SIEMENS

RUGGEDCOM ROS v4.3

Guide d'utilisation

Pour RS900GP

Avant-propos

Introduction 1

Utilisation de ROS 2

Gestion de l'appareil 3

Administration système 4

Installation et configuration 5

Dépannage 6

08/2017

RC1277-FR-05

Copyright © 2018 Siemens Canada Ltd

Tous droits réservés. La diffusion ou la reproduction du présent document, ou l'évaluation et la communication de son contenu, n'est pas autorisée sauf en cas de permission expresse. Toute violation donnera lieu à des poursuites pour dommages et intérêts. Tous droits réservés, notamment aux fins de la demande de brevets ou de l'enregistrement de marques.

Ce document contient des informations propriétaires protégées par copyright. Tous les droits sont réservés. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans l'autorisation écrite préalable de Siemens Canada Ltd.

Exclusion de responsabilité

Siemens a vérifié la conformité du contenu du présent document avec le matériel et/ou le logiciel qui y sont décrits. Toutefois, il peut y avoir des écarts entre le produit et la documentation.

Siemens ne saurait être tenu pour responsable des erreurs ou omissions dans ce document, ni des dommages indirects qui pourraient découler de la fourniture, l'efficacité ou l'utilisation de ce document.

Les informations indiquées dans cette publication sont révisées régulièrement et toutes les corrections nécessaires seront apportées dans les prochaines éditions. Toutes les suggestions d'amélioration sont les bienvenues. Nous nous réservons le droit d'apporter des améliorations techniques sans préavis.

Marques déposées

RUGGEDCOM™ et ROS™ sont des marques déposées de Siemens Canada Ltd.

Les autres noms cités dans ce manuel peuvent être des marques commerciales dont l'utilisation par un tiers à des fins propres peut avoir pour conséquence d'enfreindre les droits de ceux qui les détiennent.

Copyrights de tiers

Siemens reconnaît les copyrights des tiers suivants :

- Copyright © 2004 GoAhead Logiciels, Inc. Tous droits réservés.

Logiciels ouverts

RUGGEDCOM ROS contient un logiciel ouvert. Concernant les conditions de licence, voir le document *Conditions de licence* correspondant.

Notes relatives à la sécurité

Siemens commercialise des produits et solutions comprenant des fonctions de sécurité industrielle qui contribuent à une exploitation sûre des installations, machines, équipements et/ou réseaux. Ces fonctions jouent un rôle important dans un système global de sécurité industrielle. Dans cette optique, Siemens développe ses produits et solutions en continu. Siemens vous recommande donc vivement de vous tenir régulièrement informé des mises à jour des produits.

Pour garantir une exploitation fiable des produits et solutions Siemens, il est nécessaire de prendre des mesures préventives adéquates (par ex. concept de protection des cellules) et d'intégrer chaque composant dans un système de sécurité industrielle global et moderne. Tout produit tiers utilisé devra également être pris en considération. Pour plus d'informations sur la sécurité industrielle, rendez-vous sur https://www.siemens.com/industrialsecurity.

Abonnez-vous à la newsletter d'un produit particulier afin d'être informé des mises à jour dès qu'elles apparaissent. Pour de plus amples informations, visitez https://support.automation.siemens.com.

Garantie

Reportez-vous au Contrat de licence pour les conditions générales de garantie applicables, le cas échéant.

Pour obtenir des précisions sur la garantie, veuillez vous rendre sur https://www.siemens.com/ruggedcom ou contactez un représentant du service client de Siemens.

Contacter Siemens

Adresse
Siemens Canada Ltd
Secteur Industry
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Téléphone
Sans frais : 1 888 264 0006
Tél : +1 905 856 5288
Fax : +1 905 856 1995

E-mail
ruggedcom.info.i-ia@siemens.com

Site Web
https://www.siemens.com/ruggedcom

Table des matières

Avant-propos xiii
Conventions xiii
Documents connexes xiv
Configuration requise xv
Accès à la documentation xv
Formation xv
Assistance client xv

Chapitre 1
Introduction 1
1.1 Fonctionnalités et avantages 1
1.2 Recommandations relatives à la sécurité 3
1.3 Normes réseau prises en charge 6
1.4 Schéma de numérotation de ports 6
1.5 Services disponibles par port 7
1.6 Prise en charge de Management Interface Base (MIB) SNMP 8
1.6.1 MIB standard prises en charge 8
1.6.2 MIB RUGGEDCOM propriétaires prises en charge 9
1.6.3 Fonctionnalités d'agent prises en charge 10
1.7 Traps SNMP 11
1.8 Prise en charge de la gestion de ModBus 12
1.8.1 Codes de fonction Modbus 12
1.8.2 Mappage de la mémoire ModBus 13
1.8.3 Formats de mémoire Modbus 21
1.8.3.1 Texte 21
1.8.3.2 Cmd 21
1.8.3.3 Uint16 22
1.8.3.4 Uint32 22
1.8.3.5 PortCmd 22
1.8.3.6 Alarme 23
1.8.3.7 PSStatusCmd 23
1.8.3.8 TruthValues 24

Chapitre 2
Utilisation de ROS 25
2.1 Connexion à ROS 25
2.1.1 Connexion directe 25
2.1.2 Connexion via le réseau 26
2.2 Ouverture de session 27
2.3 Fermeture de session 28
2.4 Utilisation de l'interface Web 29
2.5 Utilisation de l'interface de console 30
2.6 Utilisation de l'interface de ligne de commande 32
2.6.1 Commandes CLI disponibles 32
2.6.2 Traçage d'événements 36
2.6.3 Exécution distante de commandes via RSH 37
2.6.4 Utilisation de commandes SQL 38
2.6.4.1 Recherche du tableau correct 38
2.6.4.2 Récupération d'informations 39
2.6.4.3 Modification de valeurs dans un tableau 40
2.6.4.4 Réinitialisation d'un tableau 41
2.6.4.5 Utilisation de RSH et SQL 41
2.7 Sélection de ports dans RUGGEDCOM ROS 41
2.8 Gestion du système de fichiers flash 42
2.8.1 Affichage d'une liste de fichiers Flash 42
2.8.2 Affichage de détails de fichier Flash 42
2.8.3 Défragmentation du système de fichiers flash 43
2.9 Accès en mode BIST 43

Chapitre 3
Gestion de l'appareil 45
3.1 Affichage d'informations produit 45
3.2 Affichage de diagnostics de la CPU 47
3.3 Restauration des valeurs par défaut 48
3.4 Gestion des clés et certificats SSH et SSL 49
3.4.1 Certificats SSL 51
3.4.2 Clé d'hôte SSH 52
3.4.3 Gestion de clés publiques SSH 54
3.4.3.1 Exigences en matière de clés publiques 54
3.4.3.2 Ajout d'une clé publique 55
3.4.3.3 Affichage d'une liste de clés publiques 56
3.4.3.4 Mise à jour d'une clé publique 56
3.4.3.5 Suppression d'une clé publique 57

3.4.4 Exemples de certificats et de clés ... 57
3.5 Chargement/téléchargement de fichiers ... 58
3.5.1 Chargement/téléchargement de fichiers à l'aide de XMODEM ... 59
3.5.2 Chargement/téléchargement de fichiers à l'aide d'un client TFTP ... 60
3.5.3 Chargement/téléchargement de fichiers à l'aide d'un serveur TFTP ... 61
3.5.4 Chargement/téléchargement de fichiers à l'aide d'un serveur SFTP ... 61
3.6 Gestion de journaux ... 62
3.6.1 Affichage de journaux locaux et système ... 62
3.6.2 Effacement de journaux locaux et système ... 63
3.6.3 Configuration du journal système local ... 63
3.6.4 Gestion de la journalisation distante ... 64
3.6.4.1 Configuration du client Syslog distant ... 64
3.6.4.2 Affichage d'une liste de serveurs Syslog distants ... 65
3.6.4.3 Ajout d'un serveur Syslog distant ... 66
3.6.4.4 Suppression d'un serveur Syslog distant ... 67
3.7 Gestion de ports Ethernet ... 68
3.7.1 Protection du contrôleur via l'indication de défaillance de liaison (Link Fault Indication, LFI) ... 69
3.7.2 Visualisation de l'état de ports Ethernet ... 70
3.7.3 Affichage des statistiques pour tous les ports Ethernet ... 71
3.7.4 Affichage de statistiques pour des ports Ethernet spécifiques ... 72
3.7.5 Effacement de statistiques pour des ports Ethernet spécifiques ... 74
3.7.6 Configuration d'un port Ethernet ... 75
3.7.7 Configuration de la limitation du débit de port ... 78
3.7.8 Configuration de la mise en miroir de ports ... 80
3.7.9 Configuration de la détection de liaison ... 81
3.7.10 Gestion d'émetteurs-récepteurs SFP ... 83
3.7.10.1 Configuration d'un port SFP ... 83
3.7.10.2 Surveillance d'un port SFP ... 84
3.7.10.3 Affichage d'informations pour un port SFP ... 85
3.7.11 Gestion des ports PoE ... 85
3.7.11.1 Configuration globale de ports PoE ... 86
3.7.11.2 Configuration d'un port PoE spécifique ... 87
3.7.11.3 Planification de ports PoE ... 89
3.7.12 Détection de défauts de câble ... 91
3.7.12.1 Affichage des résultats de diagnostics de câbles ... 91
3.7.12.2 Exécution de diagnostics de câble ... 93
3.7.12.3 Effacement de diagnostics de câble ... 95
3.7.12.4 Détermination de la distance estimée au défaut (Estimated Distance To Fault (DTF)) ... 95
3.7.13 Réinitialisation de ports Ethernet ... 96
3.8 Gestion d'interfaces IP ... 96

3.8.1 Affichage d'une liste d'interfaces IP de ... 97
3.8.2 Ajout d'une interface IP ... 97
3.8.3 Suppression d'une interface IP ... 99
3.9 Gestion de passerelles IP ... 100
3.9.1 Affichage d'une liste de passerelles IP ... 100
3.9.2 Ajout d'une passerelle IP ... 101
3.9.3 Suppression d'une passerelle IP ... 102
3.10 Configuration des services IP ... 103
3.11 Gestion de la surveillance à distance ... 105
3.11.1 Gestion des RMON History Controls ... 106
3.11.1.1 Affichage d'une liste de contrôles d'historique RMON ... 106
3.11.1.2 Ajout d'un contrôle d'historique RMON ... 106
3.11.1.3 Suppression d'un contrôle d'historique RMON ... 108
3.11.2 Gestion des alarmes RMON ... 109
3.11.2.1 Affichage d'une liste d'alarmes RMON ... 110
3.11.2.2 Ajout d'une alarme RMON ... 111
3.11.2.3 Suppression d'une alarme RMON ... 113
3.11.3 Gestion des événements RMON ... 114
3.11.3.1 Affichage d'une liste d'événements RMON ... 115
3.11.3.2 Ajout d'un événement RMON ... 115
3.11.3.3 Suppression d'un événement RMON ... 117
3.12 Chargement/téléchargement du firmware ... 118
3.12.1 Mise à niveau du firmware ... 118
3.12.2 Rétrogradage du firmware ... 119
3.13 Réinitialisation de l'appareil ... 120
3.14 Désactivation de l'appareil ... 120

Chapitre 4
Administration système ... 123
4.1 Configuration du système d'information ... 123
4.2 Personnalisation de l'écran d'ouverture de session ... 124
4.3 Gestion des mots de passe ... 124
4.3.1 Configuration de mots de passe ... 125
4.3.2 Réinitialisation de mots de passe ... 128
4.4 Effacement de données privées ... 128
4.5 Activation/désactivation de l'interface Web ... 129
4.6 Gestion des alarmes ... 129
4.6.1 Affichage d'une liste d'alarmes préconfigurées ... 130
4.6.2 Affichage et effacement d'alarmes verrouillées ... 131
4.6.3 Configuration d'une alarme ... 131
4.6.4 Alarmes de sécurité liées à l'authentification ... 134

4.6.4.1 Alarmes de sécurité pour l'authentification de connexions 134
4.6.4.2 Messages de sécurité pour l'authentification de ports 136
4.7 Gestion du fichier de configuration 137
4.7.1 Configuration du chiffrage des données 137
4.7.2 Mise à jour du fichier de configuration 139
4.8 Gestion d'un serveur d'authentification 139
4.8.1 Configuration d'extensions de nom d'utilisateur 140
4.8.2 Gestion de l'authentification RADIUS 141
4.8.2.1 Configuration de l'authentification RADIUS 141
4.8.2.2 Configuration du serveur RADIUS 142
4.8.2.3 Configuration du client RADIUS sur l'appareil 143
4.8.3 Gestion de l'authentification TACACS+ 144
4.8.3.1 Configuration de TACACS+ 144
4.8.3.2 Configuration de droits d'utilisateur 146

Chapitre 5
Installation et configuration 149
5.1 Gestion de VLAN virtuels 149
5.1.1 Concepts VLAN 150
5.1.1.1 Trames balisées contre trames non balisées 150
5.1.1.2 VLAN natif 151
5.1.1.3 Le VLAN de gestion 151
5.1.1.4 Types de port périphérie et trunk 151
5.1.1.5 Règles d'entrée et de sortie 152
5.1.1.6 Liste Forbidden Ports 152
5.1.1.7 Modes compatible VLAN et non-compatible VLAN 152
5.1.1.8 GARP VLAN Registration Protocol (GVRP) 153
5.1.1.9 Périphérie PVLAN 155
5.1.1.10 QinQ 155
5.1.1.11 Avantages du VLAN 156
5.1.2 Affichage d'une liste de VLAN 158
5.1.3 Configuration globale de VLAN 158
5.1.4 Configuration de VLAN pour des ports Ethernet spécifiques 159
5.1.5 Gestion de VLAN statiques 162
5.1.5.1 Affichage d'une liste d'adresses VLAN statiques 162
5.1.5.2 Ajout d'un VLAN statique 162
5.1.5.3 Suppression d'un VLAN statique 164
5.2 Gestion du Spanning Tree Protocol 165
5.2.1 Fonctionnement RSTP 166
5.2.1.1 États et rôles RSTP 166
5.2.1.2 Ports de périphérie 168

5.2.1.3 Liaisons point à point et multipoint ... 169
5.2.1.4 Chemin et coûts de port ... 169
5.2.1.5 Diamètre de pont ... 170
5.2.1.6 eRSTP ... 170
5.2.1.7 Fast Root Failover ... 171
5.2.2 Applications RSTP ... 172
5.2.2.1 RSTP dans des configurations de câblage structuré ... 172
5.2.2.2 RSTP dans des configurations de structure en anneau ... 174
5.2.2.3 Redondance des ports RSTP ... 176
5.2.3 Opérations MSTP ... 176
5.2.3.1 Régions MSTP et interopérabilité ... 177
5.2.3.2 Rôles de pont et port MSTP ... 178
5.2.3.3 Avantages de MSTP ... 179
5.2.3.4 Mise en œuvre de MSTP sur un réseau ponté ... 180
5.2.4 Configuration globale du STP ... 181
5.2.5 Configuration du STP pour des ports Ethernet spécifiques ... 183
5.2.6 Configuration d'eRSTP ... 185
5.2.7 Affichage de statistiques globales concernant STP ... 187
5.2.8 Affichage de statistiques STP pour des ports Ethernet ... 189
5.2.9 Gestion de Multiple Spanning Tree Instances ... 191
5.2.9.1 Affichage des statistiques pour des MSTI globales ... 191
5.2.9.2 Affichage des statistiques pour des MSTI de ports ... 192
5.2.9.3 Configuration de l'identificateur de région MST ... 193
5.2.9.4 Configuration d'une MSTI globale ... 194
5.2.9.5 Configuration d'une MSTI pour un port Ethernet ... 195
5.2.10 Effacement de statistiques de protocole Spanning Tree ... 197
5.3 Gestion des classes de service ... 198
5.3.1 Configuration globale de classes de service ... 199
5.3.2 Configuration de classes de service pour des ports Ethernet spécifiques ... 199
5.3.3 Configuration de la priorité pour le mappage CoS ... 201
5.3.4 Configuration du mappage DSCP sur CoS ... 202
5.4 Gestion des adresses MAC ... 203
5.4.1 Affichage d'une liste d'adresses MAC ... 203
5.4.2 Configuration des options d'apprentissage d'adresses MAC ... 204
5.4.3 Configuration des options d'avalanche d'adresses MAC ... 205
5.4.4 Gestion des adresses MAC statiques ... 207
5.4.4.1 Affichage d'une liste d'adresses MAC statiques ... 207
5.4.4.2 Ajout d'une adresse MAC statique ... 207
5.4.4.3 Suppression d'une adresse MAC statique ... 209
5.4.5 Purge de toutes les adresses MAC dynamiques ... 210

5.5 Gestion des services de temps ... 210
5.5.1 Configuration de la date et de l'heure ... 211
5.5.2 Gestion de NTP ... 212
5.5.2.1 Activation/désactivation du service NTP ... 212
5.5.2.2 Configuration de serveurs NTP ... 213
5.6 Gestion de SNMP ... 214
5.6.1 Gestion des utilisateurs SNMP ... 215
5.6.1.1 Affichage d'une liste d'utilisateurs SNMP ... 215
5.6.1.2 Ajout d'un utilisateur SNMP ... 216
5.6.1.3 Suppression d'un utilisateur SNMP ... 218
5.6.2 Gestion du mappage sécurité sur groupe ... 220
5.6.2.1 Affichage d'une liste de mappages sécurité sur groupe ... 220
5.6.2.2 Ajout d'un mappage sécurité sur groupe ... 220
5.6.2.3 Suppression d'un mappage sécurité sur groupe ... 222
5.6.3 Gestion de groupes SNMP ... 222
5.6.3.1 Affichage d'une liste de groupes SNMP ... 223
5.6.3.2 Ajout d'un groupe SNMP ... 223
5.6.3.3 Suppression d'un groupe SNMP ... 225
5.7 Gestion de la découverte de réseau ... 226
5.7.1 Activation/désactivation du RCDP ... 226
5.7.2 LLDP (Link Layer Discovery Protocol) ... 227
5.7.2.1 Configuration globale du LLDP ... 228
5.7.2.2 Configuration de LLDP pour un port Ethernet ... 229
5.7.2.3 Affichage de statistiques globales et d'informations système annoncées ... 230
5.7.2.4 Affichage des statistiques pour des voisins LLDP ... 231
5.7.2.5 Affichage des statistiques pour des ports LLDP ... 232
5.8 Gestion du filtrage de multidiffusion ... 234
5.8.1 Gestion d'IGMP ... 234
5.8.1.1 Concepts IGMP ... 234
5.8.1.2 Affichage d'une liste d'appartenances à des groupes de multidiffusion ... 238
5.8.1.3 Affichage d'informations de transmission pour des groupes de multidiffusion ... 239
5.8.1.4 Configuration d'IGMP ... 240
5.8.2 Gestion de GMRP ... 241
5.8.2.1 Concepts GMRP ... 242
5.8.2.2 Affichage d'un résumé de groupes de multidiffusion ... 244
5.8.2.3 Configuration globale du GMRP ... 245
5.8.2.4 Configuration de GMRP pour des ports Ethernet spécifiques ... 246
5.8.2.5 Affichage d'une liste de groupes de multidiffusion statiques ... 247
5.8.2.6 Ajout d'un groupe multidiffusion statique ... 247
5.8.2.7 Suppression d'un groupe de multidiffusion statique ... 249

5.9 Gestion du DHCP Relay Agent (agent de relais DHCP) 250
5.9.1 Configuration du DHCP Relay Agent (agent de relais DHCP) 250
5.9.2 Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques 251
5.10 Gestion de la sécurité des ports (Port security) 252
5.10.1 Concept de sécurité de port 253
5.10.1.1 Authentification basée sur des adresses MAC statiques 253
5.10.1.2 Authentification IEEE 802.1X. 253
5.10.1.3 Authentification IEEE 802.1X avec authentification basée sur l'adresse MAC 254
5.10.1.4 Affectation de VLAN avec attributs Tunnel 255
5.10.2 Affichage d'une liste d'adresses MAC autorisées 255
5.10.3 Configuration de la sécurité du port 256
5.10.4 Configuration d'IEEE 802.1X 258
5.11 Gestion de l'agrégation de liaisons 260
5.11.1 Concepts d'agrégation de liaisons 261
5.11.1.1 Règles et limitations 261
5.11.1.2 Agrégation de liaisons et fonctionnalités de couche 2 262
5.11.1.3 Agrégation de liaisons et fonctionnalités de couche physique 262
5.11.2 Gestion d'agrégations de ports 263
5.11.2.1 Affichage d'une liste d'agrégations de ports 263
5.11.2.2 Ajout d'une agrégation de ports 263
5.11.2.3 Suppression d'une agrégation de ports 265

Chapitre 6
Dépannage 267
6.1 Généralités 267
6.2 Ports Ethernet 268
6.3 Spanning Tree 268
6.4 VLAN 270

Avant-propos

Ce guide décrit la version v4.3 de ROS (Rugged Operating System) sur le RUGGEDCOM RS900GP. Il contient des instructions et des directives sur la manière d'utiliser le logiciel, ainsi que des théories générales.

Il est destiné au personnel d'assistance technique réseau familiarisé avec le fonctionnement des réseaux. Son utilisation est également recommandée aux planificateurs réseau et système, programmeurs système et techniciens de lignes électriques.

IMPORTANT !
Certains paramètres et certaines options décrits ici peuvent ne pas être disponibles en fonction des variations dans le matériel de l'appareil. Même si nous mettons tout en œuvre pour décrire avec précision les paramètres et options disponibles spécifiques, le présent guide doit être utilisé en accompagnement des textes d'aide inclus dans le logiciel.

SOMMAIRE

- "Conventions"
- "Documents connexes"
- "Configuration requise"
- "Accès à la documentation"
- "Formation"
- "Assistance client"

Conventions

CeGuide d'utilisation utilise les conventions suivantes pour présenter les informations de manière claire et efficace.

Alertes

Les types d'alertes suivants sont utilisés pour mettre en évidence certaines informations importantes en cas de besoin.

DANGER !
Les alertes DANGER indiquent des situations à danger imminent qui, si elles ne sont pas évitées, entraîneront la mort ou des blessures graves.

AVERTISSEMENT !
Les alertes AVERTISSEMENT indiquent des situations dangereuses qui, si elles ne sont pas évitées, peuvent entraîner des blessures graves et/ou un endommagement du matériel.

ATTENTION !
Les alertes ATTENTION indiquent des situations dangereuses qui, si elles ne sont pas évitées, peuvent entraîner un endommagement du matériel.

IMPORTANT !
Les alertes IMPORTANT fournissent des informations importantes qu'il faut connaître avant d'exécuter une procédure ou une étape ou avant d'utiliser une fonction.

REMARQUE
Les alertes REMARQUE fournissent des informations supplémentaires telles que des données, des conseils et des détails.

Syntaxe de commande CLI

La syntaxe des commandes utilisées dans une CLI (Command Line Interface, interface de ligne de commande) est décrite en fonction des conventions suivantes :

Exemple	Description
command	Les commandes sont en gras.
command parameter	Les paramètres sont en texte clair.
command parameter1 parameter2	Les paramètres sont énumérés dans l'ordre dans lequel ils doivent être entrés.
command parameter1 *parameter2*	Les paramètres en italique doivent être remplacés par une valeur définie par l'utilisateur.
command [parameter1 | parameter2]	Les paramètres alternatifs sont séparés par une barre verticale (|). Des crochets indiquent un choix nécessaire entre deux paramètres ou plus.
command { parameter3 | parameter4 }	Des accolades indiquent des paramètres optionnels.
command parameter1 parameter2 { parameter3 | parameter4 }	Toutes les commandes et tous les paramètres sont présentés dans l'ordre dans lequel ils doivent être entrés.

Documents connexes

D'autres documents peuvent présenter un intérêt, notamment :

- *Guide d'installation RUGGEDCOM RS900GP*
- *Release Notes RUGGEDCOM ROS v4.3*

La plupart des documents sont disponibles sur le portail Industry Online Support [https://support.industry.siemens.com] ou l'application mobile de Siemens. Pour tous les autres, contactez un représentant commercial Siemens ou l'assistance client Siemens.

Configuration requise

Chaque poste de travail utilisé pour se connecter à l'interface RUGGEDCOM ROS doit avoir la configuration requise suivante :

- L'un des navigateurs Web suivants doit être installé :
  - Microsoft Internet Explorer 8.0 (ou plus récent)
  - Mozilla Firefox
  - Google Chrome
  - Iceweasel/IceCat (Linux uniquement)
- Une interface de travail en état de fonctionnement doit être disponible avec au moins l'un des types de port sur l'appareil RUGGEDCOM
- Le système doit avoir la possibilité de configurer une adresse IP et un masque de réseau sur l'interface Ethernet de l'ordinateur

Accès à la documentation

La documentation utilisateur la plus récente pour RUGGEDCOM ROS version 4.3 est disponible en ligne sur https://www.siemens.com/ruggedcom. Pour toute demande ou renseignement à propos d'un document utilisateur, contactez l'Assistance client Siemens.

Formation

Siemens propose une large gamme de services de formation, allant de la formation en entreprise avec différents cours standard sur le fonctionnement en réseau et les commutateurs et routeurs Ethernet, aux cours personnalisés sur site adaptés aux besoins du client, à son expérience et à son application.

L'équipe des services de formation de Siemens se donne pour objectif de transmettre à nos clients les compétences pratiques essentielles pour garantir que les utilisateurs disposent du savoir et de l'expertise appropriés pour comprendre les différentes technologies associées aux technologies d'infrastructures réseau critiques.

L'association inédite réalisée par Siemens d'une expertise en informatique/télécommunications et d'une connaissance des secteurs de la fourniture d'électricité, des transports et de l'industrie permet à Siemens de proposer une formation spécifique à l'application de chaque client.

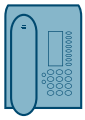
Pour plus d'informations sur les services de formation et les disponibilités des cours, rendez-vous sur https://www.siemens.com/ruggedcom ou contactez un représentant commercial Siemens.

Assistance client

L'assistance client est disponible 24 heures sur 24, 7 jours sur 7, pour tous les clients Siemens. Pour bénéficier de l'assistance technique ou obtenir des informations d'ordre général, contactez l'Assistance client Siemens par l'un des moyens suivants :

En ligne

Consultez la page http://www.siemens.com/automation/support-request pour envoyer une demande d'assistance (Support Request, SR) ou contrôler l'état d'une demande SR existante.



Téléphone

Appelez l'un de nos centres d'appel pour y déposer une demande d'assistance (SR). Pour localiser un centre d'appel local, consultez la page http://www.automation.siemens.com/mcms/aspa-db/fr/automatismes/Pages/default.aspx.

Appli mobile

Installez l'appli Industry Online Support de Siemens AG sur n'importe quel appareil mobile fonctionnant sous Android, Apple iOS ou Windows et :

- Accédez à toute la bibliothèque de documentation d'aide de Siemens, y compris aux FAQ et manuels
- Transmettez une demande SR ou vérifiez l'état d'une SR existante.
- Contactez un représentant local de Siemens pour les ventes, l'assistance technique, la formation, etc.
- Posez des questions ou partagez vos connaissances avec d'autres clients Siemens et la communauté de l'assistance client

1 Introduction

Bienvenue dans le Guide d'utilisation du logiciel RUGGEDCOM ROS v4.3 pour les appareils RUGGEDCOM RS900GP. Ce guide décrit la large gamme de fonctionnalités de type transporteur disponibles avec RUGGEDCOM ROS (Rugged Operating System).

Ce chapitre fournit une vue d'ensemble du logiciel RUGGEDCOM ROS.

SOMMAIRE

- Section 1.1, « Fonctionnalités et avantages »
- Section 1.2, « Recommandations relatives à la sécurité »
- Section 1.3, « Normes réseau prises en charge »
- Section 1.4, « Schéma de numérotation de ports »
- Section 1.5, « Services disponibles par port »
- Section 1.6, « Prise en charge de Management Interface Base (MIB) SNMP »
- Section 1.7, « Traps SNMP »
- Section 1.8, « Prise en charge de la gestion de ModBus »

Section 1.1

Fonctionnalités et avantages

La présente rubrique décrit les nombreuses fonctionnalités disponibles dans RUGGEDCOM ROS et leurs avantages :

- **Fonctionnalités de cyber-sécurité**
  La cyber-sécurité est une question centrale dans de nombreux secteurs industriels dans lesquels des réseaux d'automatisation et de communication avancés jouent un rôle crucial dans des applications critiques et où une fiabilité élevée est d'une importance capitale. Les fonctionnalités RUGGEDCOM ROS clés traitant les problèmes de sécurité au niveau du réseau local sont entre autres :

Mots de passe	Mots de passe utilisateur à plusieurs niveaux pour empêcher une configuration non autorisée
SSH/SSL	Étend la capacité de protection par mot de passe pour ajouter un chiffrement des mots de passe et des données rencontrées sur le réseau
Activation/désactivation de ports	Capacité de désactiver des ports dans lesquels le trafic ne peut pas passer
802.1Q VLAN	Fournit la capacité d'isoler logiquement le trafic entre des ports prédéfinis sur des commutateurs
SNMPv3	Authentification chiffrée et sécurisation d'accès
HTTPS	Pour sécuriser l'accès à l'interface Web.

- **eRSTP (Enhanced Rapid Spanning Tree Protocol)™**
  L'eRSTP de Siemens permet la création de réseaux en anneau en en maillage Ethernet résistants aux erreurs comprenant des liaisons redondantes *réduites* pour éviter les boucles. eRSTP met en œuvre STP et RSTP pour rendre possible l'interopérabilité avec des commutateurs du commerce, à la différence des solutions en *anneau* propriétaires. La fonctionnalité Fast Root Failover d'eRSTP fournit une convergence de réseau rapide en cas de défaillance d'un port racine RSTP dans une topologie en maillage.
- **Quality of Service (IEEE 802.1p)**
  Certaines applications de mise en réseau telles que le contrôle en temps réel ou VoIP (Voice over IP) requièrent des temps d'arrivée prévisibles pour les trames Ethernet. Les commutateurs peuvent introduire une latence en cas de trafic réseau intense en raison de files d'attente internes qui mettent en tampon des trames et transmettent ensuite sur la base du premier arrivé, premier servi. RUGGEDCOM ROS prend en charge la *classe de service*, qui permet au trafic à délai critique de passer en haut de la file d'attente, ce qui diminue la latence et réduit la *gigue* pour permettre à de telles applications exigeantes de fonctionner correctement. RUGGEDCOM ROS permet une classification de priorité par port, variable, adresse MAC et type de service (ToS) IP. Un algorithme de files d'attente pondérées équitables (*weighted fair queuing*) configurable contrôle la manière dont les trames sont vidées des files d'attente.
- **VLAN (IEEE 802.1Q)**
  Les réseaux locaux virtuels (VLAN) permettent l'isolement d'un réseau physique dans différents réseaux logiques avec des domaines de diffusion indépendants. Une mesure de sécurité est fournie car les hôtes peuvent uniquement accéder à d'autres hôtes sur le même VLAN et les tempêtes de trafic sont isolées. RUGGEDCOM ROS prend en charge les trames Ethernet balisées 802.1Q et les agrégations de VLAN. La classification basée sur les ports permet d'affecter des appareils hérités aux VLAN corrects. La prise en charge de GVRP est également fournie de manière à simplifier la configuration des commutateurs sur le VLAN.
- **SNMP (Simple Network Management Protocol)**
  SNMP fournit une méthode standardisée pour les stations de gestion de réseau d'interrogation d'appareils de différents fournisseurs. Les versions SNMP prises en charge par RUGGEDCOM ROS sont v1, v2c et v3. SNMPv3 en particulier fournit des fonctionnalités de sécurité (telles que l'authentification, la confidentialité et le contrôle d'accès) non présentes dans des versions antérieures de SNMP. RUGGEDCOM ROS prend également en charge de nombreuses MIB (Management Information Base) qui permettent une intégration facile dans tout système de gestion de réseau (Network Management System, NMS). Une fonctionnalité de SNMP est la capacité de générer des *traps* en cas d'événements système. RUGGEDCOM NMS, la solution de gestion Siemens, peut enregistrer des traps de plusieurs appareils, ce qui en fait un outil de dépannage de réseau efficace. Il fournit également une visualisation graphique du réseau et est entièrement intégré dans tous les produits Siemens.
- **Surveillance et configuration à distance avec RUGGEDCOM NMS**
  RUGGEDCOM NMS (RNMS) est le logiciel Network Management System de Siemens pour la découverte, la surveillance et la gestion de produits RUGGEDCOM et d'autres appareils compatibles IP sur un réseau. Ce produit hautement configurable complet enregistre et signale la disponibilité et la performance de composants et services réseau. Les défaillances d'appareil, de réseau et de service sont détectées et signalées rapidement pour réduire les temps d'arrêt.

  RNMS est particulièrement adapté pour la surveillance et la configuration à distance de routeurs RUGGEDCOM, d'interrupteurs, de serveurs série et d'équipement réseau sans fil WiMAX. Pour plus d'informations, contactez un représentant commercial Siemens.
- **NTP (Network Time Protocol)**
  NTP synchronise automatiquement l'horloge interne de tous les appareils RUGGEDCOM ROS sur le réseau. Ceci permet une corrélation des événements horodatés pour le dépannage.
- **Limitation du débit de port**
  RUGGEDCOM ROS prend en charge la limitation du débit configurable par port pour le trafic de monodiffusion et multidiffusion. Ceci peut être essentiel pour la gestion de la largeur de bande de réseau importante pour les prestataires de service. Il fournit également une sécurité de pointe en cas d'attaque de déni de service (DoS).

- **Filtrage de tempêtes de diffusion**
  Les tempêtes de diffusion peuvent endommager un réseau et entraîner un mauvais fonctionnement des appareils attachés. Cela peut être désastreux sur un réseau avec un équipement critique. RUGGEDCOM ROS limite ces conséquences en filtrant la diffusion de trames avec un seuil défini par l'utilisateur.
- **Agrégation de liaisons**
  Les ports Ethernet peuvent être agrégés dans une liaison logique unique statiquement ou dynamiquement pour agrandir la largeur de bande et équilibrer la charge de trafic.
- **Mise en miroir de ports**
  RUGGEDCOM ROS peut être configurer de manière à dupliquer tout le trafic sur un port vers un port miroir désigné. Combinée avec un analyseur de réseau, la mise en miroir peut être un outil de dépannage puissant.
- **Configuration et état du port**
  RUGGEDCOM ROS permet à des ports individuels d'être configurés de manière *fixe* pour la vitesse, le duplex, la négociation, le contrôle de flux, etc. Cela permet une connexion correcte à des appareils qui ne négocient pas ou ont des réglages inhabituels. L'état détaillé de ports avec alarme et trap SNMP pour des problèmes de liaison aide beaucoup pour le dépannage du système.
- **Statistiques de port et RMON (surveillance à distance, Remote Monitoring)**
  RUGGEDCOM ROS fournit une mise à jour continue des statistiques par port qui fournit des paquets d'entrée et de sortie, des compteurs d'octets et des chiffres d'erreur.

  Les statistiques RMON sont également entièrement prises en charge. RMON permet une collecte de données, une analyse et une détection de schémas de trafic sophistiquées.
- **Filtrage multidiffusion**
  RUGGEDCOM ROS prend en charge les groupes de multidiffusion statiques et la capacité de joindre ou de quitter des groupes de multidiffusion dynamiquement à l'aide d'IGMP (Internet Group Management Protocol) ou de GMRP (GARP Multicast Registration Protocol).
- **Journalisation des événements et alarmes**
  RUGGEDCOM ROS enregistre tous les événements significatifs dans un journal système non volatile permettant un dépannage légal. Les événements sont entre autres les défaillances et récupérations de liaison, l'accès non autorisé, la détection de tempêtes et les autodiagnostics. Les alarmes fournissent un instantané d'événements récents qui doivent encore être acquittés par l'administrateur réseau. Un relais matériel externe est mis hors tension en présence d'alarmes critiques, ce qui permet à un contrôleur externe de réagir le cas échéant.
- **Interface utilisateur de navigateur Web HTML**
  RUGGEDCOM ROS fournit une interface utilisateur simple et intuitive pour la configuration et la surveillance via un navigateur Web graphique standard ou via une interface utilisateur telcom standard. Tous les paramètres système ont une aide en ligne détaillée pour faciliter la configuration. RUGGEDCOM ROS a un aspect commun et un processus de configuration standardisé, ce qui permet une migration aisée vers d'autres produits RUGGEDCOM managés.
- **Prévention des attaques par force brute**
  La protection contre les attaques par force brute (BFAs) est intégrée par défaut dans RUGGEDCOM ROS. Si un hôte externe n'est pas en mesure de se connecter au terminal ou à des interfaces Web après un nombre de tentatives déterminé, le service est bloqué pendant une heure.

Section 1.2

Recommandations relatives à la sécurité

Tenez compte des recommandations relatives à la sécurité suivantes pour éviter un accès non autorisé à l'appareil :

Authentification

- Remplacez le mot de passe par défaut pour tous les comptes et processus utilisateur (le cas échéant) avant le déploiement de l'appareil.
- Utilisez des mots de passe forts avec randomisation élevée (c'est-à-dire entropie) sans répétition de caractères. Évitez les mots de passe faibles comme *password1*, *123456789*, *abcdefgh* et tout mot du dictionnaire ou nom propre dans quelque combinaison que ce soit. Pour plus d'informations sur la création de mots de passe forts, voir les conditions requises pour les mots de passe dans Section 4.3.1, « Configuration de mots de passe ».
- Assurez-vous que les mots de passe sont protégés et ne sont pas partagés avec des personnes non autorisées.
- Les mots de passe ne doivent pas être utilisés pour différents noms d'utilisateur et systèmes ou quand ils ont expiré.
- Si l'authentification RADIUS est effectuée à distance, assurez-vous que toutes les communications se trouvent dans le périmètre de sécurité ou sur une voie sécurisée.
- Générez et mettez en œuvre un certificat SSL et une paire de clés hôtes SSH personnalisées avant de mettre l'appareil en service. Pour plus d'informations, voir Section 3.4, « Gestion des clés et certificats SSH et SSL ».
- Utilisez une authentification avec clé publique SSH. Pour plus d'informations, voir Section 3.4, « Gestion des clés et certificats SSH et SSL ».

Accès physique/à distance

- Ne connectez pas l'appareil à Internet. Ne déployez l'appareil que dans un périmètre de réseau sécurisé.
- Limitez l'accès physique à l'appareil à un personnel autorisé uniquement. Une personne malveillante pourrait extraire des informations sensibles telles que des certificats, des clés, etc. (les mots de passe utilisateur sont protégés par un code de hachage) ou reprogrammer l'appareil.
- Contrôlez l'accès à la console série dans la même mesure que l'accès physique à l'appareil. L'accès à la console série permet un accès potentiel au chargeur de démarrage RUGGEDCOM ROS, qui comprend des outils pouvant être utilisés pour obtenir un accès complet à l'appareil.
- N'activez que des services qui seront utilisés sur l'appareil, notamment des ports physiques. Les ports physiques non utilisés peuvent être potentiellement utilisés pour obtenir un accès au réseau sous-jacent à l'appareil.
- Si SNMP est activé, limitez le nombre d'adresses IP pouvant se connecter à l'appareil et modifiez les noms de communauté. Configurez également SNMP de manière à générer un trap en cas d'échec d'authentification. Pour plus d'informations, voir Section 5.6, « Gestion de SNMP ».
- Évitez d'utiliser des services non sécurisés tels que Telnet et TFTP, ou désactivez-les complètement si possible. Ces services sont disponibles pour des raisons historiques et sont désactivés par défaut.
- Limitez le nombre de sessions serveur Web, Telnet et SSH simultanées autorisées.
- Configurez la journalisation système à distance de manière à ce que les journaux soient transmis à un emplacement central. Pour plus d'informations, voir Section 3.6, « Gestion de journaux ».
- Des fichiers de configuration sont fournis au format CSV (valeurs séparées par des virgules) pour une plus grande facilité d'utilisation. Assurez-vous que les fichiers de configuration sont protégés correctement lorsqu'ils se trouvent en-dehors de l'appareil. Par exemple, chiffrez les fichiers, stockez-les dans un emplacement sécurisé et ne les transmettez pas via des voies de communication non sécurisées.
- La gestion des fichiers de configuration, des certificats et des clés relève de la responsabilité du propriétaire de l'appareil. Envisagez l'utilisation de tailles de clés RSA de 2 048 bits de longueur au minimum et de certificats signés avec SHA256 pour un chiffrement optimal. Avant d'envoyer l'appareil à Siemens pour réparation, assurez-vous que le chiffrement est désactivé (pour créer une version en texte clair du fichier de configuration) et remplacez les certificats et les clés actuels avec des certificats et des clés " *jetables*" temporaires qui peuvent être détruits au retour de l'appareil.

- Sachez quels protocoles non sécurisés sont activés sur l'appareil. Certains protocoles (comme HTTPS et SSH) sont sécurisés, alors que d'autres (HTTPS et SSH) n'ont pas été conçus à cette fin. Une protection appropriée doit être développée pour les protocoles non sécurisés afin d'éviter un accès non autorisé à l'appareil/au réseau.
- Configurez les fonctionnalités de sécurité des ports sur les ports d'accès pour éviter une connexion physique à l'appareil par un tiers non autorisé. Pour plus d'informations, voir Section 5.10, « Gestion de la sécurité des ports (Port security) ».

Matériel/logiciel

- Assurez-vous que la version actuelle du firmware est installée, notamment tous les correctifs liés à la sécurité. Pour obtenir les informations actuelles sur les correctifs de sécurité pour les produits Siemens, consultez lesite Web Industrial Security [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] ou lesite Web d'avis de sécurité ProductCERT [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Des mises à jour des avis de sécurité pour les produits Siemens sont disponible via une inscription au flux RSS sur le site Web Siemens d'avis de sécurité ProductCERT ou en suivant @ProductCert sur Twitter.
- Activez BPDU Guard sur des ports où des BPDU RSTP ne sont pas attendues.
- Utilisez la dernière version de navigateur Web compatible avec RUGGEDCOM ROS pour vous assurer que les versions et chiffrements de TLS (Transport Layer Security) les plus sécurisés disponibles sont utilisés. De plus, le fractionnement d'enregistrements 1/n-1 est activé dans les dernières versions des navigateurs Web Mozilla Firefox, Google Chrome et Internet Explorer. Il limite les risques d'attaques BEAST (SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability) pour les versions non contrôlées (Non-Controlled (NC)) de RUGGEDCOM ROS.
- Modbus peut être désactivé si l'utilisateur n'en a pas besoin. Si l'activation de ModBus est requise, il est recommandé de suivre les recommandations de sécurité figurant dans le présent Guide d'utilisation et de configurer l'environnement en fonction des meilleurs pratiques de défense en profondeur.
- Éviter d'accéder à des pages Web externes non fiables lorsque vous accédez à l'appareil via un navigateur Web. De cette manière, vous pouvez éviter des menaces de sécurité potentielles, notamment un détournement de session.
- Pour une sécurité optimale, utilisez SNMPv3 si possible. Utilisez des clés d'authentification et des clés privées fortes sans chaînes répétitives (par ex. *abc* ou *abcabc*) avec cette fonctionnalité. Pour plus d'informations sur la création de mots de passe forts, voir les conditions requises pour les mots de passe dans Section 4.3.1, « Configuration de mots de passe ».
- À moins d'être nécessaire pour une topologie de réseau particulière, le réglage *IP Forward* doit être défini sur `Disabled` pour éviter le routage de paquets.

> **REMARQUE**
> *Pour des raisons de compatibilité de configuration, le réglage configuré n'est pas modifié en cas de mises à niveau depuis des versions de RUGGEDCOM ROS antérieures à v4.2.0 à la version v4.2.0 ou ultérieure. Ce réglage est toujours activé et ne peut pas être configuré sur des versions antérieures à v4.2.0. Pour les nouvelles unités avec version de firmware v4.2.0 ou ultérieure, ce réglage est configurable et désactivé par défaut.*

Stratégie

- Auditez périodiquement l'appareil pour vous assurer qu'il est conforme avec ces recommandations et/ou toute stratégie de sécurité interne.
- Consultez la documentation utilisateur d'autres produits Siemens utilisés en combinaison avec l'appareil pour des recommandations de sécurité détaillées.

Section 1.3

Normes réseau prises en charge

Les normes de réseau suivantes sont prises en charge par RUGGEDCOM ROS :

Norme	Ports 10 Mbit/s	Ports 100 Mbit/s	Ports 1 000 Mb/s	Remarques
IEEE 802.3x	✓	✓	✓	Fonctionnement en duplex intégral
IEEE 802.3z			✓	1000Base-LX
IEEE 802.3ab			✓	1000Base-Tx
IEEE 802.1D	✓	✓	✓	Ponts MAC
IEEE 802.1Q	✓	✓	✓	VLAN (Virtual LAN)
IEEE 802.1p	✓	✓	✓	Niveaux de priorité

Section 1.4

Schéma de numérotation de ports

Pour une identification rapide, un numéro est affecté à chaque port sur un appareil RUGGEDCOM RS900GP. Tous les numéros de port sont sérigraphiés sur l'appareil.

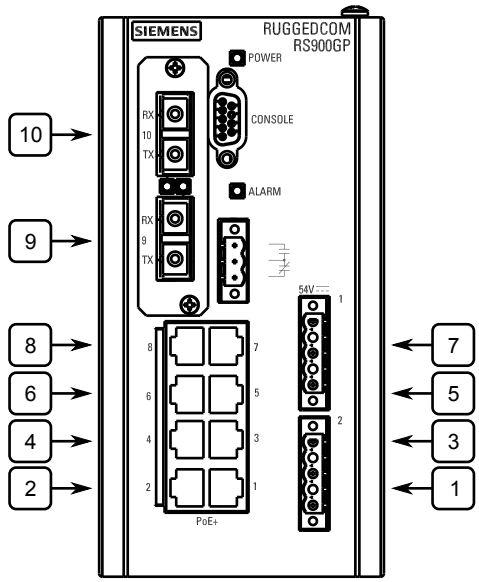


Figure 1 : Numérotation de ports RUGGEDCOM RS900GP (typique)

Utilisez ces numéros pour configurer des fonctionnalités applicables à des ports donnés.

Section 1.5

Services disponibles par port

Le tableau suivant récapitule les services disponibles sous RUGGEDCOM ROS. Ce tableau comprend les informations suivantes :

- **Services**
  Les services pris en charge par l'appareil.
- **Numéro de port**
  Le numéro de port associé au service.
- **Port ouvert**
  L'état du port, qu'il soit toujours ouvert sans pouvoir être fermé ou uniquement ouvert avec possibilité de configuration.

> **REMARQUE**
> *Dans certains cas, le service peut être désactivé, mais le port peut toujours être ouvert (par ex. TFTP).*

- **Port par défaut**
  L'état par défaut du port (c'est-à-dire ouvert ou fermé).
- **Accès autorisé**
  Indique si les ports/services sont authentifiés pendant l'accès.

Services	Numéro de port	Service activé/désactivé	Accès autorisé	Remarque
Telnet	TCP/23	Désactivé	Oui	Disponible uniquement via des interfaces de gestion.
HTTP	TCP/80	Activé (configurable), redirection vers 443	—	
HTTPS	TCP/443	Activé (configurable)	Oui	
RSH	TCP/514	Désactivé (configurable)	Oui	Disponible uniquement via des interfaces de gestion.
TFTP	UDP/69	Désactivé (configurable)	Non	Disponible uniquement via des interfaces de gestion.
SFTP	TCP/22	Activé	Oui	Disponible uniquement via des interfaces de gestion.
SNMP	UDP/161	Désactivé (configurable)	Oui	Disponible uniquement via des interfaces de gestion.
SNTP	UDP/123	Activé (configurable)	Non	Disponible uniquement via des interfaces de gestion.
SSH	TCP/22	Activé	Oui	Disponible uniquement via des interfaces de gestion.
ICMP	—	Activé	Non	
TACACS+	TCP/49 (configurable)	Désactivé (configurable)	Oui	

Services	Numéro de port	Service activé/désactivé	Accès autorisé	Remarque
RADIUS	UDP/1812 pour envoyer (configurable), ouvre un port quelconque à écouter	Désactivé (configurable)	Oui	Disponible uniquement via des interfaces de gestion.
Syslog distant	UDP/514 (configurable)	Désactivé (configurable)	Non	Disponible uniquement via des interfaces de gestion.
TCP Modbus (serveur)	TCP/502	Désactivé (configurable)	Non	Disponible uniquement via des interfaces de gestion.
TCP Modbus (commutateur)	TCP/502	Désactivé (configurable)	Non	
DHCP, agent DHCP	UDP/67, 68 envoi de message si activé - en cas de réception, arrive toujours sur la CPU, abandonné si le service n'est pas configuré	Désactivé (configurable)	Non	
RCDP	—	Activé (configurable)	Oui	

Section 1.6

Prise en charge de Management Interface Base (MIB) SNMP

RUGGEDCOM ROS prend en charge une large gamme de MIB standard, de MIB RUGGEDCOM propriétaires et de MIB de fonctionnalités d'agent, toutes pour SNMP (Simple Network Management Protocol).

SOMMAIRE

- Section 1.6.1, « MIB standard prises en charge »
- Section 1.6.2, « MIB RUGGEDCOM propriétaires prises en charge »
- Section 1.6.3, « Fonctionnalités d'agent prises en charge »

Section 1.6.1

MIB standard prises en charge

RUGGEDCOM ROS prend en charge les MIB standard suivantes :

Norme	Nom de MIB	Titre
RFC 2578	SNMPv2-SMI	Structure of Management Information Version 2
RFC 2579	SNMPv2-TC	Textual conventions for SMIv2
RFC 2580	SNMPv2-CONF	Conformance statements for SMIv2

Norme	Nom de MIB	Titre
	IANAifType	Enumerated values of the ifType Object Defined ifTable defined in IF-MIB
RFC 1907	SNMPv2-MIB	Management Information Base for SNMPv2
RFC 2011	IP-MIB	SNMPv2 Management Information Base for Internet Protocol using SMIv2
RFC 2012	TCP-MIB	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	UDP-MIB	Management Information Base for the UDP using SMIv2
RFC 1659	RS-232-MIB	Definitions of managed objects for RS-232-like hardware devices
RFC 2863	IF-MIB	The Interface Group MIB
RFC 2819	RMON-MIB	Remote Network Monitoring (RMON) management Information base
RFC 4188	BRIDGE-MIB	Definitions of managed objects for bridges
RFC 4318	RSTP-MIB	Definitions of managed objects for bridges with Rapid Spanning Tree Protocol (RSTP)
RFC 3411	SNMPAMEWORK-MIB	An architecture for describing Simple Network Management Protocol (SNMP) Management Framework
RFC 3414	SNMP-USER-BASED-SM-MIB	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	SNMP-VIEW-BASED-ACM-MIB	View-based Access Control Model (VACM) for the Simple Management Protocol (SNMP)
IEEE 802.3ad	IEEE8023-LAG-MIB	Management Information Base Module for link aggregation
IEEE 802.1AB-2005	LLDP-MIB	Management Information Base Module for LLDP configuration, statistics, local system data and remote systems data components
RFC 4363	Q-BRIDGE-MIB	Definitions of Managed Objects for Bridges with traffic classes, filtrage de multidiffusion, and virtual LAN extensions

Section 1.6.2

MIB RUGGEDCOM propriétaires prises en charge

RUGGEDCOM ROS prend en charge les MIB RUGGEDCOM propriétaires suivantes :

Nom de fichier	Nom de MIB	Description
RUGGEDCOM-MIB.mib	RUGGEDCOM-MIB	SMI d'entreprise RUGGEDCOM
RUGGEDCOM-TRAPS-MIB.mib	RUGGEDCOM-TRAPS-MIB	Définition de traps RUGGEDCOM
RUGGEDCOM-SYS-INFO-MIB.mib	RUGGEDCOM-SYS-INFO-MIB	Informations système générales à propos de l'appareil RUGGEDCOM
RUGGEDCOM-DOT11-MIB.mib	RUGGEDCOM-DOT11-MIB	Gestion d'interface sans fil sur un appareil RUGGEDCOM
RUGGEDCOM-POE-MIB.mib	RUGGEDCOM-POE-MIB	Gestion de ports PoE sur un appareil RUGGEDCOM

Nom de fichier	Nom de MIB	Description
RUGGEDCOM-SERIAL-MIB.mib	RUGGEDCOM-SERIAL-MIB	Gestion de ports série sur un appareil RUGGEDCOM
RUGGEDCOM-STP-MIB.mib	RUGGEDCOM-STP-MIB	Gestion du protocole RSTP
RUGGEDCOM-NTP-MIB.mib	RUGGEDCOM-NTP-MIB	MIB propriétaire RUGGEDCOM pour contrôler et surveiller le module NTP

Section 1.6.3

Fonctionnalités d'agent prises en charge

RUGGEDCOM ROS prend en charge les fonctionnalités d'agent suivantes pour l'agent SNMP :

REMARQUE
Pour plus d'informations sur les fonctionnalités d'agent pour SNMPv2, voir RFC 2580 [http://tools.ietf.org/html/rfc2580].

Nom de fichier	Nom de MIB	MIB prise en charge
RC-SNMPv2-MIB-AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
RC-UDP-MIB-AC.mib	RC-UDP-MIB-AC	UDP-MIB
RC-TCP-MIB-AC.mib	RC-TCP-MIB-AC	TCP-MIB
RC-SNMP-USER-BASED-SM-MIB-AC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
RC-SNMP-VIEW-BASED-ACM-MIB-AC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
RC-IF-MIB-AC.mib	RC-IF-MIB-AC	IF-MIB
RC-BRIDGE-MIB-AC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
RC-RMON-MIB-AC.mib	RC-RMON-MIB-AC	RMON-MIB
RC-Q-BRIDGE-MIB-AC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
RC-IP-MIB-AC.mib	RC-IP-MIB-AC	IP-MIB
RC-LLDP-MIB-AC.mib	RC-LLDP-MIB-AC	LLDP-MIB
RC-LAG-MIB-AC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
RC_RSTP-MIB-AC.mib	RC_RSTP-MIB-AC	RSTP-MIB
RC-RUGGEDCOM-DOT11-MIB-AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
RC-RUGGEDCOM-POE-MIB-AC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
RC-RUGGEDCOM-STP-AC-MIB.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
RC-RUGGEDCOM-SYS-INFO-MIB-AC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB
RC-RUGGEDCOM-TRAPS-MIB-AC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
RUGGEDCOM_RS-232-MIB-AC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
RC-RUGGEDCOM-SERIAL-MIB-AC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB
RC-NTP-MIB-AC.mib	RC-NTP-MIB-AC	NTP-MIB

Section 1.7

Traps SNMP

L'appareil génère les traps standard suivants :

Tableau : Traps standard

Trap	MIB
linkDown	IF-MIB
linkUp	
authenticationFailure	SNMPv2-MIB
coldStart	
newRoot	BRIDGE-MIB
topologyChage	
risingAlarm	RMON-MIB
fallingAlarm	
lldpRemoteTablesChange	LLDP-MIB

L'appareil génère également les traps propriétaires suivants :

Tableau : Traps propriétaires

Trap	MIB
genericTrap	RUGGEDCOM-TRAPS-MIB
powerSupplyTrap	
swUpgradeTrap	
cfgChangeTrap	
weakPasswordTrap	
defaultKeysTrap	

Les traps génériques comprennent des informations concernant les événements avec leur degré de gravité et leur description. Ils sont envoyés lorsqu'une alarme est générée pour l'appareil. Vous trouverez ci-après des exemples de traps RUGGEDCOM génériques :

REMARQUE
Les informations concernant les traps génériques peuvent être collectées à l'aide de la commande CLI **`alarms`**. *Pour plus d'informations sur la commande* **`alarms`**, *voir* *Section 2.6.1, « Commandes CLI disponibles »*.

Tableau : Traps génériques

Trap	Severity
heap error	Alerte
NTP server failure	Notification
real time clock failure	Erreur

Trap	Severity
failed password	Avertissement
MAC address not learned by switch fabric	Avertissement
BootP client: TFTP transfer failure	Erreur
received looped back BPDU	Erreur
received two consecutive confusing BPDUs on port, forcing down	Erreur
GVRP failed to learn – too many VLANs	Avertissement

L'appareil génère les traps suivants lorsque des événements spécifiques se produisent :

Tableau : Traps basés sur des événements

Trap	MIB	Evénement
rcRstpNewTopology	RUGGEDCOM-STP-MIB	Ce trap est généré lorsque la topologie d'appareil devient stable après une modification de topologie sur un port commutateur.
rcPoeOverheat	RUGGEDCOM-POE-MIB	Ce trap est généré par une condition de surchauffe PoE (Power over Ethernet).
rcPoeOverload		Ce trap est généré par une condition de surcharge PoE (Power over Ethernet).

Section 1.8

Prise en charge de la gestion de ModBus

La prise en charge de la gestion de ModBus dans les appareils RUGGEDCOM fournit une interface simple pour l'acquisition des informations d'état de base. La prise en charge de ModBus simplifie le travail des intégrateurs système SCADA (Supervisory Control and Data Acquisition) en fournissant des protocoles familiers pour l'acquisition d'informations d'appareils RUGGEDCOM. ModBus fournit surtout des informations d'état en lecture seule, mais il existe des registres accessibles en écriture pour les commandes opérateur.

Le format PDU (Protocol Data Unit) de protocole ModBus est le suivant :

Code de fonction	Données

SOMMAIRE

- Section 1.8.1, « Codes de fonction Modbus »
- Section 1.8.2, « Mappage de la mémoire ModBus »
- Section 1.8.3, « Formats de mémoire Modbus »

Section 1.8.1

Codes de fonction Modbus

Les appareils RUGGEDCOM prennent en charge les codes de fonction ModBus suivants pour la gestion des appareils via ModBus :

REMARQUE
Alors que les appareils RUGGEDCOM ont un nombre variable de ports, tous les registres et bits ne s'appliquent pas à tous les produits.

Les registres qui ne sont pas applicables à un appareil spécifique renvoient une valeur zéro (0). Par exemple, les registres se référant à des ports série ne sont pas applicables à des commutateurs RUGGEDCOM.

Lecture de registres d'entrée ou lecture de registres de maintien — 0x04 ou 0x03

Exemple de demande PDU

Code de fonction	1 octet	0x04(0x03)
Adresse de départ	2 octets	0x0000 à 0xFFFF (hexadécimal) 128 à 65535 (décimal)
Nombre de registres d'entrée	2 octets	Octets 0x0001 à 0x007D

Exemple de réponse PDU

Code de fonction	1 octet	0x04(0x03)
Comptage d'octets	1 octet	2 x N^a
Nombre de registres d'entrée	N^a x 2 octets	

[a] *Le nombre de registres d'entrée*

Écriture dans plusieurs registres — 0x10

Exemple de demande PDU

Code de fonction	1 octet	0x10
Adresse de départ	2 octets	0x0000 à 0xFFFF
Nombre de registres d'entrée	2 octets	Octets 0x0001 à 0x0079
Comptage d'octets	1 octet	2 x N^b
Valeur de registres	N^b x 2 octets	Valeurs du registre

[b] *Le nombre de registres d'entrée*

Exemple de réponse PDU

Code de fonction	1 octet	0x10
Adresse de départ	2 octets	0x0000 à 0xFFFF
Nombre de registres	2 octets	1 à 121 (0x79)

Section 1.8.2

Mappage de la mémoire ModBus

Vous trouverez ci-dessous une description détaillée de la manière dont les données de variables de process ModBus sont mappées.

