should represent your organization inspectments the sector access the
rohard MM 5: gister for Domain and Domain Administrator Accourd Domain Choose your domain name * Create a password for your domain * Confirm your domain password* Please enter her name of your organization * Please enter hen address of your organization * Please enter her phone number of your organization Please enter her phone number of your organization Please enter your first name * Please enter your first name * Please enter your last name *	N	Register 2.0 The Domain Hame and Domain Password will be the orecrisition of the modernial work of the angle in the modernial modernial uses in the modernial modernial uses in the modernial modernial uses the modernial the modernial uses the modernial modernial address of the modernial fame be the same as poir organization domain (leg) the modernial fame be the same as poir organization domain (leg) the modernial fame be the same as poir organization domain (leg) the modernial fame be the same as poir organization domain (leg) the modernial fame be the same as poir organization domain (leg) the modernial is access the NUS. You wide a lead to metange domain You will be able to manage
solved MM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name* Create a password for your domain* Create a password* 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 your first name* Please enter your first name* Please enter your first name* Please enter your entail address* (as legin and activation scoreman) Create a password* Confirm your password*	N	Register Lo The Domain Name and Domain Password will be the orderatio used in the modern NMS configuration. The Domain The should toppic the same should be the moderation of the should population of the should be population of the should be population of the should population of the should be population of the should
rohard MM 5: gister for Domain and Domain Administrator Accourd Domain Choose your domain name * Create a password for your domain * Confirm your domain password * Please enter hanne of your organization * Please enter your first name * Please enter your last name * please enter your	Image: Control of the second	Register 2 to The Domain Hame and Domain Password will be the order-tail used in the modern regressing your orgenization/department/region acouncily (from end) regressing your orgenization/department/region acouncily (from end) regressing your orgenization/department/region acouncil (from end) regressing your orgenization/department/regressing acouncil (from end) regressing your orgenization/department/regressing acouncil (from end) your well be able to manage ure acouncil within the domain You well be able to manage regressing within the domain Songine end) Songine end that has been
rohard MM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name " Create a password for your domain" Contim your domain password" Please enter the name of your organization" Please enter the address of your organization" Please enter the bone number of your organization Please enter the phone number of your organization Please enter your first name " Please enter your first name" Please enter your first name " Please enter your fi		The Domain Name and Domain Password will be the oregorial used in the modern Not Scotting and the second
rohard MM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name * Create a password for your domain* Confirm your domain password* Please enter hean are dryour 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 your first name* Please enter your first name* Confirm your password* Service enail address Your cell phone number		Register 2 to Register 2 to The Domain Rame and Domain Password will be the ordership set in the modership represent your oppriatelon/department/region acobdray, for on molit represent your oppriatelon/department/region acobdray, for one molit the Domain Kame Set the Domain Kame Set the Domain Kame Set the Domain Kame Set the Domain Administrator Acount (email address and possed) of a sodium present your Domain Administrator Acount (email address and possed) of a sodium possed) The Domain Administrator Acount (email address and possed) of a sodium possed) The Domain Administrator Acount (email address and possed) Sodium Sonium Senium Se
rohard MM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name " Create a password for your domain" Confirm your domain password" 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 your first name " Please enter your first name " Please enter your first name " Please enter your disat name " Please enter your disat name " Please enter your first name " Please enter your disation usersame) Create a password " Service ental address " Your cell phone number	Image: Control of the second	Register 2.0 The Domain Hame and Domain Password will be the oredential use in the modern's Well Bonfiguration The Domain Password will be the oredential use in the modern's well bonfiguration the modern's the software between the modern's moderned by the Domain Name be the same as your operation domain (age if your email is abs@got.com, port and is abs@got.c
rohard MM 5: gister for Domain and Domain Administrator Account Commin Choose your domain name * Create a password for your domain* Confirm your domain password* 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 your first name* Please enter your first name* Please enter your first name* Please enter your first name* Please enter your first name* Confirm your password* Service email address Y Your cell phone number	N	Register 2.4 Register 2.4 The Comain Rame and Domain Password will be the productional cardinal for the second seco
rohard MM 5: gister for Domain and Domain Administrator Accourd Domain Choose your domain name * Create a password for your domain * Confirm your domain password * Please enter har anne of your organization * Please enter har phone number of your organization * Please enter your first name * Please enter your first name * Please enter your last dates * Service email address * Your cell phone number	N N Son*	The Domain Hame and Domain Password will be the orecertail use in the modernix NBD bontguration bontguration in the source of the modernix or the source of the modernix means of the modernix of the modernix of the modernix of the modernix of the modernix present of the source of the Modernix of the modernix of the modernix of the modernix of the modernix of the
rohard MM 5: gister for Domain and Domain Administrator Account Choose your domain name* Create a password for your domain* Create a password for your domain* Create a password* Please enter the adme of your organization* Please enter the admes of your organization* Please enter the phone number of your organization* Please enter your first name* Please enter the characters from the above image Lases the Tomes and forefilmes*	x	Register 2 to Register 2 to The Domain Plasaword will be the the domain Plasaword will be domain the domain Plasaword will be domain them the domain Plasaword will be added by the down will be added by the domain Plasaword will be added by
rohard NM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name * Create a password for your domain* Confirm your domain password* Please enter have of your organization* Please enter mene of your organization* Please enter have address of your organization* Please enter the phone number of your organization* Please enter your first name* Please enter your fi	x 	Register 2.0 The Domain Rame and Domain Password will be the ore-derival used in the modern constant Password will be the ore-derival used in the modern regressrip your oparization/department/region according/, to be and according/, to accord
robard MM 5: gister for Domain and Domain Administrator Account Domain Choose your domain name * Create a password for your domain * Confirm your domain password* 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 enail address * Service enail address * Your cell phone number Please enter first from the above image 1 agree the Terms and Conditions * * required fields	x m m m m m m m m m	The Domain Hame and Domain Password will be the oredential used in the modernic Mills Configuration. The Domain Password will be the oredential used in the modernic modernic set of the set of the oreganization departmenting in modernic departmenting in modernic departmenting in modernic departmenting in modernic departmenting in modernic departmenting in modernic departmenting in the Second modernic department of if your email is absolged com- port opporting the sport opporting in the Second Mills and the Domain Name is your Domain Name in the sport opporting in the sport opporting opporting in the sport opporting opporting in the sport opporting opporting in the sport opporting in the devices that has been registered the domains of modernic department opporting in the used for receiving alerts and/op password recovery.

Image 4-13-4: NMS



Nom de domaine: Une zone de gestion logique pour les appareils 3G ou 4G fera rapport sur NMS, les données enregistrées est séparé de tous les autres utilisateurs qui utilisent NMS. Le nom de domaine est nécessaire dans chaque appareil 3G ou 4G pour elle de faire rapport à la zone droite. Sous ce nom de domaine de l'utilisateur, on peut créer et gérer des sous-domaine. Le sous-domaine ne peut être créé par l'administrateur de domaine, pas par la page d'abonnement NMS.

Domaine Mot de passe: Ce mot de passe est utilisé pour prévenir l'utilisation abusive du domaine. Cela doit être entré dans chaque appareil 3G ou 4G pour elle de faire rapport à la zone droite.

Adresse e-mail: L'adresse e-mail indiquée ici sera le login nom d'utilisateur. Pendant la phase d'inscription, un e-mail de confirmation vous sera envoyé par le système NMS pour la vérification et la confirmation pour activer votre compte.

Une fois confirmé, ce compte sera l'administrateur du domaine. L'administrateur peut gérer les sousdomaines et comptes d'utilisateurs qui appartiennent à ce domaine.

Une fois que NMS a été configuré, chaque BulletPlus doit être configuré pour signaler dans NMS.

System Net	twork	Carri	ier	Wirel	ess	Firewa	II VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Users Authe	enticati	ion N	MS	SNMP	Di	scovery	Logout								
NMS Configu	ration														
J															
Default Set	ttings				Edit v	vith defaul	t configura	ation							
System Setting	9														
NMS Serve	r/IP				nms.	microhardc	orp.com	Login NMS							
Domain Na	ame				defau	ult]							
Domain Pa	ssword				•••••	•		Min 5 chara	cters						
Confirm Pa	assword				•••••	•]							
NMS Report Se	etting														
Carrier Lo	cation				Ena	ble Update	Over Netw	/ork ▼							
Report Sta	atus				Enal	ble NMS R	eport 🔻								
Remote P	ORT				2020	0		[0 ~ 65535]	(Default:20	0200)					
Interval T	ïme(s)				300			[0 ~ 65535]							
Informati	on Selec	tion			Avail	able Items:									
Ethernet:					Display	sable 🔍 En	able								
Carrier:					O Di	sable 🖲 En	able								
Radio:					Distant	sable 🔍 En	able								
Com:					Distant	sable 🔍 En	able								
Webclient Sett	ing														
Status					Ena	ble 🔻									
Server Typ	e				HTT	PS V									
Server Port	t				9998]							
User Name	e				admi	n]							
Password					•••••]							
Interval					30			(Minutes)							

Image 4-13-5: NMS Paramètres



Network Management System (NMS) Configuration	
P	aramètres par défaut
Le lien Paramètres par défaut réinitialise le formulaire de configuration aux v forme doit encore être soumis avant toute modification se produira.	valeurs d'usine par défaut. La
	NMS / IP du serveur
L'adresse du serveur par défaut pour NMS est corp.com nms.microhard.	Valeurs
La NMS peut également être néberge en prive, et si tel est le cas, entrez l'adresse ici.	nms.microhardcorp.com
Nom de do	maine / Mot de passe
Ceci est le nom de domaine et mot de passe qui a été enregistré sur le site	Valeurs
NMS, il doit etre salsi pour permettre des rapports au systeme NMS.	défaut
Rapport NMS Cadre	
	Transporteur Lieu
Activer ou désactiver l'emplacement estimation via une connexion	Valeurs
données pour récupérer des informations de localisation de l'Internet.	Désactiver / Activer
	Rapport sur l'état
Activer ou désactiver les rapports UDP de données dans le système NMS.	Valeurs
	Activer le rapport NMS Désactiver Rapport NMS
	Port à distance
Ceci est le port auquel les paquets UDP sont envoyés, et le système NMS	Valeurs
valeur par défaut est 20200.	20200
	Intervalle (s)
L'intervalle définit la fréquence des données est signalé à NMC. Les	Valeurs
devrait être réglé selon le plan de données d'un utilisateur. (0 à 65535 secondes)	300



Sélec	tion de l'information
Les BulletPlus peut rapporter des informations sur les différentes interfaces dont il dispose. Par défaut le BulletPlus est configuré pour envoyer des	Valeurs
informations sur le transporteur, telles que l'utilisation et RSSI. Les données statistiques et d'utilisation sur la radio (WiFi), Ethernet et interfaces série peuvent également être signalés. Plus on a signalé, plus les données envoyées au système NMS, être conscient des contraintes du plan de données et les coûts connexes.	Ethernet Carrier Radio COM DI / DO
Webclient Cadre	
	Statut
Le service Web peut être activée ou désactivée. Ce service est utilisé pour contrôler à distance le BulletPlus. Il peut être utilisé pour programmer les	Valeurs
redémarrages, la mise à niveau du microprogramme et tâches de sauvegarde, etc.	Désactiver / Activer
	Type de serveur
Sélectionnez entre HTTPS (sécurisé), ou le type de serveur HTTP.	Valeurs
	HTTPS/ HTTP
	Port de serveur
Ceci est le port où le service est installé et l'écoute. Ce port doit être ouvert	Valeurs
	9998
Ider	ntifiant Mot de passe
Ceci est le nom d'utilisateur et mot de passe utilisé pour authentifier l'unité.	Valeurs
	admin/admin
	Intervalle
L'intervalle définit la fréquence des contrôles de BulletPlus avec le système	Valeurs
seront consommés chaque fois que le dispositif sonde le système NMS.	60



4.13.4 Admin > SNMP

Les BulletPlus peut être configuré pour fonctionner comme un agent SNMP (Simple Network Management Protocol). La gestion du réseau est le plus important dans les grands réseaux, de manière à être en mesure de gérer les ressources et mesurer la performance. SNMP peut être utilisé de plusieurs manières:

- configurer des périphériques distants
- les performances du réseau de surveillance
- détecter les défauts
- l'utilisation du réseau d'audit
- détecter les échecs d'authentification

Un système de gestion SNMP (un PC exécutant le logiciel de gestion SNMP) est nécessaire pour que ce service fonctionne. Ce système doit avoir un accès complet aux BulletPlus. Communications est sous la forme de requêtes (informations demandées par le système de gestion) ou des pièges (information initiée à, et fourni par l'agent SNMP en réponse à des événements prédéfinis).

Les objets spécifiques aux BulletPlus sont hébergés sous le numéro d'entreprise privée 21703.

Un objet est une variable dans le dispositif et est défini par une base de données d'information de gestion (MIB). À la fois le système de gestion et le dispositif ont une copie de la MIB. Le MIB dans le système de gestion prévoit l'identification et le traitement des informations envoyées par un dispositif (soit les réponses aux questions ou des pièges de l'appareil de source). Le MIB dans le dispositif concerne les adresses de sous-programme à des objets afin de lire les données à partir de, ou écrire des données sur les variables, dans le dispositif.

Un agent SNMPv1 accepte les commandes pour récupérer un objet, récupérer l'objet suivant, définissez et de l'objet à une valeur spécifiée, envoyer une valeur en réponse à une commande reçue, et envoyer une valeur en réponse à un événement (trap).

SNMPv2c ajoute à ce qui précède la possibilité de récupérer un grand nombre d'objets en réponse à une requête unique.

SNMPv3 ajoute des fonctionnalités de sécurité solides, y compris le cryptage; une clé de mot de passe partagé est utilisé. Surveillance du dispositif sécurisé sur Internet est possible. En plus des commandes notées comme supporté au-dessus, il y a une commande pour la synchronisation avec une station de gestion à distance.

Les pages qui suivent décrivent les différents champs nécessaires à la configuration SNMP sur les BulletPlus. MIBS peuvent être demandés à Microhard Systems Inc.

Le fichier MIB peut être téléchargé directement à partir de l'appareil en utilisant le bouton «Get MIB File 'dans le menu Réseau> SNMP.

SNMP: Simple Network Management Protocol fournit une méthode de gestion des périphériques réseau à partir d'un seul logiciel de gestion de réseau PC en cours d'exécution.

appareils en réseau gérés sont appelés agents SNMP.



Paramètres SNMP

Systen	Network	Carrier	Wireless	Firewal	I VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Users	Authenticati	on NMS	SNMP D	scovery	Logout								
SNMP	Settings												
SNMP	Settings												
SN	MP Agent Status		Ena	able 🔻									
Re	ad Only Commur	nity Name	pub	ic									
Re	ad Write Commu	nity Name	priva	ate									
Lis	tening Port		161										
SN	MP Version		Ver	sion 3 🔻									
N	3 User Name		use	√3									
N	3 User Read Writ	e Limit	Rea	ad Only 🔻									
N	3 User Authentic	ation Level	No	AuthNoPriv	•								
SN	MP Trap Setting	5											
S	NMP Trap Status		Ena	able 🔻									
т	rap Community I	Name	Trap	User									
т	rap Manage Host	t IP	0.0.	0.0		0.0.0.0-Dis	able						
A	uth Failure Traps	6	Dis	able 🔻									
Down	load MIB File												
G	et MIB File												

Image 4-13-6: Admin > SNMP

Mode de fonctionnement SNMP

Si elle est désactivée, un service SNMP ne sont pas fournies par le dispositif. Activé, le dispositif - maintenant un agent SNMP - peut prendre en charge SNMP v1, v2 et v3.

Désactiver/ V1&V2c&V3

Valeurs

Lecture seule Nom communautaire

En effet un mécanisme de mot de passe en texte clair utilisé pour authentifier faiblement requêtes SNMP. Faire partie de la communauté permet à l'agent SNMP pour traiter SNMPv1 et SNMPv2c demandes. Ce nom de communauté n'a LIRE priorité.

ur Valeurs

public

Lecture seule Nom communautaire

Valeurs

Aussi un mécanisme de mot de passe en texte clair utilisé pour authentifier faiblement requêtes SNMP. Faire partie de la communauté permet à l'agent SNMP pour traiter SNMPv1 et SNMPv2c demandes. Ce nom de communauté n'a LIRE / priorité WRITE.

private

SNMPv3 Nom d'utilisateur

Définit le nom d'utilisateur pour SNMPv3.

