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

Informations Utilisateur

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.

Limitations de la garantie

MICROHARD SYSTEMS INC. NE DONNE AUCUNE GARANTIE DE QUELQUE NATURE QU'ELLE SOIT, EXPRESSE OU IMPLICITE, 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 DE CORRIGER TOUT DÉFAUT DANS LE MATÉRIEL, LES 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 MARCHANDE 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, INDIRECTS, ACCESSOIRES, INTERRUPTION DES ACTIVITÉS, CATASTROPHIQUE, PUNITIFS OU AUTRES DOMMAGES 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

WARNING

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.

WARNING

MAXIMUM EIRP
FCC 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.

WARNING

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 captures 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

Table des Matières

Table des Matières

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
- Voice over IP (VoIP)
- Faciliter les communications sans fil inter-réseaux
- la migration de réseau Legacy / périphérique
- SCADA (automates, Modbus, Hart)

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

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

Consommation de courant :
(@12VDC)

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

Spécifications générales (suite)

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

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 : 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

2.0 Démarrage Rapide

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)

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.

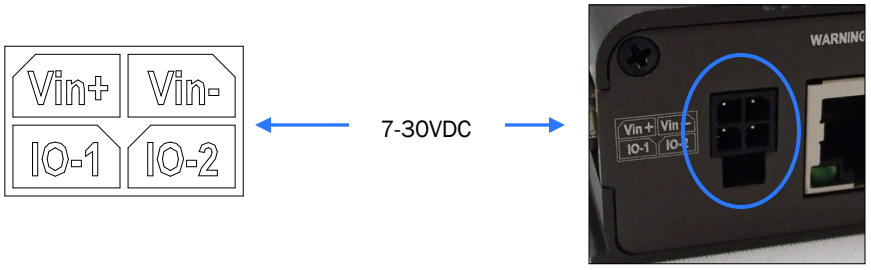
Emplacement pour carte SIM

2.2 Mise en route avec Cellular

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

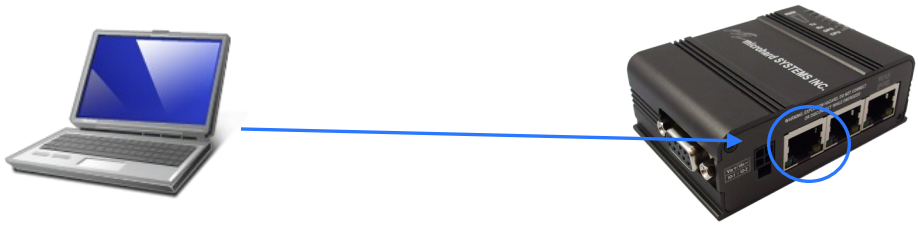
Utilisez l'adaptateur secteur fourni ou NHS une source de puissance équivalente. L'appareil peut également être alimenté par PoE à l'aide d'un injecteur PoE MHS.

✓ 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.

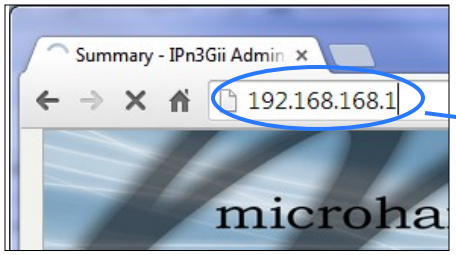


2.0 Démarrage Rapide

✓ 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 d'adresse.

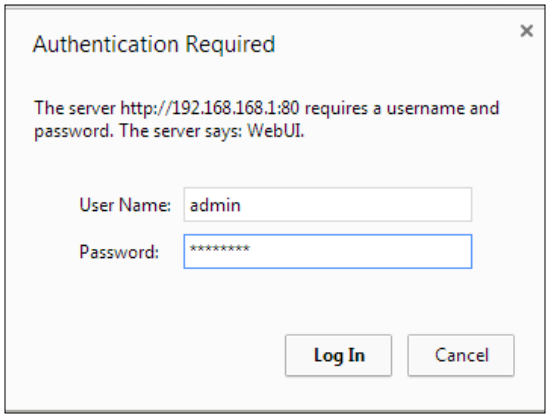


192.168.168.1

Les paramètres réseau par défaut:

IP: 192.168.168.1
Subnet: 255.255.255.0
Passerelle: 192.168.168.1

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



La connexion par défaut d'usine:

Nom d'utilisateur: admin
Mot de passe: admin

Comme la version firmware v1.3.0 -R1014 vous devrez changer le mot de passe par défaut lorsque vous vous connectez pour la première fois.

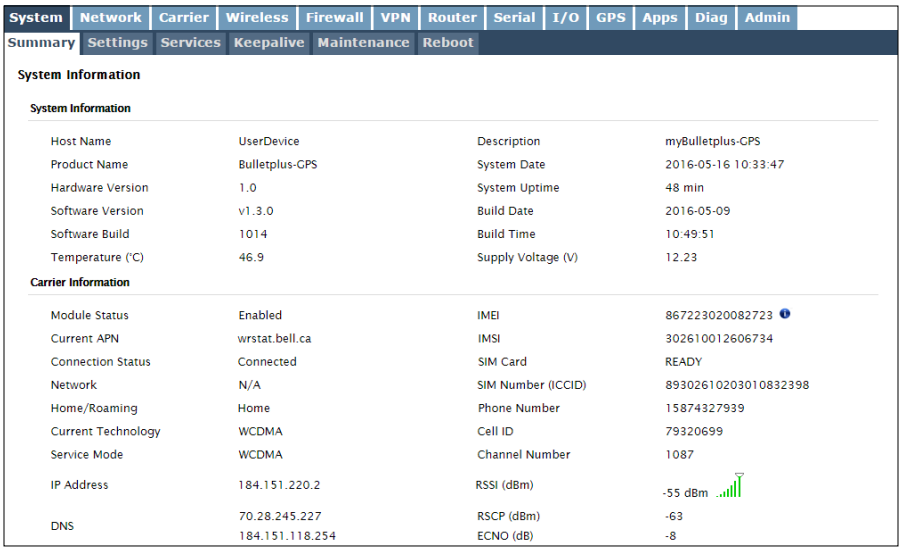
La connexion par défaut:

Nom d'utilisateur: admin
Subnet: admin

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

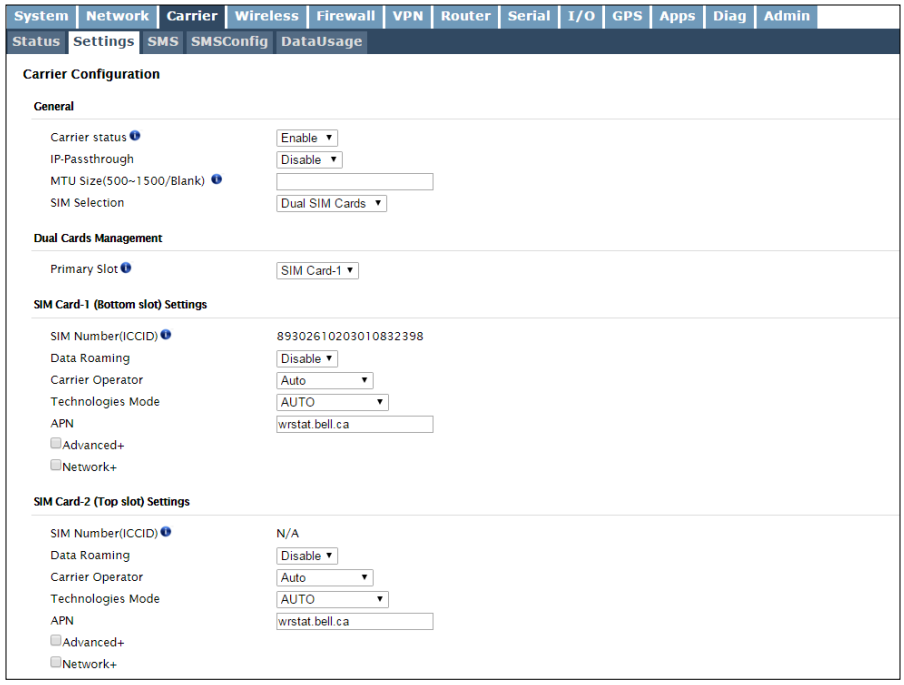
2.0 Démarrage Rapide

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



✓ 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.

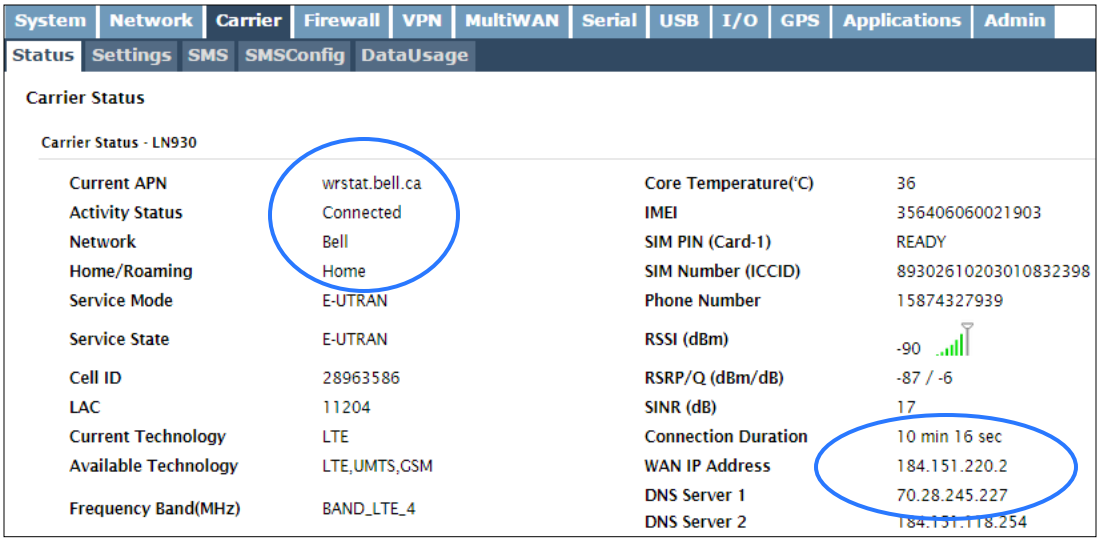
Auto APN: Le Bullet Plus va tenter de détecter le transporteur basé sur la carte SIM installée et faire défiler une liste d'APNs couramment utilisées pour fournir une connectivité réseau rapide.



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

2.0 Démarrage 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».



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

✓ 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.

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

✓ **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.)**

3.0 Caractéristiques Matérielles

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.

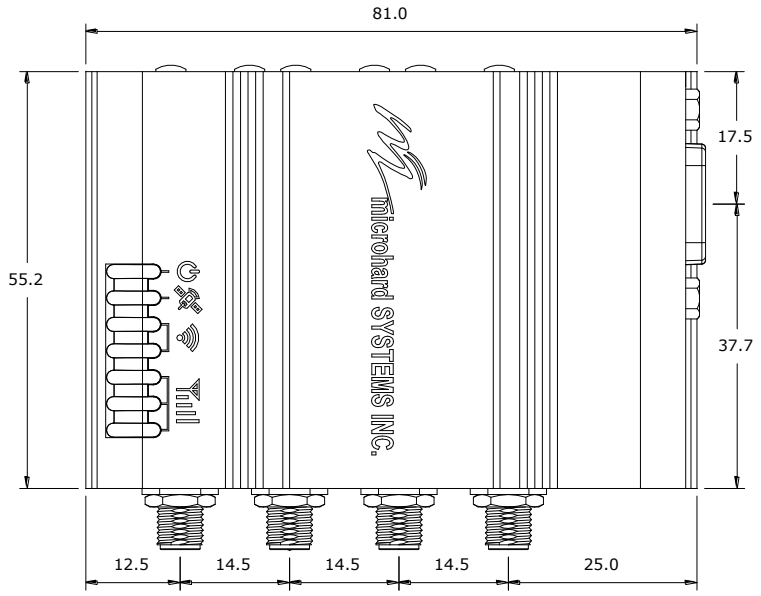
Image 3-1: BulletPlus

Les balles plus Hardware caractéristiques comprennent:

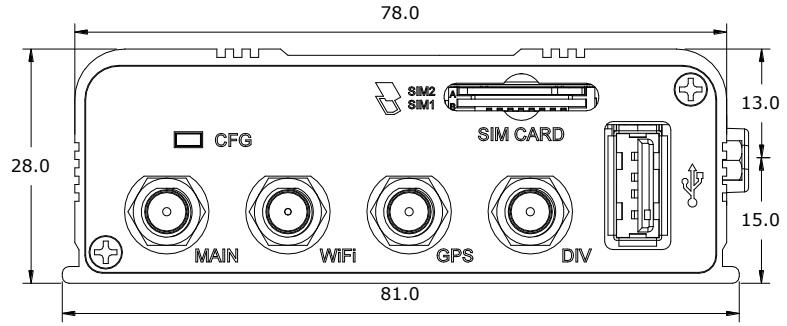
- Connecteurs standard pour:
- 3x ports 10/100 Ethernet (RJ45 - 1xWAN / 2xLAN)
- Port de données (RS232 / DB9)
- 4-Pin: MATE-N-LOK Type de connecteur pour Power / I / O 1/2
- Antenne cellulaire (Connexion SMA femelle Antenne x2)
- Antenne GPS (SMA femelle Raccordement de l'antenne)
- WiFi Antenna (RP-SMA 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

3.0 Caractéristiques Matérielles

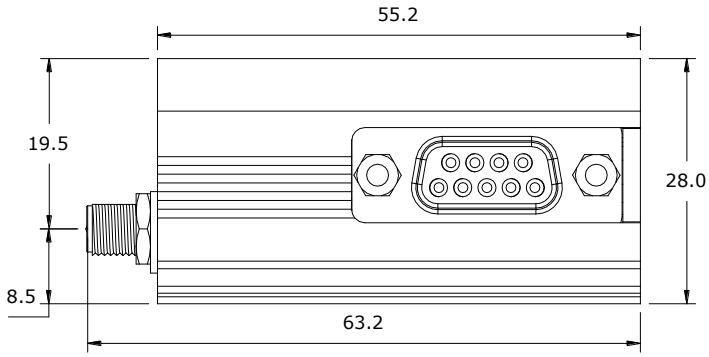
3.1.1 Dessins Mécaniques



Dessin 3-1: BulletPlus Top Voir Dimensions



Dessin 3-2: BulletPlus Retour Voir Dimensions

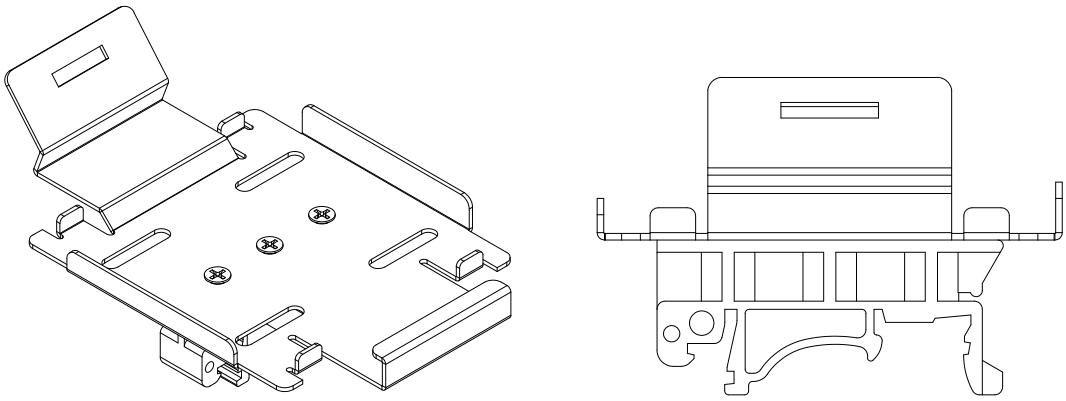


Dessin 3-3: BulletPlus Side View Dimensions

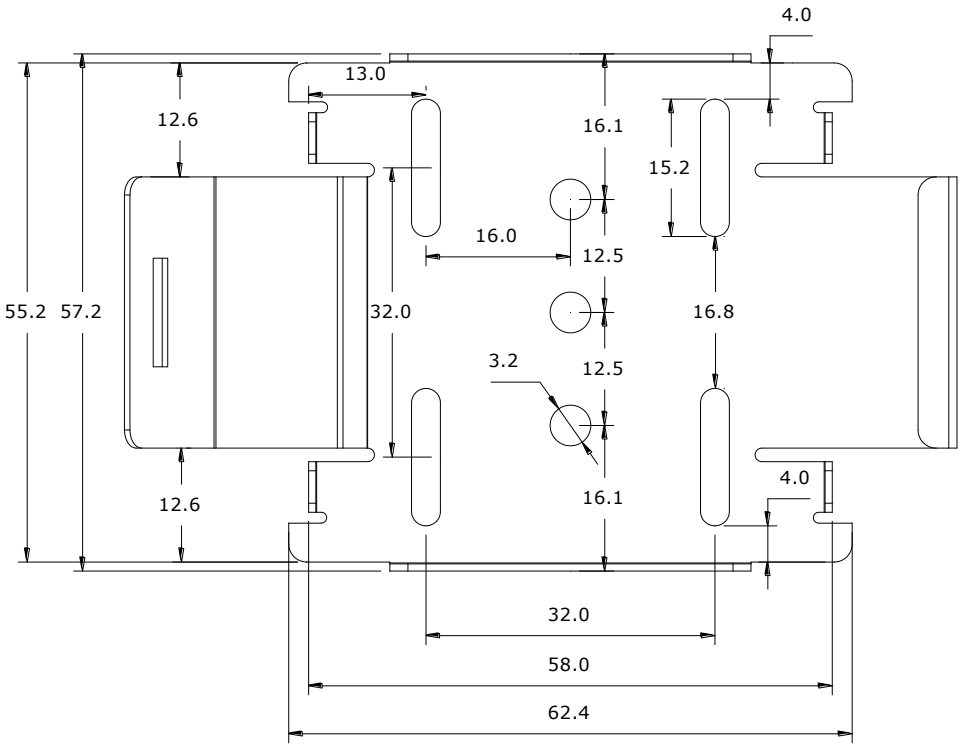
Remarque: Toutes les unités de dimension: Millimeter

3.0 Caractéristiques Matérielles

3.1.2 BulletPlus Support de fixation (Option Order)



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



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

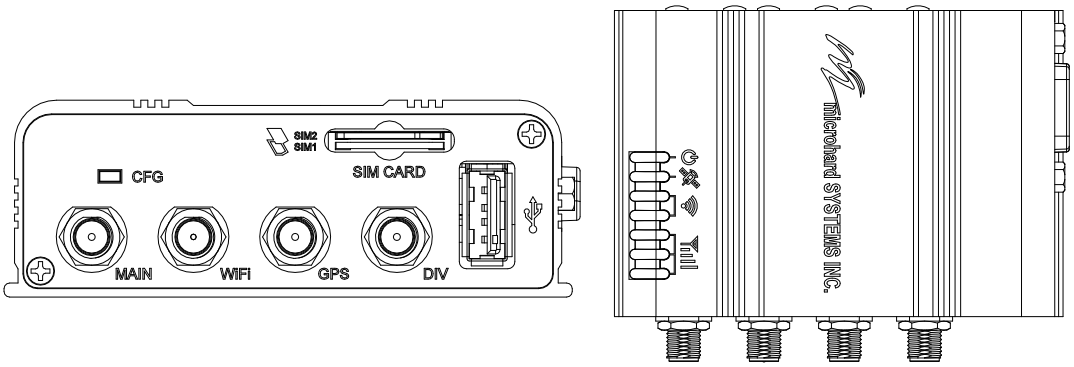
Remarque: Toutes les unités de dimension: Millimeter

3.0 Caractéristiques Matérielles

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.

Les paramètres réseau par défaut:

IP: 192.168.168.1
Subnet: 255.255.255.0
Passerelle: 192.168.168.1

Recevoir Signal Strength Indicator (RSSI) - Comme les augmentations de force de signal reçu, en commençant 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).

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 installée 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.

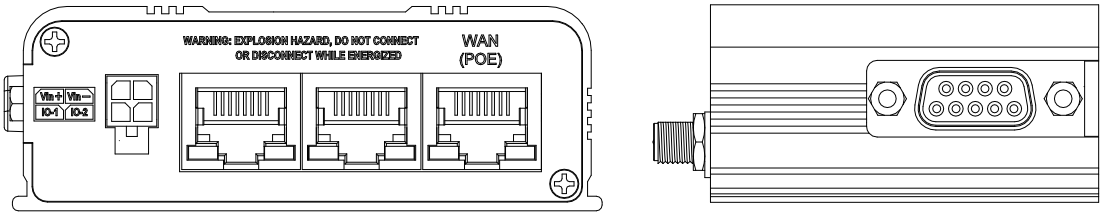
Signal (dBm)	RSSI1	RSSI2	RSSI3
(-85, 0]	sur	Sur	sur
(-90, -85]	sur	sur	FLASH
(-95, -90]	sur	sur	de
(-100, -95]	sur	FLASH	de
(-105, -100]	sur	de	de
(-109, -105]	FLASH	de	de
Autre	balayage	balayage	balayage

Tableau 3-1: LED RSSI

3.0 Caractéristiques Matérielles

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.

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

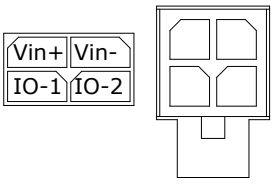
Tableau 3-2: Données RS232 Affectation des broches

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

.

Ethernet RJ45 Nombre Pin								
La source Tension	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
9 - 30 Vdc	D	D	D	DC+	DC+	D	DC-	DC-

Tableau 3-3: Connexions Ethernet PoE



4.0 Configuration

4.0 Interface Utilisateur Web

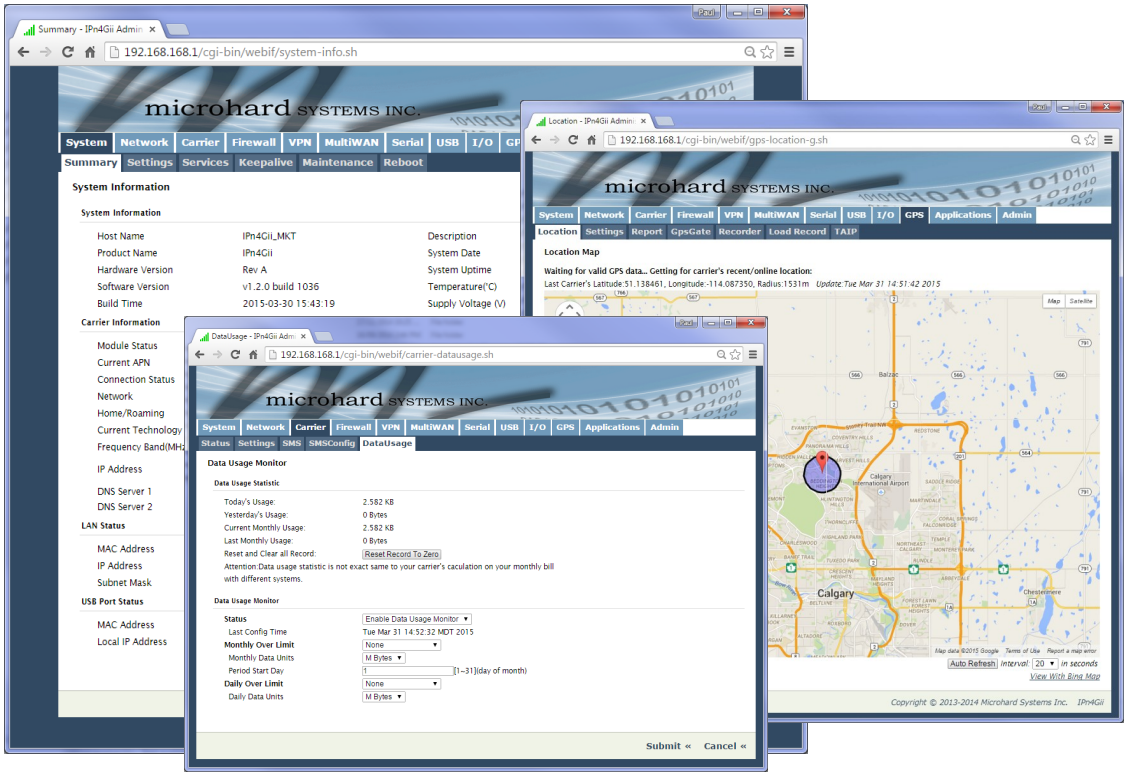


Image 4-0-1: WebUI

Les paramètres réseau par défaut:

IP: 192.168.168.1
Subnet: 255.255.255.0
Passerelle: 192.168.168.1

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 Configuration

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.

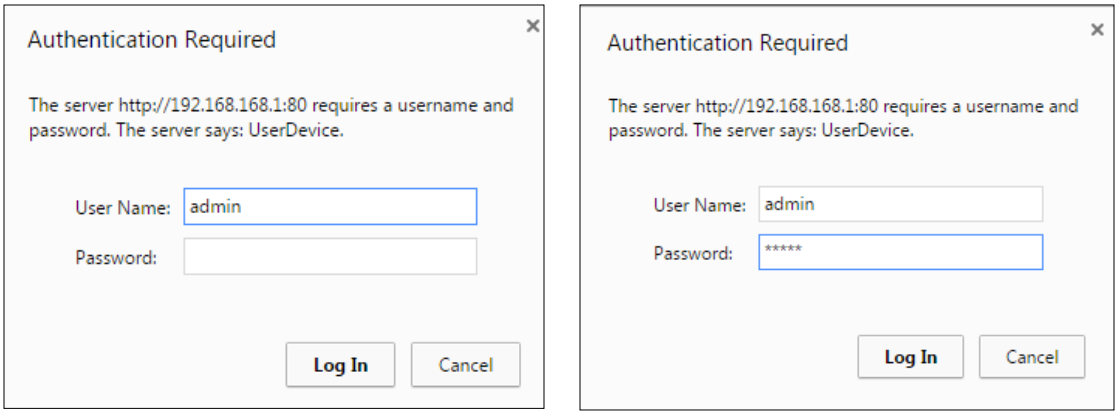


Image 4-0-2: Logon Fenêtre

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.

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.

4.0 Configuration

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.

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.

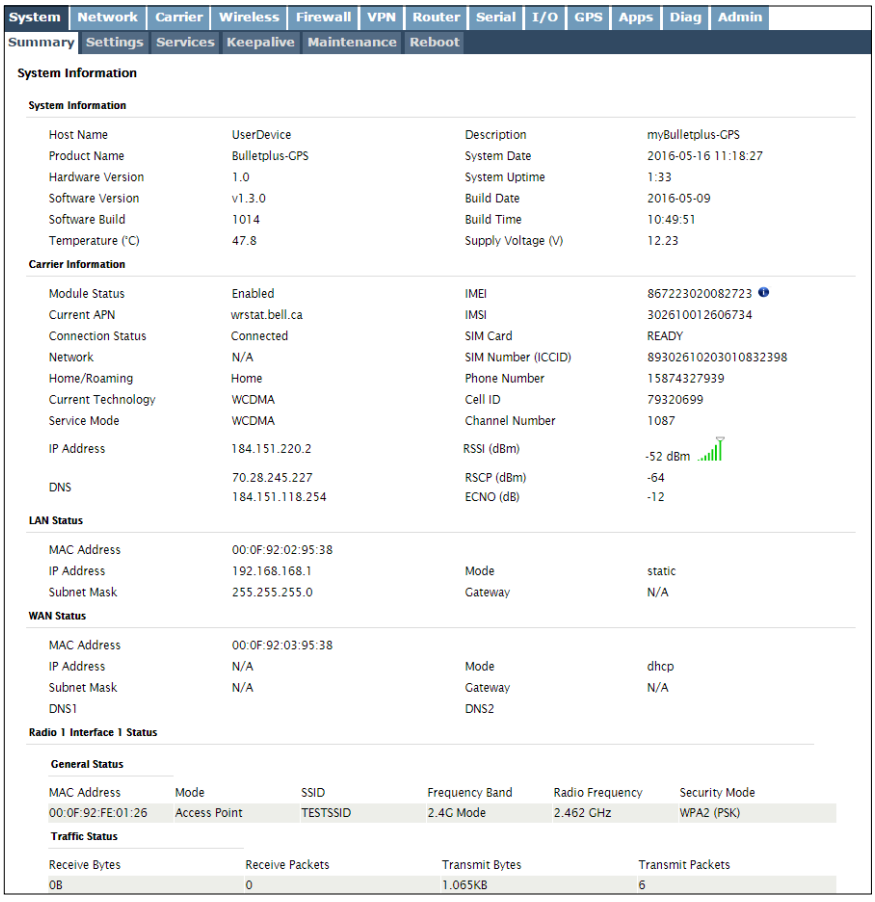


Image 4-1-1: Système Fenêtre Info

4.0 Configuration

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.

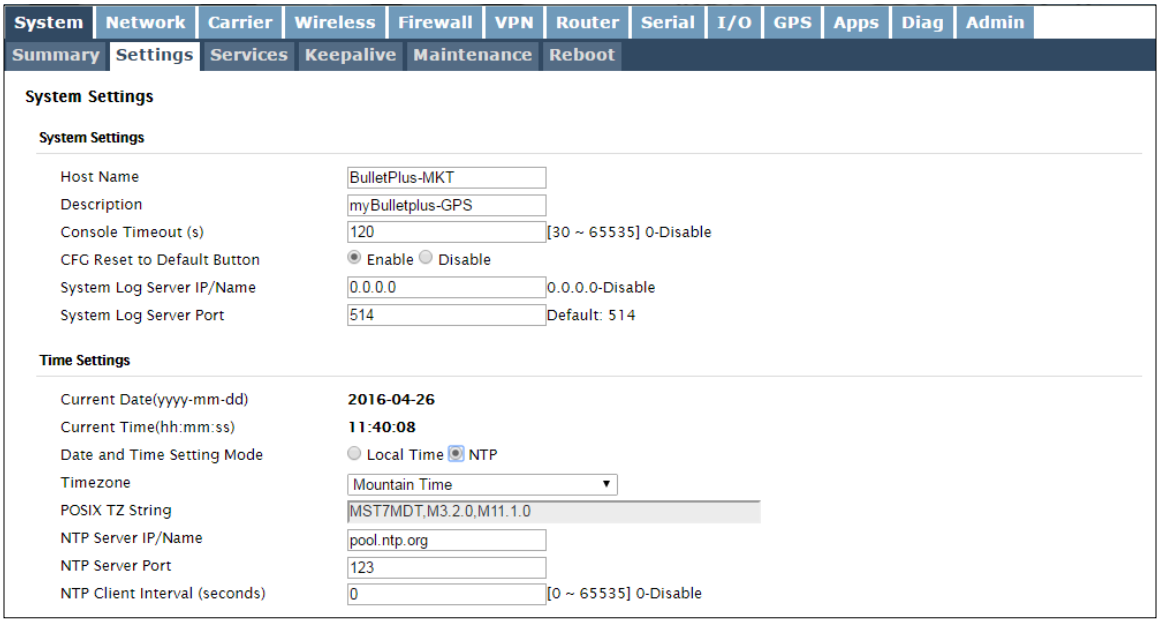


Image 4-1-2: Paramètres système> Paramètres système

Hôte Nom / La description

Le nom d'hôte est un identifiant pratique pour une unité de BulletPlus spécifique. Cette fonctionnalité est le plus utilisé lors de l'accès à distance des 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 l'appareil signale dans Microhard système NMS.

La description fournit un champ supplémentaire pour les caractères de texte, mais ne sont pas affichées partout, mais dans ce domaine.

Valeurs

BulletPlus **(varie)**

jusqu'à 30 caractères

Console Timeout (s)

Cette valeur détermine quand une connexion de la console (fait via le port console ou Telnet) le délai d'attente après être devenu inactif.

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 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.

Valeurs

Activer
Désactiver

4.0 Configuration

Système Syslog Server IP

Le BulletPlus peut signaler des événements au niveau du système à un serveur Syslog tiers, qui peut être utilisé pour surveiller les événements rapportés par le BulletPlus.

Valeurs

0.0.0.0

Port serveur 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

514

Time Settings

Les BulletPlus peut être configuré pour utiliser une source de temps locale, gardant ainsi le temps lui-même, 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.

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.

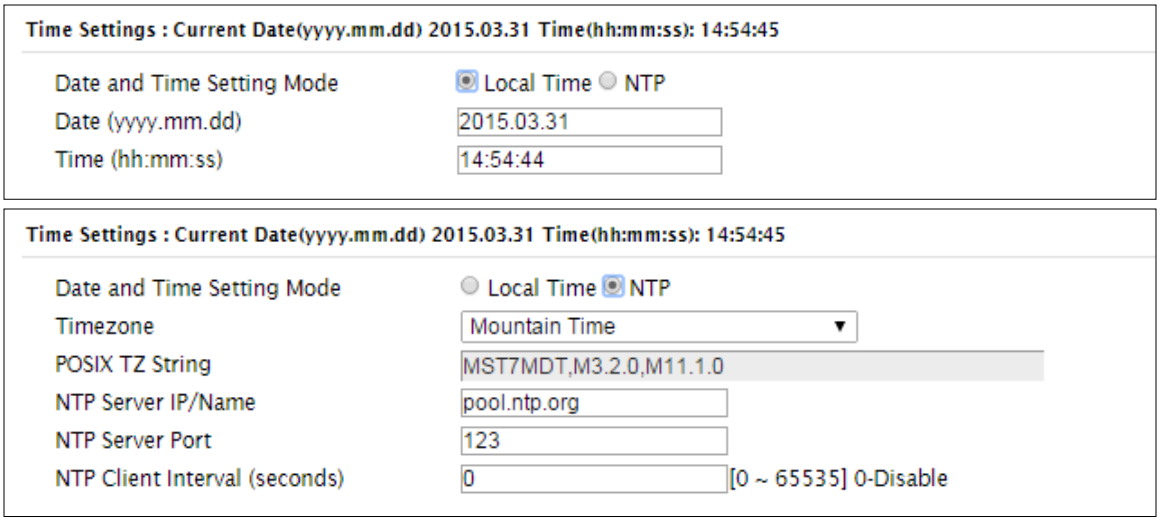


Image 4-1-3: Paramètres système> Paramètres du Temps

Date et heure Réglage du mode

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.

Valeurs

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)*

4.0 Configuration

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 quelconque.	**Valeurs** 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 déterminée par le réglage du fuseau horaire.	**Valeurs** (Variable)

Serveur NTP	
Entrez l'adresse IP ou le nom de domaine du serveur de temps NTP souhaité.	**Valeurs** **pool.ntp.org**

NTP Port	
Entrez l'adresse IP ou le nom de domaine du serveur de temps NTP souhaité.	**Valeurs** **123**

NTP client Intervalle	
Par défaut, le modem ne synchronise l'heure et la date lors du démarrage du système (par défaut: 0), mais il peut être modifié pour synchroniser à intervalles réguliers. Ce processus consomme des données et doit être réglé en conséquence.	**Valeurs** **0**

4.0 Configuration

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.

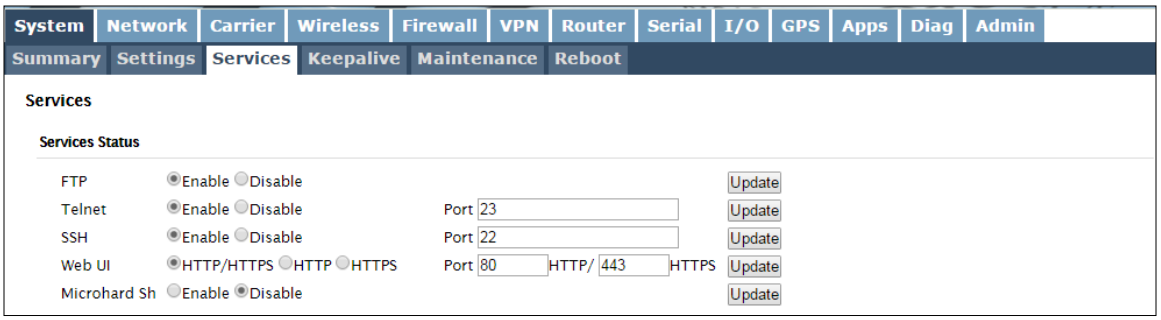


Image 4-1-5: Système> Services

FTP

Le service FTP peut être activée / désactivée à l'aide du menu des services d'état. Le service FTP est utilisé pour les opérations de récupération du micrologiciel.

Valeurs

Enable / Disable

Telnet

Utilisation du service Telnet Activer / Désactiver la fonction, vous pouvez désactiver le service Telnet de fonctionner sur le modem. Le port utilisé par le service Telnet peut également être modifié. La valeur par défaut est 23.

Valeurs

23

SSH

Utilisation du service SSH Activer / Désactiver la fonction, vous pouvez désactiver le service SSH (Port 22) de fonctionner sur le modem. Le port utilisé par le service SSH peut également être modifié. La valeur par défaut est 22.

Valeurs

22

Web UI

Le port du serveur Web par défaut pour les outils de configuration basés sur le Web utilisés dans le modem est le port 80 (http) et le port 443 (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).

Valeurs

HTTP/HTTPS
HTTP
HTTPS

Microhard Sh

Réservé à un usage interne.

4.0 Configuration

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.

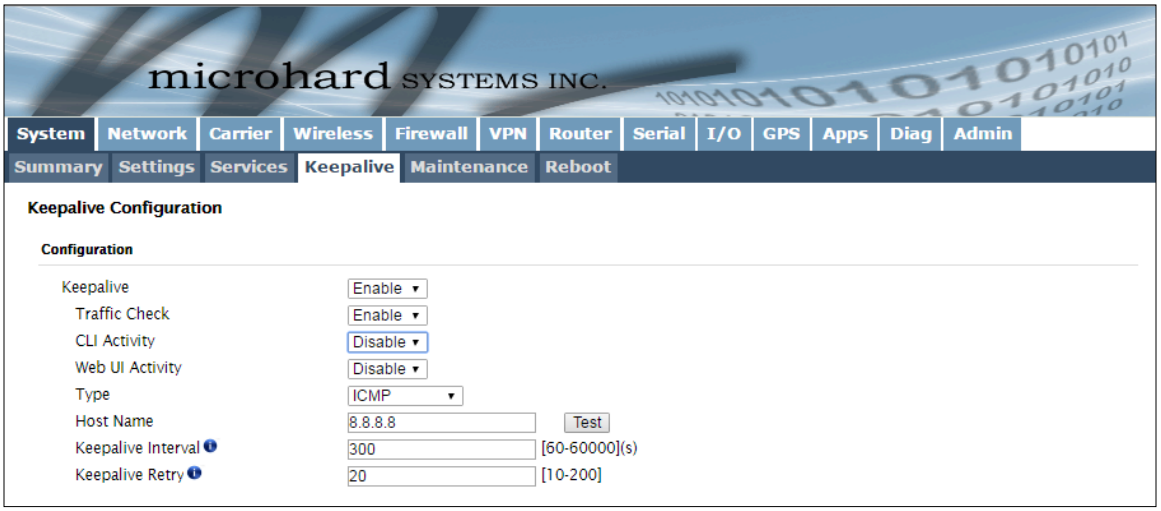


Image 4-1-6: Carrier> Keep Alive

Keep Alive

Activer ou désactiver les fonctions keep alive du modem. Si elle est désactivée, l'utilisateur peut configurer le Traffic Check séparément. L'unité sera de surveiller le trafic sur l'interface cellulaire.

Valeurs

Activer / Désactiver

Traffic Check

Surveille le trafic sur l'interface cellulaire ainsi que l'interface WAN si le port WAN est configuré comme indépendant dans les paramètres 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.

Valeurs

Activer / Désactiver

Activité CLI

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 de l'interface utilisateur Web. Si l'interface utilisateur Web est pas accessible ou actualisée dans la certaine période qui est spécifiée par Console Timeout dans Réglages système page Web, le modem envoie la demande de connexion.

Valeurs

Activer / Désactiver

4.0 Configuration

Type

Une fois que la connexion est perdue, le modem envoie une des demandes à l'hôte distant afin de déterminer l'état de la connexion. Si 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: Envoyer une requête "ping"
HTTP: Envoyer une demande "wget" à un serveur HTTP
Recherche DNS: Envoyer une demande "de dslookup" à un serveur DNS

Valeurs

ICMP
HTTP
DNS Lookup

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

8.8.8.8

Keepalive Interval

La valeur d'intervalle détermine la fréquence, ou combien de fois, l'appareil envoie des messages PING à l'hôte. Le BulletPlus va 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)

Valeurs

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 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.

Valeurs

20

4.0 Configuration

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.

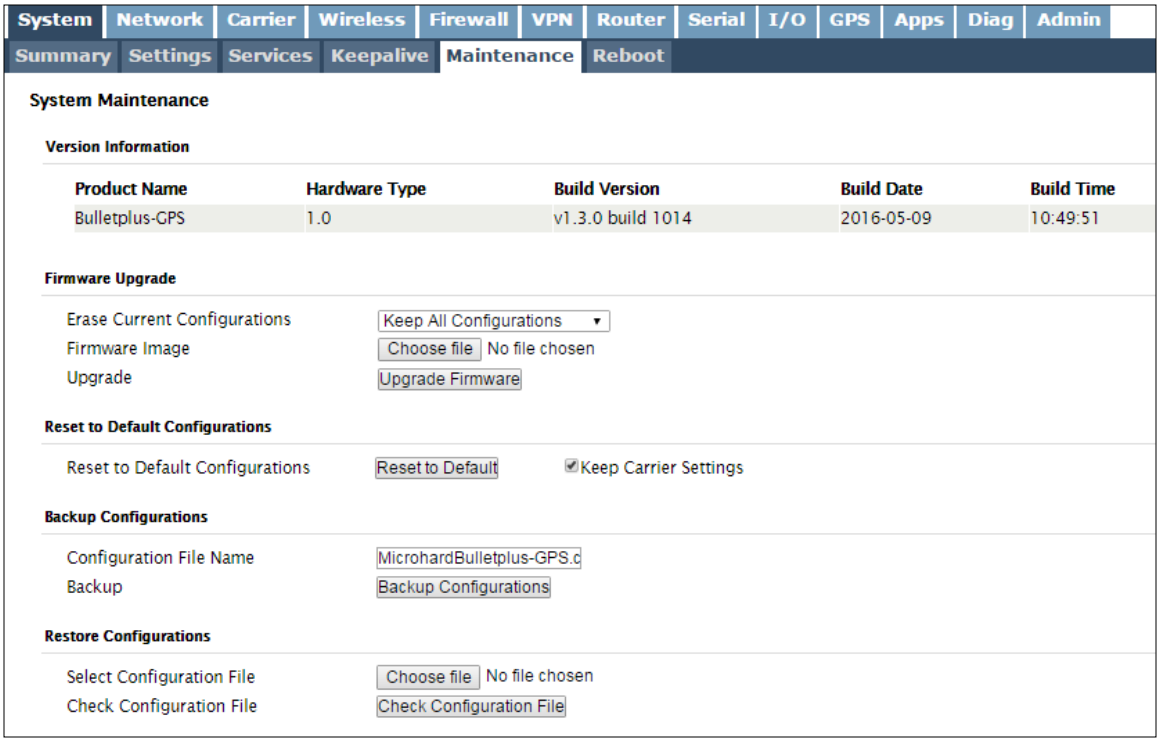


Image 4-1-7: Maintenance > Firmware Upgrade

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 !!!**

4.0 Configuration

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.