Information produit

Les données suivantes ont été mappées sur le tableau *Productinfo* :

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0000	16	Identification du produit	L	Texte
0010	32	Identification du firmware	L	Texte
0040	1	Nombre de ports Ethernet	L	Uint16
0041	1	Nombre de ports série	L	Uint16
0042	1	Nombre d'alarmes	L	Uint16
0043	1	Power Supply Status	L	PSStatusCmd
0044	1	État du relais de sécurité	L	TruthValue
0045	1	État d'ErrorAlarm	L	TruthValue

Registre d'écriture de produit

Les données suivantes ont été mappées sur différents tableaux :

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0080	1	Effacer les alarmes	E	Cmd
0081	2	Réinitialiser les ports Ethernet	E	PortCmd
0083	2	Effacer les statistiques Ethernet	E	PortCmd
0085	2	Réinitialiser les ports série	E	PortCmd
0087	2	Clear Serial Port Statistics	E	PortCmd

Alarmes

Les données suivantes ont été mappées sur le tableau *Alarms* :

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0100	64	Alarm 1	L	Alarme
0140	64	Alarm 2	L	Alarme
0180	64	Alarm 3	L	Alarme
01C0	64	Alarm 4	L	Alarme
0200	64	Alarm 5	L	Alarme
0240	64	Alarm 6	L	Alarme
0280	64	Alarm 7	L	Alarme
02C0	64	Alarm 8	L	Alarme

État des ports Ethernet

Les données suivantes ont été mappées sur le tableau *ethPortStats* :

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
03FE	2	État de la liaison du port	L	PortCmd

Statistiques Ethernet

Les données suivantes ont été mappées sur le tableau *rmonStats* :

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0400	2	Statistiques du port s1/p1 - Paquets Ethernet entrants	L	Uinst32
0402	2	Statistiques du port s1/p2 - Paquets Ethernet entrants	L	Uinst32
0404	2	Statistiques du port s1/p3 - Paquets Ethernet entrants	L	Uinst32
0406	2	Statistiques du port s1/p4 - Paquets Ethernet entrants	L	Uinst32
0408	2	Statistiques du port s2/p1 - Paquets Ethernet entrants	L	Uinst32
040A	2	Statistiques du port s2/p2 - Paquets Ethernet entrants	L	Uinst32
040C	2	Statistiques du port s2/p3 - Paquets Ethernet entrants	L	Uinst32
040E	2	Statistiques du port s2/p4 - Paquets Ethernet entrants	L	Uinst32
0410	2	Statistiques du port s3/p1 - Paquets Ethernet entrants	L	Uinst32
0412	2	Statistiques du port s3/p2 - Paquets Ethernet entrants	L	Uinst32
0414	2	Statistiques du port s3/p3 - Paquets Ethernet entrants	L	Uinst32
0416	2	Statistiques du port s3/p4 - Paquets Ethernet entrants	L	Uinst32
0418	2	Statistiques du port s4/p1 - Paquets Ethernet entrants	L	Uinst32
041A	2	Statistiques du port s4/p2 - Paquets Ethernet entrants	L	Uinst32
041C	2	Statistiques du port s4/p3 - Paquets Ethernet entrants	L	Uinst32
041E	2	Statistiques du port s4/p4 - Paquets Ethernet entrants	L	Uinst32
0420	2	Statistiques du port s5/p1 - Paquets Ethernet entrants	L	Uinst32

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0422	2	Statistiques du port s5/p2 - Paquets Ethernet entrants	L	Uinst32
0424	2	Statistiques du port s5/p3 - Paquets Ethernet entrants	L	Uinst32
0426	2	Statistiques du port s5/p4 - Paquets Ethernet entrants	L	Uinst32
0428	2	Statistiques du port s6/p1 - Paquets Ethernet entrants	L	Uinst32
042A	2	Statistiques du port s6/p2 - Paquets Ethernet entrants	L	Uinst32
042C	2	Statistiques du port s6/p3 - Paquets Ethernet entrants	L	Uinst32
042E	2	Statistiques du port s6/p4 - Paquets Ethernet entrants	L	Uinst32
0430	2	Statistiques du port s7/p1 - Paquets Ethernet entrants	L	Uinst32
0432	2	Statistiques du port s7/p2 - Paquets Ethernet entrants	L	Uinst32
0434	2	Statistiques du port s8/p1 - Paquets Ethernet entrants	L	Uinst32
0436	2	Statistiques du port s8/p2 - Paquets Ethernet entrants	L	Uinst32
0440	2	Statistiques du port s1/p1 - Paquets Ethernet sortants	L	Uinst32
0442	2	Statistiques du port s1/p2 - Paquets Ethernet sortants	L	Uinst32
0444	2	Statistiques du port s1/p3 - Paquets Ethernet sortants	L	Uinst32
0446	2	Statistiques du port s1/p4 - Paquets Ethernet sortants	L	Uinst32
0448	2	Statistiques du port s2/p1 - Paquets Ethernet sortants	L	Uinst32
044A	2	Statistiques du port s2/p2 - Paquets Ethernet sortants	L	Uinst32
044C	2	Statistiques du port s2/p3 - Paquets Ethernet sortants	L	Uinst32
044E	2	Statistiques du port s2/p4 - Paquets Ethernet sortants	L	Uinst32
0450	2	Statistiques du port s3/p1 - Paquets Ethernet sortants	L	Uinst32
0452	2	Statistiques du port s3/p2 - Paquets Ethernet sortants	L	Uinst32
0454	2	Statistiques du port s3/p3 - Paquets Ethernet sortants	L	Uinst32

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0456	2	Statistiques du port s3/p4 - Paquets Ethernet sortants	L	Uinst32
0458	2	Statistiques du port s4/p1 - Paquets Ethernet sortants	L	Uinst32
045A	2	Statistiques du port s4/p2 - Paquets Ethernet sortants	L	Uinst32
045C	2	Statistiques du port s4/p3 - Paquets Ethernet sortants	L	Uinst32
045E	2	Statistiques du port s4/p4 - Paquets Ethernet sortants	L	Uinst32
0460	2	Statistiques du port s5/p1 - Paquets Ethernet sortants	L	Uinst32
0462	2	Statistiques du port s5/p2 - Paquets Ethernet sortants	L	Uinst32
0464	2	Statistiques du port s5/p3 - Paquets Ethernet sortants	L	Uinst32
0466	2	Statistiques du port s5/p4 - Paquets Ethernet sortants	L	Uinst32
0468	2	Statistiques du port s6/p1 - Paquets Ethernet sortants	L	Uinst32
046A	2	Statistiques du port s6/p2 - Paquets Ethernet sortants	L	Uinst32
046C	2	Statistiques du port s6/p3 - Paquets Ethernet sortants	L	Uinst32
046E	2	Statistiques du port s6/p4 - Paquets Ethernet sortants	L	Uinst32
0470	2	Statistiques du port s7/p1 - Paquets Ethernet sortants	L	Uinst32
0472	2	Statistiques du port s7/p2 - Paquets Ethernet sortants	L	Uinst32
0474	2	Statistiques du port s8/p1 - Paquets Ethernet sortants	L	Uinst32
0476	2	Statistiques du port s8/p2 - Paquets Ethernet sortants	L	Uinst32
0480	2	Statistiques du port s1/p1 - Paquets Ethernet entrants	L	Uinst32
0482	2	Statistiques du port s1/p2 - Paquets Ethernet entrants	L	Uinst32
0484	2	Statistiques du port s1/p3 - Paquets Ethernet entrants	L	Uinst32
0486	2	Statistiques du port s1/p4 - Paquets Ethernet entrants	L	Uinst32
0488	2	Statistiques du port s2/p1 - Paquets Ethernet entrants	L	Uinst32

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
048A	2	Statistiques du port s2/p2 - Paquets Ethernet entrants	L	Uinst32
048C	2	Statistiques du port s2/p3 - Paquets Ethernet entrants	L	Uinst32
048E	2	Statistiques du port s2/p4 - Paquets Ethernet entrants	L	Uinst32
0490	2	Statistiques du port s3/p1 - Paquets Ethernet entrants	L	Uinst32
0492	2	Statistiques du port s3/p2 - Paquets Ethernet entrants	L	Uinst32
0494	2	Statistiques du port s3/p3 - Paquets Ethernet entrants	L	Uinst32
0496	2	Statistiques du port s3/p4 - Paquets Ethernet entrants	L	Uinst32
0498	2	Statistiques du port s4/p1 - Paquets Ethernet entrants	L	Uinst32
049A	2	Statistiques du port s4/p2 - Paquets Ethernet entrants	L	Uinst32
049C	2	Statistiques du port s4/p3 - Paquets Ethernet entrants	L	Uinst32
049E	2	Statistiques du port s4/p4 - Paquets Ethernet entrants	L	Uinst32
04A0	2	Statistiques du port s5/p1 - Paquets Ethernet entrants	L	Uinst32
04A2	2	Statistiques du port s5/p2 - Paquets Ethernet entrants	L	Uinst32
04A4	2	Statistiques du port s5/p3 - Paquets Ethernet entrants	L	Uinst32
04A6	2	Statistiques du port s5/p4 - Paquets Ethernet entrants	L	Uinst32
04A8	2	Statistiques du port s6/p1 - Paquets Ethernet entrants	L	Uinst32
04AA	2	Statistiques du port s6/p2 - Paquets Ethernet entrants	L	Uinst32
04AC	2	Statistiques du port s6/p3 - Paquets Ethernet entrants	L	Uinst32
04AE	2	Statistiques du port s6/p4 - Paquets Ethernet entrants	L	Uinst32
04B0	2	Statistiques du port s7/p1 - Paquets Ethernet entrants	L	Uinst32
04B2	2	Statistiques du port s7/p2 - Paquets Ethernet entrants	L	Uinst32
04B4	2	Statistiques du port s8/p1 - Paquets Ethernet entrants	L	Uinst32

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
04B6	2	Statistiques du port s8/p2 - Paquets Ethernet entrants	L	Uinst32
04C0	2	Statistiques du port s1/p1 - Paquets Ethernet sortants	L	Uinst32
04C2	2	Statistiques du port s1/p2 - Paquets Ethernet sortants	L	Uinst32
04C4	2	Statistiques du port s1/p3 - Paquets Ethernet sortants	L	Uinst32
04C6	2	Statistiques du port s1/p4 - Paquets Ethernet sortants	L	Uinst32
04C8	2	Statistiques du port s2/p1 - Paquets Ethernet sortants	L	Uinst32
04CA	2	Statistiques du port s2/p2 - Paquets Ethernet sortants	L	Uinst32
04CC	2	Statistiques du port s2/p3 - Paquets Ethernet sortants	L	Uinst32
04CE	2	Statistiques du port s2/p4 - Paquets Ethernet sortants	L	Uinst32
04D0	2	Statistiques du port s3/p1 - Paquets Ethernet sortants	L	Uinst32
04D2	2	Statistiques du port s3/p2 - Paquets Ethernet sortants	L	Uinst32
04D4	2	Statistiques du port s3/p3 - Paquets Ethernet sortants	L	Uinst32
04D6	2	Statistiques du port s3/p4 - Paquets Ethernet sortants	L	Uinst32
04D8	2	Statistiques du port s4/p1 - Paquets Ethernet sortants	L	Uinst32
04DA	2	Statistiques du port s4/p2 - Paquets Ethernet sortants	L	Uinst32
04DC	2	Statistiques du port s4/p3 - Paquets Ethernet sortants	L	Uinst32
04DE	2	Statistiques du port s4/p4 - Paquets Ethernet sortants	L	Uinst32
04E0	2	Statistiques du port s5/p1 - Paquets Ethernet sortants	L	Uinst32
04E2	2	Statistiques du port s5/p2 - Paquets Ethernet sortants	L	Uinst32
04E4	2	Statistiques du port s5/p3 - Paquets Ethernet sortants	L	Uinst32
04E6	2	Statistiques du port s5/p4 - Paquets Ethernet sortants	L	Uinst32
04E8	2	Statistiques du port s6/p1 - Paquets Ethernet sortants	L	Uinst32

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
04EA	2	Statistiques du port s6/p2 - Paquets Ethernet sortants	L	Uinst32
04EC	2	Statistiques du port s6/p3 - Paquets Ethernet sortants	L	Uinst32
04EE	2	Statistiques du port s6/p4 - Paquets Ethernet sortants	L	Uinst32
04F0	2	Statistiques du port s7/p1 - Paquets Ethernet sortants	L	Uinst32
04F2	2	Statistiques du port s7/p2 - Paquets Ethernet sortants	L	Uinst32
04F4	2	Statistiques du port s8/p1 - Paquets Ethernet sortants	L	Uinst32
04F6	2	Statistiques du port s8/p2 - Paquets Ethernet sortants	L	Uinst32

Statistiques série

Les données suivantes ont été mappées sur le tableau *uartPortStatus* :

Adresse	Nombre de registres	Description (tableau Reference dans l'interface utilisateur)	L/E	Format
0600	2	Statistiques du port 1 – caractères série entrants	L	Uint32
0602	2	Statistiques du port 2 – caractères série entrants	L	Uint32
0604	2	Statistiques du port 3 – caractères série entrants	L	Uint32
0606	2	Statistiques du port 4 – caractères série entrants	L	Uint32
0640	2	Statistiques du port 1 – caractères série sortants	L	Uint32
0642	2	Statistiques du port 2 – caractères série sortants	L	Uint32
0644	2	Statistiques du port 3 – caractères série sortants	L	Uint32
0646	2	Statistiques du port 4 – caractères série sortants	L	Uint32
0680	2	Statistiques du port 1 – paquets série entrants	L	Uint32
0682	2	Statistiques du port 2 – paquets série entrants	L	Uint32
0684	2	Statistiques du port 3 – paquets série entrants	L	Uint32
0686	2	Statistiques du port 4 – paquets série entrants	L	Uint32
06C0	2	Statistiques du port 1 – paquets série sortants	L	Uint32
06C2	2	Statistiques du port 2 – paquets série sortants	L	Uint32
06C4	2	Statistiques du port 3 – paquets série sortants	L	Uint32
06C6	2	Statistiques du port 4 – paquets série sortants	L	Uint32

Section 1.8.3

Formats de mémoire Modbus

Cette section définit les formats de mémoire Modbus pris en charge par RUGGEDCOM ROS.

SOMMAIRE

- Section 1.8.3.1, « Texte »
- Section 1.8.3.2, « Cmd »
- Section 1.8.3.3, « Uint16 »
- Section 1.8.3.4, « Uint32 »
- Section 1.8.3.5, « PortCmd »
- Section 1.8.3.6, « Alarme »
- Section 1.8.3.7, « PSStatusCmd »
- Section 1.8.3.8, « TruthValues »

Section 1.8.3.1

Texte

Le format texte fournit une représentation ASCII simple des informations liées au produit. L'octet de poids fort du registre d'un caractère ASCII se trouve en première position.

Par exemple, une demande *de lecture de plusieurs registres* pour lire l'identification du produit depuis l'emplacement 0x0000.

0x04	0x00	0x00	0x00	0x08

La réponse peut être la suivante :

0x04	0x10	0x53	0x59	0x53	0x54	0x45	0x4D	0x20	0x4E	0x41	0x4D	0x45
0x00	0x00	0x00	0x00	0x00								

Dans cet exemple, en démarrant de l'octet 3 jusqu'à la fin, la réponse présente une représentation ASCII des caractères pour l'identification du produit, lue sous la forme de *SYSTEM NAME*. La longueur de ce champ étant inférieure à huit registres, le reste du champ est rempli avec des zéros (0).

Section 1.8.3.2

Cmd

Le format Cmd commande à l'appareil de définir la sortie sur *true* ou *false*. L'octet de poids fort prend la première place.

- Les demandes FF 00 hex sortent à l'état True
- Les demandes 00 00 hex sortent à l'état False
- Toute valeur autre que les valeurs suggérées n'affecte pas l'opération demandée

Par exemple, une demande *d'écriture de plusieurs registres* pour effacer les alarmes de l'appareil.

0x10	0x00	0x80	0x00	0x01	2	0xFF	0x00

- FF 00 pour le registre 00 80 efface les alarmes système
- 00 00 n'efface aucune alarme

La réponse peut être la suivante :

0x10	0x00	0x80	0x00	0x01

Section 1.8.3.3

Uint16

Le format Uint16 décrit un registre 16 bits Modbus standard.

Section 1.8.3.4

Uint32

Le format Uint32 décrit 2 registres 16 bits Modbus standard. Le premier registre comprend les 16 bits de poids fort d'une valeur 32 bits. Le second registre comprend les 16 bits de poids faible d'une valeur 32 bits.

Section 1.8.3.5

PortCmd

Le format PortCmd décrit un schéma de bits par port, où 1 indique que l'action requise est True et 0 indique que l'action requise est False.

PortCmd fournit un schéma de bits de 32 ports maximum. Par conséquent, il utilise deux registres Modbus :

- Le premier registre ModBus correspond aux ports 1 – 16
- Le second registre ModBus correspond aux ports 17 – 32 pour une action particulière

Les bits qui ne s'appliquent pas à un produit particulier sont toujours définis sur zéro (0).

Une valeur de bit de 1 indique que l'action demandée est True. Par exemple, le port est *up*.

Une valeur de bit de 0 indique que l'action demandée est False. Par exemple, le port est *down*.

Lecture de données à l'aide de PortCmd

Pour comprendre comment lire les données à l'aide de PortCmd, envisagez une demande ModBus pour lire plusieurs registres depuis l'emplacement 0x03FE.

0x04	0x03	0xFE	0x00	0x02

La réponse dépend du nombre de ports disponibles sur l'appareil. Par exemple, si le nombre maximum de ports sur un appareil RUGGEDCOM connecté est 20, la réponse peut être la suivante :

0x04	0x04	0xF2	0x76	0x00	0x05

Dans cet exemple, les octets 3 et 4 se réfèrent au registre 1 à l'emplacement 0x03FE et représentent l'état des ports 1 – 16. Les octets 5 et 6 se réfèrent au registre 2 à l'emplacement 0x03FF et représentent l'état des ports 17

– 32. L'appareil est doté de seulement 20 ports, l'octet 6 contient donc l'état des ports 17 – 20 de la droite vers la gauche. Le reste des octets dans le registre 2 correspondant aux ports 21 – 31 non existants ont la valeur zéro (0).

Exécution d'actions d'écriture à l'aide de PortCmd

Pour comprendre comment des données sont écrites à l'aide de PortCmd, envisagez une demande d'écriture de plusieurs registres pour effacer les statistiques de port Ethernet.

0x10	0x00	0x83	0x00	0x01	2	0x55	0x76	0x00	0x50

Une valeur de bit de 1 efface les statistiques Ethernet du port correspondant. Une valeur de bit de 0 n'efface pas les statistiques Ethernet.

0x10	0x00	0x81	0x00	0x02

Section 1.8.3.6

Alarme

Le format Alarme est une autre forme de description de texte. Le texte d'alarme correspond à la description d'alarme du tableau contenant toutes les alarmes. De manière similaire au format de texte, ce format renvoie une représentation ASCII des alarmes.

REMARQUE
Les alarmes sont empilées dans l'appareil dans l'ordre de leur occurrence (c'est-à-dire Alarm 1, Alarm 2, Alarm 3, etc.).

Les huit premières alarmes de la pile peuvent être renvoyées le cas échéant. Une valeur zéro (0) est renvoyée si aucune alarme n'existe.

Section 1.8.3.7

PSStatusCmd

Le format PSStatusCmd décrit un format de bits pour fournir l'état d'alimentations disponibles. Les bits 0-4 de l'octet de poids faible du registre sont utilisés à cet effet.

- Bits 0-1 : état de l'alimentation 1
- Bits 2-3 : état de l'alimentation 2

Les autres bits dans le registre ne fournissent aucune information d'état système.

Valeur des bits	Description
01	Aucune alimentation électrique n'est présente (01 = 1)
10	L'alimentation électrique est fonctionnelle (10 = 2)
11	L'alimentation électrique n'est pas fonctionnelle (11 = 3)

Les valeurs utilisées pour l'état de l'alimentation sont dérivées de la MIB SNMP spécifique à RUGGEDCOM.

Lecture de l'état de l'alimentation depuis un appareil à l'aide de PSStatusCmd

Pour comprendre comment lire l'état de l'alimentation à partir d'un appareil à l'aide de PortCmd, envisagez une demande ModBus pour lire plusieurs registres depuis l'emplacement 0x0043.

0x04	0x00	0x43	0x00	0x01

La réponse peut être la suivante :

0x04	0x02	0x00	0x0A

L'octet de poids faible du registre affiche l'état de l'alimentation. Dans cet exemple, les deux alimentations dans l'unité sont fonctionnelles.

Section 1.8.3.8

TruthValues

Le format TruthValues format représente un état True ou False dans l'appareil :

- 1 indique que l'état correspondant pour l'appareil est True
- 2 indique que l'état correspondant pour l'appareil est False

Lecture de l'état de relais de sécurité depuis un appareil à l'aide de TruthValue

Pour comprendre comment utiliser l'état du format TruthValue pour lire l'état de relais de sécurité à partir d'un appareil, envisagez une demande ModBus pour lire plusieurs registres depuis l'emplacement 0x0044.

0x04	0x00	0x44	0x00	0x01

La réponse peut être la suivante :

0x04	0x02	0x00	0x01

L'octet de poids faible du registre indique l'état du relais de sécurité. Dans cet exemple, le relais de sécurité est alimenté :

Lecture de l'état ErrorAlarm depuis un appareil à l'aide de TruthValue

Pour comprendre comment utiliser l'état du format TruthValue pour lire l'état ErrorAlarm à partir d'un appareil, envisagez une demande ModBus pour lire plusieurs registres depuis l'emplacement 0x0045.

0x04	0x00	0x45	0x00	0x01

La réponse peut être la suivante :

0x04	0x02	0x00	0x01

L'octet de poids faible du registre indique l'état ErrorAlarm. Dans cet exemple, il n'y a aucune alarme ERROR, ALERT ou CRITICAL dans l'appareil.

2 Utilisation de ROS

Ce chapitre explique comment utiliser RUGGEDCOM ROS.

SOMMAIRE

- Section 2.1, « Connexion à ROS »
- Section 2.2, « Ouverture de session »
- Section 2.3, « Fermeture de session »
- Section 2.4, « Utilisation de l'interface Web »
- Section 2.5, « Utilisation de l'interface de console »
- Section 2.6, « Utilisation de l'interface de ligne de commande »
- Section 2.7, « Sélection de ports dans RUGGEDCOM ROS »
- Section 2.8, « Gestion du système de fichiers flash »
- Section 2.9, « Accès en mode BIST »

Section 2.1

Connexion à ROS

Cette section décrit les différentes méthodes de connexion à l'appareil.

SOMMAIRE

- Section 2.1.1, « Connexion directe »
- Section 2.1.2, « Connexion via le réseau »

Section 2.1.1

Connexion directe

Il est possible d'accéder à RUGGEDCOM ROS via une connexion console série RS-232 directe à des fins de gestion et de dépannage. Une connexion à une console fournit un accès à l'interface de console et à la CLI.

Procédez comme suit pour établir une connexion de console à l'appareil :

1. Connectez un poste de travail (terminal ou ordinateur exécutant un logiciel d'émulation de terminaux) au port de la console série RS-232 sur l'appareil. Pour plus d'informations sur le port de la console série RS-232, voir le *Guide d'installation RS900GP*.

REMARQUE
La vitesse de transmission de l'appareil est imprimée sur l'extérieur du châssis près du port de la console série RS-232.

2. Configurez le poste de travail comme suit :
   - Vitesse (baud) : 57600
   - Bits de données : 8
   - Parité : aucune
   - Contrôle du flux : désactivé
   - ID de terminal : VT100
   - Bit d'arrêt : 1
3. Connectez-vous à l'appareil. Une fois la connexion établie, l'écran d'ouverture de session s'affiche. Pour plus d'informations sur la connexion à l'appareil, voir Section 2.2, « Ouverture de session ».

Section 2.1.2

Connexion via le réseau

Vous pouvez accéder à RUGGEDCOM ROS via le réseau avec un navigateur Web, un terminal ou un poste de travail exécutant un logiciel d'émulation de terminaux.

Utilisation d'un navigateur Web

Les navigateurs Web fournissent une connexion sécurisée à l'interface Web pour RUGGEDCOM ROS à l'aide de la méthode de communication SSL (Secure Socket Layer). SSL chiffre le trafic échangé avec ses clients.

Le serveur Web RUGGEDCOM ROS garantit que toutes les communications avec le client sont privées. Si un client demande un accès via un port HTTP non sécurisé, le client est automatiquement redirigé vers un port sécurisé. Un accès au serveur Web via SSL est autorisé uniquement aux clients qui fournissent un nom d'utilisateur et un mot de passe valides.

Procédez comme suit pour établir une connexion via un navigateur Web :

1. Sur le poste de travail utilisé pour accéder à l'appareil, configurez un port Ethernet de manière à utiliser une adresse IP au sein du sous-réseau de l'appareil. L'adresse IP par défaut est 192.168.0.1/24.

   Par exemple, pour configurer l'appareil de manière à établir une connexion à l'un des ports Ethernet disponibles, affectez une adresse IP au port Ethernet sur le poste de travail avec une plage de 192.168.0.3 à 192.168.0.254.
2. Ouvrez un navigateur Web Vous trouverez une liste des navigateurs Web recommandés sous “Configuration requise”.

IMPORTANT !
Lors de la connexion à l'appareil, certains navigateurs Web peuvent signaler que le certificat du serveur Web ne peut pas être vérifié par rapport à tout certificat connu. Ce comportement est attendu, et vous pouvez instruire le navigateur d'accepter le certificat en toute sécurité. Une fois le certificat accepté, toutes les communications avec le serveur Web via ce navigateur sont sécurisées.

3. Dans la barre d'adresse, saisissez l'adresse IP pour le port connecté au réseau. Par exemple, pour accéder à l'appareil avec son adresse IP par défaut, saisissez**`https://192.168.0.1`** et appuyez sur **Entrée**. Une fois la connexion établie, l'écran d'ouverture de session pour l'interface Web s'affiche.

   Pour plus d'informations sur la connexion à l'appareil, voir Section 2.2, « Ouverture de session ». Pour plus d'informations sur l'interface Web, voir Section 2.4, « Utilisation de l'interface Web ».

Utilisation d'un terminal ou d'un logiciel d'émulation de terminaux

Un terminal ou un ordinateur exécutant un logiciel d'émulation de terminaux fournit un accès à l'interface de console pour RUGGEDCOM ROS via Telnet, RSH (Remote Shell) ou SSH (Secure Shell).

> **REMARQUE**
> *Les services IP peuvent être limités pour contrôler l'accès à l'appareil. Pour plus d'informations, voir Section 3.10, « Configuration des services IP ».*

Procédez comme suit pour établir une connexion via un terminal ou un logiciel d'émulation de terminaux :

1. Sélectionnez le service (c'est-à-dire Telnet, RSH ou SSH).
2. Saisissez l'adresse IP pour le port connecté au réseau.
3. Connectez-vous à l'appareil. Une fois la connexion établie, l'écran d'ouverture de session s'affiche. Pour plus d'informations sur la connexion à l'appareil, voir Section 2.2, « Ouverture de session ».

Section 2.2

Ouverture de session

Procédez comme suit pour ouvrir une session sur l'appareil :

1. Connectez-vous à l'appareil directement ou via un navigateur Web. Pour plus d'informations sur la manière de se connecter à l'appareil, voir Section 2.1, « Connexion à ROS ».

   Une fois la connexion établie, l'écran d'ouverture de session s'affiche.

Figure 2 : Écran d'ouverture de session SSH (interface de console)

1. Zone User Name **2.** Zone Password

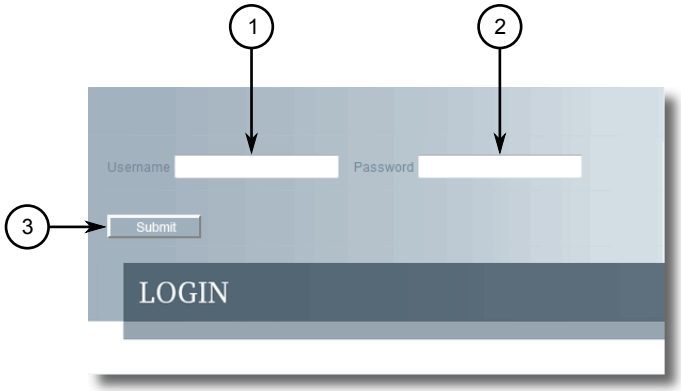


Figure 3 : Écran d'ouverture de session (interface web)

1. Zone Username **2.** Zone Password **3.** Bouton Submit

REMARQUE

Les noms d'utilisateur et mots de passe par défaut suivants sont définis sur l'appareil pour chaque type d'utilisateur :

Invité	***Opérateur***	***Administrateur***
User Name: guest	*User Name: operator*	*User Name: admin*
Password: guest	*Password: operator*	*Password: admin*

ATTENTION !

Pour éviter un accès non autorisé à l'appareil, assurez-vous de modifier les mots de passe par défaut pour les types d'utilisateur invité, opérateur et administrateur avant de mettre l'appareil en service.

Pour plus d'informations sur la modification de mots de passe, voir Section 4.3.1, « Configuration de mots de passe ».

2. Dans le champ**User Name**, saisissez le nom d'utilisateur pour un compte configuré sur l'appareil.
3. Dans le champ**Password**, saisissez le mot de passe pour le compte.
4. Cliquez sur **Entrée** ou sur **Submit** (interface Web uniquement).

Section 2.3

Fermeture de session

Pour fermer une session sur l'appareil, accédez à l'écran principal et procédez comme suit :

- Pour fermer une session sur la console ou des interfaces shell sécurisées, appuyez sur **CTRL** +**X**.
- Pour fermer une session sur l'interface Web, cliquez sur **Logout**.

Figure 4 : Interface Web (exemple)

1. Fermeture de session

REMARQUE
S'il existe des modifications de la configuration en attente qui n'ont pas encore été validées, RUGGEDCOM ROS demande confirmation avant de rejeter les modifications et de fermer la session sur l'appareil.

Section 2.4

Utilisation de l'interface Web

L'interface Web est une interface utilisateur graphique basée sur le Web permettant d'afficher des informations et des contrôles importants dans un navigateur Web. L'interface est divisée en trois cadres : la bannière, le menu et le cadre principal.

Figure 5 : Exemple de disposition de l'interface Web

1. Cadre supérieur **2.** Cadre latéral **3.** Cadre principal

Cadre	Description
Supérieur	Le cadre supérieur affiche le nom de système de l'appareil.
Latéral	Le cadre latéral contient une option de déconnexion et une liste réductible de liens ouvrant différents écrans dans le cadre principal. Pour plus d'informations sur le la déconnexion de RUGGEDCOM ROS, voir Section 2.3, « Fermeture de session ».
Principal	Le cadre principal affiche les paramètres et/ou les données liés à la fonctionnalité sélectionnée.

Chacun écran est composé d'un titre, du niveau d'accès de l'utilisateur, de paramètres et/ou données (sous forme de formulaire ou de tableau) et de contrôles (par exemple ajouter, supprimer, actualiser, etc.). Le titre donne accès à une aide contextuelle spécifique pour l'écran qui fournit des informations importantes concernant les paramètres et/ou données disponibles. Cliquez sur le lien pour ouvrir l'aide dans une nouvelle fenêtre.

Lorsqu'une alarme est générée, une notification d'alarme remplace le niveau d'accès actuel de l'utilisateur sur chaque écran jusqu'à ce que l'alarme soit résolue. La notification indique le nombre d'alarmes actuellement actives. Pour plus d'informations sur les alarmes, voir Section 4.6, « Gestion des alarmes ».

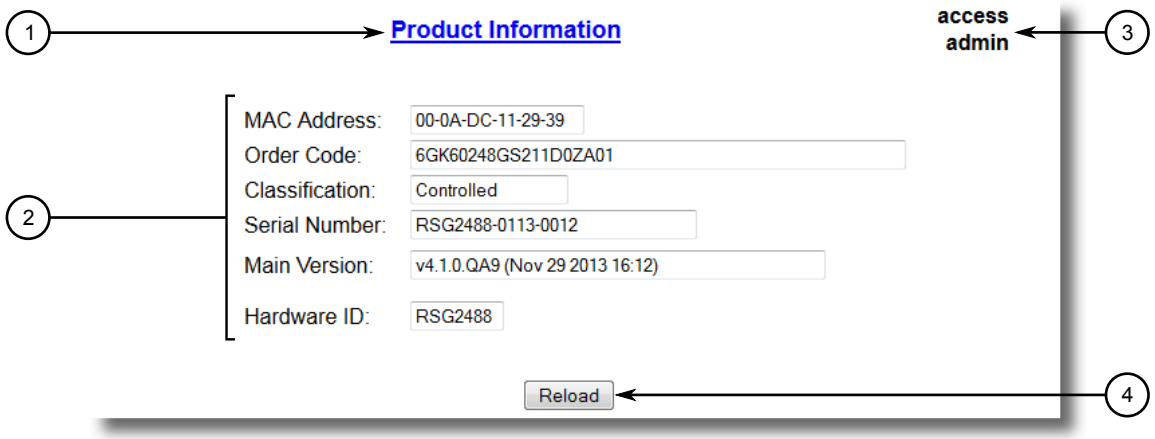


Figure 6 : Exemple d'éléments d'un écran typique

1. Titre **2.** Paramètres et/ou données **3.** Niveau d'accès ou notification d'alarme **4.** Contrôles

REMARQUE
Le cas échéant, l'interface Web peut être désactivée. Pour plus d'informations, voir Section 4.5, « Activation/désactivation de l'interface Web ».

Section 2.5

Utilisation de l'interface de console

L'interface de console est une interface utilisateur graphique organisée sous forme d'une série de menus. Elle est principalement accessible via la connexion de console série, mais est également accessible via des services IP, notamment une session Telnet, RSH (Remote Shell) et SSH (Secure Shell) ou l'exécution d'une commande SSH distante.

REMARQUE
Les services IP peuvent être limités pour contrôler l'accès à l'appareil. Pour plus d'informations, voir Section 3.10, « Configuration des services IP ».

Chaque écran est constitué d'un identificateur système, du nom du menu actuel et d'une barre de commandes. Des alarmes sont également affichées sur chaque écran dans le coin supérieur droit.

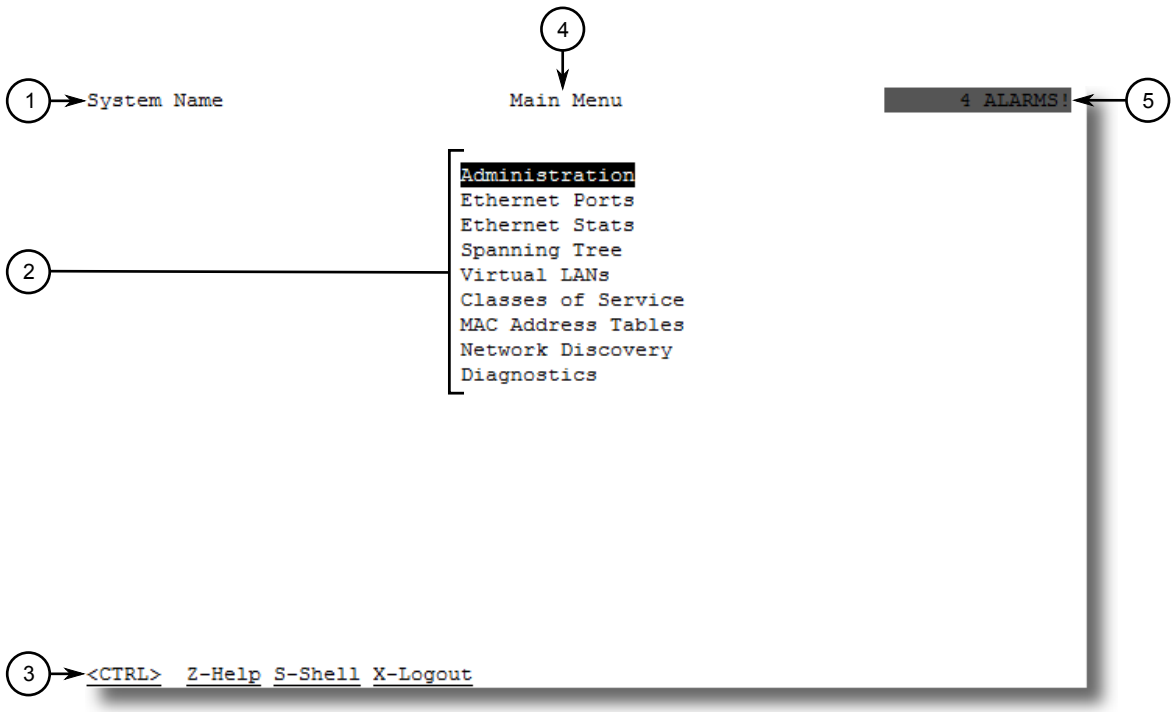


Figure 7 : Interface de console (exemple)

1. Identification système **2.** Menus **3.** Barre de commandes **4.** Nom de menu **5.** Indicateur d'alarmes

REMARQUE
L'identificateur système est configurable par l'utilisateur. Pour plus d'informations sur la définition du nom du système, voir Section 4.1, « Configuration du système d'information ».

Navigation dans l'interface

Utilisez les contrôles suivants pour naviguer entre les écrans de l'interface de console :

Entrée	Sélectionnez une commande de menu et appuyez sur **Entrée** pour ouvrir le sous-menu ou l'écran suivant.
Échap	Appuyez sur **Échap** pour revenir à l'écran précédent.

Configuration des paramètres

Utilisez les contrôles suivants pour sélectionner et configurer des paramètres dans l'interface de console :

Flèche vers le haut et flèche vers le bas	Utiliser les flèches HAUT et BAS pour sélectionner des paramètres.
Entrée	Sélectionnez un paramètre et appuyez sur **Entrée** pour démarrer l'édition d'un paramètre. Appuyez de nouveau sur **Entrée** pour appliquer la modification.
Échap	Lors de l'édition de paramètres, appuyez sur **Échap** pour annuler toutes les modifications.

Commandes

La barre de commandes répertorie les différentes commandes pouvant être générée dans l'interface de console. Certaines commandes sont spécifiques certains écrans. Les commandes standard sont entre autres :

Ctrl + A	Applique les modifications de configuration effectuées sur l'écran actuel. **REMARQUE** *Avant de quitter un écran, RUGGEDCOM ROS invite automatiquement l'utilisateur à enregistrer toute modification effectuée non encore appliquée.*
Ctrl + A	Insère un nouvel enregistrement.
Ctrl + L	Efface un enregistrement.
Ctrl + S	Ouvre l'interface CLI
Ctrl + X	Termine la session actuelle. Cette commande est disponible uniquement dans le menu principal.
Ctrl + Z	Affiche des informations importantes à propos de l'écran actuel ou du paramètre sélectionné.

Section 2.6

Utilisation de l'interface de ligne de commande

L'interface de ligne de commande (Command Line Interface, CLI) offre une série de commandes puissantes pour la mise à jour de RUGGEDCOM ROS, la génération de certificats/clés, le traçage d'événements, le dépannage, etc. Elle est accessible via l'interface de console en appuyant sur **Ctrl-S**.

SOMMAIRE

- Section 2.6.1, « Commandes CLI disponibles »
- Section 2.6.2, « Traçage d'événements »
- Section 2.6.3, « Exécution distante de commandes via RSH »
- Section 2.6.4, « Utilisation de commandes SQL »

Section 2.6.1

Commandes CLI disponibles

Les commandes suivantes sont disponibles dans la ligne de commande :

Commande	Description	Utilisateurs autorisés
`alarms` `all`	Affiche une liste des alarmes disponibles.	Invité, opérateur, administrateur

Commande	Description	Utilisateurs autorisés
	Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • `all` indique toutes les alarmes disponibles	
`arp`	Affiche le tableau de résolution d'adresse IP à MAC.	Administrateur
`clearalarms`	Efface toutes les alarmes.	Opérateur, administrateur
`clearethstats` `[ all | port ]`	Efface les statistiques Ethernet pour un ou plusieurs ports. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • `all` efface les statistiques pour tous les ports • *`port`* est une liste séparée par des virgules de numéros de port (par ex. 1,3-5,7)	Opérateur, administrateur
`clearlogs`	Efface les journaux système et d'incidents.	Administrateur
`clrcblstats` `[ all | port ]`	Efface les statistiques de diagnostics de câble pour un ou plusieurs ports. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • `all` efface les statistiques pour tous les ports • *`port`* est une liste séparée par des virgules de numéros de port (par ex. 1,3-5,7)	Administrateur
`clrstpstats`	Efface toutes les statistiques Spanning Tree.	Opérateur, administrateur
`cls`	Efface l'écran.	Invité, opérateur, administrateur
`dir`	Imprime la liste de répertoires.	Invité, opérateur, administrateur
`exit`	Termine la session.	Invité, opérateur, administrateur
`factory`	Active le mode factory, qui comprend plusieurs commandes de niveau usine utilisées pour les tests et le dépannage. Uniquement disponible pour les utilisateurs administrateurs. **ATTENTION !** *Une utilisation incorrecte des commande factory peut corrompre l'état de fonctionnement de l'appareil et/ou endommager définitivement la capacité de récupérer l'appareil sans intervention du constructeur.*	Administrateur
`flashfiles` `{ infonom de fichier | defrag }`	Un ensemble de commandes de diagnostic affichant des informations sur le système de fichiers Flash et défragmentant la mémoire Flash. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *`infonom de fichier`* affiche des informations sur le fichier spécifié dans le système de fichiers Flash • `defrag` défragmente des fichiers dans le système de fichiers Flash Pour plus d'informations sur la commande**`flashfiles`**, référez-vous à Section 2.8, « Gestion du système de fichiers flash ».	Administrateur
`flashleds` *`timeout`*	Fait clignoter les indicateurs LED sur l'appareil pour un nombre de secondes spécifié. Les paramètres optionnels facultatifs et/ou obligatoires comprennent :	Administrateur

Commande	Description	Utilisateurs autorisés
	• *timeout* est le nombre de secondes pendant lequel les indicateurs LED clignotent. Pour arrêter le clignotement des LED, définissez l'intervalle de timeout sur 0 (zéro).	
fpgacmd	Fournit un accès à l'outil de gestion FPGA pour la synchronisation du temps de dépannage.	Administrateur
help *commande*	Affiche une brève description de la commande spécifiée. Si aucune commande n'est spécifiée, une liste de toutes les commandes disponibles est affichée avec une description pour chacune. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *commande* est le nom de la commande.	Invité, opérateur, administrateur
ipconfig	Affiche l'adresse IP, le masque de sous-réseau et la passerelle par défaut actuels. Cette commande est la seule manière de déterminer ces valeurs lorsque DHCP est utilisé.	Invité, opérateur, administrateur
loaddflts	Charge la configuration par défaut.	Administrateur
logout	Ferme la session dans le shell.	Invité, opérateur, administrateur
logs	Affiche les entrées du syslog entrées dans le shell CLI.	Administrateur
ping *adresse* { *comptage* | *timeout* }	Envoie une demande d'écho ICPM à un appareil connecté à distance. La durée de boucle est affichée pour chaque réponse reçue. Utilisez cette commande pour vérifier la connectivité à l'appareil connecté suivant. Il s'agit d'un outil utile pour tester des liaisons établies. Cette commande comprend également la capacité d'envoyer un nombre spécifique de pings avec un délai d'attente de réponse paramétré. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *adresse* est l'adresse IP cible. • *comptage* est le nombre de demandes d'écho à envoyer. La valeur par défaut est 4. • *timeout* est le délai d'attente en millisecondes pour chaque réponse. La plage va de 2 à 5000 secondes. La valeur par défaut est 300. **REMARQUE** *L'appareil auquel envoyer une commande Ping doit prendre en charge l'écho ICMP. Avant le lancement de la commande Ping, une demande ARP est générée pour l'adresse MAC de l'appareil. Si l'appareil auquel envoyer une commande Ping ne se trouve pas sur le même réseau que l'appareil envoyant une commande Ping à cet appareil, la passerelle par défaut doit être programmé.*	Invité, opérateur, administrateur
purgemac	Purge le tableau d'adresses MAC.	Opérateur, administrateur
random	Affiche des valeurs initiales ou des nombres quelconques.	Administrateur
reset	Exécutez une réinitialisation matérielle du commutateur.	Opérateur, administrateur
resetport { all | *ports* }	Réinitialise un ou plusieurs ports Ethernet, ce qui peut être utile pour forcer la renégociation de la vitesse et du duplex, ou dans des situations dans lesquelles la liaison partenaire a été verrouillée dans un état inapproprié. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • all réinitialise tous les ports	Opérateur, administrateur

Commande	Description	Utilisateurs autorisés
	• *ports* est une liste séparée par des virgules de numéros de port (par ex. 1,3-5,7)	
rmon	Affiche les noms de tous les objets éligibles pour les alarmes RMON.	Invité, opérateur, administrateur
route	Affiche la configuration de la passerelle.	Invité, opérateur, administrateur
sfp *port* { base | alarms | diag | calibr | thr | all | no parameter specified }	Affiche les informations et les diagnostics d'appareils SFP (Small Form Factor Pluggable). Si des paramètres obligatoires ou facultatifs ne sont pas utilisés, cette commande affiche les informations de base et étendues. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *port* est le numéro de port pour lequel les données sont requises. • base affiche les informations de base • alarms affiche les balises d'alarme et d'avertissement. • diag affiche les données mesurées • calibr affiche les données d'étalonnage pour l'étalonnage externe • thr affiche les données de seuil • all indique toutes les données de diagnostic	Administrateur
sql { default | delete | help | info | insert | save | select | update }	Fournit une interface similaire à SQL pour la manipulation de tous les paramètres de configuration et d'état système. Toutes les colonnes, toutes les clauses, tous les tableaux et tous les noms de colonne respectent la casse. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • default réinitialise tous les enregistrements dans des tableaux aux valeurs usine • delete permet la suppression d'enregistrements d'un tableau • help fournit une brève description pour toute commande ou clause SQL • info indique une variété d'informations à propos des tableaux dans la base de données • insert permet l'insertion de nouveaux enregistrements dans un tableau • save enregistre la base de données dans le stockage en mémoire volatile • select interroge la base de données et affiche les enregistrements sélectionnés • update permet la mise à jour d'enregistrements existants dans un tableau Pour plus d'informations sur la commande**sql**, voir Section 2.6.4, « Utilisation de commandes SQL ».	Administrateur
sshkeygen *keytype N*	Génère de nouvelles clés SSH dansssh.keys. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *keytype* est le type de clé (rsa ou dsa) • *N* est le nombre de bits en longueur. Les tailles autorisées sont 1 024, 2 048 ou 3 072	Administrateur
sshpubkey	Indique, supprime et met à jour des entrées de clé dans le fichier sshpub.keys.	Administrateur
sslkeygen *keytype N*	Génère un nouveau certificat SSL dansssl.crt. Les paramètres optionnels facultatifs et/ou obligatoires comprennent :	Administrateur

Commande	Description	Utilisateurs autorisés
	• *keytype* est le type de clé, rsa ou ecc • *N* est le nombre de bits en longueur. Les tailles autorisées pour les clés RSA sont 1 024, 2 048 ou 3 072 Les tailles autorisées pour les clés ECC sont 192, 224, 256, 384 ou 521.	
telnet *dest*	Ouvre une session telnet. Utilisez**Ctrl-C** pour fermer la session. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *dest* est l'adresse IP du serveur	Invité, opérateur, administrateur
tftp { *dest* | *cmd* | *fsource* | *fdest* }	Ouvre une session TFTP. Utilisez**Ctrl-C** pour fermer la session. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *dest* est l'adresse IP du serveur TFTP distant • *cmd* est**put** (chargement) ou**get** (téléchargement) • *fsource* est le nom du fichier source • *fdest* est le nom du fichier de destination	Administrateur
trace	Démarre le traçage des événements. Exécutez**trace ?** pour obtenir plus d'aide.	Opérateur, administrateur
type *nom de fichier*	Affiche le contenu d'un fichier texte. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • *nom de fichier* est le nom du fichier à lire	Invité, opérateur, administrateur
version	Imprime la version logicielle	Invité, opérateur, administrateur
xmodem { send | receive } *nom de fichier*	Ouvre une session XModem. Les paramètres optionnels facultatifs et/ou obligatoires comprennent : • send envoie le fichier au client. • receive reçoit le fichier du client. • *nom de fichier* est le nom du fichier à lire.	Opérateur, administrateur

Section 2.6.2

Traçage d'événements

La commande CLI trace représente un moyen de tracer le fonctionnement de différents protocoles pris en charge par l'appareil. La trace fournit des informations détaillées, notamment des décodages de paquets STP, l'activité IGMP et les adresses MAC.

REMARQUE
Le traçage a été conçu pour fournir des informations détaillées à des utilisateurs experts. Notez que tout le traçage est désactivé au démarrage de l'appareil.

Procédez comme suit pour tracer un événement :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Déterminez les protocoles et les options associées disponibles en saisissant :

```
trace ?
```

Si une option telle que`allon` ou`alloff` est requise, déterminez les options disponibles pour le protocole souhaité en saisissant :

```
trace protocol ?
```

> **REMARQUE**
> *Le cas échéant, augmentez l'étendue du traçage en mélangeant des protocoles et leurs options associées à l'aide d'une barre verticale (|).*

3. Sélectionnez le type de trace à exécuter en saisissant :

```
trace protocol option
```

Où :

- *`protocol`* est le protocole à tracer
- *`option`* est l'option à utiliser pendant le traçage

Exemple :

```
>trace transport allon
TRANSPORT: Logging is enabled
```

4. Lancez le traçage en saisissant :

```
trace
```

Section 2.6.3

Exécution distante de commandes via RSH

L'utilitaire Remote Shell (RSH) peut être utilisé depuis un poste de travail pour que le produit réagisse à des commandes comme si elles étaient saisies dans l'invite de commande CLI. La syntaxe de la commande RSH a généralement la forme suivante :

```
rsh ipaddr -l auth_token command_string
```

Où :

- *`ipaddr`* est l'adresse ou le nom résolu de l'appareil.
- *`auth_token`* est le nom d'utilisateur (par ex. invité, opérateur ou administrateur) et le mot de passe correspondant séparés par une virgule. Par exemple, *admin,secret*.
- *`command_string`* est la commande CLI RUGGEDCOM ROS à exécuter.

> **REMARQUE**
> *Le niveau d'accès (correspondant au nom d'utilisateur) sélectionné doit prendre en charge la commande donnée.*

> **REMARQUE**
> *Toute sortie de la commande est renvoyée au poste de travail envoyant la commande. Les commandes qui commencent par des dialogues interactifs (comme**`trace`**) ne peuvent pas être utilisées.*

Section 2.6.4

Utilisation de commandes SQL

RUGGEDCOM ROS fournit un utilitaire *similaire à SQL* permettant aux utilisateurs experts d'exécuter plusieurs opérations impossibles dans une interface Web ou CLI traditionnelle. Par exemple :

- Restaurer les paramètres par défaut d'un tableau spécifique, mais pas de la configuration complète.
- Rechercher des tableaux dans la base de données pour des configurations spécifiques.
- Modifier des tableaux en fonction de configurations existantes.

Lorsqu'elles sont combinées avec RSH, les commandes SQL fournissent un moyen d'interroger et de configurer un grand nombre d'appareils depuis un emplacement central.

REMARQUE
Pour obtenir une liste des paramètres disponibles sous la commande **`sql`**, *voir* *Section 2.6.1, « Commandes CLI disponibles »*.

REMARQUE
Accéder en lecture/écriture à des tableaux contenant des mots de passe ou des phrases secrètes partagées à l'aide de commandes SQL.

SOMMAIRE

- Section 2.6.4.1, « Recherche du tableau correct »
- Section 2.6.4.2, « Récupération d'informations »
- Section 2.6.4.3, « Modification de valeurs dans un tableau »
- Section 2.6.4.4, « Réinitialisation d'un tableau »
- Section 2.6.4.5, « Utilisation de RSH et SQL »

Section 2.6.4.1

Recherche du tableau correct

Des commandes SQL multiples fonctionnent dans des tableaux spécifiques dans la base de données et nécessitent que le nom de tableau soit spécifié. La navigation dans le système de menu dans l'interface de console vers le menu souhaité et la combinaison de touches**Ctrl-Z** affichent le nom du tableau. Le nom de menu et le nom de tableau de la base de données correspondant sont cités.

Une autre manière de rechercher le nom de tableau consiste à saisir la commande suivante dans la CLI :

```
sql info tables
```

Cette commande affiche également les noms de menu et leurs noms de base de données correspondants en fonction des fonctionnalités prises en charge par l'appareil. Par exemple :

```
Table Description
--------------------------------------------------------------------------------
alarms Alarms
cpuDiags CPU Diagnostics
ethPortCfg Port Parameters
ethPortStats Ethernet Statistics
ethPortStatus Port Status
ipCfg IP Services
```

Section 2.6.4.2

Récupération d'informations

La présente rubrique décrit les différentes méthodes permettant de récupérer des informations sur des tableaux et des paramètres.

Récupération d'informations depuis un tableau

Utilisez la commande suivante pour afficher un résumé des paramètres au sein d'un tableau, ainsi que leurs valeurs :

```
sql select from table
```

Où :

- *table* est le nom du tableau

Exemple :

```
>sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
172.30.146.88   255.255.224.0   1001       17007888   2994       vlan1

1 records selected
```

Récupération d'informations sur un paramètre d'un tableau

Utilisez la commande suivante pour récupérer des informations sur un paramètre spécifique dans un tableau :

REMARQUE
Le paramètre doit être le même que celui affiché dans le système de menu, à moins que le nom ne contienne des espaces (par exemple une adresse IP). Les espaces doivent être remplacés par des traits de soulignement (par exemple adresse_IP) ou le nom de paramètre doit être entre guillemets doubles (par exemple "adresse IP").

```
sql select parameter from table
```

Où :

- *parameter* est le nom du paramètre
- *table* est le nom du tableau

Exemple :

```
>sql select "ip address" from ipSwitchIfCfg

IP Address
192.168.0.1

1 records selected
```

Récupération d'informations depuis un tableau à l'aide de la clause *Where*

Utilisez la commande suivante pour afficher des paramètres spécifiques d'un tableau qui ont une valeur spécifique :

```
sql select from table where parameter = value
```

Où :

- *table* est le nom du tableau
- *parameter* est le nom du paramètre
- *value* est la valeur du paramètre

Exemple :

```
>sql select from ethportcfg where media = 1000T

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl LFI Alarm
1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off      Off On
2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off      Off On
3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off      Off On
4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off      Off On

4 records selected
```

Affinez les résultats à l'aide des opérateurs`and` ou `or` :

```
sql select from table where parameter = value [ { and | or } | parameter | = | value ...]
```

Où :

- *table* est le nom du tableau
- *parameter* est le nom du paramètre
- *value* est la valeur du paramètre

Exemple :

```
>sql select from ethportcfg where media = 1000T and State = enabled

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl LFI Alarm
1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off      Off on
2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off      Off On
3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off      Off On
4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off      Off On

4 records selected
```

Section 2.6.4.3

Modification de valeurs dans un tableau

Utilisez la commande suivante pour modifier la valeur de paramètres dans un tableau :

```
sql update table set parameter = value
```

Où :

- *table* est le nom du tableau
- *parameter* est le nom du paramètre
- *value* est la valeur du paramètre

Exemple :

```
>sql update iplcfg set IP_Address_Type = static
1 records updated
```

Les conditions peuvent également être incluses dans la commande pour appliquer des modifications uniquement à des paramètres répondant à des critères spécifiques. Dans l'exemple suivant, le contrôle de flux est activé sur les ports fonctionnant en mode duplex intégral 100 Mbit/s avec le contrôle de flux désactivé :

```
>sql update ethportcfg set FlowCtrl = Off where ( Media = 100TX and FlowCtrl = On )
2 records updated
```

Section 2.6.4.4

Réinitialisation d'un tableau

Utilisez les commandes suivantes pour réinitialiser un tableau à ses valeurs par défaut :

```
sql default into table
```

Où :

- *table* est le nom du tableau

Section 2.6.4.5

Utilisation de RSH et SQL

La combinaison de scripts de shell distant et de commandes SQL permet d'interroger et de traiter un grand nombre d'appareils. Cette méthode permet de vérifier la cohérence de la configuration sur différents sites. Vous trouverez ci-dessous un exemple simple dans lequel les appareils à interroger sont déterminés depuis le fichier`Devices`:

```
C:> type Devices
10.0.1.1
10.0.1.2

C:\> for /F %i in (devices) do rsh %i -l admin,admin sql select from ipAddrtable

C:\>rsh 10.0.1.1 -l admin,admin sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
192.168.0.31    255.255.255.0   1001       274409096  2218       vlan1

1 records selected

C:\>rsh 10.0.1.2 -l admin,admin sql select from ipAddrtable
0 records selected
C:\
```

Section 2.7

Sélection de ports dans RUGGEDCOM ROS

De nombreuses fonctionnalités dans ROS peuvent être configurées pour un ou plusieurs ports sur l'appareil. La présente rubrique décrit la manière de spécifier un port unique, un groupe de ports outous les ports.

Sélectionnez un port unique en spécifiant le numéro de port :

```
2
```

Sélectionnez un groupe de ports à l'aide d'un tiret (-) entre le premier port et le dernier port dans la liste :

```
1-4
```

Sélectionnez plusieurs ports en définissant une liste séparée par des virgules :

```
1,4,6,9
```

Utilisez l'option*All* pour sélectionner tous les ports dans l'appareil ou, le cas échéant, utilisez l'option*None* pour ne sélectionner aucun port.

Section 2.8

Gestion du système de fichiers flash

Cette section décrit la manière de gérer le système de fichiers.