Valeurs V3user



1/2			4
V 5			
	ullisa		

Définit l'accessibilité des SNMPv3; Si Read Only est sélectionné, l'utilisateur SNMPv3 ne peut lire les informations; si Read Write est sélectionné, l'utilisateur SNMPv3 peut lire et écrire (set) des variables.

Définit le niveau d'authentification de l'utilisateur SNMPv3:

NoAuthNoPriv: Pas d'authentification, aucun cryptage. AuthNoPriv: authentification, aucun chiffrement.

AuthPriv: Authentification, chiffrement.

Valeurs

Read Only / Read Write

Authentification	utilisateur	V3 Niveau
------------------	-------------	-----------

Valeurs

NoAuthNoPriv AuthNoPriv AuthPriv

V3 Authentification utilisateur Mot de passe

Le mot de passe d'authentification de l'utilisateur SNMPv3. Valable uniquement lorsque l'authentification utilisateur V3 Niveau réglé sur authNoPriv ou authPriv.

0000000

Valeurs

V3 Utilisateur Mot de passe Confidentialité

Utilisateurs SNMPv3 mot de passe crypté. Valable uniquement lorsque l'authentification utilisateur V3 Niveau réglé sur authPriv (voir ci-dessus). 0000000

	SNMP	Trap Version
Sélectionnez la version du piège sera envoyé si une condition de	Valeurs	
	V1 Traps V3 Traps V1&V2&V3	V2 Traps V1&V2 Traps Traps
	Auth Piège (de défaillance

Si elle est activée, une interruption d'échec d'authentification sera généré en cas d'échec d'authentification.

Désactiver / Activer

Nom	n de trap communautaire
Le nom de communauté qui peut recevoir des interruptions.	Valeurs
	TrapUser
	Piège Gérer Host IP
Définit une adresse IP hôte où les pièges seront envoyés à (par exemple l'adresse IP du système de gestion de PC SNMP).	Valeurs

0.0.0.0



4.13.5 Admin > La découverte

Microhard radio utilisent un service de découverte qui peut être utilisé pour détecter d'autres microhard de radio sur un réseau. Cela peut être fait en utilisant un utilitaire autonome du système Microhard est appelé «Discovery IP» ou du> menu Discovery Admin. Le service de découverte rendra compte de l'adresse MAC, l'adresse IP, Description, Nom du produit, la version du micrologiciel, mode de fonctionnement, et le SSID.

	0											_	0101
	m	ICTO	naro	SYST	EMSI	NC.	1010	010	10	51	0	0	1010
System	Network	Carrier	Wireless	Firewall	VPN I	Router	Serial	I/0	GPS	Apps	Diag	Admi	n
Users A	uthenticati	on NMS	SNMP Dis	covery L	ogout								
Network	Discovery												
Server s	tatus Settings												
Disc	overy server sta	atus	O Dis	sable 🖲 Enab	e								
Server p	oort Settings												
Serv	er Port		2009	7									
Networ	k Discovery												
MA	C Address		IP Address	D	escription		Produ	ct Name			Firmwa	are Ver	
Sta	art discovery ne	twork now											

Image 4-13-7: Admin > Paramètres de découverte

									Discovery Service Status
Utilisez cette	option	pour	activer	ou	désactive	er le	servi	ce de	Valeurs
decouverte.									Disable / Discoverable / Changable
								Pa	ramètres du port serveur
Spécifiez le p BulletPlus.	oort exé	écutant	le sei	vice	de déco	uverte	e sur	l'unité	Valeurs

20077



4.13.6 Admin > Logout

La fonction de déconnexion permet à un utilisateur de mettre fin à la session de configuration actuelle et invite à un écran de connexion.

	m	icro	hard	l syst	EMS	INC.	101	010	10	17	0	1	01	0101
System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	1/0	GPS	Apps	Diag	Admir	10	210
Are you	uthenticati sure you wa ^{DW}	on NMS nt to log o	SNMP Di ut	scovery	ogout									
						Authenti The server password.	ication R r http://192 . The serve	equire 2.168.168. r says: Wi	d .1:80 requ ebUI.	uires a us	ername	× and	s Inc.	Bulletplus
						User Pass	word:]		
									Lo	g In	Can	cel		

Image 4-13-9: Admiin > logout



5.1 AT Aperçu Commande

Commandes AT peut être délivré pour configurer et gérer les BulletPlus, via le port série arrière (console), ou par TCP / IP (telnet).

5.1.1 Port Série

Pour connecter et accéder à l'interface de commande AT sur les BulletPlus, une connexion physique doit être faite sur la console (TX / RX) port série à l'arrière de l'BulletPlus Un programme d'émulation de terminal (HyperTerminal, Tera Term, ProComm, Putty etc) peuvent ensuite être utilisé pour communiquer avec les BulletPlus. Les paramètres du port de ce port peut être modifié en changeant les paramètres du port de la console, dans les menus de configuration série.

COM14 Properties	Paramètres par défaut:
Port Settings	Vitesse: 115200
<u>B</u> its per second: 115200 ▼	Bits de données: 8
<u>D</u> ata bits: 8	Parité: Aucun
Parity: None	Bits d'arrêt: 1
Stop bits: 1	
<u>∃</u> ow control: None ▼	Contrôle de flux: Aucun
Bestore Defaults	
OK Cancel Apply	

Image 5-1: Paramètres du port console

Une fois la communication établie, une connexion est nécessaire pour accéder à l'interface de commande AT, une fois connecté, le menu Command Line Interface AT est affiché. Tapez "?" Ou Aide à la liste des commandes de menu.

Pile Edit Ver Cell Trender Hep D @ @ @ D D D D BulletPlus login: admin Password: Entering character mode Escape character is '^1'. Command Line Interface BulletPlus>? help hsitory Sinfo status system network AT ATE AT ATE AT ATE AT ATE AT AT ATE AT ATE AT ATE ATE ATE ATE ATE ATE ATE BulletPlus Set or Get network configurations system Set or Get network config ATE Enable Echo ATH ATE BulletPlus List all available AT commands ATE ATE	BulletPlus - HyperTerminal	
Image: Solution of the second seco	File Edit View Call Transfer Help	
BulletPlus login: admin Password: Entering character mode Escape character is '^l'. Command Line Interface BulletPlus? help history Sinfo system info system configurations network ATE1 ATE0 ATE1 ATE2 ATE1 ATE1 ATE2 ATE2 ATE1 ATE3 ATE4 Bable Echo ATE1 ATE4 ATE3 ATE4 ATE4 ATE4 ATE4 ATE4 ATE4 Bable Echo ATE4 ATE4 Bable Echo ATE4<	D ⊯ ⊗ \$ 0 B B	
Entering character mode Escape character is '^l'. Command Line Interface BulletPlus>? help history Show a list of previously run command s info status system Setting system configurations network ATE0 ATE0 ATE1 ATE1 ATE1 ATE1 ATE1 ATE1 ATE1 ATE2 ATE1 ATE2 ATE1 ATE2 ATE2 ATE2 ATE2 ATE3 ATE3 ATE3 ATE3 ATE4 AT	BulletPlus login: admin Password:	^
Command Line Interface BulletPlus? ? help history Show a list of previously run command sinfo status system network ATE0 ATE1 ATE1 ATE1 ATE1 ATE1 ATE1 ATE2 ATE2 ATE2 ATE2 ATE2 ATE2 ATE2 ATE2	Entering character mode Escape character is '^]'.	
help Show available commands history Show a list of previously run command s info status Display the system status system Setting system configurations network Get Get network config AT AT Echo 0K ATE1 Enable Echo ATE1 Enable Echo ATH AT Echo TESI ATH Show a list of previously run AT comm ands Itst all available AT commands ATR Reserved ATRA Enable configurations you have been e ntreed Ouit ATA Ouit ATA Ouit	Command Line Interface BulletPlus> ?	
s info status system network AT ATE0 ATE0 ATE1 ATE1 ATE1 ATE0 ATE1	help history	Show available commands Show a list of previously run command
ATE1 Enable Echo AT+TEST AT Echo TEST ATH Show a list of previously run AT comm ands List all available AT commands ATL List all available AT commands AT&R Reserved AT&W Display modem active profile ATA Enable configurations you have been e ATA Quit ATA Quit ATA Quit	s info status system network AT ATE0	System info Display the system status Setting system configurations Set or 6et network config AT Echo OK Disable Echo
ands ATL List all available AT commands ATR Reserved ATRV Display modem active profile ATRW Enable configurations you have been e ATA Quit ATA Quit ATA Quit ATA Quit	ATE1 AT+TEST ATH	Enable Echo AT Echo TEST Show a list of previously run AT comm
ATA Quit ATA Quit ATO Quit AT-WSONTO Gat/Sat copsole timeout	ands ATL ATL AT&R AT&V AT&V AT&V	List all available AT commands Reserved Display modem active profile Enable configurations you have been e
Connected 000-58 Auto detect TCP/IP SCROLL CAPS NIIM Capture Print echo	ATA ATA ATO AT+MSCNTO Connected 00058 Auto detect TCP/IP SCROLL CAPS N	Quit Quit Get/Set console timeout

Paramètres par défaut:

BulletPlus connexion: admin

Mot de passe: admin



5.1.2 Telnet (TCP/IP)

Telnet peut être utilisé pour accéder à l'interface de commande AT des BulletPlus. Le port par défaut est le port TCP 23. Une session telnet peut être faite à l'unité en utilisant une application Telnet (Windows Telnet, Tera Term, ProComm etc). Une fois la communication établie, une connexion est nécessaire pour continuer.



Image 5-3: Établissement d'une session Telnet

Une session peut être faite à l'adresse IP WAN (si cela est autorisé dans les paramètres de pare-feu) pour la configuration à distance, ou à l'interface RJ45 local.

Une fois qu'une session est établie une connexion est nécessaire pour continuer. Comme on le voit dans la configuration du port série, la connexion par défaut est admin et le mot de passe est admin. Une fois vérifié, le menu Command Line Interface AT apparaît et AT Les commandes peuvent maintenant être émis. (Type "?" Ou à l'aide de la liste des commandes).

Telnet 192.168.168.1	
BulletPlus login: admin Password:	
Entering character mode Escape character is '^]'.	
Command Line Interface	
BulletPlus> ?	
help	Show available commands
history	Show a list of previously run command
S	
1nto	System info Disulay the system status
status	Display the system status Sotting system configurations
system	Setting system configurations
	AT Faha AV
	Disable Foko
0TE1	Fnable Echo
AT+TEST	AT Febo TFST
ATH	Show a list of previously run AT comm
ands	onow a 1100 of providably fan ni oonn
ATL	List all available AT commands
AT&R	Reserved
AT&U	Display modem active profile
AT&W	Enable configurations you have been e

Image 5-4: Telnet AT session de commande



Les paramètres réseau par défaut:

IP: 192.168.168.1 Subnet: 255.255.255.0 Passerelle: 192.168.168.1



5.2 AT Syntaxe de Commande

La syntaxe de suivi est utilisé lors de l'émission des commandes AT sur le BulletPlus

- Toutes les commandes commencent par les caractères AT et se terminent par la touche <Enter>
- Commandes Microhard spécifiques commencent par M +
- Aide donnera la liste des commandes de niveau supérieur (ATL donnera la liste des commandes AT ALL disponibles)
- Pour interroger la syntaxe d'une commande: AT + <command_name> =?
 - Syntaxe des commandes qui sont utilisés uniquement pour interroger un paramètre: AT <command name>
- Syntaxe des commandes qui peuvent être utilisées pour interroger et définir des valeurs: AT <command_name> = parameter1, parameter2, ... (fixe des valeurs)
 - AT <command_name>? (Interroge le réglage)

Syntaxe de requête:

AT+MSMNAME=? <Enter> +MSMNAME: Syntaxe de la commande :AT+MLEIP=<modem_name> OK

Définition d'une valeur:

AT+MSMNAME=BulletPlus-Test <Enter> OK

Interroger un cadre:

AT+MSMNAME? <Enter> Host name:BulletPlus-Test OK

Une capture d'écran des commandes ci-dessus entrés dans une unité est indiqué ci-dessous:



Image 5-5: Telnet AT Syntaxe de Commande

Une fois les commandes AT sont saisies, elles doivent être enregistrées dans le système de fichiers pour activer les modifications.

AT&W enregistre les modifications.

ATO ou **ATĂ** Quitte l'interface de ligne de commande AT, si elle est utilisée avant **AT&W**, les changements sont mis au rebut.



5.3 Commandes AT Supportées	
	AT
La description	Syntaxe de la commande(Effet: Immédiate)
Echo OK.	AT <enter></enter>
Exemple	
Commander: AT <enter> Réponse: OK</enter>	
	ATE0
La description	Syntaxe de la commande(Effet: Immédiate)
Désactiver l'écho local.	ATE0 <enter></enter>
Exemple	
Commander: ATE0 <enter> Réponse: OK</enter>	
	ATE1
La description	Syntaxe de la commande(Effet: Immédiate)
Activer l'écho local.	ATE1 <enter></enter>
Exemple	

Commander:

ATE1 <enter> Réponse: OK

© Microhard 2016



La descri	ption	Syntaxe de la commande(Effet: Immédiat
Afficher la liste	e des commandes précédemment exécutés.	ATH <enter></enter>
Exemple		
Commander: ATH <enter> Réponse: AT Command</enter>	history: 1. ATH 2. ATL 3. ATH	
La descri	ption	Syntaxe de la commande(Effet: Immédiat
Afficher une li	ste de toutes les commandes AT disponibles.	ATL <enter></enter>
Afficher une li Exemple Commander: ATL <enter> Réponse: AT Commanc AT ATEO ATE1 ATE1 ATH ATL ATL AT&R AT&R AT&W AT&W AT&W AT&W</enter>	ste de toutes les commandes AT disponibles. ds available: AT Echo OK Disable Echo Enable Echo Show a list of previously run AT commar List all available AT commands Reserved Display modem active profile Enable configurations you have been e Quit	ATL <enter></enter>



La description

Lire le profil du modem profil modifiable. (Réservé)

Syntaxe de la commande(Effet: Immédiate)

AT&R <enter>

Exemple

Commander: AT&R <enter> Réponse: OK

© Microhard 2016



	AT
La description	Syntaxe de la commande(Effet: Immédiate)
Lire modem profil actif.	AT&V <enter></enter>
Exemple	
Commander: AT&V <enter> Réponse: &V: hostname:BulletPlus-Test timezone:MST7MDT,M3.2.0,M11.1.0 systemmode:gateway time mode:local OK</enter>	
	AT&
La description	Syntaxe de la commande(Effet: Immédiate)
Activer les changements de configurations qui ont été saisies.	AT&W <enter></enter>
Exemple	
Commander: AT&W <enter> Réponse: Restarting the services to enable the configurations chang</enter>	ged recently
	ATA / A
La description	Syntaxe de la commande(Effet: Immédiate)
Quitter. Quitte à la session de commande et vous renvoie à se connecter rapidement.	ATA <enter></enter>
Exemple	
Commander: ATA <enter> Réponse:</enter>	



AT+MSCNTO

La description

Définit la valeur de délai d'attente pour les consoles série et telnet. Une fois expiré, l'utilisateur sera de retour pour vous connecter rapidement. Syntaxe de la commande(Effet: AT&W)

AT+MSCNTO=<Timeout_s> 0 - Désactivé

0 - 65535 (s)

Exemple

Commander: AT+MSCNTO=300 <enter> Réponse: OK

AT+MSPWD

La description

Utilisé pour définir ou modifier le mot de passe ADMIN.

Syntaxe de la commande(Effet: Immédiate)

AT+MSPWD=<New password>,<confirm password> mot de passe: au moins 5 caractères

Exemple

Commander: AT+MSPWD=admin,admin<enter> Réponse: OK

AT+MSGMI

La description

Obtenez identification du fabricant.