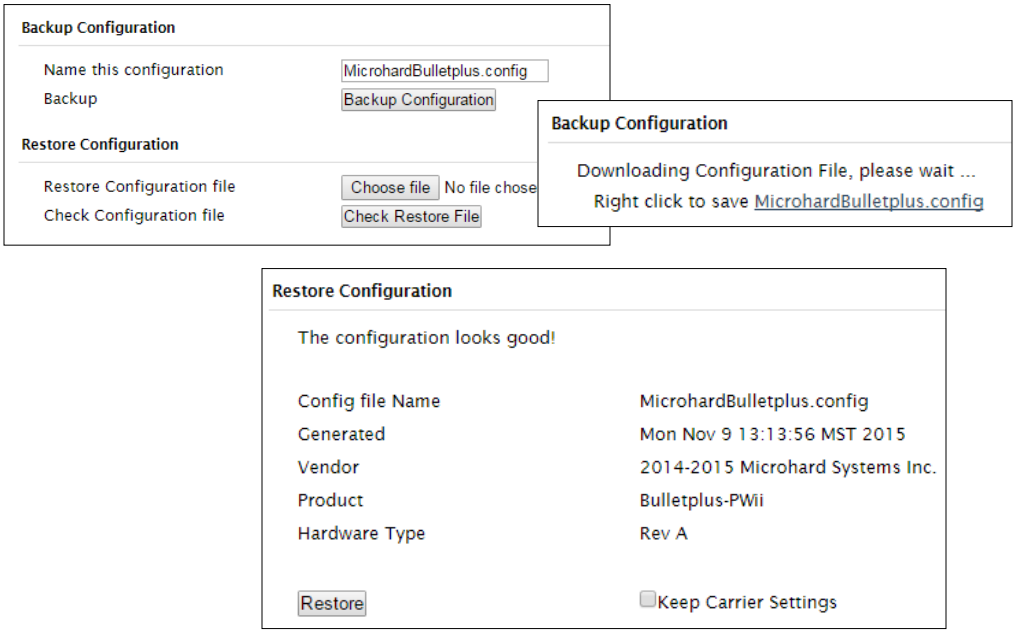


Image 4-1-8: Maintenance > Reset to Default / Backup & Restore Configuration

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.

4.0 Configuration

4.1.6 Système> Reboot

Le BulletPlus peut être redémarré à distance en utilisant le menu Système> Reboot. Comme on le voit ci-dessous 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.

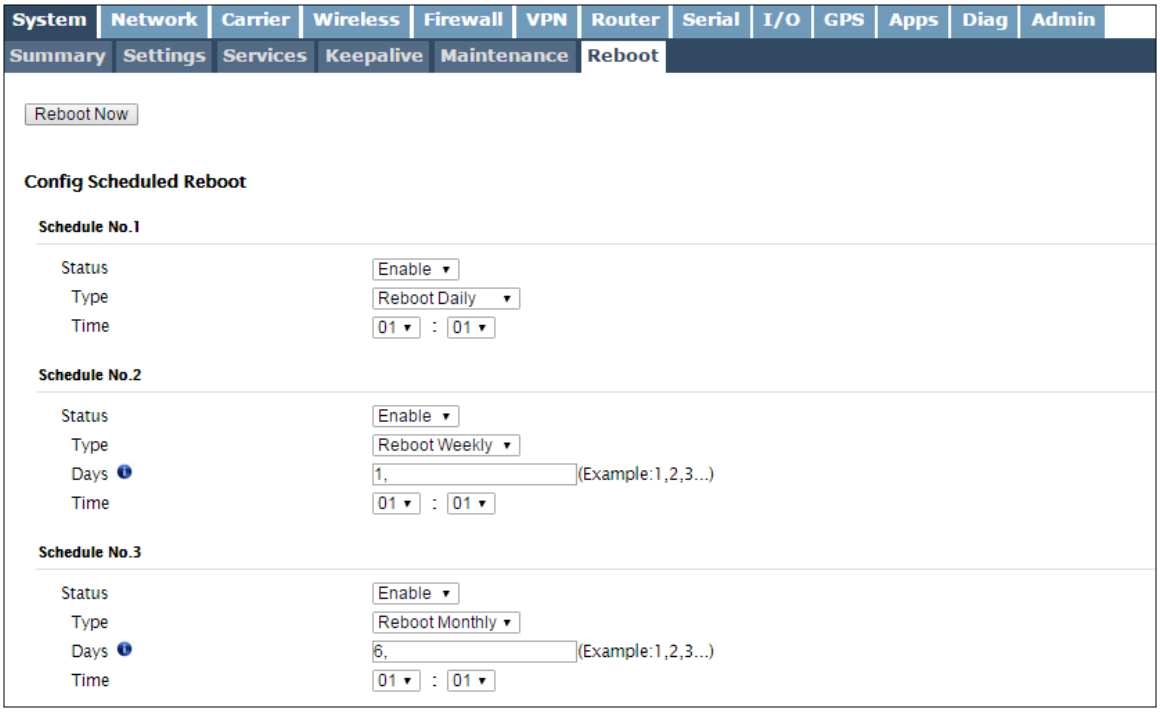


Image 4-1-9: Système> Reboot

Status

Utilisez cette option pour activer ou redémarrages scolarisés handicapés. Si elle est activée Bullet Plus est le redémarrage à l'intervalle défini ci-dessous.

Valeurs

Désactiver / Activer

Type

Horaire quotidien, hebdomadaire ou mensuel redémarrages. Mise en place d'un calendrier de redémarrage peut aider à garder le modem relié au support cellulaire et empêcher physiquement le redémarrage du modem si situé à une destination distante.

Valeurs

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 comptés 1 à 31. jours multiples peuvent être spécifiées en séparant par une virgule ','.

Réglez l'heure de la journée (24 heures d'horloge) pour lequel redémarrer l'appareil.

Valeurs

1,

4.0 Configuration

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.

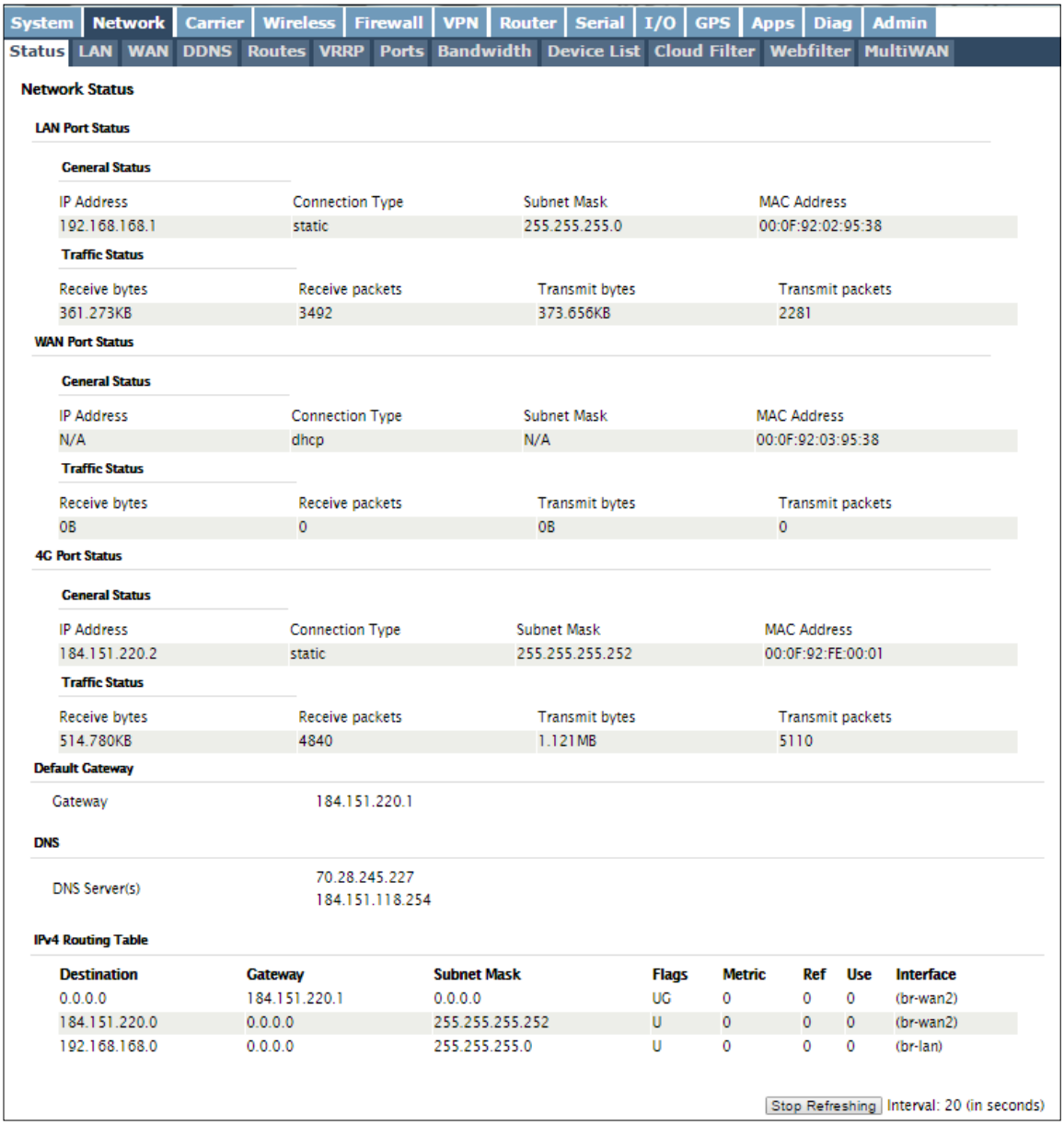


Image 4-2-1: Réseau> État du réseau

4.0 Configuration

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).

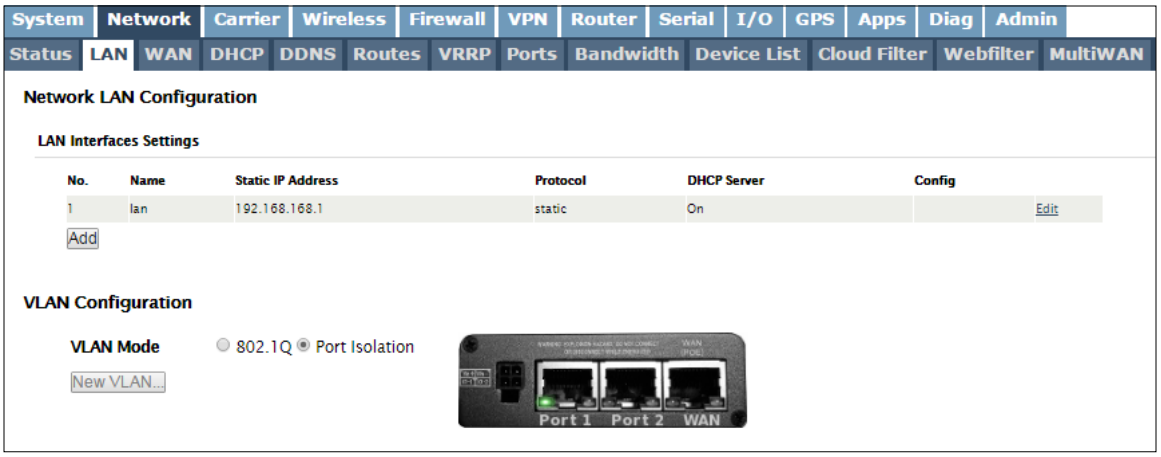


Image 4-2-2: Réseau> Configuration du réseau LAN

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.

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.

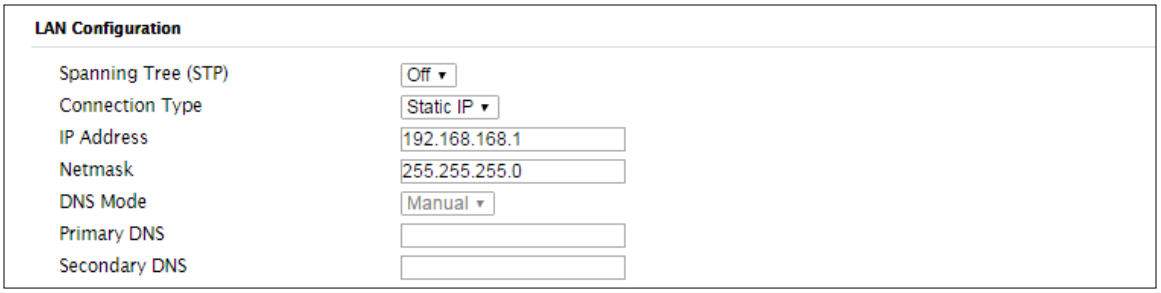


Image 4-2-3: Réseau> LAN Configuration Port

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

Spanning Tree (STP)	
Cette option permet aux BulletPlus de participer dans le protocole Spanning Tree avec d'autres dispositifs pour empêcher les boucles locales. Par défaut cette option est désactivée.	**Valeurs** **De** Sur

4.0 Configuration

Les paramètres réseau par défaut:

IP: 192.168.168.1
Subnet: 255.255.255.0
Passerelle: 192.168.168.1

UN MASQUE SUBNET est un masque de bits qui sépare les parties réseau et hôte (périphérique) d'une adresse IP.

La partie «démasqué» laisse à disposition les informations nécessaires pour identifier les différents dispositifs sur le sous-réseau.

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 d'un serveur DHCP sur le réseau connecté, ou si une adresse IP statique sera entré. Si une adresse IP statique est choisi, les champs suivants doivent également être remplis.

Valeurs

DHCP
Statique

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

192.168.168.1

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

255.255.255.0

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. Si le type de connexion est définie comme statique, les serveurs DNS peuvent être spécifiés manuellement.

Valeurs

Auto
Manuel

DNS primaire / DNS secondaire

Définissez le DNS primaire et alternatif (Domain Name Server) pour une utilisation par les périphériques sur le port LAN, si nécessaire.

Valeurs

Auto
Manuel

4.0 Configuration

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.

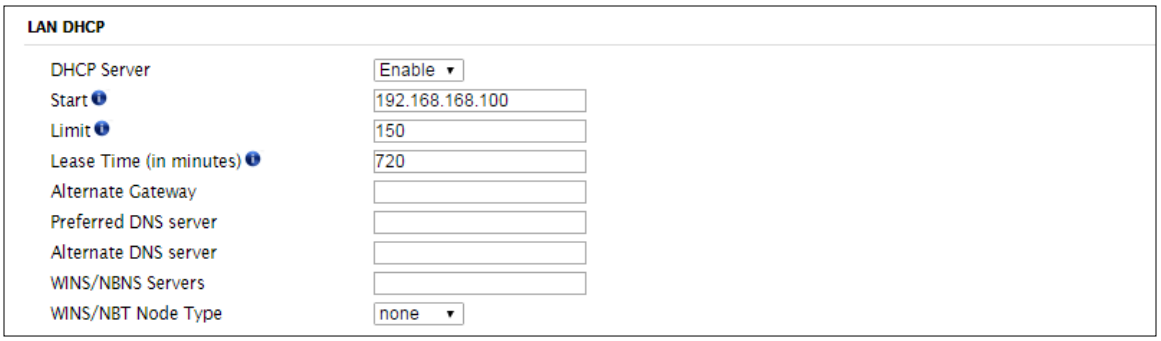


Image 4-2-4: Réseau> Serveur DHCP

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.)

Serveur DHCP

L'option est utilisée pour activer ou désactiver le service DHCP pour les périphériques connectés au port (s) LAN.

Valeurs

Enable / Disable

Démarrer

Sélectionnez les adresses à partir des adresses IP DHCP assignable. Les premiers octets du sous-réseau seront pré-série basée sur la configuration IP du réseau local, et ne peuvent pas être changé.

Valeurs

192.168.168.100

Limite

Définir le nombre maximum d'adresses IP qui peuvent être affectées par le BulletPlus.

Valeurs

150

Durée du bail

La durée du bail DHCP est la quantité de temps avant une nouvelle demande pour une adresse réseau doit être fait pour le serveur DHCP.

Valeurs

720

Autre passerelle

Spécifiez une autre passerelle pour les périphériques DHCP attribués si la passerelle par défaut est de ne pas être utilisé.

Valeurs

(IP Address)

4.0 Configuration

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

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»).

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 DHCP.

Valeurs

(Adresse IP)

WINS / NBNS Servers

Saisissez l'adresse du service WINS / NBNS (NetBIOS) Server. Le serveur WINS traduire les noms d'ordinateurs dans leurs adresses IP, semblable à un serveur DNS traduit les noms de domaine en adresses IP.

Valeurs

(Pas par défaut)

WINS / Type de nœud NBT

Sélectionnez la méthode utilisée pour résoudre les noms d'ordinateur à des adresses IP. Pour le nom des méthodes de résolution sont disponibles:
B-noeud: diffusion
P-noeud: le point-à-point
M-noeud: mixte / modifié
H-noeud: hybride

Valeurs

none
b-node
p-node
m-node
h-node

4.0 Configuration

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

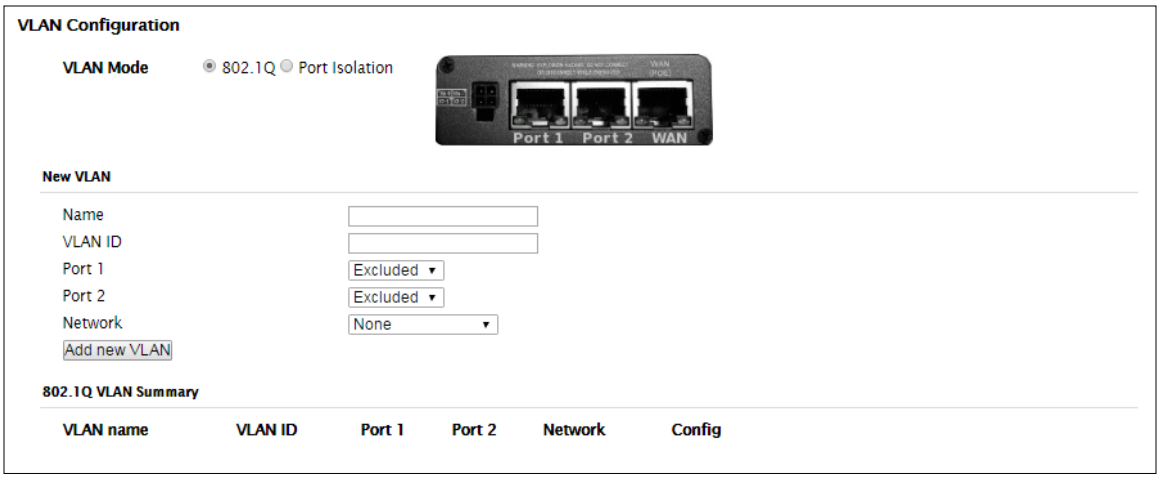


Image 4-2-5: Réseau> VLAN

Nom VLAN

Les noms de VLAN peuvent être ajoutés pour aider à l'identification de VLAN (but, I, e ingénierie, comptabilité, etc.).

Valeurs

(no default)

VLAN ID

Lors de l'ajout d'un VLAN, vous devez sélectionner un ID de VLAN. Sélectionnez entre 2 et 127 pour les ID de VLAN valides.

Valeurs

2 (2-127)

Port 1 - 2

Attribuer port au VLAN actuel.

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.

Valeurs

Excluded
Tagged
Untagged

Réseau

Permet à l'utilisateur la possibilité d'attribuer des interfaces spécifiques du réseau de configuration à un VLAN spécifique. (802.1Q)

Valeurs

Aucun
LAN
(interfaces réseau supplémentaires)

4.0 Configuration

4.2.3 Réseau> WAN

Configuration WAN

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.

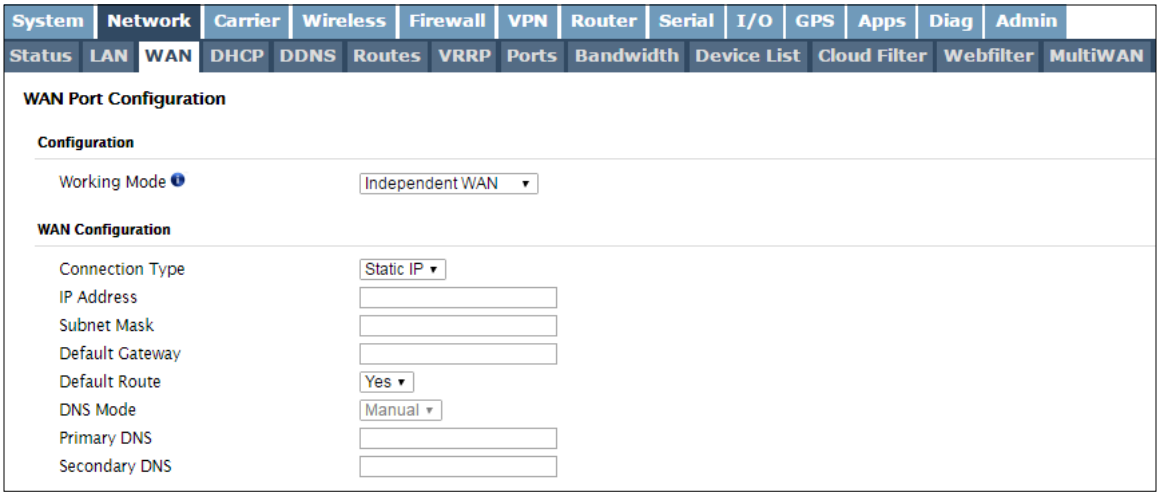


Image 4-2-6: Réseau> Configuration WAN

Mode de fonctionnement

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.

Valeurs

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 doivent également être remplis.

Valeurs

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:
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.

4.0 Configuration

Passerelle par défaut

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 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.

Valeurs

(Pas par défaut)

Route par défaut

Le paramètre Route par défaut vous permet de définir cette interface comme route par défaut dans la table de routage. Ceci est fait dans 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.

Valeurs

Non / Oui

Mode DNS

Sélectionnez entre manuelle ou automatique pour le serveur (s) DNS pour l'interface WAN. Si réglé sur Auto le BulletPlus va essayer de 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.

Valeurs

Manuel / **Auto**

DNS primaire

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 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.

Valeurs

(Pas par défaut)

DNS secondaire

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 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.

Valeurs

(Pas par défaut)

4.0 Configuration

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.

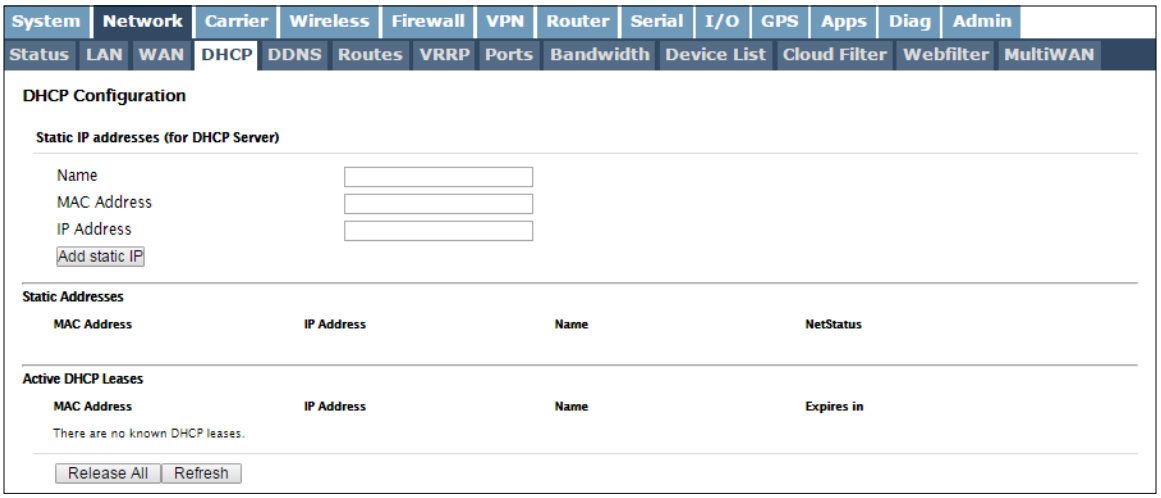


Image 4-2-7: Réseau> Adresse MAC Binding

Nom

Le champ de nom est utilisé pour donner au dispositif un nom facilement reconnaissable.

Valeurs

(Pas par défaut)

Adresse Mac

Entrez dans l'adresse MAC de l'appareil à être lié à une adresse IP définie. Définissez l'adresse IP dans le champ suivant. Doit utiliser le format: AB: CD: DF: 12: 34: D3. Il est pas sensible à la casse, mais les colons doivent être présents.

Valeurs

(Pas par défaut)

Adresse IP

Entrez l'adresse IP à attribuer à l'appareil spécifié par l'adresse MAC ci-dessus.

Valeurs

(Pas par défaut)

Adresses statiques
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)

4.0 Configuration

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.

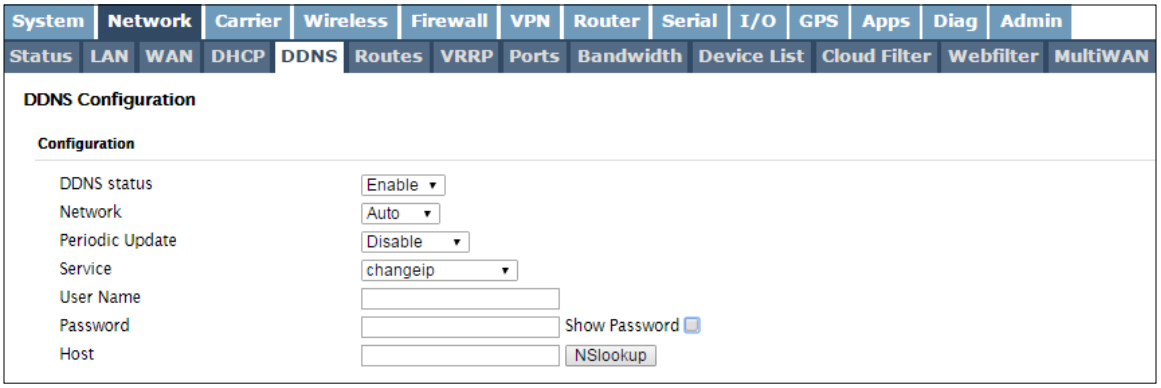


Image 4-2-8: Réseau > DDNS

DDNS Status

Cette sélection permet l'utilisation d'un Dynamic Domain Name Server (DNS), pour le Bullet Plus.

Valeurs

Activer / Désactiver

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 charge. Services gratuits et premium sont offerts, communiquez avec les fournisseurs spécifiques pour plus d'informations.

Valeurs

changeip	ods
dyndns	ovh
eurodyndns	regfish
hn	tzo
noip	zoneedit

Identifiant Mot de passe

Entrez un nom d'utilisateur et mot de passe pour le service DDNS sélectionné ci-dessus.

Valeurs

(aucun)

Hôte

Ceci est l'hôte ou le nom de domaine pour le Bullet plus attribué par le fournisseur de DDNS. Utilisez le bouton prévu pour interroger le serveur (si configuré correctement)

Valeurs

(aucun)

4.0 Configuration

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.

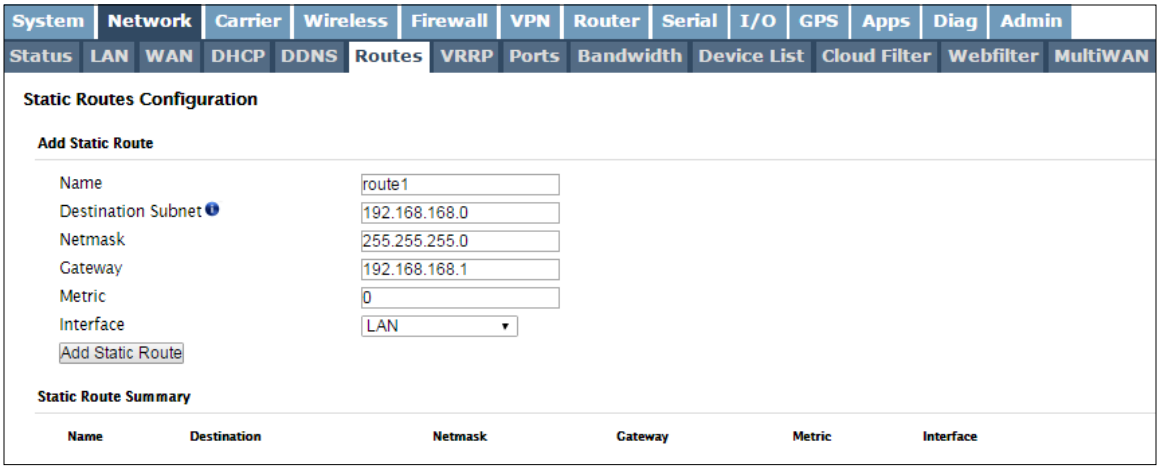


Image 4-2-9: Réseau> Routes

Nom

Les itinéraires peuvent être des noms faciles à consulter, ou de décrire l'itinéraire ajouté.

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-dessus.

Valeurs

192.168.168.1

Netmask

Entrez le masque pour le réseau de destination.

Valeurs

255.255.255.0

4.0 Configuration

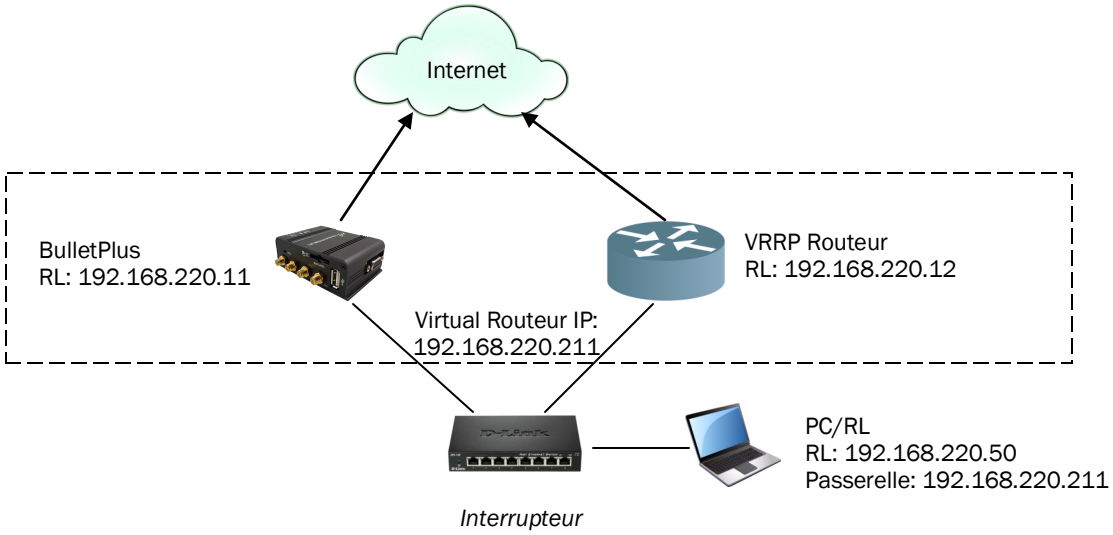
Métrique	
Dans certains cas, il peut y avoir de multiples voies pour atteindre une destination. La métrique peut être réglé pour donner des itinéraires certaine priorité, plus la métrique est, mieux la route. Plus houblon qu'il faut pour arriver à une destination, plus la métrique.	**Valeurs** **255.255.255.0**

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** **LAN** / LAN1 / WAN / Cell / USB None

4.0 Configuration

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.



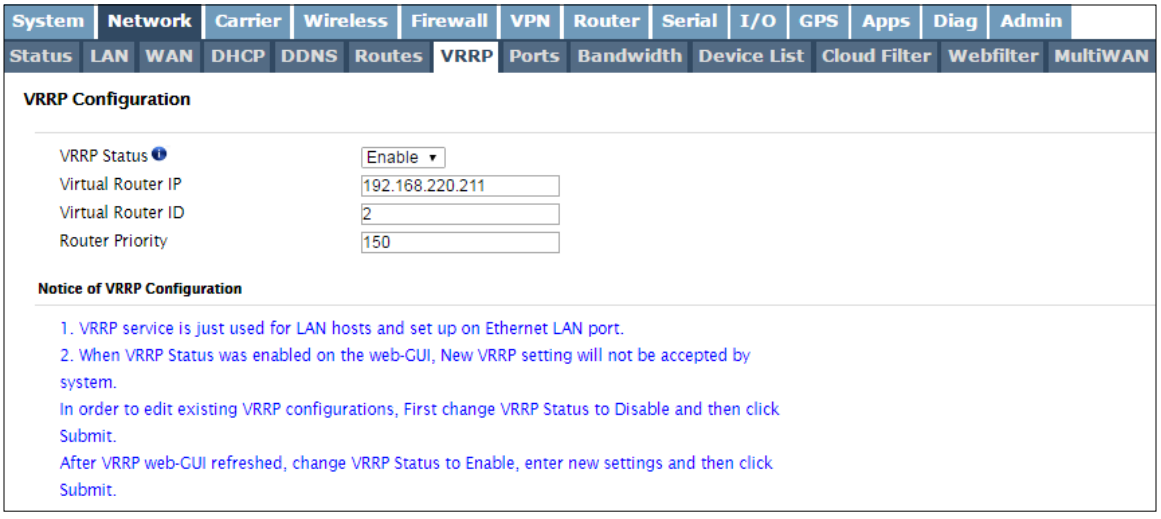


Image 4-2-10: Réseau > VRRP

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

4.0 Configuration

Virtuel Routeur IP	
Ceci est l'adresse IP du routeur virtuel, cela doit être le même sur tous les appareils participant à VRRP. Ceci est l'adresse IP que tout réseau local PC / périphérique connecté utiliserait comme sa passerelle par défaut.	**Valeurs** **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 pour déterminer quel routeur (s) sera utilisé comme premier ou primaire. Plus l'ID est élevée, plus la priorité.	**Valeurs** **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.

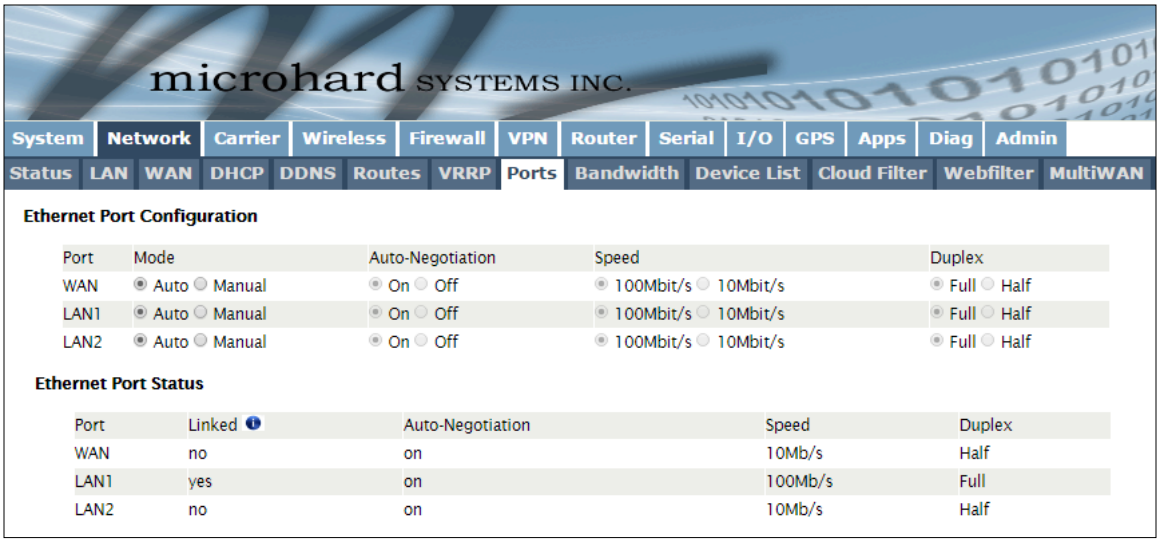


Image 4-2-11: Réseau > Ports

4.0 Configuration

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.

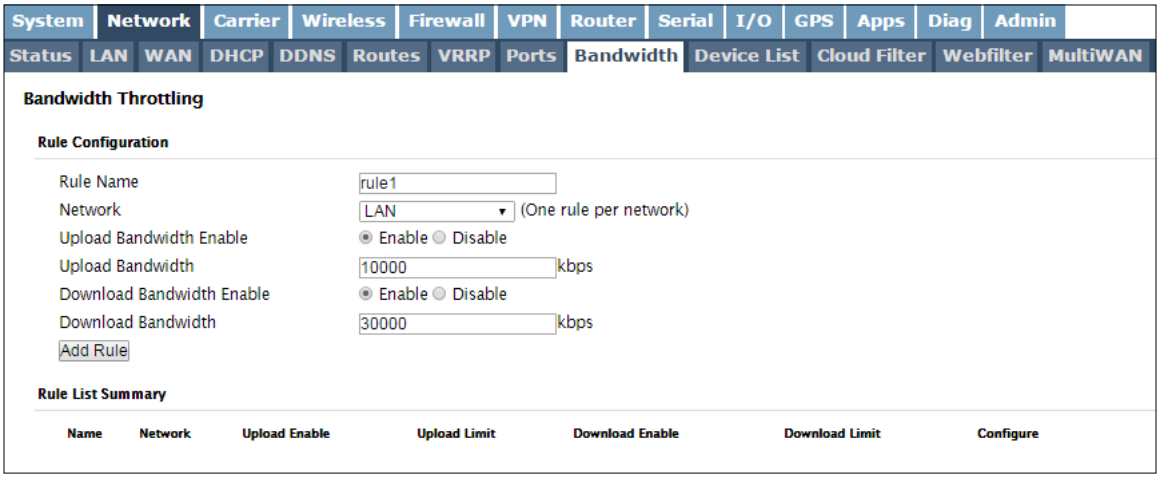


Image 4-2-12: Réseau > limitation de bande passante

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 réseau affectée.

Valeurs

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 données d'être téléchargées vers un serveur. (À savoir ajout / envoyer des vidéos ou d'autres fichiers sur un serveur).

Valeurs

Activer / Désactiver

Télécharger la bande passante

Régler la limite de données (vitesse) pour le téléchargement de fichiers si ajouts ont été autorisés en utilisant le chargement de la bande passante Activer.

Valeurs

10000

4.0 Configuration

Télécharger la bande passante Activer	Valeurs
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.).	**Enable** / Disable

Télécharger la bande passante	Valeurs
Régler la limite de données (vitesse) pour les téléchargements de fichiers si les téléchargements ont été autorisés en utilisant la bande passante de téléchargement Activer.	**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.

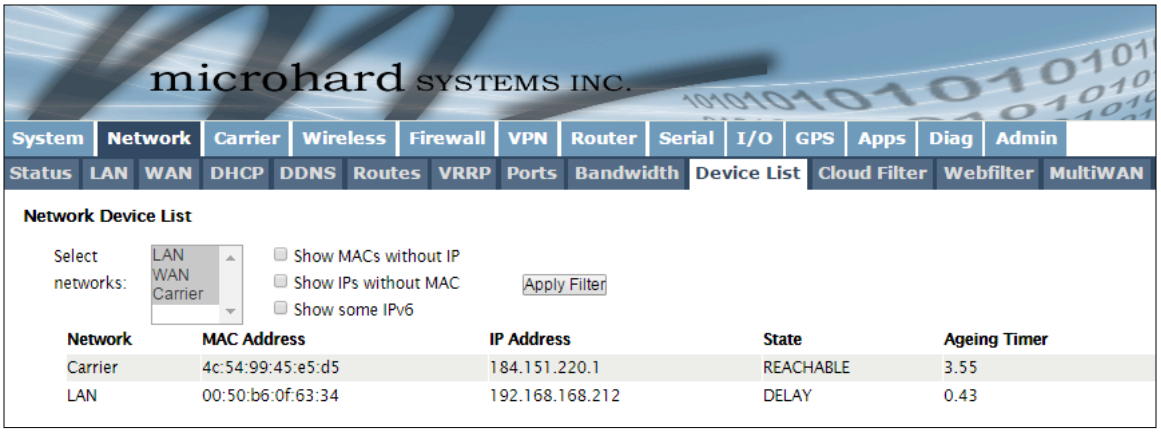


Image 4-2-13: Réseau> Liste des périphériques

4.0 Configuration

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.

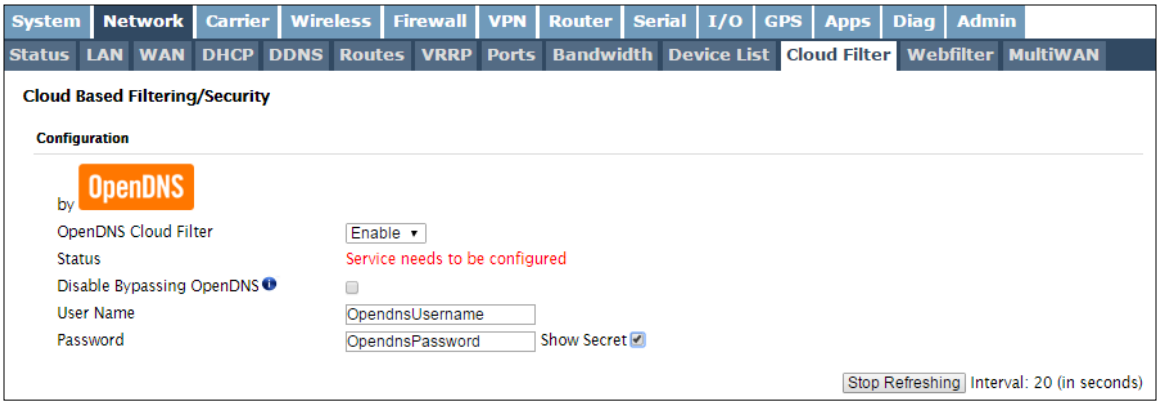


Image 4-2-14: Réseau> Nuage Filtrage

Filtre OpenDNS Nuage

Activer ou désactiver le filtrage OpenDNS nuage et sécurité basée.

Valeurs

Activer / **Désactiver**

Désactiver OpenDNS Contourner

Si activé tous les clients connectés à travers le BulletPlus seront contraints d'utiliser OpenDNS et est soumis à toute filtrage et la sécurité des contenus, pour empêcher le contournement.

Valeurs

Activer / **Désactiver**

Statut

Lorsque le filtre Cloud est activé, ce statut sera rafraîchie toutes les 30 secondes, indiquant l'état OpenDNS. Pour OpenDNS d'être actif, l'état doit être vert et afficher "Connecté à OpenDNS".

Valeurs

Activer / **Désactiver**

Identifiant Mot de passe

Entrez le nom d'utilisateur et mot de passe pour le compte OpenDNS qui a été spécifié lors de l'inscription et la configuration du service.

Valeurs

Activer / **Désactiver**

4.0 Configuration

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.

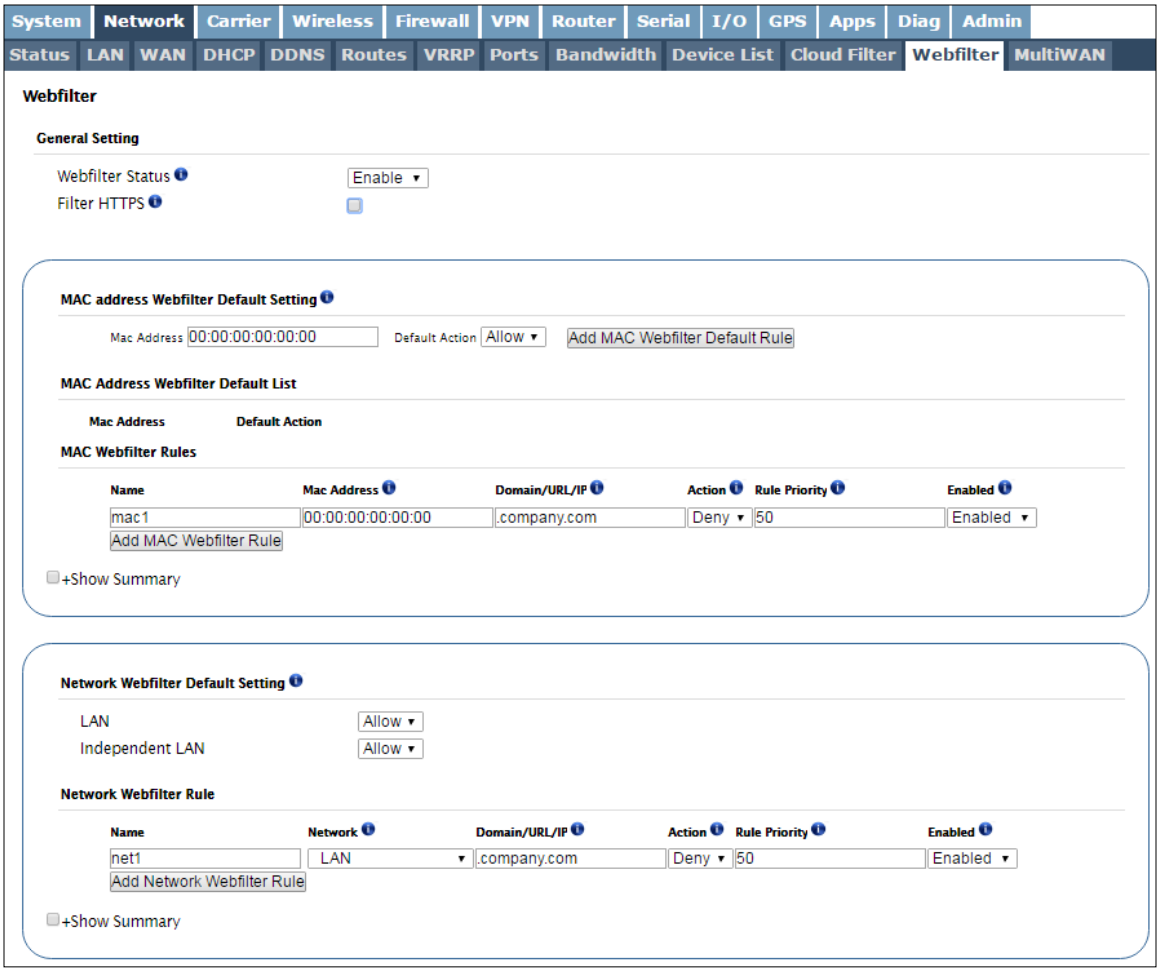


Image 4-2-15: Réseau> Filtrage Web

Webfiltre Statut

Activer ou désactiver le filtre Web du BulletPlus.