SOMMAIRE

- Section 2.8.1, « Affichage d'une liste de fichiers Flash »
- Section 2.8.2, « Affichage de détails de fichier Flash »
- Section 2.8.3, « Défragmentation du système de fichiers flash »

Section 2.8.1

Affichage d'une liste de fichiers Flash

Procédez comme suit pour afficher une liste de fichiers actuellement stockés dans la mémoire Flash :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Saisissez**`Flashfiles`**. Une liste des fichiers se trouvant actuellement dans la mémoire Flash est affichée, ainsi que leurs emplacements et le volume de mémoire qu'ils consomment. Par exemple :

```
>flashfiles
-----------------------------------------------------------------
Filename             Base    Size  Sectors     Used
-----------------------------------------------------------------
boot.bin         00000000 110000    0-16   1095790
main.bin         00110000 140000   17-36   1258403
syslog.txt       00260000 140000   38-57     19222
.
.
.
-----------------------------------------------------------------
```

Section 2.8.2

Affichage de détails de fichier Flash

Procédez comme suit pour afficher les détails d'un fichier actuellement stocké dans la mémoire Flash :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Affichez les informations concernant un fichier en saisissant :

```
flashfiles info nom de fichier
```

Où :

- *nom de fichier* est le nom du fichier stocké dans la mémoire Flash

Des détails similaires à ceux présentés ci-dessous s'affichent.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform         : ROS-CF52

File name        : main.bin
Firmware version : v4.3.0
Build date       : Sep 27 2014 15:50
File length      : 2624659
Board IDs        :  3d
Header CRC       : 73b4
Header CRC Calc  : 73b4
Body CRC         : b441
Body CRC Calc    : b441
```

Section 2.8.3

Défragmentation du système de fichiers flash

La mémoire flash est défragmentée automatiquement lorsque la mémoire disponible est suffisante pour une mise à niveau binaire. Cependant, la fragmentation peut être réalisée lorsqu'un nouveau fichier est chargé dans l'unité. La fragmentation a pour conséquence que des secteurs de mémoire disponible sont séparés de ceux affectés à des fichiers. Dans certains cas, il se peut que toute la mémoire disponible suffise pour une mise à niveau binaire, mais que la mémoire ne soit pas disponible dans une région contiguë.

Procédez comme suit pour défragmenter la mémoire flash :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Défragmentez la mémoire flash en saisissant :

```
flashfiles defrag
```

Section 2.9

Accès en mode BIST

Le mode BIST (Built-In-Self-Test) est utilisé par des techniciens de maintenance pour tester et configurer des fonctions de l'appareil. Il ne doit être utilisé qu'à des fins de dépannage.

ATTENTION !
Risque mécanique : risque d'endommagement de l'appareil. L'utilisation excessive de fonctions BIST peut entraîner une augmentation de l'usure de l'appareil pouvant annuler la garantie. Évitez d'utiliser les fonctions BIST sans les conseils d'un représentant de l'Assistance client Siemens.

Procédez comme suit pour accéder au mode BIST :

IMPORTANT !
Ne connectez pas l'appareil au réseau lorsqu'il est en mode BIST. L'appareil génèrerait un trafic de multidiffusion excessif dans ce mode.

1. Déconnectez l'appareil du réseau.
2. Connectez-vous à RUGGEDCOM ROS via le raccordement de console RS-232 et une application de terminal. Pour plus d'informations, voir Section 2.1.1, « Connexion directe ».
3. Lancez la remise à zéro du système. Pour plus d'informations, voir Section 3.13, « Réinitialisation de l'appareil ».
4. Pendant la séquence de démarrage, appuyez sur **Ctrl-C** lorsque vous y êtes invité. L'invite de commande pour BIST s'affiche.

```
>
```

5. Saisissez**`help`** pour afficher une liste d'options disponibles sous BIST.

3 Gestion de l'appareil

Ce chapitre décrit comment configurer et gérer l'appareil et ses composants, notamment les interfaces de module, les journaux et les fichiers.

REMARQUE
Pour plus d'informations sur la configuration de l'appareil de manière à ce qu'il fonctionne avec un réseau, voir Chapitre 5, Installation et configuration.

SOMMAIRE

- Section 3.1, « Affichage d'informations produit »
- Section 3.2, « Affichage de diagnostics de la CPU »
- Section 3.3, « Restauration des valeurs par défaut »
- Section 3.4, « Gestion des clés et certificats SSH et SSL »
- Section 3.5, « Chargement/téléchargement de fichiers »
- Section 3.6, « Gestion de journaux »
- Section 3.7, « Gestion de ports Ethernet »
- Section 3.8, « Gestion d'interfaces IP »
- Section 3.9, « Gestion de passerelles IP »
- Section 3.10, « Configuration des services IP »
- Section 3.11, « Gestion de la surveillance à distance »
- Section 3.12, « Chargement/téléchargement du firmware »
- Section 3.13, « Réinitialisation de l'appareil »
- Section 3.14, « Désactivation de l'appareil »

Section 3.1

Affichage d'informations produit

Lors du dépannage ou de la commande de nouveaux appareils, le personnel Siemens peut demander des informations spécifiques concernant l'appareil, notamment le modèle, le code de commande ou le numéro de série.

Pour afficher des informations concernant l'appareil, accédez à ***Diagnostics » View Product Information***. Le formulaire **Product Information** s'affiche.

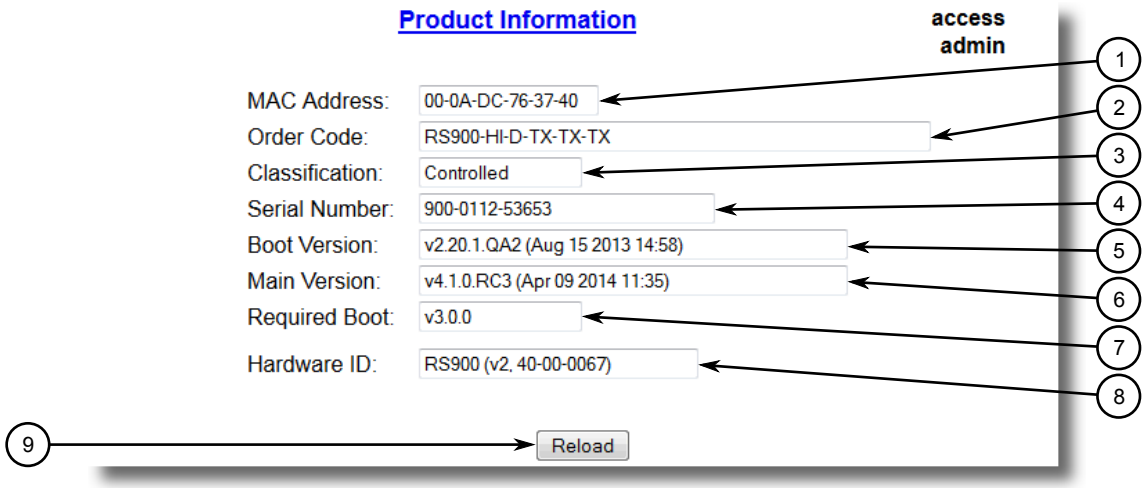


Figure 8 : Formulaire Product Information (exemple)

1. Zone MAC Address **2.** Zone Order Code **3.** Zone Classification **4.** Zone Serial Number **5.** Zone Boot Version **6.** Zone Main Version **7.** Zone Required Boot **8.** Zone Hardware ID **9.** Bouton Reload

Cet écran affiche les informations suivantes :

Paramètre	Description
MAC Address	**Synopsis :** ##-##-##-##-##-## avec une plage de 0 à FF pour ## Indique l'adresse MAC unique de l'appareil.
Order Code	**Synopsis :** 57 caractères quelconques Affiche le code de commande de l'appareil.
Classification	**Synopsis :** 15 caractères quelconques Fournit la classification système. La valeur *Controlled* indique que le firmware principal est une version contrôlée (Controlled). La valeur *Non-Controlled* indique que le firmware principal est une version non-contrôlée (Non-Controlled). Le firmware principal *Controlled* peut être exécuté sur des unités contrôlées, mais il ne peut pas être exécuté sur des unités non contrôlées. Le firmware principal *Non-Controlled* peut être exécuté sur des unités contrôlées et non contrôlées.
Serial Number	**Synopsis :** 31 caractères quelconques Indique le numéro de série de l'appareil.
Boot Version	**Synopsis :** 47 caractères quelconques Indique la version et la date de version du logiciel chargeur de démarrage.
Main Version	**Synopsis :** 47 caractères quelconques Indique la version et la date de version du système d'exploitation principal.
Required Boot	**Synopsis :** 15 caractères quelconques Indique la version de chargeur de démarrage minimum requise par le système d'exploitation.
Hardware ID	**Synopsis :** { RSMCPU (40-00-0008 Rev B1), RSMCPU2 (40-00-0026 Rev A1), RS400 (40-00-0010 Rev B2), RMC30, RS900 (40-00-0025 Rev B1), RS900 (40-00-0032 Rev B1), RS1600M, RS400 (40-00-0010 Rev C1), RSG2100, RS900G, RSG2200, RS969, RS900 (v2, 40-00-0066), RS900 (v2, 40-00-0067), , RS416 (40-00-0078), RMC30 (v2), RS930 (40-00-0089), RS969 (v2, 40-00-0090), RS910 (40-00-0091-001 Rev A), RS920L

Paramètre	Description
	(40-00-0102-001 Rev A), RS940G (40-00-0097-000 Rev A), RSi80X series CPU board, RSG2300, RS416v2, ... } Indique le type, le numéro de pièce et le niveau de révision du matériel.

Section 3.2

Affichage de diagnostics de la CPU

Pour afficher des informations de diagnostic de la CPU utiles pour le dépannage du matériel et des logiciels, accédez à ***Diagnostics » View CPU Diagnostics***. Le formulaire **CPU Diagnostics** s'affiche.

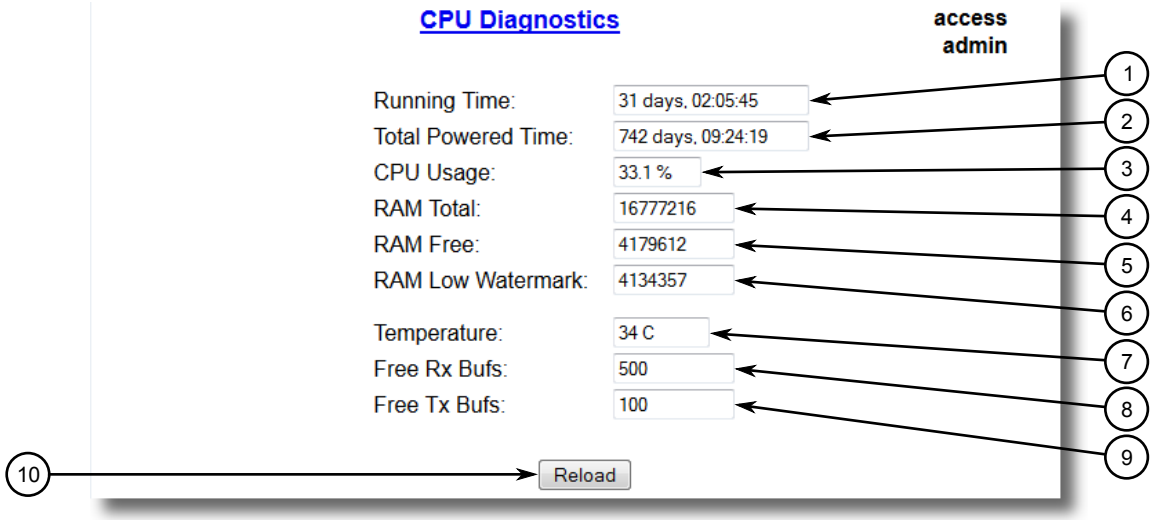


Figure 9 : Formulaire CPU Diagnostics

1. Zone Running Time **2.** Zone Total Powered time **3.** Zone CPU Usage **4.** Zone RAM Total **5.** Zone RAM Free **6.** Zone RAM Low Watermark **7.** Zone Temperature **8.** Zone Free Rx Bufs **9.** Zone Free Tx Bufs **10.** Bouton Reload

Cet écran affiche les informations suivantes :

Paramètre	Description
Running Time	**Synopsis :** DDDD jours, HH:MM:SS Temps écoulé depuis la dernière mise sous tension de l'appareil.
Total Powered time	**Synopsis :** DDDD jours, HH:MM:SS Temps cumulé de mise sous tension de l'appareil.
CPU Usage	**Synopsis :** 0.0 à 100.0% Pourcentage de cycles de CPU disponibles utilisés pour le fonctionnement de l'appareil mesuré pour la dernière seconde.
RAM Total	**Synopsis :** 0 à 4294967295 Taille totale de la mémoire RAM dans le système.
RAM Free	**Synopsis :** 0 à 4294967295

Paramètre	Description
	Taille totale de la mémoire RAM encore disponible.
RAM Low Watermark	**Synopsis :** 0 à 4294967295 Taille de la mémoire RAM qui n'a jamais été utilisée pendant l'exécution du système.
Temperature	**Synopsis :** -32768 to 32767 C Température de la carte CPU.
Free Rx Bufs	**Synopsis :** 0 à 4294967295 Tampons Rx libres.
Free Tx Bufs	**Synopsis :** 0 à 4294967295 Tampons Tx libres.

Section 3.3

Restauration des valeurs par défaut

Les réglages par défaut originaux de l'appareil peuvent être partiellement ou entièrement restaurés. Exclure des groupes de paramètres de la réinitialisation aux valeurs par défaut, notamment ceux qui affectent la connectivité de base et la gestion SNMP, est utile lorsque la communication avec l'appareil est toujours requise pendant la réinitialisation.

Les catégories suivantes ne sont pas affectées par une réinitialisation sélective de la configuration :

- IP Interfaces
- IP Gateways
- SNMP Users
- SNMP Security to Group Maps
- SNMP Access
- RUGGEDCOM Discovery Protocol™ (RCDP)

En outre, les catégories suivantes ne sont pas affectées par une réinitialisation complète de la configuration :

- Time Zone
- DST Offset
- DST Rule

Procédez comme suit pour restaurer les paramètres par défaut :

1. Accédez à ***Diagnostics » Load Factory Defaults***. Le formulaire **Load Factory Defaults** s'affiche.

Figure 10 : Formulaire Load Factory Defaults

1. Liste Defaults Choice **2.** Bouton Apply **3.** Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

> **REMARQUE**
> *Si l'ID de VLAN pour l'interface IP de gestion n'est pas* `1` *le réglage de* ***Defaults Choice*** *sur* `Selected` *le définit sur* `1`.

Paramètre	Description
Defaults Choice	**Synopsis :** { None, Selected, All } Régler certains enregistrements tels que la gestion d'interfaces IP, la passerelle par défaut et les réglages SNMP aux paramètres par défaut aurait pour conséquence que le commutateur ne soit plus accessible avec des applications de gestion. Ce paramètre permet à l'utilisateur de choisir de charger les valeurs par défaut dans les tableaux Selected, ce qui préserverait la configuration pour les tableaux critiques pour les applications de gestion de commutateurs, ou de forcer les réglages par défaut des tableaux All.

3. Cliquez sur **Apply**.

Section 3.4

Gestion des clés et certificats SSH et SSL

RUGGEDCOM ROS utilise des certificats et des clés X.509v3 pour établir des connexions distantes sécurisées (SSH) et un accès Web (SSL).

> **IMPORTANT !**
> *Siemens recommande de procéder comme suit avant la mise en service de l'appareil :*
> - *Remplacez le certificat SSL fourni en usine par un certificat signé par une autorité de certification (CA) de confiance.*
> - *Remplacez la paire de clés SSH d'hôte fournie en usine par une paire générée par une autorité de certification de confiance.*

> **REMARQUE**
> *Seuls les administrateurs peuvent écrire des certificats et des clés pour l'appareil.*

Chaque appareil RUGGEDCOM ROS est livré avec une unique paire de clés SSH d'hôte basée sur RSA 2048 et un certificat auto-signé basé sur RSA 2048 générés et mis en service en usine. L'administrateur peut charger un

nouveau certificat et de nouvelles clés qui écraseront ceux qui existent dans le système à tout moment. En outre, des commandes CLI sont disponibles pour regénérer des certificats et des paires de clés SSL ainsi que la paire de clés SSL d'hôte.

Il existe trois types de certificats et de clés utilisés dans RUGGEDCOM ROS :

REMARQUE
L'exposition d'un réseau à une unité ROS fonctionnant avec des clés par défaut doit être évitée, même si elles sont toujours conçues pour être temporaires. La meilleure manière de réduire ou d'éliminer cette exposition est de mettre en service un certificat et des clés créés par l'utilisateur aussi rapidement que possible, de préférence avant que l'unité ne soit en service dans le réseau.

REMARQUE
Par défaut, les certificats et les clés sont communs à toutes les versions de RUGGEDCOM ROS sans certificat ou fichier de clé. C'est la raison pour laquelle il est important d'autoriser la génération automatique de clés pour compléter ou mettre en service des clés personnalisées. De cette manière, des clés au moins uniques et au mieux traçables et vérifiables sont installées lors de l'établissement d'une communication sécurisée avec l'unité.

- **Par défaut**
  Un certificat par défaut et des clés SSL/SSH sont intégrés au RUGGEDCOM ROS et répandus dans toutes les unités RUGGEDCOM ROS partageant la même image de firmware. Si aucun certificat SSL et aucun fichier SSL/SSH valide n'est disponible sur l'appareil (comme c'est généralement le cas uniquement lors de la mise à niveau depuis une ancienne version de ROS ne prenant pas en charge les clés configurables par l'utilisateur et n'étant donc pas livrée avec des clés uniques générées en usine), le certificat et les clés par défaut sont activés *temporairement* afin que les sessions SSH et SSL (HTTPS) puissent être exécutées jusqu'à ce que des clés générées ou mises en service soient disponibles.
- **Générés automatiquement**
  Si un certificat SSL et des clés SSL/SSH par défaut sont utilisés, RUGGEDCOM ROS commence immédiatement à générer un certificat et des clés SSL/SSH uniques pour l'appareil en arrière-plan. Ce processus peut prendre quelques minutes selon la longueur de clé demandée et de l'occupation de l'appareil à ce moment. Si un certificat et des clés personnalisés sont chargés pendant que des certificats et des clés générés automatiquement sont en cours de génération, le générateur annule l'opération et le certificat et les clés personnalisés sont utilisés.
- **Personnalisés (recommandé)**
  Les certificats et les clés personnalisés constituent l'option la plus sécurisée. Ils donnent à l'utilisateur un contrôle complet de la gestion des certificats et de clés, permettent la mise en service de certificats signés par une autorité de certification publique ou locale, activent un accès strictement contrôlé aux clés privées et permettent la répartition autoritaire de certificats SSL, de tout certificat de CA et de clés SSH publiques.

REMARQUE
La clé privée RSA ou EC correspondant au certificat SSL doit être ajoutée au certificat dans le fichier`ssl.crt`.

SOMMAIRE

- Section 3.4.1, « Certificats SSL »
- Section 3.4.2, « Clé d'hôte SSH »
- Section 3.4.3, « Gestion de clés publiques SSH »
- Section 3.4.4, « Exemples de certificats et de clés »

Section 3.4.1

Certificats SSL

RUGGEDCOM ROS prend en charge les certificats SSH conformes aux spécifications suivantes :

- Format de certificat numérique X.509 v3
- Format PEM
- Pour les versions de RUGGEDCOM ROS contrôlées : Paire de clés RSA, 1 024, 2 048 ou 3 072 bits ; ou EC 256, 384 ou 521 bits
- Pour les versions non contrôlées (NC) de RUGGEDCOM ROS : Paire de clés RSA, 512 ou 2 048 bits

REMARQUE
Les clés RSA d'une longueur inférieure à 2 048 bits ne sont pas recommandées. La prise en charge est uniquement incluse pour des raisons de compatibilité avec l'équipement hérité.

REMARQUE
Les temps de génération de clés RSA augmentent en fonction de la longueur de clé. La génération de clés RSA de 1 024 bits prend plusieurs minutes, alors que les clés de 2 048 bits peuvent prendre beaucoup plus de temps. Un système PC moderne type peut, cependant, générer ces clés en quelques secondes.

Le fragment de script shell (bash) utilise la ligne de commande`openssl` pour générer un certificat SSL X.509 v3 auto-signé avec une clé RSA de 2 048 bits compatible avec une utilisation dans RUGGEDCOM ROS. Notez que deux fichiers PEM standard sont requis : le certificat SSL et le fichier de clé privée RSA. Ils sont concaténés dans le fichier`ssl.crt` résultant, qui peut être chargé dans RUGGEDCOM ROS :

```
# RSA key size:
BITS=2048
# 20 years validity:
DAYS=7305

# Values that will be stored in the Distinguished Name fields:

COUNTRY_NAME=CA                    # Two-letter country code
STATE_OR_PROVINCE_NAME=Ontario     # State or Province
LOCALITY_NAME=Concord              # City
ORGANIZATION=Ruggedcom.com         # Your organization's name
ORGANIZATION_CA=${ORGANIZATION}_CA # Your Certificate Authority
COMMON_NAME=RC                     # The DNS or IP address of the ROS unit
ORGANIZATIONAL_UNIT=ROS            # Organizational unit name

# Variables used in the construction of the certificate
REQ_SUBJ="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION}/OU=
${ORGANIZATIONAL_UNIT}/CN=${COMMON_NAME}/"
REQ_SUBJ_CA="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION_CA}/
OU=${ORGANIZATIONAL_UNIT}/"

#######################################################################
# Make the self-signed SSL certificate and RSA key pair:

openssl req -x509 -newkey rsa:${BITS} -nodes \
 -days ${DAYS} -subj ${REQ_SUBJ} \
 -keyout ros_ssl.key  \
 -out    ros_ssl.crt

# Concatenate Cert and Key into a single file suitable for upload to ROS:
# Note that cert must precede the RSA key:
cat  ros_ssl.crt  ros_ssl.key > ssl.crt
```

Vous trouverez ci-dessous un exemple de certificat SSL auto-signé généré par RUGGEDCOM ROS :

```
Certificate:
Data:
 Version: 3 (0x2)
 Serial Number:
  ca:01:2d:c0:bf:f9:fd:f2
 Signature Algorithm: sha1WithRSAEncryption
 Issuer: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
 Validity
  Not Before: Dec  6 00:00:00 2012 GMT
  Not After : Dec  7 00:00:00 2037 GMT
 Subject: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
 Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
   Modulus (1024 bit):
    00:83:e8:1f:02:6b:cd:34:1f:01:6d:3e:b6:d3:45:
    b0:18:0a:17:ae:3d:b0:e9:c6:f2:0c:af:b1:3e:e7:
    fd:f2:0e:75:8d:6a:49:ce:47:1d:70:e1:6b:1b:e2:
    fa:5a:1b:10:ea:cc:51:41:aa:4e:85:7c:01:ea:c3:
    1e:9e:98:2a:a9:62:48:d5:27:1e:d3:18:cc:27:7e:
    a0:94:29:db:02:5a:e4:03:51:16:03:3a:be:57:7d:
    3b:d1:75:47:84:af:b9:81:43:ab:90:fd:6d:08:d3:
    e8:5b:80:c5:ca:29:d8:45:58:5f:e4:a3:ed:9f:67:
    44:0f:1a:41:c9:d7:62:7f:3f
   Exponent: 65537 (0x10001)
 X509v3 extensions:
  X509v3 Subject Key Identifier:
   EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
  X509v3 Authority Key Identifier:
   keyid:EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
   DirName:/C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=ROS
   serial:CA:01:2D:C0:BF:F9:FD:F2
  X509v3 Basic Constraints:
   CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
 64:cf:68:6e:9f:19:63:0e:70:49:a6:b2:fd:09:15:6f:96:1d:
 4a:7a:52:c3:46:51:06:83:7f:02:8e:42:b2:dd:21:d2:e9:07:
 5c:c4:4c:ca:c5:a9:10:49:ba:d4:28:fd:fc:9d:a9:0b:3f:a7:
 84:81:37:ca:57:aa:0c:18:3f:c1:b2:45:2a:ed:ad:dd:7f:ad:
 00:04:76:1c:f8:d9:c9:5c:67:9e:dd:0e:4f:e5:e3:21:8b:0b:
 37:39:8b:01:aa:ca:30:0c:f1:1e:55:7c:9c:1b:43:ae:4f:cd:
 e4:69:78:25:5a:a5:f8:98:49:33:39:e3:15:79:44:37:52:da:
 28:dd
```

Section 3.4.2

Clé d'hôte SSH

REMARQUE
SSH n'est pas pris en charge dans des versions non contrôlées (Non-Controlled (NC)) de RUGGEDCOM ROS.

Les versions contrôlées de RUGGEDCOM ROS prennent en charge les paires de clés SSH publiques/privées conformes aux spécifications suivantes :

- Format PEM
- Paire de clés DSA, 1 024, 2 048 ou 3 072 bits de longueur
- Paire de clés RSA, 1 024, 2 048 ou 3 072 bits de longueur

REMARQUE
Les temps de génération de clés DSA ou RSA augmentent en fonction de la longueur de clé. La génération de clés RSA de 1 024 bits prend moins de 5 minutes sur une unité peu chargée, alors que les clés de 2 048 bits peuvent prendre beaucoup plus de temps. Un système PC moderne type peut, cependant, générer ces clés en quelques secondes.

Le fragment de script shell (bash) utilise la ligne de commande`ssh-keygen` pour générer une clé RSA de 2 048 bits compatible avec une utilisation dans RUGGEDCOM ROS. Le fichier`ssh.keys` résultant peut être chargé dans RUGGEDCOM ROS :

```
# RSA key size:
BITS=2048

# Make an SSH key pair:
ssh-keygen -t RSA -b $BITS -N '' -f ssh.keys
```

Vous trouverez ci-dessous un exemple de clé SSH générée par RUGGEDCOM ROS :

```
Private-Key: (1024 bit)
priv:
    00:b2:d3:9d:fa:56:99:a5:7a:ba:1e:91:c5:e1:35:
    77:85:e8:c5:28:36
pub:
    6f:f3:9e:af:e6:d6:fd:51:51:b9:fa:d5:f9:0a:b7:
    ef:fc:d7:7c:14:59:52:48:52:a6:55:65:b7:cb:38:
    2e:84:76:a3:83:62:d0:83:c5:14:b2:6d:7f:cc:f4:
    b0:61:0d:12:6d:0f:5a:38:02:67:a4:b7:36:1d:49:
    0a:d2:58:e2:ff:4a:0a:54:8e:f2:f4:c3:1c:e0:1f:
    9b:1a:ee:16:e0:e9:eb:c8:fe:e8:16:99:e9:61:81:
    ed:e4:f2:58:fb:3b:cb:c3:f5:9a:fa:ed:cd:39:51:
    47:90:5d:6d:1b:27:d5:04:c5:de:57:7e:a7:a3:03:
    e8:fb:0a:d5:32:89:40:12
P:
    00:f4:81:c1:9b:5f:1f:eb:ac:43:2e:db:dd:77:51:
    6e:1c:62:8d:4e:95:c6:e7:b9:4c:fb:39:9c:9d:da:
    60:4b:0f:1f:c6:61:b0:fc:5f:94:e7:45:c3:2b:68:
    9d:11:ba:e1:8a:f9:c8:6a:40:95:b9:93:7c:d0:99:
    96:bf:05:2e:aa:f5:4e:f0:63:02:00:c7:c2:52:c7:
    1a:70:7c:f7:e5:fe:dd:3d:57:02:86:ae:d4:89:20:
    ca:4b:46:80:ea:de:a1:30:11:5c:91:e2:40:d4:a3:
    82:c5:40:3b:25:8e:d8:b2:85:cc:f5:9f:a9:1d:ea:
    0a:ac:77:95:ee:d6:f7:61:e3
Q:
    00:d5:db:48:18:bd:ec:69:99:eb:ff:5f:e1:40:af:
    20:80:6d:5c:b1:23
G:
    01:f9:a1:91:c0:82:12:74:49:8a:d5:13:88:21:3e:
    32:ea:f1:74:55:2b:de:61:6c:fd:dd:f5:e1:c5:03:
    68:b4:ad:40:48:58:62:6c:79:75:b1:5d:42:e6:a9:
    97:86:37:d8:1e:e5:65:09:28:86:2e:6a:d5:3d:62:
    50:06:b8:d3:f9:d4:9c:9c:75:84:5b:db:96:46:13:
    f0:32:f0:c5:cb:83:01:a8:ae:d1:5a:ac:68:fb:49:
    f9:b6:8b:d9:d6:0d:a7:de:ad:16:2b:23:ff:8e:f9:
    3c:41:16:04:66:cf:e8:64:9e:e6:42:9a:d5:97:60:
    c2:e8:9e:f4:bc:8f:6f:e0
```

Section 3.4.3

Gestion de clés publiques SSH

RUGGEDCOM ROS permet aux administrateurs de répertorier, d'ajouter et de supprimer des clés publiques SSH. Les clés publiques sont ajoutées comme fichiers de stockage non volatile (c'est-à-dire Flash) sur des appareils RUGGEDCOM ROS et récupérées au moment de l'authentification du client SSH.

SOMMAIRE

- Section 3.4.3.1, « Exigences en matière de clés publiques »
- Section 3.4.3.2, « Ajout d'une clé publique »
- Section 3.4.3.3, « Affichage d'une liste de clés publiques »
- Section 3.4.3.4, « Mise à jour d'une clé publique »
- Section 3.4.3.5, « Suppression d'une clé publique »

Section 3.4.3.1

Exigences en matière de clés publiques

Les clés publiques sont stockées dans un fichier flash file appelé *sshpub.keys*. Le fichier *sshpub.keys* est constitué d'entrées de clé publique utilisateur ssh. De manière similaire au fichier config.csv, chaque entrée doit être séparée par une ligne vide. Une entrée a deux composants. Il s'agit des composants consécutifs suivants :

- En-tête
- Clé

L'en-tête contient les paramètres de l'entrée séparés par des virgules. Les paramètres sont, consécutivement :

- ID : un nombre compris entre 0 et 9999
- Entry type: UserKey
- Access Level: (Admin, Operator ou Guest)
- Revocation Status: active/inactive (toujours actif pour les clés)
- User Name: Il s'agit du nom d'utilisateur du client (pas du nom d'utilisateur RUGGEDCOM ROS). Il est utilisé par des clients pour exécuter un SSH dans l'appareil RUGGEDCOM ROS.

La clé doit être au format RFC4716 ou PEM avec l'une des lignes d'en-tête et de pied de page suivantes quelconque :

```
-----BEGIN PUBLIC KEY-----
-----END PUBLIC KEY-----

-----BEGIN SSH2 PUBLIC KEY-----
-----END SSH2 PUBLIC KEY-----

-----BEGIN RSA PUBLIC KEY-----
-----END RSA PUBLIC KEY-----
```

Vous trouverez ci-dessous un exemple d'entrée valide dans le fichier *sshpub.keys* au format PEM :

```
1,userkey,admin,active,alice
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAABIwAAAQEA4mRrqfk+RKXnmGRvzMyWVDsbq5VwpGGrlLQYCrjVEa
NdbXsphqYKop8V5VUeXFRAUFzOy82yk8TF/5JxGPWq6wRNjhnYR7IY2AiMBq0+K8XeURl/
z5K2XNRjnqTZSFwkhaUVJeduvjGgOlNN4yvgUwF3n0idU9k3E1q/na+LmYIeGhOwzCqoAc
```

```
ipHAdR4fhD5u0jbmvjv+gDikTSZIbj9eFJfP09ekImMLHwbBry0SSBpqAKbwVdWEXIKQ47
zz7ao2/rs3rSV16IXSq3Qe8VZh2irah0Md6JFMOX2qm9fo1I62q1DDgheCOsOiGPf4xerH
rI2cs6FT31rAdx2JOjvw==
---- END SSH2 PUBLIC KEY ----
```

Vous trouverez ci-dessous un exemple d'entrée valide dans le fichier *sshpub.keys* au format RFC4716 :

```
2,userkey,admin,active,bob
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDH0NivR8zzbTxlecvFPzR/
GR24NrRJa0Lc7scNsWRgi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uLJe0Su3RvyNYz1jkdSwHq2hSZCpukJxJ6CK95Po/
sVa5Gq2gMaHowiYDSkcx+AJywzK/eM6i/jc125lRxFPdfkj74u+ob3PCvmIWz5z3WAJBrQU1IDPHDets511WMu8O9/
mAPZRwjqrWhRsqmcXZuv5oo54wIopCAZSo20SPzM2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/
oMFFn934cbO5N6etsJSvplYQ4pMCw6Ok8Q/bB5cPSOa/rAt bob@work
```

RUGGEDCOM ROS permet le stockage de 16 entrées de clé utilisateur au maximum. Chaque clé doit tenir compte des limites suivantes :

- Le type de clé doit être RSA 2 048 bits ou RSA 3 072 bits
- La taille de la clé ne doit pas dépasser 4 000 caractères chiffrés en base64
- Le type d'entrée dans l'en-tête ne doit pas dépasser 8 caractères ASCII
- Le niveau d'accès dans l'en-tête ne doit pas dépasser 8 caractères ASCII (*Operator* est le maximum)
- L'état de révocation dans l'en-tête ne doit pas dépasser 8 caractères ASCII (*Inactive* au maximum)
- Le nom d'utilisateur ne doit pas dépasser 12 caractères ASCII

Section 3.4.3.2

Ajout d'une clé publique

Les administrateurs peuvent ajouter une clé publique ou plusieurs clés publiques à RUGGEDCOM ROS.

Il existe a deux manières de mettre à jour *sshpub.keys* :

- Chargez un fichier créé localement directement dans le fichier *sshpub.keys*. Le contenu du fichier remplace le contenu actuellement enregistré dans la mémoire flash.
- Chargez un fichier créé localement dans le fichier *sshaddpub.keys*. Le contenu du fichier est ajouté aux entrées du fichier *sshpub.keys*.

IMPORTANT !
*Le contenu du fichier **sshaddpub.keys** doit avoir la même syntaxe que le fichier **sshpub.keys**.*

Procédez comme suit pour ajouter des clés :

1. Créez une clé publique via un ordinateur hôte.
2. Transférez le fichier de clé publique dans l'appareil à l'aide de SFTP ou Xmodem. Pour plus d'informations sur le transfert de fichiers, voir Section 3.5, « Chargement/téléchargement de fichiers ».
3. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
4. Assurez-vous que les fichiers ont été transférés correctement dans le journal système. Pour plus d'informations sur l'affichage du journal système, voir " Section 3.6.1, « Affichage de journaux locaux et système »".

Section 3.4.3.3

Affichage d'une liste de clés publiques

Les administrateurs peuvent afficher une liste de clés publiques existantes sur l'appareil.

Procédez comme suit pour afficher des clés publiques :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Dans l'invite de commande de la CLI, entrez :

```
sshpubkey list
```

   Une liste de clés publiques s'affiche indiquant leur ID de clé, leur niveau d'accès, leur état de révocation, le nom d'utilisateur et l'empreinte de clé.

Section 3.4.3.4

Mise à jour d'une clé publique

Les administrateurs peuvent mettre à jour des clés publiques.

Procédez comme suit pour mettre à jour des clés publiques :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Dans l'invite de commande de la CLI, entrez :

```
sshpubkey list
```

   Une liste de clés publiques s'affiche indiquant leur ID de clé, leur niveau d'accès, leur état de révocation, le nom d'utilisateur et l'empreinte de clé.
3. Saisissez les commandes suivantes pour mettre à jour les clés publiques :

Commande	Description
sshpubkey update_id *current_ID new_ID*	Met à jour d'ID de la clé publique utilisateur. **REMARQUE** *L'ID de clé publique utilisateur doit être un nombre compris entre 0 et 9999* • *current_ID* est l'ID actuellement affecté à la clé publique • *new_ID* est l'ID utilisé pour identifier la clé publique
sshpubkey update_al *AL*	Met à jour le niveau d'accès d'une clé publique utilisateur. • *AL* est le niveau d'accès de la clé publique à mettre à jour
sshpubkey update_rs *RS*	Met à jour l'état de révocation (active, inactive) d'une clé publique utilisateur. • *RS* est l'état de révocation de la clé publique à mettre à jour
sshpubkey update_un *UN*	Met à jour le nom d'utilisateur d'une clé publique utilisateur. • *UN* est le nom d'utilisateur de la clé publique à mettre à jour

Section 3.4.3.5

Suppression d'une clé publique

Les administrateurs peuvent supprimer une clé publique ou plusieurs clés publiques.

Procédez comme suit pour supprimer une clé publique :

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Dans l'invite de commande de la CLI, entrez :

```
sshpubkey list
```

   Une liste de clés publiques s'affiche indiquant le niveau d'accès, l'état de révocation, le nom d'utilisateur et l'empreinte de clé.

3. Saisissez les commandes suivantes pour supprimer les clés publiques :

Commande	Description
sshpubkey remove *ID*	Supprime une clé du stockage non-volatile. • *ID* est l'ID de la clé publique à supprimer

Section 3.4.4

Exemples de certificats et de clés

Pour SSL, les versions contrôlées de RUGGEDCOM ROS requièrent un certificat X.509 au format PEM standard et une paire de clés RSA ou ECC. Le certificat peut être auto-signé ou signé par une autre autorité. La clé RSA doit avoir une longueur de 1 024, 2 048 ou 3 072 bits ; la clé ECC doit avoir une longueur de 192, 224, 256, 384 ou 521 bits.

Les versions non contrôlées (Non-Controlled (NC)) de RUGGEDCOM ROS requièrent un certificat X.509 au format PEM standard et une paire de clés RSA. La clé RSA doit avoir une longueur comprise entre 512 et 2 048 bits.

Le certificat et les clés doivent être combinés dans un fichier`ssl.crt` unique et chargés dans l'appareil.

Vous trouverez ci-dessous un exemple de combinaison d'un certificat et d'une clé SSL :


```
-----BEGIN CERTIFICATE-----
MIIC9jCCAl+gAwIBAgIJAJh6rrehMt3iMA0GCSqGSIb3DQEBBQUAMIGuMQswCQYD
VQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBxMHQ29uY29yZDESMBAG
A1UEChMJUnVnZ2VkY29tMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MSYwJAYD
VQQDEx1XUy1NSUxBTkdPVkFOL1JVR0dFRENPTS5MT0NBTDEkMCIGCSqGSIb3DQEJ
ARYVc3VwcG9ydEBydWdnZWRjb20uY29tMB4XDTEyMTAyMzIxMTA1M1oXDTE3MTAy
MjIxMTA1M1owgZwxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdPbnRhcmlvMRAwDgYD
VQQHEwdDb25jb3JkMRIwEAYDVQQKEwlSdWdnZWRDb20xGTAXBgNVBAsTEEN1c3Rv
bWVyIFN1cHBvcnQxFDASBgNVBAMTCzE5Mi4xNjguMS4yMSQwIgYJKoZIhvcNAQkB
FhVTdXBwb3J0QHJ1Z2dlZGNvbS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALfE4eh2aY+CE3W5a4Wz1Z1RGRP02COHt153wFFrU8/fFQXNhKlQirlAHbNT
RSwcTR8ZFapivwYDivn0ogOGFXknYP90gv2oIaSVY08FqZkJW77g3kzkv/8Zrw3m
W/cBsZJ8SyKLIDfy401HkHpDOle5NsQFSrziGUPjAOIvvx4rAgMBAAGjLDAqMAkG
A1UdEwQCMAAwHQYDVR0OBBYEFER0utgQOifnrflnDtsqNcnvRB0XMA0GCSqGSIb3
DQEBBQUAA4GBAHtBsNZuh8tB3kdqR7Pn+XidCsD70YnI7w0tiy9yiRRhARmVXH8h
5Q1rOeHceri3JFFIOxIxQt4KgCUYJLu+c9Esk/nXQQar3zR7IQCt0qOABPkviiY8
c3ibVbhJjLpR2vNW4xRAJ+HkNNtBOg1xUlp4vOmJ2syYZR+7XAy/OP/S
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC3xOHodmmPghN1uWuFs9WdURkT9Ngjh7ded8BRa1PP3xUFzYSp
UIq5QB2zU0UsHE0fGRWqYr8GA4r59KIDhhV5J2D/dIL9qCGklWNPBamZCVu+4N5M
5L//Ga8N5lv3AbGSfEsiiyA38uNNR5B6QzpXuTbEBUq84hlD4wDiL78eKwIDAQAB
AoGBAI2CXHuHg23wuk9zAusoOhw0MN1/M1jYz0k9aajIvvdZT3Tyd29yCADy8GwA
```

```
eUmoWXLS/C4CcBqPa9til8ei3rDn/w8dveVHsi9FXjtVSYqN+ilKw+moMAjZy4kN
/kpdpHMohwv/909VWR1AZbr+YTxaG/++tKl5bqXnZl4wHF8xAkEA5vwut8USRg2/
TndOt1e8ILEQNHvHQdQr2et/xNH4ZEo7mqot6skkCD1xmxA6XG64hR3BfxFSZcew
Wr4SOFGCtQJBAMurr5FYPJRFGzPM3HwcpAaaMIUtPwNyTtTjywlYcUI7iZVVfbdx
4B7qOadPybTg7wqUrGVkPSzzQelz9YCSSV8CQFqpIsEYhbqfTLZEl83YjsuaE801
xBivaWLIT0b2TvM2O7zSDOG5fv4I990v+mgrQRtmeXshVmEChtKnBcm7HH0CQE6B
2WUfLArDMJ8hAoRczeU1nipXrIh5kWWCgQsTKmUrafdEQvdpT8ja5GpX2Rp98eaU
NHfI0cP36JpCdome2eUCQDZN9OrTgPfeDIXzyOiUUwFlzS1idkUGL9nH86iuPnd7
WVF3rV9Dse30sVEk63Yky8uKUy7yPUNWldG4U5vRKmY=
-----END RSA PRIVATE KEY-----
```


Pour SSH, RUGGEDCOM ROS requiert une paire de clés d'hôte DSA ou RSA au format PEM. La clé doit avoir une longueur de 1 024, 2 048 ou 3 072 bits pour les versions contrôlées. Le fichier de clé est chargé dans le fichier Flash`ssh.keys` sur l'appareil.

Vous trouverez ci-dessous un exemple de clé SSH au format PEM :


```
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQD0gcGbXx/rrEMu2913UW4cYo1OlcbnuUz7OZyd2mBLDx/GYbD8
X5TnRcMraJ0RuuGK+chqQJW5k3zQmZa/BS6q9U7wYwIAx8JSxxpwfPfl/t09VwKG
rtSJIMpLRoDq3qEwEVyR4kDUo4LFQDsljtiyhcz1n6kd6gqsd5Xu1vdh4wIVANXb
SBi97GmZ6/9f4UCvIIBtXLEjAoGAAfmhkcCCEnRJitUTiCE+MurxdFUr3mFs/d31
4cUDaLStQEhYYmx5dbFdQuapl4Y32B7lZQkohi5q1T1iUAa40/nUnJx1hFvblkYT
8DLwxcuDAaiu0VqsaPtJ+baL2dYNp96tFisj/475PEEWBGbP6GSe5kKa1Zdgwuie
9LyPb+ACgYBv856v5tb9UVG5+tX5Crfv/Nd8FFlSSFKmVWW3yzguhHajg2LQg8UU
sm1/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```


Section 3.5

Chargement/téléchargement de fichiers

Des fichiers peuvent être transférés entre l'appareil et un ordinateur hôte à l'aide de l'une des méthodes suivantes :

- Xmodem à l'aide du shell CLI via une session Telnet ou de console RS-232
- Client TFTP à l'aide du shell CLI dans une session de console et un serveur TFTP distant
- Serveur TFTP depuis un client TFTP distant
- SFTP (secure FTP over SSH) depuis un client SFTP distant

IMPORTANT !
Des scripts peuvent être utilisés pour automatiser la gestion de fichiers sur l'appareil. Cependant, en fonction de la taille des fichiers cibles, un délai entre des commandes d'écriture et de lecture consécutives peut être nécessaire, car il se peut que le fichier n'ait pas été entièrement enregistré avant la génération de la commande de lecture. Un délai général de cinq secondes est recommandé, mais il est recommandé d'effectuer un test pour optimiser le délai pour les fichiers cibles et l'environnement d'exploitation.

REMARQUE
Le contenu du système de fichiers interne est fixe. Il est impossible de créer de nouveaux fichiers et répertoires, et les fichiers existants ne peuvent pas être supprimés. Seuls les fichiers qui peuvent être chargés sur l'appareil peuvent être remplacés.

Les fichiers qui peuvent nécessiter un chargement ou un téléchargement sont :

- `main.bin` – image de firmware principal d'application RUGGEDCOM ROS
- `boot.bin` – image du firmware du chargeur de démarrage
- `fpga.xsvf` – image binaire du firmware FPGA
- `config.csv` – base de données de configuration complète sous forme d'un fichier texte ASCII séparé par des virgules
- `factory.txt` – contient l'adresse MAC, le code de commande et le numéro de série. Les données d'usine doivent être signées.
- `banner.txt` – contient le texte qui s'affiche sur l'écran d'ouverture de session

SOMMAIRE

- Section 3.5.1, « Chargement/téléchargement de fichiers à l'aide de XMODEM »
- Section 3.5.2, « Chargement/téléchargement de fichiers à l'aide d'un client TFTP »
- Section 3.5.3, « Chargement/téléchargement de fichiers à l'aide d'un serveur TFTP »
- Section 3.5.4, « Chargement/téléchargement de fichiers à l'aide d'un serveur SFTP »

Section 3.5.1

Chargement/téléchargement de fichiers à l'aide de XMODEM

Procédez comme suit pour charger ou télécharger un fichier à l'aide de XMODEM :

REMARQUE
Cette méthode requiert un ordinateur hôte comprenant une émulation de terminal ou le logiciel Telnet installé et qui est en mesure d'exécuter des transferts XMODEM.

1. Établissez une connexion entre l'appareil et l'ordinateur hôte. Pour plus d'informations, voir Section 2.1, « Connexion à ROS ».
2. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
3. Dans l'invite de commande de la CLI, entrez :

   ```
   xmodem [ send | receive ] nom de fichier
   ```

   Où :

   - `send` envoie le fichier à l'ordinateur hôte
   - `get` récupère le fichier de l'ordinateur hôte
   - *`nom de fichier`* est le nom du fichier (c'est-à-dire main.bin)

   REMARQUE
   *S'il est disponible dans l'émulation de terminal ou le logiciel Telnet, sélectionnez le protocole **XModem 1K** pour une transmission via l'option **XModem** standard.*

4. Lorsque l'appareil répond par`Press Ctrl-X to cancel`, lancez le transfert XMODEM depuis l'ordinateur hôte. L'appareil signale quand le transfert est achevé.

   Vous trouverez ci-après un exemple de shell CLI d'un transfert de fichier XMODEM réussi :

   ```
   >xmodem receive main.bin
   Press Ctrl-X to cancel
   ```

```
Receiving data now ...C
Received 1428480 bytes. Closing file main.bin ...
main.bin transferred successfully
```

5. Si le fichier a été chargé, réinitialisez l'appareil. Pour plus d'informations, voir Section 3.13, « Réinitialisation de l'appareil ».

Section 3.5.2

Chargement/téléchargement de fichiers à l'aide d'un client TFTP

Procédez comme suit pour charger ou télécharger un fichier à l'aide d'un client TFTP :

IMPORTANT !
TFTP ne définit pas de schéma d'authentification. Toute utilisation d'un client ou serveur TFTP est considérée comme très risquée.

REMARQUE
Cette méthode requiert un serveur TFTP accessible via le réseau.

1. Identifiez l'adresse IP de l'ordinateur exécutant le serveur TFTP.
2. Établissez une connexion entre l'appareil et l'ordinateur hôte. Pour plus d'informations, voir Section 2.1, « Connexion à ROS ».
3. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
4. Dans l'invite de commande de la CLI, entrez :

   ```
   tftp address [ get | put ] source-filename destination-filename
   ```

   Où :

   - `get` copie des fichiers de l'ordinateur hôte vers l'appareil
   - `get` copie des fichiers de l'appareil vers l'ordinateur hôte
   - *`adresse`* est l'adresse IP de l'ordinateur exécutant le serveur TFTP
   - *`nom de fichier source`* est le nom du fichier à transférer
   - *`nom de fichier de destination`* est le nom du fichier (sur l'appareil ou le serveur TFTP) qui sera remplacé lors du transfert

   Vous trouverez ci-après un exemple de transfert de fichier SFTP client réussi :

   ```
   >tftp 10.0.0.1 get ROS-CF52_Main_v4.3.0.bin main.bin
   TFTP CMD: main.bin transfer ok. Please wait, closing file ...
   TFTP CMD: main.bin loading successful.
   ```

5. Si le fichier a été chargé, réinitialisez l'appareil. Pour plus d'informations, voir Section 3.13, « Réinitialisation de l'appareil ».

Section 3.5.3

Chargement/téléchargement de fichiers à l'aide d'un serveur TFTP

Procédez comme suit pour charger ou télécharger un fichier à l'aide d'un serveur TFTP :

IMPORTANT !
TFTP ne définit pas de schéma d'authentification. Toute utilisation d'un client ou serveur TFTP est considérée comme très risquée.

REMARQUE
Cette méthode requiert un ordinateur hôte sur lequel le logiciel de serveur TFTP est installé.

IMPORTANT !
L'interaction avec des serveurs TFTP est strictement contrôlée au sein de l'appareil pour éviter les accès non autorisés. Assurez-vous que l'appareil est configuré de manière à accepter la connexion TFTP. Pour plus d'informations, voir Section 3.10, « Configuration des services IP ».

1. Établissez une connexion entre l'appareil et l'ordinateur hôte. Pour plus d'informations, voir Section 2.1, « Connexion à ROS ».
2. Initialisez le serveur TFTP sur l'ordinateur hôte et lancez le transfert TFTP. Le serveur indique lorsque le transfert est achevé.

   Vous trouverez ci-après un exemple d'échange de serveur TFTP réussi :

   ```
   C:\>tftp -i 10.1.0.1 put C:\files\ROS-CF52_Main_v4.3.0.bin main.bin
   Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
   ```

3. Si le fichier a été chargé, réinitialisez l'appareil. Pour plus d'informations, voir Section 3.13, « Réinitialisation de l'appareil ».

Section 3.5.4

Chargement/téléchargement de fichiers à l'aide d'un serveur SFTP

SFTP (Secure File Transfer Protocol) est un mécanisme de transfert de fichiers qui utilise SSH pour chiffrer tous les aspects du transfert de fichiers entre un client et un serveur en réseau.

REMARQUE
L'appareil n'a pas de client SFTP et, pour cette raison, peut uniquement recevoir des fichiers SFTP d'une source externe. SFTP requiert une authentification pour le transfert de fichiers.

Procédez comme suit pour charger ou télécharger un fichier à l'aide d'un serveur SFTP :

REMARQUE
Cette méthode requiert un ordinateur hôte sur lequel le logiciel de client SFTP est installé.

1. Établissez une connexion SFTP entre l'appareil et l'ordinateur hôte.

2. Lancez le transfert SFTP. Le client signale quand le transfert est achevé.

   Vous trouverez ci-après un exemple d'échange de serveur SFTP réussi :

```
user@host$ sftp admin@ros_ip
Connecting to ros_ip...
admin@ros_ip's password:
sftp> put ROS-CF52_Main_v4.3.0.bin main.bin
Uploading ROS-CF52_Main_v4.3.0.bin to /main.bin
ROS-CF52_Main_v4.3.0.bin 100% 2139KB 48.6KB/s 00:44
sftp> put ROS-MPC83_Main_v4.3.0.bin main.bin
Uploading ROS-MPC83_Main_v4.3.bin to /main.bin
ROS-MPC83_Main_v4.3.0.bin 100% 2139KB 48.6KB/s 00:44
sftp>
```

3. Si le fichier a été chargé, réinitialisez l'appareil. Pour plus d'informations, voir Section 3.13, « Réinitialisation de l'appareil ».

Section 3.6

Gestion de journaux

Les fichiers journaux d'incidents (`crashlog.txt`) et système (`syslog.txt`) contiennent de informations historiques sur les événements qui se sont produits pendant le fonctionnement de l'appareil.

Le journal d'incidents contient des informations de débogage liées aux problèmes ayant provoqué un redémarrage non planifié de l'appareil ou ayant pu affecter le fonctionnement de l'appareil. Un fichier de taille 0 octet indique qu'aucun événement non attendu ne s'est produit.

Le journal système contient un enregistrement d'événements significatifs, notamment les démarrages, les modifications de configuration, les mises à niveau de firmware et les réinitialisations de bases de données en raison de nouvelles fonctionnalités. Le journal système accumule des informations jusqu'à être plein. Il peut contenir environ 2 Mo de données.

SOMMAIRE

- Section 3.6.1, « Affichage de journaux locaux et système »
- Section 3.6.2, « Effacement de journaux locaux et système »
- Section 3.6.3, « Configuration du journal système local »
- Section 3.6.4, « Gestion de la journalisation distante »

Section 3.6.1

Affichage de journaux locaux et système

Les journaux d'incidents et système peuvent être téléchargés depuis l'appareil et affichés dans un éditeur de texte. Pour plus d'informations sur le téléchargement de fichiers-journaux, voir Section 3.5, « Chargement/téléchargement de fichiers ».

Pour afficher le journal système via l'interface Web, accédez à ***Diagnostics » View System Log***. Le formulaire **syslog.txt** s'affiche.

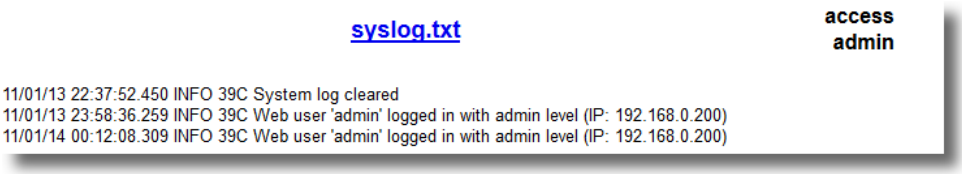


Figure 11 : Formulaire syslog.txt

Section 3.6.2

Effacement de journaux locaux et système

Pour effacer les journaux d'incidents locaux et système, connectez-vous au shell CLI et saisissez :

```
clearlogs
```

Pour effacer uniquement le journal système local, connectez-vous à l'interface Web et procédez comme suit :

1. Accédez à ***Diagnostics » Clear System Log***. Le formulaire **Clear System Log** s'affiche.

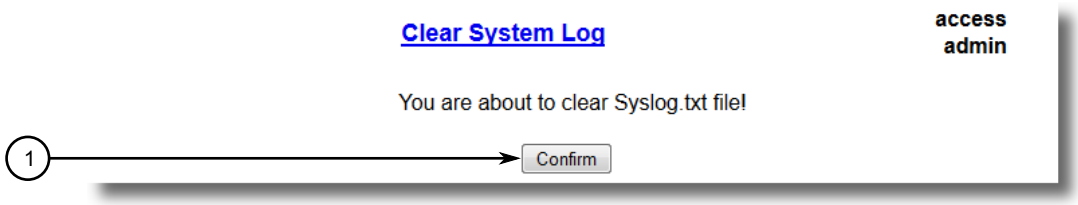


Figure 12 : Formulaire Clear System Log

1. Bouton Confirm

2. Cliquez sur **Confirm**.

Section 3.6.3

Configuration du journal système local

Procédez comme suit pour configurer le degré de gravité du journal système local :

> **REMARQUE**
> *Utilisez la journalisation distante pour une fiabilité optimale. Pour plus d'informations, voir Section 3.6.4, « Gestion de la journalisation distante ».*

1. Accédez à ***Administration » Configure Syslog » Configure Local Syslog***. Le formulaire **Local Syslog** s'affiche.

Figure 13 : Formulaire Local Syslog

1. Local Syslog Level **2.** Bouton Apply **3.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Local Syslog Level	**Synopsis :** { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING } **Par défaut :** INFORMATIONAL Degré de gravité du message généré. Notez que le degré de gravité sélectionné est considéré comme degré de gravité minimum pour le système. Par exemple, si ERROR est sélectionnés, le système envoie les messages syslog générés par Error, Critical, Alert et Emergency.

3. Cliquez sur **Apply**.

Section 3.6.4

Gestion de la journalisation distante

Outre le journal système local mis à jour sur l'appareil, un journal système distant peut être également configuré pour collecter des messages d'événement importants. Le journal système se trouve sur l'appareil et prend en charge 5 collecteurs (ou serveurs Syslog).

Le protocole de journal système distant, défini dans RFC 3164, est un transport basé sur UDP/IP qui permet à l'appareil d'envoyer des messages de notification d'événement dans des réseaux vers des collecteurs de messages d'événement, également appelés serveurs syslog. Le protocole est conçu pour transporter simplement ces messages d'événement de l'appareil qui les génère vers le(s) collecteur(s).

SOMMAIRE

- Section 3.6.4.1, « Configuration du client Syslog distant »
- Section 3.6.4.2, « Affichage d'une liste de serveurs Syslog distants »
- Section 3.6.4.3, « Ajout d'un serveur Syslog distant »
- Section 3.6.4.4, « Suppression d'un serveur Syslog distant »

Section 3.6.4.1

Configuration du client Syslog distant

Procédez comme suit pour configurer le client Syslog distant :

1. Accédez à ***Administration » Configure Syslog » Configure Remote Syslog Client***. Le formulaire **Remote Syslog Client** s'affiche.

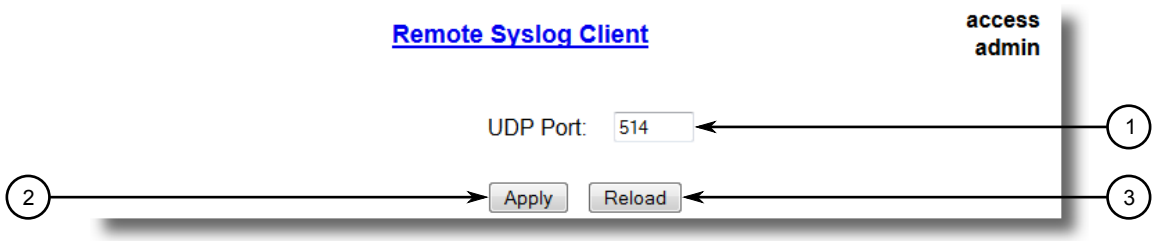


Figure 14 : Formulaire Remote Syslog Client

1. UDP Port **2.** Bouton Apply **3.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
UDP Port	**Synopsis :** 1025 à 65535 ou { 514 } **Par défaut :** 514 Port UDP local via lequel le client envoie des informations au(x) serveur(s).

3. Cliquez sur **Apply**.

Section 3.6.4.2

Affichage d'une liste de serveurs Syslog distants

Pour afficher une liste de serveurs Syslog distants connus, accédez à ***Administration » Configure Syslog » Configure Remote Syslog Server***. Le tableau **Remote Syslog Server** s'affiche.

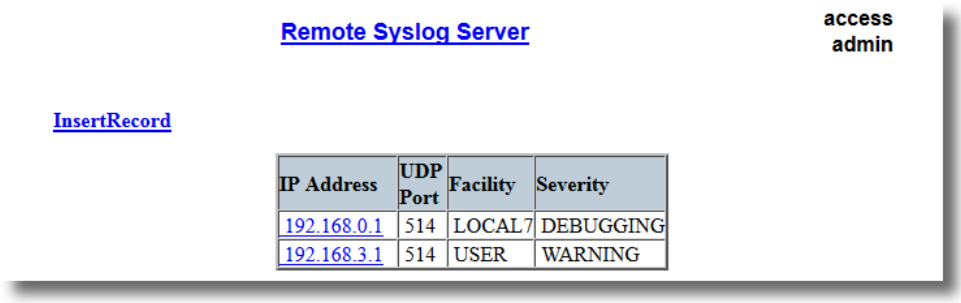


Figure 15 : Tableau Remote Syslog Server

Si aucun serveur Syslog n'a été configuré, ajoutez des serveurs en fonction de vos besoins. Pour plus d'informations, voir Section 3.6.4.3, « Ajout d'un serveur Syslog distant ».