Exemple

Commander:

AT+MSGMI<enter>

Réponse: +MSGMI: 2014-2015 Microhard Systems Inc. OK Syntaxe de la commande

AT+MSGMI=<enter>



AT+MSSYSI

La description

Résumé du système d'information

Syntaxe de la commande

AT+MSSYSI <enter>

Exemple

Commander: AT+MSSYSI <enter> Réponse: Carrier: MMIMEI:356406060882064 SIMID:89302610203010832398 MMIMSI:302610012606734 Status:Connected Network:Bell RSSI:-64 Temperature:46 Ethernet Port: MAC:00:0F:92:02:8A:05 IP:192.168.168.1 MASK:255.255.255.0 Wan MAC:00:0F:92:FE:00:01 Wan IP:184.151.220.2 Wan MASK:255.255.255.255 System: Device:BulletPlus-Test Product:Bulletplus Image:PWii Hardware:Rev A Software:v1.3.0 build 1009-28

Copyright: 2014-2015 Microhard Systems Inc. Time: Thu Nov 19 10:17:43 2015

AT+MSGMR

La description

Modem Information sur l'enregistrement

Syntaxe de la commande

AT+MSGMR <enter>

Exemple

Commander: AT+MSGMR <enter> Réponse: +MSGMR: Hardware Version:Rev A Software Version:v1.3.0 build 1009-28 Copyright: 2014-2015 Microhard Systems Inc. System Time: Thu Nov 19 10:19:42 2015 OK



	AT+MSMNAM
La description	Syntaxe de la commande(Effet: AT&W)
Description du Modem Nom / Radio. 30 caractères.	AT+MSMNAME= <modem_name></modem_name>
Exemple	
Commander: (Pour définir la valeur) AT+MSMNAME=BulletPlus-Test <enter> Réponse: OK Commander: (Pour récupérer la valeur) AT+MSMNAME?<enter> Réponse: Host name:BulletPlus-Test</enter></enter>	
ОК	
ОК	AT+MSR ⁻
OK La description	AT+MSR Syntaxe de la commande(Effet: Immédiate)
OK La description Réinitialiser le modem aux paramètres d'usine par défaut de la mémoire non-volatile.	AT+MSR Syntaxe de la commande(Effet: Immédiate) AT+MSRTF= <action> Action: 0 action prédéfinie l'action 1 confirmation</action>
OK La description Réinitialiser le modem aux paramètres d'usine par défaut de la mémoire non-volatile. Exemple	AT+MSR Syntaxe de la commande(Effet: Immédiate) AT+MSRTF= <action> Action: 0 action prédéfinie l'action 1 confirmation</action>

AT+MSREB

La description

Redémarrez le modem.

Syntaxe de la commande(Effet: Immédiate)

AT+MSREB <enter>

Exemple

Commander: AT+MSREB <enter> Réponse: OK. Rebooting...



AT+MSNTP

AT+MSSYSLOG

La description

Être / Définir serveur NTP.

Syntaxe de la commande(Effet: AT&W)

AT+MSNTP=<status>[,<NTP server>[.<Port>]] Status: 0 Local Time

1 NTP

Exemple

Commander: AT+MSNTP=1,pool.ntp.org<enter> Réponse: OK

La description

Être / Définir serveur syslog

Syntaxe de la commande(Effet: AT&W)

AT+MSSYSLOG=<Server>[,<Port>] Server : Valid IP Address or Name. 0.0.0.0 -Disable. 1 to 256 characters Port: 1 to 65535. Default is 514

Exemple

Commander: AT+MSSYSL0G=192.168.168.35,514<enter> Réponse: OK

Commander: AT+MSSYSLOG? Réponse: Syslog Server : 192.168.168.35 Syslog Port : 514 OK

La description

Être / Définir l'état de service et le port.

Exemple

Commander: AT+MSSERVICE=0,0<enter> Réponse: OK

AT+MSSERVICE

Syntaxe de la commande(Effet: AT&W)

AT+MSSERVICE[=<Service>[,<Mode>[,<Port>]]] Paramètres: <Service>: 0 - FTP 1 - Telnet 2 - SSH

- 3 Microhard Sh
- <Mode>: 0 Disable
 - 1 Enable

<Port>: 1 to 65535. Pour Telnet (23 par défaut) et SSH (22 par défaut) ne



AT+MSWEBUI

La description

Exemple

Commander:

Réponse:

ΟK

Obtenir / set protocole WebUI et le port

AT+MSWEBUI=0,80,443<enter>

Syntaxe de la commande(Effet: AT&W)

AT+MSWEBUI[=<Mode>[,<HTTP Port>] [,<HTTPS Port>]]] Paramètres: <Mode>: 0 - HTTP/HTTPS 1 - HTTP 2 - HTTPS <HTTP Port>: 1 to 65535. 80 by default <HTTPS Port>: 1 to 65535. 443 by default Usages: AT+MSWEBUI AT+MSWEBUI=<Mode> AT+MSWEBUI=<Mode>,<HTTP Port> when <Mode>=1 AT+MSWEBUI=<Mode>,<HTTPS Port> when <Mode>=2 AT+MSWEBUI=<Mode>,<HTTP Port>,<HTTPS Port> when <Mode>=0

AT+MSKA

La description

Obtenez Mode / Set ICMP Keepalive.

Syntaxe de la commande(Effet: AT&W)

AT+MSKA=<Mode> Mode: 0 Désactivé 1 Activer

Exemple

Commander: AT+MSKA=1<enter> Réponse: OK



AT+MSKAS

La description

Obtenez / Définir les paramètres ICMP Keepalive.

Syntaxe de la commande(Effet: AT&W)

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

Exemple

Commander: AT+MSKAS=8.8.8.8,300,20<enter> Réponse: OK

Commander: AT+MSKAS? Réponse: +MSKAS: ICMP status:0 hostname:8.8.8.8 interval:300 count:20 OK

AT+MNLAN

La description

Afficher / Ajouter / Editer / Supprimer l'interface réseau.

Syntaxe de la commande(Effet: AT&W)

AT+MNLAN=[<LAN Name>[,<Operation>[,<Protocol>[,STP[,<IP Address>,<Netmask>]]]]] LAN Name: Name of Network LAN interface

Operation:

SHOW - Show the details of an exsiting LAN interface

ADD - Add a new LAN interface, followed by the other parameters

EDIT - Edit an exsiting LAN interface, followed by the other parameters

DEL - Delete an existing LAN interface

Protocol : 0 - DHCP

1 - Static IP

STP: 0 - Spanning Tree Off

1 - Spanning Tree On

IP Address : Valid IP address

Netmask: Valid netmask

Exemple

Commander:

AT+MNLAN? **Réponse:** 1: lan - 192.168.168.1, static (connection type), On (LAN DHCP), off (STP) OK



AT+MNLANDHCP

La description

Obtenir / set serveur LAN DHCP sur l'interface Ethernet.

Syntaxe de la commande(Effet: AT&W)

AT+MNLANDHCP=<LAN Name>[,<Mode>[,<Start IP>, <Limit>[,<Lease Time>,<Alt. Gateway>, <Pre. DNS>, <Alt. DNS>,<WINS/NBNS Servers>,<WINS/NBT Node>]]]

LAN Name: Nom de l'interface LAN Réseau

Mode: 0 - Désactiver le serveur DHCP

1 - Activer le serveur DHCP

Start IP: Les adresses DHCP à partir des adresses IP assignable

Limit: Le nombre maximum d'adresses IP. min = 0 max = 16777214

Lease Time: La durée du bail DHCP en quelques minutes. min = 0 max = 214748364

Alt. Gateway: Autre passerelle pour DHCP appareils affecté si la passerelle par défaut est de ne pas être utilisé

Pre. DNS: adresse du serveur DNS préféré à attribuer aux dispositifs DHCP Alt. DNS: adresse du serveur DNS alternatif à attribuer aux dispositifs DHCP

WINS/NBNS Server : WINS/NBNS Serveurs

WINS/NBT Node : WINS/NBT Node Type

- 0 none
- 1 b-node
- 2 p-node
- 3 m-node
- 4 h-node

Exemple

Commander: AT+MNLANDHCP=lan<enter> Réponse: LAN Name : lan : 1 - DHCP Server enabled Mode Start IP : 192.168.168.100 Limit : 150 Lease Time : 720m Alt. Gateway: Pre. DNS : Alt. DNS WINS/NBNS Server : WINS/NBT Node : 0 - none OK



AT+MNLANSTP

La description

Get / Régler l'interface LAN du réseau: Spanning Tree (STP)

Syntaxe de la commande(Effet: AT&W)

AT+MNLANSTP=<LAN Name>[,<STP>] Paramètres: LAN Name: Name of Network LAN interface Spanning Tree: 0 - Off 1 - On

Exemple

Commander: AT+MNLANSTP=lan,0<enter> Réponse: OK

AT+	MNI	AN	DNS

La description	Syntaxe de la commande(Effet: AT&W)
Get / Régler l'interface LAN de réseau: DNS	AT+MNLANDNS= <lan name="">[,<mode> [,<primary dns="">,<secondary dns="">]] Usage: AT+MNLANDNS=<lan name=""> AT+MNLANDNS=<lan name="">,<mode> Where <mode>=0 AT+MNLANDNS=<lan name="">,<mode> [,<primary dns="">,<secondary dns="">] Where <mode>=1 Paramètres: LAN Name: Nom de l'interface LAN Réseau Mode: 0 - Auto 1 - Manual Primary DNS: Valid IP Address or 0 (Reset) Secondary DNS: Valid IP address or 0 (Reset)</mode></secondary></primary></mode></lan></mode></mode></lan></lan></secondary></primary></mode></lan>

Exemple

Commander: AT+MNLANDNS=lan,0<enter> Réponse: OK



AT+MNWAN

La description

Afficher / Ajouter / Modifier / Supprimer l'interface WAN du réseau.

Syntaxe de la commande(Effet: AT&W)

AT+MNWAN[=<Mode>[,<Protocol>[,<IP>,<Netmask>[,<Gateway>]]]] Usage: AT+MNWAN AT+MNWAN=<Mode>,<Protocol>,<IP>,<Netmask>[,<Gateway>] Where <Mode>=0/2 and <Protocol>=0 AT+MNWAN=<Mode>,<Protocol> Where <Mode>=0/2 and <Protocol>=1 AT+MNWAN=<Mode>,<Protocol> Where <Mode>=2 and <Protocol>=2 AT+MNWAN=<Mode> Where <Mode>=1 Parameters: Mode: 0 - Independent WAN 1 - Bridge with LAN Port 2 - Independent LAN Protocol: 0 - Static IP 1 - DHCP 2 - None IP: Valid IP address Netmask: Valid netmask

Exemple

Commander:

AT+MNWAN=0,1<enter> Réponse: OK

Gateway: Valid IP address. 0 - Reset

Commander: AT+MNWAN? Réponse: Working Mode: Independent WAN WAN Configuration Connection Type: DHCP Default Route: Yes DNS Server Mode: auto OK



AT+MNWANDR

La description

Obtenez / Régler l'interface WAN du réseau: Par défaut Route

Lire / Serveur DNS lorsque le port WAN défini

Syntaxe de la commande(Effet: AT&W)

AT+MNWANDR[=<Default Route>] Paramètres: Default Route : 0 - No 1 - Yes

Exemple

Commander: AT+MNWANDR=1<enter> Réponse: OK

La description

comme indépendant WAN.

AT+MNWANDNS

Syntaxe de la commande(Effet: AT&W)

AT+MNWANDNS[=<Mode>[,<Primary DNS>,<Secondary DNS>]] Paramètres: AT+MNWANDNS AT+MNWANDNS=<Mode> Where <Mode>=0 AT+MNWANDNS=<Mode> (,<Primary DNS>, <Secondary DNS>] Where <Mode>=1 Parameters: Mode: 0 - Auto 1 - Manual Primary DNS: Valid IP Address or 0 (Reset)

Secondary DNS: Valid IP address or 0 (Reset)

Exemple

Commander: AT+MNWANDR=0<enter> Réponse: OK



AT+MNWANLANDHCP

La description

Get / Régler le serveur DHCP LAN quand a été mis en port comme indépendant LAN.

Syntaxe de la commande(Effet: AT&W)

AT+MNWANLANDHCP[=<Mode>[,<Start IP>,<Limit>,<Lease Time>[,<Alt.Gateway>,<Pre.DN S>,<Alt.DNS>]]] Paramètres: AT+MNWANLANDHCP AT+MNWANLANDHCP=<Mode> Where <Mode>=0 AT+MNWANLANDHCP=<Mode>,<Start IP>,<Limit>,<Lease Time>[,<Alt.Gateway>,<Pre.DNS> ,<Alt.DNS>] Where <Mode>=1 Parameters: Mode: 0 - Disable DHCP Server 1 - Enable DHCP Server Start IP: The starting address DHCP assignable IP Addresses Limit: The maximum number of IP addresses. min=0 max=16777214 Lease Time: The DHCP lease time in minutes. 2~2147483647 minutes. 0 means 'infinity' Alt. Gateway: Alternate Gateway for DHCP assigned devices if the default gateway is not to be used Pre. DNS: Preferred DNS server address to be assigned to DHCP devices Alt. DNS: Alternate DNS server address to be assigned to DHCP devices

Exemple

Commander: AT+MNWANLANDHCP=0<enter> Réponse: OK



AT+MNIPMAC

La description

Afficher / Ajouter / Supprimer / Release / ReleaseAll la liaison Adresse MAC-IP.

Syntaxe de la commande(Effet: AT&W)

AT+MNIPMAC=<Operation>[,<Name>[,<IP Address>,<MAC Address>]]

Operation: SHOW - Show the details of the MAC-IP address binding ADD - Add a new MAC-IP address binding DEL - Delete an existing MAC-IP address binding RELEASE - Release the active DHCP lease RELEASEALL - Release all active DHCP leases Name: Name of the MAC-IP binding IP Address : Valid IP address MAC Address: The physical MAC address of the device or interface Usage: AT+MNIPMAC AT+MNIPMAC=SHOW,<Name> AT+MNIPMAC=ADD,<Name>,<IP Address>,<MAC Address> AT+MNIPMAC=RELEASE,<NAME> AT+MNIPMAC=RELEASE,<NAME> AT+MNIPMAC=RELEASEALL

Exemple

Commander: AT+MNIPMAC=add,PC,192.168.168.150,0A0B0C0D0E0F<enter> Réponse: OK

Commander: AT+MNIPMAC? Réponse: 1: PC, 192.168.168.150, 0A0B0C0D0E0F, Not active OK

Commander: AT+MNIPMAC=RELEASEALL<enter> Réponse: Network DHCP server is restarted. OK



	AT	-MN	EM	AC
--	-----------	-----	----	----

La description

Command Syntax

Récupérer l'adresse MAC de l'interface Ethernet locale.

AT+MNEMAC <enter>

Exemple

Commander: AT+MNEMAC<enter> Réponse: +MNEMAC: "00:0F:92:00:40:9A" OK

AT+MNPORT

La description

Obtenez / définir la configuration du port Ethernet.

Syntaxe de la commande(Effet: AT&W)

AT+MNPORT[=<Ethernet Port>[,<Mode>[,<Auto Negotiation>,<Speed>,<Duplex>]]]

Ethernet Port:	0 - WAN
	1 - LAN1
	2 - LAN2
Mode:	0 - Auto
	1 - Manual
Auto-Neg:	0 - Off
	1 - On
Speed:	0 - 10
	1 - 100
Duplex:	0 - Full
	1 - Half

Exemple

Commander:

AT+MNPORT<enter> **Réponse:** 0: WAN: Mode: auto 1: LAN1: Mode: auto 2: LAN2: Mode: OK

Commander: AT+MNPORT=1,0<enter> Réponse: OK



AT+MNPORT

La description

Obtenir l'état du réseau.

Syntaxe de la commande(Effet: Immédiate)

AT+MNSTATUS?