Valeurs

Activer / **Désactiver**

Filtre HTTPS

Vérifiez filtre HTTPS redirigera tout le port 443 du trafic dans le filtre web. (S'il vous plaît assurez-vous que le système fonctionne DNS.)

Valeurs

Activer / **Désactiver**

4.0 Configuration

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

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.

Valeurs

Mac1
00: 00: 00: 00: 00: 00
Company.com
Nier
50
Activée

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

MAC Règles de filtrage Web

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 ci-dessus.
Activé: Activer ou désactiver la règle Webfilter réseau.

Valeurs

net1
LAN
Company.com
Nier
50
Activée

4.0 Configuration

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.

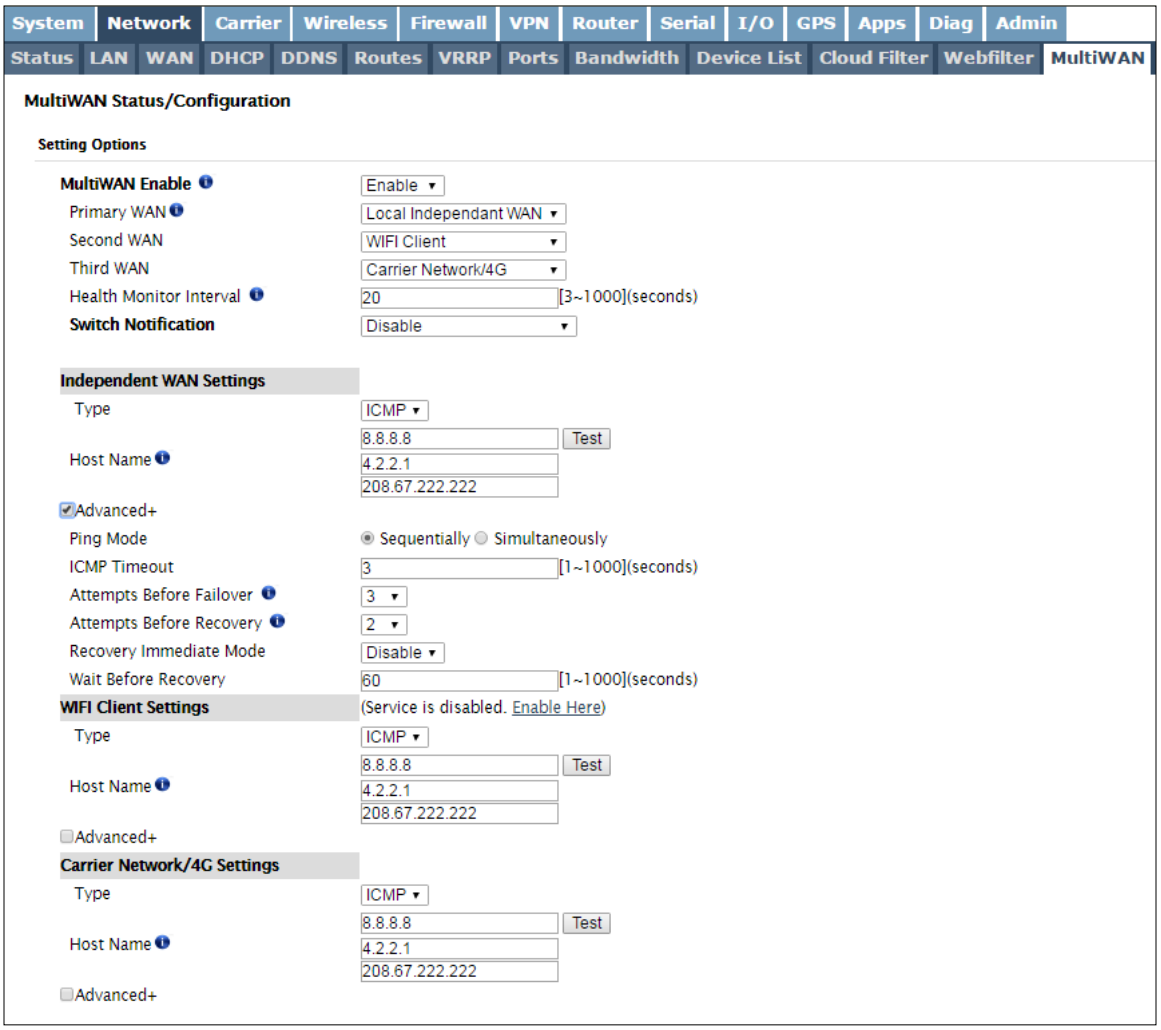


Image 4-2-16: Réseau> MultiWAN

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**

4.0 Configuration

Primaire WAN

Définir quelle connexion est la connexion réseau primaire / Internet pour le Bullet Plus. Normalement, cela est la connexion WAN filaire à un FAI.

Valeurs

WAN / Carrier / WIFI Client

Deuxième WAN

Sélectionnez le WAN connexion est la connexion secondaire. En cas d'échec de la principale WAN se produit, ce sera la première alternative. En général, ce sera la connexion cellulaire.

Valeurs

WAN / **4G** / WIFI

Troisième WAN

La connexion sur la puce Plus peut être configuré en tant que client et utilisé en tant que connexion de données pour accéder à Internet.

Valeurs

WAN / 4G / **WIFI** / Désactiver

Santé Moniteur Intervalle

Ceci est la fréquence à laquelle le BulletPlus envoie des paquets ICMP à l'hôte défini pour déterminer si l'interface est en panne.

Valeurs

20

Commutateur de notification

Il est possible pour le BulletPlus pour envoyer une notification lorsque le MultiWAN a commuté sa connexion disponible et le routage des données par une autre interface.

Valeurs

De / Email / SMS / Deux

Paramètres de basculement (Mêmes paramètres pour WAN, WIFI Client et transporteurs)

Type

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.

Valeurs

ICMP / DNS Chercher

Nom d'hôte

Jusqu'à trois (3) adresses accessibles peuvent être spécifiées pour tester le lien de la santé à la fréquence spécifiée ci-dessus pour le moniteur Intervalle de santé.

Un bouton de test est prévu pour assurer cette adresse accessible ont été saisies et qu'il n'y a pas d'erreurs.

Valeurs

8.8.8.8
4.2.2.1
208.67.222.222

Avancée + (Seulement montré si elle est sélectionnée)

4.0 Configuration

Ping Mode	
Le mode Ping permet aux hôtes sélectionnés être épinglées successivement ou simultanément. Cette option est uniquement affiché lorsque le mode de basculement est réglé sur ICMP.	**Valeurs** **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** **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 interfaces WAN.	**Valeurs** 1, **3**, 5, 10, 15, 20

Les tentatives de récupération Avant	
Le BulletPlus continuera de surveiller l'interface a échoué, même après le basculement a eu lieu. Cela définit le nombre de tentatives réussies nécessaires avant de récupérer l'interface défaillante.	**Valeurs** 1, **2,** **5**, 10, 15, 20

Mode immédiat de récupération / Wait	
Une fois la connexion préférée est de nouveau considéré comme disponible, il peut être spécifié à attendre une quantité de temps configurable avant de rétablir la connexion.	**Valeurs** **Désactiver** / Activer

4.0 Configuration

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.

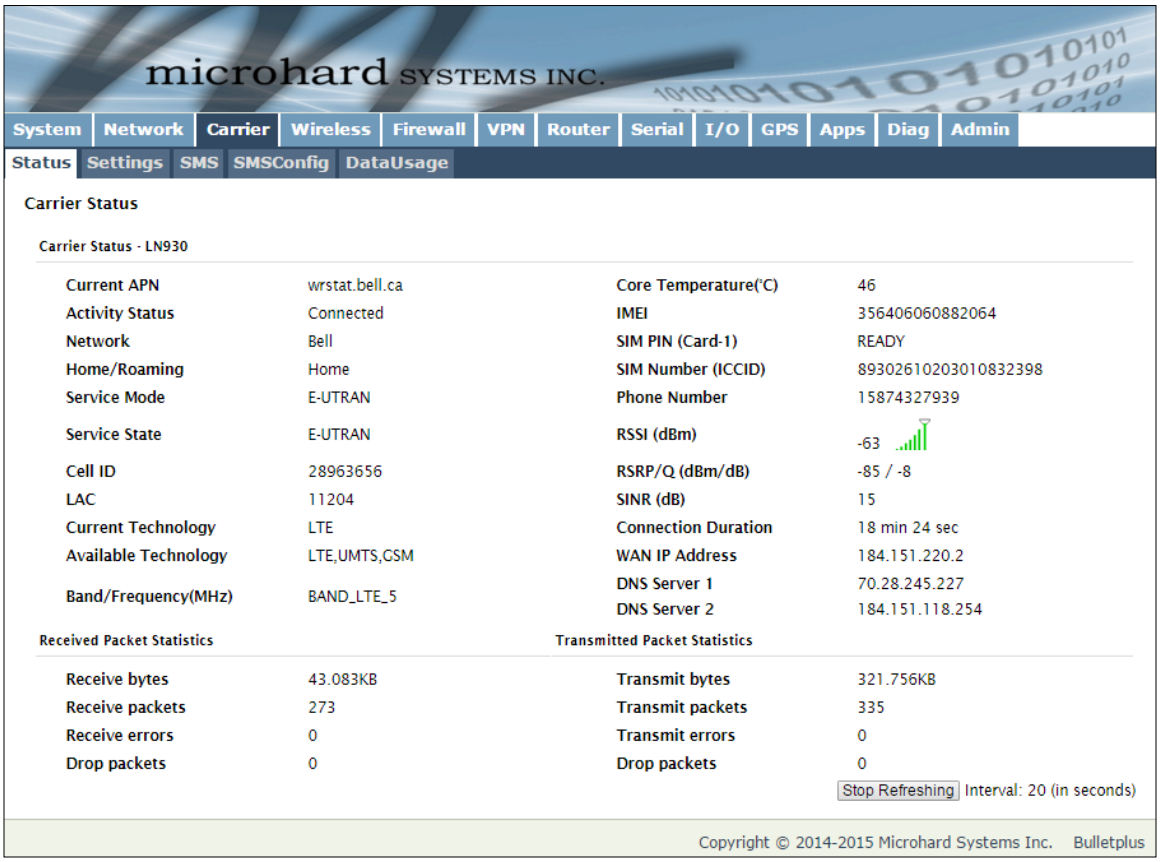


Image 4-3-1: Carrier > Statut

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.

4.0 Configuration

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.

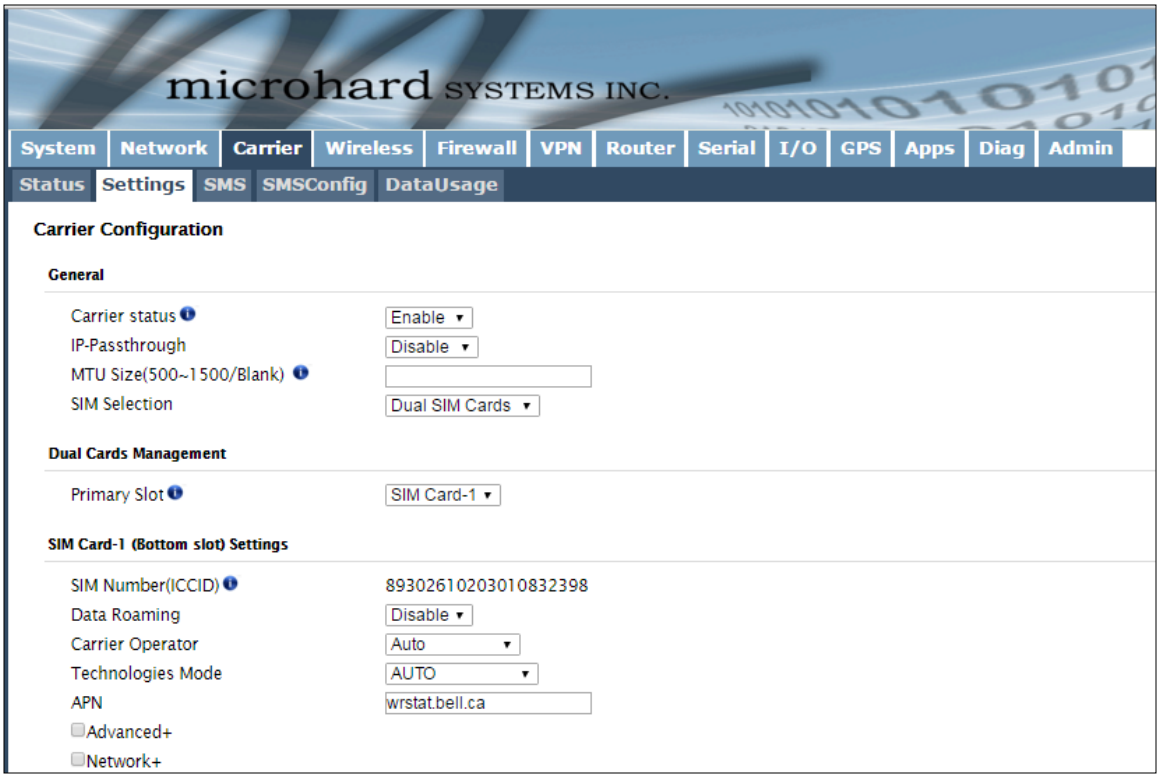


Image 4-3-2: Carrier > Paramètres

Statut Carrier

Statut du transporteur est utilisé pour activer ou désactiver la connexion au Cellular Carrier. Par défaut, cette option est activée.

Valeurs

Activer / Désactiver

MTU Taille

Permet à un utilisateur de spécifier la taille MTU pour les applications personnalisées. Dans la plupart des cas, ce sera laissée en blanc et le système déterminera la meilleure valeur.

Valeurs

(blanc)

4.0 Configuration

IP-Passthrough

IP pass-through permet l'adresse IP WAN à attribuer à l'appareil connecté aux ports LAN ou WAN. Dans ce mode, la Bullet est la plupart du temps transparent et transmet tout le trafic sur le périphérique connecté au port Ethernet sélectionné, sauf que la liste ci -dessous:

-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.

Valeurs

Désactiver
Ethernet (RL)
WAN

Sélection SIM

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.

Valeurs

Deux cartes SIM
Card-1 SIM Only
Card-2 SIM Only

Double gestion des cartes

Fente Primaire

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.

Valeurs

Card-1 SIM Only
Card-2 SIM Only

Carte SIM-1 Paramètres

Itinérance des données

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.

Valeurs

Activer / **Désactiver**

4.0 Configuration

Opérateur Carrier

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

Valeurs

Auto
Sur la base de la carte SIM
Manuel
Fixé

Mode Technologies

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

Valeurs

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

Nom APN Access Point

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.

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

Le Pin SIM est nécessaire pour certains transporteurs internationaux. Si elle est fournie et requise par l'opérateur cellulaire, entrez le code PIN SIM ici.

Valeurs

(none)

Authentification

Définit le type d'authentification requis pour négocier avec les pairs.
PAP - Protocole d'authentification par mot de passe.
CHAP - Challenge Handshake Authentication Protocol.
Seulement requis si le transporteur a besoin d'un nom d'utilisateur et mot de passe.

Valeurs

AUTO
PAP
CHAP
No Auth

4.0 Configuration

Nom d'utilisateur

Un nom d'utilisateur peut être nécessaire pour l'authentification à un homologue distant. Bien que généralement pas nécessaire pour les adresses IP attribuées dynamiquement à partir du support sans fil. Varie par le transporteur.

Valeurs

Transporteur / pairs dépendance

Mot de passe

Entrez le mot de passe pour le nom d'utilisateur ci-dessus. Ne peut pas être exigée par certains transporteurs, ou APNs

Valeurs

Transporteur / pairs dépendance

Réseau+

Adresse IP

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 des cas, l'IP sera lu à partir de la carte SIM et de ce champ doit être laissé à la valeur par défaut.

Valeurs

(blanc)

Adresse IP Utilisation à distance DNS

Si elle est activée Bullet avec l'utilisation du serveur DNS comme spécifié automatiquement par le fournisseur de services.

Valeurs

Activer / Désactiver

Route par défaut

Utilisez cette interface comme route par défaut pour tout le trafic sortant, sauf indication dans le Réseau de table> Routes.

Valeurs

Oui / Non

DNS-Passthrough

Lorsqu'elle est activée DNS-Passthrough transmettra les informations DNS affecté WAN au dispositif final.

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.

4.0 Configuration

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.

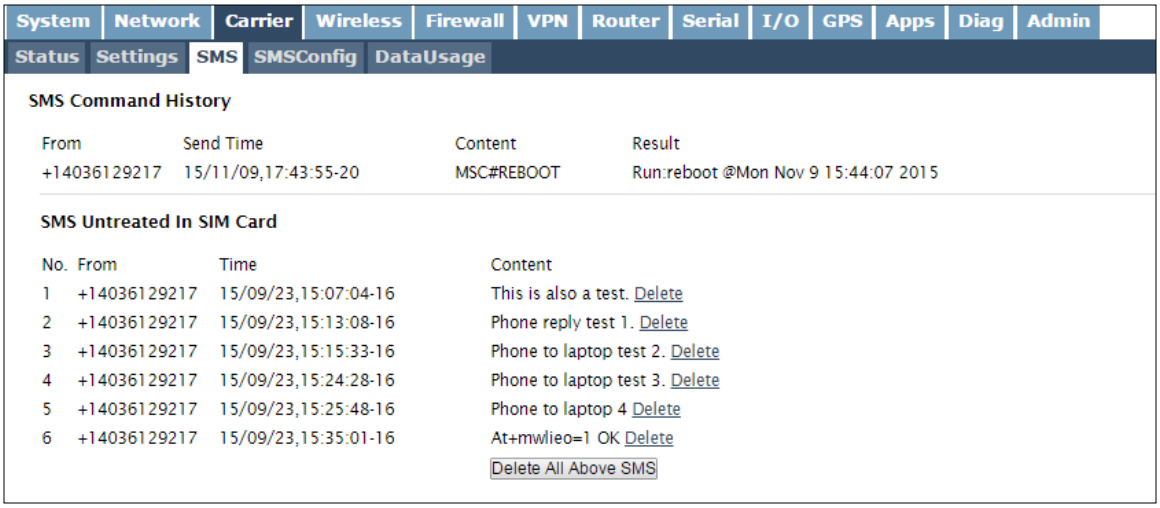


Image 4-3-3: SMS > SMS Historique des commandes

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

Image 4-3-4: SMS > SMS Configuration

4.0 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#EURD0 événement déclencheur rapport0
MSC#EURD1 événement déclencheur rapport1
MSC#EURD2 événement déclencheur rapport2
MSC#EURD3 événement déclencheur rapport3
MSC#GPSR0 gâchette gps rapport0
MSC#GPSR1 gâchette gps rapport1
MSC#GPSR2 gâchette gps rapport2
MSC#GPSR3 gâchette 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.

Valeurs

Activer / **Désactiver**

4.0 Configuration

Alertes SMS Système

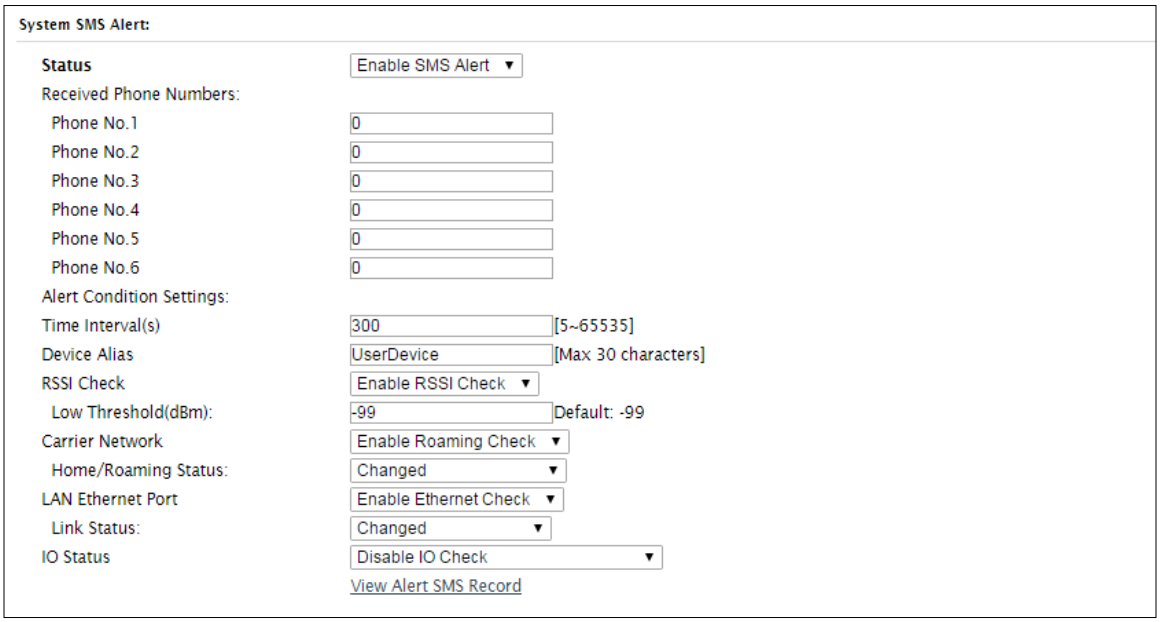


Image 4-3-6: SMS > SMS Alertes

Statut

Activer alertes SMS. IF alertes SMS activés seront envoyés lorsque les conditions sont remplies comme configuré pour les numéros de téléphone indiqués.

Valeurs

Activer / **Désactiver**

Numéros 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 ici.

Valeurs

300

Dispositif Alias

L'alias de l'appareil est un texte qui est envoyé avec le message SMS pour fournir des informations supplémentaires ou aider à identifier la source de l'alerte SMS.

Valeurs

UserDevice

4.0 Configuration

Vérifier RSSI

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 au-dessous de ce seuil, une alerte sera envoyé au numéro (s) spécifié.

Valeurs

-99

Réseau de l'opérateur

Activer ou désactiver les alertes SMS pour l'état d'itinérance.

Valeurs

Désactiver l'itinérance Vérifier
Activer l'itinérance Vérifier

Accueil / État Itinérance

The BulletPlus ne peut pas envoyer des alertes en fonction de l'état d'itinérance. Les débits de données en itinérance peuvent être coûteux et il est important de savoir quand un dispositif a commencé l'itinérance.

Valeurs

En Roaming
Modification ou En itinérance
Changé en itinérance

Ethernet

Activer ou désactiver les alertes SMS pour l'état de la liaison Ethernet du port LAN RJ45.

Valeurs

contrôle Ethernet Désactiver
Activer contrôle Ethernet

Ethernet Link Status

L'état de la liaison Ethernet du LAN (RJ45) peut être utilisé pour envoyer des alertes SMS. L'état de la liaison peut indiquer un problème avec le périphérique connecté.

Valeurs

Modifié
En aucun-link
Modification ou sans lien
Changé en no-link

I/O Status

Alertes SMS peuvent être envoyés sur la base des changements d'état des lignes numériques d'E / S.

Valeurs

Désactiver IO Vérifier
Activer: ENTREE Changed
Activer: Sortie Changed
Activer: entrée ou de sortie changé.

4.0 Configuration

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.

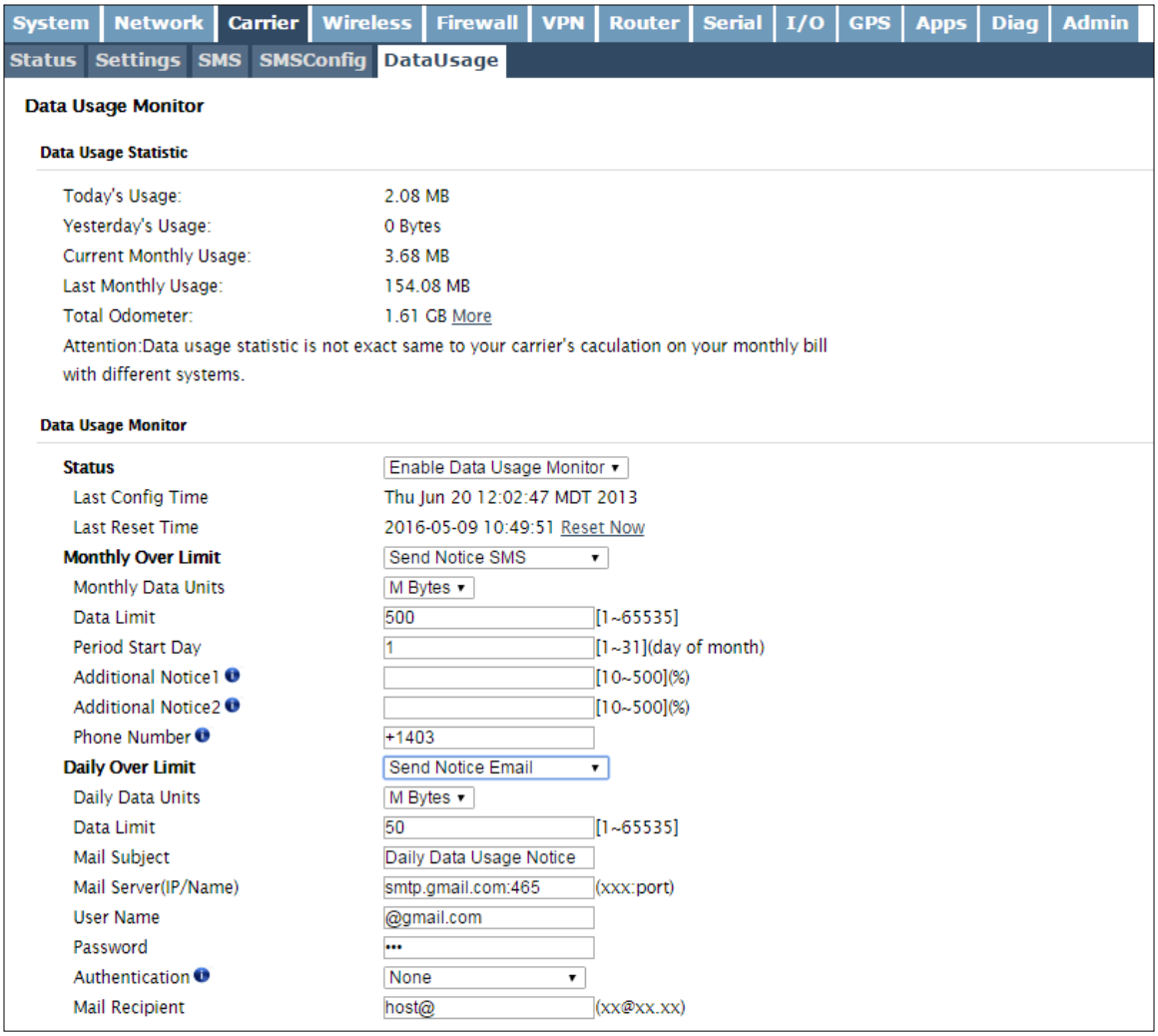


Image 4-3-7: Carrier > L'utilisation de données

Statut	Valeurs
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.	**Désactiver** Activer

4.0 Configuration

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.

Valeurs

Aucun
Envoyer avis SMS
Envoyer avis Email
Les deux SMS & Email

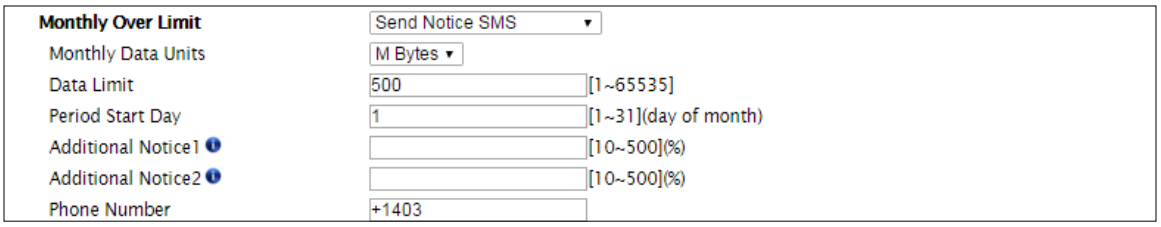


Image 4-3-9: Utilisation de données > SMS Config

Unité mensuelle / Données quotidiennes

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 données

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 la limite à 250 Mo, sélectionnez M Octets pour l'unité de données, et 250 pour la limite de données.

Valeurs

500

Période Jour Début

Pour le suivi mensuel, sélectionnez le jour où les cycles de facturation / de données commence. Ce jour chaque mois, le BulletPlus va réinitialiser les numéros de moniteur d'utilisation des données.

Valeurs

1 (Day of Month)

Avis supplémentaires 1/2

Jusqu'à deux (2) autres avis peuvent être envoyés sur la base d'un pourcentage (10-500%) de la valeur de seuil.

Valeurs

(blanc)

Numéro de téléphone

Si SMS est sélectionné comme méthode de notification, entrez le numéro de téléphone pour envoyer des messages SMS générés lors de l'utilisation de données dépasse les limites configurées.

Valeurs

+1403

4.0 Configuration

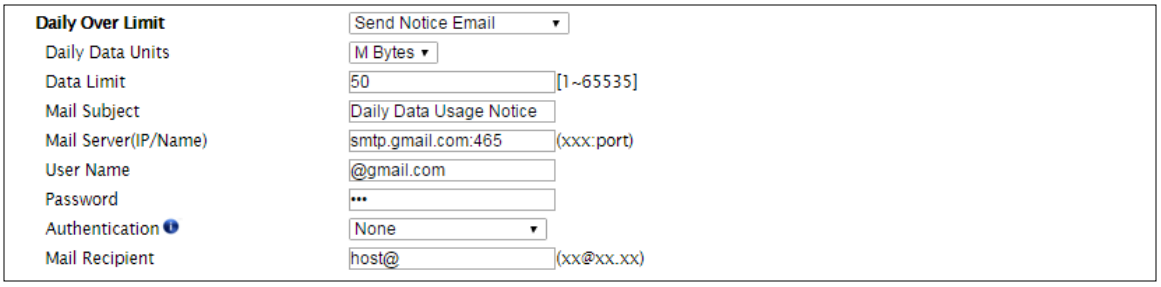


Image 4-3-10: Utilisation des données> Email Config

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 les jours et / ou des limites mensuelles d'utilisation sont dépassées.

Valeurs

Daily/Monthly Utilisation des données

Mail 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 -mail. Domaine ou adresse IP avec le port associé comme indiqué.

Valeurs

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 plupart des serveurs de messagerie nécessitent une authentification sur les e-mails sortants.

Valeurs

***

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 plupart des serveurs de messagerie nécessitent une authentification sur les e-mails sortants.

Valeurs

Aucun
SSL/TLS
STARTTLS
SSL/TLS + STARTTLS

Destinataire du courrier

Entrez l'adresse e-mail de la liste individuelle ou de distribution pour envoyer la notification par courrier électronique.

Valeurs

host@

4.0 Configuration

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.

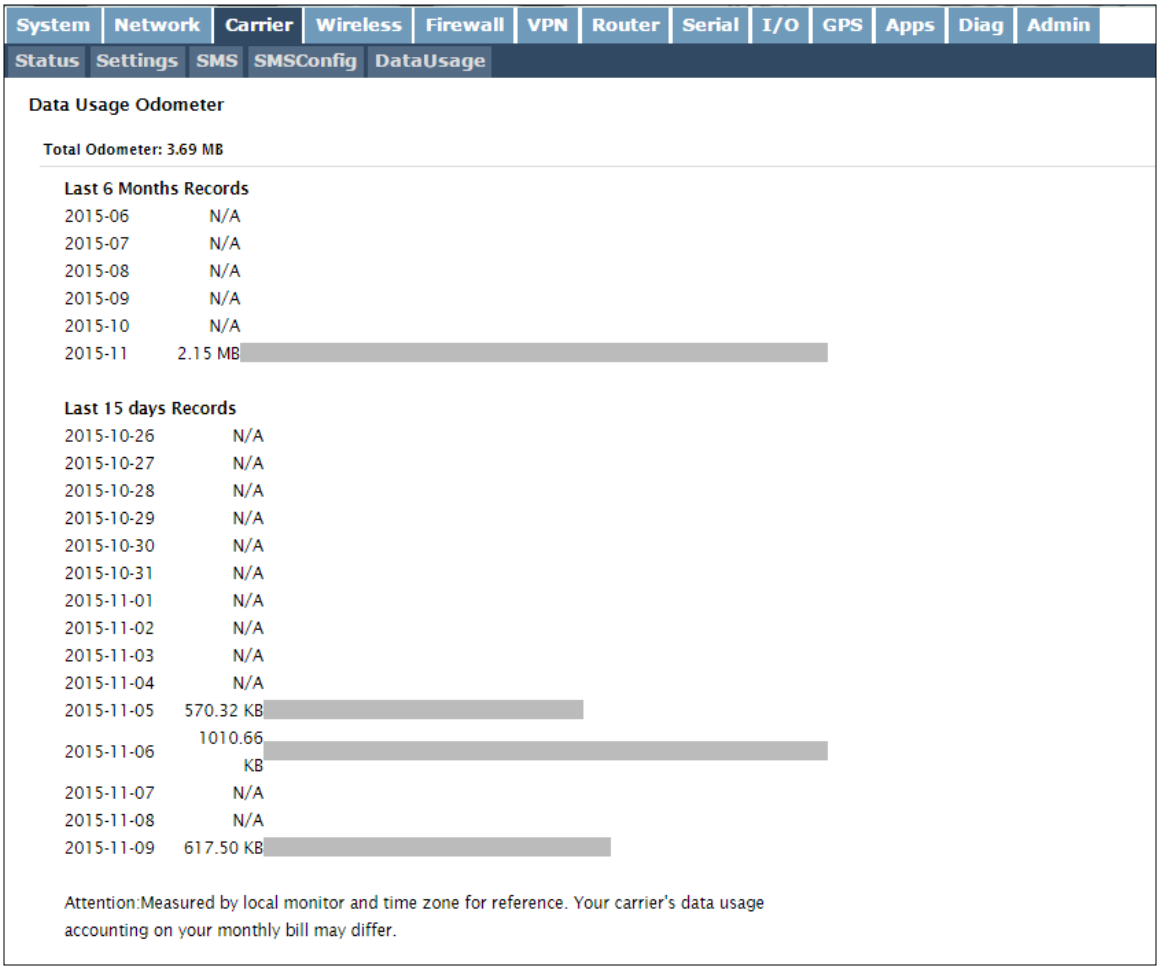


Image 4-3-11: Utilisation de données > Utilisation des données du compteur kilométrique

4.0 Configuration

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.

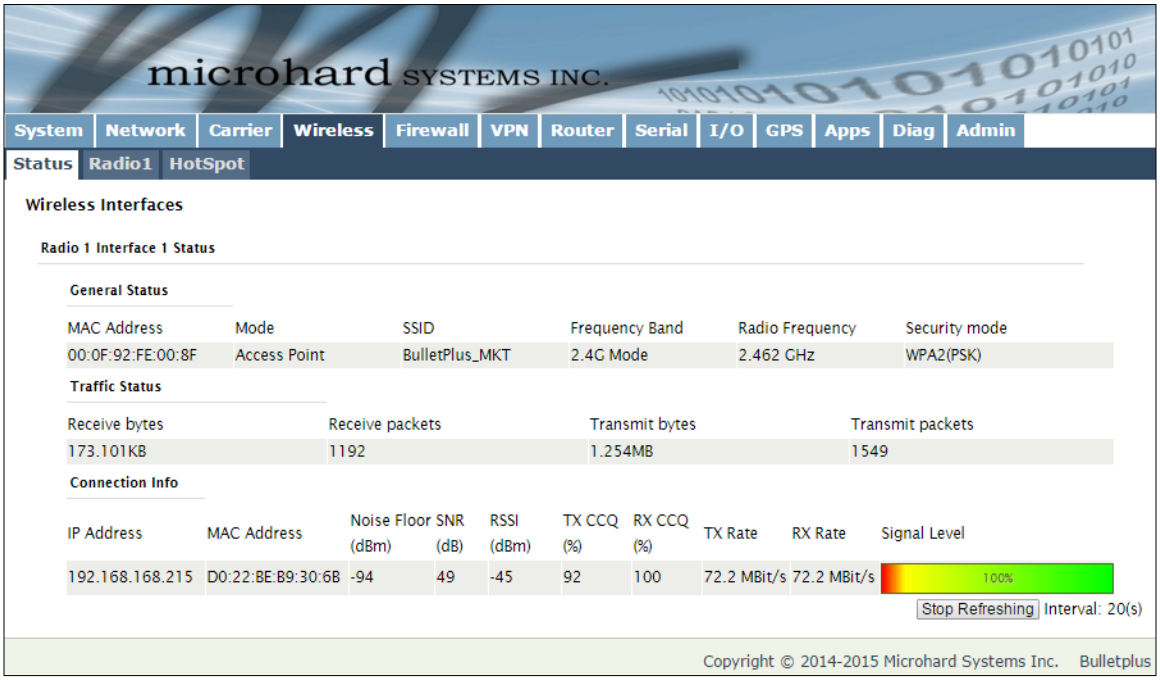


Image 4-4-1: Wireless > Statut

4.0 Configuration

4.4.2 Wireless > Radio1

Radio1 Phy Configuration

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.

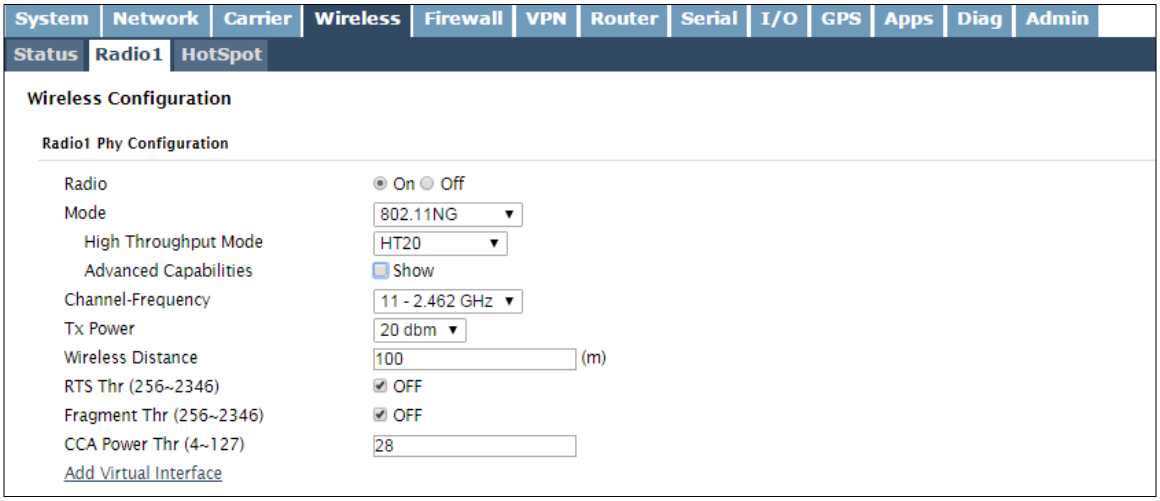


Image 4-4-2: Wireless > Radio Configuration

Radio

Cette option est utilisée pour activer le module radio ou désactiver. Si désactivé les connexions sans fil ne peuvent pas être faites. La valeur par défaut est activé.

Valeurs

Allumé / éteint

Mode

Le mode définit les standard sans fil à utiliser pour le réseau sans fil. Le BulletPlus soutient 802.11 / b / g / n modes comme on le voit ici. Sélectionnez le mode d'exploitation approprié dans la liste.

Les options ci-dessous dépendent et varient du mode de fonctionnement choisi ici.

Valeurs

802.11B SEULEMENT
802.11BG
802.11NG

Bande passante du canal

Apparaît seulement lors de l'utilisation des modes 802.11b ou b / g. largeurs de bande inférieures de canal peuvent fournir une plus grande portée et être moins sensibles au bruit, mais au compromis des débits de données. bande passante du canal supérieur peut fournir des taux plus élevés de données, mais sera plus sensible au bruit et plus courts potentiels de distance.

Valeurs

20MHz Taux normal

4.0 Configuration

Mode Haute Throughput

Sélectionnez HT20 pour un canal de 20MHz, ou HT40 pour un MHz canal 40. Le canal de 40MHz est composé de 2 canaux de 20MHz adjacents et + et désigné pour utiliser le plus élevé ou plus bas des canaux adjacents.

Valeurs

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

Channel-Freq

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.

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.

Valeurs

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

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).

4.0 Configuration

Distance sans fil

Le paramètre sans fil Distance permet à un utilisateur de régler la distance prévue le signal WiFi a besoin de voyager. La valeur par 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.

Valeurs

100

RTS Thr (256 ~ 2346)

Une fois la taille du paquet défini RTS de seuil est atteint, le système appellera RTS / CTS contrôle de flux. Un grand seuil RTS permettra 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.

Valeurs

Allumé / **éteint**

Fragment Thr (256 ~ 2346)

Le seuil de fragmentation permet au système de modifier la taille maximale des paquets RF. L'augmentation de la taille des paquets RF 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.

Valeurs

Allumé / **éteint**

CCA 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 pour la transmission. Changer le seuil aura un impact sur la façon dont le BulletPlus Wifi détermine la disponibilité des canaux.

Valeurs

28

4.0 Configuration

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.

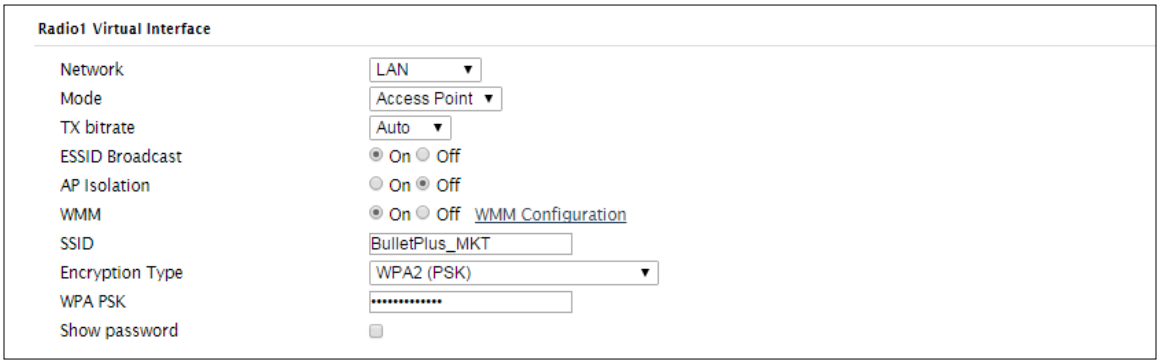


Image 4-4-3: Wireless > Radio Configuration

Réseau

Choisissez entre RL ou WAN pour l'interface virtuelle. Si les interfaces Réseau supplémentaires ont été définis dans la section Réseau> RL, le nom de l'interface apparaîtra également ici.