Section 3.6.4.3

Ajout d'un serveur Syslog distant

RUGGEDCOM ROS prend en charge jusqu'à 5 serveurs Syslog distants. De manière similaire au journal système local, un serveur de journal système distant peut être configuré de manière à journaliser des informations à un niveau de sécurité spécifique. Seuls les messages d'un niveau de gravité égal ou supérieur au niveau de sécurité spécifié sont écrits dans le journal.

Procédez comme suit pour ajouter un serveur Syslog à la liste des serveurs connus :

1. Accédez à ***Administration » Configure Syslog » Configure Remote Syslog Server***. Le tableau **Remote Syslog Server** s'affiche.

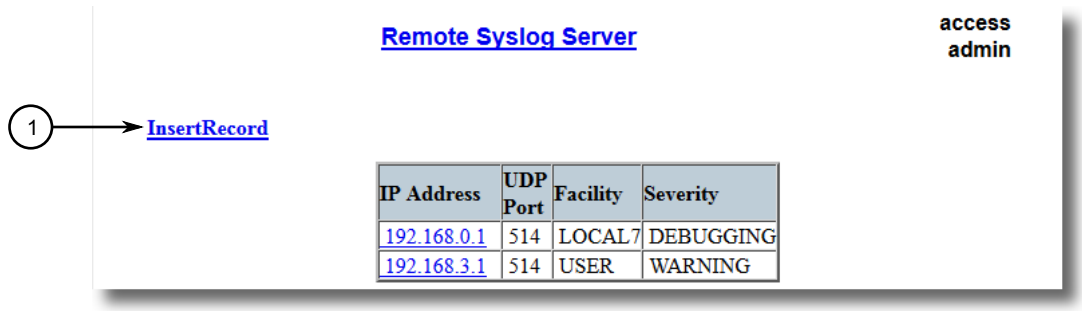


Figure 16 : Tableau Remote Syslog Server

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **Remote Syslog Server** s'affiche.

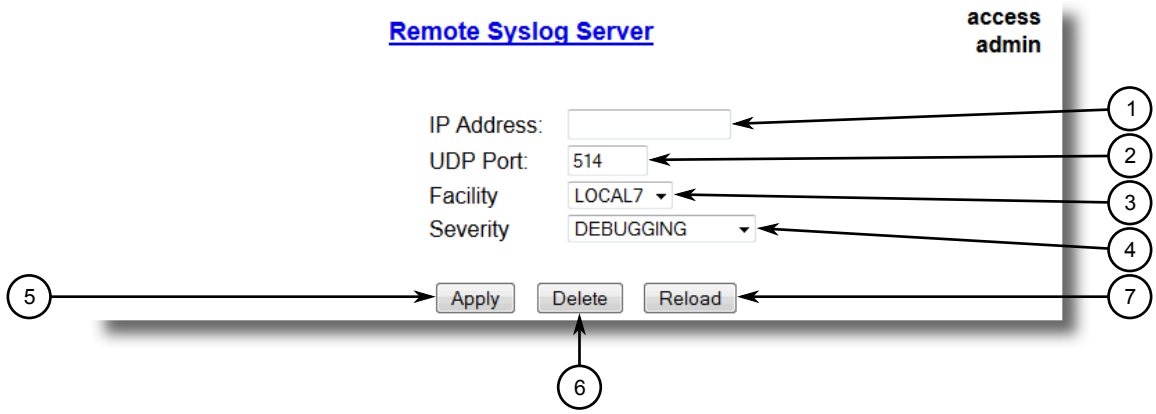


Figure 17 : Formulaire Remote Syslog Server

1. Zone IP Address **2.** Zone UDP Port **3.** Zone Facility **4.** Zone Severity **5.** Bouton Apply **6.** Bouton Delete **7.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
IP Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Adresse IP du serveur Syslog.

Paramètre	Description
UDP Port	**Synopsis :** 1025 à 65535 ou { 514 } **Par défaut :** 514 Numéro de port UDP sur lequel le serveur distant écoute.
Facility	**Synopsis :** { USER, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 } **Par défaut :** LOCAL7 L'utilitaire syslog est un champ d'information associé à un message syslog. L'utilitaire syslog est le composant d'application ou de système d'exploitation qui génère un message de journal. ROS mappe toutes les informations de journalisation dans un utilitaire unique configurable par l'utilisateur pour soulager le serveur syslog distant.
Severity	**Synopsis :** { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING } **Par défaut :** DEBUGGING Le degré de gravité est la gravité du message généré. Veuillez noter que le degré de gravité sélectionné par l'utilisateur est considéré comme degré de gravité minimum pour le système. Par exemple, si l'utilisateur sélectionne 'Error' comme degré de gravité, le système envoie les messages syslog générés par Error, Critical, Alert et Emergency.

4. Cliquez sur **Apply**.

Section 3.6.4.4

Suppression d'un serveur Syslog distant

Procédez comme suit pour supprimer un serveur Syslog de la liste des serveurs connus :

1. Accédez à ***Administration » Configure Syslog » Configure Remote Syslog Server***. Le tableau **Remote Syslog Server** s'affiche.

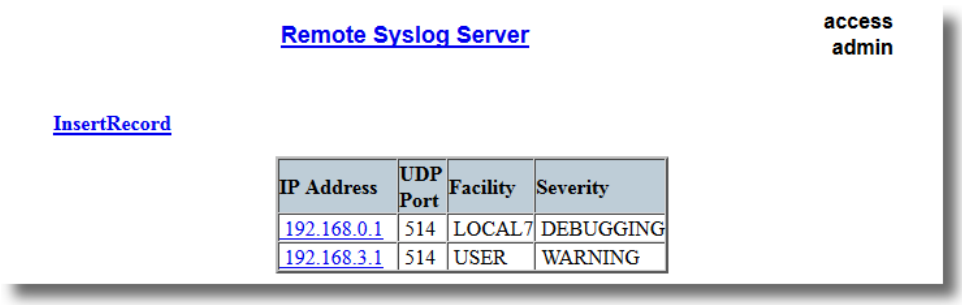


Figure 18 : Tableau Remote Syslog Server

2. Sélectionnez le serveur dans le tableau. Le formulaire **Remote Syslog Server** s'affiche.

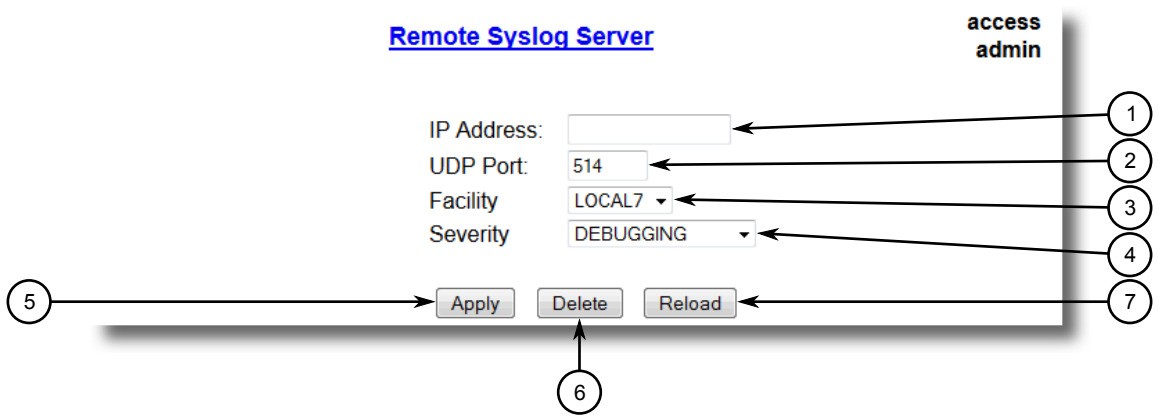


Figure 19 : Formulaire Remote Syslog Server

1. Zone IP Address **2.** Zone UDP Port **3.** Zone Facility **4.** Zone Severity **5.** Bouton Apply **6.** Bouton Delete **7.** Bouton Reload

3. Cliquez sur **Delete**.

Section 3.7

Gestion de ports Ethernet

Cette section décrit la manière de gérer les ports Ethernet.

REMARQUE
Pour plus d'informations sur la configuration de la surveillance à distance de ports Ethernet, voir Section 3.11, « Gestion de la surveillance à distance ».

SOMMAIRE

- Section 3.7.1, « Protection du contrôleur via l'indication de défaillance de liaison (Link Fault Indication, LFI) »
- Section 3.7.2, « Visualisation de l'état de ports Ethernet »
- Section 3.7.3, « Affichage des statistiques pour tous les ports Ethernet »
- Section 3.7.4, « Affichage de statistiques pour des ports Ethernet spécifiques »
- Section 3.7.5, « Effacement de statistiques pour des ports Ethernet spécifiques »
- Section 3.7.6, « Configuration d'un port Ethernet »
- Section 3.7.7, « Configuration de la limitation du débit de port »
- Section 3.7.8, « Configuration de la mise en miroir de ports »
- Section 3.7.9, « Configuration de la détection de liaison »
- Section 3.7.10, « Gestion d'émetteurs-récepteurs SFP »
- Section 3.7.11, « Gestion des ports PoE »
- Section 3.7.12, « Détection de défauts de câble »
- Section 3.7.13, « Réinitialisation de ports Ethernet »

Section 3.7.1

Protection du contrôleur via l'indication de défaillance de liaison (Link Fault Indication, LFI)

Les contrôleurs modernes industriels sont souvent dotés de ports Ethernet de sauvegarde utilisés en cas de défaillance de liaison. Lorsque ces interfaces sont prises en charge par un support (par ex. fibre) employant des chemins de transmission et de réception séparés, l'interface peut être vulnérable aux défaillances se produisant uniquement sur l'un des deux chemins.

Prenez par exemple deux commutateurs (A et B) connectés à un contrôleur. Le commutateur A est connecté au port principal sur le contrôleur, alors que le commutateur B est connecté au port de sauvegarde, qui est fermé par le contrôleur pendant que la liaison avec le commutateur A est active. Le commutateur B doit transmettre des trames vers le contrôleur via le commutateur A.

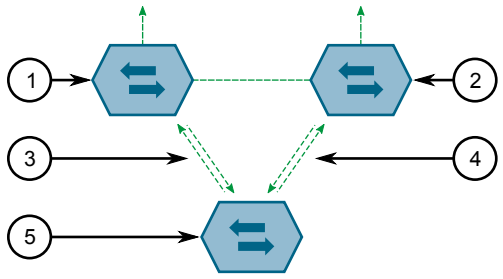


Figure 20 : Exemple

1. Commutateur A **2.** Commutateur B **3.** Chemin de transmission principal **4.** Chemin de transmission de sauvegarde **5.** Contrôleur

Si le chemin de transmission du contrôleur au commutateur A est défaillant, le commutateur A génère un signal de liaison au contrôleur via le chemin de réception. Le contrôleur continue à détecter la liaison avec le commutateur A et ne bascule pas sur le port de sauvegarde.

Cette situation illustre le besoin d'une méthode de notification indiquant à un partenaire de liaison quand l'intégrité du signal liaison est interrompue. Une telle méthode existe de manière native dans certains supports de liaison mais pas dans tous.

100Base-TX, 1000Base-T, 1000Base-X	Comprend une fonctionnalité de négociation automatique intégrée (par exemple une balise spéciale appelée Remote Fault Indication est définie dans le signal de négociation automatique transmis).
Liaisons 100Base-FX	Comprend une fonctionnalité FEFI (Far-End-Fault-Indication) définie par la norme IEEE 802.3 pour ce type de liaison. Cette fonctionnalité comprend : • **FEFI de transmission** Transmet un signal d'intégrité de liaison modifié en cas de détection d'une défaillance de liaison (c'est-à-dire qu'aucun signal n'est reçu du partenaire de liaison). • **FEFI de détection** Indique la perte de liaison dans le cas où un signal FEFI est reçu du partenaire de liaison.
Liaisons 10Base-FL	Aucun support standard.

Les liaisons 10Base-FL ne sont pas dotées d'un mécanisme de notification de partenaire de liaison natif et la prise en charge de FEFI dans les liaisons 100Base-FX est optionnelle selon la norme IEEE 802.3, ce qui signifie que certains partenaires de liaison peuvent ne pas la prendre en charge.

Siemens propose une fonctionnalité LFI (Link-Fault-Indication) avancée pour les liaisons qui ne sont pas dotées d'un mécanisme de notification du partenaire de liaison natif. Lorsque la LFI est activée, l'appareil base la

génération d'un signal d'intégrité de liaison en fonction de la réception d'un signal de liaison. Dans l'exemple décrit auparavant, si le commutateur A ne reçoit pas de signal de liaison du contrôleur, il arrête la génération d'un signal de liaison. Le contrôleur détecte la défaillance de liaison et bascule sur le port de sauvegarde.

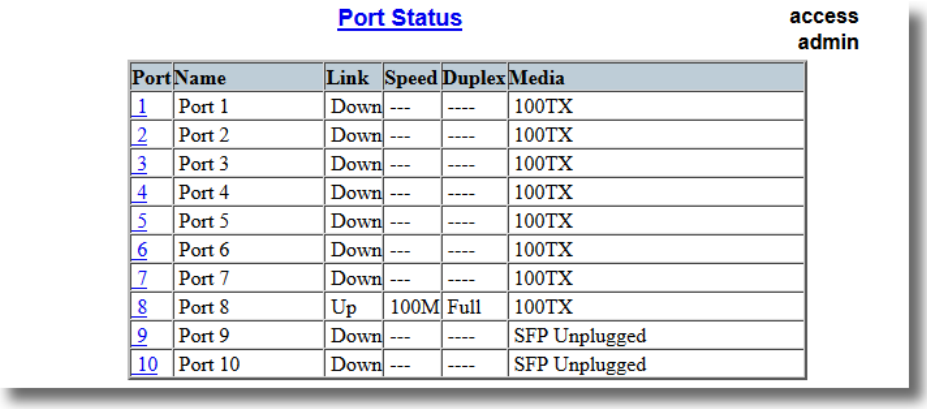
IMPORTANT !
*Si les deux partenaires de liaison sont dotés de la fonctionnalité LFI, il ne **doit pas** être activé aux deux extrémités de la liaison. Si elle est activée aux deux extrémités, la liaison ne sera jamais établie, car chaque partenaire de liaison attend que l'autre transmette le signal de liaison.*

Le commutateur peut également être configuré de manière à remettre à zéro le tableau MAC address pour le port contrôleur. Les trames destinées au contrôleur seront dirigées vers le commutateur B où elles seront transmises au contrôleur (une fois que le contrôleur transmet sa première trame).

Section 3.7.2

Visualisation de l'état de ports Ethernet

Pour afficher l'état actuel de chaque port Ethernet, accédez à ***Ethernet Ports » View Port Status***. Le tableau **Port Status** s'affiche.



Port Status

access admin

Port	Name	Link	Speed	Duplex	Media
1	Port 1	Down	---	----	100TX
2	Port 2	Down	---	----	100TX
3	Port 3	Down	---	----	100TX
4	Port 4	Down	---	----	100TX
5	Port 5	Down	---	----	100TX
6	Port 6	Down	---	----	100TX
7	Port 7	Down	---	----	100TX
8	Port 8	Up	100M	Full	100TX
9	Port 9	Down	---	----	SFP Unplugged
10	Port 10	Down	---	----	SFP Unplugged

Figure 21 : Tableau Port Status

Ce tableau affiche les informations suivantes :

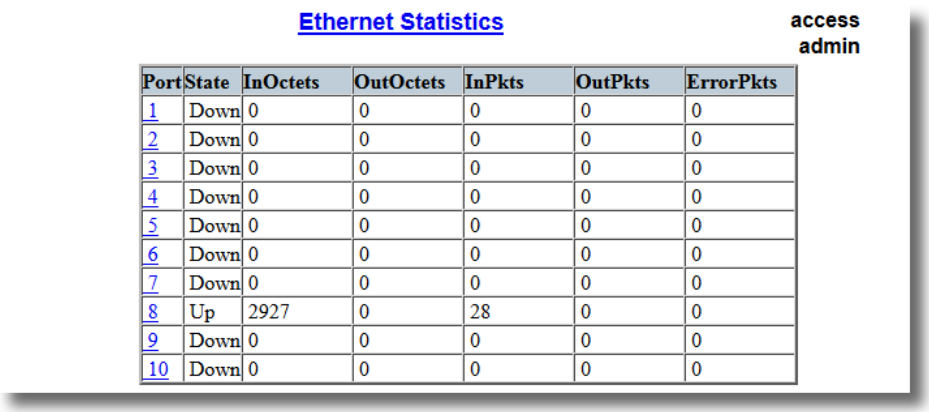
Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Name	**Synopsis :** 15 caractères quelconques Un nom descriptif pouvant être utilisé pour identifier l'appareil connecté à ce port.
Link	**Synopsis :** { ----, ----, Down, Up } État de la liaison du port.
Speed	**Synopsis :** { ---, 10M, 100M, 1G, 10G } Vitesse actuelle du port.
Duplex	**Synopsis :** { ----, Half, Full }

Paramètre	Description
	État de duplex actuel du port.

Section 3.7.3

Affichage des statistiques pour tous les ports Ethernet

Pour afficher les statistiques collectées pour tous les ports Ethernet, accédez à ***Ethernet Stats » View Ethernet Statistics***. Le tableau **Ethernet Statistics** s'affiche.



Ethernet Statistics

access admin

Port	State	InOctets	OutOctets	InPkts	OutPkts	ErrorPkts
1	Down	0	0	0	0	0
2	Down	0	0	0	0	0
3	Down	0	0	0	0	0
4	Down	0	0	0	0	0
5	Down	0	0	0	0	0
6	Down	0	0	0	0	0
7	Down	0	0	0	0	0
8	Up	2927	0	28	0	0
9	Down	0	0	0	0	0
10	Down	0	0	0	0	0

Figure 22 : Tableau Ethernet Statistics

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
State	**Synopsis :** { ----, ----, Down, Up }
InOctets	**Synopsis :** 0 à 4294967295 Nombre d'octets dans des paquets bons (monodiffusion+multidiffusion+diffusion) et abandonnés reçus.
OutOctets	**Synopsis :** 0 à 4294967295 Nombre d'octets dans les paquets bons transmis.
InPkts	**Synopsis :** 0 à 4294967295 Nombre de paquets bons (monodiffusion+multidiffusion+diffusion) et abandonnés reçus.
OutPkts	**Synopsis :** 0 à 4294967295 Nombre de paquets bons transmis.
ErrorPkts	**Synopsis :** 0 à 4294967295 Nombre de types quelconques de paquets erronés.

Section 3.7.4

Affichage de statistiques pour des ports Ethernet spécifiques

Pour afficher les statistiques collectées pour des ports Ethernet spécifiques, accédez à ***Ethernet Stats » View Ethernet Port Statistics***. Le tableau **Ethernet Port Statistics** s'affiche.

Ethernet Port Statistics access admin

Port	InOctets	OutOctets	InPkts	OutPkts	TotalInOctets	Tot:
1	2374236	2157956	13627	32698	2374236	136
2	192516	2399229	2049	33996	192516	204
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	10077906	314359	104258	1010	10077906	104
9	0	0	0	0	0	0
10	0	0	0	0	0	0

Figure 23 : Tableau Ethernet Port Statistics

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
InOctets	**Synopsis :** 0 à 18446744073709551615 Nombre d'octets dans des paquets bons (monodiffusion+multidiffusion+diffusion) et abandonnés reçus.
OutOctets	**Synopsis :** 0 à 18446744073709551615 Nombre d'octets dans les paquets bons transmis.
InPkts	**Synopsis :** 0 à 18446744073709551615 Nombre de paquets bons (monodiffusion+multidiffusion+diffusion) et abandonnés reçus.
OutPkts	**Synopsis :** 0 à 18446744073709551615 Nombre de paquets bons transmis.
TotalInOctets	**Synopsis :** 0 à 18446744073709551615 Nombre total d'octets de tous les paquets reçus. Il comprend les octets de données de paquets rejetés et locaux qui ne sont pas transférés vers le cœur de commutation pour être transmis. Il doit refléter tous les octets de données reçus sur la ligne.
TotalInPkts	**Synopsis :** 0 à 18446744073709551615 Nombre de paquets reçus. Il comprend les paquets rejetés, annulés et locaux qui ne sont pas transférés vers le cœur de commutation pour être transmis. Il doit refléter tous les paquets reçus sur la ligne.
InBroadcasts	**Synopsis :** 0 à 18446744073709551615 Nombre de bons paquets de diffusion reçus.
InMulticasts	**Synopsis :** 0 à 18446744073709551615

Paramètre	Description
	Nombre de bons paquets multidiffusion reçus.
CRCAlignErrors	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus répondant à toutes les conditions suivantes : • La longueur de données du paquet est de 64 à 1 536 octets inclus. • Le paquet a un CRC invalide. • Aucun événement de collision n'a été détecté. • Aucun événement Late Collision n'a été détecté.
OversizePkts	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus avec une longueur de données supérieure à 1 536 octets et un CRC valide.
Fragments	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus répondant à toutes les conditions suivantes : • La longueur de données du paquet est inférieure à 64 octets, ou un paquet n'a pas de SFD et a une longueur inférieure à 64 octets. • Aucun événement de collision n'a été détecté. • Aucun événement Late Collision n'a été détecté. • Le paquet a un CRC invalide.
Jabbers	**Synopsis :** 0 à 4294967295 Nombre de paquets répondant à toutes les conditions suivantes : • La longueur de données du paquet est de 1 536 octets. • Le paquet a un CRC invalide.
Collisions	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus pour lesquels l'événement Collision a été détecté.
LateCollisions	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus pour lesquels l'événement Late Collision a été détecté.
Pkt64Octets	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus et transmis avec une taille de 64 octets. Il comprend des paquets reçus et transmis, ainsi que des paquets annulés et locaux reçus. Cela n'inclut pas les paquets reçus rejetés.
Pkt65to127Octets	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus et transmis avec une taille de 65 à 127 octets. Il comprend des paquets reçus et transmis, ainsi que des paquets annulés et locaux reçus. Cela n'inclut pas les paquets reçus rejetés.
Pkt128to255Octets	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus et transmis avec une taille de 128 à 257 octets. Il comprend des paquets reçus et transmis, ainsi que des paquets annulés et locaux reçus. Cela n'inclut pas les paquets reçus rejetés.
Pkt256to511Octets	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus et transmis avec une taille de 256 à 511 octets. Il comprend des paquets reçus et transmis, ainsi que des paquets annulés et locaux reçus. Cela n'inclut pas les paquets reçus rejetés.
Pkt512to1023Octets	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus et transmis avec une taille de 512 à 1 023 octets. Il comprend des paquets reçus et transmis, ainsi que des paquets annulés et locaux reçus. Cela n'inclut pas les paquets reçus rejetés.
Pkt1024to1536Octets	**Synopsis :** 0 à 4294967295

Paramètre	Description
	Nombre de paquets reçus et transmis avec une taille de 1 024 à 1 536 octets. Il comprend des paquets reçus et transmis, ainsi que des paquets annulés et locaux reçus. Cela n'inclut pas les paquets reçus rejetés.
DropEvents	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus abandonnés en raison d'un manque de tampons de réception.
OutMulticasts	**Synopsis :** 0 à 18446744073709551615 Nombre de paquets multidiffusion transmis. Cela n'inclut pas les paquets de diffusion.
OutBroadcasts	**Synopsis :** 0 à 18446744073709551615 Nombre de paquets de diffusion transmis.
UndersizePkts	**Synopsis :** 0 à 4294967295 Nombre de paquets reçus répondant à toutes les conditions suivantes : • La longueur de données du paquet est inférieure à 64 octets. • Aucun événement de collision n'a été détecté. • Aucun événement Late Collision n'a été détecté. • Le paquet a un CRC valide.

Section 3.7.5

Effacement de statistiques pour des ports Ethernet spécifiques

Procédez comme suit pour effacer les statistiques collectées pour un ou plusieurs ports Ethernet :

1. Accédez à ***Ethernet Stats » Clear Ethernet Port Statistics***. Le formulaire **Clear Ethernet Port Statistics** s'affiche.

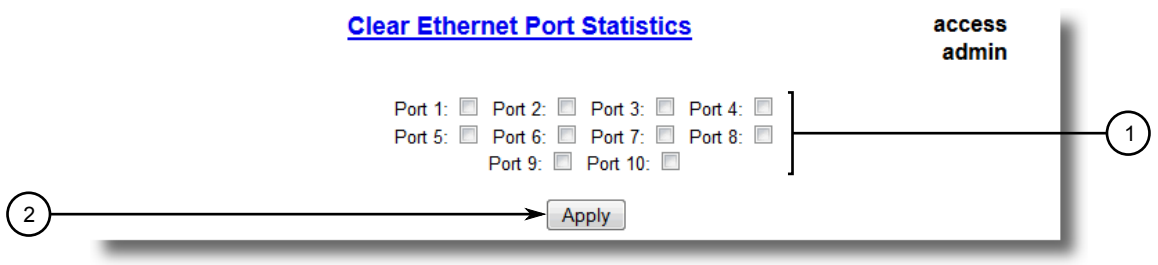


Figure 24 : Formulaire Clear Ethernet Port Statistics (typique)

1. Zones Port Check **2.** Bouton Confirm

2. Sélectionnez un ou plusieurs ports Ethernet.
3. Cliquez sur **Confirm**.

Section 3.7.6

Configuration d'un port Ethernet

Procédez comme suit pour configurer un port Ethernet :

REMARQUE
En fonction du type de support de liaison requis, un port SFP peut nécessiter une configuration explicite. Avant de configurer un port SFP, référez-vous à Section 3.7.10.1, « Configuration d'un port SFP ».

1. Accédez à ***Ethernet Ports » Configure Port Parameters***. Le tableau **Port Parameters** s'affiche.

Port Parameters

access
admin

Port	Name	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1	Port 1	100TX	Enabled	On	Auto	Auto	Off	Off	On
2	Port 2	100TX	Enabled	On	Auto	Auto	Off	Off	On
3	Port 3	100TX	Enabled	On	Auto	Auto	Off	Off	On
4	Port 4	100TX	Enabled	On	Auto	Auto	Off	Off	On
5	Port 5	100TX	Enabled	On	Auto	Auto	Off	Off	On
6	Port 6	100TX	Enabled	On	Auto	Auto	Off	Off	On
7	Port 7	100TX	Enabled	On	Auto	Auto	Off	Off	On
8	Port 8	100TX	Enabled	On	Auto	Auto	Off	Off	On
9	Port 9	1000X	Enabled	On	1G	Full	Off	Off	On
10	Port 10	1000X	Enabled	On	1G	Full	Off	Off	On

Figure 25 : Tableau Port Parameters

2. Sélectionnez un port Ethernet. Le formulaire **Port Parameters** s'affiche.

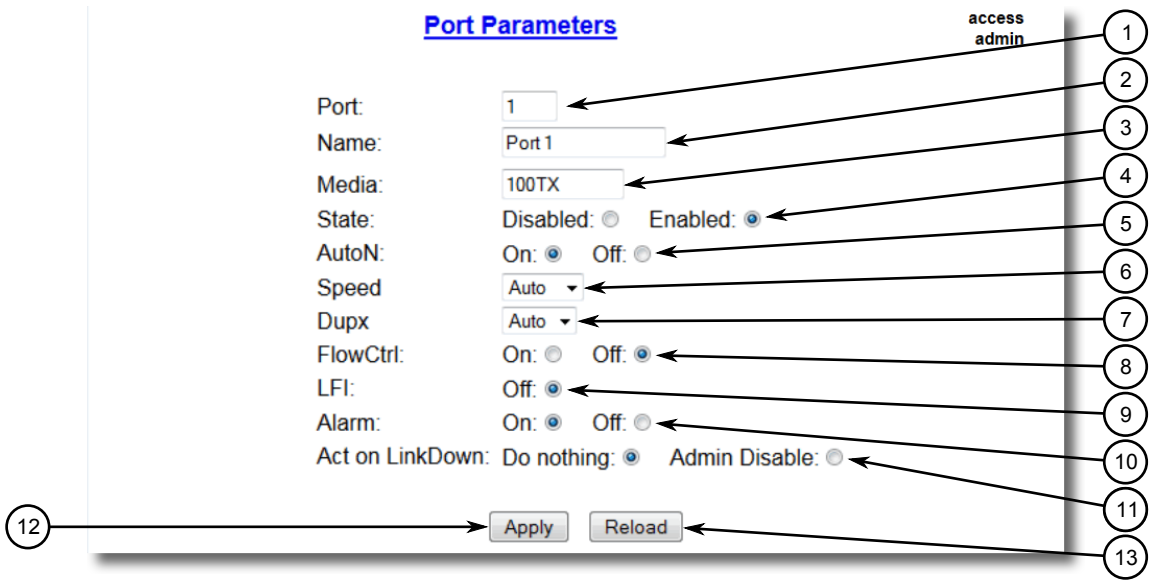


Figure 26 : Formulaire Paramètres Radius

1. Zone Port **2.** Zone Name **3.** Zone Media **4.** Options State **5.** Options AutoN **6.** Liste Speed **7.** Liste Dupx **8.** Options FlowCtrl **9.** Option LFI **10.** Options Alarm **11.** Options Act on LinkDown **12.** Bouton Apply **13.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Name	**Synopsis :** 15 caractères quelconques **Par défaut :** Port x Un nom descriptif pouvant être utilisé pour identifier l'appareil connecté à ce port.
Media	**Synopsis :** { 100TX, 10FL, 100FX, 1000X, 1000T, 802.11g, EoVDSL, 100TX Only, 10FL/100SX, 10GX } **Par défaut :** 100TX Type de support de port.
State	**Synopsis :** { Disabled, Enabled } **Par défaut :** Enabled La désactivation d'un port empêche l'envoi et la réception des trames sur ce port. De plus, en cas de désactivation, le signal d'intégrité de liaison n'est pas envoyé et la LED de lien/d'activité n'est jamais allumée. Vous pouvez désactiver un port pour le dépannage ou la sécurisation de connexions non autorisées. **REMARQUE** *La désactivation d'un port de type **802.11g** désactive le module sans fil correspondant.*
AutoN	**Synopsis :** { Off, On } **Par défaut :** On Active ou désactive la négociation automatique IEEE 802.3. L'activation de la négociation automatique entraîne la négociation de la vitesse et du duplex lors de la détection de

Paramètre	Description
	liaison. Les deux appareils terminaux doivent être compatibles avec la négociation automatique pour obtenir les meilleurs résultats possibles. Les supports 10 Mbit/s et 100 Mbit/s en fibre optique ne prennent pas en charge la négociation automatique. Ils doivent donc être configurés de manière explicite en semi-duplex ou en duplex intégral. Le fonctionnement en semi-duplex requiert que les deux extrémités soient configurées comme telles, ou une perte importante de trame peut se produire en cas de trafic réseau dense.
Speed	**Synopsis :** { Auto, 10M, 100M, 1G } **Par défaut :** Auto Vitesse (en mégabits par seconde ou en gigabits par seconde). Si la négociation automatique est activée, il s'agit de la capacité de vitesse annoncée par le processus de négociation automatique. Si la négociation automatique est désactivée, le port est forcé de manière explicite sur ce mode de vitesse. AUTO signifie l'annonce de tous les modes de vitesse pris en charge.
Dupx	**Synopsis :** { Auto, Half, Full } **Par défaut :** Auto Mode duplex. Si la négociation automatique est activée, il s'agit de la capacité de duplex annoncée par le processus de négociation automatique. Si la négociation automatique est désactivée, le port est forcé de manière explicite sur ce mode de duplex. AUTO signifie l'annonce de tous les modes de duplex pris en charge.
Flow Control	**Synopsis :** { Off, On } **Par défaut :** On Le contrôle de flux est utile pour empêcher une perte de trame en cas de trafic réseau dense. Il peut s'agir par exemple de l'envoi de données par plusieurs ports source à un unique port de destination ou par un port à vitesse plus élevé à un port à vitesse plus réduite. Lorsque le port est en mode semi-duplex, vous pouvez utiliser pour cela la contrepression ('backpressure') où le commutateur simule des collisions entraînant une nouvelle tentative de transmission par l'appareil émetteur en fonction de l'algorithme de réémission Ethernet. Lorsque le port est en mode duplex intégral, vous pouvez utiliser des trames PAUSE, ce qui entraîne l'arrêt de la transmission par l'appareil émetteur pendant une période donnée.
LFI	**Synopsis :** { Off, On } **Par défaut :** Off L'activation du mécanisme d'indication de défaut de liaison (Link-Fault-Indication (LFI)) empêche la transmission du signal d'intégrité de liaison en cas d'échec de la liaison de réception. Cela permet à l'appareil à l'extrémité de détecter les défauts de liaison dans toutes les circonstances. **REMARQUE** *Cette fonctionnalité ne doit pas être activée aux deux extrémités d'une liaison par fibre.*
Alarm	**Synopsis :** { On, Off } **Par défaut :** On La désactivation des alarmes d'état de liaison empêche l'envoi d'alarmes et de traps SNMP actifs/interrompus (LinkUp / LinkDown) pour ce port.
Act on LinkDown	**Synopsis :** { Do nothing, Admin Disable } **Par défaut :** Do nothing Cette action peut être exécutée en cas d'événement de port LinkDown. Options possibles : • `Do nothing` – Aucune action n'est exécutée • `Admin Disable` – L'état de port est désactivé

REMARQUE
Si une extrémité de la liaison a une vitesse et un type de duplex fixes et si le pair négocie automatiquement, il y a une forte possibilité que la liaison ne soit pas activée ou soit activée avec des réglages erronés côté négociation automatique. Le pair de négociation automatique repassera en mode de fonctionnement semi-duplex même si le côté fixe est en duplex intégral. Le fonctionnement en duplex intégral requiert que les deux extrémités soient configurées comme telles, ou une perte importante de trame peut se produire en cas de trafic réseau dense. La liaison peut afficher quelques erreurs ou aucune si les volumes de trafic sont moins élevés. À mesure que le trafic devient plus intense, le côté négociation fixe commence à rencontrer des paquets abandonnés alors que le côté négociation automatique rencontre des collisions excessives. Finalement, lorsque la charge de trafic approche les 100 %, la liaison devient entièrement inutilisable. Ces problèmes peuvent être évités en configurant toujours des ports avec des valeurs fixes appropriées.

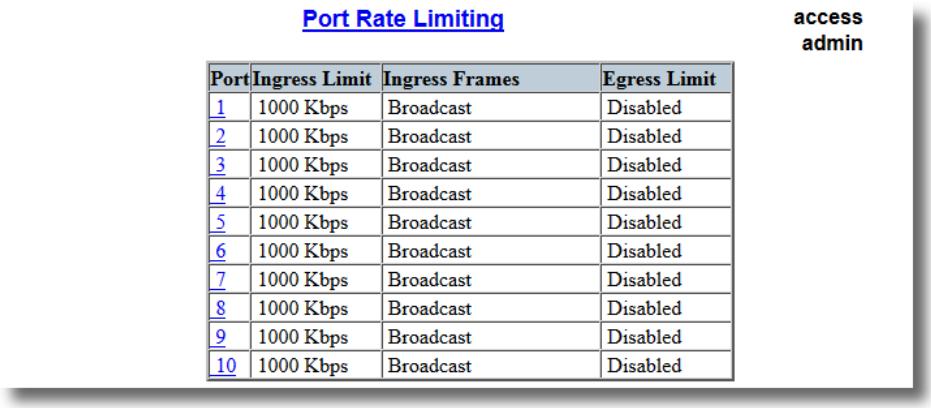
4. Cliquez sur **Apply**.

Section 3.7.7

Configuration de la limitation du débit de port

Procédez comme suit pour configurer la limitation du débit de port :

1. Accédez à ***Ethernet Ports » Configure Port Rate Limiting***. Le tableau **Port Rate Limiting** s'affiche.



Port	Ingress Limit	Ingress Frames	Egress Limit
1	1000 Kbps	Broadcast	Disabled
2	1000 Kbps	Broadcast	Disabled
3	1000 Kbps	Broadcast	Disabled
4	1000 Kbps	Broadcast	Disabled
5	1000 Kbps	Broadcast	Disabled
6	1000 Kbps	Broadcast	Disabled
7	1000 Kbps	Broadcast	Disabled
8	1000 Kbps	Broadcast	Disabled
9	1000 Kbps	Broadcast	Disabled
10	1000 Kbps	Broadcast	Disabled

Figure 27 : Tableau Port Rate Limiting

2. Sélectionnez un port Ethernet. Le formulaire **Port Rate Limiting** s'affiche.

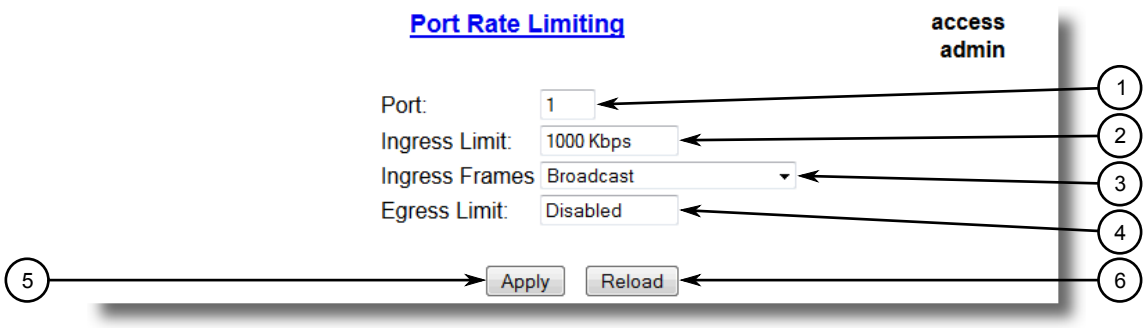


Figure 28 : Formulaire Port Rate Limiting

1. Zone Port **2.** Zone Ingress Limit **3.** Liste Ingress Frames **4.** Zone Egress Limit **5.** Bouton Apply **6.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Ingress Limit	**Synopsis :** 62 à 256000 Kbps ou { Disabled } **Par défaut :** 1000 Kbps Le débit auquel des trames reçues (du type décrit par le paramètre Ingress Frames) sont rejetées par le commutateur.
Ingress Frames	**Synopsis :** { Broadcast, Bcast&Mcast, Bcast&Mcast&FloodUcast, Bcast&FloodUcast, FloodUcast, All } **Par défaut :** Broadcast Ce paramètre spécifie les types de trame dont le débit doit être limité pour ce port. Il s'applique uniquement aux trames reçues : • Broadcast - uniquement les trames de diffusion • Bcast&Mcast - trames de diffusion et multidiffusion • Bcast&FloodUcast - trames de diffusion et monodiffusion saturées • Bcast&Mcast&FloodUcast - trames de diffusion, multidiffusion et monodiffusion saturées • FloodUcast - uniquement les trames monodiffusion saturées • All - toutes les trames (multidiffusion, diffusion et monodiffusion)
Egress Limit	**Synopsis :** { Broadcast, Multicast, Mcast&FloodUcast, All }">62 to 256000 Kbps or { Disabled } **Par défaut :** Disabled La fréquence maximum de transmission (multidiffusion, diffusion et monodiffusion) par le commutateur de trames sur ce port. Le commutateur rejette le cas échéant les trames afin de respecter cette fréquence.

4. Cliquez sur **Apply**.

Section 3.7.8

Configuration de la mise en miroir de ports

La mise en miroir de ports est un outil de dépannage qui copie, ou met en miroir, tout le trafic reçu ou transmis sur un port désigné vers un port miroir spécifié. Si un analyseur de protocole est attaché au port cible, le flux de trafic de trames valides sur tout port source devient disponible pour une analyse.

IMPORTANT !
Sélectionnez un port cible avec une vitesse plus élevée que celle du port source. La mise en miroir d'un port 100 Mbit/s vers un port 10 Mbit/s peut entraîner un flux mis en miroir incorrect.

IMPORTANT !
Les trames sont abandonnées si le débit duplex intégral des trames sur le port source dépasse la vitesse de transmission sur le port cible. Les trames transmises et reçues sur le port source étant mises en miroir vers le port cible, les trames sont abandonnées si le trafic total dépasse la vitesse de transmission du port cible. Ce problème est particulièrement sérieux si le trafic sur un port en duplex intégral 100 Mbit/s est mis en miroir sur un port en semi-duplex 10 Mbit/s

IMPORTANT !
Tenez compte des points suivants avant de configurer la mise en miroir de ports :

- *Le trafic est mis en miroir sur le port cible indépendamment son appartenance au VLAN. Elle peut être la même que celle du port source ou être différente.*
- *Les trames de gestion de réseau (telles que RSTP, GVRP etc.) ne peuvent pas être mises en miroir.*
- *Les trames de gestion de commutateurs générées par le commutateur (telles que Telnet, HTTP, SNMP, etc.) ne peuvent pas être mises en miroir.*

REMARQUE
Des trames incorrectes reçues sur le port source ne sont pas mises en miroir. Il s'agit notamment des erreurs CRC, de paquets dont la tailles est trop importante ou trop petite, de fragments, de transmissions anormalement longues, de collisions, de collisions en retard et d'événements abandonnés.

Procédez comme suit pour configurer la mise en miroir de ports :

1. Accédez à ***Ethernet Ports » Configure Port Mirroring***. Le formulaire **Port Mirroring** s'affiche.

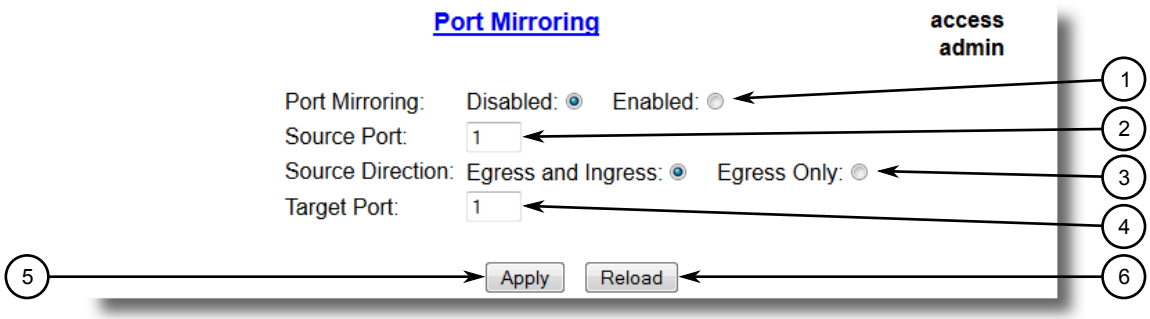


Figure 29 : Formulaire Port Mirroring

1. Options Port Mirroring **2.** Zone Source Port **3.** Options Source Direction **4.** Zone Target Port **5.** Bouton Apply **6.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Mise en miroir de ports	**Synopsis :** { Disabled, Enabled } **Par défaut :** Disabled Si la mise en miroir de ports la transmission est activée, toutes les trames reçues et transmises par le(s) port(s) source sont envoyées hors du port cible.
Source Port	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Le(s) port(s) surveillé(s).
Source Direction	**Synopsis :** Egress and Ingress, Egress Only **Par défaut :** Egress and Ingress Spécifie les trafics entrant et sortant ou uniquement le trafic sortant du port source.
Target Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Port où un appareil de surveillance doit être connecté.

3. Cliquez sur **Apply**.

Section 3.7.9

Configuration de la détection de liaison

Procédez comme suit pour configurer la détection de liaison :

1. Accédez à ***Ethernet Ports » Configure Link Detection***. Le formulaire **Link Detection** s'affiche.

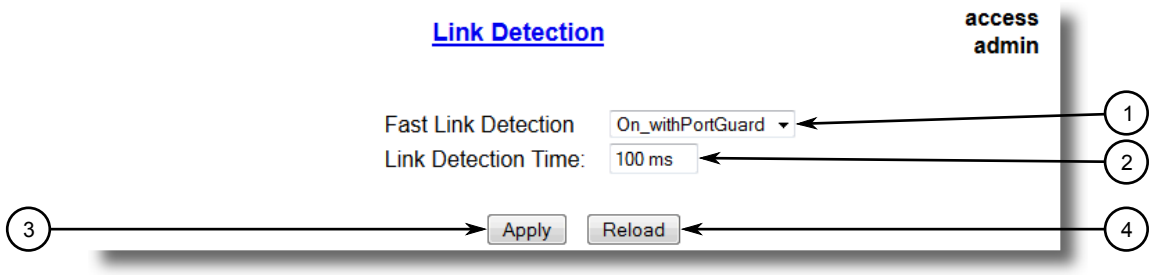


Figure 30 : Formulaire Link Detection

1. Zone Fast Link Detection **2.** Zone Link Detection Time **3.** Bouton Apply **4.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

REMARQUE
Lorsque la détection rapide de liaison (Fast Link Detection) est activée, le système empêche que le traitement des modifications de l'état de liaison ne consomme toutes les ressources disponibles de la CPU. Cependant, si Port Guard n'est pas utilisé, il est possible que pratiquement toutes les ressources de CPU disponibles soient utilisées par des modifications fréquentes de l'état des liaisons, ce qui aurait un impact négatif sur la réactivité globale du système.

Paramètre	Description
Fast Link Detection	**Synopsis :** { Off, On, On_withPortGuard } **Par défaut :** On_withPortGuard Ce paramètre fournit une protection contre les appareils terminaux défaillants générant un signal d'intégrité de liaison incorrect. Lorsqu'un appareil terminal défaillant ou un port à fibre sans correspondance correcte est connecté à l'unité, un nombre important de modifications d'états de liaison continues pourraient être signalés dans un intervalle de temps réduit. Ce grand nombre de fausses modifications d'état de liaison pourrait entraîner une non-réactivité du système car la plupart des ressources système (sinon toutes) sont utilisées pour traiter les changements d'état de liaison. Un grave problème peut alors se produire sur le réseau car il se peut que le traitement RSTP de l'unité ne soit pas exécutable, ce qui peut entraîner la création d'une boucle réseau. Trois différents réglages sont disponibles pour ce paramètre : • ON_withPortGuard - Il s'agit du réglage recommandé. Avec ce réglage, une période étendue (~2 minutes) de changements d'état de liaison excessifs signalés par un port pousseront la fonctionnalité Port Guard à désactiver la FAST LINK DETECTION (détection de liaison rapide) sur ce port et à générer une alarme. Une fois la FAST LINK DETECTION désactivée sur le port problématique, les changements d'état de liaison excessifs ne peuvent plus utiliser un volume important de ressource système. Cependant, si la FAST LINK DETECTION est désactivée, le port nécessitera plus de temps pour détecter une défaillance de liaison. Cela peut entraîner un temps de récupération du réseau plus long pouvant atteindre 2 s. Une fois que Port Guard désactive FAST LINK DETECTION sur un port spécifique, l'utilisateur peut l'activer de nouveau sur le port en effaçant l'alarme. • ON - Dans des cas spéciaux dans lesquels des changements d'état de liaison excessifs constituent une opération de liaison légitime, l'utilisation de ce réglage peut empêcher Port Guard de désactiver la FAST LINK DETECTION sur le port en question. Si les changements d'état de liaison excessifs persistent plus de 2 minutes, une alarme est générée pour avertir l'utilisateur de la liaison instable détectée. Si la condition de changements d'état de liaison excessifs est résolue ultérieurement, l'alarme est effacée automatiquement. Cette action ne désactivant pas la FAST LINK DETECTION, une liaison instable persistante peut affecter le temps de réponse du système. Ce réglage doit être utilisé avec prudence.

Paramètre	Description
	• OFF - La désactivation de ce paramètre désactive entièrement la FAST LINK DETECTION. Le port nécessitera plus de temps pour détecter une défaillance de liaison. Cela entraîne un temps de récupération du réseau plus long pouvant atteindre 2 s.
Link Detection Time	**Synopsis :** 100 ms à 1000 ms **Par défaut :** 100 ms Temps pendant lequel la liaison reste continuellement active avant que la décision "link up" ne soit prise par l'appareil. L'appareil exécute la stabilisation de la détection de liaison Ethernet afin d'éviter des réponses multiples à des événements d'instabilité de liaison occasionnels, par exemple lorsqu'un câble est secoué lorsqu'il est branché ou débranché.

3. Cliquez sur **Apply**.

Section 3.7.10

Gestion d'émetteurs-récepteurs SFP

RUGGEDCOM ROS prend en charge les émetteurs-récepteurs Small Form Factor Pluggable (SFP) pour fournir une liaison 1000Base-X, 100Base-FX, 1000Base-T ou 100Base-TX.

REMARQUE

Les émetteurs-récepteurs 1000Base-X SFP en fibres étant normalisés, RUGGEDCOM ROS prend en charge tout modèle de ce type. Il est vivement recommandé d'utiliser uniquement des modèles d'émetteurs-récepteurs SFP proposés par Siemens. Siemens soumet les émetteurs-récepteurs à des essais approfondis dans des conditions difficiles. Si un autre modèle d'émetteurs-récepteurs est utilisé, l'utilisateur assume la responsabilité de vérifier s'il est conforme aux exigences environnementales et d'utilisation.

Les émetteurs-récepteurs 1000Base-T SFP en cuivre n'étant pas normalisés, RUGGEDCOM ROS ne prend en charge que certains modèles de ce type.

REMARQUE

Les émetteurs-récepteurs SFP peuvent être remplacés à chaud.

*Lorsqu'un émetteur-récepteur SFP est inséré dans une cage SFP, les réglages de vitesse et de négociation automatique pour le port sont automatiquement ajustés aux valeurs appropriées. Par exemple, si un émetteur-récepteur SFP 1 G est installé, la vitesse du port est automatiquement modifiée sur 1 G et la négociation automatique réglée sur **On**.*

SOMMAIRE

• Section 3.7.10.1, « Configuration d'un port SFP »
• Section 3.7.10.2, « Surveillance d'un port SFP »
• Section 3.7.10.3, « Affichage d'informations pour un port SFP »

Section 3.7.10.1

Configuration d'un port SFP

En fonction du type de support de liaison requis, un port SFP peut nécessiter une configuration explicite :

- Pour les liaisons 1000Base-X ou 1000Base-T, la vitesse du port SFP doit être définie sur 1 Gbit/s.
- Pour les liaisons 100Base-FX ou 100Base-TX, la vitesse doit être définie sur 100 Mbit/s.
- La négociation automatique peut être configurée sur *On* lorsque la vitesse du port est définie sur 1 Gbit/s, ou sur *Off* lorsque la vitesse du port est définie sur 100 Mbit/s.
- Le mode duplex ne peut pas être configuré sur un port SFP et est toujours forcé sur duplex intégral.

Pour plus d'informations à propos de configuration de ports émetteurs-récepteurs SFC et d'autres ports Ethernet sur l'appareil, voir Section 3.7.6, « Configuration d'un port Ethernet ».

Section 3.7.10.2

Surveillance d'un port SFP

RUGGEDCOM ROS prend en charge le remplacement à chaud d'émetteurs-récepteurs SFP sur des ports SFP et détecte automatiquement quand un émetteur-récepteur SFP est supprimé ou installé.

Lorsque RUGGEDCOM ROS détecte qu'un émetteur-récepteur SFP est embroché dans le port SFP, il lit les informations de l'émetteur-récepteur et détermine le type d'émetteur-récepteur. La décision consiste pour RUGGEDCOM ROS à *accepter*, *accepter et reconfigurer* ou *rejeter* le port SFP.

Le tableau suivant montre les cas dans lesquels un émetteur-récepteur SFP est *accepté* ou *accepté et reconfiguré*.

Vitesse configurée	Type SFP détecté : 1000Base-X	Type SFP détecté : 100Base-FX	Type SFP détecté : 1000Base-T
1 Gbit/s	Accepter	Acceptez et définissez automatiquement la vitesse sur 100 Mbit/s et définissez la négociation automatique sur *Off*	Accepter
100 Mbit/s	Acceptez et définissez automatiquement la vitesse sur 1 Gbit/s et définissez la négociation automatique sur *On*	Accepter	Comparez le modèle d'émetteur-récepteur à une liste de modèles pris en charge.Acceptez-le s'il est dans la liste. Sinon, définissez automatiquement la vitesse sur 1 Gbit/s et définissez la négociation automatique sur *On*.

Si l'émetteur-récepteur est *accepté*, le paramètre`Media` sous***Ethernet Ports » Configure Port Parameters*** indique des informations détaillées sur l'émetteur-récepteur SFP, notamment le code de conformité Gigabit Ethernet, le support de transmission, le type de connecteur et la longueur de liaison. Par exemple :

```
SFP 1000LX SM LC 10 km
SFP 1000T 100 m
```

Si l'émetteur-récepteur n'est pas reconnu, il est *rejeté*. Une alarme est également générée et le port est bloqué afin qu'aucune liaison ne puisse être établie jusqu'à ce que l'émetteur-récepteur soit remplacé. Le paramètre`Media` indique que l'émetteur-récepteur SFP n'est pas identifié. Par exemple :

```
SFP Unidentified
```

Si aucun émetteur-récepteur n'est installé sur un port SFP, le paramètre`Media` indique que l'émetteur-récepteur SFP est débranché :

```
SFP Unplugged
```

Section 3.7.10.3

Affichage d'informations pour un port SFP

Procédez comme suit pour afficher des informations détaillées sur un port SFP :

1. Connectez-vous à l'appareil et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Saisissez la commande suivante :

   ```
   sfp port
   ```

   Où :

   - *port* est le numéro de port

   Les informations sur le port SFP sont affichées. Par exemple :

   ```
   >sfp 1
   ID: SFP
   Extended ID: GBIC/SFP function is defined by serial ID only
   Connector: LC
   Transceiver:
   Gigabit Ethernet Compliance Codes:
   1000LX
   Fibre Channel link length:
   Long Distance (L)
   Fibre Channel transmitter technology:
   Longwave laser (LC)
   Fibre Channel transmission media:
   Single Mode (SM)
   Fibre Channel speed:
   100 MBytes/Sec
   Baud Rate, nominal: 1300 MBits/sec
   Encoding type: 8B10B
   Length(9um): 10 km
   Length(9um): 10000 m
   Length(50um): 550 m
   Length(62.5um): 550 m
   Length(Copper): Not specified
   Vendor: xxxxxxx
   IEEE company ID: xxxxxxx
   Part number: xxxxxxxxxx
   Revision: 0000
   Laser wavelength: 1310 nm
   >
   ```

Section 3.7.11

Gestion des ports PoE

Le RUGGEDCOM RS900GP comprendhuitports Power over Ethernet (POE) conformes à IEEE 802.3at alimentés par une alimentation externe. Ces ports peuvent être managés comme suit via RUGGEDCOM ROS :

- **Protection contre la surcharge**
  Priorisez et activez/désactivez automatiquement les ports de priorité la plus basse selon les besoins en alimentation.
- **Conservation de l'énergie**
  Planifiez l'activation/la désactivation automatique de ports à des heures spécifiques pendant la semaine afin de conserver l'énergie.

Pour plus d'informations sur les ports PoE, voir le *Guide d'installation RUGGEDCOM RS900GP*.

SOMMAIRE

- Section 3.7.11.1, « Configuration globale de ports PoE »
- Section 3.7.11.2, « Configuration d'un port PoE spécifique »
- Section 3.7.11.3, « Planification de ports PoE »

Section 3.7.11.1

Configuration globale de ports PoE

Procédez comme suit pour configurer des réglages globaux pour tous les ports PoE (Power-over-Ethernet) :

1. Accédez à ***Ethernet Ports » Configure/View PoE Parameters » Configure/View System PoE Parameters***. Le formulaire **System PoE Parameters** s'affiche.

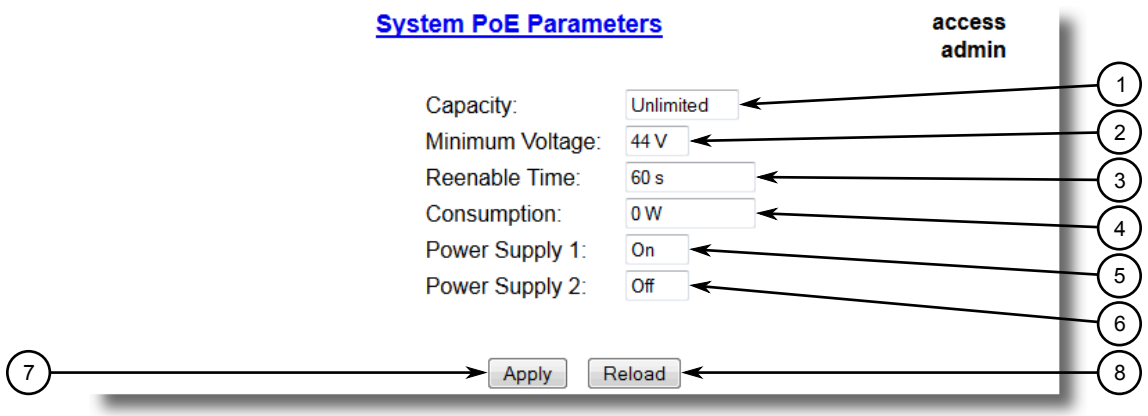


Figure 31 : Formulaire System PoE Parameters

1. Zone Capacity **2.** Zone Minimum Voltage **3.** Zone Reenable Time **4.** Zone Consumption **5.** Zone Power Supply 1 **6.** Zone Power Supply 2 **7.** Bouton Apply **8.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Capacity	**Synopsis :** 1 à 400 W ou { Unlimited } **Par défaut :** Unlimited Capacité de l'alimentation électrique PoE. C'est-à-dire la puissance de sortie totale maximum pouvant être fournie par tous les ports PoE. Lorsque la consommation électrique totale a atteint cette limite, certains ports sont fermés. Si le paramètre est défini sur Unlimited, la puissance de sortie totale n'est pas limitée par le logiciel.
Minimum Voltage	**Synopsis :** 39 à 57 V **Par défaut :** 44 V La tension minimum requise pour les ports PoE. Si la tension PoE baisse en-dessous de ce seuil, certains ports sont fermés. La norme IEEE 802.3af spécifie la plage de tension plage PoE 44 - 57 V.

Paramètre	Description
	La norme IEEE 802.3at spécifie la plage de tension plage PoE 50 - 57 V.
Reenable Time	**Synopsis :** 10 à 4294967295 s **Par défaut :** 60 s Temps d'attente pour la réactivation de ports PoE après leur fermeture en raison de la condition de surcharge.
Consumption	**Synopsis :** 0 à 4294967295 W Consommation électrique totale de tous les appareils PoE.
Power Supply 1	**Synopsis :** { On, Off } État de l'alimentation.
Power Supply 2	**Synopsis :** Synopsis : { On, Off } État de l'alimentation.