Exemple

Commander:

AT+MNSTATUS<enter> Réponse: LAN Port Status General Status IP Address : 192.168.168.1 Connection Type : static Subnet Mask : 255.255.255.0 MAC Address : 00:0F:92:02:A8:E4 Traffic Status Receive bytes : 1.884MB Receive packets: 18542 Transmit bytes : 2.694MB Transmit packets: 14377 WAN Port Status **General Status** IP Address : N/A Connection Type : dhcp Subnet Mask : N/A MAC Address : 00:0F:92:03:A8:E4 Traffic Status Receive bytes : OB Receive packets : 0 Transmit bytes : 684B Transmit packets : 2 4G Port Status General Status IP Address : 184.151.220.2 Connection Type : static Subnet Mask : 255.255.255.255 MAC Address : 00:0F:92:FE:00:01 Traffic Status Receive bytes : 1.096MB Receive packets : 8602 Transmit bytes : 10.021MB Transmit packets : 9461 Default Gateway : 184.0.0.1 DNS Server(s) : 70.28.245.227 184.151.118.254 Kernel IP routing table Destination Gateway Subnet Mask Flags Metric Ref Use Iface 0.0.0.0 UG 0 0 br-wan2 0.0.0.0 184.0.0.1 169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br-lan 184.0.0.1 0.0.0.0 255.255.255.255 UH 0 0 0 br-wan2 192.168.168.0 0.0.0.0 255.255.255.0 U 0 0 0 br-lan



AT+MNDDNSE

AT+MNDDNS

La description

Obtenez Mode / Set Dynamic DNS (DDNS).

Syntaxe de la commande(Effet: AT&W)

AT+MNDDNSE=<Mode> Mode: 0 Désactivé 1 Activer

Exemple

Commander: AT+MNDDNSE? Réponse: +MNDDNSE: Mode 0 OK

Commander: AT+MNDDNSE=1<enter> Réponse: OK

La description

Obtenez paramètres / Set Dynamic DNS (DDNS).

Syntaxe de la commande(Effet: AT&W)

AT+MNDDNS=<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

Exemple

Commander:

AT+MNDDNSE? Réponse: +MNDDNSE: Mode 0 OK

Commander:

AT+MNDDNSE=4,mydomain.com,user1,password21<enter> **Réponse:**OK


AT+MFGEN

La description

Obtenir définir la configuration / pare-feu général

Exemple

Commander: AT+MFGEN=6,0<enter> Réponse: OK

Syntaxe de la commande

AT+MFGEN[=<Config>[,<Mode>]] Paramètres

Config: 0 - WAN Remote Management 1 - WAN Request

- 2 LAN to WAN Access Control
- 3 Anti-Spoof
- 4 Packet Normalization
- 5 Carrier Remote Management
- 6 Carrier Request
- 7 LAN to Carrier Access Control
- Mode: 0 Disable (Block)
 - 1 Enable (Allow)

AT+MFDMZ

La description

Obtenir la configuration / Set pare-feu DMZ

Exemple

Commander: AT+MFDMZ=0,0<enter> Réponse: OK

Syntaxe de la commande

Exception Port: 0 - 65535

AT+MFDMZ[=<DMZ Source>[,<DMZ Mode> [,<DMZ Server IP>,<Exception Port>]]] Paramètres DMZ Source: 0 - WAN 1 - Carrier DMZ Mode: 0 - Disable 1 - Enable DMZ Server IP: Valid IP address

© Microhard 2016



AT+MFDMZ

La description

Obtenir / set règles de redirection de port du pare-feu

Syntaxe de la commande

AT+MFPORTFWD[=<Name>[,<Operation>[,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>]]] Paramètres Name: Name of Port Forwarding rule, 1 - 64 characters Operation: ADD - Add a rule EDIT - Edit a rule DEL - Delete a rule Source: 0 - WAN 1 - Carrier 2 - WIFI Internal IP: Valid IP address Internal Port: Valid port number, 1 - 65535 Protocol: 0 - TCP 1 - UDP 2 - TCPUDP External Port : Valid port number, 1 - 65535 Usage: AT+MFPORTFWD AT+MFPORTFWD=<Name> AT+MFPORTFWD=<Name>,DEL AT+MFPORTFWD=<Name>,ADD,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port> AT+MFPORTFWD=<Name>,EDIT,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>

Exemple

Commander: AT+MFPORTFWD=rule1,add,0,192.168.168.203,20001,0,20001<enter> Réponse: OK

Commander: AT+MFPORTFWD? Réponse: Name : rule1 Source : WAN Internal IP : 192.168.168.203 Internat Port : 20001 Prorocol : TCP External Port : 20001 OK



AT+MFMAC

La description

Lire / Liste MAC pare-feu

Syntaxe de la commande

AT+MFMAC[=<Name>[,<Operation>[,<Action>,<Mac Address>]]] Paramètres Name: Name of firewall MAC list name, 1 - 64 characters Operation: ADD - Add a firewall MAC list EDIT - Edit a firewall MAC list DEL - Delete a firewall MAC list Action: 0 - Accept 1 - Drop 2 - Reject MAC Address : Valid MAC address Usage: AT+MFMAC AT+MFMAC=<Name> AT+MFMAC=<Name>,DEL AT+MFMAC=<Name>,ADD,<Action>,<Mac Address> AT+MFMAC=<Name>,EDIT,<Action>,<Mac Address>

Exemple

Commander: AT+MFMAC=mac1,add,1,00:0A:0A:0A:0B:FF<enter> Réponse: OK

Commander:

AT+MFMAC? **Réponse:** Name: mac1 Action: DROP MAC address: 00:0A:0A:0A:0B:FF OK



AT+MFIP

La description

Lire / Liste IP pare-feu

Syntaxe de la commande

AT+MFIP[=<Name>[,<Operation>[,<Action>,<Source>,<IP Address>[,<Prefix>]]]] Paramètres Name: Name of firewall IP list name, 1 - 64 characters Operation: ADD - Add a firewall IP list EDIT - Edit a firewall IP list DEL - Delete a firewall IP list Action: 0 - Accept 1 - Drop 2 - Reject Source: 0 - LÁN 1 - Independent LAN 2 - WAN 3 - Carrier 4 - WIFI Source IP: Valid IP address Prefix: 0 ~ 32. 32 (default) - single IP address Usage: AT+MFIP AT+MFIP=<Name> AT+MFIP=<Name>,DEL AT+MFIP=<Name>,ADD,<Action>,<Source>,<IP Address>[,<Prefix>] AT+MFIP=<Name>,EDIT,<Action>,<Source>,<IP Address>[,<Prefix>]

Exemple

Commander: AT+MFIP=iplist1,add,0,2,184.71.46.138,32<enter>

Réponse: OK

Commander:

AT+MFIP? **Réponse:** Name: ip1 Action: ACCEPT Source: WAN Source IP: 184.71.46.126 Prefix: 32 Name: iplist1 Action: ACCEPT Source: WAN Source IP: 184.71.46.138 Prefix: 32 OK



AT+MFRULE

La description

Obtenir / définir la règle de pare-feu.

Syntaxe de la commande

AT+MFRULE[=<Name>[,<Operation>[,<Action>,<Source>,<Src IP Format>,<Src IP From/Subnet >,<Src IP To/Prefix>,<Destination>,<Dest IP Format>,<Dest IP From/Subnet>,<Dest IP To/Prefix>,<Dest Port>,<Protocol>]]] Paramètres Name: Name of firewall rule name, 1 - 64 characters Operation: ADD - Add a firewall rule EDIT - Edit a firewall rule DEL - Delete a firewall rule Action: 0 - Accept 1 - Drop 2 - Reject Source: 0 - LAN 1 - Independent LAN 2 - WAN 3 - Carrier 4 - WIFI 5 - None IP Format: 0 - IP Range 1 - Subnet / Prefix IP From/Subnet: Valid IP address. 0 - Set to blank IP To/Prefix: Valid IP address. 0 - Set to blank; or 0 ~ 32 for Prefix Destination: 0 - LAN 1 - Independent LAN 2 - WAN 3 - Carrier 4 - WIFI 5 - None IP Format: 0 - IP Range 1 - Subnet / Prefix IP From/Subnet: Valid IP address. 0 - Set to blank IP To/Prefix: Valid IP address. 0 - Set to blank; or 0 ~ 32 for Prefix Port/Range: Port 0 ~ 65535 or Port range specified as 100:200 format Protocol: 0 - TCP 1 - UDP 2 - TCPUDP 3 - ICMP 4 - GRE

Exemple

Commander: AT+MFRULE=rule1,ADD,0,3,0,0,0,5,0,0,0,34567,2<enter> Réponse: OK Commander: AT+MFRULE? Réponse: Name :rule1 : ACCEPT Action Source Src IP From : Src IP To : 0 Destination : Dest IP From : Dest IP To : 0 Dest Port : 34567 Protocol : tcpudp ΟK



	AT+MFRST
La description	Syntaxe de la commande
Réinitialiser par défaut le pare-feu	AT+MFRST <enter></enter>
Exemple	
Commander: AT+MFRST <enter></enter>	
	AT+MMIMEI
La description	Syntaxe de la commande
Obtenez IMEI de modem.	AT+MMIMEI <enter></enter>
Exemple	
Commander: AT+MMIMEI <enter> Réponse: +MMIMEI: 356406060882064 OK</enter>	
	AT+MMIMSI
La description	Syntaxe de la commande
Obtenez modem IMEI.	AT+MMIMSI <enter></enter>
Exemple	
Commander: AT+MMIMSI <enter> Réponse: +MMIMSI: 302610012606734 OK</enter>	
	AT+MMNETRSSI
La description	Syntaxe de la commande
Obtenez modem RSSI.	AT+MMNETRSSI <enter></enter>
Exemple	

Commander: AT+MMNETRSSI<enter> Réponse: +MMNETRSSI:-59 OK



AT+MMPOWERIN

La description

Obtenez tension de contribution du modem.

Exemple

Commander: AT+MMPOWERIN<enter> Réponse: +MMPOWERIN: 12.27 OK

AT+MMBOARDTEMP

La description

Obtenez la température du modem.

Syntaxe de la commande

Syntaxe de la commande

AT+MMPOWERIN <enter>

AT+MMBOARDTEMP <enter>

Exemple

Commander: AT+MMBOARDTEMP<enter> Réponse: +MMBOARDTEMP: 46.65 OK

AT+MMWANIP

La description

Obtenir l'adresse IP WAN de modem (Carrier).

Syntaxe de la commande

AT+MMWANIP <enter>

Exemple

Commander: AT+MMWANIP<enter> Réponse: +MMWANIP: 184.151.220.2 OK



AT+MMPIPP

La description

Obtenir / Activer IP-Passthrough.

Syntaxe de la commande(Effet: AT&W)

AT+MMPIPP=<Mode> Mode: 0 Désactivé 1 Ethernet

Exemple

Commander: AT+MMPIPP=1<enter> Réponse: OK

Commander: AT+MMPIPP? Réponse: +MMPIPP: 1 Ethernet OK

AT+MMNUM

La description

Obtenez le numéro de téléphone du modem.

Exemple

Commander: AT+MMNUM <enter> Réponse: +MMNUM: 15874327939 OK

AT+MMIMI

La description

Obtenez IMEI et IMSI de modem.

Syntaxe de la commande

Syntaxe de la commande

AT+MMIMI <enter>

Exemple

Commander: AT+MMIMI <enter> Réponse: +MMIMI: MMIMEI:356406060882064, MMIMSI:302610012606734 OK

AT+MMNUM <enter>



AT+MMCID

La description

Obtenez modem numéro de carte SIM.

Exemple

Commander: AT+MMCID <enter> Réponse: +MMCID: 89302610203010832398 OK

AT+MMMGS

La description

Envoyer un message SMS.

Syntaxe de la commande(Immediate)

Syntaxe de la commande

AT+MMCID <enter>

AT+MMMGS=<Phone Number><CR> <Numéro de téléphone>: numéro de téléphone Le texte est entré et a fini par <ctrl-Z / ESC>

Exemple

Commander: AT+MMMGS=4035555151<enter>

Test Message <esc>

Réponse: OK > +CMGS: 15

ΟK

AT+MMMGR

La description

Lire des messages SMS.

Exemple

Commander: AT+MMMGR=1<enter>

Réponse:

+CMGL: 1,"REC READ","+19022110349",,"15/11/14,23:41:39-20" Test Message

ΟK

Syntaxe de la commande(Immediate)

AT+MMMGR=<index>

© Microhard 2016



AT+MMMGL

La description

Liste de tous les messages SMS.

Exemple

Commander: AT+MMMGL<enter>

Réponse: +CMGL: 1,"REC READ","+19022060349",,"15/11/14,23:41:39-20" Test Message

+CMGL: 6,"REC READ","+14036129217",,"15/09/23,15:07:04-16" This is also a test.

ΟK

AT+MMMGD

La description

Syntaxe de la commande(Immediate)

Syntaxe de la commande(Immediate)

AT+MMMGL<enter>

Supprimer des messages SMS à partir du système.

AT+MMMGD=<index> <Index> : l'index du message à supprimer

Exemple

Commander: AT+MMMGD=12<enter>

Réponse: OK

AT+MMSCMD

La description

Lire / Commande service SMS du système.

Syntaxe de la commande(Effet: AT&W)

AT+MMSCMD=<Mode>[,<Filter Mode>[,<Phone No.1>[,...,<Phone No.6>]]] Mode: 0 Désactiver 1 Activer commande SMS Filtre Mode: 0 Désactivé 1 Activer le filtre de téléphone

Exemple

Commander: AT+MMSCMD=1 <enter>

Réponse: OK



AT+MIOMODE

La description

Obtenez entrée / Set IO ou le mode de sortie.

Syntaxe de la commande(Effet: AT&W)

AT+MIOMODE=<Index>,<Mode> Indice: L'index du port de IO 1 à 2 Mode: 0 entrée 1 sortie

Exemple

Commander: AT+MIOMODE=1,0 <enter>

Réponse: OK

Commander: AT+MIOMODE?

Réponse:

+MIOMODE: IO port mode Mode1: 0 Contribution Mode2: 0 Contribution OK

AT+MIOOC

La description

Obtenez / Régler la commande de sortie. (Point I / O doit être réglé en sortie)

Syntaxe de la commande(Immediate)

AT+MIOOC=<Index>,<Output Control> Indice:

L'index du port de IO 1 à 2 Contrôle de sortie: 0 Ouvert 1 Fermer

Exemple

Commander: AT+MIOOC=1,1 <enter>

Réponse: OK

Commander: AT+MIOOC?

Réponse:

+MIOOC: IO Output Control OutputCtrl1: 1 Close OutputCtrl2: 0 Open OK



AT+MIOSTATUS

La description

GET état IO.

Exemple

Commander: AT+MIOSTATUS <enter>

Réponse:

+MIOSTATUS: IO status iodigiinval1=High iodigiinval2=High OK

AT+MIOMETER

AT+MCPS2

La description

GET IO meter (V).

Syntaxe de la commande

AT+MIOMETER <enter>

Syntaxe de la commande

AT+MIOSTATUS <enter>

Exemple

Commander: AT+MIOMETER <enter>

Réponse:

+MIOMETER: IO meter(V) iovolts1=2.77 iovolts2=2.81 OK

La description

Configurez le port série que ce soit un port console (Commandes AT) ou un port de données.

Exemple

Commander: AT+MCPS2=0<enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MCPS2=<Mode> Mode: 0 Console 1 données



AT+MCBR2

La description	Syntaxe de la commande(Effet: AT&W)
Get / Set vitesse de transmission du port série.	AT+MCBR2= <baud rate=""> Baud Rate: 0 300 1 600 2 1200 3 2400</baud>
Exemple	4 3600 5 4800
Commander: AT+MCBR2=13 <enter> Réponse: OK Commander: AT+MCBR2? Réponse: +MCBR2: 13 115200 OK</enter>	6 7200 7 9600 8 14400 9 19200 10 28800 11 38400 12 57600 13 115200 14 230400 15 460800 16 921600

AT+MCDF2

La description	Syntaxe de la commande(Effet: AT&W)
Obtenez le format / Set de port série de données	AT+MCDF2= <data format=""> Data Format: 0 8N1 2 8E1</data>

Exemple

Commander: AT+MCDF2=0<enter> Réponse: ΟK

3 801

AT+MCDM2

La description

Réglez le mode de données du port série.