Valeurs

RL
WAN
Etc..
(Interfaces supplémentaires ...)

Mode

Point d'accès - Un point d'accès peut fournir une connexion de données sans fil à de nombreux clients, tels que les gares, les répéteurs, ou d'autres dispositifs sans fil pris en charge, tels que les ordinateurs portables, etc.

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.

Valeurs

Point d'accès
Client
Répétiteur

Gare / Client - Une station peut maintenir une connexion sans fil, à savoir 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.

4.0 Configuration

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

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)

802.11n (HT20/HT40)

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 désactivation de la diffusion SSID permet de sécuriser le réseau sans fil. Activation de la diffusion du SSID (nom du réseau) permettra d'autres de «voir» le réseau sans fil et peut-être tenter de 'rejoindre' elle.

Valeurs

On / Off

AP Isolation

Lorsque Isolement AP est activé dispositifs sans fil connectés à ce SSID ne sera pas en mesure de communiquer les uns avec les autres. En d'autres termes, si l'BulletPlus est utilisé comme un point chaud pour de nombreux clients sans fil, AP Isolation assurerait la sécurité pour les clients en ne permettant pas l'accès à un autre appareil sans fil.

Valeurs

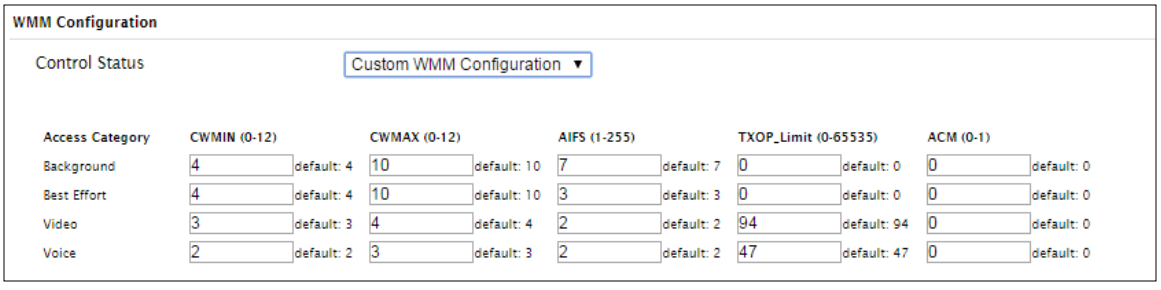
On / **Off**

WMM

WiFi Multimedia (WMM) est une fonction qui améliore la qualité de service sur un réseau en donnant la priorité des paquets de données en fonction du type de données. (Vidéo, voix, Best Effort, Fond).

Valeurs

On / **Off**



4.0 Configuration

SSID: Service Set Identifier. Le «nom» d'un réseau sans fil. Dans un réseau sans fil ouvert, le SSID est diffusé; dans un système fermé non. Le SSID doit être connue par un client potentiel pour qu'il soit en mesure d'accéder au réseau sans fil.

Modifiez la valeur par défaut pour le nom du réseau à quelque chose d'unique pour votre réseau. Pour ce faire, pour une mesure supplémentaire de sécurité et de différencier votre réseau à partir d'autres pouvant se trouver à proximité.

SSID

Tous les dispositifs de connexion aux BulletPlus dans un réseau donné doivent utiliser le SSID du BulletPlus. Cette adresse de réseau 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.

Valeurs

BulletPlus

Type de chiffrement

Les types de chiffrement définit le type de sécurité utilisé pour l'interface sans fil, à se joindre à un réseau d'un périphérique doit connaître le mot de passe / mot de passe / clé correcte.

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.

Valeurs

Désactiver
WPA (PSK)
WPA2 (PSK)
WPA+WPA2 (PSK)
WPA Enterprise (RADIUS)
WPA2 Enterprise (RADIUS)
WPA+WPA2 Enterprise(RADIUS)

WPA PSK

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

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 serveur d'authentification RADIUS ici.

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

4.0 Configuration

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.

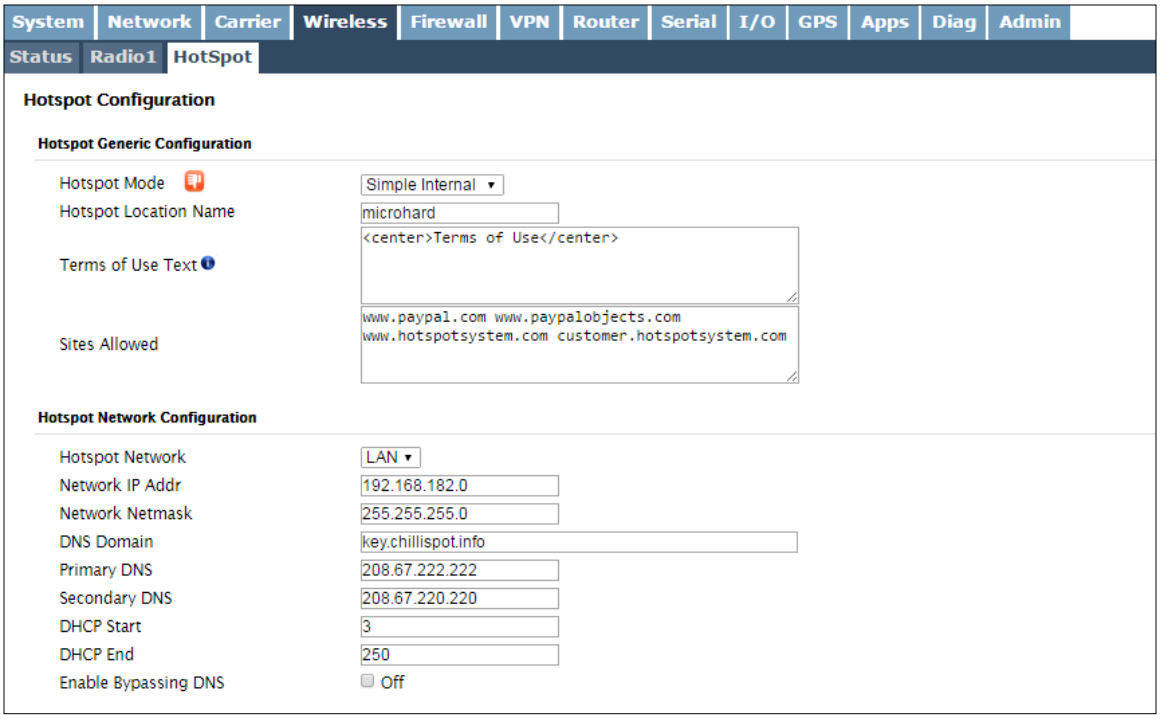


Image 4-4-4: Wireless > Configuration Réseau Hotspot

Hotspot Mode

Utilisez cette option pour activer ou désactiver le service d'authentification hotspot. Il y a trois options différentes pour le mode Hotspot:

Simple interne - Afficher les termes d'un texte simple basé sur l'utilisation ou de la déclaration aux utilisateurs connectés.
Simple externe - Afficher une page externe
RADIUS / UAM - Utiliser un service d'authentification 3ème Partie pour authentifier et / ou inviter les utilisateurs à accepter les conditions de service.

Valeurs

Désactiver
interne simple
simple externe
RADIUS / UAM

UAM URL de connexion

Si le mode Hotspot, RADIUS / UAM est choisi, spécifiez le hotspot URL donnée par votre fournisseur de services. L'adresse de l'UAM Server, le portail d'authentification.

Valeurs

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

4.0 Configuration

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> LAN, qui sont dédiées aux dispositifs hotspot. * 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. *	**Valeurs** *Varies*

Réseau Adresse IP	
Indiquez l'adresse IP de l'application Hotspot. Tous les clients hotspot recevront une adresse IP dans le même réseau que le Hotspot.	**Valeurs** 192.168.182.0

Netmask Réseau	
Spécifiez le Netmask de l'application Hotspot. Tous les clients hotspot recevront une adresse IP dans le même réseau que le Hotspot.	**Valeurs** 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 périphériques connectés au réseau Hotspot.	**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 est activé, le Hotspot attribue les adresses IP aux appareils connectés, sélectionnez la plage de départ ici.	**Valeurs** 3

DHCP Fin	
Lorsque les périphériques se connectent au Bullet plus Wifi et Hotspot est activé, le Hotspot attribue les adresses IP aux appareils connectés, sélectionnez la plage de fin ici.	**Valeurs** 250

4.0 Configuration

Hotspot Radius Configuration

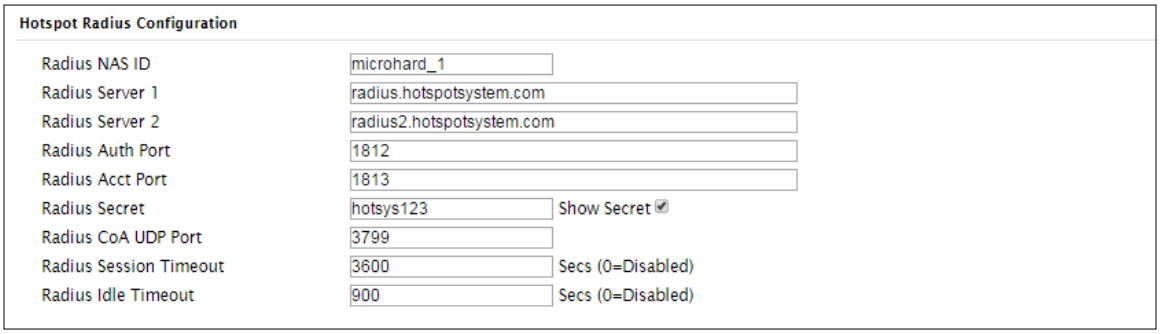


Image 4-4-5: Wireless > Hotspot Radius Configuration

Radius NAS ID

Ceci est le nom de RADIUS de votre Hotspot comme donné par votre fournisseur de services Hotspot.

Valeurs

Microhard_1

Radius Server 1

Comme attribué par le fournisseur de services de Hotspot, le nom ou l'adresse IP du RADIUS Server principal.

Valeurs

radius.hotspotsystem.com

Radius Server 2

Comme attribué par le fournisseur de services de Hotspot, le nom ou l'adresse IP de l'autre serveur RADIUS.

Valeurs

radius2.hotspotsystem.com

Radius Auth Port

Le numéro Radius Authentication Port. La valeur par défaut est 1812. Cela est fourni par votre fournisseur de services de Hotspot.

Valeurs

1812

Radius Acct Port

Le numéro de compte Radius Port. La valeur par défaut est 1813. Cela est fourni par votre fournisseur de services de Hotspot.

Valeurs

1813

Radius Secret

Aussi appelé une clé partagée, tel est le mot de passe RADIUS attribué par votre fournisseur Hotspot.

Valeurs

hotsys123

4.0 Configuration

Radius CoA UDP Port	
Spécifiez le rayon CoA UDP Port ici. Ces informations sont fournies par le fournisseur de service de hotspot.	**Valeurs** 3799

Radius expiration de la session	
Spécifiez le rayon Session Timeout. En quelques secondes, 0 = désactivé.	**Valeurs** 3600

Radius Délai d'inactivité	
Spécifiez le délai d'inactivité Radius. En quelques secondes, 0 = désactivé.	**Valeurs** 900

4.0 Configuration

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 pare-feu fonctionne. Le Tout, Filtre, Nat, Raw, et les options Mangle peuvent être utilisés pour afficher les différents aspects du pare-feu.

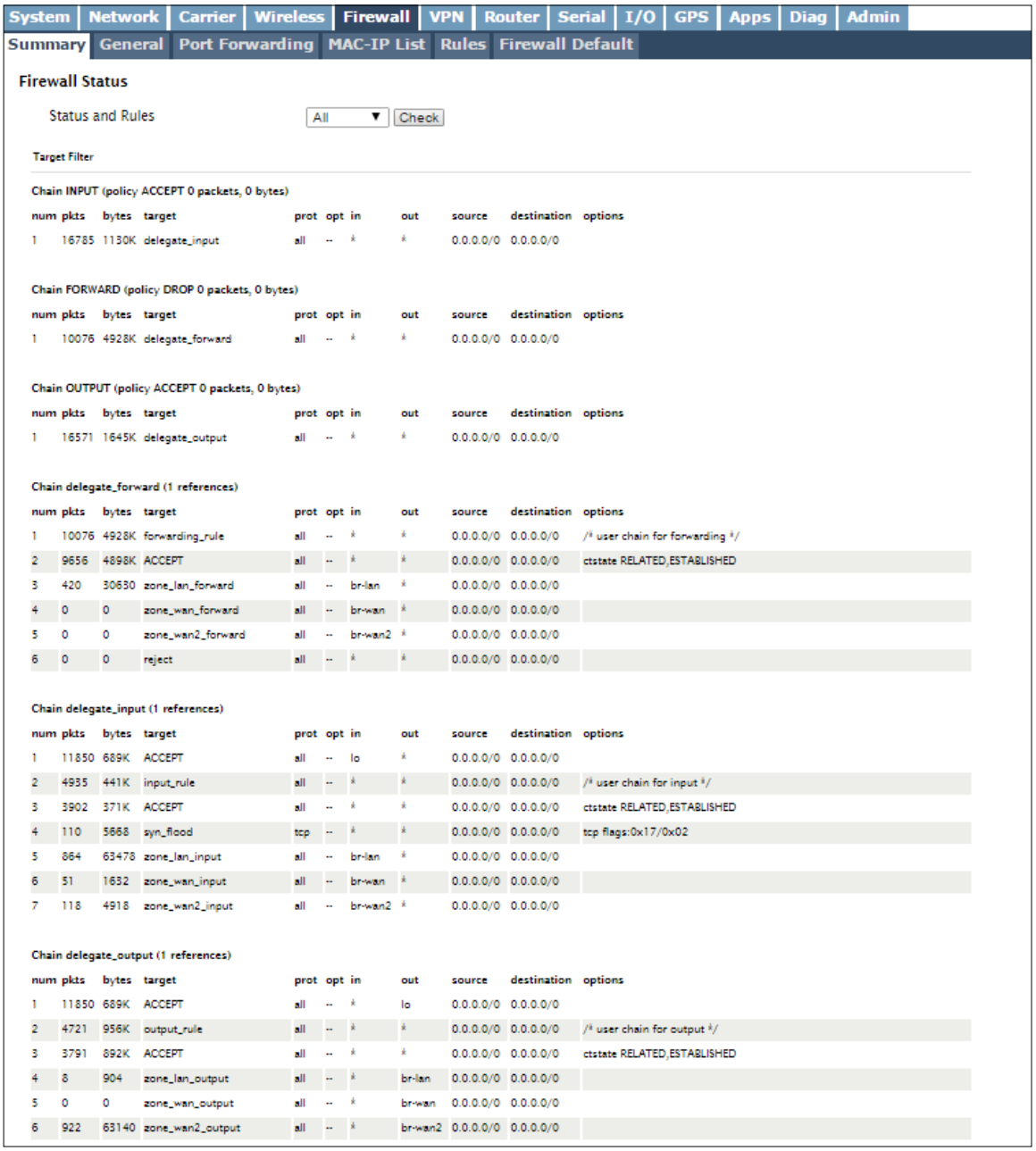


Image 4-5-1: Pare-feu > Statut

4.0 Configuration

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.

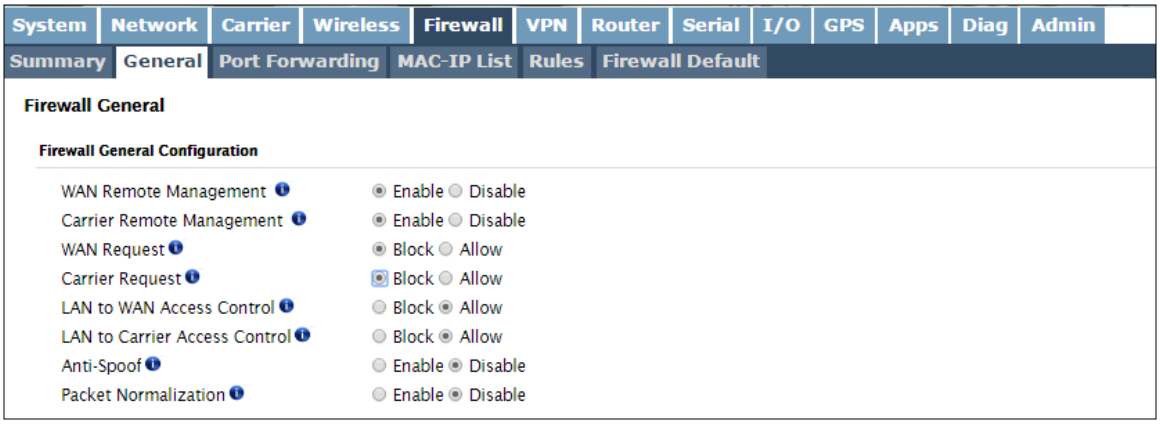


Image 4-5-2: Pare-feu > Général

Pour les meilleures pratiques et de contrôler l'utilisation des données, il est essentiel que le pare-feu 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.

Gestion à distance WAN

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 peut être accessible à partir du réseau local (ou cellulaire si elle est activée).

Valeurs

Activer / Désactiver

Gestion à distance des transporteurs

Autoriser la gestion à distance du BulletPlus du côté cellulaire de l'utilisation de l'interface utilisateur Web sur le port 80 (HTTP), et 443 (HTTPS). Si elle est désactivée, la configuration ne peut être accessible à partir du réseau local (ou WAN si activé).

Valeurs

Activer / Désactiver

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.

Demande WAN

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 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.

Valeurs

Bloquer / Autoriser

Demande Carrier

Lorsque bloqué toutes les demandes provenant d'appareils sur le côté cellulaire (Wireless transporteur) sera bloqué, sauf indication contraire dans les règles 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.

Valeurs

Bloquer / Autoriser

4.0 Configuration

LAN to WAN Access Control

Autorise ou bloque le trafic du réseau local d'accéder au WAN, sauf indication contraire en utilisant les règles d'accès, MAC, et la configuration Liste IP.

Valeurs

Bloquer / **Autoriser**

LAN Access Control Transporteur

Autorise ou bloque le trafic du réseau local accéder à la connexion cellulaire, sauf indication contraire en utilisant la configuration des règles d'accès, MAC et IP Liste.

Valeurs

Bloquer / **Autoriser**

Anti-Spoof

La protection anti-Spoof est de créer des règles de pare-feu attribués à l'interface externe (WAN & Cellular) du pare-feu qui examine l'adresse de la source de tous les paquets qui traversent cette interface provenant de l'extérieur. Si l'adresse appartient au réseau interne ou le pare-feu lui-même, le paquet est abandonné.

Valeurs

Activer / **Désactiver**

Normalisation de paquets

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**

4.0 Configuration

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.

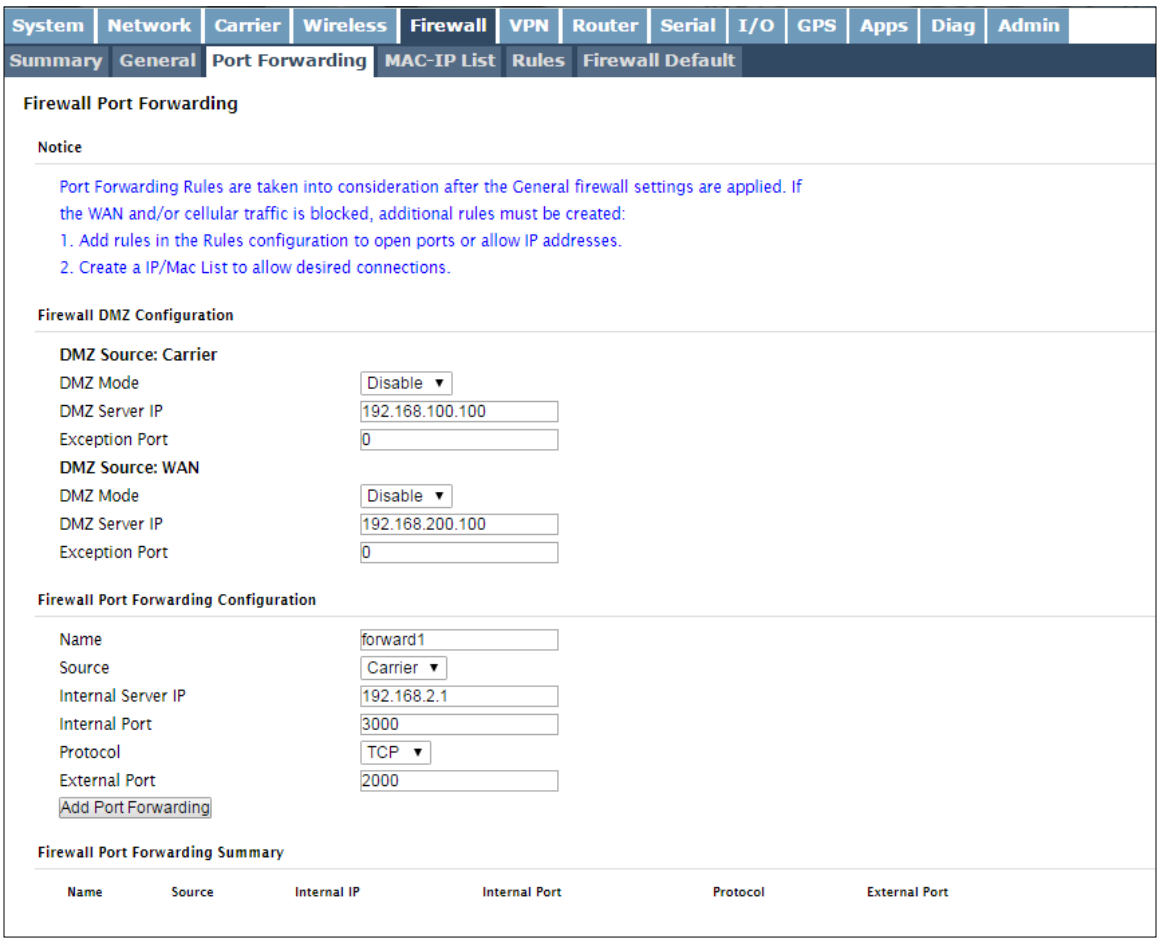


Image 4-5-3: Pare-feu > Port Forwarding

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.

4.0 Configuration

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.

DMZ Mode

Activer ou désactiver le mode DMZ. DMZ peut être utilisé pour transférer tout le trafic vers l'adresse IP du serveur DMZ énumérés ci-dessous.

Valeurs

Désactiver / Activer

DMZ Server IP

Entrez l'adresse IP de l'appareil sur le côté LAN du BulletPlus où tout le trafic sera transmis à.

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 qui est exclu de conserver le contrôle externe de la BulletPlus.

Valeurs

0

Pare-feu Configuration du port Forwarding

Nom

Ceci est tout simplement un domaine où on ajoute une référence commode ou la description à la règle. Chaque Forward doit avoir un nom de règle unique et peut utiliser jusqu'à 10 caractères.

Valeurs

Forward

La source

Sélectionnez la source pour le trafic, soit de la 3G / cellulaire ou à partir du WAN.

Valeurs

Carrier / WAN

Internal Server IP

Entrez l'adresse IP de l'interne destiné (i.p. sur le côté LAN de Bullet Plus) serveur. Ceci est l'adresse IP du périphérique que vous transférez le trafic vers.

Valeurs

192.168.2.1

Port Interne

Cible numéro de port du serveur interne sur le LAN IP est entré ci-dessus.

Valeurs

3000

Protocole

Sélectionnez le type de protocole de transport utilisé. Par exemple Telnet utilise le protocole TCP, SNMP utilise UDP, etc.

Valeurs

TCP / UDP / Both

Port Externe

Numéro de port de la demande entrante (de 4G / WAN côté).

Valeurs

2000

4.0 Configuration

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.

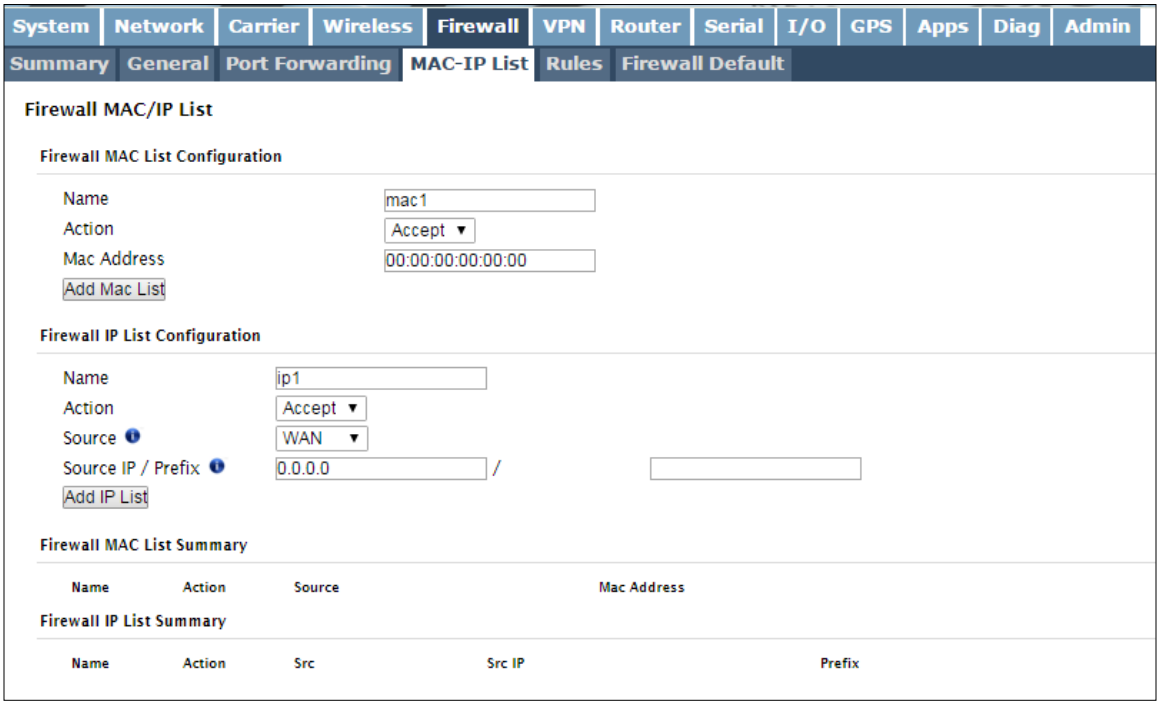


Image 4-5-5: Pare-feu > Liste MAC-IP

Pare-feu Configuration Liste MAC

Nom de la règle

Le champ Nom de la règle est tenu de donner la règle un nom commode pour référence. Chaque règle doit avoir un nom unique, jusqu'à 10 caractères.

Valeurs

MAC_List

Adresse Mac

Indiquez l'adresse MAC à ajouter à la liste. Doit être entré dans le format correct comme on le voit ci-dessus. Pas sensible à la casse.

Valeurs

00:00:00:00:00:00

4.0 Configuration

Pare-feu Configuration Liste MAC (Suite)

Action	
L'action est utilisée pour définir comment la règle gère la demande de connexion. ACCEPTER permettra une connexion, alors que REJETER (erreur) et DROP (tranquillement abandonné), refusera les connexions.	**Valeurs** **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 pour référence. Chaque règle doit avoir un nom unique, jusqu'à 10 caractères.	**Valeurs** **IP_List**

Action	
L'action est utilisée pour définir comment la règle gère la demande de connexion. ACCEPTER permettra une connexion, alors que REJETER (erreur) et DROP (tranquillement abandonné), refusera les connexions.	**Valeurs** **ACCEPTER** / DROP / REJET

La source	
Entrez la zone spécifique que la Liste IP s'appliquera, Cellular, LAN, WAN ou None (les deux).	**Valeurs** LAN/LAN1/WAN/Cell/USB **NONE**

Source IP Address	
Faites correspondre le trafic entrant de la gamme IP source spécifiée. Boîtes acceptent les adresses IP individuelles sans masques de 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.)	**Valeurs** **192.168.0.0**

4.0 Configuration

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.

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

Annexe D: Exemple de pare-feu

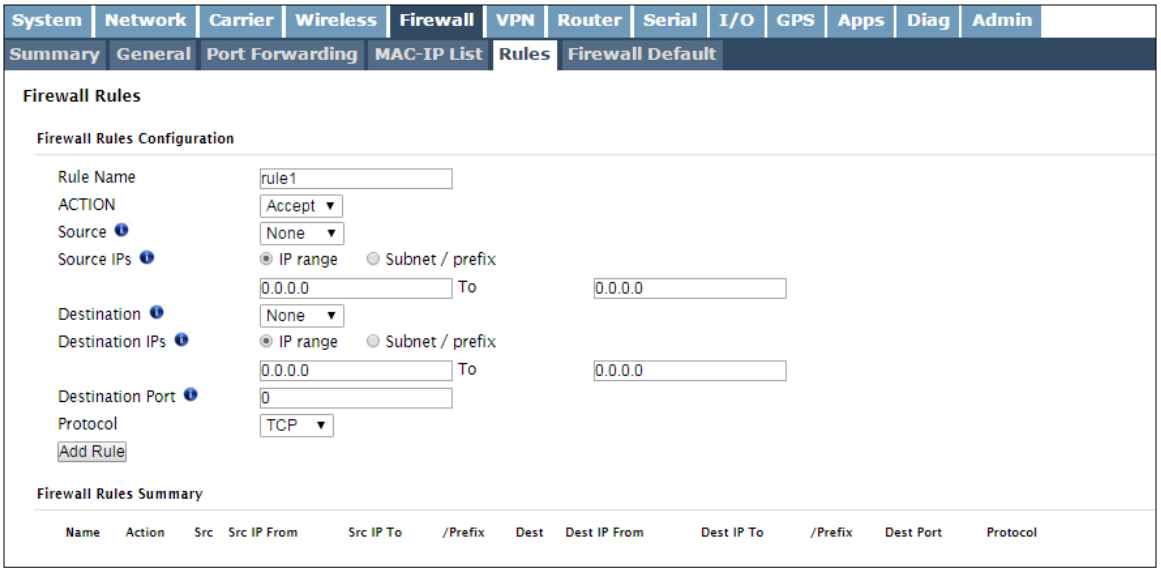


Image 4-5-6: Pare-feu > Règles

Nom de la règle

Le nom de la règle est utilisée pour identifier la règle créée. Chaque règle doit avoir un nom unique et jusqu'à 10 caractères peut être utilisé.

Valeurs

personnages

Action

L'action est utilisée pour définir comment la règle gère la demande de connexion.
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.

Valeurs

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

4.0 Configuration

Source IPs

Faites correspondre le trafic entrant de la gamme IP source spécifiée. Boîtes acceptent les adresses IP individuelles sans masques de 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.)

Valeurs

192.168.0.0 à 192.168.0.0

Destination

Sélectionnez la zone qui est la destination prévue du trafic de données. 3G / 4G applique à la connexion sans fil à l'opérateur cellulaire et le réseau local, LAN1, USB se réfère aux connexions locales sur les BulletPlus.

Valeurs

LAN/LAN1/cellules/WAN/ USB

IP de destination

Faites correspondre le trafic entrant de la gamme IP de destination spécifié. Boîtes acceptent les adresses IP individuelles sans masques de 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.)

Valeurs

192.168.0.0 à 192.168.0.0

Le port de destination

Faites correspondre le trafic entrant dirigé vers le port de destination ou port plage donnée. (Pour spécifier une plage de ports utilisent un De: A (100: 200) format)

Valeurs

0

Protocole

Le champ de protocole définit le type de protocole de transport contrôlé par la règle.

Valeurs

TCP
UDP
Tous les deux
ICMP

4.0 Configuration

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.

Image 4-4-7: Pare-feu > Pare-feu par défaut

4.0 Configuration

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.

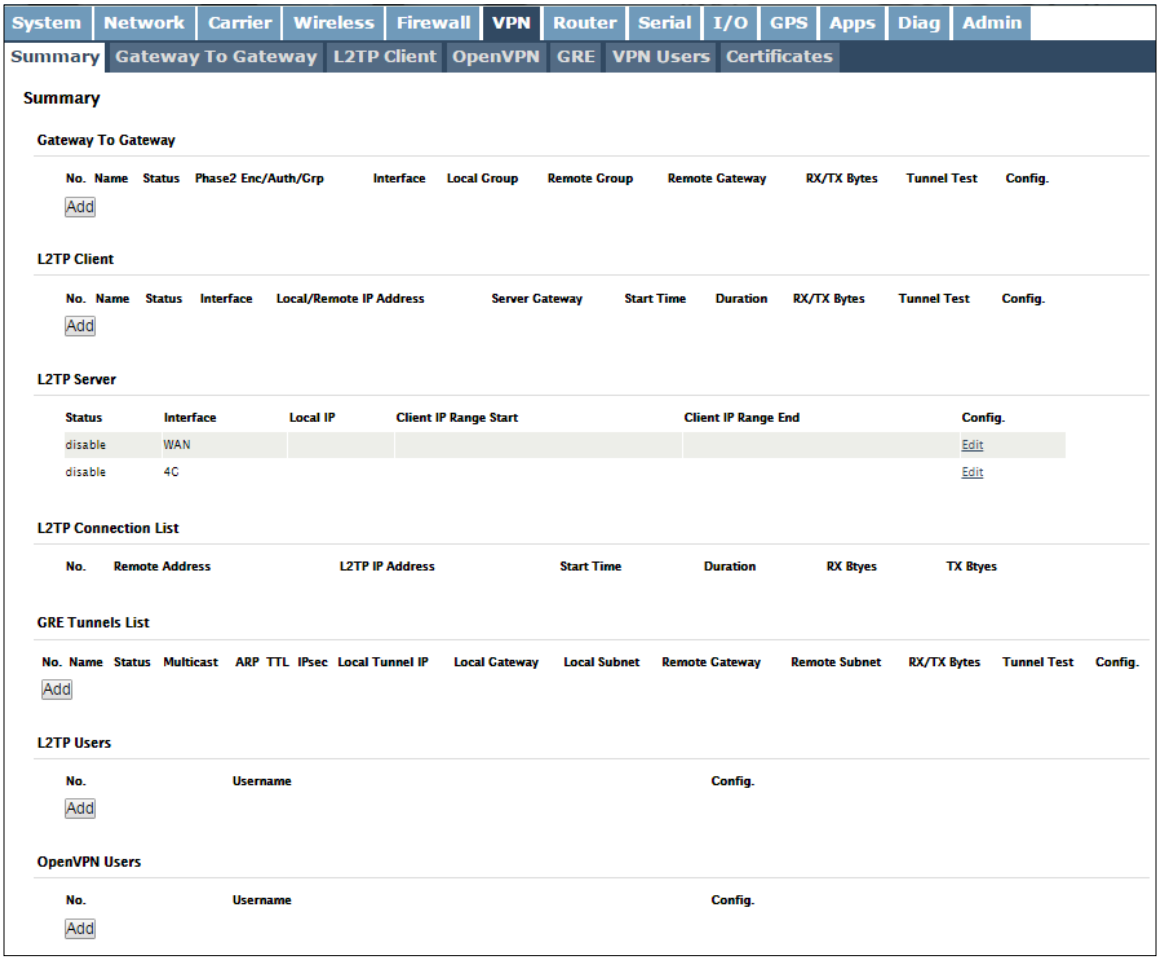


Image 4-6-1: VPN > Résumé

4.0 Configuration

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.

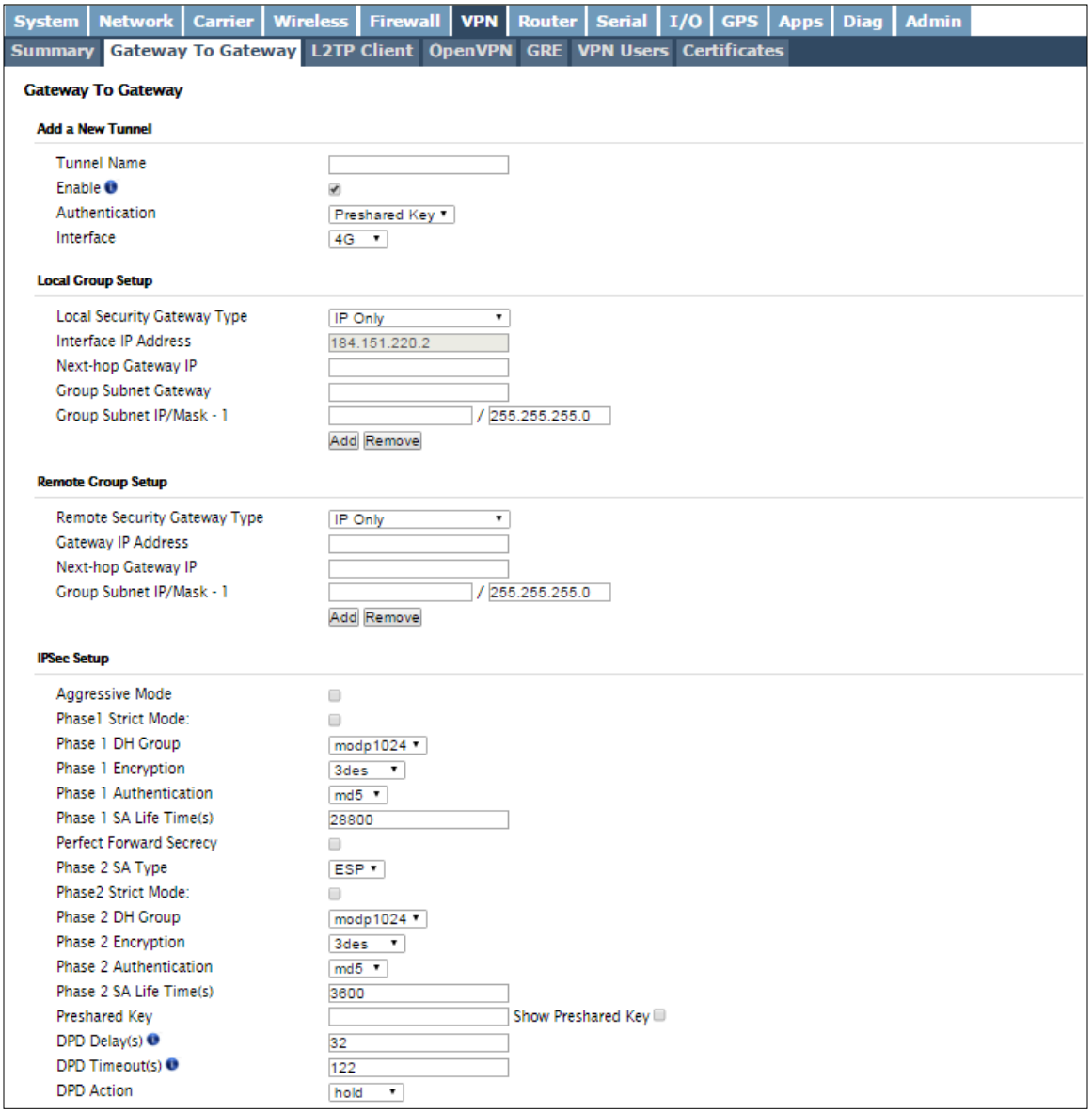


Image 4-6-2: VPN > Passerelle Gateway

Tunnel Nom

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

Valeurs

tunnel1

4.0 Configuration

Activer

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

Valeurs

Enable (Checked)

Local Group Setup

Local Security Gateway Type

Spécifiez la méthode d'identification du routeur pour établir le tunnel VPN. 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 une adresse IP statique ou une adresse IP dynamique avec l'id de serveur pour établir une connexion.

Valeurs

IP Only
IP + Server ID
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 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 routeurs doivent connaître les uns les autres noms pour établir une connexion.

Valeurs

(Pas par défaut)

Next-hop passerelle IP

Next-hop passerelle signifie que l'adresse IP de nouvelle passerelle-hop pour la connexion du participant de la passerelle locale ou à distance au réseau public.

Valeurs

(Pas par défaut)

Groupe Subnet IP

Définir le réseau local en spécifiant le sous-réseau local. Les routeurs locaux et distants doivent utiliser différents sous-réseaux.

Valeurs

(Pas par défaut)

4.0 Configuration

Groupe Subnet Mask

Spécifiez le masque de sous-réseau de l'adresse du réseau local.

Valeurs

255.255.255.0

Groupe sous-réseau Passerelle

Entrez la porte d'entrée pour le réseau de groupe local.

Valeurs

(Pas par défaut)

Configuration des groupes à distance

Télécommande Type 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 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)

Valeurs

IP seulement
IP + serveur ID
Dynamic IP + serveur ID

Adresse IP de la passerelle

Si le routeur VPN distant possède une adresse IP statique, entrez l'adresse IP de la passerelle VPN à distance ici.

Valeurs

(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 dans le format @name, où nom peut être quelque chose. Les deux routeurs doivent connaître les uns les autres noms pour établir une connexion.

Valeurs

(Pas par défaut)

Next-hop passerelle IP

Next-hop passerelle signifie que l'adresse IP de nouvelle passerelle-hop pour la connexion du participant de la passerelle locale ou à distance au réseau public.

Valeurs

(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

4.0 Configuration

Configuration IPsec

Phase 1 DH Group

Sélectionner la valeur pour correspondre aux valeurs requises par le routeur VPN distant.

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

Phase 1 Authentication

Sélectionner la valeur pour correspondre à la Phase d'Authentification 1 utilisée par le routeur VPN distant.

Valeurs

md5
sha1

Phase 1 SA Life Time

Sélectionner la valeur pour correspondre aux valeurs requises par le routeur VPN distant.

Valeurs

28800

Perfect Forward 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 routeur VPN distant.

Valeurs

modp1024
modp1536
modp2048

Phase 2 Le chiffrement

Sélectionner la valeur pour correspondre à la phase 1 type de cryptage utilisé par le routeur VPN distant.

Valeurs

3des
aes
aes128
aes256

4.0 Configuration

Authentification Phase 2

Sélectionner la valeur pour correspondre à la Phase d'Authentification 1 utilisée par le routeur VPN distant.

Valeurs

md5
sha1

Phase 2 SA Life Time

Sélectionner la valeur pour correspondre aux valeurs requises par le routeur VPN distant.

Valeurs

3600

Clé Pré-Partagée

Réglez le Shared Key Pré requis pour l'authentification avec le routeur VPN distant.

Valeurs

password

Retards DPD

Dead Peer Detection est utilisé pour détecter s'il y a un pair mort. Réglez le DPD Délai (secondes), selon les besoins.

Valeurs

32

DPD temps libre(s)

Réglez le DPD (de Dead Peer Detection) Délai (secondes), selon les besoins.

Valeurs

122

DPD Action

Réglez le DPDaction, détenir ou clair, selon les besoins.