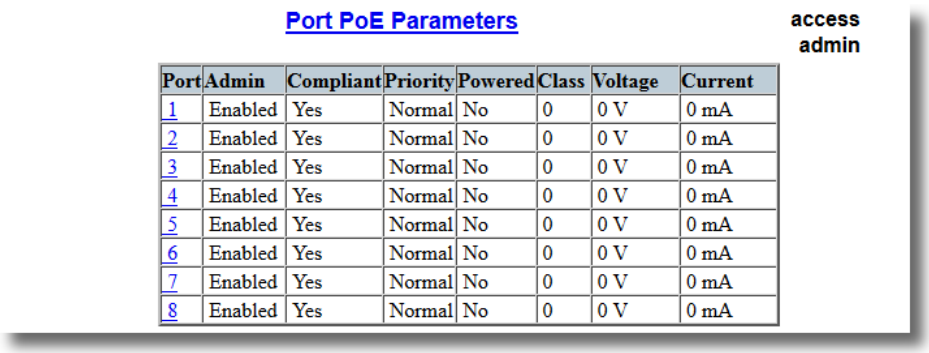
3. Cliquez sur **Apply**.

Section 3.7.11.2

Configuration d'un port PoE spécifique

Procédez comme suit pour configurer les réglages PoE (Power-over-Ethernet) pour un port Ethernet spécifique :

1. Accédez à ***Ethernet Ports » Configure/View PoE Parameters » Configure/View Port PoE Parameters***. Le tableau **Port PoE Parameters** s'affiche.



Port	Admin	Compliant	Priority	Powered	Class	Voltage	Current
1	Enabled	Yes	Normal	No	0	0 V	0 mA
2	Enabled	Yes	Normal	No	0	0 V	0 mA
3	Enabled	Yes	Normal	No	0	0 V	0 mA
4	Enabled	Yes	Normal	No	0	0 V	0 mA
5	Enabled	Yes	Normal	No	0	0 V	0 mA
6	Enabled	Yes	Normal	No	0	0 V	0 mA
7	Enabled	Yes	Normal	No	0	0 V	0 mA
8	Enabled	Yes	Normal	No	0	0 V	0 mA

Figure 32 : Tableau Port PoE Parameters

2. Sélectionnez un port Ethernet. Le formulaire **Port PoE Parameters** s'affiche.

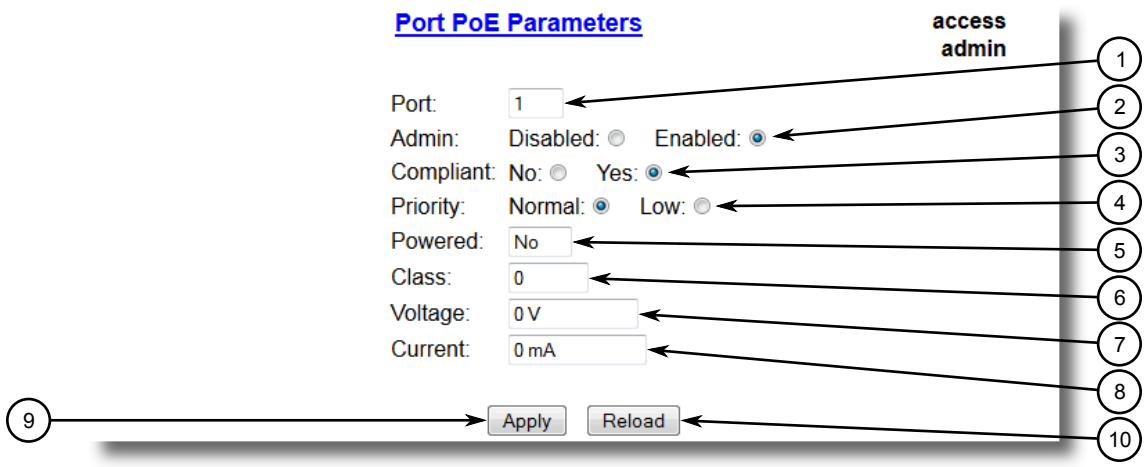


Figure 33 : Formulaire Port PoE Parameters

1. Zone Port **2.** Option Admin **3.** Options Compliant **4.** Options Priority **5.** Zone Powered **6.** Zone Class **7.** Zone Voltage **8.** Zone Current **9.** Bouton Apply **10.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 à 8 **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Admin	**Synopsis :** { Disabled, Enabled } **Par défaut :** Enabled Ce paramètre permet d'activer ou de désactiver l'alimentation électrique par le port.
Compliant	**Synopsis :** { No, Yes } **Par défaut :** Oui Définissez cette valeur sur Yes (par défaut) si l'appareil alimenté attaché est conforme aux normes IEEE802.3at/IEEE802.3af. Définissez cette valeur sur No si l'appareil attaché n'est pas conforme aux normes. L'alimentation au port est forcée sans l'exécution du test de signature POE normal.
Priority	**Synopsis :** { Normal, Low } **Par défaut :** Normal Spécifie si la priorité de ce port est basse. Les ports à basse priorité sont fermés en premier si l'alimentation est surchargée. D'autres ports peuvent être également fermés si la condition de surcharge existe toujours après la fermeture de ports à basse priorité.
Powered	**Synopsis :** { No, Yes } Définit si l'alimentation est actuellement fournie par le port.
Class	**Synopsis :** 0 à 65535 Valeur de classe PoE définissant le niveau de puissance minimum fourni. Pour plus d'informations, référez-vous aux normes IEEE 802.1af et 802.1at. 0 = 15.4 W (par défaut) 1 = 4.0 W 2 = 7.0 W 3 = 15.4 W

Paramètre	Description
	4 = 34.2 W
Voltage	**Synopsis :** 0 à 65535 Niveau de tension fourni.
Current	**Synopsis :** 0 à 65535 Niveau de courant fourni.

4. Cliquez sur **Apply**.

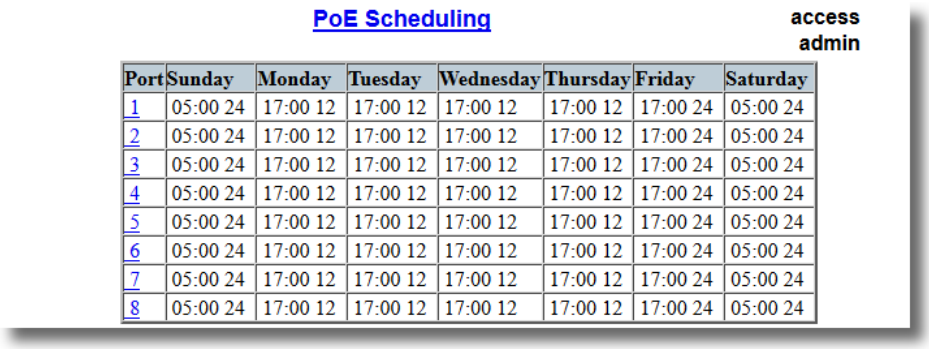
Section 3.7.11.3

Planification de ports PoE

Pour économiser de l'énergie, des ports PoE (Power-over-Ethernet) peuvent être configurés de manière à s'arrêter et redémarrer à des moments précis de la semaine.

Procédez comme suit pour configurer une planification de la mise sous tension d'un port PoE :

1. Accédez à ***Ethernet Ports » Configure/View PoE Parameters » Configure PoE Scheduling***. Le tableau **PoE Scheduling** s'affiche.



Port	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
2	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
3	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
4	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
5	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
6	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
7	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24
8	05:00 24	17:00 12	17:00 12	17:00 12	17:00 12	17:00 24	05:00 24

Figure 34 : Tableau PoE Scheduling

2. Sélectionnez un port Ethernet. Le formulaire **PoE Scheduling** s'affiche.

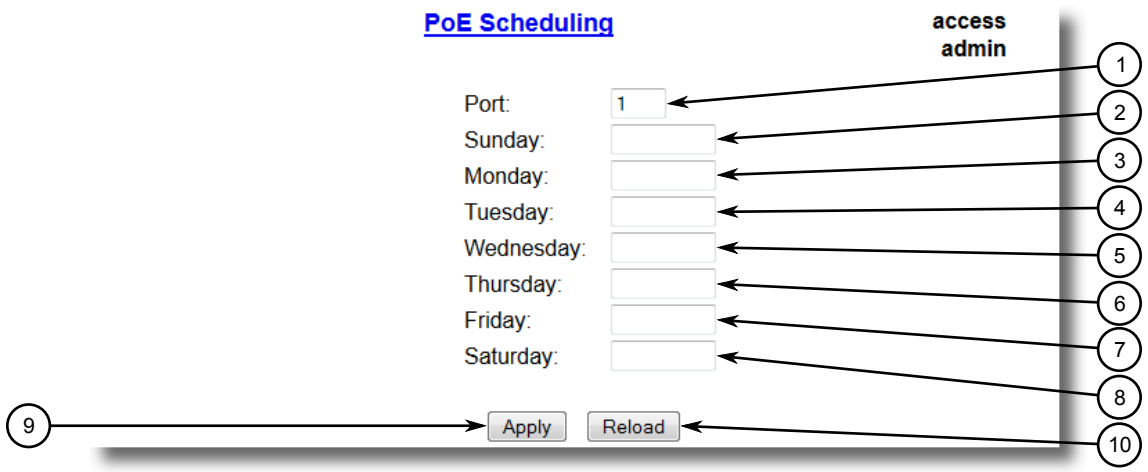


Figure 35 : Formulaire PoE Scheduling

1. Zone Port **2.** Zone Sunday **3.** Zone Monday **4.** Zone Tuesday **5.** Zone Wednesday **6.** Zone Thursday **7.** Zone Friday **8.** Zone Saturday **9.** Bouton Apply **10.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Sunday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple : '17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.
Monday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple : '17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.
Tuesday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple : '17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.
Wednesday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple : '17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.
Thursday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple : '17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.
Friday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple :

Paramètre	Description
	'17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.
Saturday	Intervalle de temps d'extinction de ce port PoE pour économiser de l'énergie Exemple : '17:00 12' signifie que le port est fermé à 17h00 pendant 12 heures. Il sera réactivé à 5h00 du matin le jour suivant.

4. Cliquez sur **Apply**.

Section 3.7.12

Détection de défauts de câble

Des problèmes de connectivité peuvent parfois être attribués à des défauts dans des câbles Ethernet. Pour aider à détecter les défauts de câble, les courts-circuits, les câbles ouverts et les câbles trop longs, RUGGEDCOM ROS comprend un utilitaire de diagnostic de câble intégré.

SOMMAIRE

- Section 3.7.12.1, « Affichage des résultats de diagnostics de câbles »
- Section 3.7.12.2, « Exécution de diagnostics de câble »
- Section 3.7.12.3, « Effacement de diagnostics de câble »
- Section 3.7.12.4, « Détermination de la distance estimée au défaut (Estimated Distance To Fault (DTF)) »

Section 3.7.12.1

Affichage des résultats de diagnostics de câbles

Pour afficher les résultats de tests de diagnostics précédents, accédez à ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. Le tableau **Cable Diagnostics Parameters** s'affiche.

REMARQUE
Pour plus d'informations sur le démarrage d'un test de diagnostic, voir Section 3.7.12.2, « Exécution de diagnostics de câble ».

Cable Diagnostics Parameters access admin

Port	State	Runs	Calib.	Good	Open	Short	Imped	Pass /Fail /Total
1	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
2	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
3	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
4	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
5	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
6	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
7	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
8	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
9	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
10	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0

Figure 36 : Tableau Cable Diagnostics Parameters

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
State	**Synopsis :** { Stopped, Started } Contrôle le lancement/l'arrêt des diagnostics de câble sur le port sélectionné. Si un port ne prend pas en charge les diagnostics de câble, l'état est signalé comme N/A.
Runs	**Synopsis :** 0 à 65535 Le nombre total de diagnostics de câble à exécuter sur le port sélectionné. Si ce nombre est défini sur 0, les diagnostics de câble sont exécutés en continu sur le port sélectionné.
Calib.	**Synopsis :** -100.0 à 100.0m Cette valeur d'étalonnage peut être utilisée pour ajuster ou étalonner la distance estimée au défaut. Vous pouvez procéder comme suit pour étalonner la distance estimée au défaut des diagnostics de câble : • Choisissez un port spécifique pour lequel un étalonnage est nécessaire. • Connectez un câble Ethernet avec une longueur connue (par ex. 50 m) au port. • Ne connectez pas l'autre extrémité du câble à un partenaire de liaison quelconque. • Exécutez quelques fois les diagnostics de câble sur le port. Un défaut d'ouverture doit être détecté. • Déterminez la distance moyenne entre le défaut d'ouverture enregistré dans le journal et comparez-la à la longueur connue du câble. La différence peut être utilisée comme valeur d'étalonnage. • Saisissez la valeur d'étalonnage et exécutez à nouveau quelques fois les diagnostics de câble. • La distance au défaut d'ouverture doit maintenant être similaire à la longueur du câble. • La distance au défaut pour le port sélectionné est maintenant étalonnée.
Good	**Synopsis :** 0 à 65535 Nombre de détections d'arrêts bons (GOOD, sans erreur) sur les paires de câbles du port sélectionné.
Open	**Synopsis :** 0 à 65535 Nombre de détections d'ouvertures (OPEN) sur les paires de câbles du port sélectionné.
Short	**Synopsis :** 0 à 65535 Nombre de détections de courts-circuits (SHORT) sur les paires de câbles du port sélectionné.

Paramètre	Description
Imped	**Synopsis :** 0 à 65535 Nombre de détections de discordances d'impédance (IMPEDANCE MISMATCH) sur les paires de câbles du port sélectionné.
Pass /Fail /Total	**Synopsis :** 19 caractères quelconques Ce champ résume les résultats des diagnostics de câble exécutés jusqu'ici. Pass - nombre de diagnostics de câble exécutés avec succès sur le port sélectionné. Fail - nombre de diagnostics de câble ayant échoué sur le port sélectionné. Total - nombre total de tentatives de diagnostics de câble sur le port sélectionné.

REMARQUE
*Pour chaque test de diagnostic réussi, les valeurs pour**Good**,**Open**,**Short** ou**Imped** sont incrémentées selon le nombre pairs de câbles connectées au port. Pour un port a 100Base-T, qui comprend deux paires de câbles. le nombre est incrémenté de deux. Pour un port a 1000Base-T, qui comprend quatre paires de câbles. le nombre est incrémenté de quatre.*

REMARQUE
Lorsqu'une défaillance de câble est détectée, une distance estimée au défaut est calculée et enregistrée dans le journal système. Le journal répertorie la paire de câble, la défaillance détectée et la valeur de la distance au défaut. Pour plus d'informations sur le journal système, voir Section 3.6.1, « Affichage de journaux locaux et système ».

Section 3.7.12.2

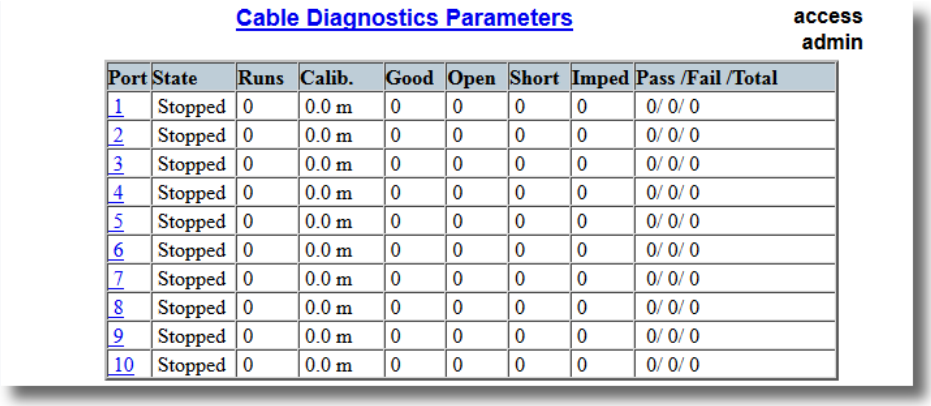
Exécution de diagnostics de câble

Procédez comme suit pour exécuter un diagnostic de câble sur un ou plusieurs ports Ethernet :

1. Connectez un câble Ethernet CAT-5 (ou de meilleure qualité) au port Ethernet sélectionné.

   IMPORTANT !
   *Le port Ethernet sélectionné et son port partenaire peuvent être configurés de manière à s'exécuter en mode **Enabled** avec négociation automatique ou en mode **Disabled**. Les autres modes ne sont pas recommandés car ils interfèrent avec la procédure de diagnostic de câble.*

2. Reliez l'autre extrémité du câble à un port réseau similaire. Par exemple, connectez un port 100Base-T à un port 100Base-T, ou un port 1000Base-T à un port 1000Base-T.
3. Dans RUGGEDCOM ROS, accédez à ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. Le tableau **Cable Diagnostics Parameters** s'affiche.



Cable Diagnostics Parameters

access admin

Port	State	Runs	Calib.	Good	Open	Short	Imped	Pass /Fail /Total
1	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
2	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
3	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
4	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
5	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
6	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
7	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
8	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
9	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
10	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0

Figure 37 : Tableau Cable Diagnostics Parameters

4. Sélectionnez un port Ethernet. Le formulaire **Cable Diagnostics Parameters** s'affiche.

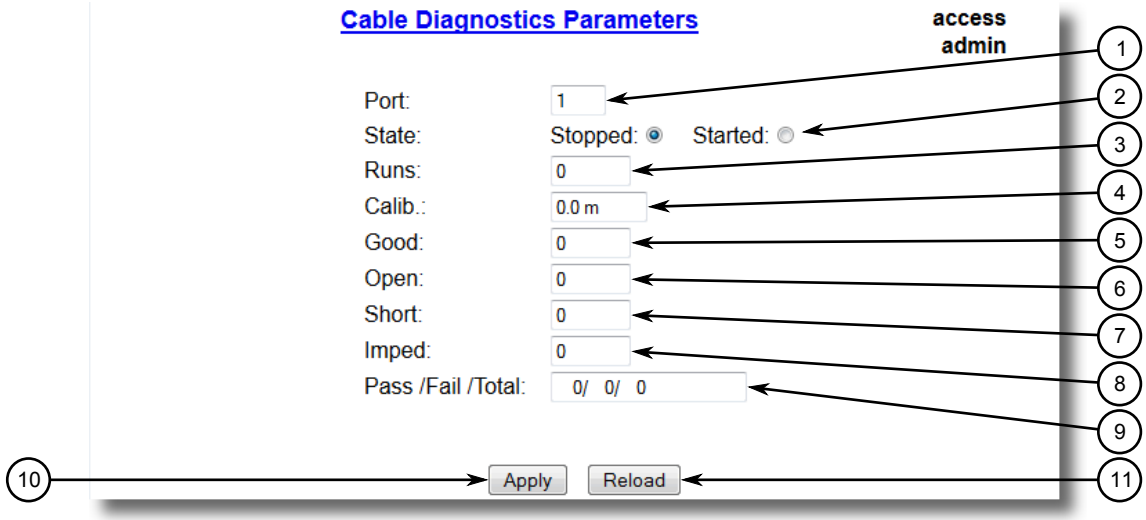


Figure 38 : Formulaire Cable Diagnostics Parameters

1. Zone Port **2.** Options State **3.** Zone Runs **4.** Calib. (zone) **5.** Zone Good **6.** Zone Open **7.** Zone Short **8.** Zone Imped **9.** Zone Pass /Fail /Total **10.** Bouton Apply **11.** Bouton Reload

5. Sous**Runs**, saisissez le nombre de tests de diagnostic consécutifs à exécuter. Une valeur de 0 indique que le test est exécuté en continu jusqu'à ce qu'il soit stoppé par l'utilisateur.
6. Sous**Calib.**, saisissez la valeur de la distance estimée au défaut (Estimated Distance To Fault (DTF)). Pour plus d'informations sur la manière de déterminer la valeur DTF, voir Section 3.7.12.4, « Détermination de la distance estimée au défaut (Estimated Distance To Fault (DTF)) ».
7. Sélectionnez**Started**.

> **IMPORTANT !**
> *Un test de diagnostic peut être stoppé en sélectionnant**Stopped** et en cliquant sur **Apply**. Cependant, si le test est arrêté pendant l'exécution d'un diagnostic, il sera exécuté jusqu'à ce qu'il soit terminé.*

8. Cliquez sur **Apply**. L'état du port Ethernet est automatiquement modifié en `Stopped` lorsque le test est terminé. Pour plus d'informations sur la manière de surveiller le test et d'afficher les résultats, voir Section 3.7.12.1, « Affichage des résultats de diagnostics de câbles ».

Section 3.7.12.3

Effacement de diagnostics de câble

Procédez comme suit pour effacer les résultats de diagnostic de câble :

1. Accédez à ***Ethernet Ports » Clear Cable Diagnostics Statistics***. Le formulaire **Clear Cable Diagnostics Statistics** s'affiche.

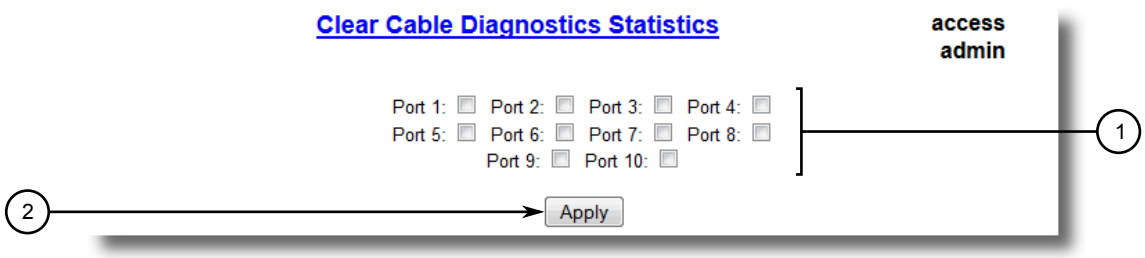


Figure 39 : Formulaire Clear Cable Diagnostics Statistics

1. Zones Port Check **2.** Bouton Apply

2. Sélectionnez un ou plusieurs ports Ethernet.
3. Cliquez sur **Apply**.

Section 3.7.12.4

Détermination de la distance estimée au défaut (Estimated Distance To Fault (DTF))

Procédez comme suit pour déterminer la distance estimée au défaut (Estimated Distance To Fault (DTF))

1. Connectez un câble Ethernet CAT-5 (ou de meilleure qualité) avec une longueur connue au port. Ne connectez pas l'autre extrémité du câble à un autre port.
2. Configurez l'utilitaire de diagnostic de câble de manière à ce qu'il s'exécute quelques fois sur le port Ethernet sélectionné et lancez le test. Pour plus d'informations, voir Section 3.7.12.2, « Exécution de diagnostics de câble ». Les défauts d'ouverture doivent être détectés et consignés dans le journal système.
3. Passez en revue les erreurs consignées dans le journal système et déterminez la distance moyenne aux défauts d'ouverture. Pour plus d'informations sur le journal système, voir Section 3.6.1, « Affichage de journaux locaux et système ».
4. Soustrayez la distance moyenne de la longueur de câble pour déterminer la valeur d'étalonnage.

5. Configurez l'utilitaire de diagnostic de câble de manière à ce qu'il s'exécute quelques fois avec la nouvelle valeur d'étalonnage. La distance au défaut d'ouverture doit maintenant être égale à la longueur effective du câble. La distance au défaut (Distance To Fault (DTF)) est maintenant étalonnée pour le port Ethernet sélectionné.

Section 3.7.13

Réinitialisation de ports Ethernet

Il peut être parfois nécessaire de réinitialiser un port Ethernet spécifique, par exemple lorsque le partenaire de liaison est bloqué à un état inapproprié. Une réinitialisation peut être également utile pour forcer la renégociation de la vitesse et des modes de duplex.

Procédez comme suit pour réinitialiser des ports Ethernet spécifiques :

1. Accédez à ***Ethernet Ports » Reset Port(s)***. Le formulaire **Reset Port(s)** s'affiche.

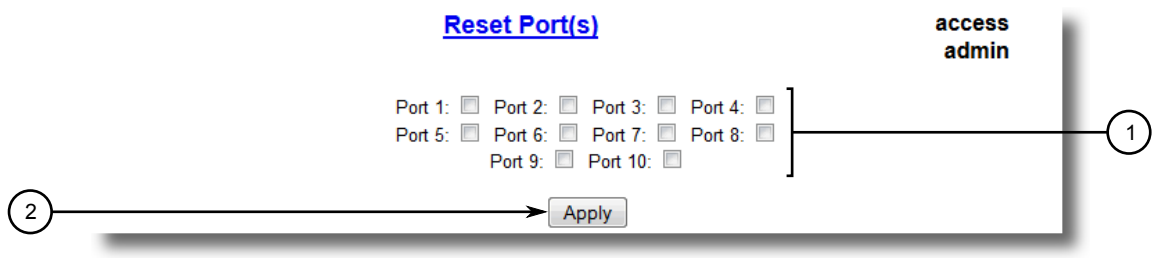


Figure 40 : Formulaire Reset Port(s)

1. Ports **2.** Bouton Apply

2. Sélectionnez un ou plusieurs ports Ethernet à réinitialiser.
3. Cliquez sur **Apply**. Les ports Ethernet sélectionnés sont réinitialisés.

Section 3.8

Gestion d'interfaces IP

RUGGEDCOM ROS permet la configuration d'une interface IP pour chaque sous-réseau (ou VLAN), jusqu'à 255 interfaces au maximum. L'une des interfaces doit également être configurée comme interface de gestion pour certains services IP, notamment le DHCP Relay Agent.

Une adresse IP doit être affectée à chaque interface IP. Dans le cas de l'interface de gestion, le type d'adresse IP peut être statique, DHCP, BOOTP ou dynamique. Pour toutes les autres interfaces, l'adresse IP doit être statique.

ATTENTION !
Risque pour la configuration - risque d'interruption de la communication. La modification de l'ID pour le VLAN de gestion coupe toute connexion Raw Socket TCP active. Si cela se produit, réinitialisez tous les ports série.

SOMMAIRE

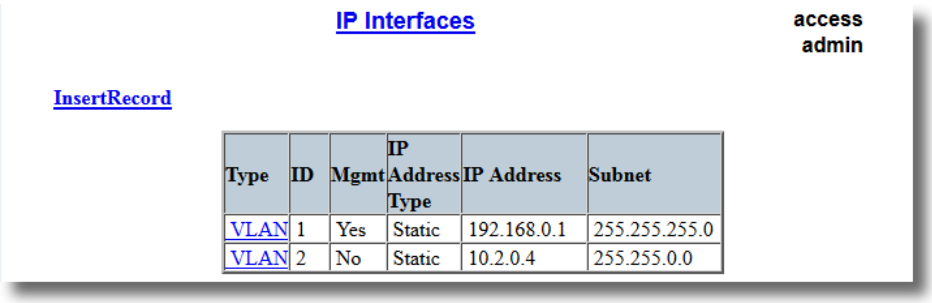
- Section 3.8.1, « Affichage d'une liste d'interfaces IP de »

- Section 3.8.2, « Ajout d'une interface IP »
- Section 3.8.3, « Suppression d'une interface IP »

Section 3.8.1

Affichage d'une liste d'interfaces IP de

Pour afficher une liste d'interfaces IP de configurés sur l'appareil, accédez à ***Administration » Configure IP Interfaces » Configure IP Interfaces***. Le tableau **IP Interfaces** s'affiche.



Type	ID	Mgmt	IP Address Type	IP Address	Subnet
VLAN	1	Yes	Static	192.168.0.1	255.255.255.0
VLAN	2	No	Static	10.2.0.4	255.255.0.0

Figure 41 : tableau IP Interfaces

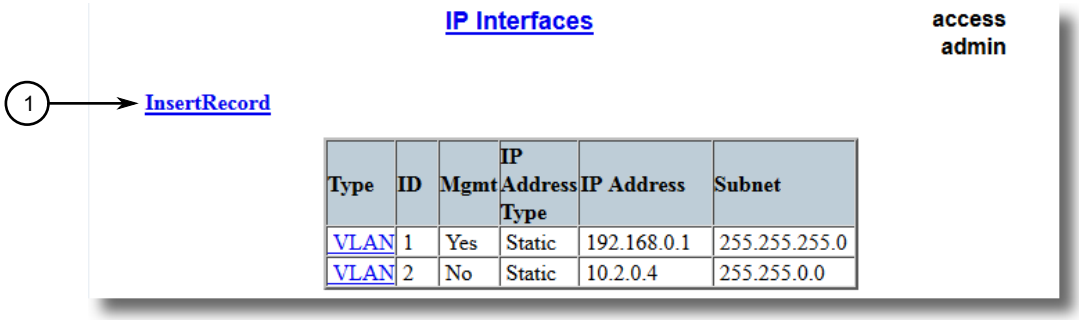
Si aucune interface IP de n'a été configurée, ajoutez des interfaces IP en fonction de vos besoins. Pour plus d'informations, voir Section 3.8.2, « Ajout d'une interface IP ».

Section 3.8.2

Ajout d'une interface IP

Procédez comme suit pour ajouter une interface IP :

1. Accédez à ***Administration » Configure IP Interfaces***. Le tableau **IP Interfaces** s'affiche.



Type	ID	Mgmt	IP Address Type	IP Address	Subnet
VLAN	1	Yes	Static	192.168.0.1	255.255.255.0
VLAN	2	No	Static	10.2.0.4	255.255.0.0

Figure 42 : tableau IP Interfaces

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **Switch IP Interfaces** s'affiche.

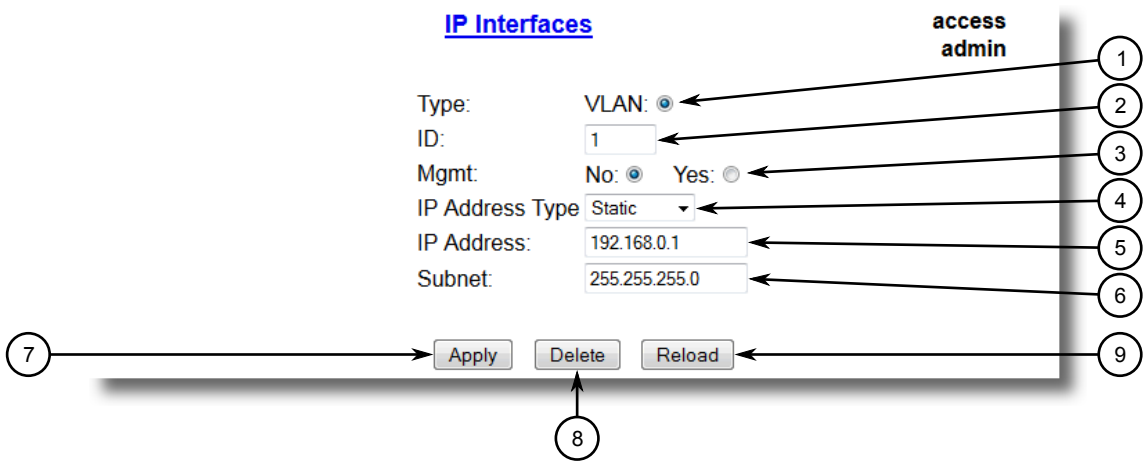


Figure 43 : formulaire IP Interfaces

1. Options Type **2.** Zone ID **3.** Options Mgmt **4.** Zone IP Address Type **5.** Zone IP Address **6.** Zone Subnet **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

REMARQUE

L'adresse et le masque IP configurés pour le VLAN de gestion ne sont pas modifiés lors de la réinitialisation de tous les paramètres de configuration aux valeurs par défaut, et 1 leur est affecté comme ID de VLAN. Les modifications de l'adresse IP sont effectives immédiatement. Toutes les connexions IP mises en œuvre au moment d'une modification d'une adresse IP sont perdues.

Paramètre	Description
Type	**Synopsis :** { VLAN } **Par défaut :** VLAN Spécifie le type d'interface pour lequel cette interface IP est créée.
ID	**Synopsis :** 1 à 4094 **Par défaut :** 1 Spécifie l'ID d'interface pour lequel cette interface IP est créée. Si le type d'interface est VLAN, il représente l'ID de VLAN.
Mgmt	**Synopsis :** { No, Yes } **Par défaut :** No Spécifie si l'interface IP est l'interface de gestion de l'appareil.
IP Address Type	**Synopsis :** { Static, Dynamic, DHCP, BOOTP } **Par défaut :** Static Spécifie si l'adresse IP est statique ou affectée de manière dynamique via DHCP ou BOOTP. L'option Dynamic commute automatiquement entre BOOTP et DHCP jusqu'à recevoir la réponse du serveur approprié. L'option Static doit être utilisée pour des interfaces qui ne sont pas des interfaces de gestion.
IP Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### **Par défaut :** 192.168.0.1 Spécifie l'adresse IP de cet appareil. Une adresse IP est un nombre 32 bits noté à l'aide de quatre nombres de 0 à 255 séparés par des points. Seule une adresse IP de monodiffusion est autorisée dans une plage de 1.0.0.0 à 233.255.255.255.

Paramètre	Description
Subnet	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### **Par défaut :** 255.255.255.0 Spécifie le masque de sous-réseau IP de cet appareil. Un masque de sous-réseau IP est un nombre 32 bits noté à l'aide de quatre nombres de 0 à 255 séparés par des points. Généralement, les nombres de masque de sous-réseau utilisent 0 ou 255 comme valeur (par exemple 255.255.255.0), mais ils peuvent comprendre d'autres nombres. **IMPORTANT !** *Chaque interface IP doit avoir une adresse réseau unique.*

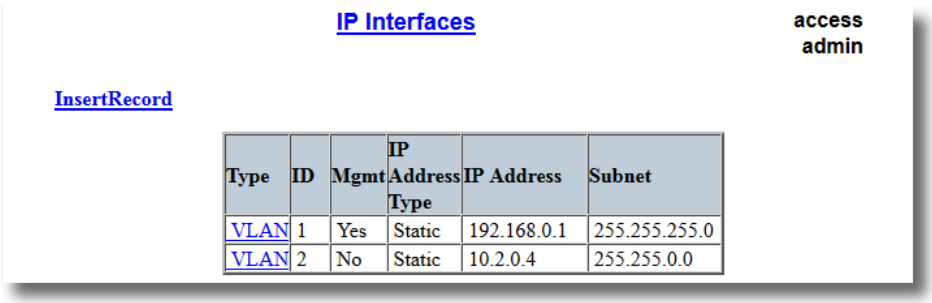
4. Cliquez sur **Apply**.

Section 3.8.3

Suppression d'une interface IP

Procédez comme suit pour supprimer une interface IP configurée sur l'appareil :

1. Accédez à ***Administration » Configure IP Interfaces***. Le tableau **IP Interfaces** s'affiche.



Type	ID	Mgmt	IP Address Type	IP Address	Subnet
VLAN	1	Yes	Static	192.168.0.1	255.255.255.0
VLAN	2	No	Static	10.2.0.4	255.255.0.0

Figure 44 : tableau IP Interfaces

2. Sélectionnez l'interface IP dans le tableau. Le formulaire **IP Interfaces** s'affiche.

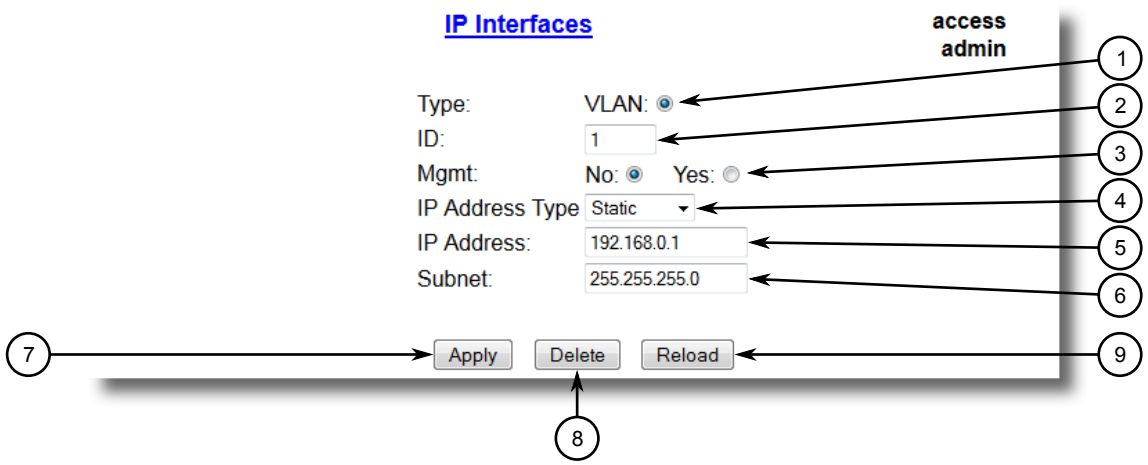


Figure 45 : formulaire IP Interfaces

1. Options Type **2.** Zone ID **3.** Options Mgmt **4.** Zone IP Address Type **5.** Zone IP Address **6.** Zone Subnet **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton Reload

3. Cliquez sur **Delete**.

Section 3.9

Gestion de passerelles IP

RUGGEDCOM ROS permet la configuration de jusqu'à dix passerelles IP. Lorsque les paramètres**Destination** et**Subnet** sont tous les deux vides, la passerelle est considérée comme une passerelle par défaut.

REMARQUE
La configuration de la passerelle par défaut n'est pas modifiée lors de la réinitialisation de tous les paramètres de configuration à leurs valeurs par défaut.

SOMMAIRE

- Section 3.9.1, « Affichage d'une liste de passerelles IP »
- Section 3.9.2, « Ajout d'une passerelle IP »
- Section 3.9.3, « Suppression d'une passerelle IP »

Section 3.9.1

Affichage d'une liste de passerelles IP

Pour afficher une liste de passerelles IP configurées sur l'appareil, accédez à ***Administration » Configure IP Gateways***. Le tableau **IP Gateways** s'affiche.

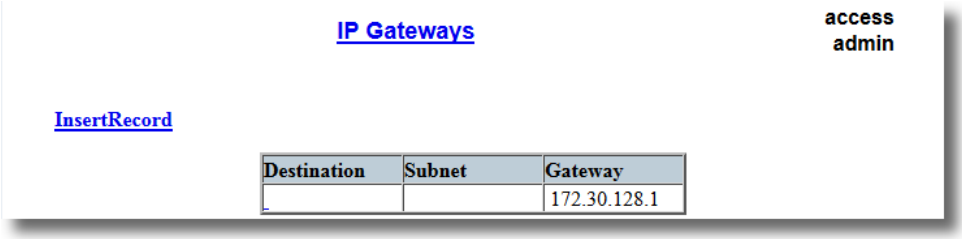


Figure 46 : Tableau IP Gateways

Si aucune passerelle IP n'a été configurée, ajoutez des passerelles IP en fonction de vos besoins. Pour plus d'informations, voir Section 3.9.2, « Ajout d'une passerelle IP ».

Section 3.9.2

Ajout d'une passerelle IP

IMPORTANT !
Les adresses de passerelle fournies par DHCP remplacent les valeurs configurées manuellement.

Procédez comme suit pour ajouter une passerelle IP :

1. Accédez à ***Administration » Configure IP Gateways***. Le tableau **IP Gateways** s'affiche.

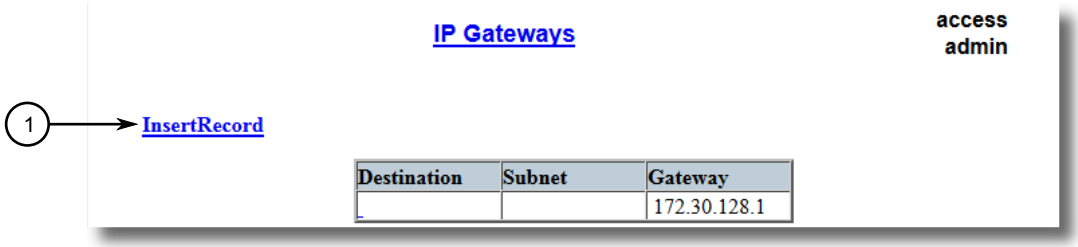


Figure 47 : Tableau IP Gateways

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **IP Gateways** s'affiche.

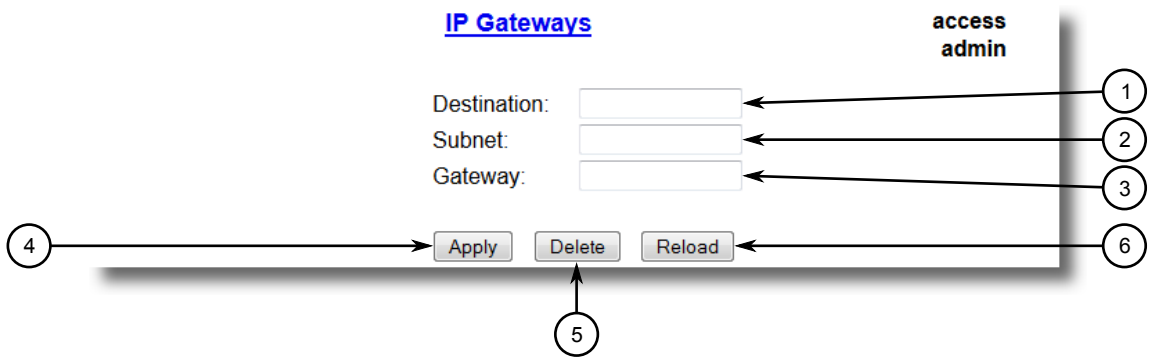


Figure 48 : IP Gateways

1. Zone Destination **2.** Zone Subnet **3.** Zone Gateway **4.** Bouton Apply **5.** Bouton Delete **6.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Destination	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Spécifie l'adresse IP du réseau de destination ou de l'hôte. Pour la passerelle par défaut, la destination et le sous-réseau sont 0.
Subnet	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Spécifie le masque de sous-réseau IP de destination. Pour la passerelle par défaut, la destination et le sous-réseau sont 0.
Gateway	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Spécifie la passerelle à utiliser pour atteindre la destination.

4. Cliquez sur **Apply**.

Section 3.9.3

Suppression d'une passerelle IP

Procédez comme suit pour supprimer une passerelle IP configurée sur l'appareil :

1. Accédez à ***Administration » Configure IP Gateways***. Le tableau **IP Gateways** s'affiche.

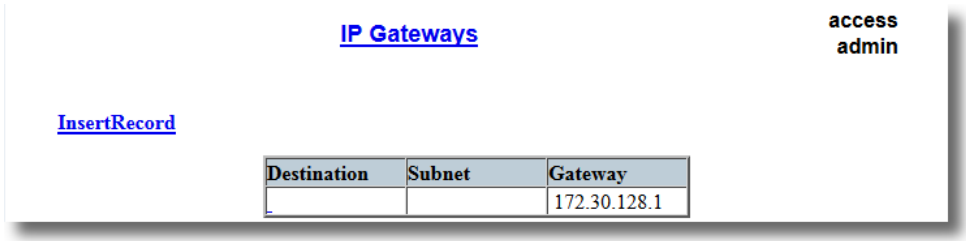


Figure 49 : Tableau IP Gateways

2. Sélectionnez la passerelle IP dans le tableau. Le formulaire **IP Gateways** s'affiche.

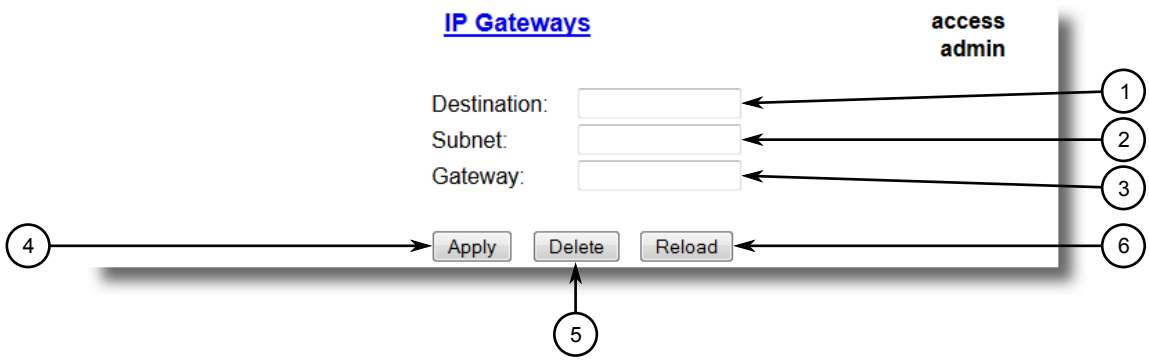


Figure 50 : Formulaire IP Gateways

1. Zone Destination **2.** Zone Subnet **3.** Zone Gateway **4.** Bouton Apply **5.** Bouton Delete **6.** Bouton Reload

3. Cliquez sur **Delete**.

Section 3.10

Configuration des services IP

Procédez comme suit pour configurer les services IP fournis par l'appareil :

1. Accédez à ***Administration » Configure IP Services***. Le formulaire **IP Services** s'affiche.

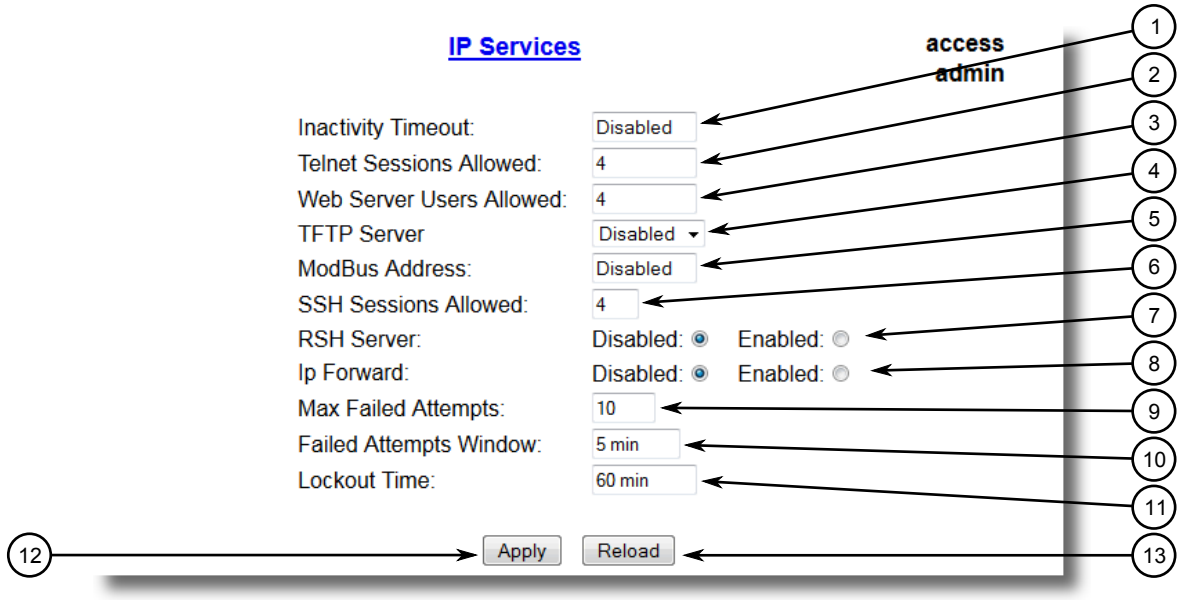


Figure 51 : Formulaire IP Services

1. Zone Inactivity Timeout **2.** Zone Telnet Sessions Allowed **3.** Zone Web Server Users Allowed **4.** Zone TFTP Server **5.** Zone Modbus Address **6.** Zone SSH Sessions Allowed **7.** Options RSH Server **8.** Options IP Forward **9.** Zone Max Failed Attempts **10.** Zone Failed Attempts Window **11.** Zone Lockout Time **12.** Bouton Apply **13.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Inactivity Timeout	**Synopsis :** 1 à 60 ou { Disabled } **Par défaut :** 5 min Spécifie l'expiration de la console et affiche l'écran de connexion si aucun utilisateur n'est actif. La valeur zéro désactive les délais d'expiration. La valeur de délai d'expiration maximum pour les utilisateurs de serveur Web est de 30 minutes.
Telnet Sessions Allowed	**Synopsis :** 1 à 4 ou { Disabled } **Par défaut :** Disabled Limite le nombre de sessions Telnet. La valeur zéro empêche tout accès Telnet.
Web Server Users Allowed	**Synopsis :** 1 à 4 ou { Disabled } **Par défaut :** 4 Limite le nombre d'utilisateurs de serveur Web simultanés.
TFTP Server	**Synopsis :** { Disabled, Get Only, Enabled } **Par défaut :** Disabled TFTP étant un protocole non sécurisé, ce paramètre permet à l'utilisateur de limiter ou de désactiver l'accès au serveur TFTP. DISABLED - désactive l'accès en lecture et en écriture au serveur TFTP GET ONLY - permet uniquement la lecture de fichiers via le serveur TFTP ENABLED - permet la lecture et l'écriture de fichiers via le serveur TFTP
ModBus Address	**Synopsis :** 1 à 255 ou { Disabled } **Par défaut :** Disabled Détermine l'adresse Modbus à utiliser pour la gestion via Modbus.

Paramètre	Description
SSH Sessions Allowed (version contrôlée uniquement)	**Synopsis :** 1 à 4 **Par défaut :** 4 Limite le nombre de sessions SSH.
RSH Server	**Synopsis :** { Disabled, Enabled } **Par défaut :** Disabled (version contrôlée) ou Enabled (version non contrôlée) Active/désactive l'accès Shell distant.
IP Forward	**Synopsis :** { Disabled, Enabled } Contrôle la capacité de transfert IP entre des VLAN dans un serveur série ou des segments IP. **REMARQUE** *Lors de la mise à jour à ROS v4.3, la valeur par défaut est définie sur { Enabled }.*
Max Failed Attempts	**Synopsis :** 1 à 20 **Par défaut :** 10 Nombre maximum d'échecs de tentatives d'accès consécutifs au service au sein de la Failed Attempts Window avant le blocage du service.
Failed Attempts Window	**Synopsis :** 1 à 30 min **Par défaut :** 5 min Temps en minutes (min) pendant lequel le nombre maximum d'échecs de tentatives de connexion doit être dépassé avant le blocage du service. Le compteur d'échecs de tentatives est remis à 0 lorsque la temporisation expire.
Lockout Time	**Synopsis :** 1 à 120 min **Par défaut :** 60 min Temps en minutes (min) pendant lequel le service reste bloqué lorsque le nombre maximum d'échecs de tentatives d'accès a été atteint.

3. Cliquez sur **Apply**.

Section 3.11

Gestion de la surveillance à distance

La surveillance à distance (Remote Monitoring (RMON)) est utilisée pour collecter et afficher des statistiques historiques liées à la performance et au fonctionnement de ports Ethernet. Elle peut également enregistrer une entrée de journal et/ou générer un trap SNMP lorsque le taux d'occurrences d'un événement spécifique est dépassé.

SOMMAIRE

- Section 3.11.1, « Gestion des RMON History Controls »
- Section 3.11.2, « Gestion des alarmes RMON »
- Section 3.11.3, « Gestion des événements RMON »

Section 3.11.1

Gestion des RMON History Controls

Les contrôles d'historique pour la surveillance distante (Remote Monitoring) collectent des échantillons de statistiques d'historique RMON-MIB d'un port Ethernet à intervalles réguliers.

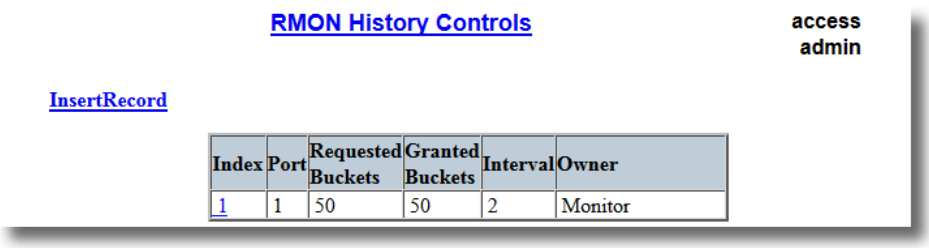
SOMMAIRE

- Section 3.11.1.1, « Affichage d'une liste de contrôles d'historique RMON »
- Section 3.11.1.2, « Ajout d'un contrôle d'historique RMON »
- Section 3.11.1.3, « Suppression d'un contrôle d'historique RMON »

Section 3.11.1.1

Affichage d'une liste de contrôles d'historique RMON

Pour afficher une liste de contrôles d'historique RMON, accédez à ***Ethernet Stats » Configure RMON History Controls***. Le tableau **RMON History Controls** s'affiche.



Index	Port	Requested Buckets	Granted Buckets	Interval	Owner
1	1	50	50	2	Monitor

Figure 52 : Tableau RMON History Controls

Si aucun contrôle d'historique n'a été configuré, ajoutez des contrôles en fonction de vos besoins. Pour plus d'informations, voir Section 3.11.1.2, « Ajout d'un contrôle d'historique RMON ».

Section 3.11.1.2

Ajout d'un contrôle d'historique RMON

Procédez comme suit pour ajouter un contrôle d'historique RMON :

1. Accédez à ***Ethernet Stats » Configure RMON History Controls***. Le tableau **RMON History Controls** s'affiche.

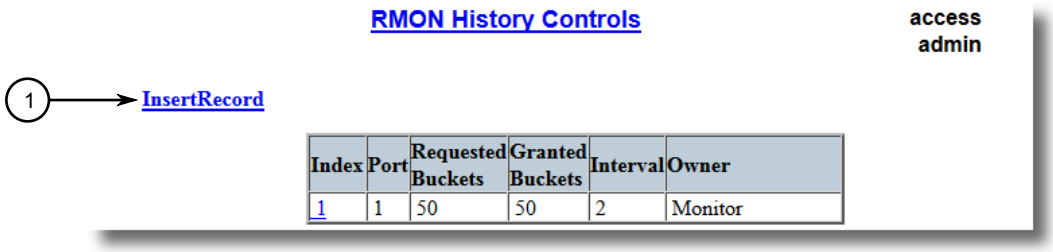


Figure 53 : Tableau RMON History Controls

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **RMON History Controls** s'affiche.

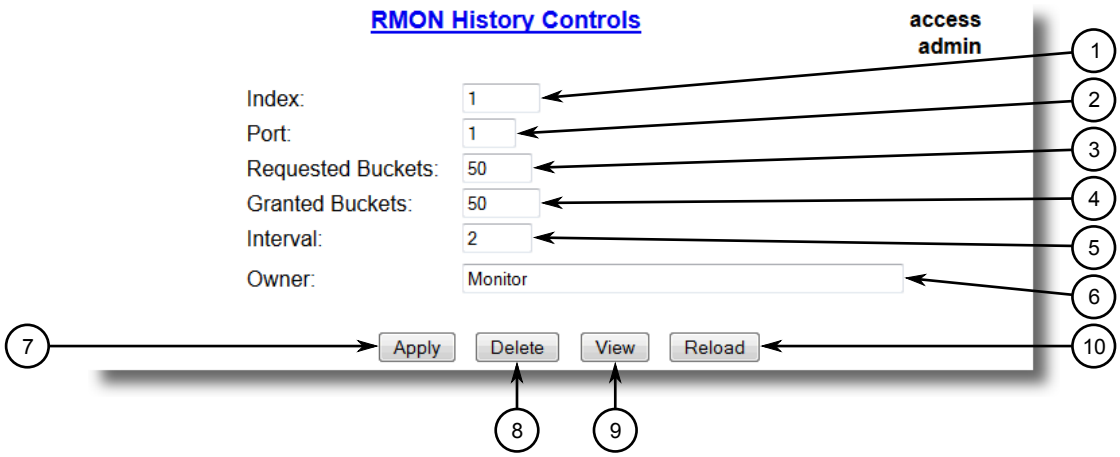


Figure 54 : Formulaire RMON History Controls

1. Zone Index **2.** Zone Port **3.** Zone Requested Buckets **4.** Zone Granted Buckets **5.** Zone Interval **6.** Zone Owner **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Index	**Synopsis :** 1 à 65535 **Par défaut :** 1 Index de cet enregistrement RMON History Contol.
Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Requested Buckets	**Synopsis :** 1 à 4000 **Par défaut :** 50 Nombre maximum de compartiments requis pour le groupe de statistiques d'historique de collecte RMON. La plage va de 1 à 4000. La valeur par défaut est 50.
Granted Buckets	**Synopsis :** 0 à 65535

Paramètre	Description
	Nombre de compartiments accordés pour cet historique de collecte RMON. Le champ ne peut pas être édité.
Interval	**Synopsis :** 1 à 3600 **Par défaut :** 1800 Nombre de secondes pendant lesquelles les données sont échantillonnées pour chaque compartiment. La plage va de 1 à 3600. La valeur par défaut est 1800.
Owner	**Synopsis :** 127 caractères quelconques **Par défaut :** Monitor Le propriétaire de cet enregistrement. Nous recommandons de démarrer cette chaîne avec le mot 'monitor'.

4. Cliquez sur **Apply**.

Section 3.11.1.3

Suppression d'un contrôle d'historique RMON

Procédez comme suit pour supprimer un contrôle d'historique RMON :

1. Accédez à ***Ethernet Stats » Configure RMON History Controls***. Le tableau **RMON History Controls** s'affiche.

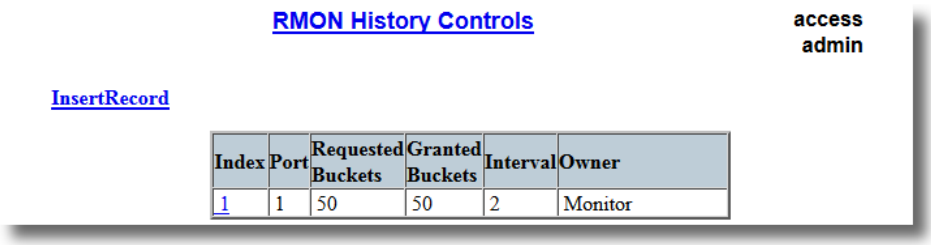


Figure 55 : Tableau RMON History Controls

2. Sélectionnez le contrôle d'historique dans le tableau. Le formulaire **RMON History Controls** s'affiche.

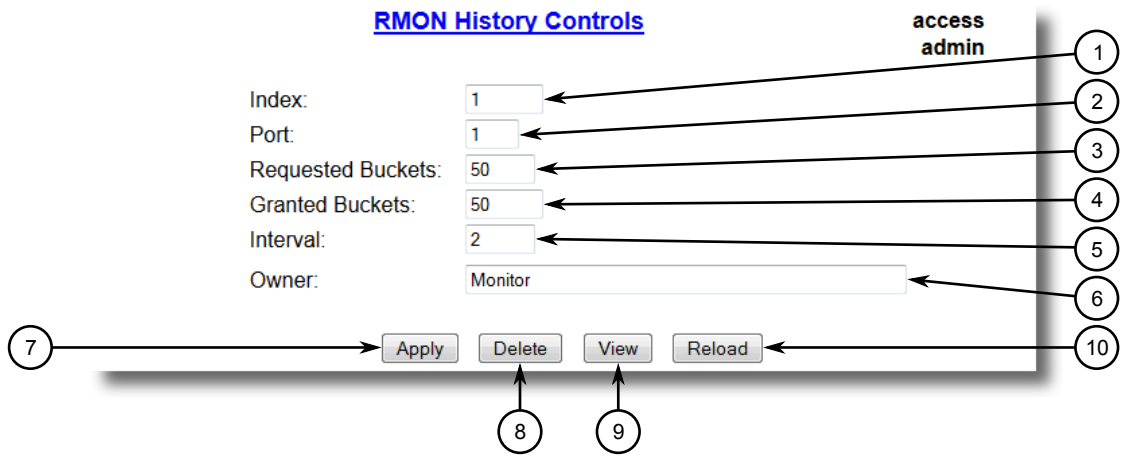


Figure 56 : Formulaire RMON History Controls

1. Zone Index **2.** Zone Port **3.** Zone Requested Buckets **4.** Zone Granted Buckets **5.** Zone Interval **6.** Zone Owner **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton Reload

3. Cliquez sur **Delete**.

Section 3.11.2

Gestion des alarmes RMON

Lorsque des alarmes Remote Monitoring (RMON) sont configurées, RUGGEDCOM ROS examine l'état d'une variable statistique spécifique.