Syntaxe de la commande(Effet: AT&W)

AT+MCDM2=<Data Mode> Data Mode:

- 0 Seamless
- Transparent 1

Exemple

Commander: AT+MCDM2=1<enter> Réponse: OK



AT+MCCT2

La description

Définir le délai de caractères Comport.

Syntaxe de la commande(Effet: AT&W)

AT+MCCT2=<timeout_s> (0 to 65535 secondes)

Exemple

Commander: AT+MCCT2=0<enter> Réponse: OK

AT+MCMPS2

La description

Get / Set port série taille de paquet maximale.

Syntaxe de la commande(Effet: AT&W)

AT+MCMPS2=<size> size: 0 to 65535

Exemple

Commander: AT+MCMPS2=1024<enter> Réponse: OK

AT+MCNCDI2

La description

Activer / désactiver le port série apport de données sans connexion.

Syntaxe de la commande(Effet: AT&W)

AT+MCNCDI2=<Mode> Mode: 0 Désactivé 1 Activer

Exemple

Commander: AT+MCNCDI2=1<enter> Réponse: OK



AT+MCMTC2

La description

Obtenir la configuration modbus TCP / Set de port série.

Syntaxe de la commande(Effet: AT&W)

AT+MCMTC2=<Status>, <Protection status>, <Protection Key> Statut et protection Statut: 0 Désactivé 1 Activer

Exemple

Commander: AT+MCMTC2=0,0,1234<enter> Réponse: OK

AT+MCIPM2

La description

Réglez le port série en mode IP.

Exemple

Commander: AT+MCIPM2=1<enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MCIPM2=<Mode>

- Mode:
- 0 TCP Client 1 TCP Server
- 2 TCP Client/Se
- 2 TCP Client/Server 3 UDP Point to Point
- 7 SMTP Client
- 8 PPP
- 11 GPS Transparent Mode

AT+MCTC2

La description

Réglez les paramètres du client le port TCP série lorsque le mode protocole IP est réglé sur TCP Client.

Syntaxe de la commande(Effet: AT&W)

AT+MCTC2=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s> Remote Server IP : valid IP address Remote Server Port : 1 to 65535 Outgoning timeout_s: 0 to 65535

Exemple

Commander: AT+MCTC2=0.0.0.0,20002,60<enter> Réponse: OK



AT+MCTS2

La description

Réglez les paramètres du serveur TCP lorsque le mode protocole IP est réglé sur TCP Server.

Exemple

Commander: AT+MCTS2=20002,300<enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MCTS2=<Local Listener Port>,<Connection timeout_s> Local Listener Port : 1 to 65535 Connection timeout_s: 0 to 65535

AT+MCTCS2

La description

Définissez les paramètres TCP Client / Server lorsque le Protocole IP est réglé en mode Client / Serveur TCP.

Syntaxe de la commande(Effet: AT&W)

AT+MCTCS2=<Remote Server IP>,<Remote Server Port>,<Outgoning timeout_s>,<Local Listener Port>

Remote Server IP : valid IP address Remote Server Port : 1 to 65535 Outgoning timeout_s: 0 to 65535 Local Listener Port: 1 to 65535

Exemple

Commander: AT+MCCS2=0.0.0.0,20002,60,20002<enter> Réponse: OK

AT+MCUPP2

La description

Définir les paramètres UDP point à point lorsque le Protocole IP est réglé sur UDP en mode point à point.

Syntaxe de la commande(Effet: AT&W)

AT+MCUPP2=<Remote IP>,<Remote Port>,<Listener Port> Remote IP : valid IP address Remote Port : 1 to 65535 Listener Port: 1 to 65535

Exemple

Commander: AT+MCUPP2=0.0.0.0,20002,20002<enter> Réponse: OK



AT+MCSMTP2

La description

Obtenez la configuration du client SMTP / Set de port série lorsque le mode protocole IP est réglé sur le client SMTP. Syntaxe de la commande(Effet: AT&W)

AT+MCSMTP2=<Mail Subject>,<Mail Server>,<Username>,<Pas sword>,<Mail Recipient>,<Message Max Size>,<TimeOut>,<Transfer Mode> Mail Subject : 1 to 63 bytes : Valid IP Address or Name Mail Server Username : 1 to 63 bytes Password : 1 to 63 bytes Mail Recipient : 1 to 63 bytes Message Max Size : [1 .. 65535] : [0 .. 65535] in seconds TimeOut Transfer Mode : 0: Text; 1: Attached File; 2: Hex Code

AT+MCPPP2

La description

Obtenir la configuration / Set de port série PPP lorsque le mode de protocole IP défini sur PPP.

Syntaxe de la commande(Effet: AT&W)

AT+MCPPP2=<Mode>,<LCP Echo Failure Number>,<LCP Echo Int erval>,<Local IP>,<Host IP>,<Idle Timeout>[,<Expected String>,<Response String>]

COM2: Mode : 0 - Active; 1 - Passive LCP Echo Failure Number : [0 .. 65535] LCP Echo Interval : [0 .. 65535] : Valid IP address Local IP Host IP : Valid IP address : [0 .. 65535] in seconds Idle Timeout Expected String : (Optional) 0 - 63 characters Response String : (Optional) 0 - 63 characters

Exemple

Commander: AT+MCPPP2? Réponse: +MCPPP2: Mode : 1 - Passive LCP Echo Failure Number: 0 LCP Echo Interval : 0 Local IP : 192.168.12.1 Host IP : 192.168.12.99 Idle Timeout(s) : 30 Expected String : CLIENT Response String : CLIENTSERVER ΟK



	AT+MAEURD1 AT+MAEURD2 AT+MAEURD3
La description	Syntaxe de la commande(Effet: AT&W)
Définir l'événement Rapport UDP Rapport No.1 / 2/3.	AT+MAEURD1= <mode>[,<remote IP>,<remote port="">,<interval time=""> [,Interfaces]] Mode : 0. Disable</interval></remote></remote </mode>
Exemple	1 Modern Event Report
Commander: AT+MAEURD1=1,192.168.168.111,2010,10 <enter> Réponse: OK</enter>	2 SDP Event Report 3 Management Report Remote IP : valid IP address Remote Port : 0 to 65535 Interval Time: 0 to 65535 seconds Interfaces : (optional) 0 Disable; 1 Enable Modem, Carrier and WAN for Modem Event Report. For instant, "1,1,1" to enable all interfaces Ethernet, Carrier, USB, COM and IO for Management Report. For instant, "0,0,0,0,0" to disable all interfaces

Syntaxe de la commande(Effet: AT&W)

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

Enable NMS Report 1

AT+MANMSSR\

Syntaxe de la commande(Effet: AT&W)

AT+MANMSSRV[=<Server>,<Name>, <Password>,<Confirm Password>] <Server>:

- NMS Server/IP. 1 to 63 characters <Name>:
- Domain Name. 1 to 63 characters <Password>:
- Domain Password. 5 to 64 characters <Confirm Password>:
- Same as <Password>. 5 to 64 characters

La description

Définir Rapport NMS.

Exemple

Commander: AT+MANMSR=1,20200,300<enter> Réponse: OK

La description

Get/Set NMS Server.

Exemple

Commander: AT+MANMSSRV=nms.microhardcorp.com,mytech,myp ass, mypass <enter> Réponse: ΟK



AT+MADISS

La description

Configurer le service de mode de découverte utilisée par pX2 et des utilitaires tels que "Discovery IP".

Syntaxe de la commande(Effet: AT&W)

AT+MADISS=<Mode> Mode: 0

- Disable
- 1 Discoverable

Exemple

Commander: AT+MADISS=1 <enter> Réponse: ΟK

AT+MAWSCLIENT

La description

Obtenez Client / Service Set Web.

Syntaxe de la commande(Effet: AT&W)

AT+MAWSCLIENT[=<Mode>[,<ServerType>,<Port>,<UserName>,<Password>,<Interval>]] Mode: 0 - Disable 1 - Enable ServerType: 0 - https 1 - http Port: 1 to 65535. Default is 9998 UserName: 1 to 63 characters Password: 1 to 63 characters Interval: In minute. 1 to 65535 minutes.

Exemple

Commander: AT+MAWSCLIENT=1,1,9998,username,password,10<enter> Réponse: ΟK



AT+MASNMP

La description

Obtenez le service / Set SNMP.

Syntaxe de la commande(Effet: AT&W)

AT+MASNMP[=<Mode>[,<ROCommunity>,<RWCommunity>,<Port>,<Version>]]

3 - Version 3 (Use AT+MASNMPV3 to set Authentication and Privacy parameters)

Exemple

Commander: AT+MASNMP=1,public,private,161,2<enter> Réponse: OK



AT+MASNMPV3

La description

Get / Set version 3 de SNMP.

Syntaxe de la commande(Effet: AT&W)

AT+MASNMPV3=<UserName>,<RWLimit>,<AuthLevel>[,<Auth>,<AuthPassword> <Privacy> [,<PrivacyPassword>]] UserName: V3 User Name 1 to 31 characters RWLimit: V3 User Read Write Limit 0 - Read Only 1 - Read Write AuthLevel: V3 User Authentication Level 0 - NoAuthNoPriv 1 - AuthNoPriv 2 - AuthPriv Auth: V3 Authentication Protocol 0 - MD5 1 - SHA AuthPassword: V3 Authentication Password 1 to 255 characters Privacy: V3 Privacy Protocol 0 - DES 1 - AES PrivacyPassword: V3 Privacy Password 1 to 255 characters Usage: AT+MASNMPV3=<UserName>,<RWLimit>,0 If <AuthLevel>=0 (NoAuthNoPriv) AT+MASNMPV3=<UserName>,<RWLimit>,1,<Auth>,<AuthPassword> If <AuthLevel>=1 (Au thNoPriv) AT+MASNMPV3=<UserName>,<RWLimit>,2,<Auth>,<AuthPassword>,<Privacy>,<PrivacyPas sword> If <AuthLevel>=2 (AuthPriv)

Exemple

Commander:

AT+MASNMPV3 <enter> **Réponse:** +MASNMPV3: UserName : userV3 RWLimit : Read Only AuthLevel : NoAuthNoPriv OK



AT+MASNMPTRAP

La description

Obtenez Piège / Set SNMP.

Exemple

Commander: AT+MASNMPTRAP=1 <enter> Réponse: OK

Commander: AT+MASNMPTRAP? Réponse: +MASNMPTRAP: Mode : 1 - Enable Name : TrapUser IP : 0.0.0.0 AuthFailureTraps : 0 - Disable OK

Syntaxe de la commande(Effet: AT&W)

AT+MASNMPTRAP[=<Mode>[,<Name>,<IP> [,<AuthFailureTraps>]] <Mode>: 0 - Disable 1 - Enable <Name>: Trap Community Name. 1 to 32 characters <IP>: Trap Manage Host IP. Default 0.0.0.0 (Disable) <AuthFailureTraps>: 0 - Disable 1 - Enable Usage: AT+MASNMPTRAP AT+MASNMPTRAP=0 AT+MASNMPTRAP=1[,<Name>,<IP> [,<AuthFailureTraps>]]

AT+MAAUTH

La description

Obtenir la configuration d'authentification / Set.

Exemple

Commander:

AT+MAAUTH? **Réponse:** +MAAUTH: Mode : 1 - Local&RADIUS ServerIP : 0.0.0.0 ServerPort : 1812 SharedSecret : nosecret OK Syntaxe de la commande(Effet: AT&W)

AT+MAAUTH[=<Mode>[,<ServerIP>, <ServerPort>,<SharedSecret>]] <Mode>: 0 - Local 1 - Local&RADIUS <ServerIP>: Remote Server IP Address <ServerPort>: Remote Server IP Port. 0 to 65535. Default 1812 <SharedSecret>: 5 to 64 characters Usage: AT+MAAUTH AT+MAAUTH=0 AT+MAAUTH=1 [,<ServerIP>,<ServerPort>,<SharedSecret>]



AT+MWRADIO

La description

Exemple

Commander:

Réponse: OK

AT+MWRADIO=1 <enter>

Obtenir le statut de radio / Set, ou le désactiver.

Syntaxe de la commande(Effet: AT&W)

AT+MWRADIO=<Radio> Radio: 0 - Off 1 - On

AT+MWMODE Syntaxe de la commande(Effet: AT&W) AT+MWMODE=<Mode>

- Mode: 0 - 802.11B ONLY
- 1 802.11BG
- 2 802.11NG High Throughput on 2.4GHz

La description

Obtenez le mode radio / Set.

Exemple

Commander: AT+MWMODE=2 <enter> Réponse: 0K

La description

Exemple

Commander:

Réponse:

OK

Obtenez / radio Set TX Power.

AT+MWTXPOWER

Syntaxe de la commande(Effet: AT&W)

AT+MWTXPOWER=<Tx Power>

AT+MWTXPOWER=10 <enter>

Tx Power: 0 - 20 dbm 1 - 21 dbm 2 - 22 dbm 3 - 23 dbm 4 - 24 dbm 5 - 25 dbm 6 - 26 dbm 7 - 27 dbm 8 - 28 dbm 9 - 29 dbm 10 - 30 dbm



AT+MWDISTANCE

La description

Obtenez / radio Set sans fil Distance.

Exemple

Commander: AT+MWDISTANCE=1000 <enter> Réponse: ΟK

Syntaxe de la commande(Effet: AT&W)

AT+MWDISTANCE=<Distance> Distance (m): Minimum 1

AT+MWCHAN

La description

Canal radio Set

Exemple

Commander: AT+MWCHAN=0 <enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MWCHAN=<Channel>

Available radio channels for mode 11ng and high throughput mode HT20:

- 0 auto
- 1 1 2 - 2
- 3 3
- 4 4
- 5 5
- 6 6
- 7 7
- 8 8
- 9 9
- 10 10
- 11 11

AT+MWHTMODE

La description

Obtenez / Réglez le mode haut débit radio.

Exemple

Commander: AT+MWHTMODE=2 <enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MWHTMODE=<High Throughput Mode>

- High Throughput Mode:
- 0 HT20
- 1 HT40-2 - HT40+
- 3 Force HT40-
- 4 Force HT40+



AT+MWMPDUAGG

La description

Exemple

Commander:

Réponse: OK

Obtenez / radio Set MPDU Agrégation.

Syntaxe de la commande(Effet: AT&W)

AT+MWMPDUAGG=<MPDU Aggregation> MPDU Aggregation: 0 - Disable 1 - Enable

AT+MWSHORTGI

La description

Obtenir / set radio courte GI

AT+MWMPDUAGG=1<enter>

Exemple

Commander: AT+MWSHORTGI=1<enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MWSHORTGI=<Short GI> Short GI: 0 - Disable 1 - Enable

AT+MWHTCAPAB

La description

Obtenez Capacités Radio HT Infos

Exemple

Commander: AT+MWHTCAPAB <enter> Réponse: +MWHTCAPAB: HT Capabilities Info -OK Syntaxe de la commande

AT+MWHTCAPAB <enter>



	AT+MWAMSDU
La description	Syntaxe de la commande
Obtenez un maximum de radio A MPDU (octet).	AT+MWAMSDU
Exemple	
Commander: AT+MWAMSDU <enter> Réponse: +MWAMSDU: Maximum AMSDU (byte) - 3839 OK</enter>	
	AT+MWAMPDU
La description	Syntaxe de la commande
Obtenez un maximum de radio AMPDU (octet).	AT+MWAMPDU
Exemple	
Commander: AT+MWAMPDU <enter> Réponse: +MWAMPDU: Maximum AMPDU (byte) - 65535</enter>	
	AI+MWRISIHRESH
La description	Syntaxe de la commande(Effet: AT&W)
Obtenir / set la radio RTS Threshold.	AT+MWRTSTHRESH= <rts threshold=""> RTS Threshold: 0 Disabled</rts>
Exemple	256-2346 Enabled with the value
Commander:	

AT+MWRTSTHRESH=0 <enter> Réponse: OK



AT+MWFRAGTHRESH

La description

Get/Set radio Fragment Seuil.