Valeurs

Hold
Clear

4.0 Configuration

4.6.3 VPN > L2TP Client

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

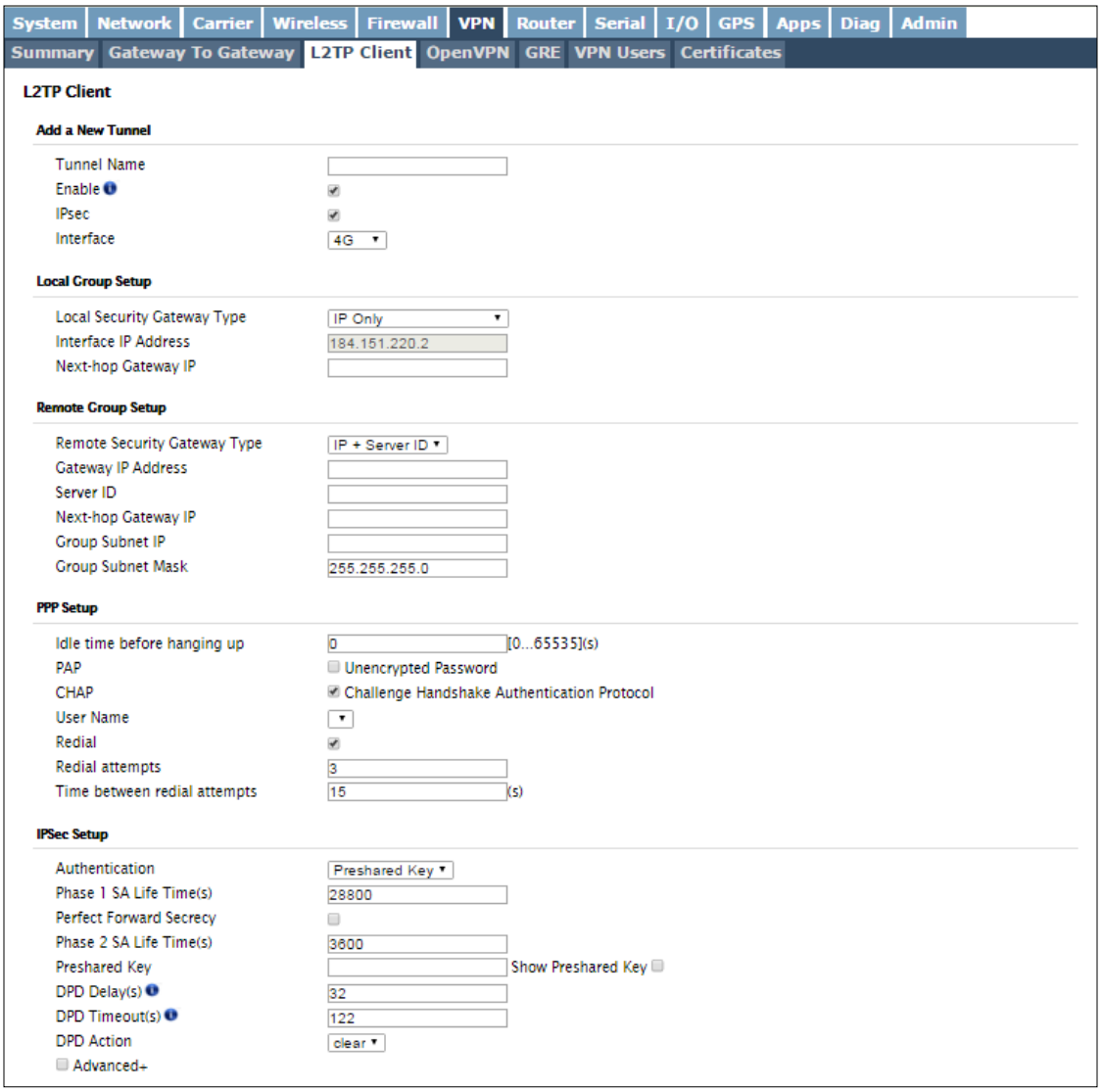


Image 4-6-3: VPN > Client to Gateway

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.

Valeurs

Activer (Vérifié)

4.0 Configuration

Local Adresse IP Interface

Cela permet d'afficher le courant BulletPlus WAN (cellulaire) Adresse IP.

Valeurs

Current IP

Adresse distante IP de la passerelle

Entrez l'adresse IP de la passerelle à distance que vous souhaitez établir une connexion avec.

Valeurs

none

ID de serveur distant

Certains serveurs exigent que vous connaissez l'ID du serveur, ainsi que l'adresse IP. Entrez l'ID du serveur du routeur distant ici.

Valeurs

none

IP Subnet à distance

Afin de communiquer avec les dispositifs de l'autre côté du tunnel, le BulletPlus doit connaître les données à passer à travers le tunnel, pour ce faire entrer l'adresse IP du réseau de sous-réseau à distance ici.

Valeurs

none

Masque de sous-réseau à distance

Saisissez le masque de sous-réseau à distance.

Valeurs

none

Temps d'inactivité avant de raccrocher

Saisissez le temps d'inactivité (en secondes) à attendre avant 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

Clé Pré-Partagée

La clé pré partagée est nécessaire pour se connecter au serveur L2TP.

Valeurs

0

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

4.0 Configuration

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.

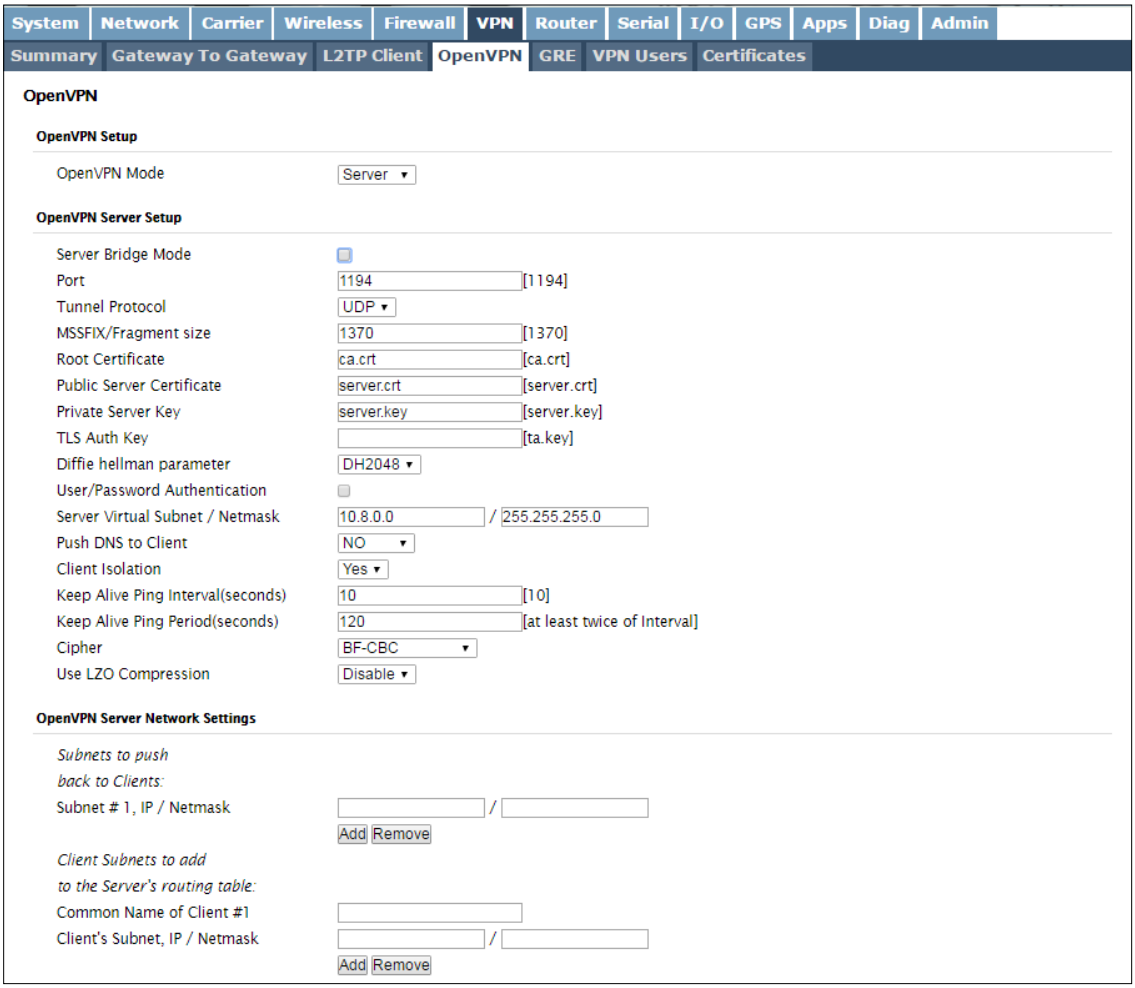


Image 4-6-4: VPN > OpenVPN Serveur

OpenVPN Mode

Activer / Désactiver le mode OpenVPN en sélectionnant le mode d'opérer dans, client ou serveur. Lorsque le serveur est activée, il sera l'écoute des demandes de connexion entrantes des clients OpenVPN.

Valeurs

Client / Serveur / **Désactiver**

Port

Le port TCP / UDP que le serveur est à l'écoute. Par défaut est 1194

Valeurs

1194

4.0 Configuration

Protocole de tunnel

Sélectionnez le protocole de tunnel à utiliser. Les options sont TCP et UDP, la valeur par défaut est UDP.

Valeurs

TCP / **UDP**

MSSFIX / taille de Fragment

Le maximum résultant UDP envoyer la taille des paquets après la OpenVPN a entièrement encapsulé données. Les paquets qui dépassent la valeur maximale seront fragmentés.

Valeurs

1370

Root Certificate

Le fichier racine de certificat (fichier CA) que tout le serveur et les clients doivent avoir en commun.

Valeurs

ca.crt

Certificat de serveur public

Le certificat de serveur public qui est le fichier de certificat qui réside uniquement sur le serveur.

Valeurs

server.crt

Key Private Server

La clé de serveur privé, qui ne devrait pas être divulguée.

Valeurs

server.key

TLS Auth Key

Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS.

Valeurs

(Pas par défaut)

Authentification utilisateur / mot de passe

Sélectionnez le nom d'utilisateur OpenVPN comme setup / défini dans le menu Utilisateurs VPN.

Valeurs

(Pas par défaut)

Diffie paramètre hellman

Sélectionnez entre 1024 et 2048 bit clés bits Diffie Hellman pour la sécurité.

Valeurs

DH2048 / DH1024

Serveur virtuel Subnet / Subnet Mask

Le sous-réseau et sous-réseau masque que le serveur va créer pour attribuer l'adresse à lui-même et les clients.

Valeurs

10.8.0.0

4.0 Configuration

Poussez 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 être saisie manuellement.

Valeurs

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 «voir» les uns des autres. Par défaut, les clients ne verront le serveur.

Valeurs

Non / **Oui**

Keep Alive Ping Interval

La directive vie keep provoque des messages de ping-like à envoyer avant en arrière sur le lien afin que chaque partie sait quand l'autre côté est descendu. Par défaut 10 secondes.

Valeurs

10

Keep Alive Ping Période

Par défaut 120 secondes. Ping toutes les 10 secondes, on suppose que les pairs à distance est en panne si aucun ping reçu au cours d'une deuxième période de 120 fois. (Doit être au moins deux fois l'intervalle spécifié ci-dessus)

Valeurs

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-192-CBC
AES-256-CBC
SEED-CBC

Utiliser LZO Compression

Activer / Désactiver la compression LZO sur le lien VPN. Lempel-Ziv-Oberhumer (LZO) est un algorithme de compression sans perte de données.

Valeurs

Activer / **Désactiver**

OpenVPN Paramètres réseau serveur

OpenVPN supporte plusieurs sous-réseaux derrière serveur / client. Alors que la connexion vpn peut atteindre le sous-réseau derrière. Chaque sous-réseau doit être spécifié pour les données peuvent être acheminés correctement.

Valeurs

(Pas par défaut)

4.0 Configuration

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.

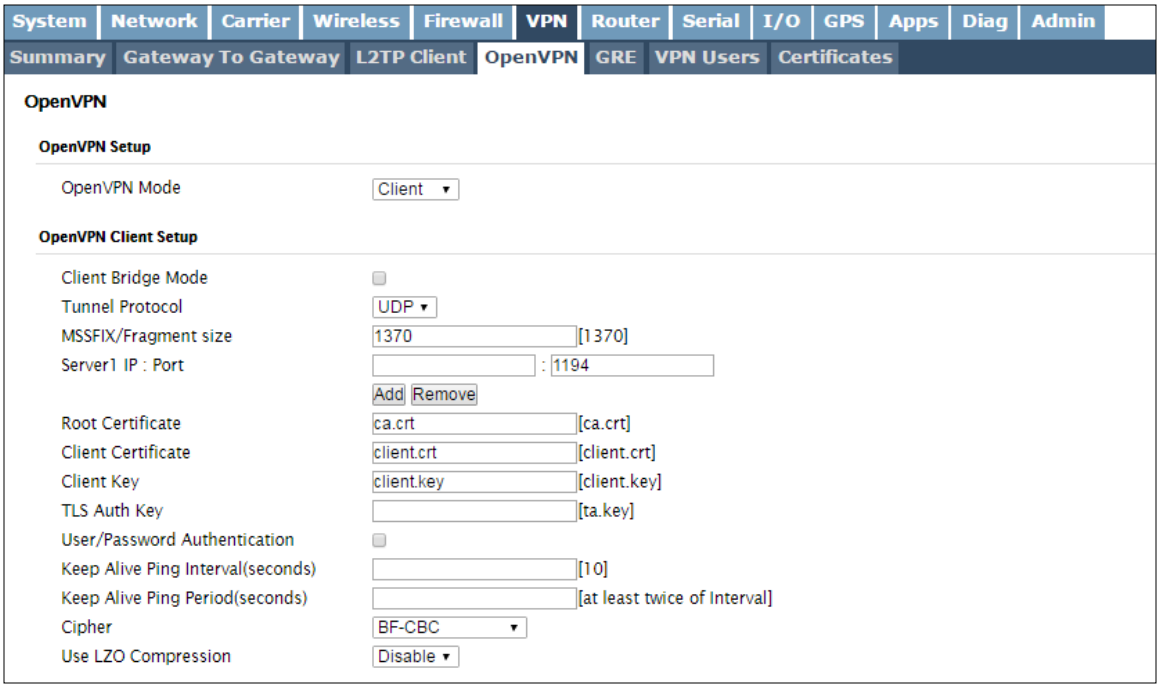


Image 4-6-4: VPN > OpenVPN Client

OpenVPN Mode

Activer / Désactiver le mode OpenVPN en sélectionnant le mode d'opérer dans, client ou serveur. Lorsque le serveur est activée, il sera l'écoute des demandes de connexion entrantes des clients OpenVPN.

Valeurs

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 mode pseudowire est mis à disposition.

Valeurs

(Décochée)

Protocole de tunnel

Sélectionnez le protocole de tunnel à utiliser. Les options sont TCP et UDP, la valeur par défaut est UDP.

Valeurs

TCP / **UDP**

4.0 Configuration

MSSFIX / taille de Fragment

Le maximum résultant UDP envoyer la taille des paquets après la OpenVPN a entièrement encapsulé données. Les paquets qui dépassent la valeur maximale seront fragmentés.

Valeurs

1370

Serveur IP / Port

L'adresse IP et le port TCP / UDP qui se trouve le serveur. Ceci est généralement l'adresse IP publique du routeur / modem sur lequel le serveur est en cours d'exécution.

Valeurs

(Pas par défaut)

Root Certificate

Le fichier racine de certificat (fichier CA) que tout le serveur et les clients doivent avoir en commun.

Valeurs

ca.crt

Certificat client

Le certificat client qui est le fichier de certificat qui réside uniquement sur le client.

Valeurs

client.crt

Client Key

La clé du client privé, qui ne devrait pas être divulguée.

Valeurs

client.key

TLS Auth Key

Le serveur et chaque client doit disposer d'une copie de cette clé pour faire l'authentification TLS.

Valeurs

(Pas par défaut)

Cipher

Sélectionnez un algorithme de chiffrement cryptographique. Doit être le même sur le serveur et le client.

Valeurs

DES-CBC	RC2-40-CBC
RC2-CBC	CAST5-CBC
DES-EDE-CBC	RC2-64-CBC
DES-EDE3-CBC	AES-128-CBC
DESX-CBC	AES-192-CBC
BF-CBC	AES-256-CBC
	SEED-CBC

Utiliser LZO Compression

Activer / Désactiver la compression LZO sur le lien VPN. Lempel-Ziv-Oberhumer (LZO) est un algorithme de compression sans perte de données.

Valeurs

Activer / **Désactiver**

4.0 Configuration

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.

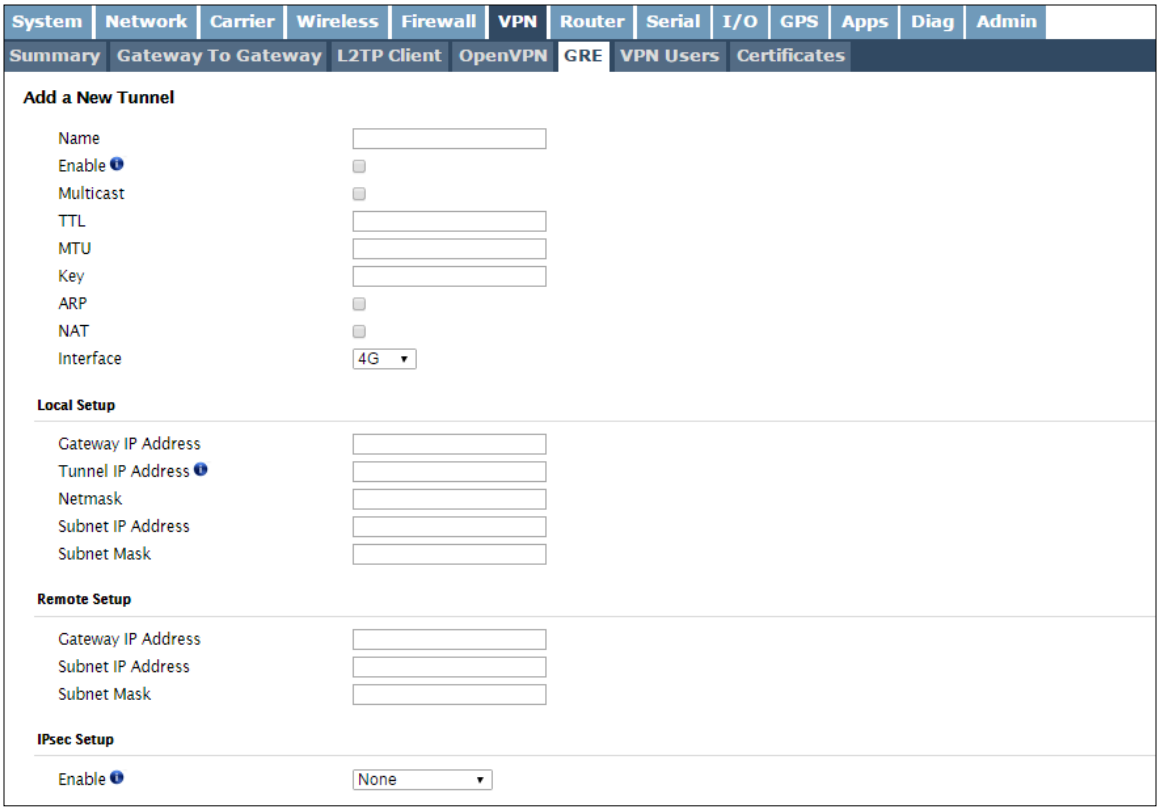


Image 4-6-5: VPN > Modifier / Ajouter GRE Tunnel

Nom

Chaque tunnel GRE doit avoir un nom unique. Jusqu'à 10 tunnels GRE sont pris en charge par la puce Plus.

Valeurs

gre

Activer

Activer / Désactiver le Tunnel GRE.

Valeurs

Désactiver / **Activer**

4.0 Configuration

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 tunnel GRE.

Valeurs

1 - **255**

Clé

Entrez une clé est nécessaire, la clé doit être le même pour chaque extrémité du tunnel GRE.

Valeurs

(Pas par défaut)

ARP

Activer / Désactiver ARP (Address Resolution Protocol) support sur le tunnel GRE.

Valeurs

Désactiver / **Activer**

Configuration locale

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

Adresse IP de la passerelle

Ceci est l'adresse IP WAN des BulletPlus, ce champ doit être rempli avec l'adresse IP actuelle WAN.

Valeurs

(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)

4.0 Configuration

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.

Adresse IP de la passerelle	
Entrez l'adresse IP WAN du Bullet Plus ou autre GRE dispositif pris en charge dans lequel un tunnel doit être créé avec à l'extrémité éloignée.	**Valeurs** *(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.

4.0 Configuration

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.

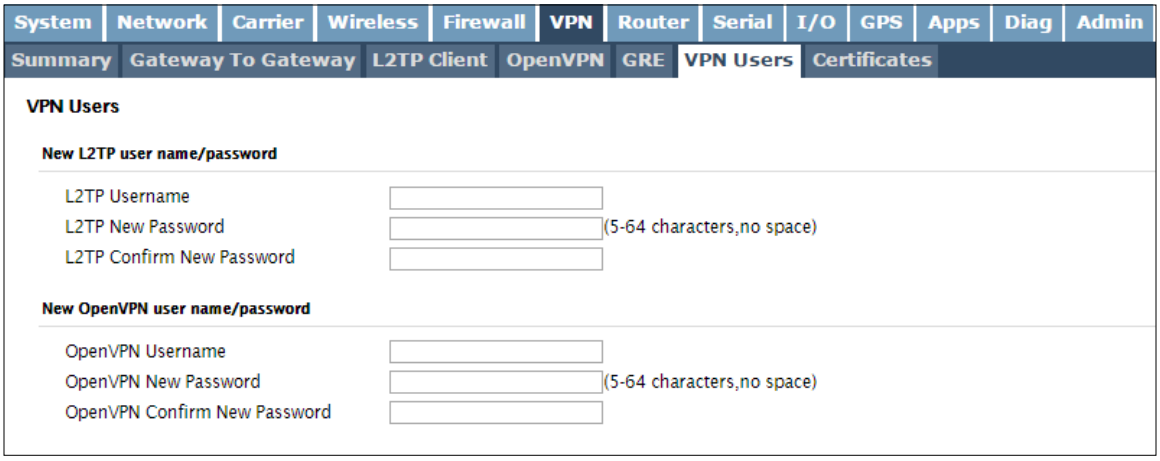


Image 4-6-6: VPN > Accès Client VPN

Nom d'utilisateur

Entrez un nom d'utilisateur pour l'utilisateur en cours d'installation.

Valeurs

(Pas par défaut)

Nouveau mot de passe

Entrez un mot de passe pour l'utilisation.

Valeurs

(Pas par défaut)

Confirmer le nouveau mot de passe

Entrez à nouveau le mot de passe, les BulletPlus veillera à ce que le match de mot de passe.

Valeurs

(Pas par défaut)

4.0 Configuration

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.

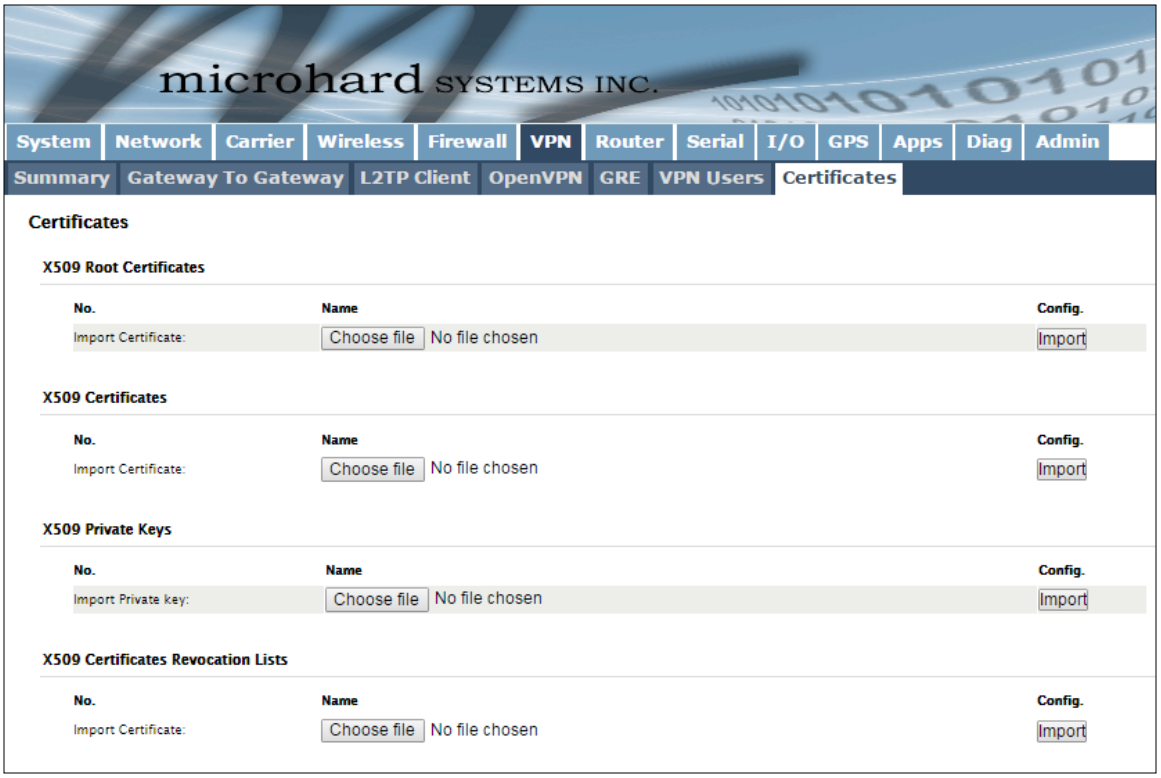


Image 4-6-7: VPN > Gestion des certificats

4.0 Configuration

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.

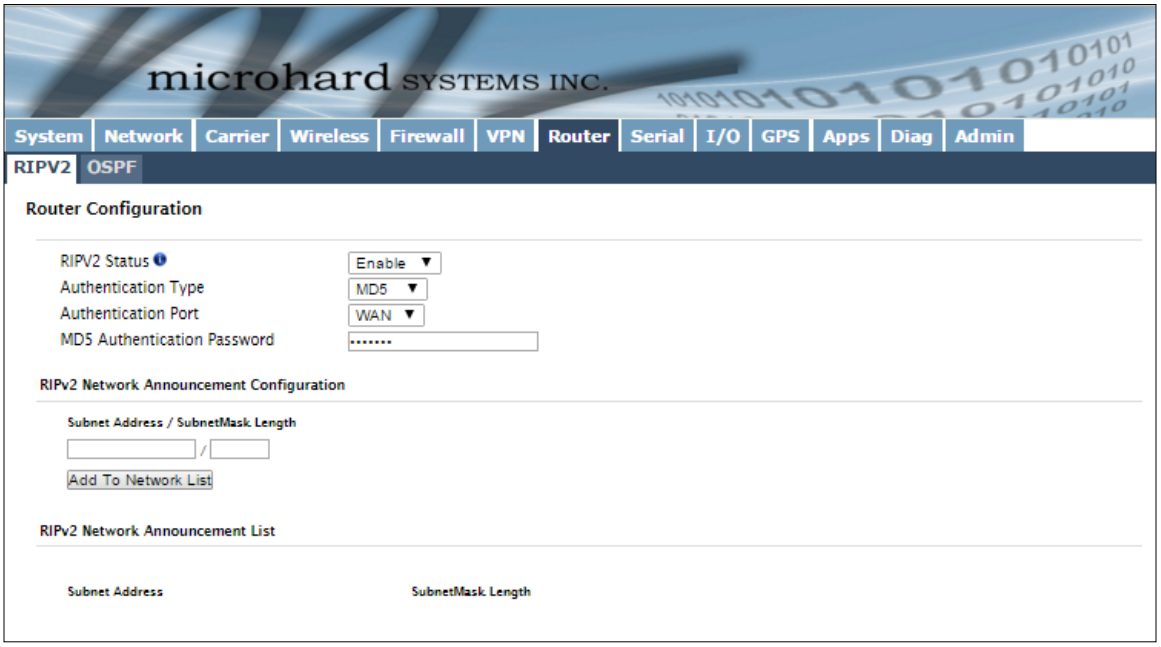


Image 4-7-1: Routeur > RIPv2

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 par défaut)

4.0 Configuration

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.

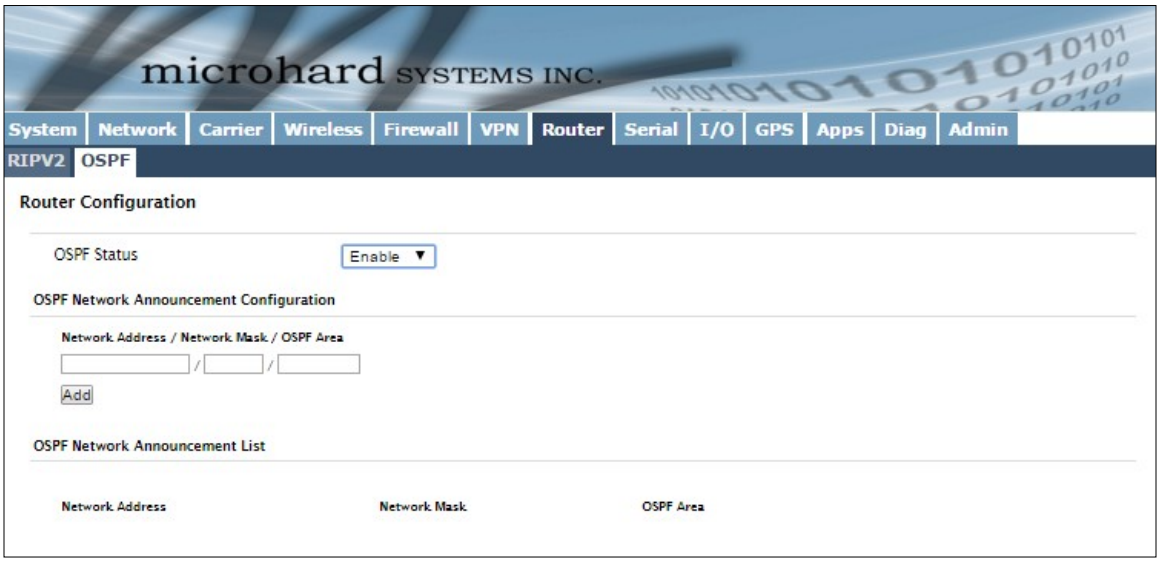


Image 4-7-2: Router > OSPF

OSPF Status

Activer ou désactiver le routage OSPF sur les BulletPlus. Si activé le BulletPlus échangera des informations de routage sur les interfaces spécifiées () réseaux connectés.

Valeurs

Activer / **Désactiver**

Configuration Annonce OSPF Réseau

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.

Valeurs

(Pas par défaut)

4.0 Configuration

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.

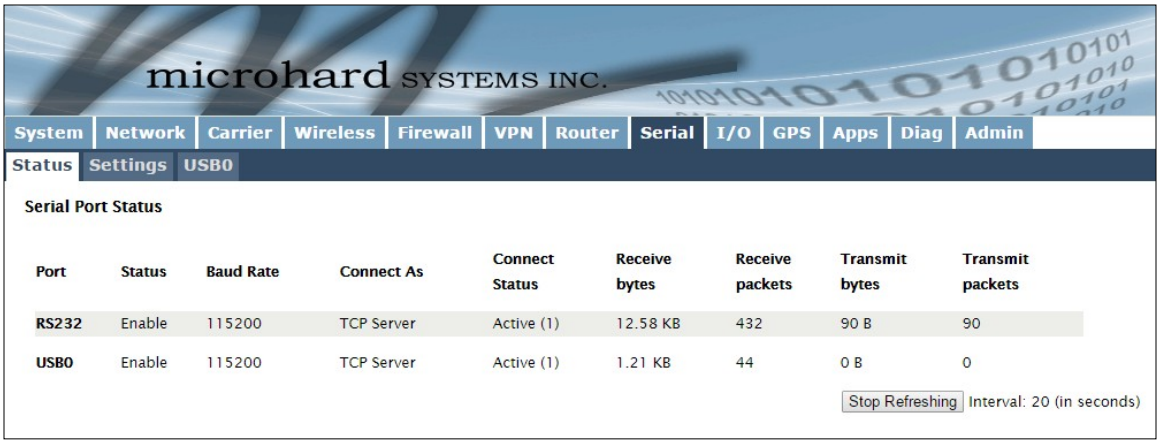


Image 4-8-1: Serial > Statut

4.0 Configuration

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.

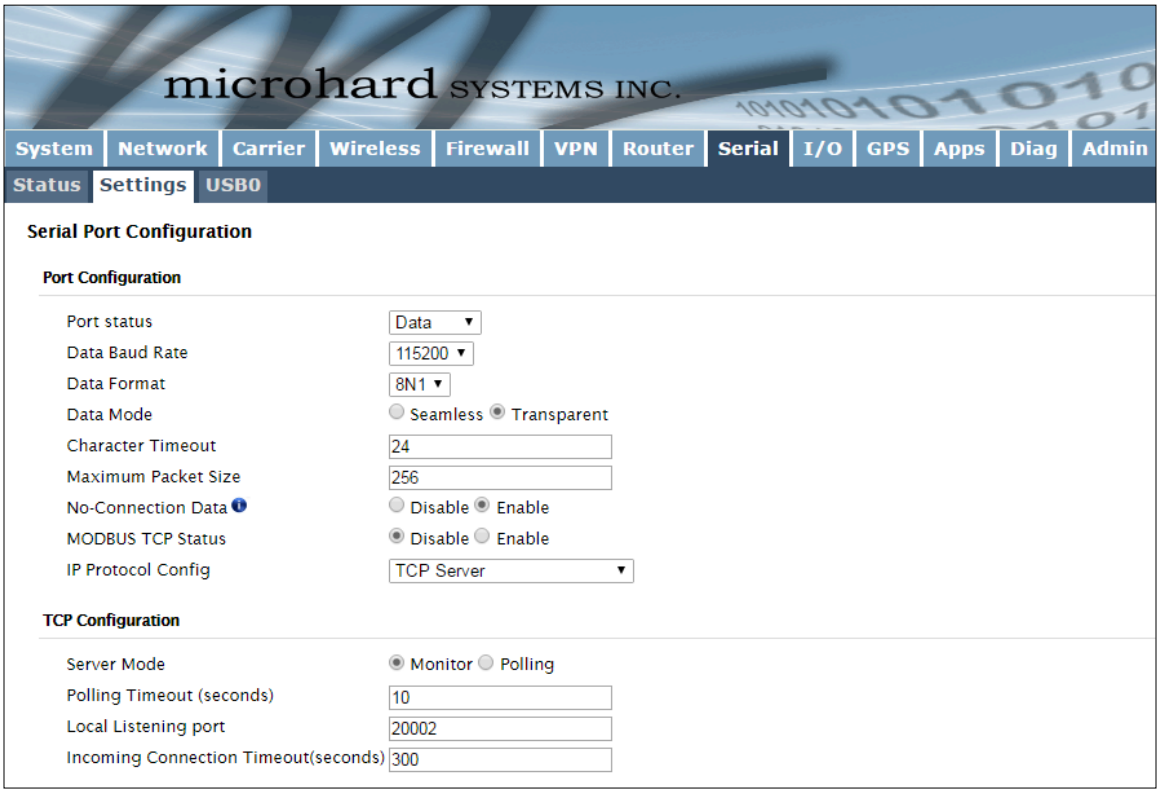


Image 4-8-2: Serial > Configuration des paramètres

4.0 Configuration

Port Status

Sélectionnez l'état de fonctionnement du port série. Le port est désactivé par défaut.

Valeurs

Désactivé / Activer

Données 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	**9600**
460800	7200
230400	4800
115200	3600
57600	2400
38400	1200
28800	600
19200	300
14400	

Remarque: La plupart des ordinateurs ne prennent pas facilement les communications série supérieures à 115200 bps.

Format de données

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.

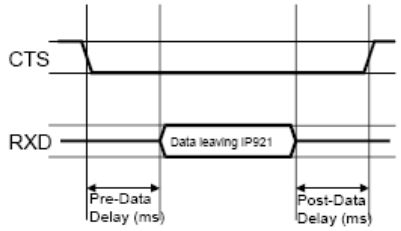
Valeurs

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.



Dessin 4A: Données CTS Sortie Encadrement

Valeurs

Aucun
Matériel
CTS Framing

Pure-données de retard

Voir le dessin ci-dessus 4A.

Valeurs

100

Post-données Délai

Voir le dessin ci-dessus 4A.

Valeurs

100

4.0 Configuration

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

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.

Valeurs

24

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 pour recevoir des données du port série. Lorsque le serveur détecte 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.

Valeurs

1024

Pas de connexion-Data

Lorsqu'elle est activée les données continueront à le tampon reçu sur le port série de données lorsque la radio perd la synchronisation. Lorsqu'il est désactivé, les BulletPlus sera ignorer toutes les données reçues sur le port série de données lorsque la synchronisation radio est perdu.

Valeurs

Désactiver / Activer

MODBUS TCP Status

Cette option activer ou désactiver les fonctions MODBUS de décodage et d'encodage.

Valeurs

Désactiver / Activer

MODBUS TCP Protection Key

Clé de chiffrement MODBUS utilisée pour la fonction d'état MODBUS Protection TCP.

Valeurs

1234

4.0 Configuration

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.

Valeurs

TCP client
Serveur TCP
TCP Client / Serveur
UDP Point-to-Point
client SMTP
PPP
Mode transparent GPS

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.

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.

- **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 deux données série côté client et côté serveur de données série, le cas échéant, seront rejetées.

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.

- **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)

4.0 Configuration

IP Protocol Config (a continué…)

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.

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.

- **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.

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.

- **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: 0.0.0.0

- **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

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 sous-réseau.

- **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

4.0 Configuration

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.

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

- **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

4.0 Configuration

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:

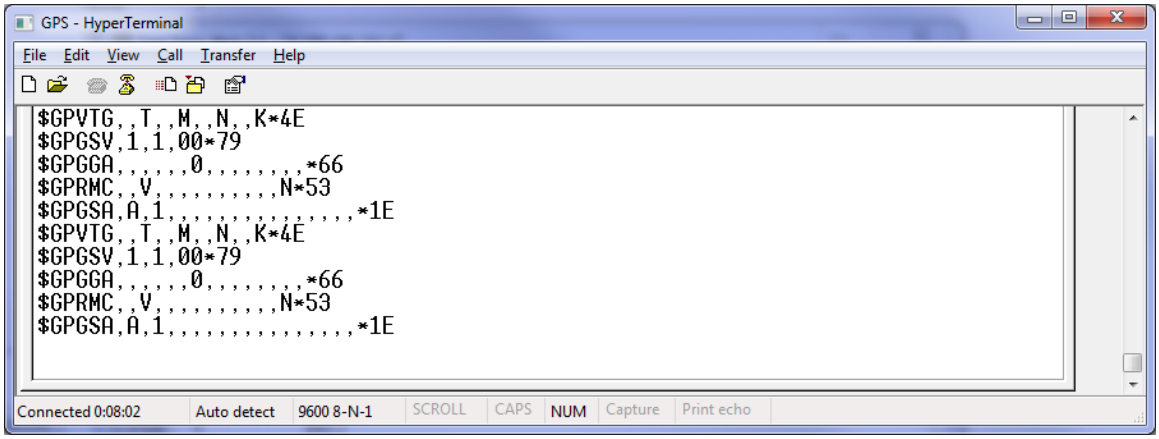


Image 4-8-3: Serial > Mode transparent GPS

4.0 Configuration

4.9 I/O

4.9.1 I/O > Paramètres

Le BulletPlus a 8 I 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.

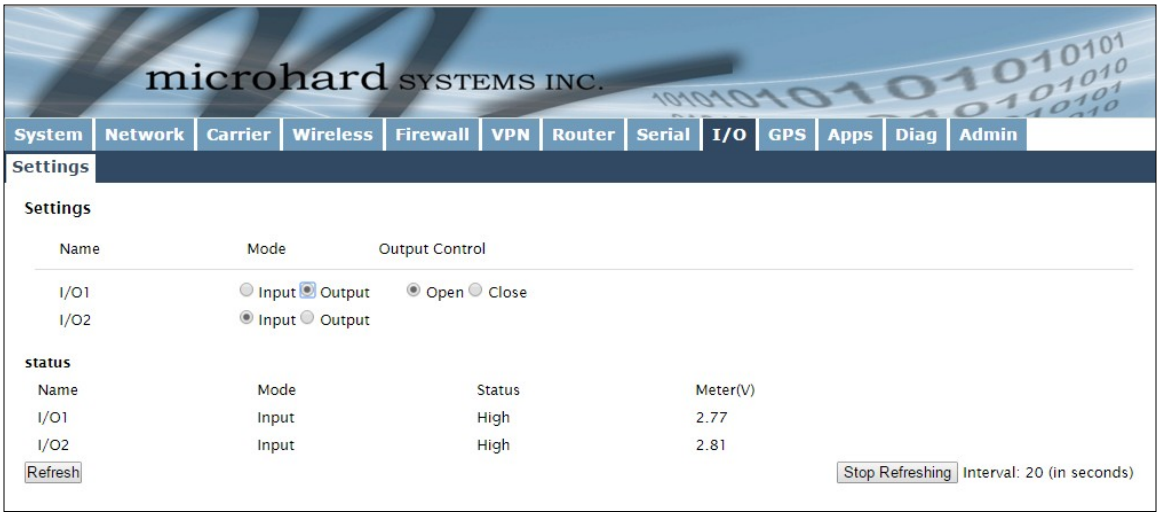


Image 4-9-1: I/O Paramètres

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.

4.0 Configuration

Nom	La description	Paramètre	Min.	Typ.	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 typique est un contact de commutation à sec au sol. Pin comprend une résistance de 56KΩ interne tirer jusqu'à 3,3 VDC.					
I/O 1 - 2 (Sortie)	Ouvrir lecteur de drain à la masse	Idc	—-	100	110	mA
	Tension maximale en circuit ouvert appliquée	Voc	—-	3.3	30	V
	Une application typique est de conduire une bobine de relais à la masse.					

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

4.0 Configuration

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.

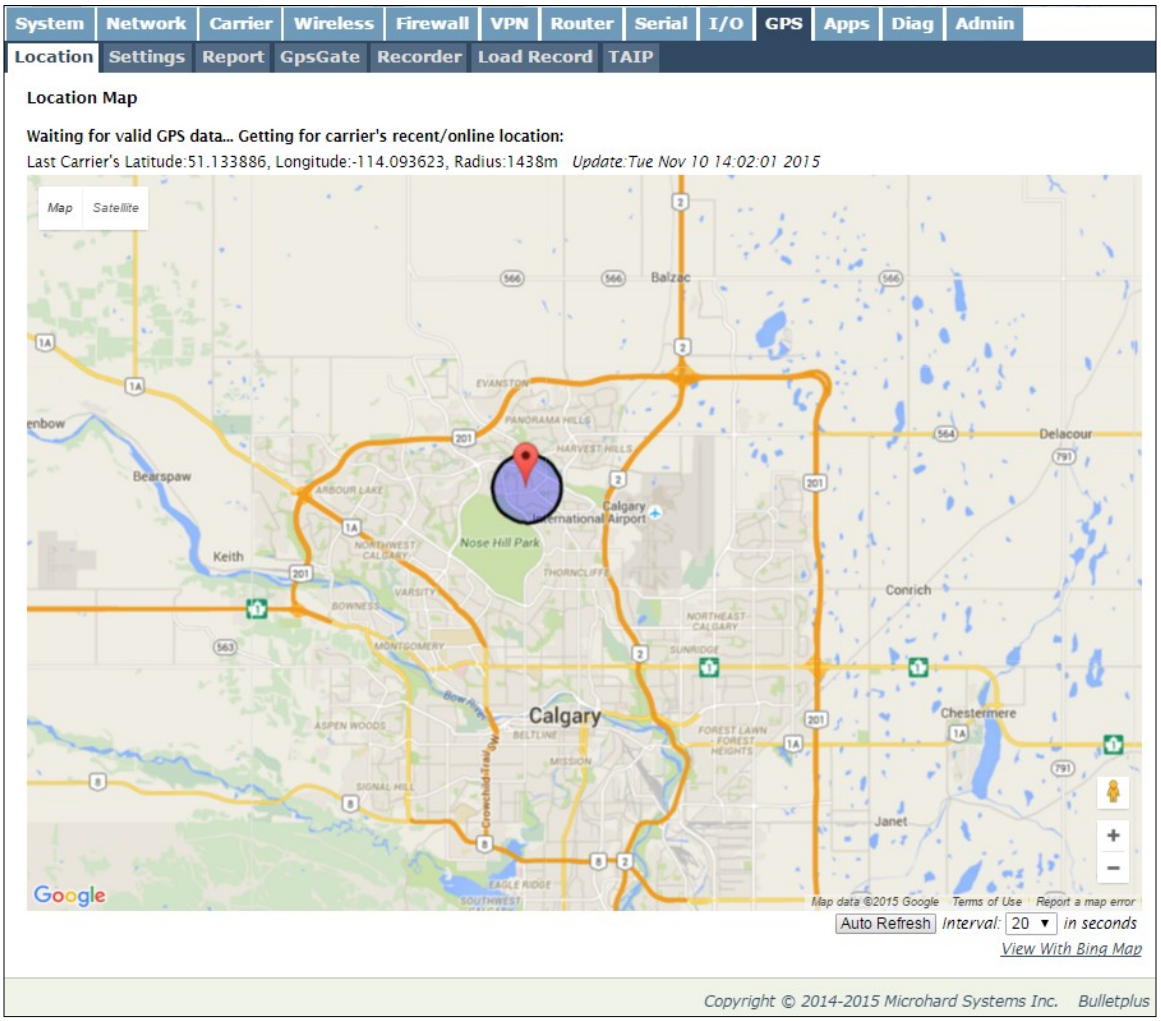


Image 4-10-1: GPS > Une carte

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.