Les alarmes Remote Monitoring (RMON) définissent des seuils supérieurs et inférieurs pour les valeurs réglementaires de variables statistiques dans un intervalle donné. Cela permet à RUGGEDCOM ROS de détecter des événements qui se produisent plus rapidement qu'une fréquence maximum spécifiée et moins rapidement qu'une fréquence minimum.

Lorsque la fréquence de modification d'une valeur statistique dépasse sa limite, une alarme INFO interne est toujours générée. Pour plus d'informations sur l'affichage d'alarmes, voir Section 4.6.2, « Affichage et effacement d'alarmes verrouillées ».

En outre, un dépassement de seuil statistique peut entraîner une activité supplémentaire. Une alarme RMON peut être configurée de manière à pointer vers un événement RMON spécifique, qui peut générer un trap SNMP, une entrée dans le journal des événements ou les deux. L'événement RMON peut également diriger des alarmes vers différents utilisateurs définis pour SNMP.

L'alarme peut pointer vers un événement différent pour chacun des seuils. Par conséquent, des combinations telles que *trap en cas de seuil montant* ou *trap en cas de seuil montant, journal et trap en cas de seuil descendant* sont possibles.

Chaque alarme RMON peut être configurée de manière à ce que sa première occurrence se produise pour les seuils montants, les seuils descendants ou tous les seuils dépassant leurs limites.

La possibilité de configurer des seuils supérieurs et inférieurs de la valeur d'une statistique mesurée donne la possibilité d'ajouter une hystérésis au processus de génération d'alarme.

Si la valeur de la statistique mesurée pendant un certain intervalle est comparée à un seuil unique, des alarmes sont générées chaque fois que la statistique dépasse le seuil. Si la valeur de la statistique fluctue autour du seuil,

une alarme peut être générée à chaque intervalle de mesure. Programmer des seuils supérieurs et inférieurs différents élimine les alarmes parasites. La valeur statistique doit *fluctuer* entre les seuils avant qu'une alarme ne puisse être générée. Vous trouverez ci-dessous une illustration de différents schémas de génération d'alarmes résultant d'un échantillon statistique et le même échantillon avec l'hystérésis appliquée.

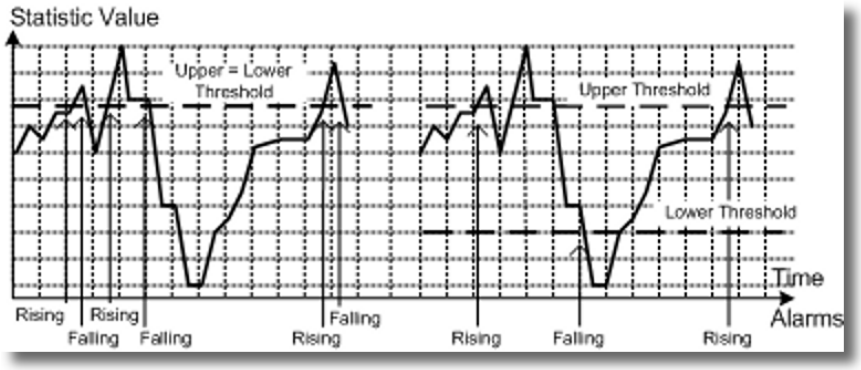


Figure 57 : Le processus d'alarme

Il existe deux méthodes d'évaluation d'une statistique pour déterminer quand générer un événement : delta et absolue.

Pour plus de statistiques, par exemple des erreurs de ligne, il est recommandé de générer une alarme lorsqu'un débit est dépassé. L'alarme par défaut de la méthode de mesure *delta*, qui examine les modifications dans une statistique à la fin de chaque intervalle de mesure.

Il est préférable de générer des alarmes lors que le nombre total ou absolu d'événements dépasse un seuil. Dans ce cas, définissez le type d'intervalle de mesure sur *absolu*.

SOMMAIRE

- Section 3.11.2.1, « Affichage d'une liste d'alarmes RMON »
- Section 3.11.2.2, « Ajout d'une alarme RMON »
- Section 3.11.2.3, « Suppression d'une alarme RMON »

Section 3.11.2.1

Affichage d'une liste d'alarmes RMON

Pour afficher une liste d'alarmes RMON, accédez à ***Ethernet Stats » Configure RMON Alarms***. Le tableau **RMON Alarms** s'affiche.

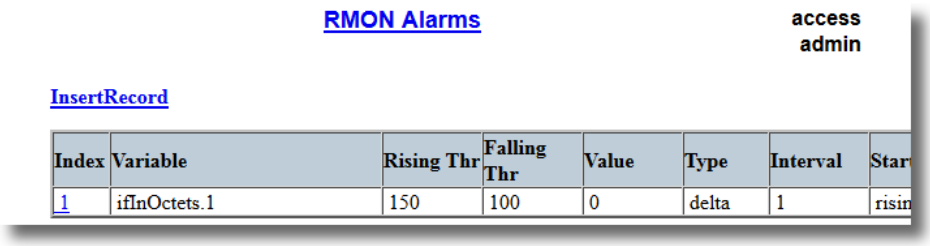


Figure 58 : Tableau RMON Alarms

Si aucune alarme n'a été configurée, ajoutez des alarmes en fonction de vos besoins. Pour plus d'informations, voir Section 3.11.2.2, « Ajout d'une alarme RMON ».

Section 3.11.2.2

Ajout d'une alarme RMON

Procédez comme suit pour ajouter une alarme RMON :

1. Accédez à ***Ethernet Stats » Configure RMON Alarms***. Le tableau **RMON Alarms** s'affiche.

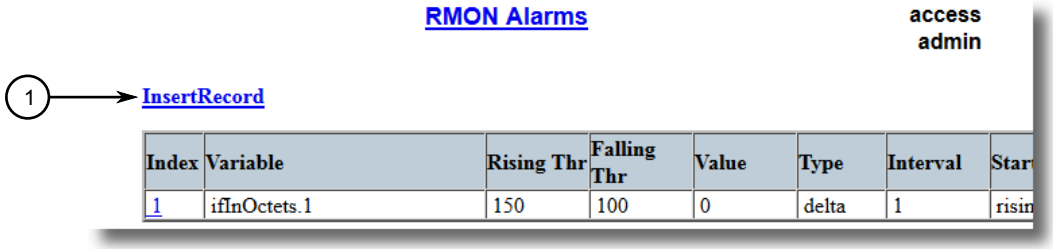


Figure 59 : Tableau RMON Alarms

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **RMON Alarms** s'affiche.

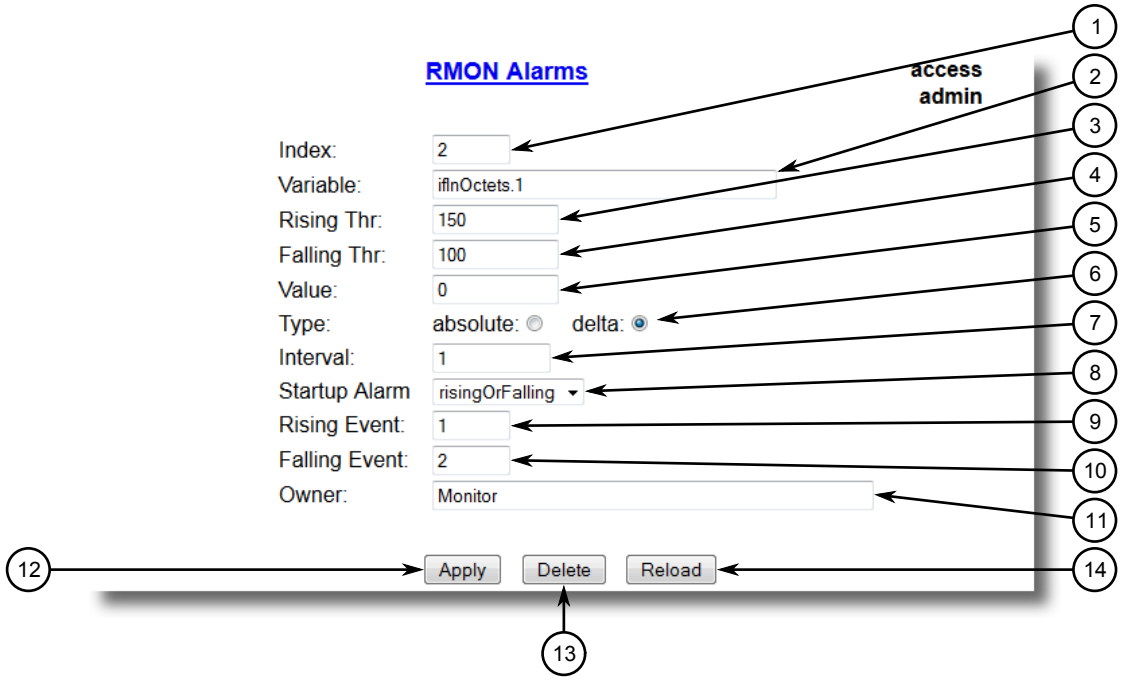


Figure 60 : Formulaire RMON Alarms

1. Zone Index **2.** Zone Variable **3.** Zone Rising Thr **4.** Zone Falling Thr **5.** Zone Value **6.** Options Type **7.** Zone Interval **8.** Liste Startup Alarm **9.** Zone Rising Event **10.** Zone Falling Event **11.** Zone Owner **12.** Bouton Apply **13.** Bouton Delete **14.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Index	**Synopsis :** 1 à 65535 **Par défaut :** 1 Index de cet enregistrement RMON Alarm.
Variable	**Synopsis :** Identificateur d'objet SNMP - jusqu'à 39 caractères L'identificateur d'objet SNMP (OID) de la variable spécifique à échantillonner. Seules les variables qui résolvent une primitive ASN.1 de type INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge ou TimeTicks) peuvent être échantillonnées. Une liste d'objets peut être imprimée à l'aide de la commande d'environnement 'rmon'. Le format OID : objectName.index1.index2... ou le format d'index dépend du type d'objet d'index.
Rising Thr	**Synopsis :** -2147483647 à 2147483647 **Par défaut :** 0 Seuil de la variable échantillonnée. Lorsque la valeur de variable échantillonnée actuelle est supérieure ou égale à ce seuil, et si la valeur au dernier intervalle d'échantillonnage est inférieure à ce seuil, un événement unique est généré. Un événement unique est également généré si le premier échantillon créé après cet enregistrement est supérieur ou égal à ce seuil et l'alarme de démarrage associée est 'rising' (montante). Une fois l'alarme montante générée, un autre événement similaire ne sera pas généré avant que la valeur échantillonnée passe en-dessous de ce seuil et atteigne la valeur de FallingThreshold.
Falling Thr	**Synopsis :** -2147483647 à 2147483647 **Par défaut :** 0

Paramètre	Description
	Seuil de la variable échantillonnée. Lorsque la valeur de variable échantillonnée actuelle est inférieure ou égale à ce seuil, et si la valeur au dernier intervalle d'échantillonnage est supérieure à ce seuil, un événement unique est généré. Un événement unique est également généré si le premier échantillon créé après cet enregistrement est inférieur ou égal à ce seuil et l'alarme de démarrage associée est 'falling' (descendante). Une fois l'alarme descendante générée, un autre événement similaire ne sera pas généré jusqu'à ce que la valeur échantillonnée passe au-dessus de ce seuil et atteigne la valeur de RisingThreshold.
Value	**Synopsis :** -2147483647 à 2147483647 Valeur de l'objet de surveillance pendant la dernière période d'échantillonnage. La présentation de la valeur dépend du type d'échantillon ('absolute' or 'delta').
Type	**Synopsis :** { absolute, delta } **Par défaut :** delta Méthode d'échantillonnage de la variable sélectionnée et de calcul de la valeur à comparer avec les seuils. La valeur du type d'échantillon peut être 'absolu' ou 'Delta'.
Interval	**Synopsis :** 0 à 2147483647 **Par défaut :** 60 Nombre de secondes pendant lesquelles les données sont échantillonnées avec le seuil montant et le seuil descendant.
Startup Alarm	**Synopsis :** { rising, falling, risingOrFalling } **Par défaut :** risingOrFalling Alarme pouvant être envoyée lorsque cet enregistrement est créé si la condition pour l'alarme montante est remplie. La valeur de l'alarme de démarrage peut être 'rising', 'falling' ou 'risingOrFalling'.
Rising Event	**Synopsis :** 0 à 65535 **Par défaut :** 0 L'index de l'événement utilisé lorsqu'un seuil descendant est dépassé. S'il n'existe aucune entrée correspondante dans le tableau Event, aucune association n'existe. Aucun événement n'est généré en particulier si la valeur est zéro.
Falling Event	**Synopsis :** 0 à 65535 **Par défaut :** 0 L'index de l'événement utilisé lorsqu'un seuil montant est dépassé. S'il n'existe aucune entrée correspondante dans le tableau Event, aucune association n'existe. Aucun événement n'est généré en particulier si la valeur est zéro.
Owner	**Synopsis :** 127 caractères quelconques **Par défaut :** Monitor Le propriétaire de cet enregistrement. Nous recommandons de démarrer cette chaîne avec le mot 'monitor'.

4. Cliquez sur **Apply**.

Section 3.11.2.3

Suppression d'une alarme RMON

Procédez comme suit pour supprimer une alarme RMON :

1. Accédez à ***Ethernet Stats » Configure RMON Alarms***. Le tableau **RMON Alarms** s'affiche.

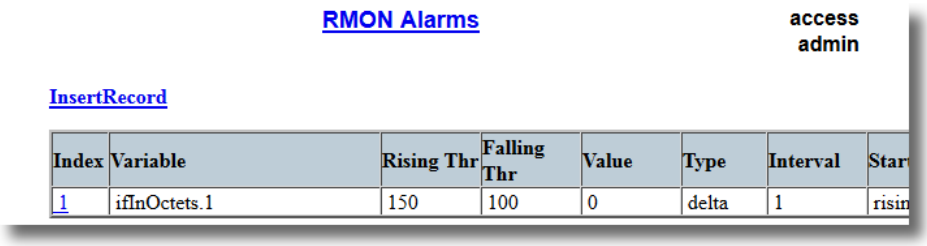


Figure 61 : Tableau RMON Alarms

2. Sélectionnez l'alarme dans le tableau. Le formulaire **RMON Alarms** s'affiche.

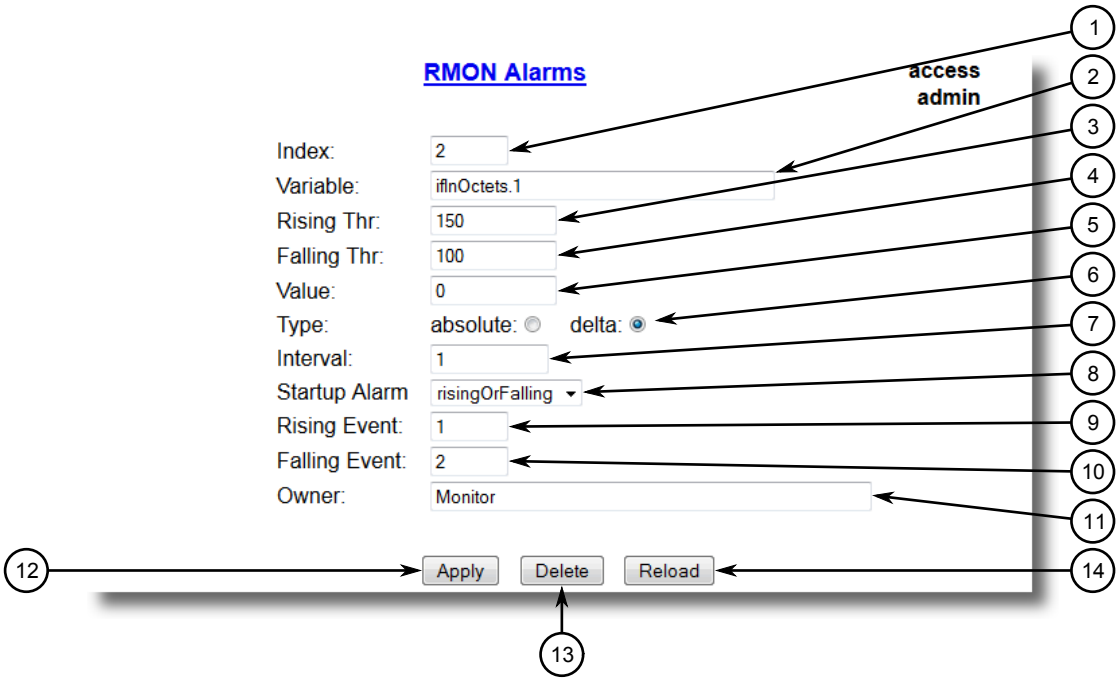


Figure 62 : Formulaire RMON Alarms

1. Zone Index **2.** Zone Variable **3.** Zone Rising Thr **4.** Zone Falling Thr **5.** Zone Value **6.** Options Type **7.** Zone Interval **8.** Liste Startup Alarm **9.** Zone Rising Event **10.** Zone Falling Event **11.** Zone Owner **12.** Bouton Apply **13.** Bouton Delete **14.** Bouton Reload

3. Cliquez sur **Delete**.

Section 3.11.3

Gestion des événements RMON

Les événements RMON (Remote Monitoring) définissent des profils de comportement utilisés pour la journalisation des événements. Ces profils sont utilisés par les alarmes RMON pour envoyer des traps et des journaliser des événements.

Chaque alarme peut spécifier qu'une entrée de journal est créée en son nom lorsque l'événement se produit. Chaque entrée peut également spécifier qu'une notification doit être générée au moyen de messages de trap SNMP. Dans ce cas, l'utilisateur pour le message de trap est spécifié comme la *Communauté*.

Deux traps sont définis : risingAlarm et fallingAlarm.

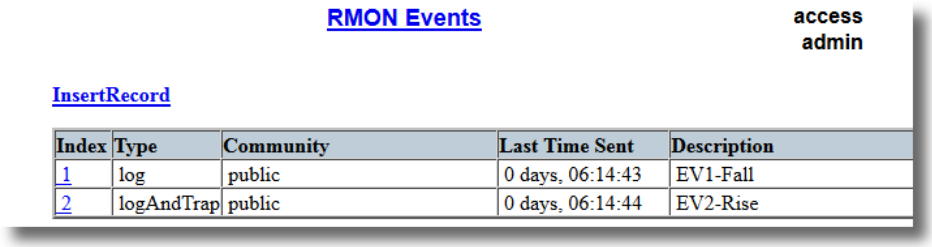
SOMMAIRE

- Section 3.11.3.1, « Affichage d'une liste d'événements RMON »
- Section 3.11.3.2, « Ajout d'un événement RMON »
- Section 3.11.3.3, « Suppression d'un événement RMON »

Section 3.11.3.1

Affichage d'une liste d'événements RMON

Pour afficher une liste d'événements RMON, accédez à ***Ethernet Stats » Configure RMON Events***. Le tableau **RMON Events** s'affiche.



Index	Type	Community	Last Time Sent	Description
1	log	public	0 days, 06:14:43	EV1-Fall
2	logAndTrap	public	0 days, 06:14:44	EV2-Rise

Figure 63 : Tableau RMON Events

Si aucun événement n'a été configuré, ajoutez des événements en fonction de vos besoins. Pour plus d'informations, voir Section 3.11.3.2, « Ajout d'un événement RMON ».

Section 3.11.3.2

Ajout d'un événement RMON

Procédez comme suit pour ajouter une alarme RMON :

1. Accédez à ***Ethernet Stats » Configure RMON Events***. Le tableau **RMON Events** s'affiche.

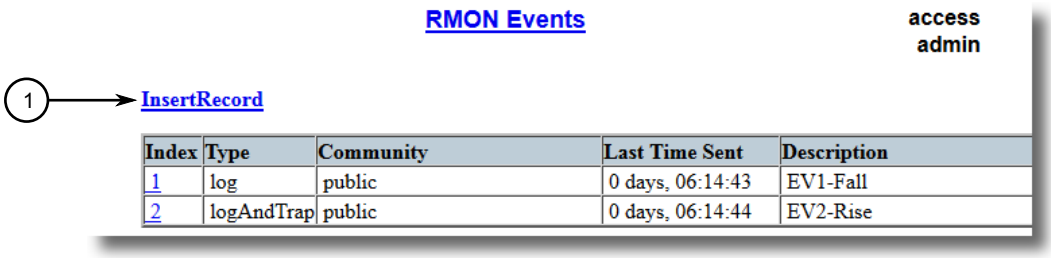


Figure 64 : Tableau RMON Events

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **RMON Events** s'affiche.

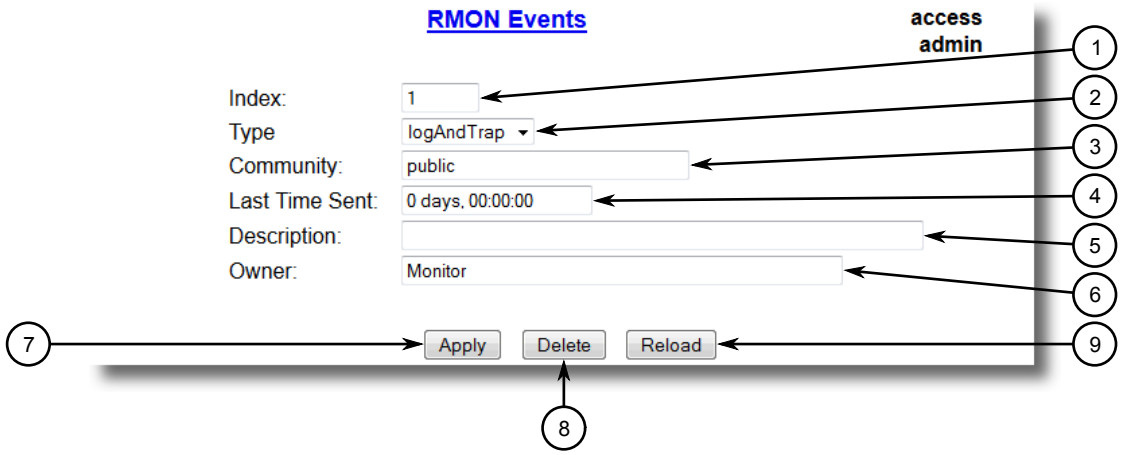


Figure 65 : Formulaire RMON Events

1. Zone Index **2.** Liste Type **3.** Zone Community **4.** Zone Last Time Sent **5.** Zone Description **6.** Zone Owner **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton View **10.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Index	**Synopsis :** 1 à 65535 **Par défaut :** 3 Index de cet enregistrement RMON Event.
Type	**Synopsis :** { none, log, snmpTrap, logAndTrap } **Par défaut :** logAndTrap Type de notification générée par la sonde à propos de cet événement. Dans le cas de 'log', une entrée est ajoutée dans le tableau RMON Log pour chaque événement. Dans le cas de snmp_trap, un trap SNMP est envoyé à une ou plusieurs stations de gestion.
Community	**Synopsis :** 31 caractères quelconques **Par défaut :** public Si le trap SNMP doit être envoyé, il est envoyé à la communauté SNMP spécifiée par cette chaîne.

Paramètre	Description
Last Time Sent	**Synopsis :** DDDD jours, HH:MM:SS Temps depuis le dernier redémarrage au moment où cette entrée d'événement a généré un événement en dernier. Si cette entrée n'a pas généré d'événement, cette valeur est 0.
Description	**Synopsis :** 127 caractères quelconques **Par défaut :** EV2-Rise Commentaire décrivant cet événement.
Owner	**Synopsis :** 127 caractères quelconques **Par défaut :** Monitor Le propriétaire de cet enregistrement d'événement. Nous recommandons de démarrer cette chaîne avec le mot 'monitor'.

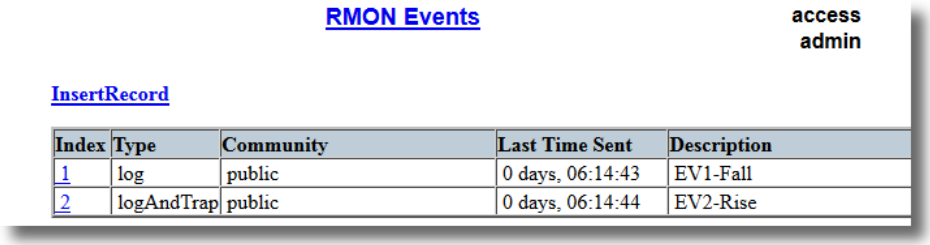
4. Cliquez sur **Apply**.

Section 3.11.3.3

Suppression d'un événement RMON

Procédez comme suit pour supprimer un événement RMON :

1. Accédez à ***Ethernet Stats » Configure RMON Events***. Le tableau **RMON Events** s'affiche.



Index	Type	Community	Last Time Sent	Description
1	log	public	0 days, 06:14:43	EV1-Fall
2	logAndTrap	public	0 days, 06:14:44	EV2-Rise

Figure 66 : Tableau RMON Events

2. Sélectionnez l'événement dans le tableau. Le formulaire **RMON Events** s'affiche.

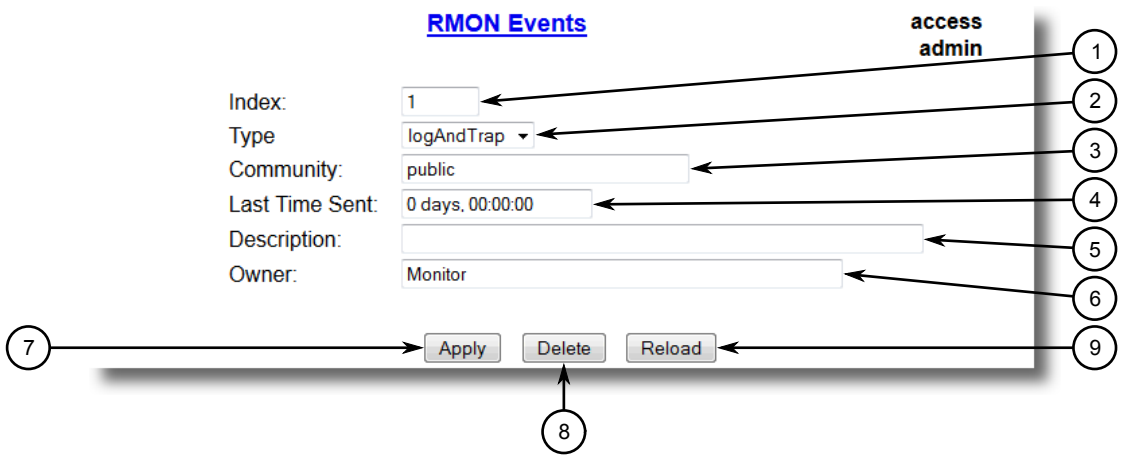


Figure 67 : Formulaire RMON Events

1. Zone Index **2.** Liste Type **3.** Zone Community **4.** Zone Last Time Sent **5.** Zone Description **6.** Zone Owner **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton View **10.** Bouton Reload

3. Cliquez sur **Delete**.

Section 3.12

Chargement/téléchargement du firmware

Cette section décrit la manière de mettre à niveau ou rétrograder le firmware pour RUGGEDCOM ROS.

SOMMAIRE

- Section 3.12.1, « Mise à niveau du firmware »
- Section 3.12.2, « Rétrogradage du firmware »

Section 3.12.1

Mise à niveau du firmware

Une mise à niveau du firmware RUGGEDCOM ROS (notamment lefirmware principal, du chargeur de démarrage et FPGA) peut être nécessaire pour tirer parti des nouvelles fonctionnalités ou correctifs bug fixes. Des versions de firmware binaires, notamment les mises à jour, sont disponibles en envoyant une demande de support via le site Web Siemens Industry Online Support [https://support.industry.siemens.com]. Pour plus d'informations, voir https://support.industry.siemens.com/My/ww/en/requests.

Les images de firmware binaires transférées sur l'appareil sont stockées dans une mémoire flash non volatile et requièrent une réinitialisation de l'appareil pour prendre effet.

REMARQUE
L'adresse IP définie pour l'appareil n'est pas modifiée après une mise à niveau du firmware.

Procédez comme suit pour mettre à niveau le firmware RUGGEDCOM ROS :

1. Chargez une différente version de l'image de firmware binaire dans l'appareil. Pour plus d'informations, voir Section 3.5, « Chargement/téléchargement de fichiers ».
2. Réinitialisez l'appareil pour terminer l'installation. Pour plus d'informations, voir Section 3.13, « Réinitialisation de l'appareil ».
3. Accédez au shell CLI et vérifiez que la nouvelle version logicielle a été installée en saisissant**`version`**. Les versions actuellement installées du firmware principal et de démarrage sont affichées.

```
>version
Current ROS-CF52 Boot Software v2.20.0 (Jan 01 4.3 00:01)
Current ROS-CF52 Main Software v4.3.0 (Jan 01 4.3 00:01)
```

Section 3.12.2

Rétrogradage du firmware

Le rétrogradage du firmware RUGGEDCOM ROS n'est généralement pas recommandé car il peut avoir des effets non prévisibles. Cependant, procédez comme suit si un rétrogradage est requis :

IMPORTANT !
Avant de rétrograder le firmware, assurez-vous que le matériel et les types de code FPGA installés dans l'appareil sont pris en charge par la version antérieure du firmware. Consultez les Release Notes de la version antérieure du firmware pour confirmer.

ATTENTION !
Ne rétrogradez pas la version de démarrage de RUGGEDCOM ROS.

1. Déconnectez l'appareil du réseau.
2. Connectez-vous à l'appareil en tant qu'administrateur. Pour plus d'informations, voir Section 2.2, « Ouverture de session ».
3. Effectuez une copie locale du fichier de configuration actuel. Pour plus d'informations, voir Section 3.5, « Chargement/téléchargement de fichiers ».

   IMPORTANT !
   Ne rétrogradez jamais le firmware avec chiffrement activé à une version ne prenant pas en charge le chiffrement.

4. Restaurez l'appareil à ces paramètres par défaut. Pour plus d'informations, voir Section 3.3, « Restauration des valeurs par défaut ».
5. Chargez et appliquez la version de firmware antérieure et ses fichiers FPGA associés avec les méthodes utilisées pour installer des versions de firmware plus actuelles. Pour plus d'informations, voir Section 3.12.1, « Mise à niveau du firmware ».
6. Appuyez sur **Ctrl-S** pour accéder à la CLI.
7. Effacez tous les journaux en saisissant :

   ```
   clearlogs
   ```

8. Effacez toutes les alarmes en saisissant :

   ```
   clearalarms
   ```

IMPORTANT !
Une fois le firmware et les fichiers FPGA rétrogradés, sachez que certains réglages de l'ancienne version peuvent être perdus ou réinitialisés aux valeurs par défaut (notamment les mots de passe utilisateur en cas de rétrogradage depuis une version liée à la sécurité), car ces tableaux ou champs spécifiques peuvent ne pas exister dans la version de firmware antérieure. Pour cette raison, l'unité doit être configurée après le rétrogradage.

9. Configurez l'appareil en fonction de vos besoins.

Section 3.13
Réinitialisation de l'appareil

Procédez comme suit pour réinitialiser l'appareil :

1. Accédez à ***Diagnostics » Reset Device***. Le formulaire **Reset Device** s'affiche.

Figure 68 : Formulaire Reset Device

1. Bouton Confirm

2. Cliquez sur **Confirm**.

Section 3.14
Désactivation de l'appareil

Avant de mettre l'appareil hors service (de manière permanente ou pour la maintenance par un tiers), assurez-vous que ce dernier a été complètement désactivé. Ceci implique la suppression de toutes les informations propriétaires sensibles.

Procédez comme suit pour désactiver l'appareil :

1. Déconnectez tous les câbles réseau de l'appareil.
2. Connectez-vous à l'appareil via le port de console série RS-232. Pour plus d'informations, voir Section 2.1.1, « Connexion directe ».
3. Restaurez tous les réglages par défaut pour l'appareil. Pour plus d'informations, voir Section 3.3, « Restauration des valeurs par défaut ».
4. Accédez à la CLI. Pour plus d'informations, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
5. Chargez une version vierge du fichier`banner.txt` sur l'appareil pour remplacer le fichier existant. Pour plus d'informations sur le chargement d'un fichier, voir Section 3.5, « Chargement/téléchargement de fichiers ».
6. Confirmez la réussite du chargement en saisissant :

```
type banner.txt
```

7. Effacez les journaux système et d'incidents en saisissant :

```
clearlog
```

8. Générez un certificat SSL quelconque en saisissant :

```
sslkeygen
```

Ceci peut prendre plusieurs minutes. Pour vérifier que le certificat a été généré, saisissez :

```
type syslog.txt
```

Lorsque la phrase

```
Generated ssl.crt was saved
```

s'affiche dans le journal, le certificat SSL a été généré.

9. Générez des clés SSH quelconques en saisissant :

```
sshkeygen
```

Ceci peut prendre plusieurs minutes. Pour vérifier que les clés ont été générées, saisissez :

```
type syslog.txt
```

Lorsque la phrase

```
Generated ssh.keys was saved
```

s'affiche dans le journal, les clés SSH ont été générées.

10. Défragmentez et effacez toute la mémoire flash libre en saisissant :

```
flashfile defrag
```

Ceci peut prendre plusieurs minutes.

4 Administration système

Le présent chapitre décrit la manière d'exécuter différentes tâches administratives liées à l'identification d'appareil, aux autorisations utilisateur, à la configuration d'alarmes, aux certificats et aux clés, etc.

SOMMAIRE

- Section 4.1, « Configuration du système d'information »
- Section 4.2, « Personnalisation de l'écran d'ouverture de session »
- Section 4.3, « Gestion des mots de passe »
- Section 4.4, « Effacement de données privées »
- Section 4.5, « Activation/désactivation de l'interface Web »
- Section 4.6, « Gestion des alarmes »
- Section 4.7, « Gestion du fichier de configuration »
- Section 4.8, « Gestion d'un serveur d'authentification »

Section 4.1

Configuration du système d'information

Procédez comme suit pour configurer les informations de base pouvant être utilisées pour identifier l'appareil, son emplacement et/ou son propriétaire :

1. Accédez à ***Administration » Configure System Identification***. Le formulaire **System Identification** s'affiche.

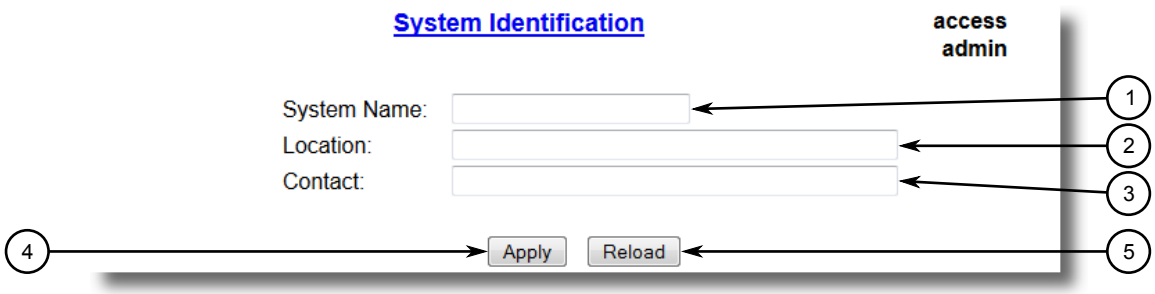


Figure 69 : Formulaire System Identification

1. Zone System Name **2.** Zone Location **3.** Zone Contact **4.** Bouton Apply **5.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
System Name	**Synopsis :** 24 caractères quelconques Le nom du système est affiché dans tous les écrans de menu RUGGEDCOM ROS. Il peut être ainsi plus facile d'identifier les commutateurs au sein de votre réseau si tous les commutateurs ont un nom univoque.
Location	**Synopsis :** 49 caractères quelconques L'emplacement peut être utilisé pour indiquer l'emplacement physique du commutateur. Il est affiché dans l'écran de connexion comme moyen supplémentaire de vous assurer que vous utilisez le commutateur souhaité.
Contact	**Synopsis :** 49 caractères quelconques Le contact peut être utilisé pour identifier la personne responsable de la gestion du commutateur. Vous pouvez entrer un nom, un numéro de téléphone, une adresse e-mail, etc. Le contact est affiché dans l'écran de connexion afin que cette personne puisse être contactée en cas de besoin.

3. Cliquez sur **Apply**.

Section 4.2

Personnalisation de l'écran d'ouverture de session

Pour afficher un message de bienvenue personnalisé, des informations sur l'appareil ou toute autre information dans l'écran d'ouverture de session pour les interfaces Web et de console, ajoutez un texte au fichier`banner.txt` stocké sur l'appareil.

Si le fichier`banner.txt` est vide, seuls les champs**Username** et**Password** apparaissent sur l'écran d'ouverture de session.

Pour mettre à jour le fichier`banner.txt`, téléchargez le fichier depuis l'appareil, modifiez-le et rechargez-le sur l'appareil. Pour plus d'informations sur le chargement et le téléchargement de fichiers, voir Section 3.5, « Chargement/téléchargement de fichiers ».

Section 4.3

Gestion des mots de passe

RUGGEDCOM ROS permet la configuration de jusqu'à trois profils utilisateur localement sur l'appareil. Chaque profil correspond à l'un des niveaux d'accès suivants :

- Invité
- Opérateur
- Administrateur

Les niveaux d'accès donnent ou retirent à l'utilisateur la possibilité de modifier des réglages et d'exécuter des commandes.

Droits	Type d'utilisateur		
	Invité	Opérateur	Administrateur
Réglages d'affichage	✓	✓	✓

Droits	Type d'utilisateur		
	Invité	Opérateur	Administrateur
Effacer les journaux	×	✓	✓
Réinitialiser les alarmes	×	✓	✓
Effacer les statistiques	×	✓	✓
Modifier les réglages de base	×	✓	✓
Modifier les réglages avancés	×	×	✓
Exécuter des commandes	×	×	✓

Les mots de passe par défaut sont configurés initialement pour chaque type d'utilisateur. Il est recommandé de les modifier avant la mise en service de l'appareil.

REMARQUE
Les utilisateurs peuvent également être vérifiés via le serveur RADIUS or TACACS+. En cas d'activation pour l'authentification et l'autorisation, le serveur RADIUS ou TACACS+ est utilisé si aucun réglage local n'existe. Pour plus d'informations sur la configuration d'un serveur RADIUS ou TACACS+, voir Section 4.8, « Gestion d'un serveur d'authentification ».

ATTENTION !
Pour éviter un accès non autorisé à l'appareil, assurez-vous de modifier les mots de passe par défaut pour chaque profil avant de mettre l'appareil en service.

SOMMAIRE

- Section 4.3.1, « Configuration de mots de passe »
- Section 4.3.2, « Réinitialisation de mots de passe »

Section 4.3.1

Configuration de mots de passe

Procédez comme suit pour configurer des mots de passe pour un ou plusieurs profils utilisateur :

1. Accédez à ***Administration » Configure Passwords***. Le formulaire **Configure Passwords** s'affiche.

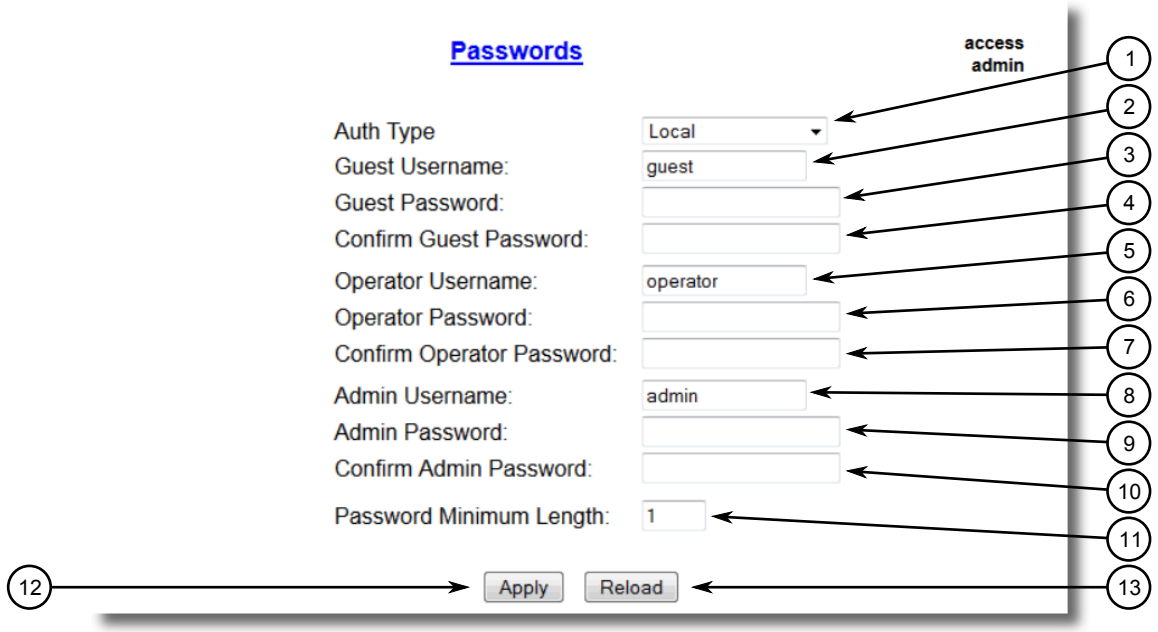


Figure 70 : Formulaire Configure Passwords

1. Zone Auth Type **2.** Zone Guest Username **3.** Zone Guest Password **4.** Zone Confirm Guest Password **5.** Zone Operator Username **6.** Zone Operator Password **7.** Zone Confirm Operator Password **8.** Zone Admin Username **9.** Zone Admin Password **10.** Zone Confirm Admin Password **11.** Zone Password Minimum Length **12.** Bouton Apply **13.** Bouton Reload

REMARQUE

RUGGEDCOM ROS requiert que tous les mots de passes répondent à des directives strictes afin d'éviter l'utilisation de mots de passe faibles. Lors de la création d'un nouveau mot de passe, assurez-vous que les règles suivantes sont respectées :

- *Sa longueur ne doit pas dépasser 8 caractères.*
- *Il ne doit pas inclure le nom d'utilisateur ou 4 caractères continus figurant dans le nom d'utilisateur. Par exemple, si le nom d'utilisateur est **Subnet25**, le mot de passe ne peut pas être **subnet25admin** ou **subnetadmin** ou **net25admin**. **net25admin** ou **Sub25admin** sont cependant autorisés.*
- *Il doit comprendre au moins un caractère alphabétique et un chiffre. Les caractères spéciaux ne sont pas autorisés.*
- *Il ne doit pas comprendre plus de 3 chiffres à incrémentation ou décrémentation continue. Par exemple, **Sub123** et **Sub19826** sont autorisés, mais pas **Sub12345**.*

Une alarme est générée si un mot de passe faible est configuré. L'alarme de mot de passe faible peut être désactivée par l'utilisateur. Pour plus d'informations sur la désactivation d'alarmes, voir Section 4.6, « Gestion des alarmes ».

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Auth Type	**Synopsis :** { Local, RADIUS, TACACS+, RADIUSorLocal, TACACS+orLocal } **Par défaut :** Local

Paramètre	Description
	Le mot de passe peut être authentifié à l'aide de valeurs configurées localement ou du serveur distant RADIUS ou TACACS+. La définition d'une valeur résultant d'une combinaison quelconque comprenant RADIUS ou TACACS+ requiert la configuration du tableau Security Server. Réglages : • Local - authentification depuis le tableau Password local. • RADIUS - authentification à l'aide d'un serveur RADIUS. • TACACS+ - authentification à l'aide d'un serveur TACACS+. • RADIUSOrLocal - authentification à l'aide de RADIUS. Si le serveur n'est pas accessible, authentifiez-vous depuis le tableau Password local. • TACACS+OrLocal - Authentification à l'aide de TACACS+. Si le serveur n'est pas accessible, authentifiez-vous depuis le tableau Password local. **REMARQUE** *Lors de l'accès à la console, seules les informations d'identification locales sont vérifiées si Local, RADIUS ou TACACS+ est sélectionné. Si l'authentification RADIUSOrLocal ou TACACS+OrLocal est sélectionnée, les informations d'identification RADIUS ou TACACS+ sont respectivement vérifiées en premier. En cas d'échec de l'authentification, les informations d'identification locales sont vérifiées.*
Guest Username	**Synopsis :** 15 caractères quelconques **Par défaut :** guest Le mot de passe correspondant se trouve dans le champ Guest Password ; affichage uniquement, ne peut pas modifier des réglages ou exécuter une commande quelconque.
Guest Password	**Synopsis :** chaîne de 19 caractères ascii Le nom d'utilisateur correspondant se trouve dans le champ Guest Username ; affichage uniquement, ne peut pas modifier des réglages ou exécuter une commande quelconque.
Confirm Guest Password	**Synopsis :** chaîne de 19 caractères ascii Le nom d'utilisateur correspondant se trouve dans le champ Guest Username ; affichage uniquement, ne peut pas modifier des réglages ou exécuter une commande quelconque.
Operator Username	**Synopsis :** 15 caractères quelconques **Par défaut :** operator Le mot de passe correspondant se trouve dans le champ Operator Password ; ne peut pas modifier des réglages ; peut réinitialiser des alarmes, des statistiques, des journaux, etc.
Operator Password	**Synopsis :** chaîne de 19 caractères ascii Le nom d'utilisateur correspondant se trouve dans le champ Oper Username ; ne peut pas modifier des réglages ; peut réinitialiser des alarmes, des statistiques, des journaux, etc.
Confirm Operator Password	**Synopsis :** chaîne de 19 caractères ascii Le nom d'utilisateur correspondant se trouve dans le champ Oper Username ; ne peut pas modifier des réglages ; peut réinitialiser des alarmes, des statistiques, des journaux, etc.
Admin Username	**Synopsis :** 15 caractères quelconques **Par défaut :** admin Le mot de passe correspondant se trouve dans le champ Admin Password ; accès en lecture/écriture complet à tous les réglages et à toutes les commandes.
Admin Password	**Synopsis :** chaîne de 19 caractères ascii Le nom d'utilisateur correspondant se trouve dans le champ Admin Username ; accès en lecture/écriture complet à tous les réglages et à toutes les commandes.
Confirm Admin Password	**Synopsis :** chaîne de 19 caractères ascii

Paramètre	Description
	Le nom d'utilisateur correspondant se trouve dans le champ Admin Username ; accès en lecture/écriture complet à tous les réglages et à toutes les commandes.
Password Minimum Length	**Synopsis :** 1 à 17 **Par défaut :** 1 Configure la longueur minimale du mot de passe. Un nouveau mot de passe d'une longueur inférieure à la longueur minimale est rejeté.

3. Cliquez sur **Apply**.

Section 4.3.2

Réinitialisation de mots de passe

Les mots de passe doivent être enregistrés dans un emplacement sécurisé pour s'y référer ultérieurement Pour plus d'informations sur les meilleures pratiques d'authentification, voir Section 1.2, « Recommandations relatives à la sécurité ».

Lorsque le nom d'utilisateur et/ou le mot de passe pour le compte d'administrateur a été oublié, un utilisateur avec un accès physique à l'appareil peut restaurer tous les noms d'utilisateur et tous les mots de passe aux réglages par défaut.

Pour plus d'informations sur la réinitialisation de mots de passe, voir Section 4.4, « Effacement de données privées ».

Section 4.4

Effacement de données privées

En cas d'activation pendant un démarrage du système, un utilisateur avec accès console série peut effacer toutes les données de configuration et clés stockées sur l'appareil et restaurer tous les noms d'utilisateur et mots de passe aux paramètres par défaut.

Procédez comme suit pour effacer des données privées :

> **REMARQUE**
> *Les commandes utilisées dans la procédure ci-dessous sont dépendantes du temps. Si les limites de temps spécifiées sont dépassées avant la génération d'une réponse appropriée, l'appareil continue un démarrage normal.*

1. Connectez-vous à l'appareil via le port de console série RS-232. Pour plus d'informations, voir Section 2.1.1, « Connexion directe ».
2. Raccordez l'alimentation à l'appareil. L'invite suivante s'affiche au démarrage de l'appareil :

```
Press any key to start
```

3. Dans les quatre secondes, appuyez sur **CTRL** +**r**. La bannière d'accès s'affiche, suivie par l'invite de commande :

```
>
```

4. Saisissez la commande suivante, puis appuyez sur **Entrée** dans les 30 secondes :

```
clear private data
```

5. Lorsque la question "Do you want to clear private data (Yes/No)?" s'affiche, répondez par *yes* et appuyez sur **Entrée** dans les cinq secondes. La configuration et les clés dans la mémoire Flash sont remises à 0. Une entrée est créée dans le journal des événements. Les fichiers crashlog.txt (le cas échéant) et syslog.txt sont préservés. L'appareil est redémarré automatiquement.

Section 4.5

Activation/désactivation de l'interface Web

Dans certains cas, les utilisateurs peuvent souhaiter désactiver l'interface Web pour optimiser la cyber-sécurité.

Procédez comme suit pour désactiver ou activer l'interface Web :

> **REMARQUE**
> *L'interface Web peut être désactivée via l'interface utilisateur Web en configurant le paramètre Web Server Users Allowed dans le**formulaire IP Services**. Pour plus d'informations, voir Section 3.10, « Configuration des services IP ».*

1. Connectez-vous à l'appareil en tant qu'administrateur et accédez au shell CLI. Pour plus d'informations sur l'accès au shell CLI, voir Section 2.6, « Utilisation de l'interface de ligne de commande ».
2. Accédez à ***Administration » Configure IP Services » Web Server Users Allowed***.
3. Sélectionnez**Disabled** pour désactiver l'interface Web, ou sélectionnez le nombre désiré d'utilisateurs du serveur Web autorisés à activer l'interface.

Section 4.6

Gestion des alarmes

Les alarmes indiquent les occurrences d'événements pouvant être importants ou intéressants consignés par l'appareil.

Il existe deux types d'alarmes :

- Les**alarmes actives** signifient que les états de fonctionnement ne correspondent pas à un fonctionnement normal. Il peut s'agir par exemple de liaisons qui devraient être actives mais ne le sont pas, ou de fréquences d'erreur qui dépassent un certain seuil. Ces alarmes sont continuellement actives et ne sont effacées que lorsque le problème qui a généré une alarme est résolu.
- Les**alarmes passives** enregistrent les conditions anormales qui se sont produites dans le passé et n'affectent pas le fonctionnement actuel de l'appareil. Il peut s'agir par exemple de défaillances d'authentification, d'alarmes Remote Network MONitoring (RMON) générées par MIB ou d'états d'erreur qui ont temporairement dépassé un seuil donné. Ces alarmes peuvent être effacées de la liste des alarmes.

> **REMARQUE**
> *Pour plus d'informations sur les alarmes RMON, voir Section 3.11.2, « Gestion des alarmes RMON ».*

Lorsqu'une alarme de l'un des deux types est générée, un message s'affiche dans le coin supérieur droit de l'interface utilisateur. Si plusieurs alarmes ont été générées, le message indique le nombre d'alarmes. Les alarmes déclenchent également la LED Critical Failure Relay sur l'appareil. Le message et la LED restent actifs jusqu'à ce que l'alarme soit effacée.

REMARQUE
Les alarmes sont volatiles par nature. Toutes les alarmes (actives et passives) sont effacées au démarrage.

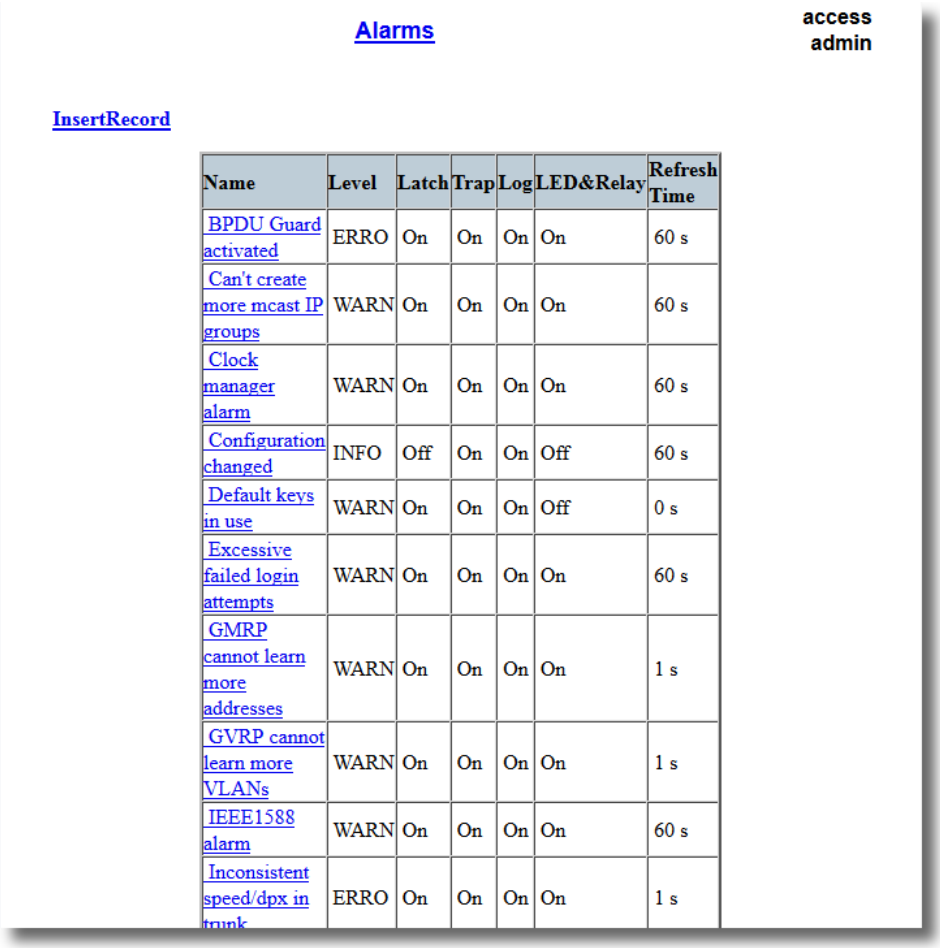
SOMMAIRE

- Section 4.6.1, « Affichage d'une liste d'alarmes préconfigurées »
- Section 4.6.2, « Affichage et effacement d'alarmes verrouillées »
- Section 4.6.3, « Configuration d'une alarme »
- Section 4.6.4, « Alarmes de sécurité liées à l'authentification »

Section 4.6.1

Affichage d'une liste d'alarmes préconfigurées

Pour afficher une liste d'alarmes préconfigurées pour l'appareil, accédez à ***Diagnostic » Configure Alarms***. Le tableau **Alarms** s'affiche.



Alarms

access
admin

InsertRecord

Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	ERRO	On	On	On	On	60 s
Can't create more mcast IP groups	WARN	On	On	On	On	60 s
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
GMRP cannot learn more addresses	WARN	On	On	On	On	1 s
GVRP cannot learn more VLANs	WARN	On	On	On	On	1 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Inconsistent speed/dpx in trunk	ERRO	On	On	On	On	1 s

Figure 71 : Tableau Alarms

REMARQUE
Cette liste d'alarmes (configurables et non-configurables) est accessible via l'interface de ligne de commande (CLI) à l'aide des **`alarmes`**. *Pour plus d'informations, voir Section 2.6.1, « Commandes CLI disponibles ».*

Pour plus d'informations sur la modification d'une alarme préconfigurée, voir Section 4.6.3, « Configuration d'une alarme ».

Section 4.6.2

Affichage et effacement d'alarmes verrouillées

Pour afficher une liste d'alarmes configurées pour être verrouillées, accédez à ***Diagnostics » View Latched Alarms***. Le tableau **Latched Alarms** s'affiche.

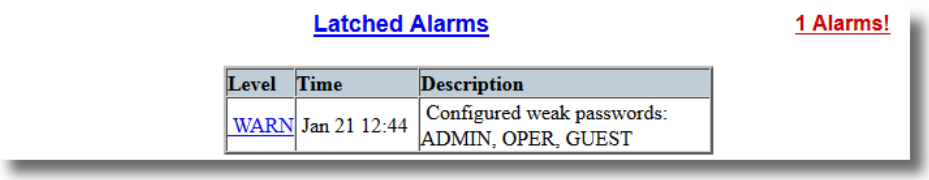


Figure 72 : Tableau Latched Alarms

Procédez comme suit pour effacer les alarmes passives de la liste :

1. Accédez à ***Diagnostics » Clear Latched Alarms***. Le formulaire **Clear Latched Alarms** s'affiche.

Figure 73 : Formulaire Clear Latched Alarms

1. Bouton Confirm

2. Cliquez sur **Confirm**.

Section 4.6.3

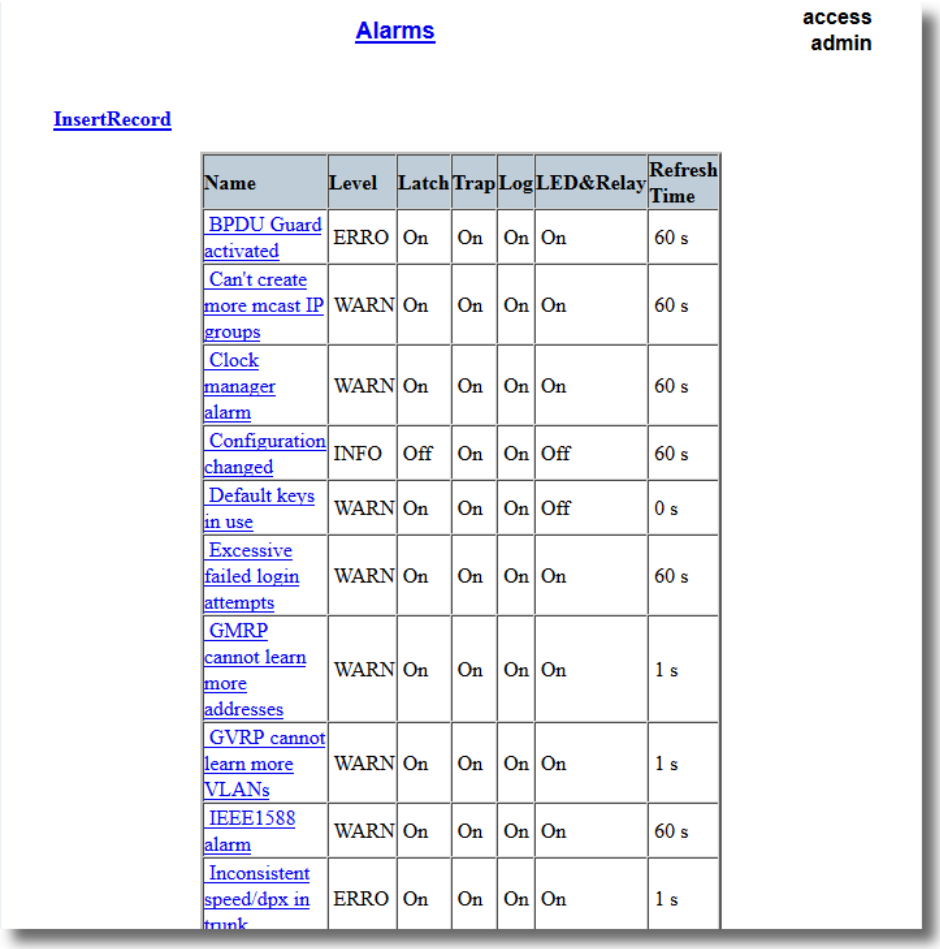
Configuration d'une alarme

Si toutes les alarmes sont préconfigurées sur l'appareil, certaines alarmes peuvent être modifiées en fonction de l'application. Cela comprend l'activation/la désactivation de certaines fonctionnalités et la modification du délai de rafraîchissement.