Exemple

Commander: AT+MWFRAGTHRESH=0 <enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MWFRAGTHRESH=<Fragmentation Threshold> Fragmentation Threshold: 0 Disabled 256-2346 Enabled with the value

AT+MWCCATHRESH

Syntaxe de la commande(Effet: AT&W)

AT+MWCCATHRESH=<CCA Threshold> CCA Threshold: Range of values: 4-127

La description

Get / Set Radio CCA Seuil.

Exemple

Network

TX bitrate

Mode

SSID

ΟK

Commander: AT+MWCCATHRESH=28 <enter> Réponse: OK

Radio Virtual Interface [0]:

ESSID Broadcast : Off AP Isolation : Off

: lan

:ap

: PWii Encryption Type : psk2 WPA PSK : 1234567890

: auto

AT+MWIFACE

La description	Syntaxe de la commande(Effet: AT&W)		
Liste / Ajouter / Supprimer interface virtuelle radio.	List one or all radio virtual interface(s) : AT+MWIFACE=0[,<index>]</index> Add one radio virtual interface :		
Exemple	AT+MWIFACE=1		
Commander: AT+MWIFACE=0 <enter> Réponse:</enter>	AT+MWIFACE=2, <index> Index: Radio Virtual Interface Index: 0-3</index>		

© Microhard 2016



AT+MWNETWORK

La description

Get / Set interface virtuelle radio: Réseau

Exemple

Commander: AT+MWNETWORK=0 <enter> Réponse: +MWNETWORK: Virtual Interface 0: 0 - LAN OK

Syntaxe de la commande(Effet: AT&W)

AT+MWNETWORK=[<Index>[,<Network>]] Index: Radio Virtual Interface Index: 0-3 Network: Radio Virtual Interface Network: 0 - LAN 1 - Ian1

Syntaxe de la commande(Effet: AT&W)

Radio Virtual Interface SSID: 1 - 63 character

AT+MWSSID=[<Index>[,<SSID>]]

Radio Virtual Interface Index: 0-3

Index:

SSID:

AT+MWSSID

La description

Get / Set interface virtuelle radio: SSID

Exemple

Commander: AT+MWSSID=0,MySSID <enter> Réponse: OK

AT+MWDEVICEMODE

La description

Obtenez interface virtuelle / radio Set: Mode

Exemple

Commander: AT+MWDEVICEMODE=0,0 <enter> Réponse: OK Syntaxe de la commande(Effet: AT&W)

AT+MWDEVICEMODE=[<Index>[,<Device Mode>]]

Index: Radio Virtual Interface Index: 0-3 Device Mode: Radio Virtual Interface Mode: 0 - Access Point 1 - Client

2 - Repeater



AT+MWRATE

la	des	crii	ntic	۱n
La	400	U 11	Juic	

Get / Set interface virtuelle radio: TX bitrate

Exemple

Commander: AT+MWTXRATE=0,0 <enter> Réponse: OK

Syntaxe de la commande(Effet: AT&W)

AT+MWRATE=[<Index>[,<TX bitrate>]]

Index: Radio Virtual Interface Index: 0-3 TX bitrate:

Radio Virtual Interface TX bitrate:

0 - auto

1 - mcs-0 2 - mcs-1

3 - mcs-2

4 - mcs-3

- 5 mcs-4
- 6 mcs-5

7 - mcs-6

8 - mcs-7

9 - mcs-8 10 - mcs-9

11 - mcs-10

12 - mcs-11

- 13 mcs-12
- 14 mcs-13
- 15 mcs-14
- 16 mcs-15

AT+MWWDS

Syntaxe de la commande(Effet: AT&W)

AT+MWWDS[=<Index>[,<WDS>]]

<Index> Radio Virtual Interface Index: 0-3 <WDS> 0 - Off 1 - On

AT+MWSSIDBCAST

La description

Get / Set interface virtuelle radio: diffusion du SSID.

Exemple

Commander: AT+MWSSIDBCAST=0,1 <enter> Réponse: OK Syntaxe de la commande(Effet: AT&W)

AT+MWSSIDBCAST=[<Index>[,<ESSID Broadcast>]]

Index: Radio Virtual Interface Index: 0-3 ESSID Broadcast: Radio Virtual Interface ESSID Broadcast: 0 - Off

1 - On

La description

Get / Set interface virtuelle radio: WDS

Exemple

Commander: AT+MWWDS=0,1 <enter> Réponse: OK



La description

Get / Set interface virtuelle radio: AP Isolation

Exemple

Commander: AT+MWAPISOLATION=0,0 <enter> Réponse: OK

AT+MWAPISOLATION

Syntaxe de la commande(Effet: AT&W)

AT+MWSSIDBCAST=[<Index>[,<AP Isolation>]] Index: Radio Virtual Interface Index: 0-3 AP Isolation: Radio Virtual Interface AP Isolation: 0 - Off 1 - On

AT+MWENCRYPT

La description

Obtenez interface virtuelle / radio Set: Type de chiffrement

Exemple

Commander: AT+MWENCRYPT=0,1,#microhard123 <enter> Réponse: OK

Commander: AT+MWENCRYPT> <enter> Réponse: +MWENCRYPT: Virtual Interface 0: Encryption Type: 1 - WPA (PSK) Password: #microhard123 OK Syntaxe de la commande(Effet: AT&W)

For PSK, AT+MWENCRYPT=[<Index>, [<Encryption Type>[,<PSK Password>]]]

For RADIUS, AT+MWENCRYPT=[<Index>, [<Encryption Type>[,<RADIUS Server Key> [,<RADIUS IP Address>,<RADIUS Port>]]]]

<Index>

Radio Virtual Interface Index: 0-3

<Encryption Type>

Radio Virtual Interface Encryption Type:

- 0 Disabled
- 1 WPA (PSK)
- 2 WPA2 (PSK)
- 3 WPA+ŴPAŹ (PSK)
- 4 WPA Enterprise (RADIUS)
- 5 WPA2 Enterprise (RADIUS)
- 6 WPA+WPA2 Enterprise (RADIUS)
- <PSK Password>:

Min 8 characters, Max 63 characters <RADIUS Server Key>:

Min 4 characters, Max 63 characters <RADIUS IP Address>:

Valid IP address

<RADIUS Port>:

Valid port 0 - 65535



AT+WSCAN

La description

Obtenez réseau radio des données de numérisation. (Doit être en mode client, scanne les réseaux disponibles).

Exemple

Commander: AT+WSCAN <enter> Réponse: Varies

Syntaxe de la commande

AT+WSCAN <enter>

AT+MWRSSI

La description

Obtenez radio (WIFI) RSSI.

Syntaxe de la commande AT+MWRSSI <enter>

Exemple

Commander: AT+MWRSSI <enter) Réponse: +MWRSSI: -76 dBm OK



Annexe A: Interface Série

Module (DCE)	Host (e.g. PC) (DTE)	Les flèches indiquent la direction que les signaux sont revendiqués (par exemple, DCD provient à la DCE, en informant le DTE qu'une porteuse est présente).
1	Signal $DCD \rightarrow$	IN	
2	$RX \rightarrow$	IN	L'interface est conforme à la RS-232 standard des signaux, de sorte que la
3	← TX	OUT	connexion directe a un PC note (par exemple) est loge.
4	\leftarrow DTR	OUT	
5	SG		
6	DSR \rightarrow	IN	
7	\leftarrow RTS	OUT	
8	CTS \rightarrow	IN	Les signaux de l'interface série asynchrone sont décrites ci-dessous:

- **DCD** Data Carrier Detect Sortie du module Lorsque affirmé (TTL bas), DCD informe la date à laquelle un lien de communication a été établie avec un autre appareil.
- **RX** Réception de données Sortie du module Signaux transférés des BulletPlus sont reçus par le DTE via RX.
- **TX** Transmettre des données Entrée de Module Les signaux sont transmis de la DTE via TX aux BulletPlus.
- **DTR** Data Terminal Ready Entrée de Module Affirmé (TTL bas) par les données pour informer le module qu'il est vivant et prêt pour les communications.
- SG Signal Ground Fournit une référence de masse pour tous les signaux émis par les deux DTE et DCE.
- **DSR** Data Set Ready Sortie du module Affirmé (TTL bas) par la DCE pour informer le DTE qu'il est vivant et prêt pour les communications. DSR est l'équivalent du module du signal DTR.
- **RTS** Demande d'envoi Entrée au module Un signal "handshake" qui est affirmé par le DTE (TTL bas) quand il est prêt. Lorsque handshaking matériel est utilisé, le signal RTS indique au DCE que l'hôte peut recevoir des données.
- **CTS** Clear to Send Sortie du module Un signal "handshake" qui est affirmé par la DCE (TTL bas) quand il a permis la communication et la transmission de la DTE peut commencer. Lorsque handshaking matériel est utilisé, le signal CTS indique à l'hôte que la DCE peut recevoir des données.

Notes: Il est typique de se référer à RX et TX du point de vue de l'DTE. Il faut garder à l'esprit quand on regarde les signaux relatifs au module (DCE); le module transmet des données sur la ligne RX, et reçoit le TX.

"DCE" et "module" sont souvent synonymes depuis un module est typiquement un dispositif DCE. "DTE" est, dans la plupart des applications, un dispositif tel qu'un PC hôte.



Annexe B: IP-Passthrough Exemple (Page 1 de 2)

En remplissant le processus de démarrage rapide, un utilisateur aurait dû être en mesure de se connecter et configurer les BulletPlus à travailler avec leur opérateur cellulaire. En remplissant ce, le modem est prêt à être utilisé pour accéder à Internet et fournir une connectivité mobile. Cependant, une application commune des BulletPlus est d'accéder à des périphériques connectés à distance. Pour ce faire, les BulletPlus doit être dit comment traiter le trafic entrant, où envoyer. Pour accomplir cela, il y a trois options:

- IP-Passthrough
- Port Forwarding
- DMZ (un type de Port Forwarding)

Dans cette section, nous allons parler de IP-Passthrough et comment configurer le BulletPlus et le périphérique / PC connecté à travailler avec IP-Passthrough. IP-Passthrough signifie que le BulletPlus est transparent, et tout à l'extérieur (WAN), le trafic est simplement envoyé directement à un seul périphérique connecté au LAN RJ-45 port physique sur le BulletPlus (À l'exception du port 80, qui est retenu pour la configuration à distance (configurable). en outre, tout le trafic qui est envoyé au port RJ45 est envoyé directement sur le port WAN et ne sont pas traitées par les BulletPlus.

IP-Passthrough est idéal pour les applications où un seul appareil est connecté au BulletPlus, et d'autres caractéristiques des BulletPlus ne sont pas nécessaires. En mode pass-through, la plupart des caractéristiques des BulletPlus sont contournés, ce qui inclut les ports série, les fonctions GPS, VPN, et bien plus encore. L'avantage de IP-Passthrough est que la configuration est très simple.

Dans l'exemple ci-dessous, nous avons un BulletPlus connecté à un PC (PC2). L'application nécessite que PC1 être en mesure d'accéder à plusieurs services sur le PC2. Utilisation de Port Forwarding cela nécessiterait une nouvelle règle créée pour chaque port, et quelques applications ou services peut nécessiter plusieurs ports donc cela nécessiterait plusieurs règles et les règles peuvent être différentes pour chaque installation, ce qui rend l'entretien futur difficile. Pour IP-passthrough, PC1 seulement besoin de connaître l'adresse IP publique statique du BulletPlus, l'BulletPlus serait alors attribuer automatiquement, via DHCP, l'adresse IP WAN du PC2 ci -joint, la création d'une connexion transparente.



Connectez-vous au BulletPlus (Reportez-vous à démarrage rapide), et veiller à ce que DHCP est activé sur le (modifier) la page Réseau> LAN.

DHCP Server Enable • Start 192.168.168.100 Limit 150 Lease Time (in minutes) 720

Étape 2

Depuis PC2 nécessite le port 80 pour être utilisé comme port de serveur Web, le port 80 ne peut être utilisé sur le BulletPlus, par défaut, il conserve ce port pour la configuration à distance. Pour modifier le port utilisé par le BulletPlus, accédez à la page Système> Services. Pour cette Exemple, nous allons le changer pour le port 8080. Lors de la modification des numéros de port sur les BulletPlus, il est recommandé de redémarrer l'unité avant de continuer, rappelez-vous le nouveau port de WebUI est maintenant 8080 lorsque vous vous connectez de nouveau dans le BulletPlus. (Par exemple 192.168.168.1:8080).

Services Statu	5		
FTP	●Enable ○Disable		Update
Telnet	⊙Enable ®Disable	Port 23	Update
SSH	⊙Enable ®Disable	Port 22	Update
Web UI	●HTTP/HTTPS ●HTTP ●HTTPS	Port 8080 HTTP/ 443 HTTPS	Update



Étape 3

microhard

Maintenant, IP-Passthrough peut être activé sur le BulletPlus. Sous l'onglet Transporteur> Paramètres, IP-Passthrough peut être trouvé. Pour activer cette fonction, sélectionnez "Ethernet" dans le menu déroulant. Une fois que les modifications sont appliquées, quel appareil est connecté physiquement au port LAN RJ45, sera dynamiquement être assigné l'adresse IP WAN. Dans ce Exemple, ce serait 74.198.186.193.

L'adresse IP par défaut de 192.168.168.1 sur le réseau local est plus disponible, mais il est toujours possible d'accéder et de configurer les BulletPlus sur le côté LAN, en utilisant l'adresse XXX1 IP, où les 3 premiers octets de l'IP WAN sont à la place de les X. (Par exemple 74.198.186.1, et rappelez-vous le port HTTP dans ce Exemple a été changé en 8080).

Le pare-feu doit être configuré et / ou des règles doit être créé pour permettre le trafic Carrier. Voir Firewall Exemple pour plus d'informations.

Étape 4

Fixer le dispositif à distance ou PC au port RJ45 du BulletPlus. Le dispositif final doit être mis en place pour DHCP pour obtenir une adresse IP à partir des BulletPlus. Dans la configuration de test / Exemple nous pouvons vérifier cela en regardant l'adresse IP actuelle. Dans la capture d'écran à droite, nous pouvons voir que l'ordinateur portable est connecté à l'BulletPlus a une adresse IP de 74.198.186.193, qui est l'adresse IP attribuer par le transporteur cellulaire pour le modem.

Étape 5 (Optionnel)

Opération IP-Passthrough peut également être vérifiée dans le BulletPlus. Une fois IP-Passthrough est activé, vous pouvez accéder à la BulletPlus WebUI par l'une des méthodes suivantes:

- À distance sur le côté WAN (généralement Internet), en utilisant l'adresse IP WAN, et le port spécifié pour le fonctionnement de HTTP (ou, si elle est activée, en utilisant le (443) ports HTTPS), dans ce Exemple avec serait 74.198.186.193:8080.
- Sur le côté LAN, en entrant dans les 3 premiers octets de l'adresse IP WAN et 0,1 pour le quatrième, donc dans notre Exemple 74.198.186.1:8080.

Une fois connecté, accédez au Carrier> page d'état. Dans le champ Adresse IP WAN, il devrait ressembler montré dans l'image à droite, 74.198.186.193 on LAN.

Connection Duration	1 min 43 sec
WAN IP Address	74.198.186.193 on LAN
DNS Server 1	64.71.255.198

Étape 6

La dernière étape consiste à vérifier le dispositif à distance peut être consulté. Dans ce Exemple d'un PC est connecté au port RJ45 du BulletPlus. Sur ce PC un serveur web apache simple est en cours d'exécution pour illustrer un système de fonctionnement. Sur un PC à distance, entrez l'adresse IP WAN des BulletPlus dans un navigateur web. Comme on le voit ci-dessous, lorsque l'adresse IP de l'BulletPlus est entré, les données sont transmises par l'intermédiaire du PC connecté. La capture d'écran ci-dessous montre que notre configuration de test a réussi.

Firefox	+		☆ ▼ C
This is the Web Server	Running on the Microh	ard Laptop.	
If you can read this, it means that the IP-Passthrough or Port Forwarding exercise works!			