4.0 Configuration

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.

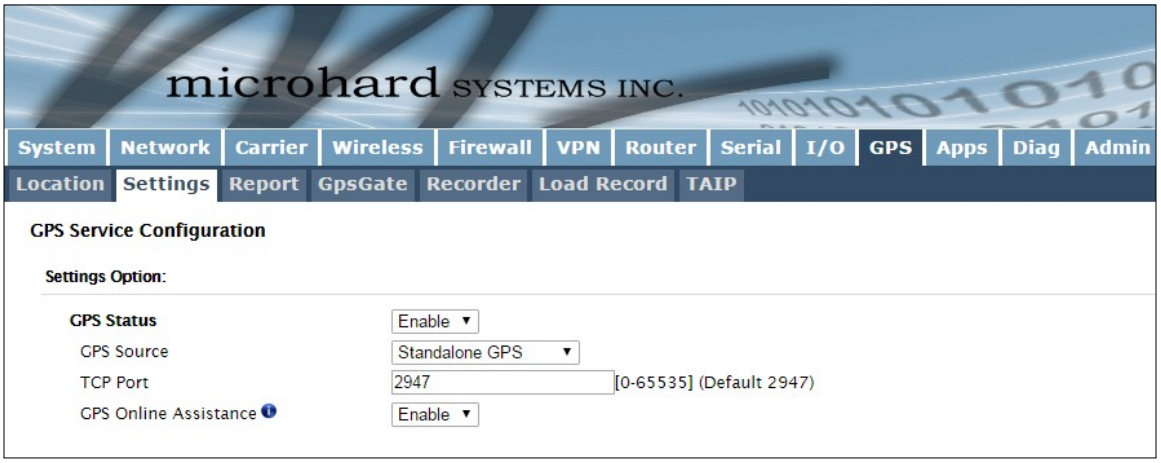


Image 4-10-2: GPS > Paramètres

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 l'antenne GPS Port.

Valeurs

GPS autonome
GPS Module cellulaire

TCP Port

Spécifiez le port TCP sur le BulletPlus où le service GPS est en cours d'exécution et les systèmes distants peuvent se connecter et interroger des données GPS.

Valeurs

2947

Assistance en ligne GPS

Lorsque les permis BulletPlus utilisera l'Internet pour télécharger un fichier au démarrage avec des informations sur son emplacement pour aider à rapidement connecter des satellites GPS. Ce service consomme une petite quantité de données.

Valeurs

Activer

4.0 Configuration

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.

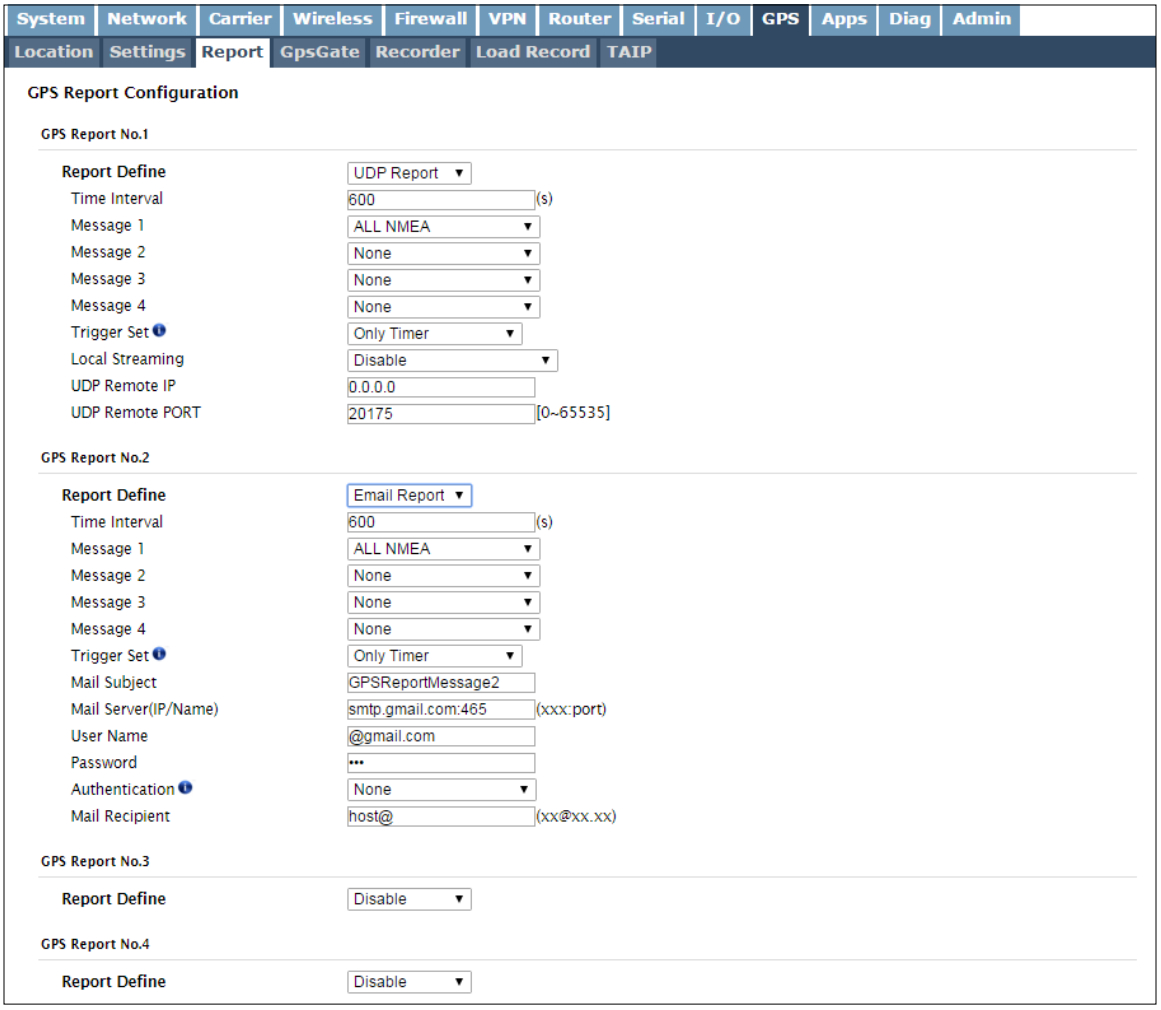


Image 4-10-3: GPS > Rapport GPS

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 GPS est rapporté en secondes.

Valeurs

600

4.0 Configuration

Message 1-4

Le champ du message permet de personnaliser jusqu'à 4 messages GPS différents pour être envoyées à l'hôte spécifié.

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

Valeurs

Aucun
ALL NMEA
GGA
GSA
GSV
RMC
VTG
Latitude Longitude
GPSGate protocole UDP

Déclencheur est choisi

La condition de déclenchement définit les conditions qui doivent être remplies avant qu'une mise à jour du GPS est signalée. Si OR est choisi, la minuterie répéteur ou les conditions de déclenchement à distance doivent 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.

Valeurs

Seulement Minuteur
Minuteur ET Distance
Temps ou la distance

Distance Set

Le paramètre de distance permet aux données GPS à seulement être envoyés lorsqu'une distance spécifiée a été parcourue depuis le dernier rapport.

Valeurs

1000

UDP IP à distance / Port

Ceci est l'adresse IP et le port de l'hôte distant dans lequel les paquets UDP doivent être envoyés.

Valeurs

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 ici.

Valeurs

1000

Serveur de courrier

Si un rapport d'email doit être envoyé, le serveur de courrier sortant doit être défini, et le numéro de port.

Valeurs

smtp.gmail.com:465

Identifiant Mot de passe

Certains serveurs de messagerie sortants requis nom d'utilisateur et mot de passe pour empêcher un compte d'être utilisés pour le spam. Entrez les informations de connexion ici.

Valeurs

Identifiant Mot de passe

Destinataire du courrier

Certains serveurs de messagerie sortants nécessitent un nom d'utilisateur et mot de passe pour empêcher un compte utilisé pour le spam. Entrez les informations de connexion ici.

Valeurs

host@email.com

4.0 Configuration

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)

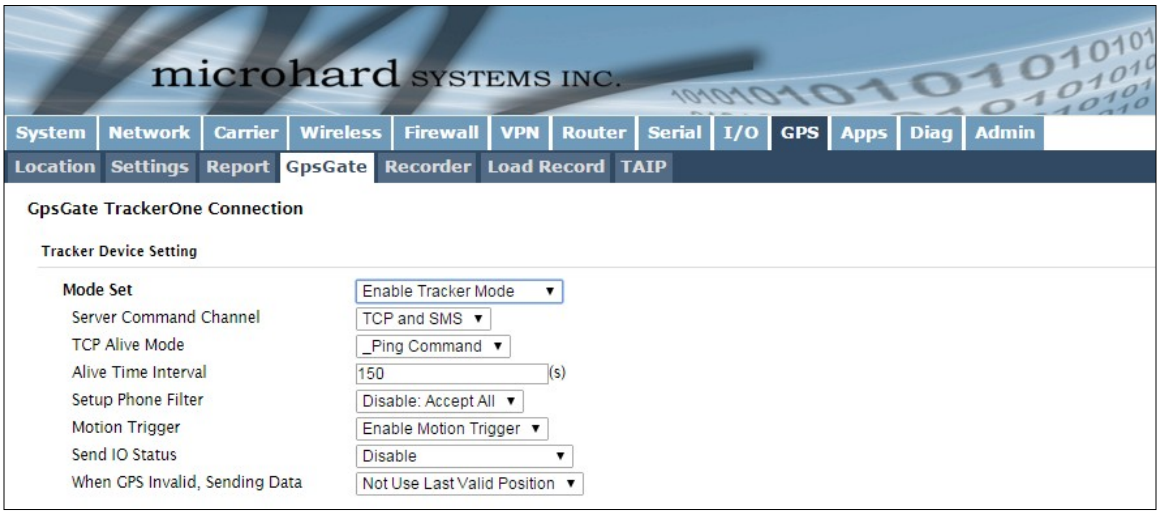


Image 4-10-4: GPS > GpsGate Tracker Mode

Mode Tracker GpsGate

Mode Set

Activer GpsGate mode Tracker ou modes TCP. En mode tracker Le logiciel BulletPlus et GpsGate communiquera via TCP / IP, si une connexion ne sont pas disponibles, il va tenter d'utiliser la messagerie SMS.

Valeurs

Désactiver
Activer le mode Piste
Activer TCP Envoyer mode

Serveur Commande Canal

Par défaut BulletPlus et GpsGate utilisera TCP et SMS pour assurer la communication entre eux. Il est également possible de spécifier le protocole TCP ou le SMS uniquement la communication. La configuration initiale en mode Tracker doit être via SMS.

Valeurs

TCP et SMS
TCP seulement
SMS seulement

Mode TCP Vivant / Vivant 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 secondes.

Valeurs

150

4.0 Configuration

Configuration Téléphone Filtre

Un filtre de numéro de téléphone peut être utilisé pour empêcher les commandes SMS non destinées au BulletPlus d'être 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 et / ou sorties d'E / S numérique I du GpsGate Server.

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

GpsGate - TCP Mode

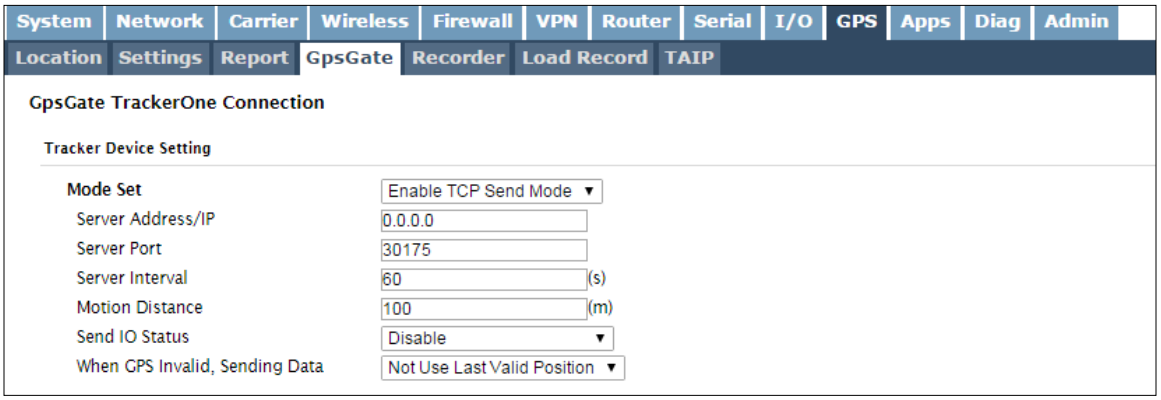


Image 4-10-5: GPS > GpsGate TCP Mode

4.0 Configuration

Mode Set

Activer GpsGate mode Tracker ou modes TCP. En mode TCP l'BulletPlus établit une connexion avec le serveur GpsGate directement sans le 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.

Valeurs

Désactiver
Activer le mode Piste
Activer TCP Envoyer mode

Adresse 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 GpsGate Server.

Valeurs

60

Mouvement Distance

Régler le seuil de mouvement dans lequel le BulletPlus sera déclenchée pour envoyer des données de localisation.

Valeurs

100

Envoyer IO Status

Lorsqu'elle est activée, les BulletPlus va envoyer l'état actuel des entrées et / ou sorties d'E / S numérique I du GpsGate Server.

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

4.0 Configuration

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.

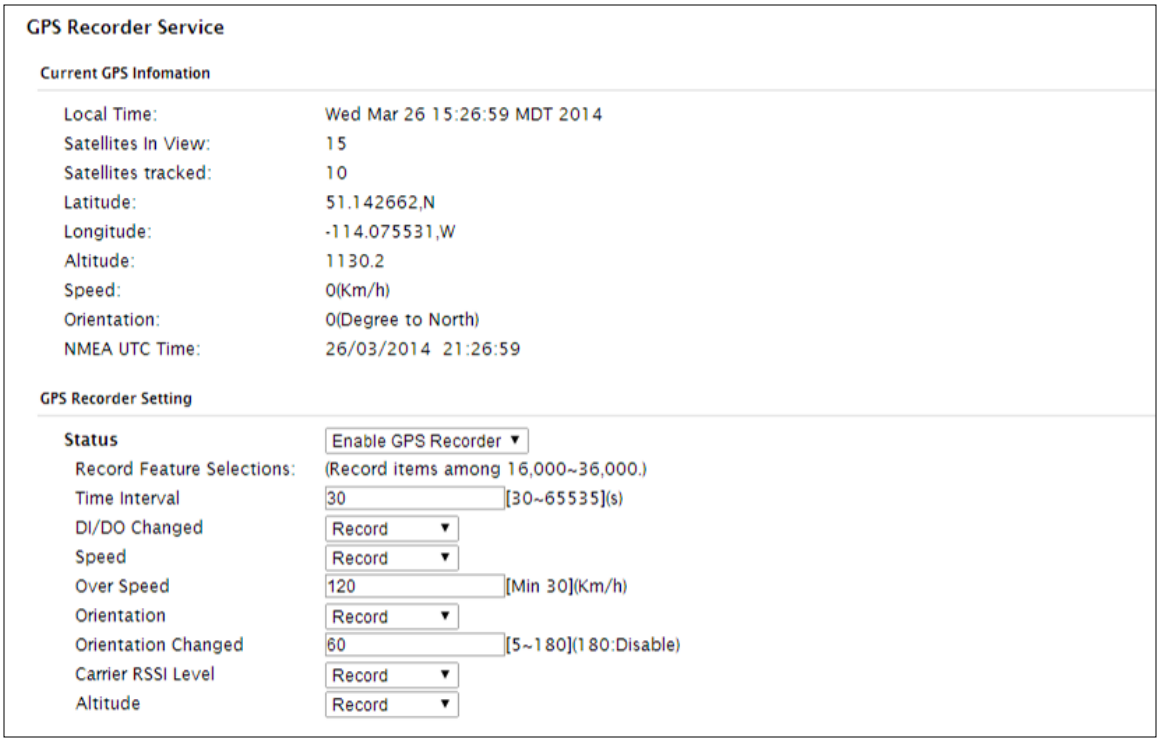


Image 4-10-6: GPS > GPS service Enregistreur

Statut

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.

Valeurs

Désactiver
Activer Enregistreur GPS

Intervalle de temps

Définir l'intervalle auquel le BulletPlus enregistrera les données GPS. S'il n'y a pas de données valides disponibles à l'heure indiquée (à savoir pas de satellites connectés), l'unité attendra jusqu'à ce que la prochaine fois que l'information valide est reçu.

Valeurs

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.

Valeurs

Record / **Will not Record**

4.0 Configuration

La vitesse

Sélectionnez Enregistrer pour inclure la vitesse actuelle dans les données déclarées.

Valeurs

Record / **aucun enregistrement**

Plus de vitesse

Déclencher une entrée d'enregistrement GPS lorsque la vitesse a dépassé le seuil configuré. Un minimum de 30 Km / h est nécessaire.

Valeurs

120

Orientation

Sélectionner le registre pour enregistrer l'orientation courante lorsqu'une entrée GPS est enregistrée. (Degré Nord).

Valeurs

Record / **aucun enregistrement**

Orientation Change

Enregistrer un GPS, quel que soit l'intervalle de temps, si l'orientation des changements unitaires. (5 ~ 180: 180 = Désactiver)

Valeurs

60

Transporteur Niveau RSSI

Sélectionnez Enregistrer pour enregistrer le niveau 3G / cellulaire RSSI courant lorsqu'une entrée GPS est enregistrée. (-dB).

Valeurs

Record / **aucun enregistrement**

Altitude

Sélectionnez Enregistrer pour enregistrer l'altitude actuelle lorsqu'une entrée GPS est enregistrée (mètres).

Valeurs

Record / **aucun enregistrement**

4.0 Configuration

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 ci-dessous montrent les données brutes qui peuvent être consultés et Trace Carte / sortie Trace rapide.

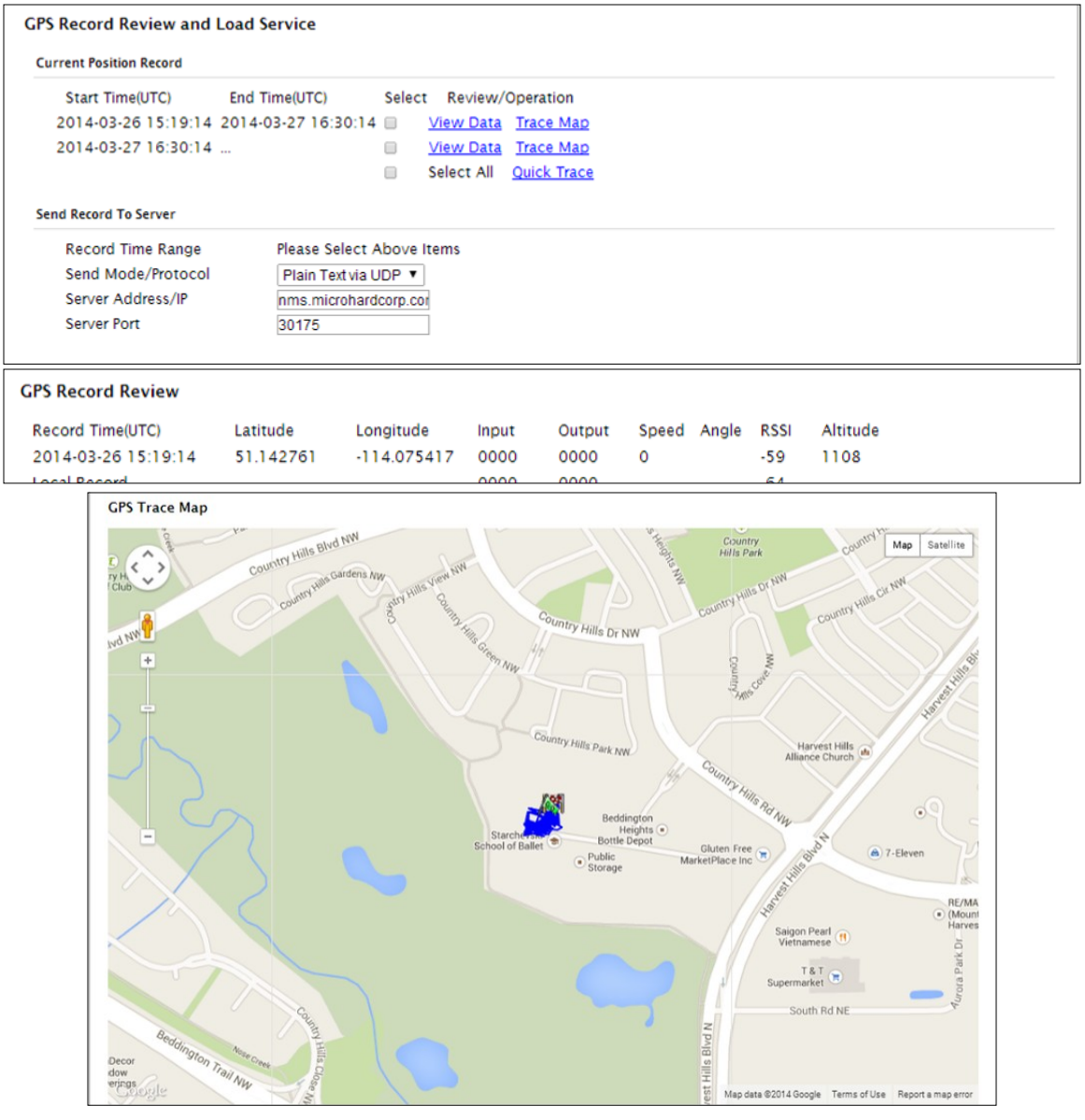


Image 4-10-7: GPS > GPS Record charge

4.0 Configuration

Record Time Range	
Cochez les cases à côté des dossiers énumérés ci-dessus qui doivent être envoyées au serveur.	**Valeurs** *(Pas par défaut)*

Envoyer Mode / Protocole	
Spécifiez le type format de données / protocole pour les données à envoyer.	**Valeurs** NMEA via UDP NMEA via TCP GpsGate via UDP GpsGate via TCP **Texte brut via UDP** Texte brut via TCP

Adresse du serveur / IP	
Saisissez l'adresse ou l'adresse IP du serveur distant sur lequel les données doivent être envoyées.	**Valeurs** 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

4.0 Configuration

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.

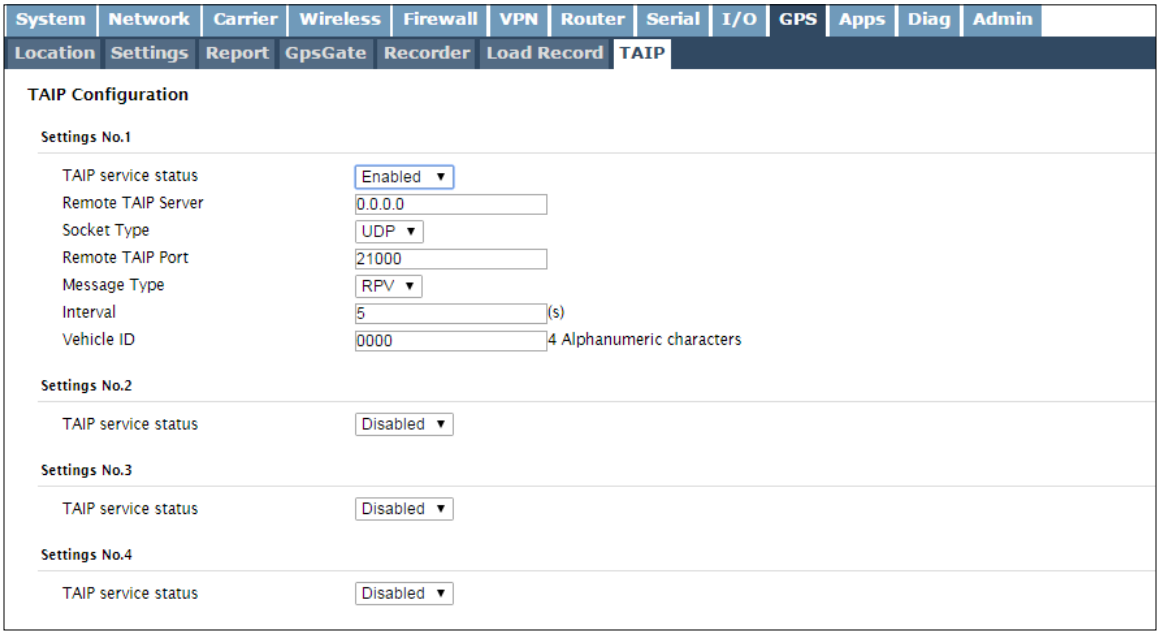


Image 4-10-8: GPS > TAIP

TAIP état du service

Activer ou désactiver le service TAIP sur le modem. L'unité peut rapporter TAIP à un maximum de 4 hôtes différents.

Valeurs

Activer / **Désactiver**

Télécommande 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 distance. Sélectionner TCP ou UDP, il va définir comment la connexion (TCP), ou les données sont envoyées (UDP) au serveur.

Valeurs

UDP / TCP

Port IP à distance

Entrez le numéro de port TCP ou UDP utilisé sur le serveur TAIP à distance.

Valeurs

UDP / TCP

4.0 Configuration

Type de message	
Sélectionnez entre RPV et types de messages RLN. RPV - Position / Velocity RLN - Message long Navigation	**Valeurs** **RPV** / RLN

Intervalle	
Réglez la fréquence à laquelle des messages de type sont signalés au serveur distant. L'unité utilisée est secondes, et la valeur par défaut est de 60 secondes.	**Valeurs** 60

ID du véhicule	
Définissez l'ID du véhicule à l'aide de 4 caractères alphanumériques.	**Valeurs** **0000**

4.0 Configuration

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.

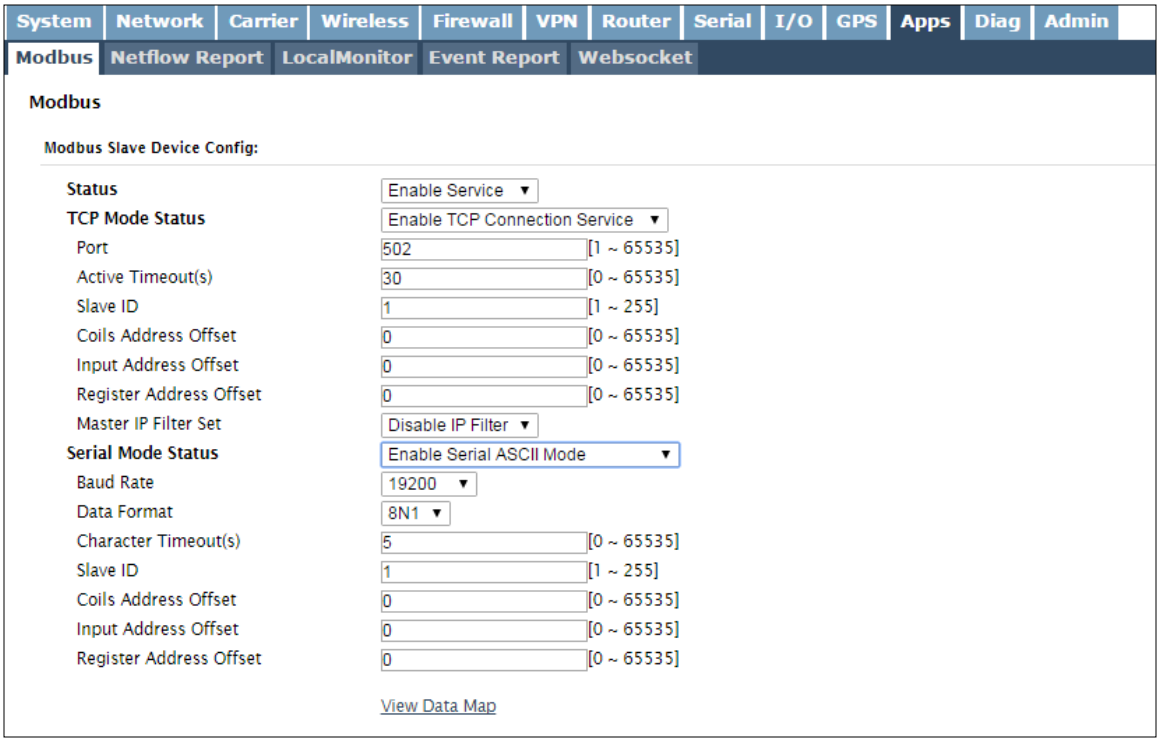


Image 4-11-1: Apps > Modbus

Statut

Désactiver ou activer le service Modbus sur le BulletPlus.

Valeurs

service Désactiver
Activer le service

TCP Mode Statut

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

Valeurs

Désactiver
Activer

4.0 Configuration

Port	
Spécifiez le port dans lequel le service Modbus TCP est d'écouter et répondre aux sondages.	**Valeurs** **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 l'esclave. Entrez cette valeur ici comme requis par le système hôte Modbus.	**Valeurs** **1**

Coils 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**

Register Address Offset	
Entrez le décalage tel que requis par le maître Adresse d'entrée.	**Valeurs** **0**

Master IP Filter Set	
Il est possible d'accepter uniquement les connexions à partir Modbus spécifique Maître IP, pour utiliser cette fonctionnalité activer le filtre IP maître et de spécifier les adresses IP dans les champs prévus.	**Valeurs** **Désactiver** / Activer

4.0 Configuration

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.

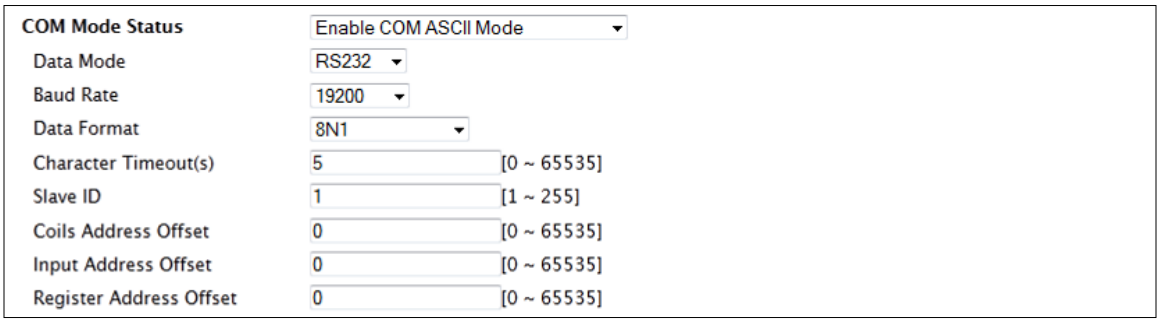


Image 4-11-2: Apps > Modbus Configuration série

COM Mode Statut

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

Bauds

La vitesse de transmission de série est la vitesse à laquelle le modem est de communiquer avec le périphérique série local connecté.

Valeurs (bps)

921600	57600	14400	3600
460800	38400	**9600**	2400
230400	28800	7200	1200
115200	19200	4800	600

Format de données

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.

Valeurs

8N1 / 8E1 / 8O1

4.0 Configuration

4.10.1.3 Modbus > Modbus Data Map

Modbus Data Map

Supported Function Codes:

1---Read Coils
2---Read Inputs
3---Read Registers
5---Write Single Coil
6---Write Single Register
Data Address = Offset + Basic Address

Coil Bits (Output(if config) and Internal Status):

Bit Address	Hex Format	Definition
0	0x0000	OUTPUT 1
1	0x0001	OUTPUT 2
9	0x0009	Serial Status
12	0x000c	LAN/eth0 Status(Read)
13	0x000d	WAN/eth1 Status(Read)
16	0x0010	Carrier Status
18	0x0012	Wifi Status
22	0x0016	GPS Status
23	0x0017	Location Over Network
24	0x0018	Event UDP Report 1
25	0x0019	Event UDP Report 2
26	0x001a	Event UDP Report 3
27	0x001b	NMS Report
28	0x001c	Web Client Service
32	0x0020	Carrier Connection(Read)
40	0x0028	SYSTEM Reboot

Input Bits:(if config)

Bit Address	Hex Format	Definition
0	0x0000	INPUT 1
1	0x0001	INPUT 2

Registers:

16 Bits Address	Hex Format	Definition
0	0x0000	Modem Model Type...
1	0x0001	Build Version
2	0x0002	Modem ID Highest 2 Bytes
3	0x0003	Modem ID Higher 2 Bytes
4	0x0004	Modem ID Lower 2 Bytes
5	0x0005	Modem ID Lowest 2 Bytes
6	0x0006	RSSI(dbm)
7	0x0007	VDC(x100)(V)
8	0x0008	Core Temperature(C)
9	0x0009	Carrier Received Bytes(MB)
10	0x000a	Carrier Transmitted Bytes(MB)
11	0x000b	GPS Altitude(m)
12	0x000c	GPS Latitude High 2 Bytes
13	0x000d	Latitude Low 2 Bytes(x1000000)
14	0x000e	GPS Longitude High 2 Bytes
15	0x000f	Longitude Low 2 Bytes(x1000000)
18	0x0012	Serial Baud Rate(/100)(bps)
19	0x0013	Serial Data Format...

Caculation: Real Latitude = (signed integer)[High 2 Bytes + Low 2 Bytes] / 1

Modem Model Types:

Type ID	Definition
0	Unknow
6	IPn3G
7	VIP4G
8	IPn4G
9	IPn3Gii
10	IPn4Gii
11	PWii/BulletPlus

Com Data Format Definition:

Type ID	Definition
0	Unknow
1	8N1
2	8N2
3	8E1
4	8O1
5	7N1
6	7N2
7	7E1
8	7O1
9	7E2
10	7O2

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

4.0 Configuration

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.

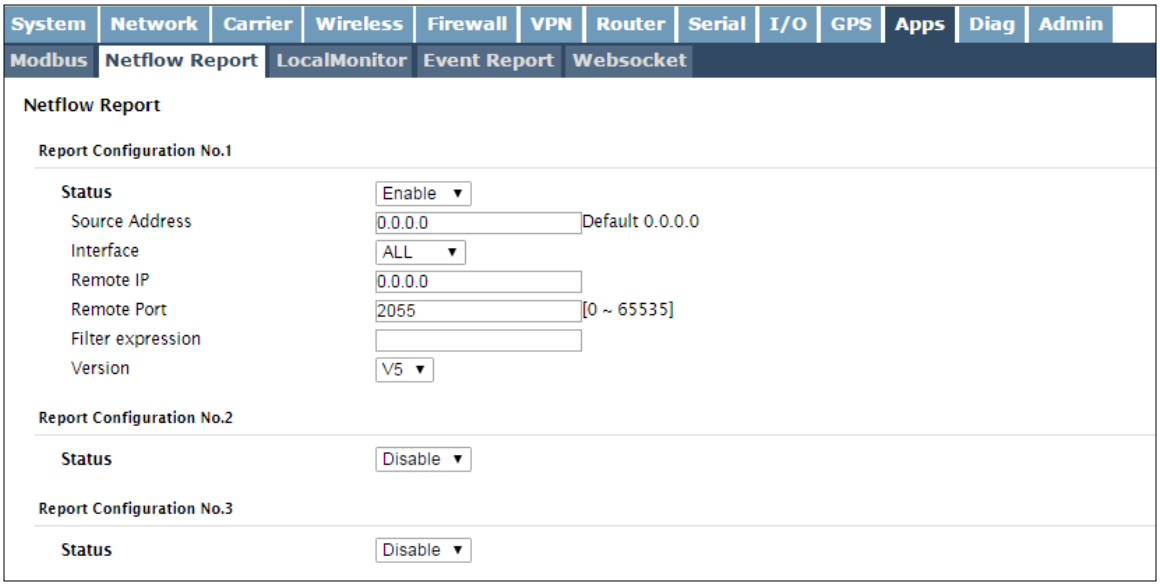


Image 4-11-4: Apps > Rapport Netflow

Status

Activer / Désactiver Netflow Reporting.

Valeurs

Désactiver / Activer

Source Address

La Source Adresse est l'adresse IP, dont les données doivent être collectées et analysées. La valeur par défaut de 0.0.0.0 va recueillir et communiquer des informations sur toutes les adresses connectés à l'interface sélectionnée ci-dessous.

Valeurs

0.0.0.0

Interface

Sélectionnez entre LAN, WAN et transporteurs interfaces, ou des données de capture de toutes les interfaces.

Valeurs

LAN / WAN / Carrier / ALL

4.0 Configuration

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 expression est donnée, tous les paquets seront capturés. Sinon, seuls les paquets dont l'expression est `vrai 'sera capturé. Exemple: tcp&&port 80 *Le manuel "tcpdump", disponible sur Internet fournit une syntaxe d'expression détaillée.*	**Valeurs** *(Pas par défaut)*

4.0 Configuration

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.

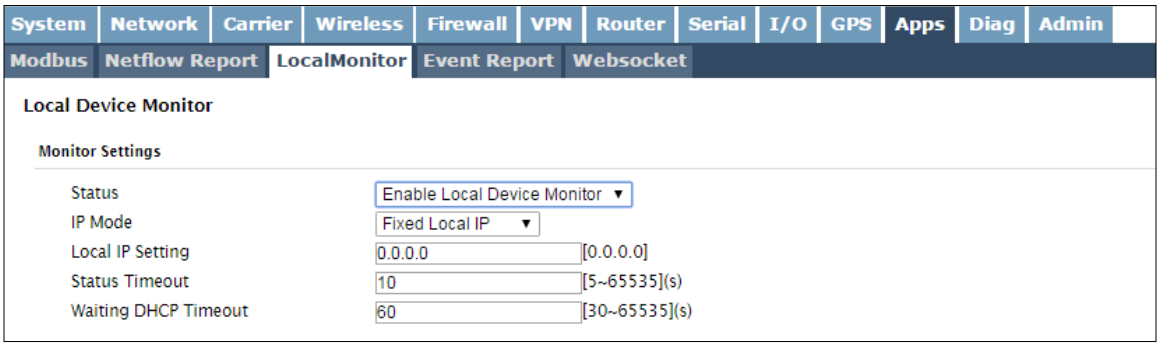


Image 4-11-5: Apps > Moniteur local

Statut

Activer ou désactiver le service de surveillance de périphérique local.

Valeurs

Désactiver / Activer

IP Mode

Sélectionnez le mode IP. En sélectionnant une adresse IP fixe, le service va superviser la connexion à cette adresse IP spécifique. Si la détection automatique est sélectionné, le BulletPlus va détecter et surveiller DHCP adresse IP attribuée.

Valeurs

Fixed IP locale
Détection automatique IP

Locale IP Configuration

Ce champ est affiché uniquement si IP fixe local est sélectionné pour le mode IP. Entrez le adresse IP statique à surveiller dans ce domaine.

Valeurs

0.0.0.0

Statut Timeout

Le délai d'attente d'état est le temps maximum que le BulletPlus attendra pour détecter le dispositif surveillé. A ce moment le BulletPlus va redémarrer le service DHCP. (5-65535 secondes)

Valeurs

10

Attente DHCP Timeout

Ce champ définit la quantité de temps le BulletPlus attendra pour détecter le dispositif surveillé avant qu'il redémarre le modem. (30-65535 secondes)

Valeurs

60

4.0 Configuration

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.

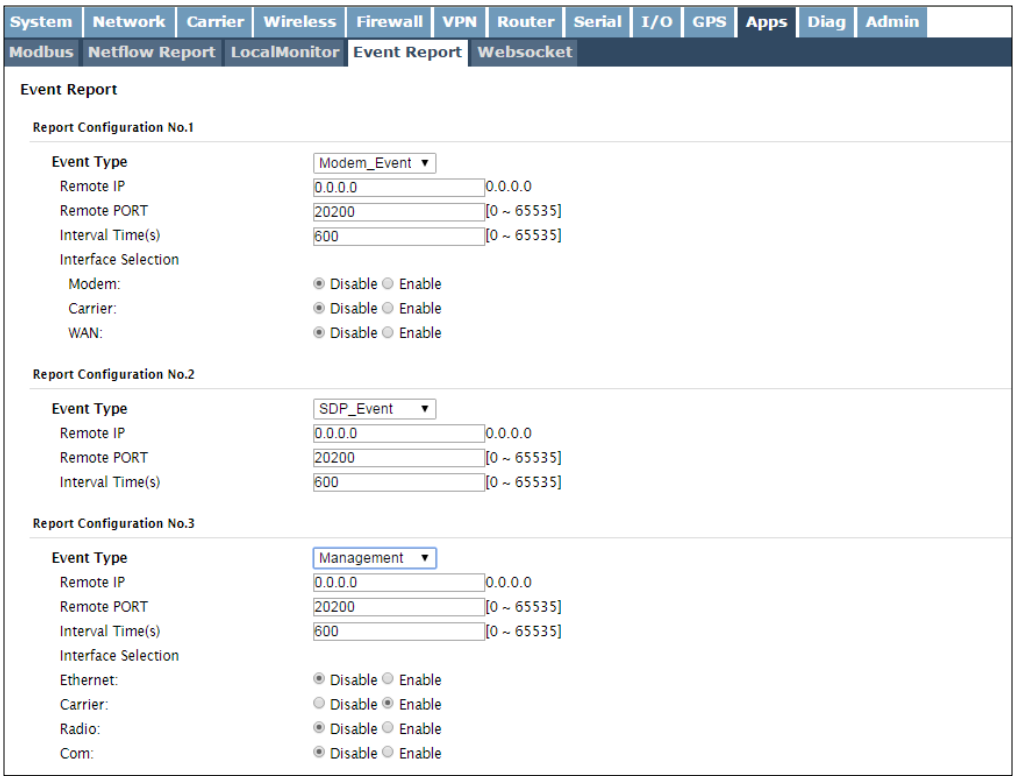


Image 4-11-6: Apps > Rapport d'événement

Type d'événement

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.