Procédez comme suit pour configurer une alarme :

IMPORTANT !
Les alarmes de niveau critique et alerte ne sont pas configurables et ne peuvent pas être désactivées.

1. Accédez à ***Diagnostic » Configure Alarms***. Le tableau **Alarms** s'affiche.



Alarms

access
admin

InsertRecord

Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	ERRO	On	On	On	On	60 s
Can't create more mcast IP groups	WARN	On	On	On	On	60 s
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
GMRP cannot learn more addresses	WARN	On	On	On	On	1 s
GVRP cannot learn more VLANs	WARN	On	On	On	On	1 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Inconsistent speed/dpx in trunk	ERRO	On	On	On	On	1 s

Figure 74 : Tableau Alarms

2. Sélectionnez une alarme. Le formulaire **Alarms** s'affiche.

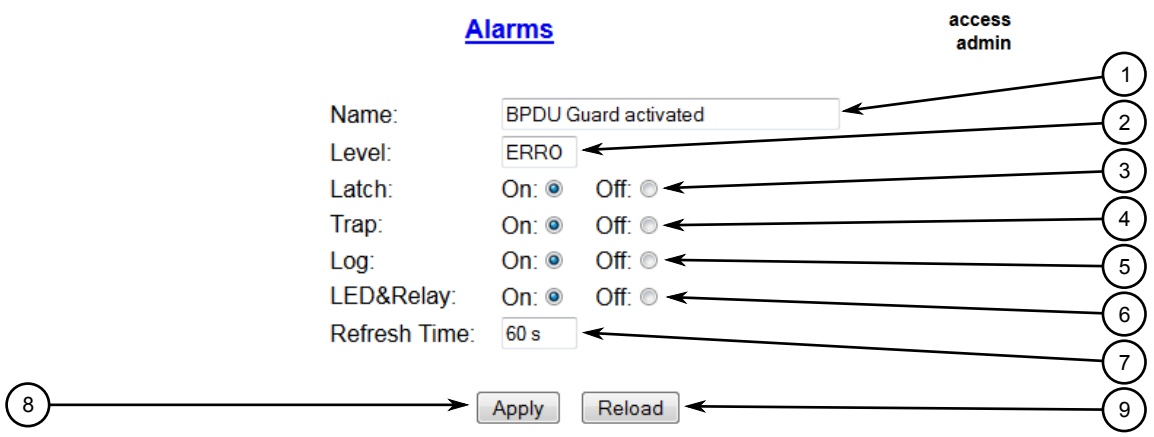


Figure 75 : Formulaire Alarms

1. Zone Name **2.** Zone Level **3.** Zone Latch **4.** Zone Trap **5.** Zone Log **6.** Zone LED & Relay **7.** Zone Refresh Time **8.** Bouton Apply **9.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Name	**Synopsis :** 34 caractères quelconques **Par défaut :** sys_alarm Nom d'alarme obtenu via la commande CLI`alarms`.
Level	**Synopsis :** { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG } Degré de gravité de l'alarme : • EMERG - l'appareil a rencontré une défaillance sérieuse qui a entraîné un redémarrage du système. • ALERT - l'appareil a rencontré une défaillance sérieuse qui n'a pas entraîné un redémarrage du système. • CRITICAL - l'appareil a rencontré un problème irrécupérable sérieux. • ERROR - l'appareil a rencontré un problème récupérable qui n'affecte pas sérieusement le fonctionnement. • WARNING - problème éventuellement sérieux affectant le fonctionnement général du système. • NOTIFY - une condition non attendue ou non autorisée a été détectée. • INFO - événement faisant partie d'un fonctionnement normal, par exemple un démarrage à froid, une connexion utilisateur, etc. • DEBUG - destiné uniquement au dépannage en usine. Ce paramètre n'est pas configurable.
Latch	**Synopsis :** { On, Off } **Par défaut :** Off Active l'occurrence de verrouillage de cette alarme dans le tableau Alarms.
Trap	**Synopsis :** { On, Off } **Par défaut :** Off Active l'envoi d'un trap SNMP pour cette alarme.
Log	**Synopsis :** { On, Off } **Par défaut :** Off Active la journalisation de l'occurrence de cette alarme dans syslog.txt.

Paramètre	Description
LED & Relay	**Synopsis :** { On, Off } **Par défaut :** Off Active le contrôle par LED et relais de sécurité pour cette alarme. Si le verrouillage n'est pas activé, ce champ reste désactivé.
Refresh Time	**Synopsis :** 0 s à 60 s **Par défaut :** 60 s Délai d'actualisation pour cette alarme.

4. Cliquez sur **Apply**.

Section 4.6.4

Alarmes de sécurité liées à l'authentification

Cette section décrit les messages de sécurité liés à l'authentification pouvant être générés par RUGGEDCOM ROS.

SOMMAIRE

- Section 4.6.4.1, « Alarmes de sécurité pour l'authentification de connexions »
- Section 4.6.4.2, « Messages de sécurité pour l'authentification de ports »

Section 4.6.4.1

Alarmes de sécurité pour l'authentification de connexions

RUGGEDCOM ROS propose différentes options de journalisation liées à l'authentification de connexions. Un utilisateur peut se connecter à un appareil RUGGEDCOM ROS de quatre manières différentes : Web, console, SSH ou Telnet. RUGGEDCOM ROS peut consigner des messages dans un journal système, envoyer un trap pour notifier un responsable SNMP et/ou générer une alarme lorsque des événements de connexion réussie ou d'échec de connexion se produisent. En outre, lorsqu'un mot de passe faible est configuré sur une unité ou si le serveur d'authentification principal pour TACACS+ ou RADIUS n'est pas accessible, RUGGEDCOM ROS génère des alarmes, envoie des traps SNMP et consigne des messages dans le journal système.

Vous trouverez ci-après une liste de messages d'alarme liés à l'authentification des utilisateurs :

- Weak Password Configured
- Login and Logout Information
- Excessive Failed Login Attempts
- RADIUS Server Unreachable
- TACACS Server Unreachable
- TACACS Response Invalid
- SNMP Authentication Failure

REMARQUE
Toutes les alarmes et tous les messages de journaux liés à l'authentification de connexions sont configurables. Pour plus d'informations sur la configuration d'alarmes, voir Section 4.6.3, « Configuration d'une alarme ».

Weak Password Configured

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsqu'un mot de passe faible est configuré dans le tableau **Passwords**.

Nom de message	Alarme	Trap SNMP	Syslog
Weak Password Configured	Oui	Oui	Oui

Default Keys In Use

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsque des clés par défaut sont utilisées. Pour plus d'informations sur les clés par défaut, voir Section 3.4, « Gestion des clés et certificats SSH et SSL ».

REMARQUE
Pour les versions non contrôlées (Non-Controlled (NC)) de RUGGEDCOM ROS, cette alarme est générée uniquement lorsque les clés SSL par défaut sont utilisées.

Nom de message	Alarme	Trap SNMP	Syslog
Default Keys In Use	Oui	Oui	Oui

Login and Logout Information

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsque des tentatives de connexion réussissent et échouent. Un message est également consigné dans le journal système lorsqu'un utilisateur avec un certain niveau de privilèges est déconnecté de l'appareil.

Les tentatives de connexion sont consignées quelle que soit la manière dont l'utilisateur accède à l'appareil (c'est-à-dire SSH, Web, Console, Telnet ou RSH). Cependant, lorsqu'un utilisateur se déconnecte, un message est uniquement consigné lorsque cet utilisateur accède à l'appareil via SSH, Telnet ou Console.

Nom de message	Alarme	Trap SNMP	Syslog
Successful Login	Oui	Oui	Oui
Failed Login	Oui	Oui	Oui
User Logout	Non	Non	Oui

Excessive Failed Login Attempts

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système après 10 tentatives de connexion non réussies par un utilisateur pendant un intervalle de cinq minutes. En outre, le service auquel l'utilisateur a tenté d'accéder est bloqué pendant une heure afin d'empêcher de nouvelles tentatives.

Nom de message	Alarme	Trap SNMP	Syslog
Excessive Failed Login Attempts	Oui	Oui	Oui

RADIUS Server Unreachable

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsque le serveur RADIUS principal n'est pas accessible.

Nom de message	Alarme	Trap SNMP	Syslog
Primary RADIUS Server Unreachable	Oui	Oui	Oui

TACACS+ Server Unreachable

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsque le serveur TACACS + principal n'est pas accessible.

Nom de message	Alarme	Trap SNMP	Syslog
Primary TACACS Server Unreachable	Oui	Oui	Oui

TACACS+ Response Invalid

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsque la réponse du serveur TACACS+ est reçu avec un CRC non valide.

Nom de message	Alarme	Trap SNMP	Syslog
TACACS Response Invalid	Oui	Oui	Oui

SNMP Authentication Failure

RUGGEDCOM ROS génère cette alarme, envoie un trap de défaillance d'authentification et consigne un message dans le journal système lorsqu'un responsable SNMP avec des informations d'identification incorrectes communique avec l'agent SNMP dans RUGGEDCOM ROS.

Nom de message	Alarme	Trap SNMP	Syslog
SNMP Authentication Failure	Oui	Oui	Oui

Section 4.6.4.2

Messages de sécurité pour l'authentification de ports

Vous trouverez ci-après une liste de messages d'alarme liés au contrôle d'accès aux ports dans RUGGEDCOM ROS :

- MAC Address Authorization Failure
- Secure Port X Learned MAC Addr on VLAN X
- Port Security Violated

MAC Address Authorization Failure

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsqu'un hôte connecté à un port sécurisé sur l'appareil communique à l'aide d'une adresse MAC source qui n'a pas été autorisée par RUGGEDCOM ROS, ou lorsque l'adresse MAC apprise de manière dynamique dépasse le nombre total d'adresses MAC configurées pour être apprises dynamiquement sur le port sécurisé. Ce message est applicable uniquement si le mode de sécurité du port est défini sur *Static MAC*.

Nom de message	Alarme	Trap SNMP	Syslog
MAC Address Authorization Failure	Oui	Oui	Oui

Secure Port X Learned MAC Addr on VLAN X

RUGGEDCOM ROS consigne un message dans le journal système et envoie un trap de modification de configuration lorsqu'une adresse MAC est apprise sur un port sécurisé. Port X indique le numéro de port sécurisé et le numéro de VLAN sur ce port. Ce message n'est pas configurable dans RUGGEDCOM ROS.

Nom de message	Trap SNMP	Syslog
Secure Port X Learned MAC Addr on VLAN X	Oui	Oui

Port Security Violated

Ce message est applicable uniquement si le mode de sécurité du port est défini sur "802.1X or 802.1X/MAC-Auth"

RUGGEDCOM ROS génère cette alarme et consigne un message dans le journal système lorsque l'hôte connecté à un port sécurisé tente de communiquer à l'aide d'informations d'identification de connexion incorrectes.

Nom de message	Alarme	Trap SNMP	Syslog
802.1X Port X Authentication Failure	Oui	Oui	Oui
802.1X Port X Authorized Addr. XXX	Non	Non	Oui

Section 4.7

Gestion du fichier de configuration

Le fichier de configuration de l'appareil pour RUGGEDCOM ROS est un fichier texte unique CSV (Comma-Separate Value) formaté ASCII ayant pour nom`config.csv`. Il peut être téléchargé depuis l'appareil pour être affiché, comparé à d'autres fichiers de configuration ou stocké à des fins de sauvegarde. Il peut également être remplacé par un fichier de configuration complet ou partiel chargé sur l'appareil.

Pour éviter un accès non autorisé au contenu du fichier de configuration, le fichier peut être chiffré et un mot de passe/une phrase secrète peut lui être affecté(e).

SOMMAIRE

- Section 4.7.1, « Configuration du chiffrage des données »
- Section 4.7.2, « Mise à jour du fichier de configuration »

Section 4.7.1

Configuration du chiffrage des données

Procédez comme suit pour chiffrer le fichier de configuration et le protéger avec un mot de passe/une phrase secrète :

REMARQUE
Le chiffrage de données n'est pas disponible dans les versions non contrôlées (Non-Controlled (NC)) de RUGGEDCOM ROS. Lorsque vous commutez entre les versions contrôlées (Controlled) et (non contrôlées Non-Controlled (NC)) de RUGGEDCOM ROS, assurez-vous que le chiffrage de données est désactivé. Sinon, la version NC de RUGGEDCOM ROS ignore le fichier de configuration chiffré et charge les valeurs par défaut.

REMARQUE
Seules les données de configuration sont chiffrées. Tous les commentaires et noms de tableau dans le fichier de configuration sont enregistrés comme texte clair.

REMARQUE
Lorsqu'un fichier de configuration est partagé entre plusieurs appareils, assurez-vous que tous les appareils ont la même phrase secrète configurée. Sinon, le fichier de configuration est rejeté.

REMARQUE
Le chiffrement doit être désactivé avant que l'appareil ne soit renvoyé à Siemens ou le fichier de configuration est partagé avec l'assistance client.

IMPORTANT !
Ne rétrogradez jamais la version logicielle de RUGGEDCOM ROS au-delà de RUGGEDCOM ROS v4.3 lorsque le chiffrement est activé. Assurez-vous que les paramètres par défaut de l'appareil ont été restaurés avant le rétrogradage.

1. Accédez à ***Administration » Configure Data Storage***. Le formulaire **Data Storage** s'affiche.

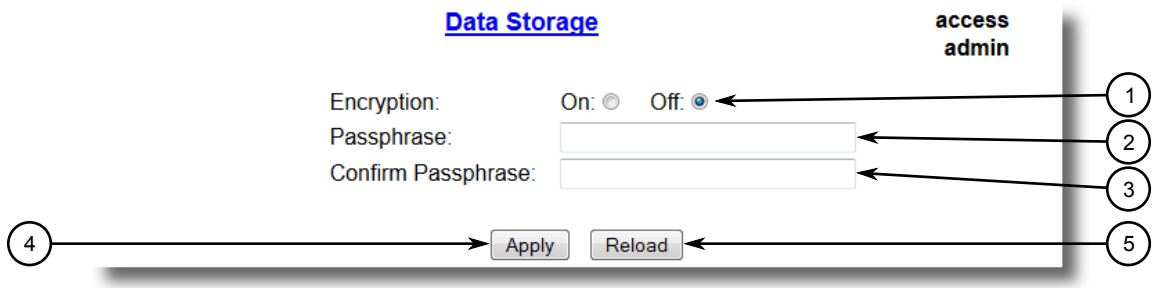


Figure 76 : Formulaire Data Storage

1. Options Encryption **2.** Zone Passphrase **3.** Zone Confirm Passphrase **4.** Bouton Apply **5.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Encryption	**Synopsis :** { On, Off } Active/désactive le chiffrement de données dans le fichier de configuration.
Passphrase	**Synopsis :** chaîne de 31 caractères ascii Cette phrase secrète est utilisée comme clé secrète pour chiffer les données de configuration. Les données chiffrées peuvent être déchiffrées par tout appareil configuré avec la même phrase secrète.

Paramètre	Description
Confirm Passphrase	**Synopsis :** chaîne de 31 caractères ascii Cette phrase secrète est utilisée comme clé secrète pour chiffer les données de configuration. Les données chiffrées peuvent être déchiffrées par tout appareil configuré avec la même phrase secrète.

3. Cliquez sur **Apply**.

Section 4.7.2

Mise à jour du fichier de configuration

Une fois téléchargé de l'appareil, le fichier de configuration peut être mis à jour à l'aide de plusieurs outils différents :

REMARQUE
Pour plus d'informations sur le chargement/téléchargement de fichiers, voir Section 3.5, « Chargement/téléchargement de fichiers ».

- Tout programme de traitement de texte capable de lire et d'écrire des fichiers ASCII.
- Outils de différence/mise à jour (par exemple les utilitaires de ligne de commande UNIX *diff* and *patch*)
- Systèmes de contrôle de code source (par ex. CVS, SVN)

ATTENTION !
Risque pour la configuration - risque de perte de données. N'éditez pas un fichier de configuration chiffré. Toute ligne modifiée manuellement est ignorée.

RUGGEDCOM ROS est également en mesure d'accepter des mises à jour de configuration partielles. Par exemple, pour mettre à jour uniquement les paramètres du port Ethernet 1 et ne modifier aucun autre paramètre, transférez un fichier contenant uniquement les lignes suivantes dans l'appareil :

```
# Port Parameters
ethPortCfg
Port,Name,Media,State,AutoN,Speed,Dupx,FlowCtrl,LFI,Alarm,
1,Port 1,100TX,Enabled,On,Auto,Auto,Off,Off,On,
```

Section 4.8

Gestion d'un serveur d'authentification

Cette section décrit la manière de gérer les authentifications RADIUS et TACACS+.

SOMMAIRE

- Section 4.8.1, « Configuration d'extensions de nom d'utilisateur »
- Section 4.8.2, « Gestion de l'authentification RADIUS »
- Section 4.8.3, « Gestion de l'authentification TACACS+ »

Section 4.8.1

Configuration d'extensions de nom d'utilisateur

Lorsqu'il est configuré pour authentifier des utilisateurs à l'aide de RADIUS ou TACACS+, RUGGEDCOM ROS peut être configuré de manière à ajouter des informations à chaque nom d'utilisateur significatif pour le serveur d'authentification. Il peut s'agir entre autres de l'adresse IP NAS, du nom du système, de l'emplacement du système ou de tout texte défini par l'utilisateur.

Si le paramètre**Username Extension** reste vide, seul le nom d'utilisateur est envoyé au serveur d'authentification.

> **REMARQUE**
> *Les extensions sont ignorées lorsque l'authentification IEEE 802.1x basée sur des ports. RUGGEDCOM ROS reste transparent et n'apporte aucune modification au nom d'utilisateur. Pour plus d'informations sur l'authentification IEEE 802.1x, voir Section 5.10.1, « Concept de sécurité de port ».*

Procédez comme suit pour configurer une extension de nom d'utilisateur :

1. Accédez à ***Administration » Configure Security Server » Configure Common Security Parameters***. Le formulaire **Common Security Parameters** s'affiche.

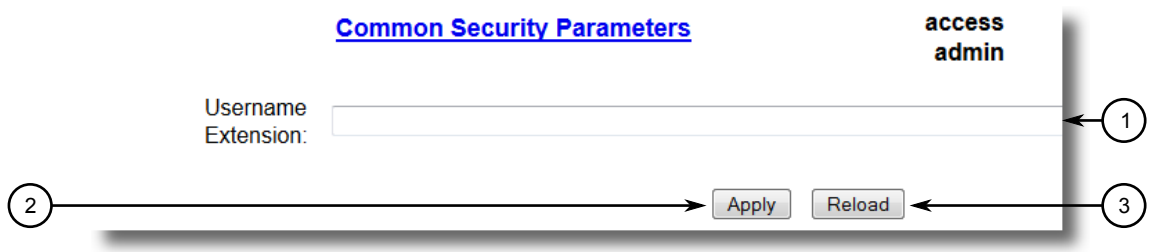


Figure 77 : Formulaire Common Security Parameters

1. Zone Username Extension **2.** Bouton Apply **3.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Username Extension	**Synopsis :** 127 caractères quelconques Définit le format de tous les noms d'utilisateur envoyés à un serveur RADIUS ou TACACS + pour authentification. Un préfixe ou un suffixe peut être ajouté au nom d'utilisateur à l'aide de mots-clés prédéfinis (entre délimiteurs %) ou de chaînes de caractères définies par l'utilisateur. Les valeurs délimitées sont : %Username% : le nom associé au profil utilisateur (par exemple admin, opérateur, etc.) %IPaddr% : L'adresse IP de gestion du commutateur agissant comme Network Access Server (NAS). %SysName% : le nom système donné à l'appareil. %SysLocation% : l'emplacement système donné à l'appareil. Tous les mots-clés prédéfinis ne respectent pas la casse. Exemples : %Username%@ABC.com %Username%_%SysLocation% Si aucune extension n'est définie, seul le nom d'utilisateur est envoyé au serveur d'identification.

3. Cliquez sur **Apply**.

Section 4.8.2

Gestion de l'authentification RADIUS

RUGGEDCOM ROS peut être configuré de manière à agir comme client RADIUS et transmettre les informations d'identification de l'utilisateur à un serveur RADIUS (Remote Authentication Dial In User Service) pour l'authentification et l'autorisation à distance.

RADIUS est un protocole basé UDP utilisé pour transmettre de informations d'authentification, d'autorisation et de configuration entre un NAS (Network Access Server) souhaitant authentifier ses liaisons et un serveur d'authentification partagé. Il fournit une authentification centralisée et une authentification pour l'accès au réseau.

RADIUS est également largement utilisé en liaison avec la norme IEEE 802.1X pour la sécurité des ports à l'aide de l'Extensible Authentication Protocol (EAP).

IMPORTANT !
Les messages RADIUS sont envoyés comme messages UDP. Le commutateur et le serveur RADIUS doivent utiliser la même clé d'authentification et de chiffrement.

IMPORTANT !
RUGGEDCOM ROS prend en charge le PEAP (Protected Extensible Authentication Protocol) et EAP-MD5. PEAP est plus sécurisé et est recommandé s'il est disponible pour le demandeur.

REMARQUE
Pour plus d'informations sur le protocole RADIUS, voir RFC 2865 [http://tools.ietf.org/html/rfc2865].

Pour plus d'informations sur l'EAP (Extensible Authentication Protocole), voir RFC 3748 [http://tools.ietf.org/html/rfc3748].

SOMMAIRE

- Section 4.8.2.1, « Configuration de l'authentification RADIUS »
- Section 4.8.2.2, « Configuration du serveur RADIUS »
- Section 4.8.2.3, « Configuration du client RADIUS sur l'appareil »

Section 4.8.2.1

Configuration de l'authentification RADIUS

Dans une demande d'accès RADIUS, les attributs et valeurs suivants sont généralement envoyés par le client RADIUS (RUGGEDCOM ROS) vers le serveur RADIUS :

Attributs	Valeur
User-Name	{ Guest, Operator, Admin }
User-Password	{ Mot de passe }
Service-Type	1
Vendor-Specific	Vendor-ID: 15004

Attributs	Valeur
	Type: 1 Length: 11 String: RuggedCom

Un serveur RADIUS peut également être utilisé pour une authentification de l'accès à des ports avec une prise en charge de sécurité 802.1x. Le cas échéant, les attributs suivants sont envoyés par le client RADIUS () vers le serveur RADIUS :

Attributs	Valeur
User-Name	{ Nom d'utilisateur dérivé de la réponse d'identité EAP du client }
NAS-IP-Address	{ Adresse IP de serveur pour l'accès réseau }
Service-Type	2
Frame-MTU	1500
EAP-Message[a]	{ Message(s) reçu(s) du pair d'authentification }

[a] *Un message EAP est un attribut d'extension pour RADIUS comme définit dans RFC 2869 [http://freeradius.org/rfc/rfc2869.html#EAP-Message].*

Procédez comme suit pour configurer l'authentification RADIUS :

1. Configurez le serveur RADIUS. Pour plus d'informations, voir Section 4.8.2.2, « Configuration du serveur RADIUS ».
2. Configurez le client RADIUS. Pour plus d'informations, voir Section 4.8.2.3, « Configuration du client RADIUS sur l'appareil ».

Section 4.8.2.2

Configuration du serveur RADIUS

REMARQUE
Pour plus d'informations sur la configuration du serveur RADIUS, référez-vous aux instructions du constructeur du serveur à configurer.

Le Vendor-Specific Attribute (ou VSA) envoyé au serveur RADIUS en tant qu'élément de la demande RADIUS est utilisé pour déterminer le niveau d'accès depuis le serveur RADIUS. Cet attribut peut être configuré au sein du serveur RADIUS avec les informations suivantes :

Attributs	Valeur
Vendor-Specific	Vendor-ID: 15004 Format: String Number: 2 Attribute: { Guest, Operator, Admin }

REMARQUE
Si aucun niveau d'accès n'est reçu dans le paquet de réponse du serveur RADIUS, l'accès est refusé.

Section 4.8.2.3

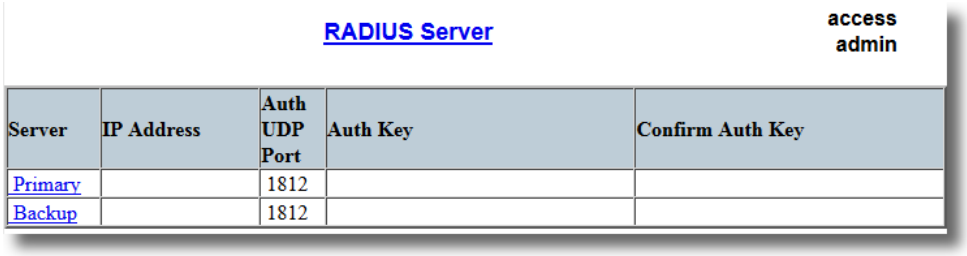
Configuration du client RADIUS sur l'appareil

Le client RADIUS peut être configuré de manière à utiliser deux serveurs RADIUS : un serveur principal (Primary) et un serveur de sauvegarde (Backup). Si le serveur principal n'est pas disponible, l'appareil tente automatiquement de se connecter au serveur de sauvegarde.

> **REMARQUE**
> *Le client RADIUS utilise le PAP (Password Authentication Protocol) pour vérifier l'accès.*

Procédez comme suit pour configurer l'accès au serveur RADIUS principal ou de sauvegarde :

1. Accédez à ***Administration » Configure Security Server » Configure RADIUS Server***. Le tableau **RADIUS Server** s'affiche.



Server	IP Address	Auth UDP Port	Auth Key	Confirm Auth Key
Primary		1812		
Backup		1812		

Figure 78 : Tableau RADIUS Server

2. Sélectionnez**Primary** ou**Backup** dans le tableau. Le formulaire **RADIUS Server** s'affiche.

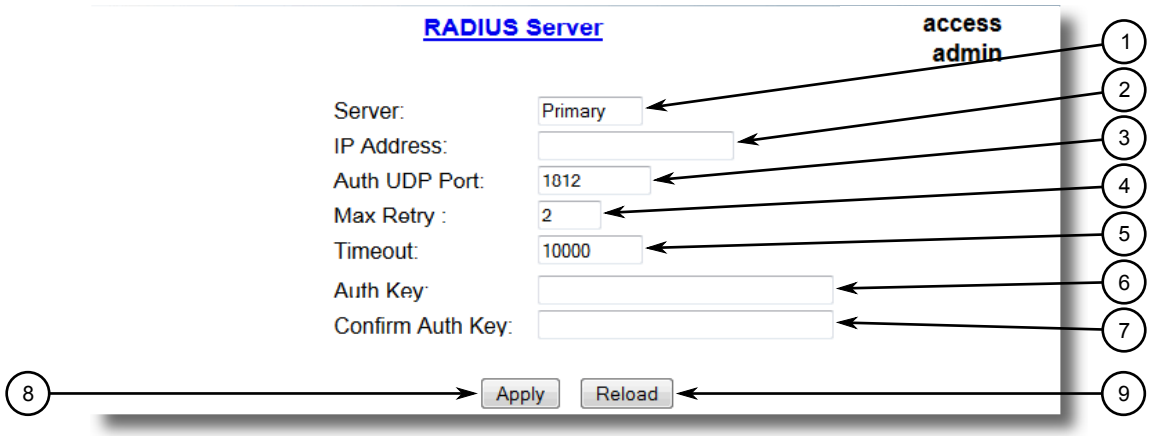


Figure 79 : Formulaire RADIUS Server

1. Zone Server **2.** Zone IP Address **3.** Zone Auth UDP Port **4.** Zone Max Retry **5.** Zone Timeout **6.** Zone Auth Key **7.** Zone Confirm Auth Key **8.** Bouton Apply **9.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Server	**Synopsis :** 8 caractères quelconques

Paramètre	Description
	Par défaut : Primary Ce champ indique si cette configuration est valable pour un serveur principal ou de sauvegarde.
IP Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### L'adresse IP du serveur.
Auth UDP Port	**Synopsis :** 1 à 65535 **Par défaut :** 1812 Port IP sur le serveur.
Max Retry	**Synopsis :** 1 à 10 **Par défaut :** 2 Nombre maximum de tentatives par l'authentificateur de contact du serveur d'authentification pour authentifier l'utilisateur en cas de défaillance quelconque.
Timeout	**Synopsis :** 1000 à 120000 **Par défaut :** 10000 Délai d'attente en millisecondes pendant lequel l'authentificateur attend une réponse du serveur d'authentification.
Auth Key	**Synopsis :** chaîne de 31 caractères ASCII Clé d'authentification à partager avec le serveur.
Confirm Auth Key	**Synopsis :** chaîne de 31 caractères ASCII Clé d'authentification à partager avec le serveur.

4. Cliquez sur **Apply**.

Section 4.8.3

Gestion de l'authentification TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) est un protocole de contrôle d'accès basé sur TCP qui fournit des services d'authentification, d'autorisation et de comptabilisation aux routeurs, aux NAS (Network Access Servers) et aux autres appareils informatiques mis en réseau via un ou plusieurs serveurs centralisés.

SOMMAIRE

- Section 4.8.3.1, « Configuration de TACACS+ »
- Section 4.8.3.2, « Configuration de droits d'utilisateur »

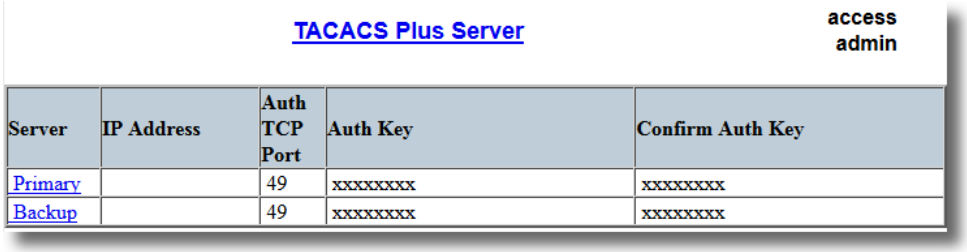
Section 4.8.3.1

Configuration de TACACS+

RUGGEDCOM ROS peut être configuré de manière à utiliser deux serveurs TACACS+ : un serveur principal (Primary) et un serveur de sauvegarde (Backup). Si le serveur principal n'est pas disponible, l'appareil tente automatiquement de se connecter au serveur de sauvegarde.

Procédez comme suit pour configurer l'accès au serveur TACACS+ principal ou de sauvegarde :

1. Accédez à ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACACS Plus Server***. Le tableau **TACACS Plus Server** s'affiche.



Server	IP Address	Auth TCP Port	Auth Key	Confirm Auth Key
Primary		49	xxxxxxxx	xxxxxxxx
Backup		49	xxxxxxxx	xxxxxxxx

Figure 80 : Tableau TACACS Plus Server

2. Sélectionnez**Primary** ou**Backup** dans le tableau. Le formulaire **TACACS Plus Server** s'affiche.

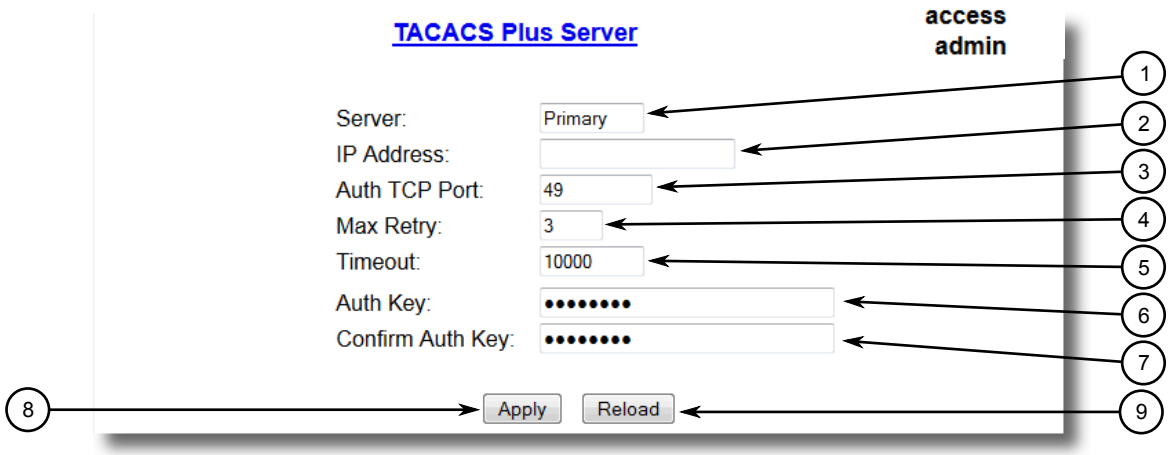


Figure 81 : Formulaire TACACS Plus Server

1. Zone Server **2.** Zone IP Address **3.** Zone Auth TCP Port **4.** Zone Max Retry **5.** Zone Timeout **6.** Zone Auth Key **7.** Zone Confirm Key **8.** Bouton Apply **9.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Server	**Synopsis :** 8 caractères quelconques **Par défaut :** Primary Ce champ indique si cette configuration est valable pour un serveur principal ou de sauvegarde.
IP Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### L'adresse IP du serveur.
Auth TCP Port	**Synopsis :** 1 à 65535 **Par défaut :** 49 Port IP sur le serveur.
Max Retry	**Synopsis :** 1 à 10 **Par défaut :** 3 Nombre maximum de tentatives par l'authentificateur de contact du serveur d'authentification pour authentifier l'utilisateur en cas de défaillance quelconque.

Paramètre	Description
Timeout	**Synopsis :** 1000 à 120000 **Par défaut :** 10000 Délai d'attente en millisecondes pendant lequel l'authentificateur attend une réponse du serveur d'authentification.
Auth Key	**Synopsis :** chaîne de 31 caractères ascii **Par défaut :** mySecret Clé d'authentification à partager avec le serveur.
Confirm Auth Key	**Synopsis :** chaîne de 31 caractères ascii Clé d'authentification à partager avec le serveur.

4. Définissez le niveau de privilèges pour chaque type d'utilisateur (par exemple administrateur, opérateur et invité). Pour plus d'informations, voir Section 4.8.3.2, « Configuration de droits d'utilisateur ».
5. Cliquez sur **Apply**.

Section 4.8.3.2

Configuration de droits d'utilisateur

Chaque demande d'authentification TACACS+ comprend un attribut *priv_lvl* utilisé pour accorder l'accès à l'appareil. L'attribut utilise les plages suivantes par défaut :

- `15` représente le niveau d'accès *administrateur*
- `2-14` représente le niveau d'accès *opérateur*
- `1` représente le niveau d'accès *invité*

Procédez comme suit pour configurer les niveaux de droits d'accès pour chaque type d'utilisateur :

1. Accédez à ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACPLUS Serv Privilege Config***. Le formulaire **TACPLUS Serv Privilege Config** s'affiche.

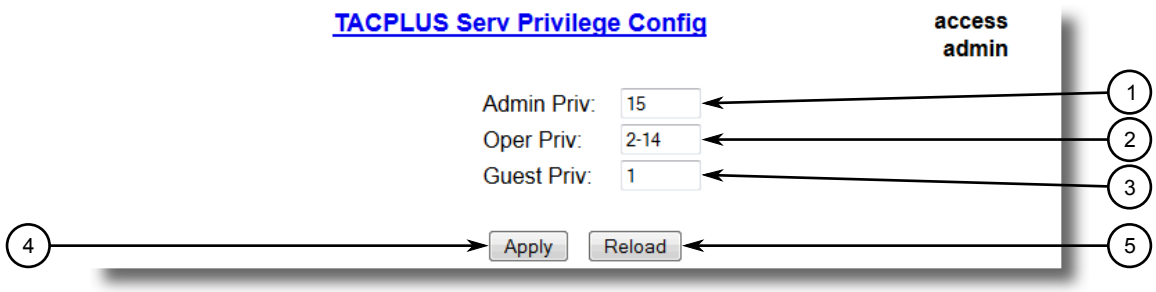


Figure 82 : Formulaire TACPLUS Serv Privilege Config

1. Zone Admin Priv **2.** Zone Oper Priv **3.** Zone Guest Priv **4.** Bouton Apply **5.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Admin Priv	**Synopsis :** (0 à 15)-(0 à 15) **Par défaut :** 15 Niveau de privilège à affecter à l'utilisateur.

Paramètre	Description
Oper Priv	**Synopsis :** (0 à 15)-(0 à 15) **Par défaut :** 2-14 Niveau de privilège à affecter à l'utilisateur.
Guest Priv	**Synopsis :** (0 à 15)-(0 à 15) **Par défaut :** 1 Niveau de privilège à affecter à l'utilisateur.

3. Cliquez sur **Apply**.

5 Installation et configuration

Ce chapitre décrit la manière d'installer et de configurer l'appareil pour une utilisation sur un réseau à l'aide de différentes fonctionnalités disponibles dans RUGGEDCOM ROS.

SOMMAIRE

- Section 5.1, « Gestion de VLAN virtuels »
- Section 5.2, « Gestion du Spanning Tree Protocol »
- Section 5.3, « Gestion des classes de service »
- Section 5.4, « Gestion des adresses MAC »
- Section 5.5, « Gestion des services de temps »
- Section 5.6, « Gestion de SNMP »
- Section 5.7, « Gestion de la découverte de réseau »
- Section 5.8, « Gestion du filtrage de multidiffusion »
- Section 5.9, « Gestion du DHCP Relay Agent (agent de relais DHCP) »
- Section 5.10, « Gestion de la sécurité des ports (Port security) »
- Section 5.11, « Gestion de l'agrégation de liaisons »

Section 5.1

Gestion de VLAN virtuels

Un VLAN (Virtual Local Area Network) est un groupe d'appareils sur un ou plusieurs segments LAN qui communiquent comme s'ils étaient attachés au même segment de LAN physique. Les VLAN sont extrêmement flexibles car ils sont basés sur des connexions logiques plutôt que sur des connexions physiques.

Lorsque des VLAN sont introduits, tout le trafic dans le réseau doit appartenir à un VLAN ou à un autre. Le trafic sur un VLAN ne peut pas passer à un autre, sauf avec un routeur inter-réseaux ou un commutateur de couche 3.

Les VLAN sont créés de trois manières :

- **Explicitement**
  Les VLAN statiques peuvent être créés dans le commutateur. Pour plus d'informations sur les VLAN statiques, voir Section 5.1.5, « Gestion de VLAN statiques ».
- **Implicitement**
  Lorsqu'un ID de VLAN (VID) est défini pour un VLAN basé sur des ports, l'adresse MAC statique ou l'interface IP, un VLAN approprié est automatiquement créé s'il n'existe pas déjà.
- **Dynamiquement**
  Les VLAN peuvent être appris via GVRP. Pour plus d'informations sur GVRP, voir Section 5.1.1.8, « GARP VLAN Registration Protocol (GVRP) ».

Pour plus d'informations sur les VLAN, voir Section 5.1.1, « Concepts VLAN ».

SOMMAIRE

- Section 5.1.1, « Concepts VLAN »
- Section 5.1.2, « Affichage d'une liste de VLAN »
- Section 5.1.3, « Configuration globale de VLAN »
- Section 5.1.4, « Configuration de VLAN pour des ports Ethernet spécifiques »
- Section 5.1.5, « Gestion de VLAN statiques »

Section 5.1.1

Concepts VLAN

Cette section décrit certains concepts importants de la mise en œuvre de VLAN dans RUGGEDCOM ROS.

SOMMAIRE

- Section 5.1.1.1, « Trames balisées contre trames non balisées »
- Section 5.1.1.2, « VLAN natif »
- Section 5.1.1.3, « Le VLAN de gestion »
- Section 5.1.1.4, « Types de port périphérie et trunk »
- Section 5.1.1.5, « Règles d'entrée et de sortie »
- Section 5.1.1.6, « Liste Forbidden Ports »
- Section 5.1.1.7, « Modes compatible VLAN et non-compatible VLAN »
- Section 5.1.1.8, « GARP VLAN Registration Protocol (GVRP) »
- Section 5.1.1.9, « Périphérie PVLAN »
- Section 5.1.1.10, « QinQ »
- Section 5.1.1.11, « Avantages du VLAN »

Section 5.1.1.1

Trames balisées contre trames non balisées

Les balises VLAN identifient les trames comme faisant partie d'un réseau VLAN. Lorsqu'un commutateur reçoit une trame avec une balise VLAN (ou 802.1Q), l'identificateur de VLAN (VID) est extrait et la trame est transmise à d'autres ports sur le même VLAN.

Lorsqu'une trame ne contient pas de balise VLAN ou contient une balise 802.1p (priorisation) qui comprend uniquement des informations de priorisation et un VID de 0, elle est considérée comme trame non balisée.

Section 5.1.1.2

VLAN natif

Un numéro de VLAN natif est affecté à chaque port, l'ID de VLAN de port (PVID). Lorsqu'une trame non balisée entre dans un port, elle est associée au VLAN natif du port.

Par défaut, un commutateur envoie la trame sans balise lorsqu'il la transmet sur le VLAN natif. Le commutateur peut être configuré de manière à transmettre des trames balisées sur le VLAN natif.

Section 5.1.1.3

Le VLAN de gestion

Le trafic de gestion, comme tout autre trafic sur le réseau, doit appartenir à un VLAN spécifique. Le VLAN de gestion est configurable et est toujours configuré par défaut sur VLAN 1. Ce VLAN est également le VLAN natif par défaut pour tous les ports, ce qui donne à tous les ports la possibilité de gérer le produit. Le VLAN de gestion peut être modifié pour restreindre l'accès de gestion à un groupe spécifique d'utilisateurs.

Section 5.1.1.4

Types de port périphérie et trunk

Chaque port peut être configuré comme port de périphérie ou trunk.

Un port de périphérie s'attache à un unique appareil terminal comme un PC ou un appareil électronique intelligent (Intelligent Electronic Device (IED)). Un port de périphérie achemine le trafic sur le VLAN natif.

Les ports trunk font partie du réseau et acheminent le trafic pour tous les VLAN entre des commutateurs. Les ports trunk sont automatiquement membres de tous les VLAN configurés dans le commutateur.

Le commutateur peut faire transiter ('pass through') le trafic en transmettant les trames reçues sur un port trunk d'un autre port trunk. Les ports trunk doivent être membres de tous les VLAN dont le trafic 'pass through' fait partie, même si aucun de ces VLAN n'est utilisé sur des ports de périphérie.

Les trames transmises depuis le port à tous les VLAN autres que le VLAN natif du port sont toujours balisées.

REMARQUE

Il est recommandé de réduire manuellement le trafic sur le trunk à un groupe spécifique de VLAN. Par exemple, lorsque le trunk se connecte à un appareil tel qu'un routeur de couche 3, qui prend en charge un sous-ensemble de LAN disponibles. Pour empêche que le port trunk soit un membre du VLAN, incluez-le dans la liste des ports interdits du VLAN.

Pour plus d'informations sur la liste des ports interdits, voir *Section 5.1.1.6, « Liste Forbidden Ports »*.

Type de port	VLAN pris en charge	Format PVID	Utilisation
Périphérie	1 (natif) configuré	Non balisé	*Réseaux non compatibles VLAN* :toutes les trames sont envoyées et reçues sans que des balises de VLAN ne soient nécessaires.
		Balisé	*Réseaux compatibles VLAN* :les domaines de trafic VLAN sont mis en œuvre sur un VLAN unique.
Trunk	Tous configurés	Balisé ou non balisé	*Connexions commutateur à commutateur* : les VLAN doivent être crées et gérés manuellement, ou ils peuvent être appris via GVRP. *Appareils terminaux à VLAN multiples* : mise en œuvre des connexions vers des appareils terminaux prenant en charge des VLAN multiples simultanément.

Section 5.1.1.5

Règles d'entrée et de sortie

Les règles d'entrée et de sortie déterminent comment le trafic est reçu et transmis par le commutateur.

Les règles d'entrée sont appliquées comme suit à toutes les trames lorsqu'elles sont reçues par le commutateur :

Trame reçue[a]	Non balisée	Priorité balisée (VID = 0)	Balisée (VID valide)
ID de VLAN associée à la trame	PVID	PVID	VID dans la variable
Trame abandonnée en raison de son format balisé/non balisé	Non	Non	Non
Trame abandonnée si le port d'entrée n'est pas membre du VLAN auquel la trame est associée et le filtrage d'entrée est activé.			Oui

[a] *Ne dépend pas des paramètres de configuration de VLAN du port d'entrée.*

Les règles de sortie sont appliquées comme suit à toutes les trames lorsqu'elles sont transmises par le commutateur.

Type de port de sortie	Sur le VLAN natif du port de sortie	Sur d'autres VLAN	
		Le port est un membre du VLAN	Le port n'est pas membre du VLAN
Périphérie	En fonction du paramètre**PVID Format** du port de sortie	Abandonné	
Trunk		Balisé	Abandonné

Section 5.1.1.6

Liste Forbidden Ports

Chaque VLAN peut être configuré de manière à exclure des ports de l'appartenance au VLAN à l'aide de la liste des ports interdits. Pour plus d'informations, voir Section 5.1.5.2, « Ajout d'un VLAN statique ».

Section 5.1.1.7

Modes compatible VLAN et non-compatible VLAN

Le mode de fonctionnement natif d'un commutateur conforme à IEEE 802.1Q est compatible VLAN. Même si une architecture de réseau spécifique n'utilise pas de VLAN, les réglages de VLAN par défaut de RUGGEDCOM ROS permettent au commutateur de continuer à fonctionner en mode compatible VLAN, tout en fournissant la fonctionnalité requise pour pratiquement toutes les applications réseau. Cependant, la norme IEEE 802.1Q définit un ensemble de règles à suivre par tous les commutateurs compatibles VLAN :

- Les VID valides se trouvent dans une page allant de 1 à 4094. Des VID de 0 ou 4095 sont invalides.
- Chaque trame entrant dans un commutateur compatible VLAN est associée à un VID valide.
- Chaque trame sortant d'un commutateur compatible VLAN est balisée ou non avec un VID valide. Les trames balisées avec une priorité avec un VID invalide ne sont jamais envoyées par un commutateur compatible VLAN.

REMARQUE
Certaines applications ont des conditions requises en conflit avec le mode de fonctionnement natif de IEEE 802.Q1. Par exemple, certaines applications requièrent explicitement des trames balisées avec une priorité que des appareils terminaux doivent recevoir.

Pour empêcher des conflits et permettre une compatibilité complète avec des appareils hérités (non-compatibles VLAN), RUGGEDCOM ROS peut être configuré de manière à fonctionner en mode non-compatible VLAN.

Dans ce mode :

- *Des trames entrant dans un appareil non-compatible VLAN ne sont associées à aucun VLAN.*
- *Des trames sortant d'un appareil non-compatible VLAN sont envoyées sans modification (c'est-à-dire dans le même format non balisé, balisé 802.1Q ou balisé avec priorité)*

Section 5.1.1.8

GARP VLAN Registration Protocol (GVRP)

Le GARP VLAN Registration Protocol (GVRP) est un protocole standard basé sur GARP (Generic Attribute Registration Protocol) afin de distribuer automatiquement la configuration VLAN dans un réseau. Chaque commutateur dans un réseau a uniquement besoin d'être configuré avec des VLAN qu'il requiert localement. Les VLAN configurés à d'autres endroits du réseau sont appris via GVRP. Une station terminale tenant compte de GVRP (par ex. un PC ou un appareil électronique intelligent) configurée pour un VID spécifique peut être connectée à un trunk sur un commutateur tenant compte de GVRP et faire automatiquement partie du VLAN souhaité.

Lorsqu'un commutateur envoie des BPDU (bridge protocol data units) de tous les ports tenant compte de GVRP, les BPDU GVRP annoncent tous les VLAN connus de ce commutateur (configurés manuellement ou appris dynamiquement via GVRP) au reste du réseau.

Lorsqu'un commutateur tenant compte de GVRP reçoit une BPDU GVRP annonçant un ensemble de VLAN, le port qui reçoit devient membre de ces VLAN annoncés et le commutateur commence à annoncer ces VLAN dans tous les ports tenant compte de GVRP (qui ne sont pas le port sur lequel les VLAN ont été appris).

Pour améliorer la sécurité du réseau à l'aide de VLAN, les ports compatibles GVRP peuvent être configurés de manière à interdire l'apprentissage de tout nouveau VLAN dynamique mais à autoriser cependant l'annonce des VLAN configurés sur le commutateur.

Vous trouverez ci-après un exemple d'utilisation de GVRP :

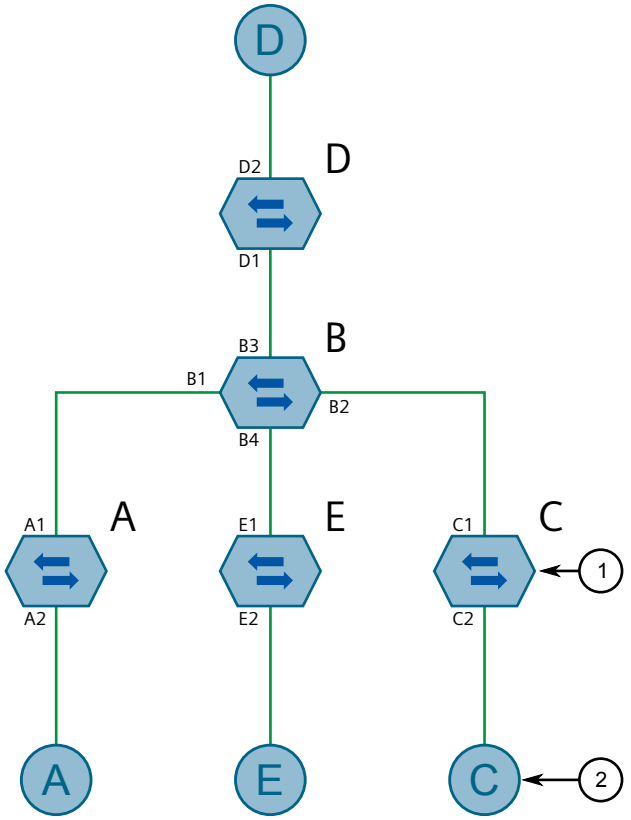


Figure 83 : Utilisation de GVRP

1. Commutateur **2.** Nœud terminal

- Le commutateur B est le commutateur principal, tous les autres sont des commutateurs de périphérie
- Les ports A1, B1 à B4, C1, D1, D2 et E1 tiennent compte de GVRP
- Les ports B1 à B4, D1 et D2 sont définis de manière à annoncer et apprendre
- Les ports A1, C1 et E1 sont définis pour annoncer uniquement
- Les ports A2, C2 et E2 sont des ports de périphérie
- Le nœud terminal D tient compte de GVRP
- Les nœuds terminaux A, E et C ignorent GVRP
- Les ports A2 et C2 sont configurés avec PVID 7
- Le port E2 est configuré avec PVID 20
- Le nœud terminal D est intéressé par le VLAN 20, donc le VLAN 20 est annoncé par ce nœud au commutateur D
- D2 devient membre du VLAN 20
- Les ports A1 et C1 annoncent le VID 7
- Les ports B1 et B2 deviennent membres du VLAN 7
- Les ports B1, B2 et D1 annoncent le VID 20
- Les ports B3, B4 et D1 deviennent membres du VLAN 20

Pour plus d'informations sur la configuration de GVRP, voir Section 5.1.4, « Configuration de VLAN pour des ports Ethernet spécifiques ».

Section 5.1.1.9

Périphérie PVLAN

La périphérie VLAN privée (PVLAN) isole plusieurs ports de périphérie VLAN les uns des autres sur un seul appareil. Lorsque des ports de périphérie VLAN sont configurés comme *protégés*, il leur est interdit d'envoyer des trames les uns aux autres, mais ils sont toujours autorisés à envoyer des trames à d'autres ports non protégés au sein du même VLAN. Cette protection s'étend à tout le trafic sur le VLAN, notamment le trafic de monodiffusion, multidiffusion et diffusion.

Pour plus d'informations sur la configuration d'un port comme *protégé*, voir Section 5.1.4, « Configuration de VLAN pour des ports Ethernet spécifiques ».

REMARQUE
Cette fonctionnalité est strictement locale au niveau du commutateur. Les ports de périphérie PVLAN sont autorisés à communiquer avec des ports en dehors du commutateur, qu'ils soient protégés (à distance) ou non.

Section 5.1.1.10

QinQ

QinQ, également appelé VLAN empilés, pontage de ponts, balisage de VLAN double et VLAN imbriqués, est utilisé pour superposer un réseau privé de couche 2 sur un réseau public de couche 2.

Un grand prestataire de services de réseau, par exemple, peut avoir plusieurs clients dont les réseaux utilisent chacun plusieurs VLAN. Il est probable que les ID de VLAN utilisés par ces différents réseaux clients entreraient en conflit les uns avec les autres s'ils étaient mélangés sur le réseau du prestataire. S'ils utilisent QinQ en double, chaque réseau client pourrait en outre être balisé à l'aide d'un VID spécifique au client aux périphéries où les réseaux du client sont connectés à l'infrastructure du prestataire de services de réseau.

Toute trame balisée entrant dans un port de périphérie du commutateur du prestataire de services est balisée avec des VID du réseau privé du client. Lorsque ces trames sortent du port du commutateur activé pour QinQ pour atteindre le réseau du prestataire de service, le commutateur ajoute toujours une balise supplémentaire (appelée *balise externe*) sur la balise VLAN originale des trames (appelée *balise interne*). Le VID de la balise externe est le PVID du port de périphérie d'entrée de la trame. Cela signifie que le trafic provenant d'un client individuel est balisé avec son VID unique et est dont séparé des autres trafics du client. Pour les trames d'entrée non balisées, le commutateur ajoute uniquement la balise VLAN externe.

Au sein du réseau du prestataire de services, la commutation est basée sur le VID dans la balise externe.

Lorsque des trames à double balisage quittent le réseau du prestataire de services, ils sortent d'un port compatible QinQ d'un autre commutateur. Le commutateur supprime la balise externe tout en associant les trames au VID extrait de la trame avant la suppression. Les trames sont donc commutées vers les ports de périphérie appropriés (c'est-à-dire des clients)

La figure suivante montre un exemple de flux de trafic avec QinQ.

Pour les trames balisées :

- Les trames reçues du client 1 avec le VID 100 comprennent une balise interne de 100 et une balise externe de VID X (c'est-à-dire VLAN 110) configurée sur le port de périphérie connecté au client 1.

- Les trames du client 1 sont ensuite transmises via le port QinQ comportant une balise interne et une balise externe.
- Enfin, à l'arrivée des trames dans le commutateur pair, la balise VLAN externe est supprimée et les trames sont transmises avec la balise VLAN interne vers le client 1.

Pour les trames non balisées :

- Les trames reçues du client 2 comprennent une balise externe VID Y (c'est-à-dire VLAN 220) configurée sur le port de périphérie connecté au client 2.
- Les trames du client 2 sont ensuite transmises via le port QinQ comportant la balise externe.
- Enfin, à l'arrivée des trames dans le commutateur pair, la balise VLAN externe est supprimée avant que les trames ne soient transmises au client 2.

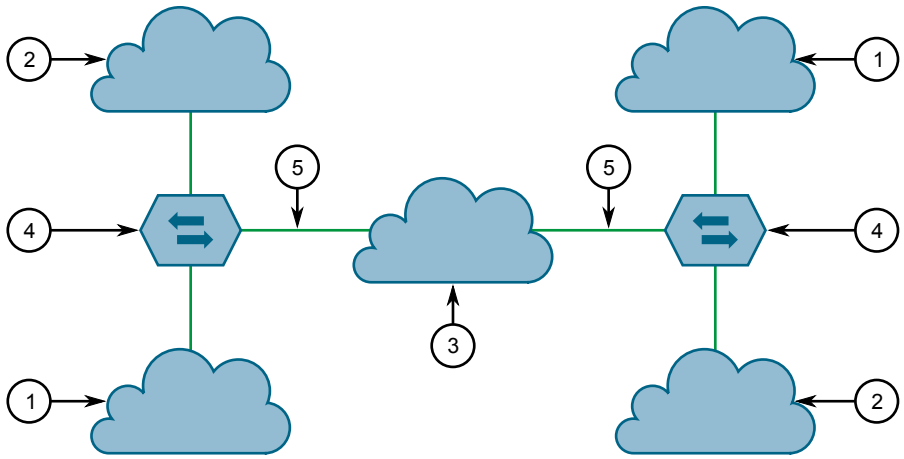


Figure 84 : Utilisation de QinQ

1. Client 1 (PVID est X) **2.** Client 2 (PVID est Y) **3.** Infrastructure du prestataire de services de réseau **4.** Commutateur **5.** QinQ

REMARQUE
Selon le matériel installé, certains modèles de commutateur permettent uniquement la configuration d'un port commutateur en mode QinQ à la fois.

REMARQUE
Lorsque QinQ est activé, tous les ports non-QinQ ne sont pas balisés et ne peuvent pas être modifiés, et tous les ports QinQ sont balisés et ne peuvent pas être modifiés.

Section 5.1.1.11

Avantages du VLAN

Vous trouverez ci-après quelques avantages offerts par les VLAN.

Isolation du domaine de trafic

Les VLAN sont le plus souvent utilisés pour leur capacité à réduire les flux de trafic entre des groupes d'appareils.