JS Vé. General

Carrier Configuration



BulletPlus





Annexe C: Port Forwarding Exemple (Page 1 de 2)

En remplissant le processus de démarrage rapide, un utilisateur aurait dû être en mesure de se connecter et configurer les BulletPlus à travailler avec leur opérateur cellulaire. En remplissant ce, le modem est prêt à être utilisé pour accéder à Internet et fournir une connectivité mobile. Cependant, l'une des principales applications des BulletPlus est d'accéder aux périphériques connectés à distance. Pour ce faire, les BulletPlus doit être dit comment traiter le trafic entrant, où envoyer. Pour accomplir cela, il y a trois options:

- IP-Passthrough
- Port Forwarding
- DMZ (un type de Port Forwarding)

Dans la section précédente, nous avons illustré comment utiliser et la configuration IP-Passthrough. Dans cette section, nous allons parler de la redirection de port. La redirection de port est idéal quand il y a plusieurs appareils connectés au BulletPlus, ou si d'autres caractéristiques des BulletPlus sont nécessaires (ports série, Pare-feu, GPS, etc.). Dans le transfert de port, le BulletPlus regarde chaque paquet Ethernet entrant sur le réseau étendu et en utilisant le numéro de port de destination, détermine l'endroit où il va envoyer les données sur le réseau local privé. Le BulletPlus fait avec chaque paquet entrant.

DMZ (une forme de redirection de port) est utile pour les situations où il y a plusieurs appareils connectés au BulletPlus, mais tout le trafic entrant est destiné à un seul appareil. Il est également populaire à utiliser DMZ dans les cas où un seul appareil est connecté, mais plusieurs ports sont transmis et d'autres caractéristiques des BulletPlus sont nécessaires, car en mode passthrough toutes ces fonctionnalités sont perdues.

Prenons l'Exemple suivant. Un utilisateur dispose d'un emplacement distant qui a plusieurs dispositifs qui doivent être accessibles à distance. L'utilisateur à PC1 ne peut voir le BulletPlus directement en utilisant l'adresse IP statique publique attribué par le transporteur sans fil, mais pas les appareils derrière elle. Dans ce cas, le BulletPlus agit d'une passerelle entre le réseau cellulaire et le réseau local de ses appareils connectés. Utilisation de la redirection de port, nous pouvons tracer la voie que les données passe par le BulletPlus.



Connectez-vous au BulletPlus (Reportez-vous à démarrage rapide), et veiller à ce que le pare-feu est activé. Cela peut être trouvé sous Pare-feu> Général. Assurez-vous également que les règles que suffisantes ou des listes de propriété intellectuelle ont été mis en place pour permettre le trafic spécifique de passer par le BulletPlus. Voir le Pare-feu Exemple dans le prochain annexe pour obtenir des informations sur la façon d'autoriser les connexions à partir d'un IP ou d'ouvrir des ports. Une fois qui est complet, pensez à «Soumettre» les modifications

Firewall General Configuration				
WAN Remote Management 🔍	Enable Disable			
Carrier Remote Management	Enable Disable			
WAN Request 0	Block Allow			
Carrier Request 0	Block Allow			
LAN to WAN Access Control 0	Block Allow			

Annexe C: Port Forwarding Exemple (Page 2 de 2)

Étape 2

Déterminer quels ports externes (WAN) sont mappées sur les adresses IP internes et des ports (LAN). Il est important de comprendre quel port, accessible à l'extérieur, est connecté ou mappé sur lequel des dispositifs à l'intérieur. Pour cela, nous allons Exemple d'utiliser les ports suivants, dans ce cas, il est purement arbitraire ports sont affectés, certains systèmes peuvent être configurable, d'autres systèmes peuvent nécessiter des ports spécifiques à utiliser.

La description	WAN IP	Externe Port	Interne IP	Interne Port
BulletPlus WebUI	74.198.186.193	80	192.168.0.1	80
PC2 Web Serveur	74.198.186.193	8080	192.168.0.20	80
PLC Web Serveur	74.198.186.193	8081	192.168.0.30	80
PLC Modbus	74.198.186.193	10502	192.168.0.30	502
Camera Web Serveur	74.198.186.193	8082	192.168.0.40	80

Notez que l'utilisateur extérieur, l'adresse IP pour chaque périphérique est le même, seul le port change de numéro, mais sur le réseau local, chaque port externe est mappé à un numéro de périphérique et le port interne. Notez également que le numéro de port utilisé pour l'interface graphique de configuration pour tous les périphériques sur le réseau local est le même, cela est bien parce qu'ils sont situés sur des adresses IP différentes, et les différents ports externes mappés par le BulletPlus (80, 8080, 8081, 8082), envoie les données à la destination prévue.

Étape 3

Créer une règle pour chacune des lignes ci-dessus. n'a pas besoin de règles à créer pour la première ligne, car cela a été inscrit tout simplement pour montrer que le port externe 80 a déjà été utilisé, par défaut, par le BulletPlus lui-même. Pour créer des règles de transfert de port, Allez dans le menu Firewall> Port Forwarding. Lors de la création de règles, chaque règle exige un nom unique, ceci est seulement pour la référence et peut être quelque chose souhaitée par l'utilisateur. Cliquez sur le bouton "Ajouter Port Forwarding" pour ajouter chaque règle aux BulletPlus.

Une fois que toutes les règles ont été ajoutées, la configuration de BulletPlus devrait ressembler à ce qui est illustré dans la capture d'écran à droite. Assurezvous de «Soumettre» la liste Port Forwarding aux BulletPlus.

Pour de meilleurs résultats, redémarrez les BulletPlus.

Étape 4

Configurez les adresses statiques sur tous les périphériques connectés. La redirection de port exigé que tous les périphériques connectés ont des adresses IP statiques, ce veiller à ce que les règles de redirection de port sont toujours correctes, que la modification des adresses IP sur les périphériques connectés rendrait les règles configurées inutile et le système ne fonctionnera pas.

Étape 5

Testez le système. Les appareils connectés aux BulletPlus devraient être accessibles à distance. Pour accéder aux périphériques:

Pour le serveur Web sur le PC, utilisez un navigateur pour se connecter à 74.198.186: 193: 8080, dans ce cas, le même serveur Web est en cours d'exécution comme dans le IP-Passthrough Exemple, de sorte que le résultat devrait être comme suit:

Pour accéder aux autres appareils / services: Pour l'automate Web Server: 74.198.186.193:8081, pour la caméra 74.198.186.193:8082, et pour le Modbus sur le telnet PLC pour 74.198.186.193:10502 etc.

Firefox T http://74.198.186.193:8080/	+ second logs best	Barthouthy Sophist.	(married and a state of the second se	
74.198.186.193:8080				☆ マ C ^a
This is the Web Server l	Running on the M	icrohard Laptop.		
If vou can read this, it n	neans that the IP-J	Passthrough or Port	t Forwarding exerci	se works!

NamePC2_WSSourceCarrier ▼Internal Server IP192.168.0.20Internal Port80ProtocolTCP ▼External Port8080Add Port Forwarding

Firewall Port Forwarding Configuration

ewall Port Forwarding Summary					
Name	Source	Internal IP	Internal Port	Protocol	External Port
PC2_WS	Carrier 🔻	192.168.0.20	80	TCP V	8080
PLC_WS	Carrier 🔻	192.168.0.30	80	TCP V	8081
PLC_modebus	Carrier 🔻	192.168.0.30	502	TCP V	10502
Camera	Carrier V	192.168.0.40	80	TCP V	8082


Annexe D: VPN Exemple (Page 1 de 2)

En remplissant le processus de démarrage rapide, un utilisateur aurait dû être en mesure de se connecter et configurer les BulletPlus à travailler avec leur opérateur cellulaire. En remplissant ce, le modem est prêt à être utilisé pour accéder à Internet et fournir une connectivité mobile. Cependant, l'une des principales applications des BulletPlus est d'accéder aux périphériques connectés à distance. En plus de Port Forwarding et IP-Passthrough, l'BulletPlus dispose de plusieurs fonctionnalités VPN, la création d'un tunnel entre deux sites, ce qui permet à des périphériques distants sont accessibles directement.

VPN permet à plusieurs dispositifs d'être connectés aux BulletPlus sans la nécessité de cartographier individuellement ports à chaque appareil. Accès complet aux périphériques distants est disponible lors de l'utilisation d'un tunnel VPN. Un tunnel VPN peut être créé à l'aide de deux dispositifs de BulletPlus, chacun avec une adresse IP publique. Au moins un des modems nécessitent une adresse IP statique. tunnels VPN peuvent également être créés en utilisant les BulletPlus aux dispositifs existants VPN capables, tels que Cisco ou Firebox.

Exemple: BulletPlus à BulletPlus (site à site)



Étape 1

Connectez-vous à chaque BulletPlus (Reportez-vous à démarrage rapide) et veiller à ce que le pare-feu est configuré. Cela peut être trouvé sous Pare-feu> Général. Veiller à ce que les règles suffisantes ou des listes de propriété intellectuelle ont été mis en place pour permettre le trafic spécifique de passer par le BulletPlus. Une fois que est terminée, rappelez-vous "Appliquer" les modifications.

Étape 2

Configurez l'adresse IP LAN et sous-réseau pour chaque BulletPlus. Les sous-réseaux doivent être différents et ne peuvent pas se chevaucher.

Site A

Site B

letwork LAN Configuration		Network LAN Configuration	
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



Annexe D: VPN Exemple (Page 2 de 2)

Étape 3

Ajouter une passerelle VPN Gateway tunnel sur chaque BulletPlus.

System	Network	Carrier	Wire	eless	Firew	vall	VPN	Router	Serial	I/0	GPS	Apps	Diag	Admin	
Summary	Gatewa	y To Gate	way	L2TP	Client	Оре	enVPN	Server	OpenVPI	l Clien	t L2T	P Users	Certi	ficates	
Summar	/														
Gateway	To Gateway														
Add	Name Status	Phase2 Enc/Au	ith/Grp	Int	terface	Local G	Group	Remote Grou	p Remote	Gateway	RX/1	TX Bytes	Tunnel To	est Confi	g.



Étape 4

Soumettre des modifications à deux unités. Il devrait être possible de faire un ping et d'atteindre des dispositifs à chaque extrémité du tunnel VPN si les deux appareils ont été configurés correctement et disposer d'une connectivité réseau.



Annexe E: Pare-feu Exemple (Page 1 de 2)

En remplissant le processus de démarrage rapide, un utilisateur aurait dû être en mesure de se connecter et configurer les BulletPlus à travailler avec leur opérateur cellulaire. En remplissant ce, le modem est prêt à être utilisé pour accéder à Internet et fournir une connectivité mobile. Cependant, l'une des principales applications des BulletPlus est d'accéder aux périphériques connectés à distance. La sécurité joue un rôle important dans les déploiements M2M comme dans la plupart des cas, le modem est publiquement disponible sur Internet. Limiter l'accès à l'BulletPlus est primordiale pour un déploiement sécurisé. Les fonctionnalités de pare-feu des BulletPlus permettent à un utilisateur de limiter l'accès aux BulletPlus et les dispositifs qui lui sont connectés par les moyens suivants

- Règles personnalisables
- Et / Liste IP ou MAC
- (Access Control List) ACL ou Blacklist en utilisant les outils ci-dessus.

Prenons l'Exemple suivant. Un BulletPlus est déployé sur un site distant pour recueillir des données à partir d'un dispositif terminal tel qu'un PLC ou RTU connecté au port de données série (Port 20001). Il est nécessaire que seul un hôte spécifique (hôte A) ont accès aux BulletPlus déployés et les périphériques attachés, y compris les fonctions de gestion à distance.



Étape 1

Connectez-vous à la BulletPlus (Reportez-vous à démarrage rapide). Accédez à l'> onglet Général Pare-feu, comme indiqué ci-dessous et bloquer tout le trafic du transporteur en réglant le transporteur Demande de bloc, et désactiver la gestion à distance des transporteurs. Assurez-vous d'appliquer les paramètres. À ce stade, il devrait être impossible d'accéder aux BulletPlus de la connexion cellulaire.

Firewall General Configuration		
WAN Remote Management 🔍	Enable O Disable	
Carrier Remote Management 0	Enable Disable	
WAN Request 0	Block Allow	
Carrier Request 0	Block Allow	
LAN to WAN Access Control 0	Block I Allow	
LAN to Carrier Access Control 0	Block I Allow	
Anti-Spoof 0	Enable Isable	
Packet Normalization 🕕	Enable Isable	



Annexe E: Firewall Exemple (Page 2 de 2)

Étape 2

Sous l'onglet Règles, nous devons créer deux nouvelles règles. Une règle pour permettre à l'hôte A accès au port de gestion à distance (port TCP 80), et un autre pour accéder au périphérique connecté au port série (port TCP 20001).

Règle 1	Firewall Rules		
	Firewall Rules Configuration	1	
	Rule Name	Rem_Mgt	
	ACTION	Accept V	
	Source 🕕	Carrier •	
	Source IPs 🕚	IP range	
		184.71.46.126 To	184.71.46.126
	Destination 🕕	None •	
	Destination IPs 🕕	IP range Subnet / prefix	
		0.0.0.0 To	255.255.255.255
	Destination Port 🕕	80	
	Protocol	TCP V	
	Add Rule		
	5. H.S. I		
Póalo 2	Firewall Rules		
Negle Z	· · · · · · · · · · · · · · · · · · ·		
Negle 2	Firewall Rules Configuration		
Regie Z	Firewall Rules Configuration Rule Name	Device	
itegie 2	Firewall Rules Configuration Rule Name ACTION	Device	
Negle 2	Firewall Rules Configuration Rule Name ACTION Source 🖤	Device Accept ▼ Carrier	
Negle 2	Firewall Rules Configuration Rule Name ACTION Source T Source T	Device Accept Carrier IP range Subnet / prefix	
Keyle 2	Firewall Rules Configuration Rule Name ACTION Source IPs I	Device Accept V Carrier V IP range Subnet / prefix 184.71.46.126 To	184.71.46.126
	Firewall Rules Configuration Rule Name ACTION Source • Source IPs • Destination •	Device Accept V Carrier V IP range Subnet / prefix 184.71.46.126 None V	184.71.46.126
	Firewall Rules Configuration Rule Name ACTION Source • Source IPs • Destination • Destination IPs •	Device Accept V Carrier V IP range Subnet / prefix 184.71.46.126 None V IP range Subnet / prefix	184.71.46.126
	Firewall Rules Configuration Rule Name ACTION Source • Source IPs • Destination • Destination IPs •	Device Accept V Carrier V IP range Subnet / prefix 184.71.46.126 None V IP range Subnet / prefix 0.0.0.0 To	184.71.46.126 265.265.265.255
	Firewall Rules Configuration Rule Name ACTION Source • Source IPs • Destination • Destination IPs • Destination Port •	Device Accept V Carrier V © IP range © Subnet / prefix 184.71.46.126 To None V © IP range © Subnet / prefix 0.0.0.0 To 20001	184.71.46.126 265.265.265.255
	Firewall Rules Configuration Rule Name ACTION Source • Source IPs • Destination • Destination IPs • Destination Port • Protocol	Device Accept V Carrier V © IP range © Subnet / prefix 184.71.46.126 To None V © IP range © Subnet / prefix 0.0.0.0 To 20001 TCP V	184.71.46.126 265.255.255.255

Après chaque règle est créée assurez-vous de cliquer sur le bouton Ajouter une règle, une fois les deux règles sont créées sélectionnez le bouton Soumettre pour écrire les règles aux BulletPlus. Le résumé des règles de pare-feu devrait ressembler à ce qui est indiqué ci-dessous.

Firewall	Rules Sumr	mary								
Name	Action	Src	Src IP From	Src IP To	/Prefix Dest		Dest IP From	Dest IP To	/Prefix Dest Port	Protocol
Rem_Mg	t Accept 🔻	Carrier	184.71.46.126	184.71.46.126	None	۲	0.0.0.0	255.255.255.25	80	TCP • Remove
Device	Accept 🔻	Carrier	184.71.46.126	184.71.46.126	None	۲	0.0.0.0	255.255.255.25	20001	TCP • Remove

Étape 3

Testez les connexions. Le BulletPlus ne doit autoriser les connexions au port spécifié de l'hôte A. Un autre moyen de limiter les connexions à l'BulletPlus à une adresse IP spécifique aurait été d'utiliser l'outil Liste MAC-IP. En utilisant les règles, nous pouvons non seulement limiter spécifique IP, mais nous pouvons aussi spécifier des ports qui peuvent être utilisés par une adresse IP autorisée.