Valeurs

Modem événement
SDP Event
La gestion

IP à distance

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

Valeurs

0.0.0.0

4.0 Configuration

Port à distance	
Indiquez le numéro de port UDP de l'adresse IP distante. * Numéros de port par défaut pour Microhard NMS (20100 pour les événements de modem, 20200 pour la gestion)	**Valeurs** **20200**

Intervalle Times	
Ceci est l'intervalle de temps en secondes, que les BulletPlus enverra le message UDP configuré pour l'IP à distance et le port spécifié.	**Valeurs** **600**

Message Info Type	
Quand Modem_Event est sélectionné, jusqu'à trois charges utiles différentes peuvent être sélectionnées.	**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

4.0 Configuration

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)
RSSI	-	1 BYTE (UINT8_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

4.0 Configuration

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

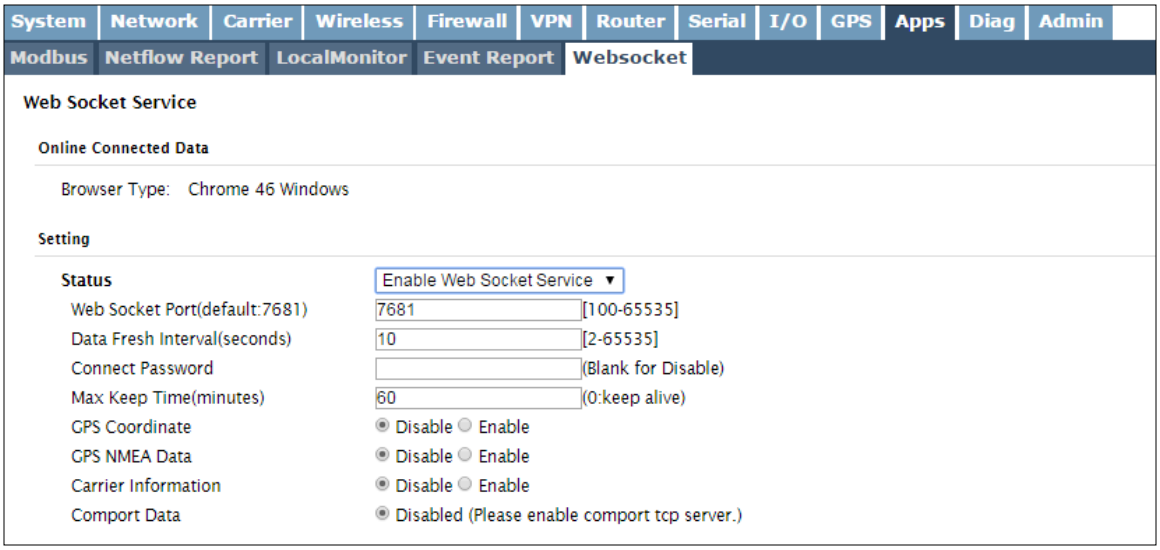


Image 4-11-7: Applications > Service Websocket

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 est 7681, et la plage valide est 100-65535.

Valeurs

7681

4.0 Configuration

Intervalles données Actualiser	
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 passe	
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 Time	
Ce champ détermine la durée de la prise de web est ouvert une fois démarré / activé. La valeur par défaut est de 60 minutes, une valeur de zéro signifie que le service de continuer à fonctionner indéfiniment.	**Valeurs** **60**

Coordonner GPS	
Si elle est activée, le modem rapport GPS données de coordonnées à l'websocket.	**Valeurs** **Désactiver** / Activer

GPS NMEA données	
Si elle est activée, le modem rapport des données NMEA GPS au websocket.	**Valeurs** **Désactiver** / Activer

Renseignements sur le transporteur	
Si elle est activée, le modem rapport des informations de support à l'websocket.	**Valeurs** **Désactiver** / Activer

Comport données	
Si elle est activée, et le port RS232 est configuré pour TCP Server, les données de Comport seront communiqués à la prise Web.	**Valeurs** **Désactiver** / Activer

4.0 Configuration

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.

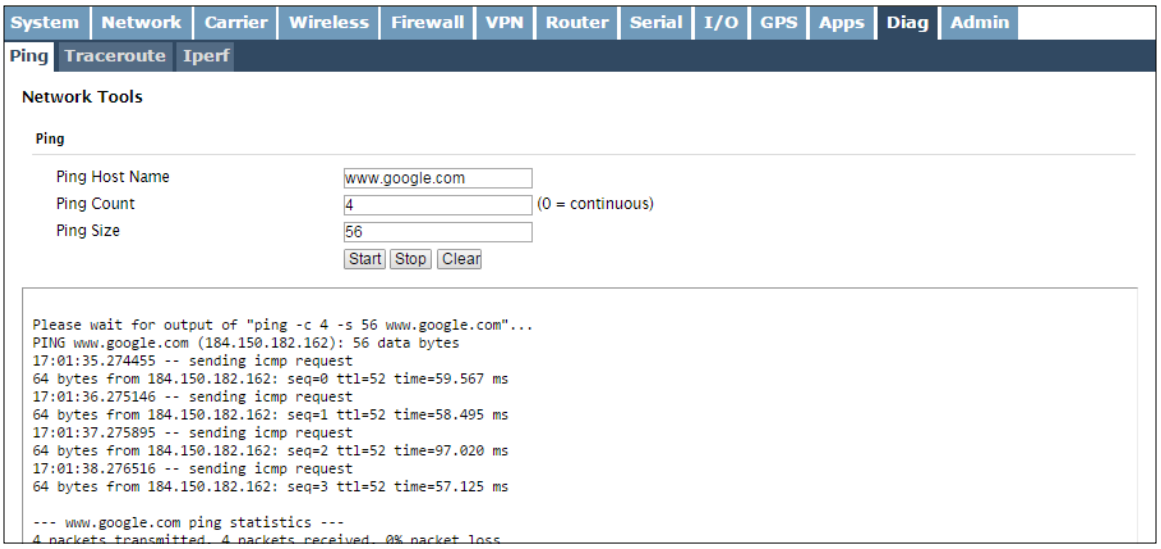


Image 4-12-1: Diag > Ping

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.

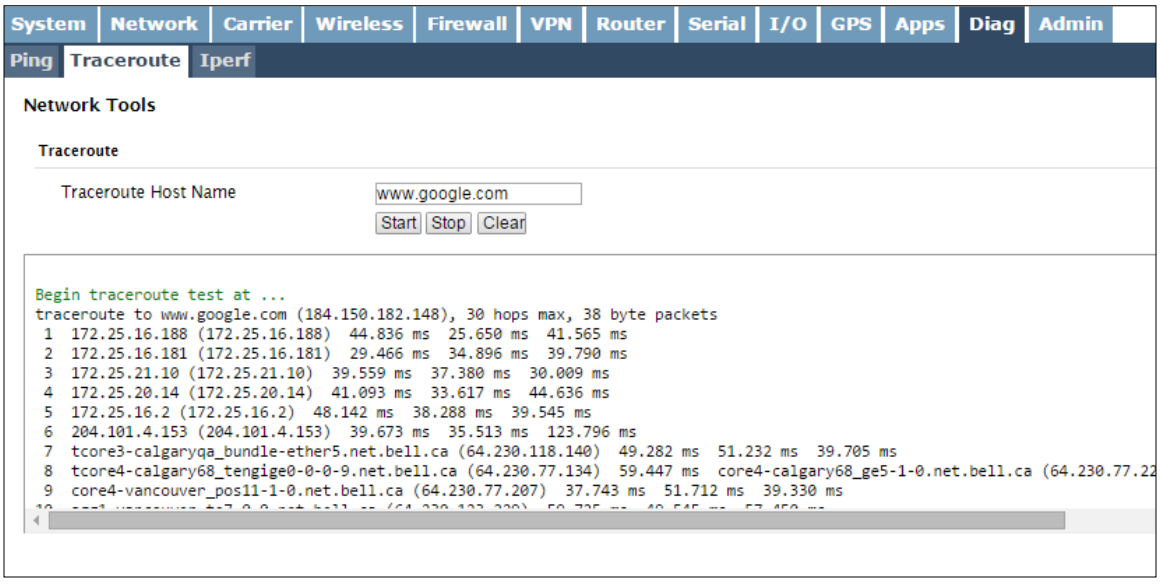


Image 4-12-2: Diag > Traceroute

4.0 Configuration

4.12.3 Iperf

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.

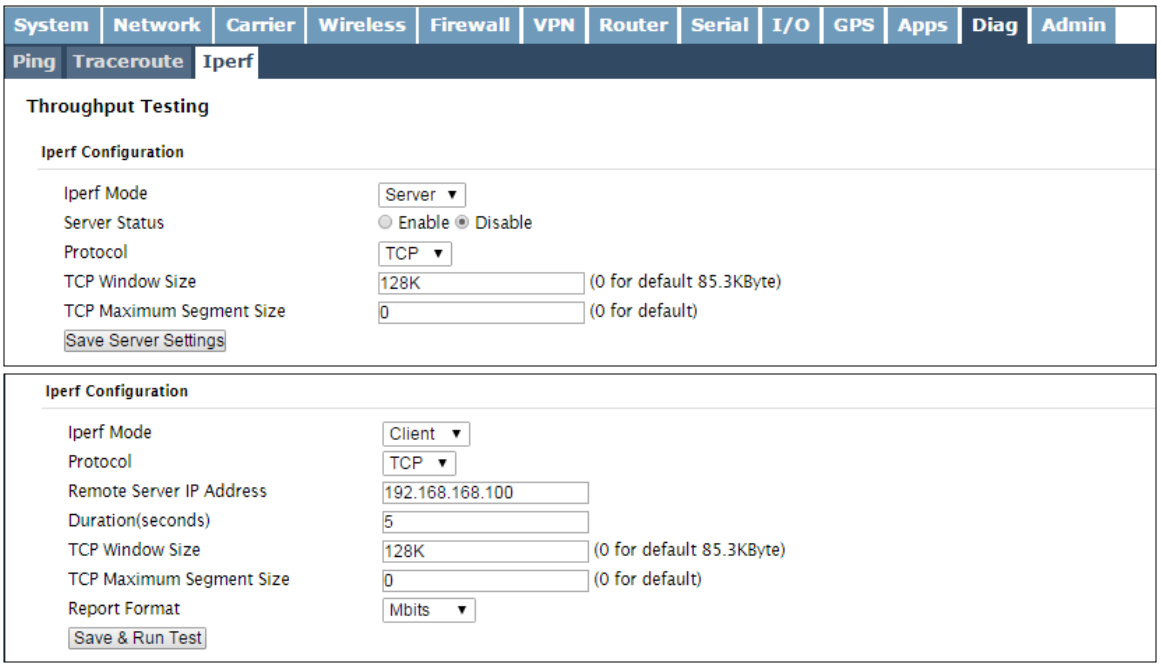


Image 4-12-3: Diag > Iperf

Iperf Mode

Sélectionnez entre un serveur Iperf (écoute pour les connexions entrantes) et le client (établit une connexion avec un serveur)

Valeurs

Serveur / Client

Serveur Status

Si le mode Iperf pour régler sur le serveur, ce serveur Statut permet à un utilisateur d'activer ou désactiver le serveur.

Valeurs

Activer / **Désactiver**

Protocol

SelSélectionner le type de paquets à envoyer à tester le débit. les paquets TCP sont orientés connexion et nécessitent une charge supplémentaire pour le handshaking qui se produit, alors que UDP est un, le meilleur effort de protocole orienté.

Valeurs

TCP / UDP

4.0 Configuration

TCP Window Size

Définissez la taille de la fenêtre TCP pour le Iperf Client / Serveur. La valeur par défaut recommandée est 85.3KG, qui peut être réglé en entrant 0.

Valeurs

0

TCP Maximum Segment Size

Définissez la taille TCP Max Segment pour le Iperf Client / Serveur. Mettre à 0 pour les paramètres recommandés.

Valeurs

0

Serveur distant Adresse

En mode client, sélectionnez le serveur Iperf en saisissant son adresse IP ici.

Valeurs

192.168.168.100

Durée

En mode client, sélectionnez la durée de l'essai (en secondes). La valeur par défaut est 5.

Valeurs

5

Format du rapport

Sélectionnez le format pour afficher les numéros de bande passante dans les formats pris en charge sont les suivants:

'Kbits' = Kbits/sec
'Mbits' = Mbits/sec
'Kbytes' = KBytes/sec
'M'bytes = MBytes/sec

Valeurs

Kbits
Mbits
Kbytes
Mbytes

4.0 Configuration

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.

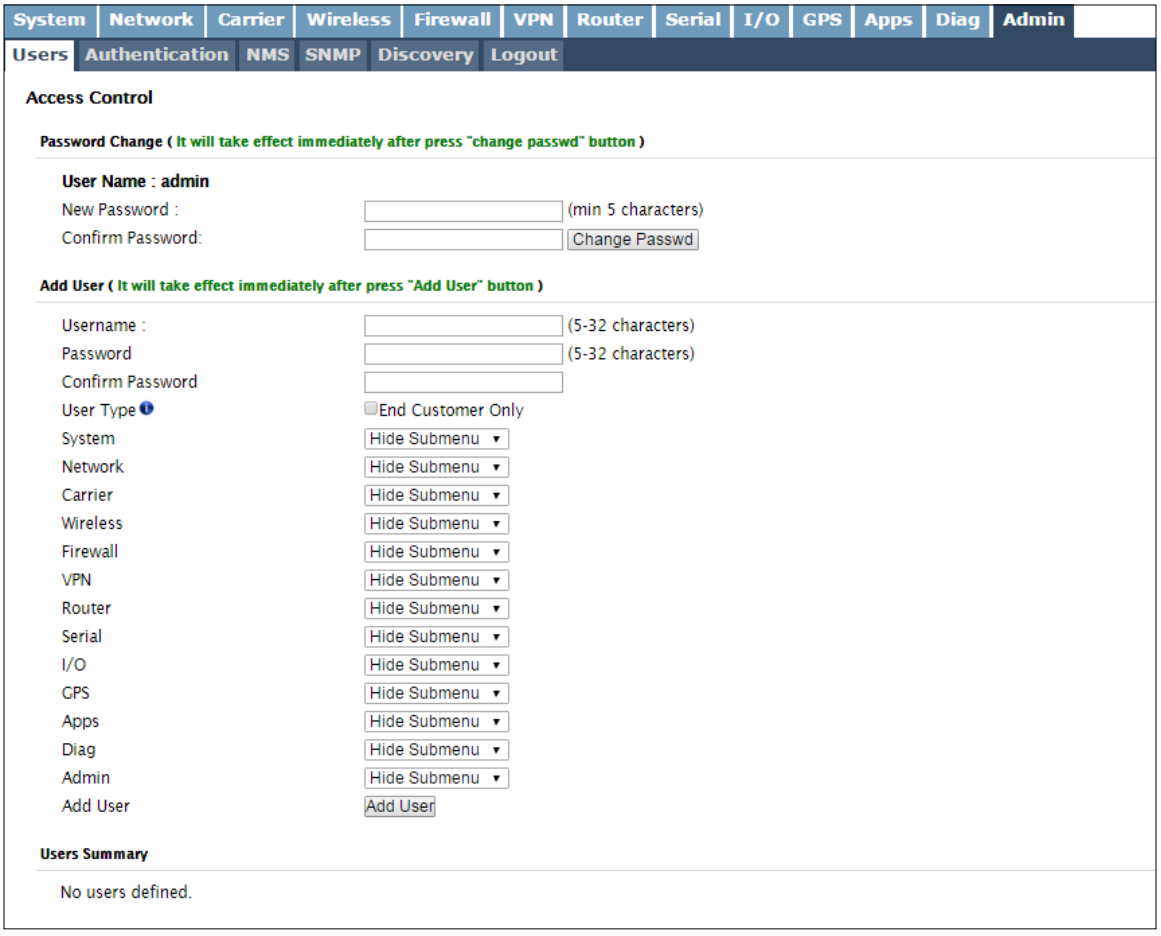


Image 4-13-1: Utilisateurs > Mot de passe Changer

Nouveau mot de passe

Entrez un nouveau mot de passe pour l'utilisateur 'admin'. Il doit être d'au moins 5 caractères. Le mot de passe par défaut pour 'admin' est 'admin'.

Valeurs

admin

Confirmez le mot de passe

Le mot de passe exact doit être entré pour confirmer le changement de mot de passe, s'il y a une erreur toutes les modifications seront rejetées.

Valeurs

admin

4.0 Configuration

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.

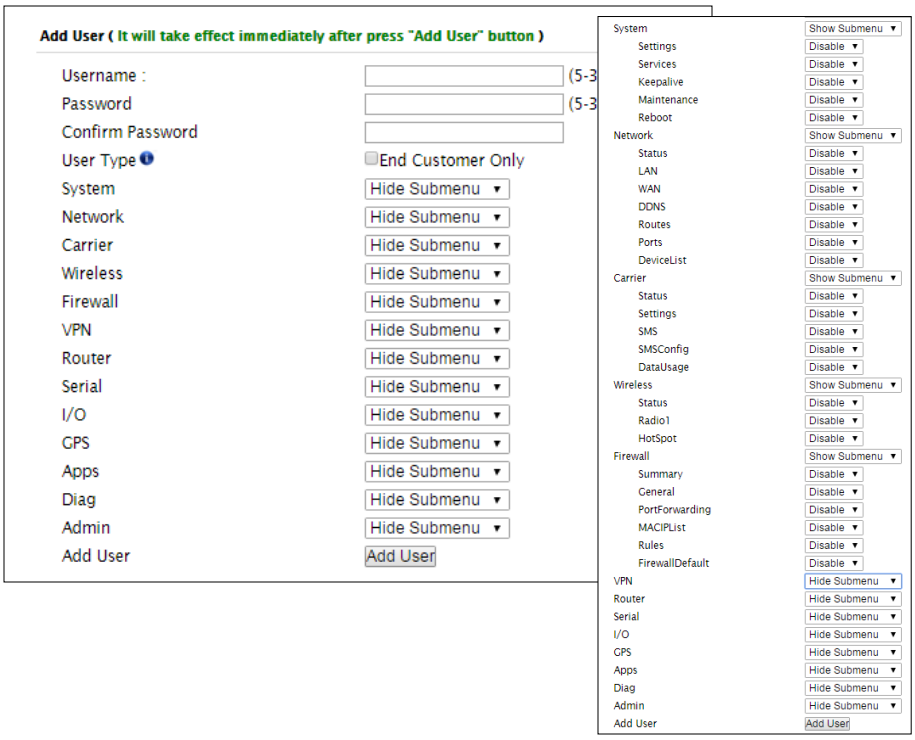


Image 4-13-2: Contrôle d'accès> Utilisateurs

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 lorsque le système a été redémarré.

Valeurs

(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.

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

4.0 Configuration

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.

RADIUS: distance Authentication Dial In User Service. Un protocole d'authentification, d'autorisation et de comptabilité qui peuvent être utilisés dans des applications d'accès au réseau.

Un serveur RADIUS est utilisé pour vérifier que les informations sont correctes.

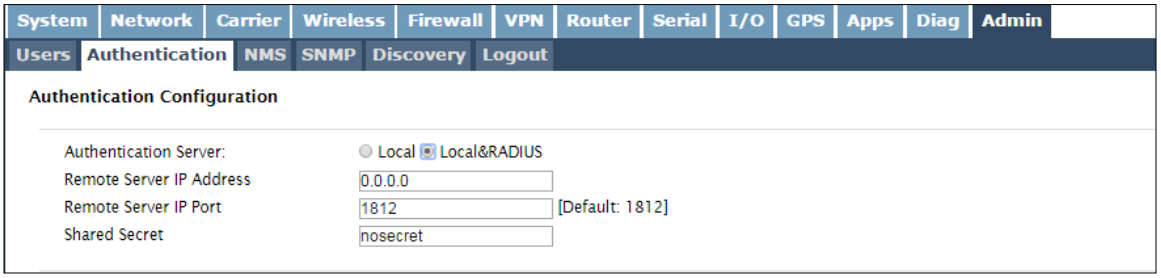


Image 4-13-3: Configuration de l'authentification

Serveur d'authentification

Sélectionnez le mode d'authentification: Local (par défaut) ou RADIUS local. Pour cette dernière sélection, l'authentification RADIUS doit être tentée FIRST; en cas d'échec, l'authentification locale peut être tentée.

Valeurs

Locale
Local&RADIUS

Serveur distant Adresse IP

Dans ce domaine, l'adresse IP du serveur RADIUS doit être saisi si RADIUS local a été sélectionné comme mode d'autorisation.

Valeurs

RADIUS valide adresse IP du serveur

0.0.0.0

RADIUS Secret

Si le mode d'autorisation a été défini sur RADIUS Local, RADIUS obtenir le secret de son client particulier de votre RADIUS Server Administrator et entrez dans ce champ.

Valeurs

nosecret

4.0 Configuration

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.

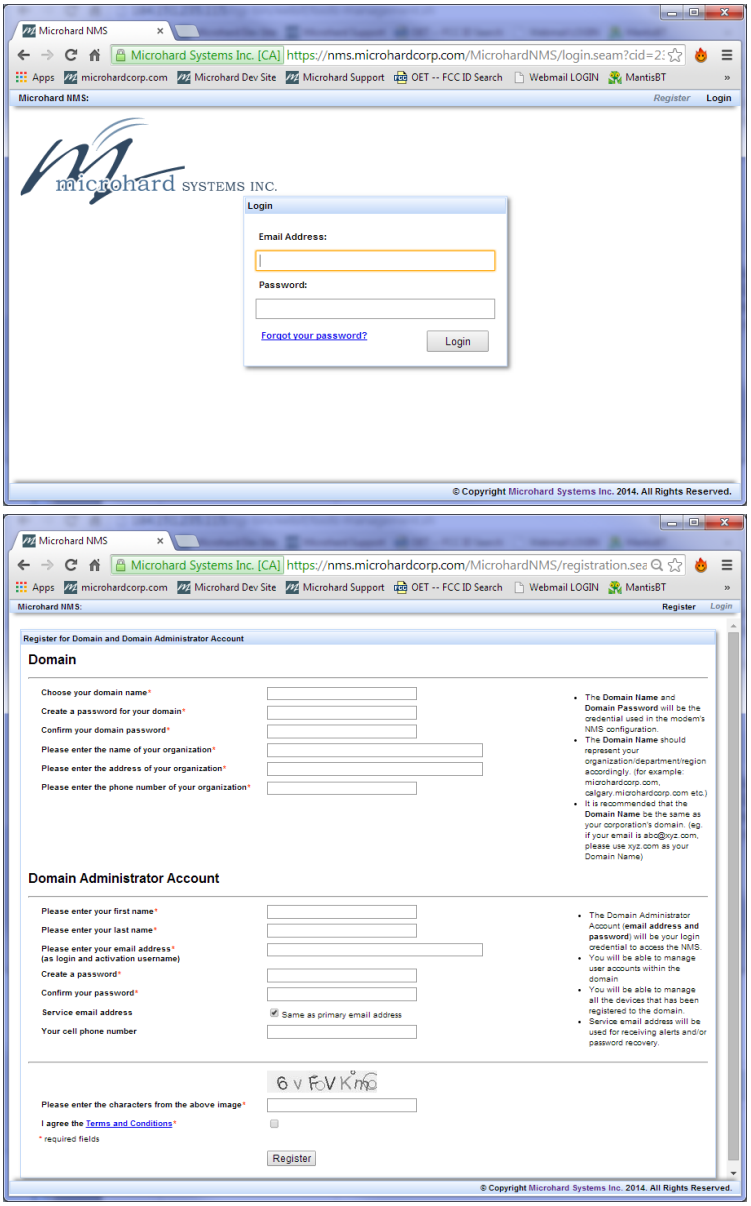


Image 4-13-4: NMS

4.0 Configuration

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 sous-domaines 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.

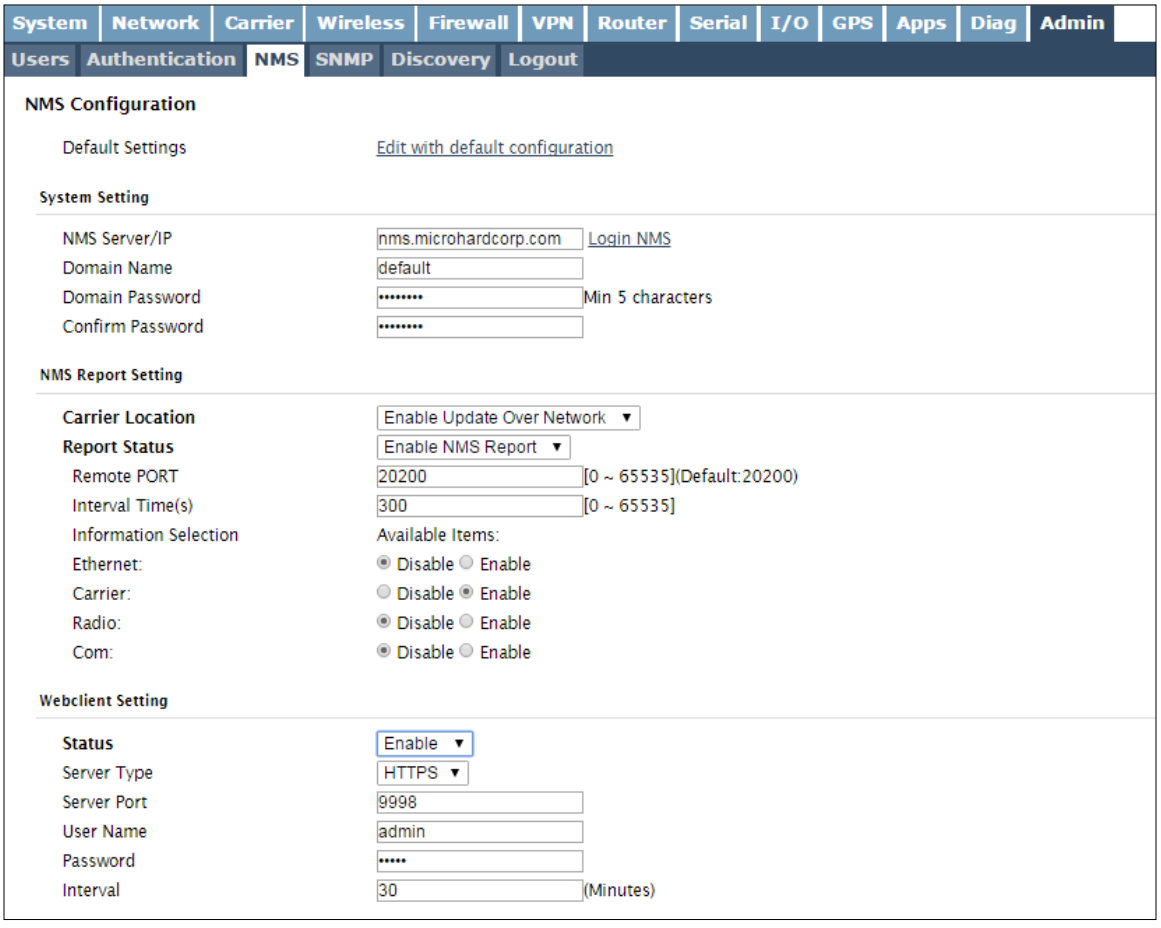


Image 4-13-5: NMS Paramètres

4.0 Configuration

Network Management System (NMS) Configuration

Paramètres par défaut

Le lien Paramètres par défaut réinitialise le formulaire de configuration aux valeurs d'usine par défaut. La forme doit encore être soumis avant toute modification se produira.

NMS / IP du serveur

L'adresse du serveur par défaut pour NMS est corp.com nms.microhard. La NMS peut également être hébergé en privé, et si tel est le cas, entrez l'adresse ici.

Valeurs

nms.microhardcorp.com

Nom de domaine / Mot de passe

Ceci est le nom de domaine et mot de passe qui a été enregistré sur le site NMS, il doit être saisi pour permettre des rapports au système NMS.

Valeurs

défaut

Rapport NMS Cadre

Transporteur Lieu

Activer ou désactiver l'emplacement estimation via une connexion porteuse. Lorsqu'elle est activée, les BulletPlus va consommer des données pour récupérer des informations de localisation de l'Internet.

Valeurs

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 écoute. Assurez-vous cela correspond à ce qui est configuré sur NMS. La valeur par défaut est 20200.

Valeurs

20200

Intervalle (s)

L'intervalle définit la fréquence des données est signalé à NMC. Les données le plus souvent est rapporté, plus de données est utilisé, ce qui devrait être réglé selon le plan de données d'un utilisateur. (0 à 65535 secondes)

Valeurs

300

4.0 Configuration

Sélection 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 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.

Valeurs

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 redémarrages, la mise à niveau du microprogramme et tâches de sauvegarde, etc.

Valeurs

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 sur les pare-feu installés.

Valeurs

9998

Identifiant 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 NMS pour déterminer s'il y a des tâches à accomplir. données Carrier seront consommés chaque fois que le dispositif sonde le système NMS.

Valeurs

60

4.0 Configuration

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

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.

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.

4.0 Configuration

Paramètres SNMP

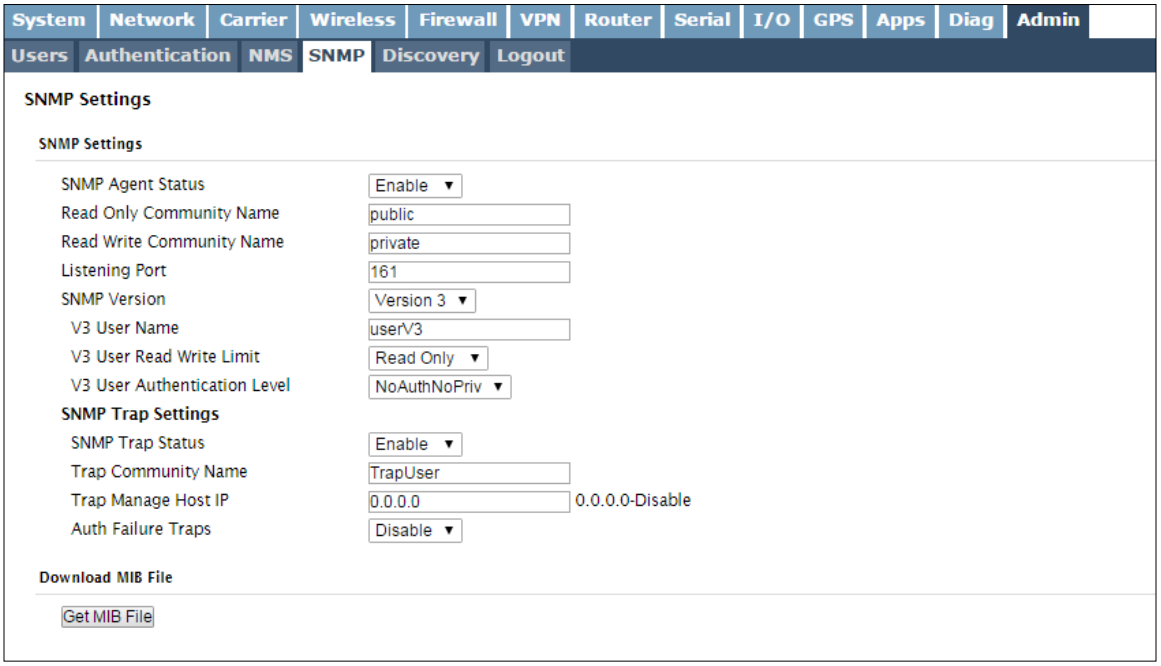


Image 4-13-6: Admin > SNMP

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.

Valeurs

Désactiver/ V1&V2c&V3

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.

Valeurs

public

Lecture seule Nom communautaire

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.

Valeurs

private

SNMPv3 Nom d'utilisateur

Définit le nom d'utilisateur pour SNMPv3.

Valeurs

V3user

4.0 Configuration

V3 utilisateur Read Write Limit

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.

Valeurs

Read Only / Read Write

Authentification utilisateur V3 Niveau

Définit le niveau d'authentification de l'utilisateur SNMPv3:
NoAuthNoPriv: Pas d'authentification, aucun cryptage.
AuthNoPriv: authentification, aucun chiffrement.
AuthPriv: Authentification, chiffrement.

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.

Valeurs

00000000

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).

Valeurs

00000000

SNMP Trap Version

Sélectionnez la version du piège sera envoyé si une condition de panne ou d'alarme se produire.

Valeurs

V1 Traps V2 Traps
V3 Traps V1&V2 Traps
V1&V2&V3 Traps

Auth Piège de défaillance

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

Valeurs

Désactiver / Activer

Nom 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

4.0 Configuration

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.

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

Discovery Service Status

Utilisez cette option pour activer ou désactiver le service de découverte.

Valeurs

Disable / **Discoverable** / Changable

Paramètres du port serveur

Spécifiez le port exécutant le service de découverte sur l'unité BulletPlus.

Valeurs

20077

4.0 Configuration

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.

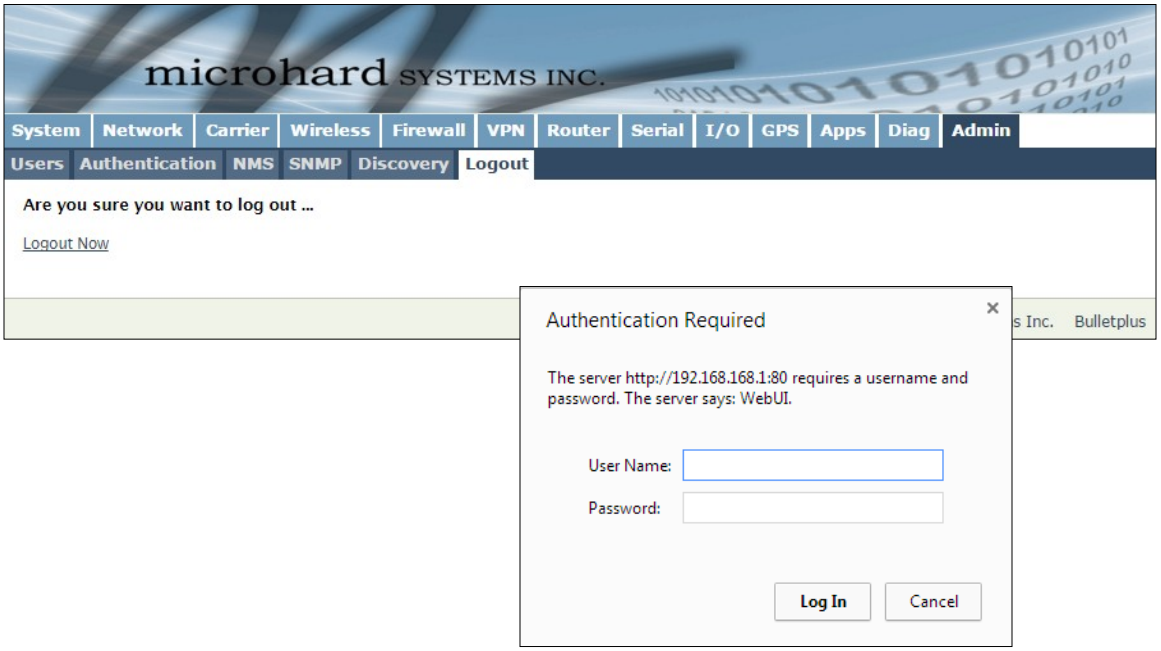


Image 4-13-9: Admiin > logout

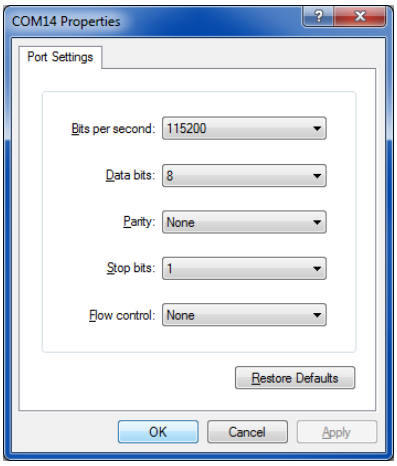
5.0 AT Command Line Interface

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.



Paramètres par défaut:

Vitesse: 115200

Bits de données: 8

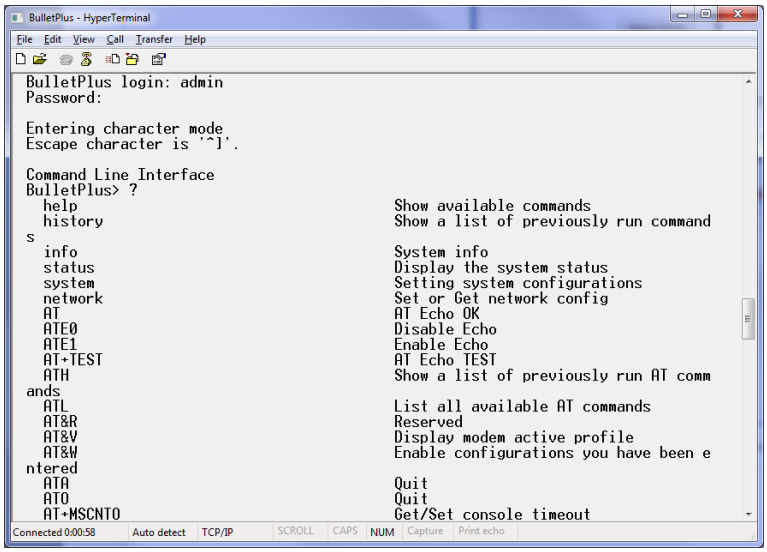
Parité: Aucun

Bits d'arrêt: 1

Contrôle de flux: Aucun

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.



Paramètres par défaut:

BulletPlus connexion: admin

Mot de passe: admin

Image 5-2: AT fenêtre de commande

5.0 AT Command Line Interface

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.

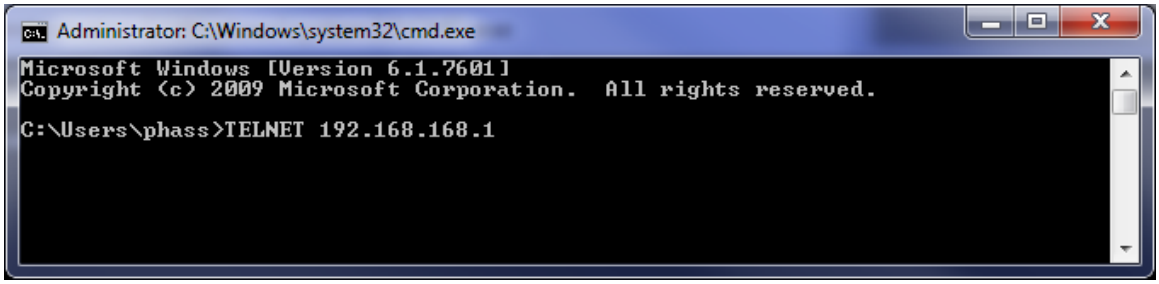


Image 5-3: Établissement d'une session Telnet

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).

Les paramètres réseau par défaut:

IP: 192.168.168.1
Subnet: 255.255.255.0
Passerelle: 192.168.168.1

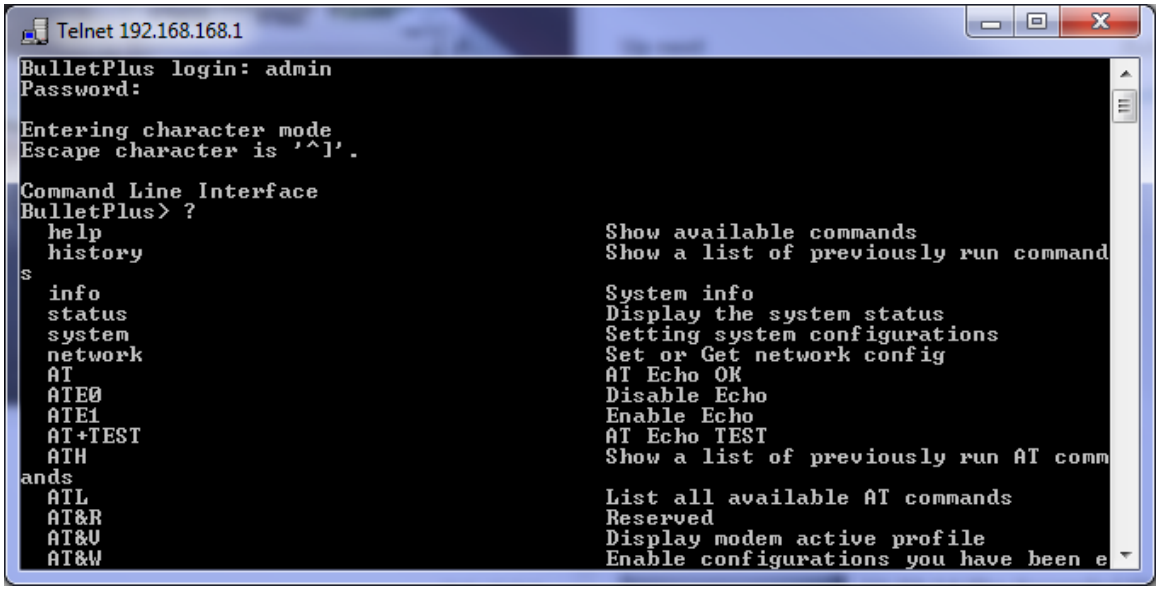


Image 5-4: Telnet AT session de commande

5.0 AT Command Line Interface

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:

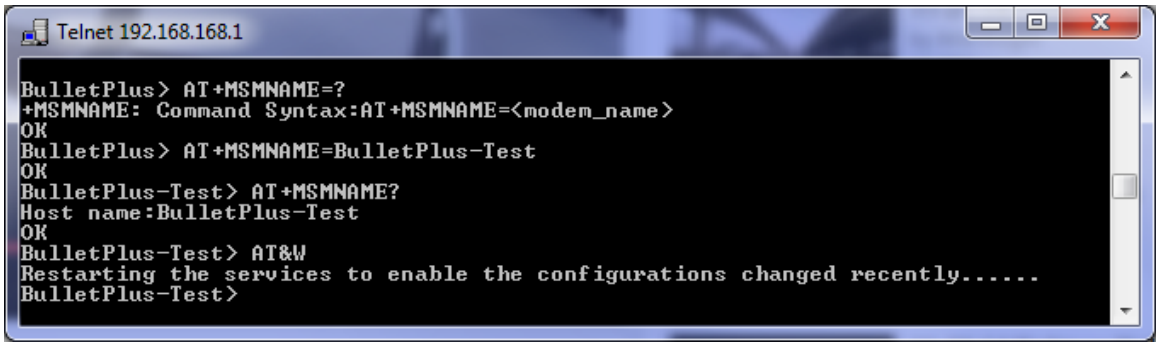


Image 5-5: Telnet AT Syntaxe de Commande

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

5.0 AT Command Line Interface

5.3 Commandes AT Supportées

AT	
La description	**Syntaxe de la commande(Effet: Immédiate)**
Echo OK.	**AT <enter>**

Exemple

Commander:
AT <enter>
Réponse:
OK

ATE0	
La description	**Syntaxe de la commande(Effet: Immédiate)**
Désactiver l'écho local.	**ATE0 <enter>**

Exemple

Commander:
ATE0 <enter>
Réponse:
OK

ATE1	
La description	**Syntaxe de la commande(Effet: Immédiate)**
Activer l'écho local.	**ATE1 <enter>**

Exemple

Commander:
ATE1 <enter>
Réponse:
OK

5.0 AT Command Line Interface

ATH

La description

Afficher la liste des commandes précédemment exécutés.

Syntaxe de la commande(Effet: Immédiate)

ATH <enter>

Exemple

Commander:
ATH <enter>
Réponse:
AT Command history: 1. ATH 2. ATL 3. ATH

ATL

La description

Afficher une liste de toutes les commandes AT disponibles.

Syntaxe de la commande(Effet: Immédiate)

ATL <enter>

Exemple

Commander:
ATL <enter>
Réponse:
AT Commands available:

AT	AT Echo OK
ATE0	Disable Echo
ATE1	Enable Echo
ATH	Show a list of previously run AT commands
ATL	List all available AT commands
AT&R	Reserved
AT&V	Display modem active profile
AT&W	Enable configurations you have been entered
ATA	Quit
ATO	Quit

.
.
.
<Output Omitted>

AT&R

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

5.0 AT Command Line Interface

AT&V

La description

Lire modem profil actif.

Syntaxe de la commande(Effet: Immédiate)

AT&V <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

AT&W

La description

Activer les changements de configurations qui ont été saisies.

Syntaxe de la commande(Effet: Immédiate)

AT&W <enter>

Exemple

Commander:
AT&W <enter>
Réponse:
Restarting the services to enable the configurations changed recently.....

ATA / ATO

La description

Quitter. Quitte à la session de commande et vous renvoie à se connecter rapidement.

Syntaxe de la commande(Effet: Immédiate)

ATA <enter>

Exemple

Commander:
ATA <enter>
Réponse:
OKConnection closed by foreign host

5.0 AT Command Line Interface

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.

Syntaxe de la commande

AT+MSGMI=<enter>

Exemple

Commander:
AT+MSGMI<enter>

Réponse:
+MSGMI: 2014-2015 Microhard Systems Inc.
OK

5.0 AT Command Line Interface

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

5.0 AT Command Line Interface

AT+MSMNAME

La description

Description du Modem Nom / Radio. 30 caractères.

Syntaxe de la commande(Effet: AT&W)

AT+MSMNAME=<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
OK

AT+MSRTF

La description

Réinitialiser le modem aux paramètres d'usine par défaut de la mémoire non-volatile.