Annexe F: Port Forwarding avec IP-Passthrough (Page 1 de 2)

Lorsque le BulletPlus est réglé en mode IP-Passthrough le modem passe tout le trafic sur le périphérique connecté à l'exception de WebUI, SNMP et les règles de transfert de port interne. L'Exemple suivant montre comment utiliser la redirection de port à utiliser les capacités Iperf internes du modem tout en conservant les caractéristiques restantes de IP-Passthrough.

Étape 1: Activer IP-Passthrough

Syst	em Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/O	GPS	Apps	Diag	Admin	
Stat	us Settings S	MS SMS	Config Dat	aUsage									
Car	rier Configurati	on											
Ge	eneral												
	Carrier status 🛈		Enal	ble 🗘									
	Connectivity Mana	gement 0	Auto	D ‡									
Г	IP-Passthrough		Ethe	ernet 🌲									
	MTU Size(500~150	00/Blank) 🔍											
	Lease Time (in m	inutes) 0	2										
	Virtual IP Address	5 🛈	192.1	168.168.1									
	SIM Selection		Dua	l SIM Cards	*								

Après le mode pass-through IP est activé, l'adresse IP du réseau LAN est changé en 184.151.218.1

Étape 2. Ajouter Port Forwarding

A) Indiquez l'adresse IP interne et le port de redirection de port. Nous démontrons avant le port 5001, qui est le port par défaut Iperf.

Syst	em N	letwork	Carrier	Wireless	Firewall	VPN	Router	Serial	I/O	GPS	Apps	Diag	Admin	
Sum	mary	General	Port For	warding	MAC-IP List	Rules	Firewa	ll Defaul	t					
Fire	ewall P	ort Forwa	arding											
Fir	rewall Po	ort Forward	ding Summa	iry										
	Name	Source	Internal I	P		Internal	Port			Protoc	ol Exte	rnal Port		SNAT
Г	forward]	Carrier	\$ 184.151	.218.1		5001				ТСР	\$ 500)1		No

Utilisez l'adresse IP de l'interface LAN que IP interne du serveur.

B) Autoriser le trafic entrant. Méthode 1: Autoriser tout le trafic entrant sur le support. (Non recommandé)

System Netw	work Carrie	r Wireles	s Firewall	VPN	Router	Serial	I/O	GPS	Apps	Diag	Admin	
Summary Ger	neral Port F	orwarding	MAC-IP List	Rules	Firewa	ll Defaul	t					
Firewall Gene	eral											
Firewall Gener	ral Configuration	n										
WAN Remot	te Management	0 0	Enable 🔿 Disal	ble								
Carrier Rem	note Managemer	nt 🛈 🛛 💿	Enable 🔿 Disal	ble								
WAN Reque	st 🛈	۲										
Carrier Requ	uest 🛈	0	Block 🖲 Allow]								
LAN to WAN	Access Control	0	Block 🖲 Allow	_								
LAN to Carr	ier Access Contr	rol 🛈 🛛 🔿	Block 🖲 Allow									
Anti-Spoof	Ð	0	Enable 🖲 Disal	ble								
Packet Norr	nalization 0	0	Enable 🖲 Disal	ble								



Annexe F: Port Forwarding with IP-Passthrough (Page 2 de 2)

System Network Carrier Wireless Firewall VPN Router Serial 1/0 GPS Apps Diag Admin Summary General Port Forwarding MAC-IP List Rules Firewall Default Firewall MAC//P List Firewall MAC//P List Firewall MAC List Configuration Name mac1 Action Accept 1 Mac Address 00:00:00:00:00:00 Add Mac List Firewall IP List Configuration Name [p1] Action Accept 1 0.0.0 / Prefix 0.0.0 Add IP List Firewall MAC List Summary Name Action Source IP / 0.0.0 0.0.0 / Firewall MAC List Summary Name Action Source IP / 0.0.0 Prefix Nac Address Firewall IP List Summary Name Action Source IP / 0.0.0 Image: Action Source Mac Address Firewall IP List Summary Name Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source IP / Image: Action Source I	Méthode	2: Spécifi	iez la sol	urce Adres	ses IP sont	autoris	sés.						
Summary General Port Forwarding MAC-IP List Rules Firewall Default Firewall MAC//P List Firewall MAC//P List Name Action Accept 2 Mac Address 00:00:00:00:00:00:00 Add Mac List Firewall IP List Configuration Name Ip1 Action Accept 2 Source IP / 0.0.0 / Add IP List Firewall MAC List Summary Name Action Source IP / 0.0.0 / Add IP List Firewall IP List Summary Name Action Source IP / 0.0.0 / Prefix Action Source Summary Firewall IP List Summary Name Action Source IP / 0.0.0 / Ip I Action Source IP / 0.0.0 / Ip I Action Source IP / Ip I Action Source IP / Ip I Action Source IP / Ip I Action Source IP / Ip I Action Source IP / Ip I Ip I <th>System</th> <th>Network</th> <th>Carrier</th> <th>Wireless</th> <th>Firewall</th> <th>VPN</th> <th>Router</th> <th>Serial</th> <th>I/O</th> <th>GPS</th> <th>Apps</th> <th>Diag</th> <th>Admin</th>	System	Network	Carrier	Wireless	Firewall	VPN	Router	Serial	I/O	GPS	Apps	Diag	Admin
Firewall MAC/IP List Image: Imag	Summary	General	Port Fo	rwarding	MAC-IP List	Rules	Firewa	ll Defaul	t				
Firewall MAC List Configuration Name Action Accept 2 Mac Address 00:00:00:00:00:00 Add Mac List Firewall IP List Configuration Name Action Accept 2 Source 0 LAN Source 1P / 0.0.0.0 / Firewall MAC List Summary Name Action Source 1P / 0.0.0.0 / Firewall MAC List Summary Name Action Source 1P / 0.0.0.0 / Firewall IP List Summary Name Action Source 1P / 0.0.0.0 / Firewall IP List Summary Name Action Source 1P / Accept 2 (p1 Accept 2) (p2 Accept 2)	Firewall	MAC/IP Li	st										
Name mac1 Action Accept : Mac Address 00:00:00:00:00 Add Mac List Firewall IP List Configuration Name ip1 Accept : Source IP / 0.0.0.0 / Prefix IP List Summary Firewall IP List Summary Name Action Source Mac Address Firewall IP List Summary Name Action Source Name Action Source Mac Address Firewall IP List Summary Name Action Source Source Name Action Source Source Name Action Source Mac Address Firewall IP List Summary Name Action Source <	Firewall	MAC List Co	nfiguratior	1									
Action Accept ‡ Mac Address 00:00:00:00:00 Add Mac List	Name			ma	c1								
Mac Address 00:00:00:00:00:00 Add Mac List Firewall IP List Configuration Name ip1 Action Accept ‡ Source ① LAN Source ② LAN Prefix ③ 0.0.0.0 / / Firewall MAC List Summary Name Action Source ③ Last Mac Address Firewall IP List Summary Name Action Source ③ Mac Address Firewall IP List Summary Name Action Source ③ Source Mac Address Firewall IP List Summary Name Action Source ③ Source Yame Action Source ③ Source Yama Yama Yama Yama <	Action	i		Ac	cept 💲								
Add Mac List Firewall IP List Configuration Name ip1 Action Accept : Source () LAN () Add IP List	Mac A	ddress		00:0	00:00:00:00:00)							
Firewall IP List Configuration Name ip1 Action Accept : Source IAN Source IAN Source IP / 0.0.0.0 Prefix 0.0.0.0 Add IP List Jaccept Mare Action Source Mac Address Firewall IP List Summary Name Action Source Mac Address Firewall IP List Summary Source Source Prefix 191 Accept : Carrier : 184.71.46.138 32 Remove IP List	Add	Mac List											
Name ip1 Action Accept : Source • LAN : Source IP / 0.0.0.0 Prefix • 0.0.0.0 Add IP List Firewall MAC List Summary Name Action Source Mac Address Firewall IP List Summary Name Action Source Mac Address Firewall IP List Summary Name Action Src Src IP Prefix ip1 Accept : Carrier : 184.71.46.138 32	Firewall	IP List Confi	guration										
Action Accept : Source : LAN : Source : IAN : Source : 0.0.0.0 Prefix : 0.0.0.0 Add IP List	Name	į	p1										
Source IP /	Action		Accept 🗧	:									
Source IP / Prefix 0 0.0.0.0 / Add IP List / // Firewall MAC List Summary Mac Address Firewall IP List Summary // Name Action Source Mame Action Src Source Mac Address Firewall IP List Summary ////////////////////////////////////	Source	e 🛈 🛛	LAN	÷									
Prefix Image: Constraint of the second s	Source	eIP/	0.0.0.0		1								
Add IP List Firewall MAC List Summary Name Action Source Mac Address Firewall IP List Summary Source Mac Address Name Action Src Src IP Prefix ip1 Accept ‡ Carrier 184.71.46.138 32 Remove IP List	Prefix	•											
Firewall MAC List Summary Mare Action Source Mac Address Firewall IP List Summary Mare Address Name Action Src Src IP Prefix ip1 Accept 1 Carrier 1 184.71.46.138 32 Remove IP List	Add	IP List											
Name Action Source Mac Address Firewall IP List Summary Name Action Src Src IP Prefix ip1 Accept 1 Carrier 184.71.46.138 32 Remove IP List	Firewall	MAC List Su	mmary										
Firewall IP List Summary Name Action Src Src IP Prefix ip1 Accept ‡) Carrier 184.71.46.138 32 Remove IP List	Name	Act	ion s	Source			Mac Address						
Name Action Src Src IP Prefix ip1 Accept \$ Carrier 184.71.46.138 32 Remove IP List	Firewall	IP List Sumr	nary										
ip1 Accept \$ Carrier \$ 184.71.46.138 32 Remove IP List	Name	Acti	ion s	Src			Src IP			Pr	efix		
	ip1	Ac	cept 拿	Carrier	÷		184.7	1.46.138		3	2	Remo	ve IP List

La requête entrante sur le port 5001 du transporteur ne transmettra pas à l'appareil derrière le modem, le serveur lperf en cours d'exécution sur le modem va maintenant obtenir cette requête entrante.



Annexe G: Dépannage

Ci-dessous un certain nombre de questions communes de soutien qui sont posées sur les BulletPlus. Le but de la section est de fournir des réponses et / ou des directives sur la façon de résoudre des problèmes communs avec les BulletPlus.

Question: Pourquoi ne puis-je pas me connecter à l'Internet / réseau?

Réponse: Pour vous connecter à Internet une carte SIM émise par le transporteur sans fil doit être installé et l'APN programmé dans la configuration porteuse des BulletPlus. Pour obtenir des instructions sur la façon de se connecter aux BulletPlus se référer à la mise en route rapide.

Question: Quelle est l'adresse IP par défaut des BulletPlus?

Réponse: L'adresse IP par défaut pour le (connecteur RJ45 à l'arrière de l'unité) LAN est 192.168.168.1.

Question: Quelle est la connexion par défaut pour les BulletPlus?

Réponse: Le nom d'utilisateur par défaut est admin, le mot de passe par défaut est admin.

Question: Quelles informations dois-je obtenir de mon opérateur de téléphonie mobile pour mettre en place les BulletPlus?

Réponse: L'APN est nécessaire pour configurer les BulletPlus pour communiquer avec un opérateur sans fil. Certains transporteurs exigent également un nom d'utilisateur et mot de passe. L'APN, le nom d'utilisateur et mot de passe ne sont disponibles auprès de votre opérateur de téléphonie mobile.

unités les plus récents peuvent soutenir une fonction APN AUTO, qui va tenter de déterminer l'APN à partir d'une liste préconfigurée de transporteurs et couramment utilisés APN de. Ceci est conçu pour fournir une connectivité réseau rapide, mais ne fonctionnera pas avec le secteur privé APN de. Le succès avec AUTO APN varie selon le transporteur.

Question: Comment puis-je réinitialiser mon modem aux paramètres d'usine par défaut?

Réponse: Si vous êtes connecté au BulletPlus accédez au Système> Maintenance Tab. Si vous ne pouvez pas vous connecter, allumez le BulletPlus et attendre que le voyant d'état dans le solide (ne clignote pas). Appuyez et maintenez enfoncé le bouton CONFIG jusqu'à ce que l'appareil redémarre (environ 8-10 secondes).

Question: Je peux connecter le transporteur, mais je ne peux pas accéder à Internet / WAN / réseau à partir d'un PC connecté?

Réponse: Assurez-vous que vous avez activé DHCP ou manuellement une IP valide, sous-réseau, la passerelle et le DNS définis sur le périphérique local.

Question: Je me suis connecté un périphérique au port série des BulletPlus et rien ne se passe?

Réponse: En plus des paramètres série de base du port, le protocole de configuration IP doit être configuré. Reportez-vous aux pages de configuration série pour une description La des différentes options.



Annexe G: Troubleshooting

Question: Comment puis-je accéder aux périphériques derrière le modem à distance?

Réponse: Pour les dispositifs d'accès derrière les BulletPlus à distance, plusieurs méthodes peuvent être utilisées:

A. IP Passthrough - Le BulletPlus est transparent et l'appareil connecté peut être directement accès. Se référer à IP-Passthrough Annexe pour une Exemple détaillé de la façon dont cela peut être déployé.
B. Port Forwarding / DMZ - ports WAN externes individuels sont mappés sur LAN interne IP et des ports. Voir le Port-Forwarding Annexe pour une Exemple détaillé.

C. VPN - Un tunnel peut être créé et un accès complet aux périphériques distants peuvent être obtenus. Required l'utilisation de plusieurs modems ou routeurs VPN. Voir l'Annexe VPN sur un exemple de la façon de mettre en place un VPN.

Question: J'ai accès Internet / Transporteur mais je ne peux pas cingler l'appareil à distance?

Réponse: Assurez-vous que les règles ont été approprie créé dans le pare-feu pour autoriser le trafic.

Question: Je suis en utilisant IP-Passthrough mais les ports série ne fonctionnera pas?

Réponse: Lorsque vous utilisez IP-Passthrough, l'IP transporteur est affecté à l'appareil connecté au port Ethernet, tout le trafic est passé à travers à ce dispositif. Comme un port résultat des publications en série ne fonctionnera pas. Le seul port ne pas être passé à travers le port de gestion à distance (port 80 par défaut), qui peut être modifié dans les paramètres de sécurité.

Question: Je suis en utilisant IP-Passthrough mais le modem ne prendrai pas mes paramètres de parefeu?

Réponse: Lorsque vous utilisez IP-Passthrough, l'IP transporteur est affecté à l'appareil connecté au port Ethernet, tout le trafic est passé à travers à ce dispositif. Par conséquent, les paramètres de pare-feu n'a aucun effet sur l'unité, et est automatiquement désactivé.

Question: Pourquoi mon modem ne réinitialise toutes les 10 minutes (ou autre moment)?

Réponse: Il y a un certain nombre de processus dans le BulletPlus qui assurent que l'unité communique à tout moment, et si un problème est détecté pour redémarrer le modem pour tenter de résoudre les problèmes:

1. Keepalive - Les tentatives de communiquer avec un hôte configuré sur une base définie. Redémarrera modem si l'hôte est inaccessible. Activé par défaut pour tenter de faire un ping 8.8.8.8. Il peut être nécessaire de désactiver sur les réseaux privés, ou fournir une adresse accessible à vérifier. Accès via Système> Keepalive.

2. Moniteur de périphérique local - Le BulletPlus surveillera un dispositif local, si ce dispositif ne présente les BulletPlus peut redémarrer. Applications> LocalMonitor.

Question: Comment puis-je configurer VPN?

Réponse: Se reporter à l'Annexe VPN pour un exemple.



1010101



101010101 BulletPlus

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

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