Syntaxe de la commande(Effet: Immédiate)

AT+MSRTF=<Action>
Action:
0 action prédéfinie
l'action 1 confirmation

Exemple

Commander: (Pour définir la valeur)
AT+MSRTF=1<enter>
Réponse:
OK

AT+MSREB

La description

Redémarrez le modem.

Syntaxe de la commande(Effet: Immédiate)

AT+MSREB <enter>

Exemple

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

5.0 AT Command Line Interface

AT+MSNTP

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

AT+MSSYSLOG

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+MSSYSLOG=192.168.168.35,514<enter>
Réponse:
OK

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

AT+MSSERVICE

La description

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

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

Exemple

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

5.0 AT Command Line Interface

AT+MSWEBUI

La description

Obtenir / set protocole WebUI et le port

Exemple

Commander:
AT+MSWEBUI=0,80,443<enter>
Réponse:
OK

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.

Exemple

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

Syntaxe de la commande(Effet: AT&W)

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

5.0 AT Command Line Interface

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

5.0 AT Command Line Interface

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
Mode         : 1 - DHCP Server enabled
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
```

5.0 AT Command Line Interface

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+MNLANDNS

La description

Get / Régler l'interface LAN de réseau: DNS

Syntaxe de la commande(Effet: AT&W)

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)

Exemple

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

5.0 AT Command Line Interface

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
Gateway: Valid IP address. 0 - Reset

Exemple

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

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

5.0 AT Command Line Interface

AT+MNWANDR

La description

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

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

AT+MNWANDNS

La description

Lire / Serveur DNS lorsque le port WAN défini comme indépendant WAN.

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

5.0 AT Command Line Interface

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.DNS>,<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

5.0 AT Command Line Interface

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=DEL,<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

5.0 AT Command Line Interface

AT+MNEMAC

La description

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

Command Syntax

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

5.0 AT Command Line Interface

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   : 0B
    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         184.0.0.1       0.0.0.0         UG    0      0        0 br-wan2
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
```

5.0 AT Command Line Interface

AT+MNDDNSE

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

AT+MNDDNS

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

5.0 AT Command Line Interface

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

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
Exception Port: 0 - 65535

5.0 AT Command Line Interface

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

5.0 AT Command Line Interface

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

5.0 AT Command Line Interface

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 - LAN
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

5.0 AT Command Line Interface

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
Action : ACCEPT
Source :
Src IP From :
Src IP To : 0
Destination :
Dest IP From :
Dest IP To : 0
Dest Port : 34567
Protocol : tcpudp
OK

5.0 AT Command Line Interface

AT+MFRST

La description	Syntaxe de la commande
Réinitialiser par défaut le pare-feu	**AT+MFRST <enter>**

Exemple

Commander:
AT+MFRST<enter>

AT+MMIMEI

La description	Syntaxe de la commande
Obtenez IMEI de modem.	**AT+MMIMEI <enter>**

Exemple

Commander:
AT+MMIMEI<enter>
Réponse:
+MMIMEI: 356406060882064
OK

AT+MMIMSI

La description	Syntaxe de la commande
Obtenez modem IMEI.	**AT+MMIMSI <enter>**

Exemple

Commander:
AT+MMIMSI<enter>
Réponse:
+MMIMSI: 302610012606734
OK

AT+MMNETRSSI

La description	Syntaxe de la commande
Obtenez modem RSSI.	**AT+MMNETRSSI <enter>**

Exemple

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

5.0 AT Command Line Interface

AT+MMPOWERIN

La description

Obtenez tension de contribution du modem.

Syntaxe de la commande

AT+MMPOWERIN <enter>

Exemple

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

AT+MMBOARDTEMP

La description

Obtenez la température du modem.

Syntaxe de la commande

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

5.0 AT Command Line Interface

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.

Syntaxe de la commande

AT+MMNUM <enter>

Exemple

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

AT+MMIMI

La description

Obtenez IMEI et IMSI de modem.

Syntaxe de la commande

AT+MMIMI <enter>

Exemple

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

5.0 AT Command Line Interface

AT+MMCID

La description

Obtenez modem numéro de carte SIM.

Syntaxe de la commande

AT+MMCID <enter>

Exemple

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

AT+MMMGS

La description

Envoyer un message SMS.

Syntaxe de la commande(Immediate)

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

OK

AT+MMMGR

La description

Lire des messages SMS.

Syntaxe de la commande(Immediate)

AT+MMMGR=<index>

Exemple

Commander:
AT+MMMGR=1<enter>

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

OK

5.0 AT Command Line Interface

AT+MMMGL

La description

Liste de tous les messages SMS.

Syntaxe de la commande(Immediate)

AT+MMMGL<enter>

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.

OK

AT+MMMGD

La description

Supprimer des messages SMS à partir du système.

Syntaxe de la commande(Immediate)

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

5.0 AT Command Line Interface

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

5.0 AT Command Line Interface

AT+MIOSTATUS

La description

GET état IO.

Syntaxe de la commande

AT+MIOSTATUS <enter>

Exemple

Commander:
AT+MIOSTATUS <enter>

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

AT+MIOMETER

La description

GET IO meter (V).

Syntaxe de la commande

AT+MIOMETER <enter>

Exemple

Commander:
AT+MIOMETER <enter>

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

AT+MCPS2

La description

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

Syntaxe de la commande(Effet: AT&W)

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

Exemple

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

5.0 AT Command Line Interface

AT+MCBR2

La description

Get / Set vitesse de transmission du port série.

Syntaxe de la commande(Effet: AT&W)

AT+MCBR2=<Baud Rate>
Baud Rate:
0 300
1 600
2 1200
3 2400
4 3600
5 4800
6 7200
7 9600
8 14400
9 19200
10 28800
11 38400
12 57600
13 115200
14 230400
15 460800
16 921600

Exemple

Commander:
AT+MCBR2=13<enter>
Réponse:
OK

Commander:
AT+MCBR2?
Réponse:
+MCBR2: 13 115200
OK

AT+MCDF2

La description

Obtenez le format / Set de port série de données

Syntaxe de la commande(Effet: AT&W)

AT+MCDF2=<data format>
Data Format:
0 8N1
2 8E1
3 8O1

Exemple

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

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
1 Transparent

Exemple

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

5.0 AT Command Line Interface

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

5.0 AT Command Line Interface

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/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.

Exemple

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

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

5.0 AT Command Line Interface

AT+MCTS2

La description

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

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

Exemple

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

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

5.0 AT Command Line Interface

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>,<Password>,<Mail Recipient>,<Message Max Size>,<TimeOut>,<Transfer Mode>
Mail Subject : 1 to 63 bytes
Mail Server : Valid IP Address or Name
Username : 1 to 63 bytes
Password : 1 to 63 bytes
Mail Recipient : 1 to 63 bytes
Message Max Size : [1 .. 65535]
TimeOut : [0 .. 65535] in seconds
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 Interval>,<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]
Local IP : Valid IP address
Host IP : Valid IP address
Idle Timeout : [0 .. 65535] in seconds
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
OK

5.0 AT Command Line Interface

AT+MAEURD1
AT+MAEURD2
AT+MAEURD3

La description

Définir l'événement Rapport UDP Rapport No.1 / 2/3.

Exemple

Commander:
AT+MAEURD1=1,192.168.168.111,2010,10<enter>
Réponse:
OK

Syntaxe de la commande(Effet: AT&W)

AT+MAEURD1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Time>[,Interfaces]]
Mode : 0 Disable
1 Modem Event Report
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

AT+MANMSR

La description

Définir Rapport NMS.

Exemple

Commander:
AT+MANMSR=1,20200,300<enter>
Réponse:
OK

Syntaxe de la commande(Effet: AT&W)

AT+MANMSR=<Mode>[,<Remote Port>,<Interval Time_s>]
Mode:
0 Disable
1 Enable NMS Report

AT+MANMSSRV

La description

Get/Set NMS Server.

Exemple

Commander:
AT+MANMSSRV=nms.microhardcorp.com,mytech,mypass,mypass <enter>
Réponse:
OK

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

5.0 AT Command Line Interface

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:
OK

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:
OK

5.0 AT Command Line Interface

AT+MASNMP

La description

Obtenez le service / Set SNMP.

Syntaxe de la commande(Effet: AT&W)

AT+MASNMP[=<Mode>[,<ROCommunity>,<RWCommunity>,<Port>,<Version>]]
Mode: 0 - Disable
1 - Enable
ROCommunity: Read Only Community Name 1 to 31 characters
RWCommunity: Read Write Community Name 1 to 31 characters
Port: Listening Port 0 to 65535. Default is 161
Version: SNMP version
1 - Version 1
2 - Version 2
3 - Version 3 (Use AT+MASNMPV3 to set Authentication and Privacy parameters)

Exemple

Commander:
AT+MASNMP=1,public,private,161,2<enter>
Réponse:
OK

5.0 AT Command Line Interface

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 (AuthNoPriv)
AT+MASNMPV3=<UserName>,<RWLimit>,2,<Auth>,<AuthPassword>,<Privacy>,<PrivacyPassword> If <AuthLevel>=2 (AuthPriv)

Exemple

Commander:
AT+MASNMPV3 <enter>
Réponse:
+MASNMPV3:
UserName : userV3
RWLimit : Read Only
AuthLevel : NoAuthNoPriv
OK

5.0 AT Command Line Interface

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>]

5.0 AT Command Line Interface

AT+MWRADIO

La description

Obtenir le statut de radio / Set, ou le désactiver.

Exemple

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

Syntaxe de la commande(Effet: AT&W)

AT+MWRADIO=<Radio>
Radio:
0 - Off
1 - On

AT+MWMODE

La description

Obtenez le mode radio / Set.

Exemple

Commander:
AT+MWMODE=2 <enter>
Réponse:
OK

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

AT+MWTXPOWER

La description

Obtenez / radio Set TX Power.

Exemple

Commander:
AT+MWTXPOWER=10 <enter>
Réponse:
OK

Syntaxe de la commande(Effet: AT&W)

AT+MWTXPOWER=<Tx Power>
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

5.0 AT Command Line Interface

AT+MWDISTANCE

La description

Obtenez / radio Set sans fil Distance.

Exemple

Commander:
AT+MWDISTANCE=1000 <enter>
Réponse:
OK

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+

5.0 AT Command Line Interface

AT+MWMPDUAGG

La description

Obtenez / radio Set MPDU Agrégation.

Exemple

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

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

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>

5.0 AT Command Line Interface

AT+MWAMSDU

La description

Obtenez un maximum de radio A MPDU (octet).

Syntaxe de la commande

AT+MWAMSDU

Exemple

Commander:
AT+MWAMSDU <enter>
Réponse:
+MWAMSDU: Maximum AMSDU (byte) - 3839

OK

AT+MWAMPDU

La description

Obtenez un maximum de radio AMPDU (octet).

Syntaxe de la commande

AT+MWAMPDU

Exemple

Commander:
AT+MWAMPDU <enter>
Réponse:
+MWAMPDU: Maximum AMPDU (byte) - 65535

OK

AT+MWRTSTHRESH

La description

Obtenir / set la radio RTS Threshold.

Syntaxe de la commande(Effet: AT&W)

AT+MWRTSTHRESH=<RTS Threshold>
RTS Threshold:
0 Disabled
256-2346 Enabled with the value

Exemple

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

5.0 AT Command Line Interface

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

La description

Get / Set Radio CCA Seuil.

Exemple

Commander:
AT+MWCCATHRESH=28 <enter>
Réponse:
OK

Syntaxe de la commande(Effet: AT&W)

AT+MWCCATHRESH=<CCA Threshold>
CCA Threshold:
Range of values: 4-127

AT+MWIFACE

La description

Liste / Ajouter / Supprimer interface virtuelle radio.

Exemple

Commander:
AT+MWIFACE=0 <enter>
Réponse:
Radio Virtual Interface [0]:
Network : lan
Mode : ap
TX bitrate : auto
ESSID Broadcast : Off
AP Isolation : Off
SSID : PWii
Encryption Type : psk2
WPA PSK : 1234567890
OK

Syntaxe de la commande(Effet: AT&W)

List one or all radio virtual interface(s) :
AT+MWIFACE=0[,<Index>]
Add one radio virtual interface :
AT+MWIFACE=1
Delete one radio virtual interface :
AT+MWIFACE=2,<Index>
Index:
Radio Virtual Interface Index: 0-3

5.0 AT Command Line Interface

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 - lan1

AT+MWSSID

La description

Get / Set interface virtuelle radio: SSID

Exemple

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

Syntaxe de la commande(Effet: AT&W)

AT+MWSSID=[<Index>[,<SSID>]]
Index:
  Radio Virtual Interface Index: 0-3
SSID:
  Radio Virtual Interface SSID: 1 - 63 character

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

5.0 AT Command Line Interface

AT+MWRATE

La description

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

La description

Get / Set interface virtuelle radio: WDS

Exemple

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

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

5.0 AT Command Line Interface

AT+MWAPISOLATION

La description

Get / Set interface virtuelle radio: AP Isolation

Exemple

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

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+WPA2 (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

5.0 AT Command Line Interface

AT+WSCAN

La description

Obtenez réseau radio des données de numérisation. (Doit être en mode client, scanne les réseaux disponibles).

Syntaxe de la commande

AT+WSCAN <enter>

Exemple

Commander:
AT+WSCAN <enter>
Réponse:
Varies

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)		Signal		Host (e.g. PC) (DTE)
1		DCD	→	IN
2		RX	→	IN
3	←	TX		OUT
4	←	DTR		OUT
5		SG		
6		DSR	→	IN
7	←	RTS		OUT
8		CTS	→	IN

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).

L'interface est conforme à la RS-232 standard des signaux, de sorte que la connexion directe à un PC hôte (par exemple) est logé.

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)

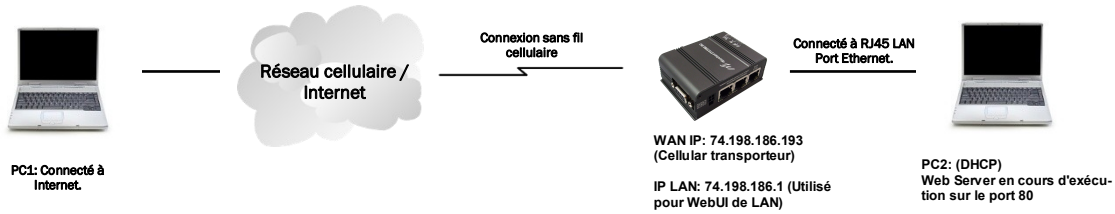
En remplissant le processus de démarrage rapide, un utilisateur aurait dû être en mesure de se connecter et configurer les BulletPlus à travailler avec leur opérateur cellulaire. En remplissant ce, le modem est prêt à être utilisé pour accéder à Internet et fournir une connectivité mobile. Cependant, 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.

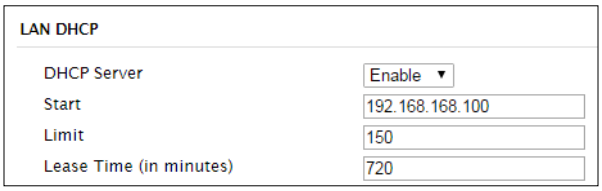
IP-Passthrough est idéal pour les applications où un seul appareil est connecté au BulletPlus, et d'autres caractéristiques des BulletPlus ne sont pas nécessaires. En mode pass-through, la plupart des caractéristiques des BulletPlus sont contournés, ce qui inclut les ports série, les fonctions GPS, VPN, 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.



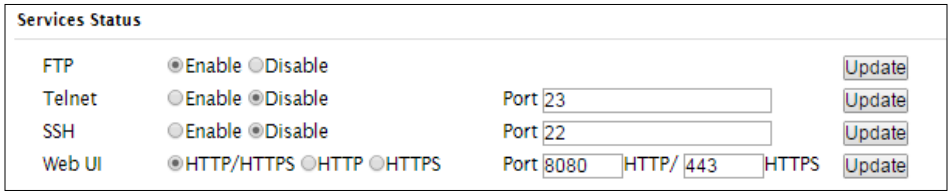
Étape 1

Connectez-vous au BulletPlus (Reportez-vous à démarrage rapide), et veiller à ce que DHCP est activé sur le (modifier) la page Réseau> LAN.



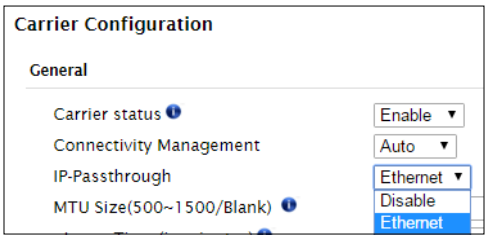
Étape 2

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).



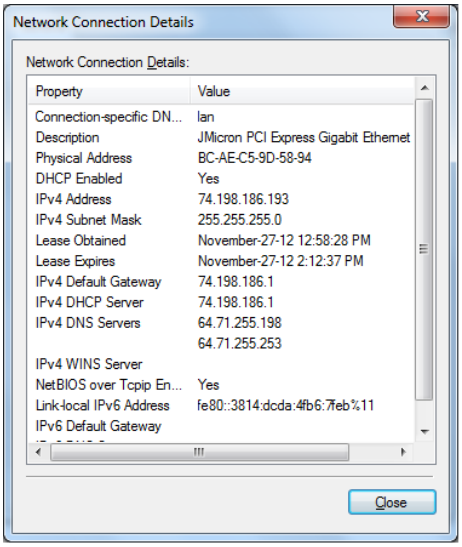
Annexe B: IP-Passthrough Exemple (Page 2 de 2)

Étape 3



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

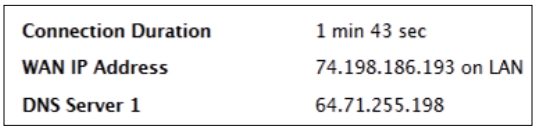
Fixer le dispositif à distance ou PC au port RJ45 du BulletPlus. Le dispositif final doit être mis en place pour DHCP pour obtenir une adresse IP à partir des BulletPlus. Dans la configuration de test / Exemple nous pouvons vérifier cela en regardant l'adresse IP actuelle. Dans la capture d'écran à droite, 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:

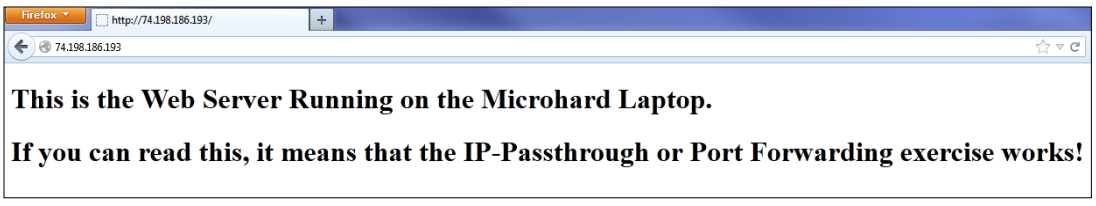
- À distance sur le côté WAN (généralement Internet), en utilisant l'adresse IP WAN, et le port spécifié pour le fonctionnement de HTTP (ou, si elle est activée, en utilisant le (443) ports HTTPS), dans ce Exemple avec serait 74.198.186.193:8080.
- Sur le côté LAN, en entrant dans les 3 premiers octets 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.



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.



Annexe C: Port Forwarding Exemple (Page 1 de 2)

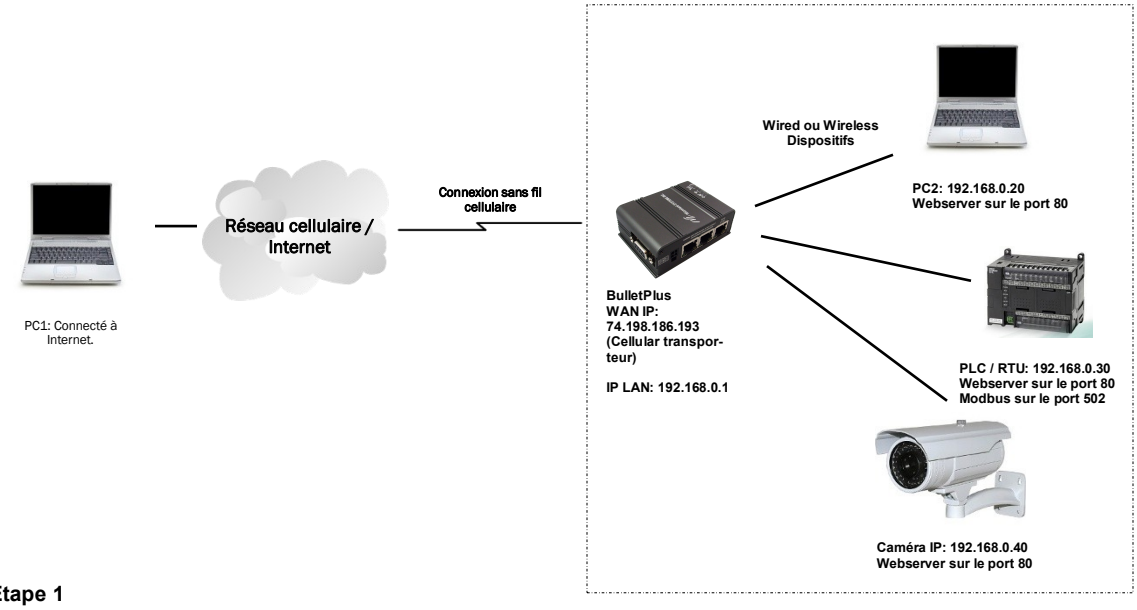
En remplissant le processus de démarrage rapide, un utilisateur aurait dû être en mesure de se connecter et configurer les BulletPlus à travailler avec leur opérateur cellulaire. En remplissant ce, le modem est prêt à être utilisé pour accéder à Internet et fournir une connectivité mobile. Cependant, 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.

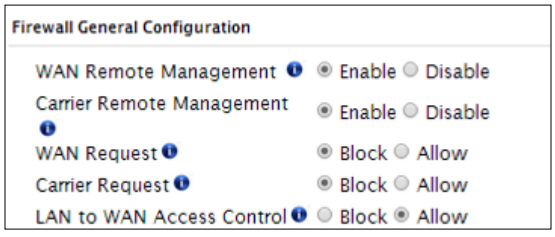
DMZ (une forme de redirection de port) est utile pour les situations où il y a plusieurs appareils connectés au BulletPlus, mais tout le trafic entrant est destiné à un seul appareil. Il est également populaire à utiliser DMZ dans les cas où un seul appareil est connecté, mais plusieurs ports sont transmis 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.



Étape 1

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.



Annexe C: Port Forwarding Exemple (Page 2 de 2)

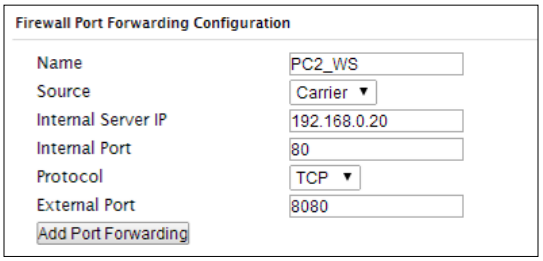
Étape 2

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.

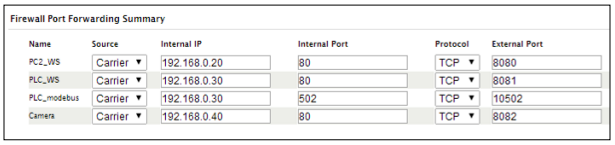
La description	WAN IP	Externe Port	Interne IP	Interne Port
BulletPlus WebUI	74.198.186.193	80	192.168.0.1	80
PC2 Web Serveur	74.198.186.193	8080	192.168.0.20	80
PLC Web Serveur	74.198.186.193	8081	192.168.0.30	80
PLC Modbus	74.198.186.193	10502	192.168.0.30	502
Camera Web Serveur	74.198.186.193	8082	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. Assurez-vous 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:

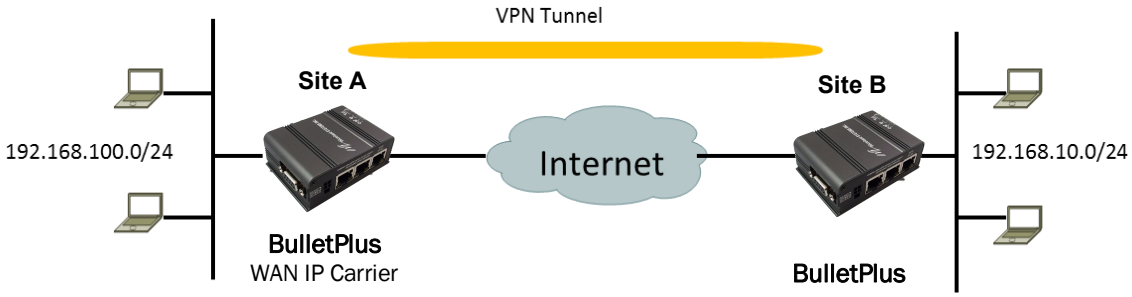
Pour le serveur Web sur le PC, utilisez un navigateur pour se connecter à 74.198.186: 193: 8080, dans ce cas, le même serveur Web est en cours d'exécution comme dans le IP-Passthrough Exemple, de sorte que le résultat devrait être comme suit:
Pour accéder aux autres appareils / services: Pour l'automate 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.

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)



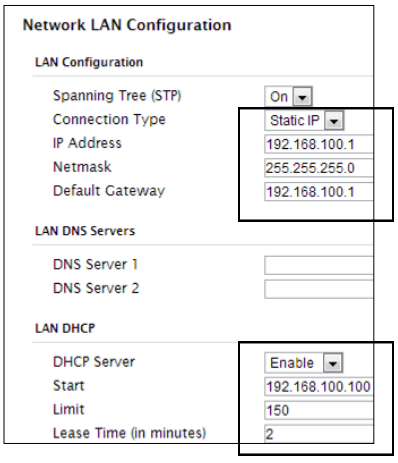
Étape 1

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.

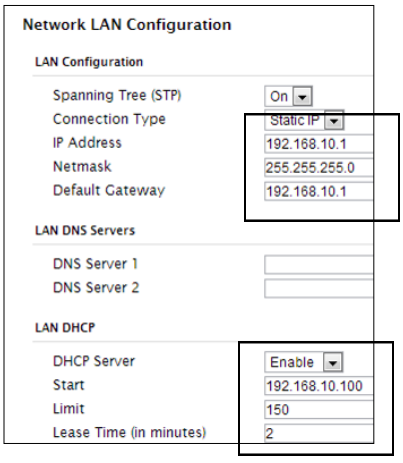
Étape 2

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



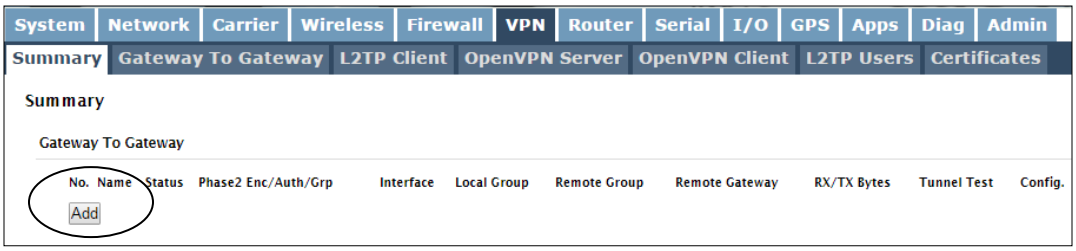
Site B



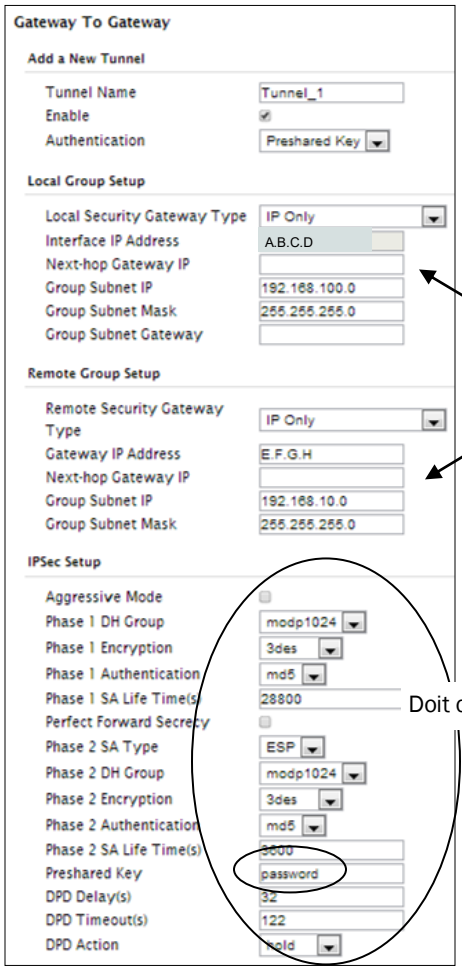
Annexe D: VPN Exemple (Page 2 de 2)

Étape 3

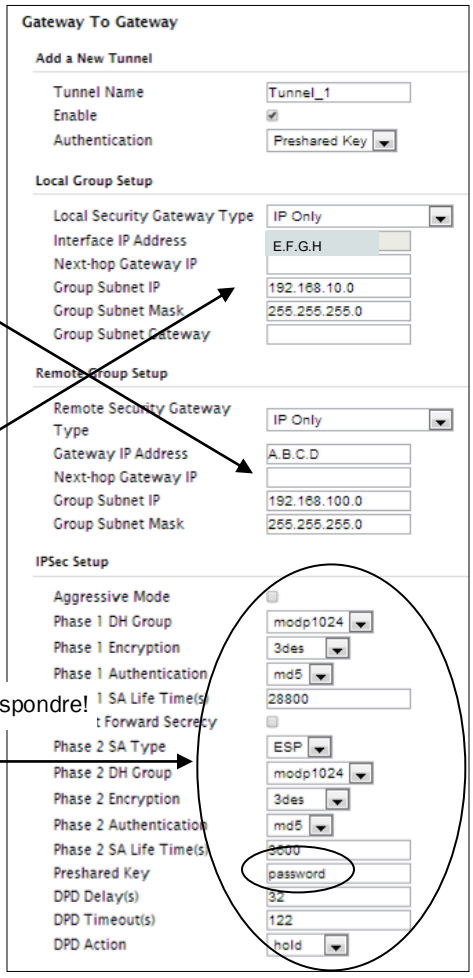
Ajouter une passerelle VPN Gateway tunnel sur chaque BulletPlus.



Site A



Site B



Doit correspondre!

Étape 4

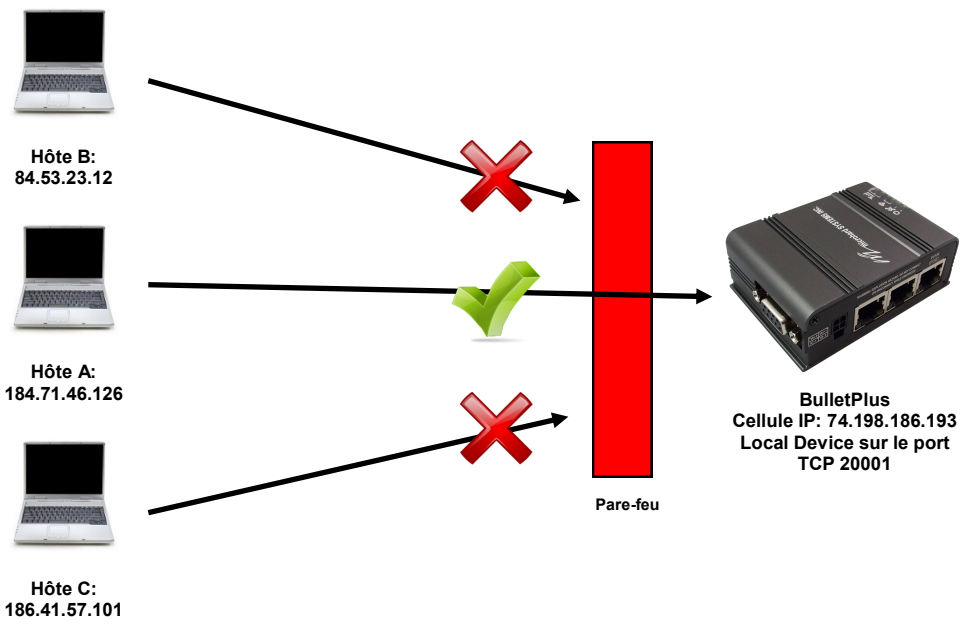
Soumettre des modifications à deux unités. Il devrait être possible de faire un ping et d'atteindre des dispositifs à chaque extrémité du tunnel VPN si les deux appareils ont été configurés correctement et disposer d'une connectivité réseau.

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

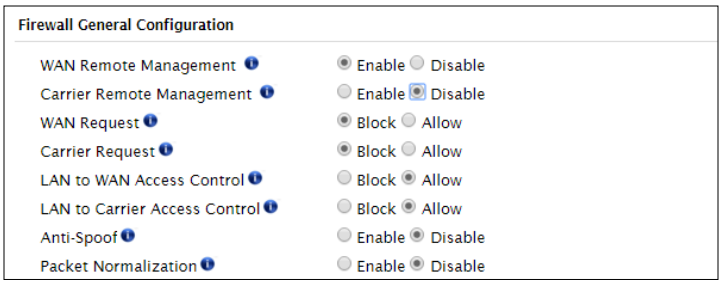
- Règles personnalisables
- Et / Liste IP ou MAC
- (Access Control List) ACL ou Blacklist en utilisant les outils ci-dessus.

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.

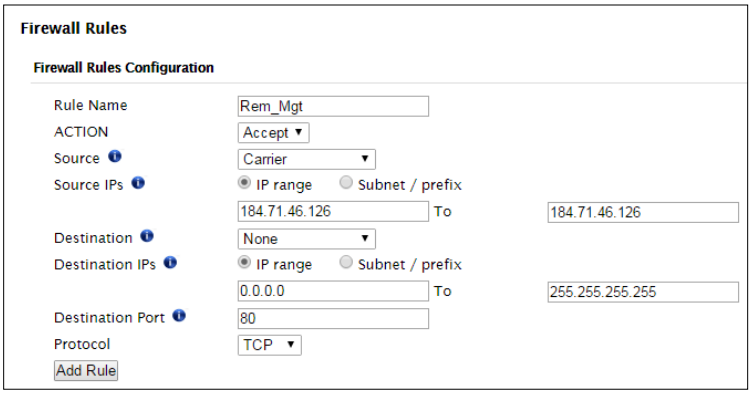


Annexe E: Firewall Exemple (Page 2 de 2)

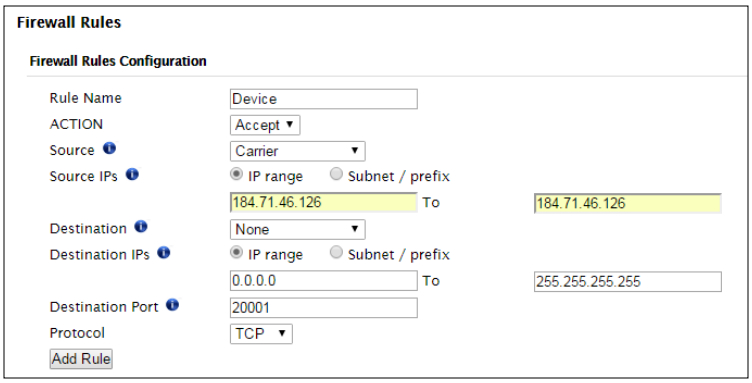
Étape 2

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).

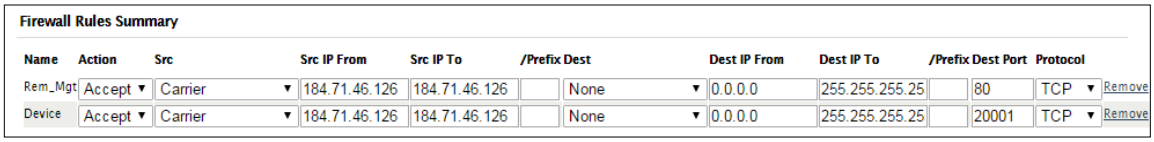
Règle 1



Règle 2



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.



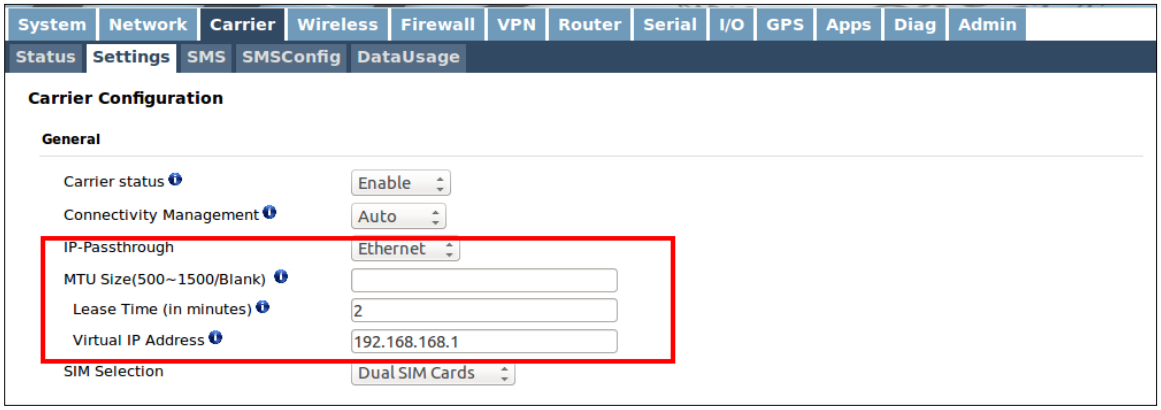
Étape 3

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.

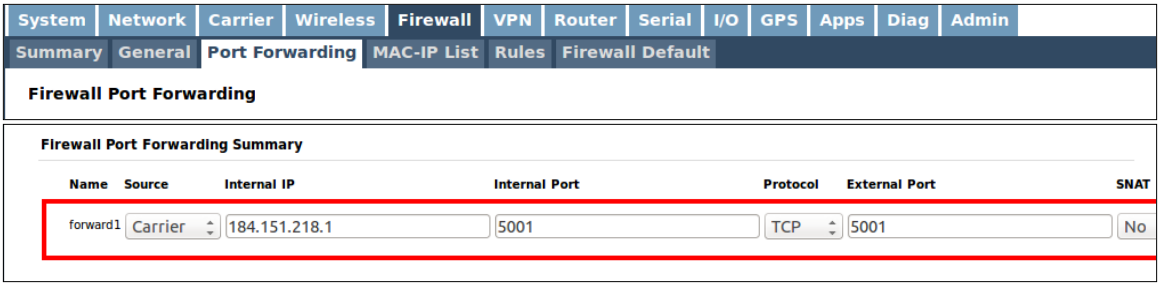
Étape 1: Activer IP-Passthrough



Après le mode pass-through IP est activé, l'adresse IP du réseau LAN est changé en 184.151.218.1

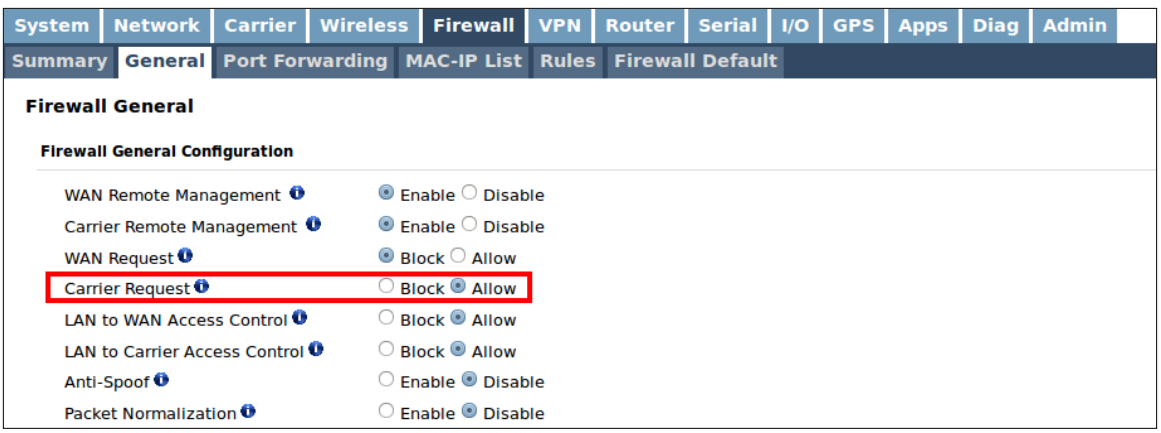
Étape 2. Ajouter Port Forwarding

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.



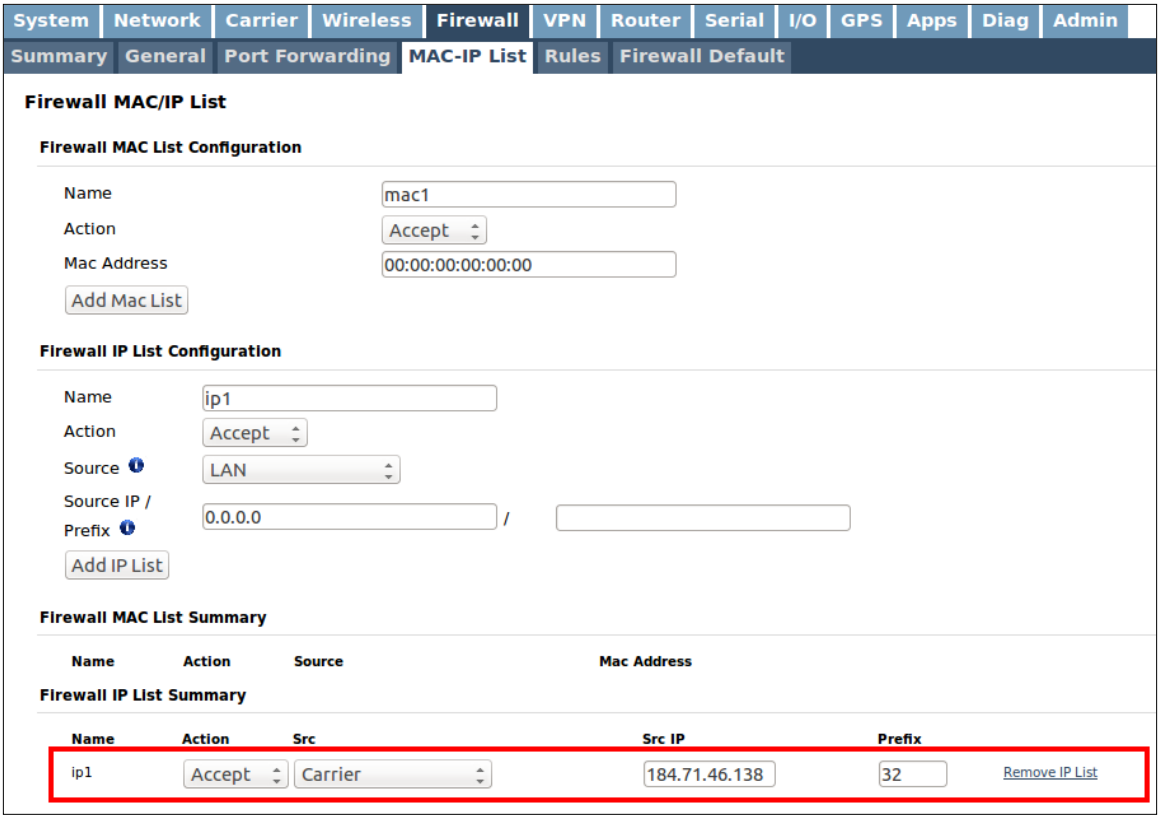
Utilisez l'adresse IP de l'interface LAN que IP interne du serveur.

B) Autoriser le trafic entrant. Méthode 1: Autoriser tout le trafic entrant sur le support. (Non recommandé)



Annexe F: Port Forwarding with IP-Passthrough (Page 2 de 2)

Méthode 2: Spécifiez la source Adresses IP sont autorisés.



La requête entrante sur le port 5001 du transporteur ne transmettra pas à l'appareil derrière le modem, le serveur Iperf 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 pare-feu?

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.

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

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