Le trafic de diffusion non nécessaire peut être réduit au VLAN qui en a besoin. Des tempêtes de diffusion dans un VLAN n'affectent pas les utilisateurs dans d'autres VLAN.

Il est possible d'empêcher les hôtes sur un VLAN d'utiliser de manière accidentelle ou délibérée l'adresse IP d'un hôte sur un autre VLAN.

L'utilisation d'un filtrage de pont créatif et de plusieurs VLAN peut partager des sous-réseaux IP apparemment unifiés en plusieurs régions régies par différentes stratégies de sécurité/d'accès.

Plusieurs hôtes VLAN peuvent affecter différents types de trafic à différents VLAN.

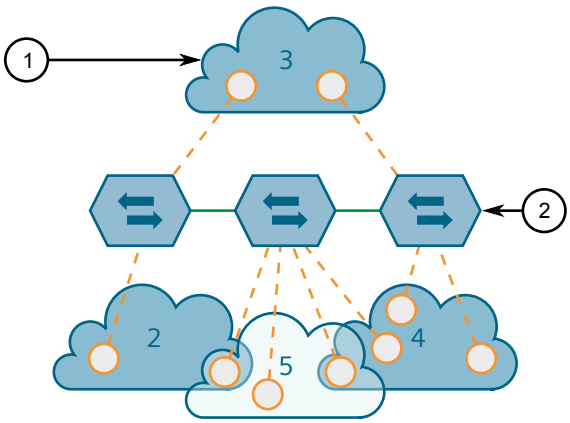


Figure 85 : Plusieurs VLAN se chevauchant

1. VLAN **2.** Commutateur

Commodité administrative

Les VLAN permettent un traitement des déplacements d'équipements par reconfiguration logicielle et non par gestion des câbles physiques. Lorsque l'emplacement physique d'un hôte est modifié, son point de connexion est souvent également modifié. Avec des VLAN, l'appartenance de l'hôte au VLAN et la priorité sont simplement copiées sur le nouveau port.

Réduction du matériel

Sans VLAN, l'isolation du domaine de trafic requiert l'utilisation de ponts séparés pour des réseaux séparés. Les VLAN éliminent le besoin de ponts séparés.

Le nombre d'hôtes de réseau peut souvent être réduit. Souvent, un serveur est affecté pour fournir des services pour des réseaux indépendants. Ces hôtes peuvent être remplacés par un hôte unique à plusieurs interfaces réseau prenant en charge chaque réseau sur son propre VLAN. Cet hôte peut exécuter le routage entre des VLAN.

Plusieurs hôtes VLAN peuvent affecter différents types de trafic à différents VLAN.

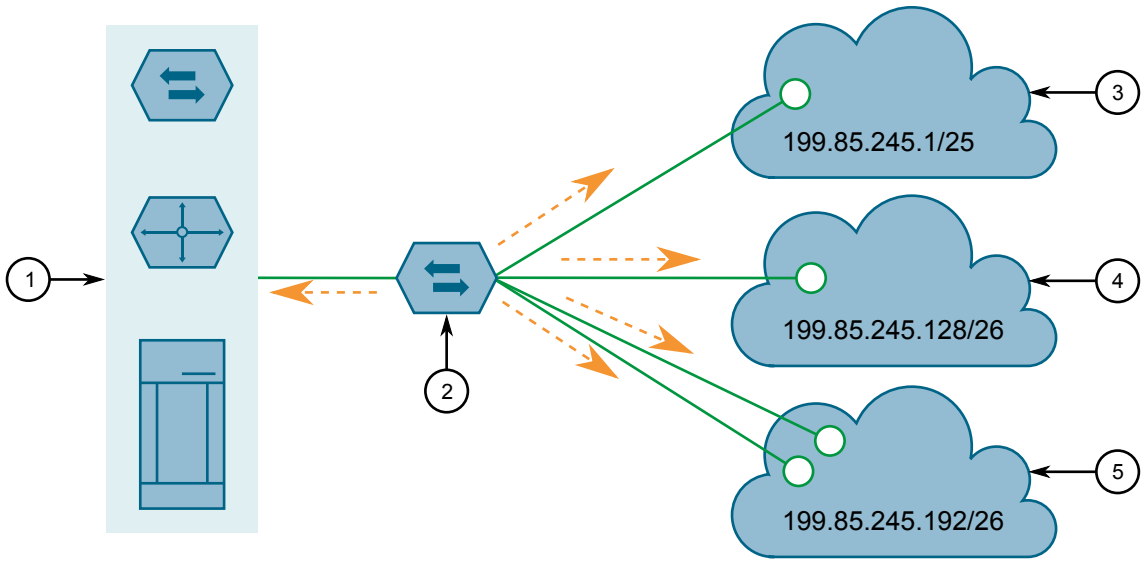


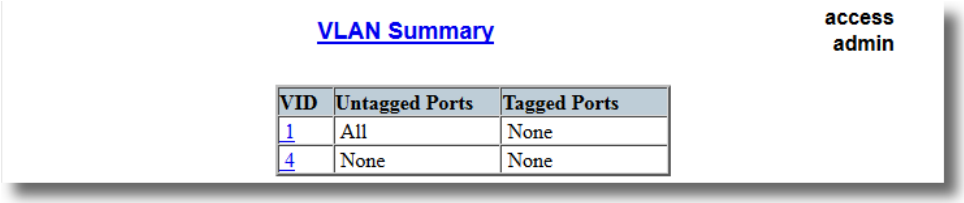
Figure 86 : Communications inter-VLAN

1. Serveur, routeur ou commutateur de couche 3 **2.** Commutateur **3.** VLAN 2 **4.** VLAN 3 **5.** VLAN 4

Section 5.1.2

Affichage d'une liste de VLAN

Pour afficher une liste de tous les VLAN, qu'ils aient été créés de manière statique, implicite ou dynamique, accédez à ***Virtual LANs » View VLAN Summary***. Le tableau **VLAN Summary** s'affiche.



VID	Untagged Ports	Tagged Ports
1	All	None
4	None	None

Figure 87 : Tableau VLAN Summary

Si aucun VLAN n'est répertorié, ajoutez des VLAN statiques en fonction de vos besoins. Pour plus d'informations, voir Section 5.1.5.2, « Ajout d'un VLAN statique ».

Section 5.1.3

Configuration globale de VLAN

Procédez comme suit pour configurer des réglages globaux pour tous les VLAN :

1. Accédez à ***Virtual LANs » Configure Global VLAN Parameters***. Le formulaire **Global VLAN Parameters** s'affiche.

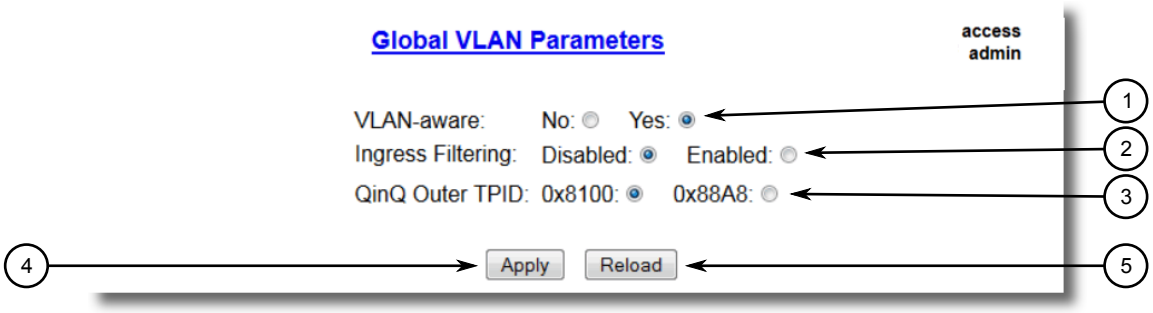


Figure 88 : Formulaire Global VLAN Parameters

1. Options VLAN-aware **2.** Options Ingress Filtering **3.** Options QinQ Outer TPID **4.** Bouton Apply **5.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
VLAN-aware	**Synopsis :** { No, Yes } **Par défaut :** Oui Sélectionnez un mode de fonctionnement compatible ou non-compatible VLAN.
Ingress Filtering	**Synopsis :** { Disabled, Enabled } **Par défaut :** Disabled Active ou désactive le filtrage d'entrée de VLAN sur tous les ports. Lorsque le paramètre est activé, tout paquet balisé arrivant sur un port qui n'est pas membre d'un VLAN avec lequel ce paquet est associé est abandonné. Lorsque le paramètre est désactivé, les paquets ne sont pas abandonnés. **REMARQUE** *Le filtrage d'entrée n'a pas d'effet lorsque des ports sont en mode non-basé sur un VLAN ou en mode Q-in-Q.*
QinQ Outer TPID	**Synopsis :** { 0x8100, 0x88A8 } **Par défaut :** 0x8100 Sélectionne un Ethertype à utiliser comme Tag Protocol Identifier (TPID) sur des ports QinQ VLAN si QinQ est activé. Les trames entrant dans un port QinQ VLAN sont identifiées comme VLAN externe si le premier Ethertype correspond à cette valeur. Une balise VLAN externe avec le champ TPID affecté à cette valeur est insérée dans des trames sortant d'un port QinQ VLAN. **REMARQUE** *Lorsque QinQ est activé, tous les ports non-QinQ ne sont pas balisés et ne peuvent pas être modifiés, et tous les ports QinQ sont balisés et ne peuvent pas être modifiés.*

3. Cliquez sur **Apply**.

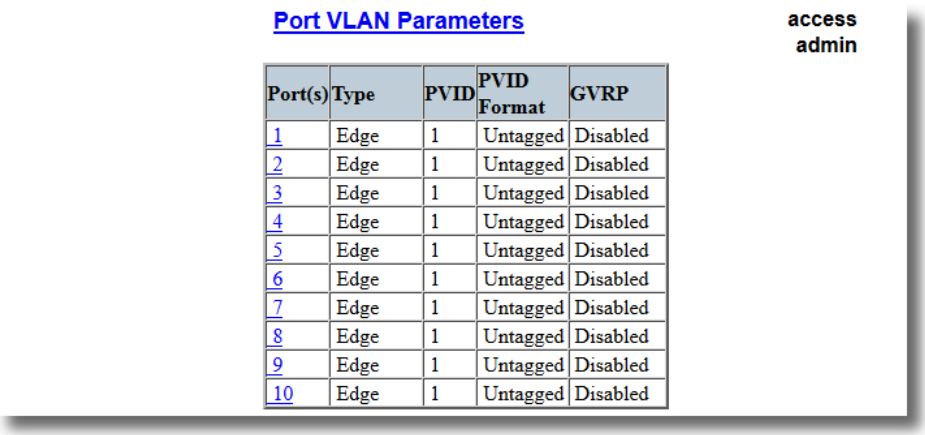
Section 5.1.4

Configuration de VLAN pour des ports Ethernet spécifiques

Lorsqu'un ID de VLAN est affecté à un port Ethernet, le VLAN apparaît dans le tableau VLAN Summary où il peut être configuré.

Procédez comme suit pour configurer un VLAN pour un port Ethernet spécifique :

1. Accédez à ***Virtual LANs » Configure Port VLAN Parameters***. Le tableau **Port VLAN Parameters** s'affiche.



Port(s)	Type	PVID	PVID Format	GVRP
1	Edge	1	Untagged	Disabled
2	Edge	1	Untagged	Disabled
3	Edge	1	Untagged	Disabled
4	Edge	1	Untagged	Disabled
5	Edge	1	Untagged	Disabled
6	Edge	1	Untagged	Disabled
7	Edge	1	Untagged	Disabled
8	Edge	1	Untagged	Disabled
9	Edge	1	Untagged	Disabled
10	Edge	1	Untagged	Disabled

Figure 89 : Tableau Port VLAN Parameters

2. Sélectionnez un port. Le formulaire **Port VLAN Parameters** s'affiche.

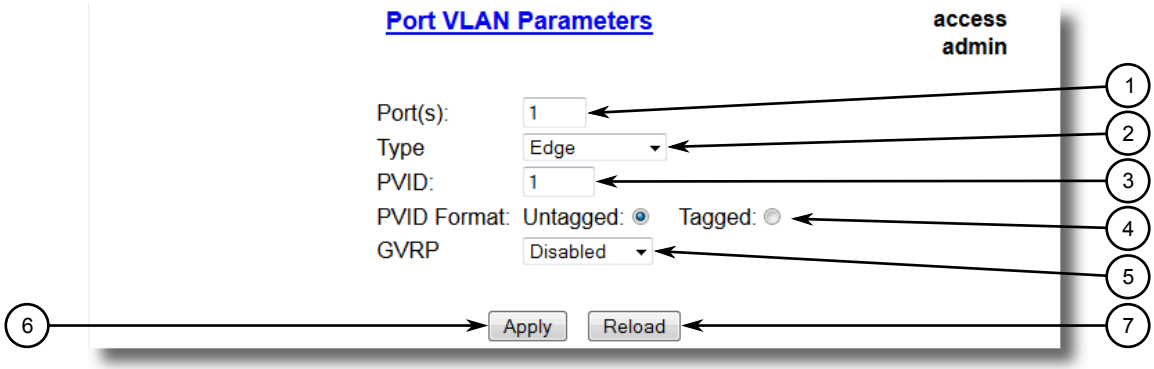


Figure 90 : Formulaire Port VLAN Parameters

1. Zone Port(s) **2.** Liste Type **3.** Zone PVID **4.** Options PVID Format **5.** Liste GVRP **6.** Bouton Apply **7.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
Type	**Synopsis :** { Edge, Trunk, PVLANEdge, QinQ } **Par défaut :** Edge Ce paramètre spécifie comment le port détermine son appartenance dans des VLAN. Il existe quelques types de ports : • Edge - le port est uniquement membre d'un VLAN (son VLAN natif spécifié par le paramètre `PVID`).

Paramètre	Description
	• Trunk - le port est automatiquement membre de tous les VLAN configurés. Les trames transmises depuis le port sur tous les VLAN à l'exception du VLAN natif du port sont toujours balisées. Il peut également être configuré de manière à utiliser GVRP pour la configuration automatique du VLAN. • PVLANEdge - le port est uniquement membre d'un VLAN (son VLAN natif spécifié par le paramètre *PVID*) et ne transmet pas le trafic vers d'autres ports PVLANedge au sein du même VLAN. • QinQ - le port est un port trunk utilisant un double balisage VLAN ou des VLAN imbriqués. Une balise VLAN supplémentaire est toujours ajoutée à toutes les trames sortant de ce port. Le VID dans la balise supplémentaire ajoutée est le PVID du port d'entrée de la trame. Une balise VLAN est toujours retirée des trames entrant dans ce port. **REMARQUE** *Selon le matériel installé, certains modèles de commutateur permettent uniquement la configuration d'un port commutateur en mode QinQ à la fois.*
PVID	**Synopsis :** 1 à 4094 **Par défaut :** 1 L'identificateur de VLAN de port spécifie l'ID de VLAN associé à des trames non balisées (et balisées avec une priorité 802.1p) reçues sur ce port. Les trames balisées avec un ID VLAN non-zéro sont toujours associées à l'ID de VLAN récupéré de la balise de trame. Faites attention lorsque vous modifiez ce paramètre ! Par défaut, le commutateur est programmé pour utiliser le VLAN 1 pour la gestion et chaque port sur le commutateur est programmé pour utiliser le VLAN 1. Si vous modifiez un port de commutateur pour utiliser un VLAN autre que le VLAN de gestion, les appareils sur ce port ne seront pas en mesure de gérer le commutateur.
Format PVID	**Synopsis :** { Untagged, Tagged } **Par défaut :** Untagged Spécifie si les trames transmises depuis le port sur son VLAN natif (spécifié par le paramètre *PVID*) sont balisées ou non balisées. **REMARQUE** *Lorsque QinQ est activé, tous les ports non-QinQ ne sont pas balisés et ne peuvent pas être modifiés, et tous les ports QinQ sont balisés et ne peuvent pas être modifiés.*
GVRP	**Synopsis :** { Adv&Learn, Adv Only, Disabled } **Par défaut :** Disabled Configure le fonctionnement GVRP (Generic VLAN Registration Protocol) sur le port. Il existe plusieurs modes de fonctionnement GVRP : • DISABLED - le port n'est capable d'aucun traitement GVRP. • ADVERTISE ONLY - le port déclare tous les VLAN existants dans le commutateur (configuré ou appris) mais n'apprend aucun VLAN. • ADVERTISE & LEARN - le port déclare tous les VLAN existants dans le commutateur (configuré ou appris) et peut apprendre de VLAN de manière dynamique. Seuls les ports Trunk sont compatibles GVRP.

4. Cliquez sur **Apply**.

Section 5.1.5

Gestion de VLAN statiques

Cette section décrit la configuration et la gestion de VLAN statiques.

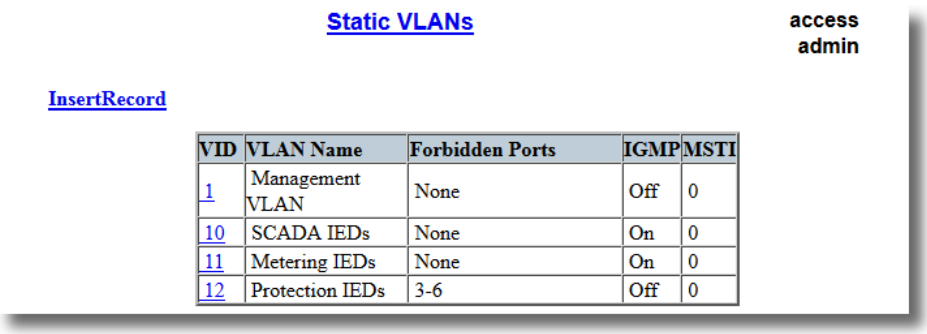
SOMMAIRE

- Section 5.1.5.1, « Affichage d'une liste d'adresses VLAN statiques »
- Section 5.1.5.2, « Ajout d'un VLAN statique »
- Section 5.1.5.3, « Suppression d'un VLAN statique »

Section 5.1.5.1

Affichage d'une liste d'adresses VLAN statiques

Pour afficher une liste de groupes de VLAN statiques, accédez à ***Virtual LANs » Configure Static VLANs***. Le tableau **Static VLANs** s'affiche.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 91 : Tableau Static VLANs

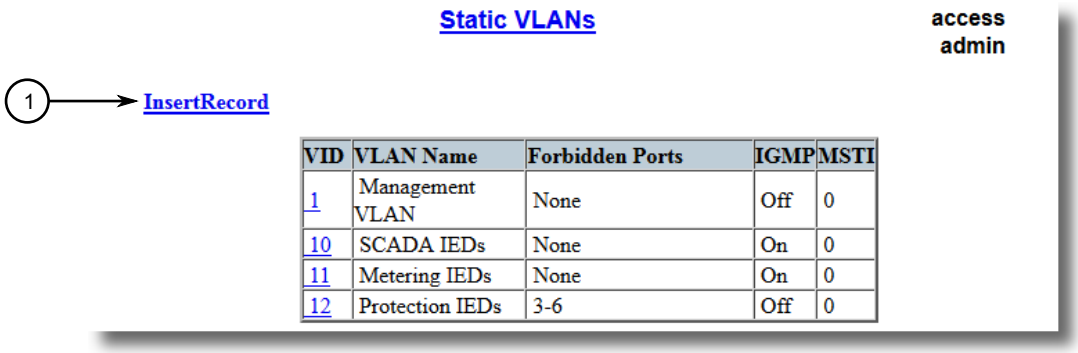
Si aucun VLAN statique n'est répertorié, ajoutez le VLAN. Pour plus d'informations, voir Section 5.1.5.2, « Ajout d'un VLAN statique ».

Section 5.1.5.2

Ajout d'un VLAN statique

Procédez comme suit pour ajouter un VLAN statique :

1. Accédez à ***Virtual LANs » Configure Static VLANs***. Le tableau **Static VLANs** s'affiche.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 92 : Tableau Static VLANs

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **Static VLANs** s'affiche.

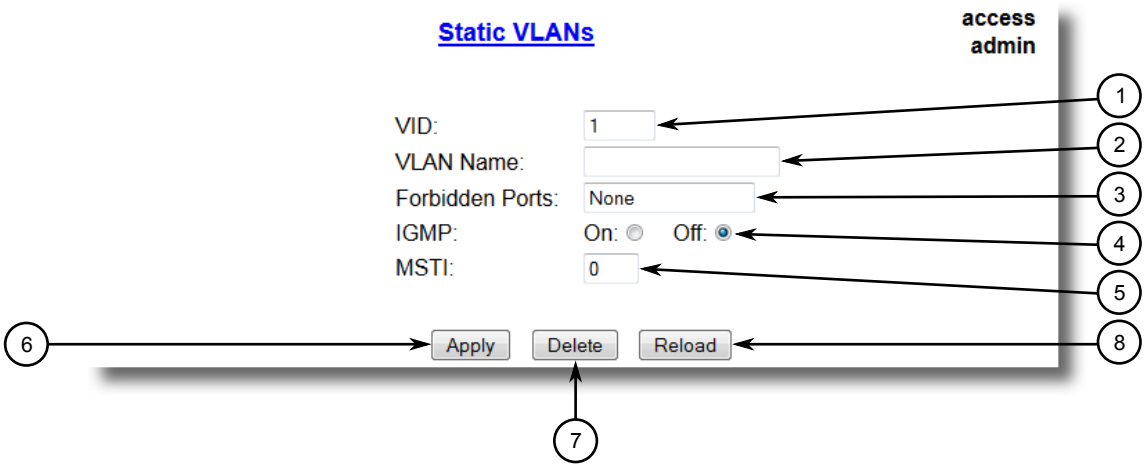


Figure 93 : Formulaire Static VLANs

1. Zone VID **2.** Zone VLAN Name **3.** Zone Forbidden Ports **4.** Options IGMP **5.** Zone MSTI **6.** Bouton Apply **7.** Bouton Delete **8.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

REMARQUE

*Si les**IGMP Options** ne sont pas activées pour le VLAN, les messages IGMP et les flux multidiffusion sont transmis directement à tous les membres du VLAN. Si un membre quelconque du VLAN rejoint un groupe multidiffusion, tous les membres du VLAN recevront le trafic de multidiffusion.*

Paramètre	Description
VID	**Synopsis :** 1 à 4094 **Synopsis :** 1 à 4094 **Par défaut :** 1

Paramètre	Description
	L'identificateur de VLAN est utilisé pour identifier le VLAN dans les trames Ethernet balisées selon IEEE 802.1Q.
VLAN Name	**Synopsis :** 19 caractères quelconques Le nom de VLAN fournit une description de l'utilisation du VLAN (par exemple, Engineering VLAN).
Forbidden Ports	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Il s'agit de ports non autorisés comme membres du VLAN. Exemples : • None - tous les ports du commutateur sont autorisés comme membres du VLAN • 2,4-6,8 - tous les ports sauf 2, 4, 6, 7 et 8 sont autorisés comme membres du VLAN
IGMP	**Synopsis :** { Off, On } **Par défaut :** Off Ce paramètre active ou désactive l'espionnage IGMP sur le VLAN.
MSTI	**Synopsis :** 0 à 16 **Par défaut :** 0 Ce paramètre est valide uniquement pour le Multiple Spanning Tree Protocol (MSTP) et n'a pas d'effet sur le MSTP s'il n'est pas utilisé. Le paramètre spécifie la Multiple Spanning Tree Instance (MSTI) sur laquelle le VLAN doit être mappé.

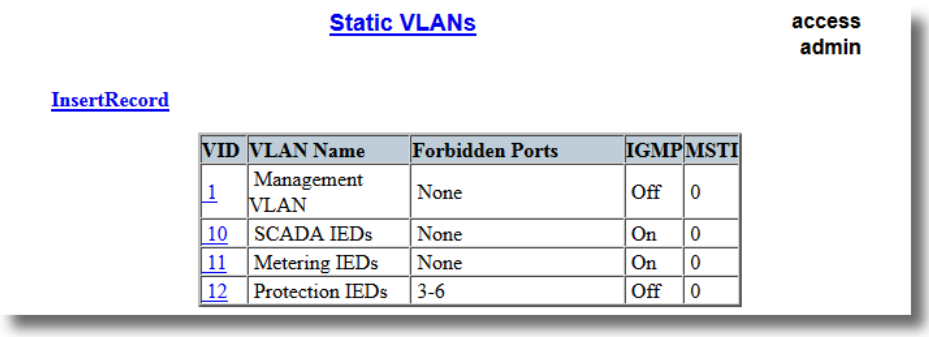
4. Cliquez sur **Apply**.

Section 5.1.5.3

Suppression d'un VLAN statique

Procédez comme suit pour supprimer un VLAN statique :

1. Accédez à ***Virtual LANs » Configure Static VLANs***. Le tableau **Static VLANs** s'affiche.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 94 : Tableau Static VLANs

2. Sélectionnez le VLAN statique dans le tableau. Le formulaire **Static VLANs** s'affiche.

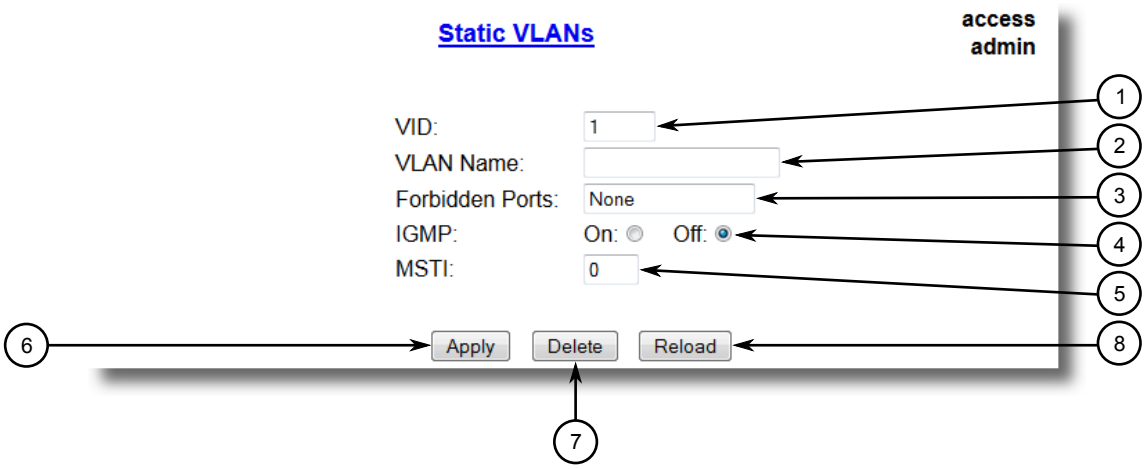


Figure 95 : Formulaire Static VLANs

1. Zone VID **2.** Zone VLAN Name **3.** Zone Forbidden Ports **4.** Options IGMP **5.** Zone MSTI **6.** Bouton Apply **7.** Bouton Delete **8.** Bouton Reload

3. Cliquez sur **Delete**.

Section 5.2

Gestion du Spanning Tree Protocol

Cette section décrit la manière de gérer le Spanning Tree Protocol.

SOMMAIRE

- Section 5.2.1, « Fonctionnement RSTP »
- Section 5.2.2, « Applications RSTP »
- Section 5.2.3, « Opérations MSTP »
- Section 5.2.4, « Configuration globale du STP »
- Section 5.2.5, « Configuration du STP pour des ports Ethernet spécifiques »
- Section 5.2.6, « Configuration d'eRSTP »
- Section 5.2.7, « Affichage de statistiques globales concernant STP »
- Section 5.2.8, « Affichage de statistiques STP pour des ports Ethernet »
- Section 5.2.9, « Gestion de Multiple Spanning Tree Instances »
- Section 5.2.10, « Effacement de statistiques de protocole Spanning Tree »

Section 5.2.1

Fonctionnement RSTP

Le 802.1D Spanning Tree Protocol (STP) a été développé pour permettre la construction de réseaux robustes comprenant une redondance tout en réduisant la topologie active du réseau pour éviter les boucles. Lorsque STP est exécuté, il requiert l'interruption du transfert de trames après une défaillance de liaison jusqu'à être certain que tous les ponts dans le réseau tiennent compte de la nouvelle topologie. Si les valeurs recommandées par 802.1D sont utilisées, cette période dure 30 secondes.

Le Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) constitue une évolution supplémentaire du Spanning Tree Protocol 802.1D. Il remplace le temps de stabilisation par un établissement de liaison actif entre des ponts qui garantit une propagation rapide des informations de topologie au sein du réseau. RSTP offre également un certain nombre d'autres innovations significatives, dont voici quelques exemples :

- Les modifications de topologie dans le RSTP peuvent provenir de et être traitées par tout pont désigné, permettant ainsi une propagation plus rapide des informations d'adresses, contrairement aux modifications de topologie dans STP, qui doivent être transmises au pont racine avant de pouvoir être propagées sur le réseau.
- RSTP reconnaît de manière explicite deux rôles de blocage (port alternatif et port de sauvegarde) inclus dans des calculs des phases d'apprentissage et de transmission. STP, cependant, ne reconnaît qu'un état (blocage) pour les ports qui ne doivent pas transmettre.
- Les ponts RSTP génèrent leurs propres messages de configuration, même s'ils n'en reçoivent aucun du pont racine. La détection de défaillances est ainsi plus rapide. STP, au contraire, doit relayer des messages de configuration reçus sur le port racine de ses ports désignés. Si un pont STP ne reçoit pas de message de son voisin, il ne peut pas être certain de l'endroit où la défaillance s'est produite sur le chemin vers la racine.
- RSTP offre une reconnaissance de ports de périphérie permettant aux ports à la périphérie du réseau de transmettre des trames immédiatement après activation tout en les protégeant contre les boucles.

Tout en fournissant une performance supérieure à STP, IEEE 802.1w RSTP nécessite cependant quelques secondes pour restaurer la connectivité réseau en cas de modification de la topologie.

Une version de RSTP révisée et largement optimisée a été définie dans la norme IEEE édition 802.1D-2004. RSTP IEEE 802.1D-2004 réduit les temps de récupération du réseau à quelques millisecondes et optimise le fonctionnement de RSTP dans différents cas.

RUGGEDCOM ROS prend en charge RSTP IEEE 802.1D-2004.

SOMMAIRE

- Section 5.2.1.1, « États et rôles RSTP »
- Section 5.2.1.2, « Ports de périphérie »
- Section 5.2.1.3, « Liaisons point à point et multipoint »
- Section 5.2.1.4, « Chemin et coûts de port »
- Section 5.2.1.5, « Diamètre de pont »
- Section 5.2.1.6, « eRSTP »
- Section 5.2.1.7, « Fast Root Failover »

Section 5.2.1.1

États et rôles RSTP

Les ports RSTP assument des rôles (ports racines ou ports désignés). Un pont (le pont racine) est le centre logique du réseau. Tous les autres ponts dans le réseau sont des ponts désignés. RSTP affecte un état et un rôle également

à chaque port du pont. L'état RSTP décrit ce qui se passe dans le port en fonction de l'apprentissage d'adresse et de la transmission de trames. Le rôle RSTP décrit principalement si le port fait face au centre ou à la périphérie du réseau et s'il peut être utilisé actuellement.

State

Il existe trois états RSTP : Discarding, Learning et Forwarding.

L'état de rejet (Discarding) est l'état du port lorsqu'il est mis en service pour la première fois. Le port n'apprend pas d'adresses dans cet état et ne participe pas à la transmission de trames. Le port recherche le trafic RSTP pour déterminer son rôle dans le réseau. Lorsqu'il est déterminé que le port doit participer activement au réseau, l'état passe à apprentissage (Learning).

Le port passe à l'état Learning lorsque le port se prépare à jouer un rôle actif dans le réseau. Le port apprend des adresses dans cet état mais ne participe pas à la transmission de trames. Dans un réseau de ponts RSTP, le temps passé dans cet état est généralement très court. Les ponts RSTP fonctionnant en mode de compatibilité STP passent entre 6 et 40 secondes dans cet état.

Après l'état *Learning*, le pont place le port à l'état Forwarding (transmission). Dans cet état, le port apprend des adresses et participe à la transmission de trames.

IMPORTANT !
RUGGEDCOM ROS introduit deux états supplémentaires - Disabled et Link Down. Conçus uniquement à des fins de gestion, ces états peuvent être considérés comme des sous-classes de l'état RSTP Discarding. L'état Disabled (désactivé) se réfère à des liaisons pour lesquelles RSTP a été désactivé. L'état Link Down (liaison interrompue) se réfère à des liaisons pour lesquelles RSTP est activé mais qui sont actuellement interrompues.

Rôle

Il existe quatre rôles de port RSTP : Root, Designated, Alternate et Backup (racine, désigné, alternatif et sauvegarde). Si le pont n'est pas le pont racine, il doit avoir un port racine unique. Le port racine est la "meilleure" manière (c'est-à-dire la plus rapide) d'envoyer le trafic vers le pont racine.

Un port est marqué comme désigné s'il s'agit du port adéquat pour alimenter le segment LAN auquel il est connecté. Tous les ponts sur le même segment LAN écoutent leurs messages respectifs et conviennent du pont qui doit être le pont désigné. Les ports d'autres ponts sur le segment doivent devenir des ports racines, alternatifs ou de sauvegarde.

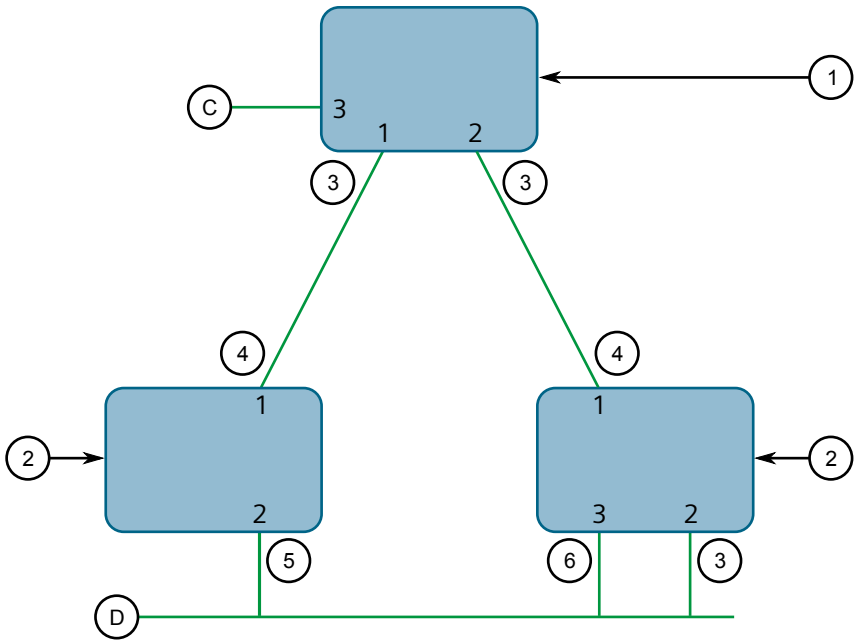


Figure 96 : Rôles de pont et port

1. Port racine **2.** Pont désigné **3.** Port désigné **4.** Port racine **5.** Port alternatif **6.** Port de sauvegarde

Un port est alternatif lorsqu'il reçoit un meilleur message d'un autre pont sur le segment LAN auquel il est connecté. Le message reçu par un port alternatif est meilleur que celui que le port lui-même génère, mais n'est pas assez bon pour le convaincre de devenir le port racine. Le port devient le port alternatif du port racine actuel et deviendra le nouveau port racine en cas de défaillance du port racine actuel. Le port alternatif ne participe pas au réseau.

Un port est un port de sauvegarde lorsqu'il reçoit un meilleur message du segment LAN auquel il est connecté provenant d'un autre port sur le même pont. Le port est un port de sauvegarde pour un autre port sur le pont est deviendra actif en cas de défaillance du port. Le port de sauvegarde ne participe pas au réseau.

Section 5.2.1.2

Ports de périphérie

Un port peut être désigné comme port de périphérie s'il est connecté directement à une station terminale. En tant que tel, il ne peut pas créer de boucles de pontage dans le réseau et peut donc effectuer directement une transition aux étapes de transmission, d'abandon de l'écoute et d'apprentissage.

Les ports de périphérie qui reçoivent des messages de configuration perdent immédiatement leur état de port de périphérie et deviennent des ports Spanning Tree normaux. Une boucle créée sur un port de périphérie qui n'est pas connecté correctement est réparée rapidement

Un port de périphérie travaillant uniquement pour des stations terminales, les messages de modification de topologie ne sont pas générés lorsque sa liaison bascule.

Section 5.2.1.3

Liaisons point à point et multipoint

RSTP utilise un protocole pair-pair appelé Proposing-Agreeing pour assurer la transition en cas de défaillance de liaison. Ce protocole est point à point et est désactivé dans des situations multipoint, c'est-à-dire lorsque plus de deux ponts fonctionnent sur une liaison de support partagé.

Si RSTP détecte une telle circonstance (sur la base de l'état de duplex du port après activation de la liaison), il désactive le mode Proposing-Agreeing. Le port doit passer par les états d'apprentissage et de transmission, avec un délai de transmission pour chaque état.

Il existe des circonstances dans lesquelles RSTP prend une décision incorrecte concernant l'état point à point de la liaison simplement en examinant l'état de semi-duplex. C'est-à-dire :

- Le port s'attache uniquement à un seul partenaire, mais via une liaison en semi-duplex.
- Le port s'attache à un concentrateur de support partagé via une liaison en duplex intégral. La liaison de support partagé s'attache à plus d'un pont compatible RSTP.

Dans de tels cas, l'utilisateur peut configurer le pont pour remplacer la définition du mécanisme semi-duplex et forcer la liaison à être traitée de sa propre manière.

Section 5.2.1.4

Chemin et coûts de port

Le coût de chemin STP est la métrique principale permettant de choisir la racine et les ports désignés. Le coût de chemin pour un port désigné est la somme des coûts de port individuels des liaisons entre le pont racine et ce pont désigné. Le port avec le coût de chemin le plus bas est la route optimale vers le pont racine et est choisi comme port racine.

REMARQUE
Dans les faits, le déterminant principal pour la sélection du port racine est l'ID de pont racine. L'ID de pont est particulièrement importante au démarrage du réseau lorsque le pont avec l'ID la plus basse est choisi comme pont racine. Après le démarrage (lorsque tous les ponts conviennent de l'ID de pont racine), le coût de chemin est utilisé pour sélectionner les ports racines. Si les coûts de chemin de candidats pour le port racine sont les mêmes, l'ID du pont pair est utilisé pour sélectionner le port. Enfin, si les ports racine candidats ont le même coût de chemin et le même ID de port pair, l'ID de port du pont pair est utilisé pour sélectionner le port racine. Dans tous les cas, l'ID, le coût de chemin ou l'ID de port bas est sélectionné comme meilleure solution.

» Procédure de génération des coûts de port

Des coûts de port peuvent être générés comme résultat de la négociation automatique de liaison ou d'une configuration manuelle. Lorsque la méthode de négociation automatique de liaison est utilisée, le coût de port est dérivé de la vitesse de la liaison. Cette méthode est utile lorsqu'un réseau bien connecté a été établi. Elle peut être utilisée lorsque le configurateur n'est pas concerné par la topologie résultante tant qu'une connectivité est assurée.

La configuration manuelle est utile lorsque la topologie exacte du réseau doit être prévisible dans toutes les circonstances. Le coût de chemin peut être utilisé pour établir la topologie du réseau exactement comme le concepteur l'a envisagé.

Coûts STP contre RSTP

La spécification IEEE 802.1D-1998 limite les coûts de port à des valeurs comprises entre 1 et 65536. Conçue lorsque les liaisons 9 600 bits/s étaient une technologie de pointe, cette méthode n'est plus utilisée dans des configurations modernes, car elle ne peut pas représenter une vitesse de liaison supérieure à 10 gigabits par seconde.

Pour régler ce problème dans des applications futures, la spécification IEEE 802.1w limite les coûts de port à des valeurs comprises entre 1 et 20000000, et une vitesse de liaison jusqu'à 10 Tb par seconde peut être représentée avec une valeur de 2.

Les ponts RUGGEDCOM prennent en charge l'interopérabilité avec des ponts STP hérités en sélectionnant le style à utiliser. Dans la pratique, le style n'a pas d'influence tant qu'il est appliqué de manière cohérente au sein du réseau, ou si les coûts sont affectés manuellement.

Section 5.2.1.5

Diamètre de pont

Le diamètre de pont est le nombre maximum de ponts entre deux points possibles d'attachement de stations terminales quelconques dans le réseau.

Le diamètre de pont reflète la réalisation que les informations de topologie ont besoin de temps pour être propagées saut après saut à travers un réseau. Si des messages de configuration mettent trop de temps à être propagés d'une extrémité à l'autre du réseau, ce dernier sera instable.

Il existe une relation entre le diamètre de pont et le paramètre de vieillissement maximum. Pour obtenir des tailles d'anneau étendues, Siemens eRSTP™ utilise un incrément de vieillissement d'¼ de seconde. La valeur du diamètre de pont maximum correspond donc à quatre fois le paramètre de vieillissement maximum paramétré.

REMARQUE
L'algorithme RSTP se présente comme suit :

- *Les messages de configuration STP contiennent des informations de **vieillissement**.*
- *Les messages transmis par le pont racine ont pour âge 0. Chaque pont suivant spécifié transmettant le message de configuration doit incrémenter l'âge d'au moins 1 seconde.*
- *Lorsque l'âge dépasse la valeur du paramètre de vieillissement maximum, le pont suivant devant recevoir le message le rejette immédiatement.*

IMPORTANT !
Augmentez la valeur du paramètre de vieillissement maximum si vous mettez en œuvre des réseaux pontés ou des anneaux de taille importante.

Section 5.2.1.6

eRSTP

L'eRSTP (Rapid Spanning Tree Protocol) de Siemens améliore la performance du RSTP de deux manières :

- il améliore le temps de récupération après erreur (< 5 ms par saut),
- Il améliore la performance pour des topologies réseau de taille importante (jusqu'à 80 commutateurs).

eRSTP est également compatible avec le RSTP standard pour une interopérabilité avec des commutateurs du commerce.

Par exemple, si un réseau comprenant 15 commutateurs Ethernet durcis RUGGEDCOM dans une topologie en anneau, le temps de récupération après erreur est inférieur à 75 ms (c'est-à-dire 5 ms x 15). Cependant, avec eRSTP, le pire temps de récupération après erreur est inférieur à 26 ms.

Section 5.2.1.7

Fast Root Failover

La fonctionnalité *Fast Root Failover* de Siemens est une amélioration apportée à RSTP pouvant être activée ou désactivée. Fast Root Failover améliore le traitement de défaillances de ponts racines par RSTP dans des réseaux connectés en maillage.

IMPORTANT !
Dans les réseaux comportant des commutateurs RUGGEDCOM et non- RUGGEDCOM et dans ceux comportant des algorithmes Fast Root Failover, RSTP Fast Root Failover ne fonctionne pas correctement et une défaillance du pont racine entraîne un temps de basculement non prévisible. Tenez compte des points suivants pour éviter des problèmes potentiels :

- *En cas d'utilisation de l'algorithme robuste, tous les commutateurs doivent être des commutateurs RUGGEDCOM.*
- *En cas d'utilisation de l'algorithme souple, tous les commutateurs doivent être des commutateurs RUGGEDCOM à l'exception du commutateur racine.*
- *Tous les commutateurs RUGGEDCOM dans le réseau doivent utiliser le même algorithme Fast Root Failover.*

Deux algorithmes Fast Root Failover sont disponibles :

- **Robuste** – Garantit un temps de basculement de la racine déterministe, mais requiert une prise en charge par tous les commutateurs dans le réseau, notamment le commutateur racine.
- **Souple** – Assure un temps de basculement de la racine déterministe dans la plupart des configurations réseau, mais permet l'utilisation d'un pont standard dans le rôle racine.

REMARQUE
L'intervalle minimum de défaillances de racine est d'une seconde. Plusieurs défaillances de racine pratiquement simultanées (à moins d'une seconde d'écart) ne sont pas prises en charge par Fast Root Failover.

Performance de Fast Root Failover et de RSTP

- L'exécution de RSTP avec Fast Root Failover désactivé n'a pas d'impact sur la performance du RSTP dans des réseaux connectés en anneau.
- Fast Root Failover n'a pas d'effet sur la performance du RSTP en cas de défaillances ne concernant pas le pont racine ou l'une de ses liaisons.
- Le traitement supplémentaire introduit par Fast Root Failover réduit de manière significative le pire temps de basculement en raison d'une défaillance de pont racine dans des réseaux en maillage.

Recommandations pour l'utilisation de Fast Root Failover

- Il n'est pas recommandé d'activer Fast Root Failover dans des topologies de réseau en anneau.

- Il est recommandé de toujours connecter le pont racine à chacun de ses ponts voisins utilisant plus d'une liaison en cas d'activation dans des réseaux à connexion en anneau.

Section 5.2.2

Applications RSTP

Cette section décrit différentes applications de RSTP.

SOMMAIRE

- Section 5.2.2.1, « RSTP dans des configurations de câblage structuré »
- Section 5.2.2.2, « RSTP dans des configurations de structure en anneau »
- Section 5.2.2.3, « Redondance des ports RSTP »

Section 5.2.2.1

RSTP dans des configurations de câblage structuré

RSTP peut être utilisé pour construire des systèmes à câblage structuré ou la connectivité est conservée en cas de défaillances de liaison. Par exemple, une seule défaillance de toute liaison entre A et N dans Figure 97 maintient la connexion de tous les ports des ponts 555 à 888 au réseau.

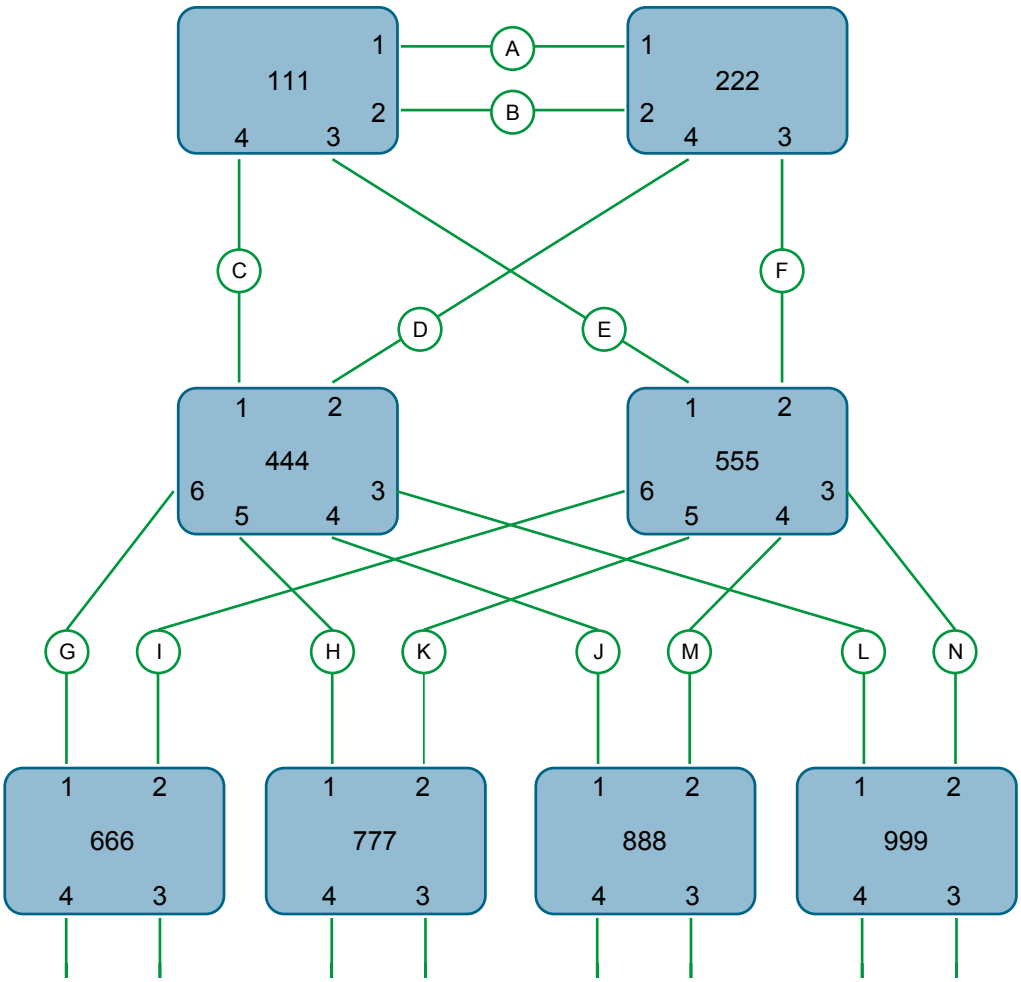


Figure 97 : Exemple - configuration de câblage structuré

Procédez comme suit pour concevoir une configuration de câblage structuré :

1. **Sélectionnez les paramètres de conception pour le réseau.**

   Quelles sont les conditions requises pour la robustesse et les temps de basculement/de récupération de réseau ? Existe-t-il des conditions requises spéciales pour un routage vers un ordinateur hôte central ? Existe-t-il des conditions requises spéciales pour la redondance de ports ?

2. **Identifiez la prise en charge du système hérité requise.**

   Des ponts STP sont-ils utilisés dans le réseau ? Ces ponts ne prennent pas en charge la transition rapide vers la transmission. Si ces ponts sont présents, peuvent-ils être redéployés plus près de la périphérie de réseau ?

3. **Identifiez les ports de périphérie et les ports avec restrictions de mode semi-duplex/de supports partagés.**

   Les ports se connectant à des ordinateurs hôtes, des IED (Intelligent Electronic Devices) et des contrôleurs peuvent être définis sur des ports de périphérie pour garantir une transition rapide vers le transfert et réduire le nombre de notifications de modification de topologie dans le réseau. Les ports avec restrictions de mode semi-duplex/de supports partagés requièrent une attention particulière pour garantir qu'ils n'entraînent pas d'extensions des temps de basculement/de récupération.

4. **Choisissez le pont racine et le pont racine de sauvegarde avec attention.**

   Le pont racine doit être sélectionné de manière à se trouver au point de concentration du trafic réseau. Localisez le pont racine de sauvegarde adjacent au pont racine. Une stratégie à utiliser consiste à modifier la priorité de pont pour établir le pont racine et ensuite modifier la priorité de chaque pont de manière à ce qu'elle corresponde à sa distance au pont racine.

5. **Identifiez la topologie d'état stable souhaitée.**

   Identifiez la topologie d'état stable souhaitée en tenant compte des vitesses de liaison, du trafic offert et de la qualité de service. Examinez les effets de la coupure de liaisons sélectionnées en tenant compte de la charge du réseau et de la qualité des liaisons alternatives.

6. **Décidez de la stratégie de calcul du coût de pont.**

   Sélectionnez si des coûts fixes ou à négociation automatique doivent être utilisés. Il est recommandé d'utiliser le style de coût avec négociation automatique, à moins qu'il ne soit nécessaire pour la conception du réseau de modifier le style de coût avec négociation automatique. Sélectionnez si le style de coût STP ou RSTP doit être utilisé. Assurez-vous de configurer le même style de coût sur tous les appareils du réseau.

7. **Activez l'option RSTP Fast Root Failover.**

   Il s'agit d'une fonctionnalité propriétaire de Siemens. Dans un réseau en maillage avec uniquement des appareils RUGGEDCOM au cœur du réseau, il est recommandé d'activer l'option RSTP Fast Root Failover pour minimiser les temps d'arrêt du réseau en cas de défaillance du pont racine.

8. Calculez et configurez les priorités et les coûts.

9. Mettez le réseau en œuvre et testez-le avec une charge.

Section 5.2.2.2

RSTP dans des configurations de structure en anneau

RSTP peut être utilisé dans des configurations de structure en anneau où une récupération rapide après défaillance de liaison est requise. En fonctionnement normal, RSTP bloque le trafic sur l'une des liaisons, par exemple, comme indiqué par les doubles barres sur la liaison H dans la Figure 98. En cas de défaillance sur la liaison D, le pont 444 déverrouille la liaison H. Le pont 333 communique avec le réseau via la liaison F.

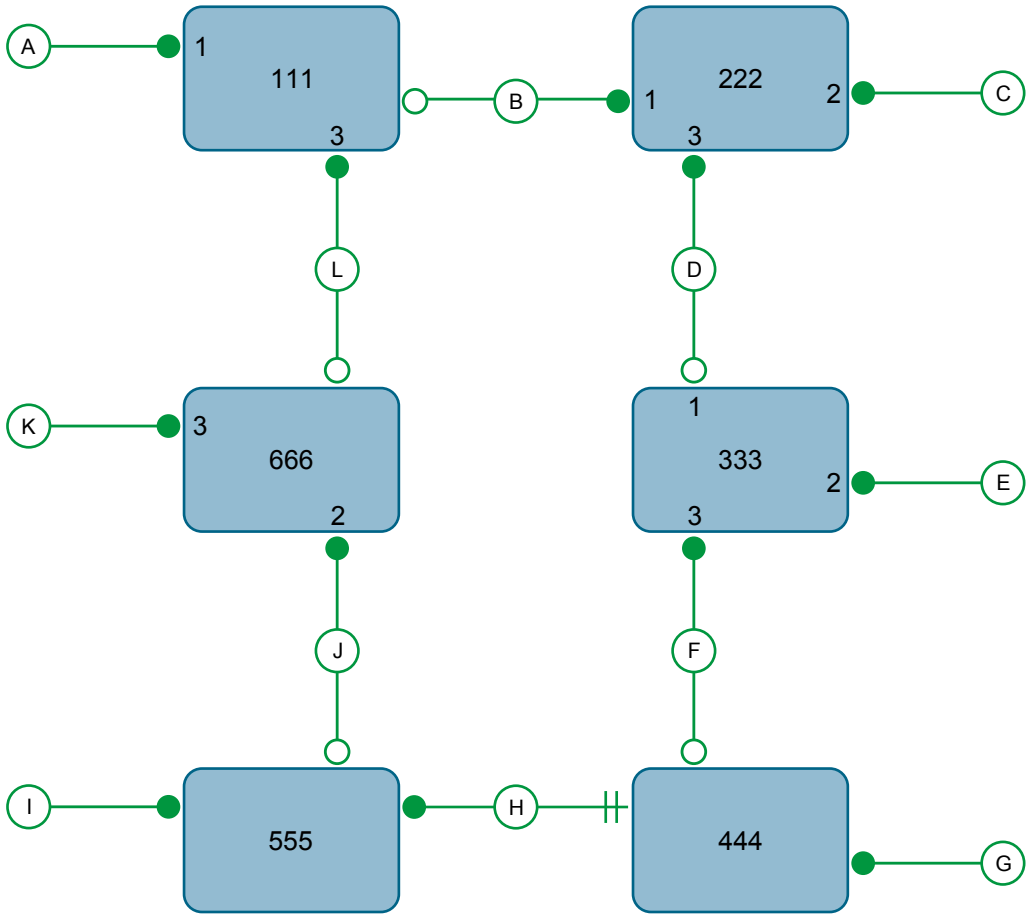


Figure 98 : Exemple - Configuration de structure en anneau

Procédez comme suit pour concevoir une configuration de structure en anneau avec RSTP :

1. **Sélectionnez les paramètres de conception pour le réseau.**

   Quelles sont les conditions requises pour la robustesse et les temps de basculement/de récupération de réseau ? Généralement, les structures en anneau sont choisies pour créer des conceptions de réseau économiques mais robustes.

2. **Identifiez la prise en charge de système hérité requise et les ports avec restrictions de mode semi-duplex/de supports partagés requis.**

   Ces ponts ne doivent pas être utilisés si les temps de basculement/de récupération de réseau doivent être minimisés.

3. **Identifiez les ports de périphérie.**

   Les ports se connectant à des ordinateurs hôtes, des IED (Intelligent Electronic Devices) et des contrôleurs peuvent être définis sur des ports de périphérie pour garantir une transition rapide vers le transfert et réduire le nombre de notifications de modification de topologie dans le réseau.

4. **Choisissez le pont racine.**

   Le pont racine peut être sélectionné pour équilibrer le nombre de ponts, le nombre de stations ou le volume de trafic sur l'un de ses segments. Il est important de savoir que l'anneau est toujours coupé à un endroit et que le trafic s'écoule toujours via la racine

5. **Affectez des priorités de pont à l'anneau.**

   La stratégie à utiliser consiste à affecter la priorité de chaque pont de manière à ce qu'elle corresponde à sa distance au pont racine. Si la priorité la plus basse (0) est affectée au pont racine, les ponts de chaque côté doivent utiliser une priorité de 4096, les ponts suivants de 8192, etc. Comme il existe 16 niveaux de priorité de pont disponibles, cette méthode fournit jusqu'à 31 ponts dans l'anneau.

6. **Décidez de la stratégie de calcul du coût de pont.**

   Il est recommandé d'utiliser le style de coût avec négociation automatique, à moins qu'il ne soit nécessaire pour la conception du réseau de modifier le style de coût avec négociation automatique. Sélectionnez si le style de coût STP ou RSTP doit être utilisé. Assurez-vous de configurer le même style de coût sur tous les appareils du réseau.

7. **Désactivez l'option RSTP Fast Root Failover.**

   Il s'agit d'une fonctionnalité propriétaire de Siemens. L'option RSTP Fast Root Failover est activée par défaut dans RUGGEDCOM ROS. Il est recommandé de désactiver cette fonctionnalité en cas de fonctionnement dans un réseau en anneau.

8. Mettez le réseau en œuvre et testez-le avec une charge.

Section 5.2.2.3

Redondance des ports RSTP

Dans des cas dans lesquels la redondance des ports est essentielle, RSTP permet à plusieurs ports ponts de traiter un LAN. Dans l'exemple suivant, si le port 3 est désigné pour acheminer le trafic réseau du LAN A, le port 4 bloque le trafic. Si une défaillance d'interface se produit sur le port 3, le port 4 prend le contrôle du LAN.

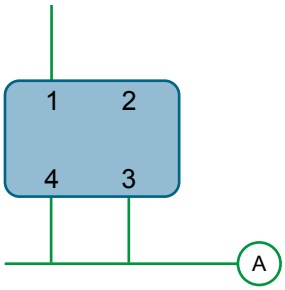


Figure 99 : Exemple - Redondance de ports

Section 5.2.3

Opérations MSTP

L'algorithme et le protocole MST (Multiple Spanning Tree) fournissent un meilleur contrôle et plus de flexibilité que RSTP et le STP hérité. MSTP (Multiple Spanning Tree Protocol) est une extension de RSTP dans laquelle plusieurs Spanning Trees peuvent être traités sur le même réseau ponté. Le trafic de données est affecté à un ou plusieurs Spanning Trees par le mappage d'un ou de plusieurs VLAN sur le réseau.

Le niveau de sophistication de l'utilitaire de mise en œuvre de Multiple Spanning Tree sur un réseau ponté donné est proportionnel au degré de planification et de conception investi dans la configuration de MSTP.

Si MSTP est activé sur certains ou tous les ponts dans un réseau sans configuration supplémentaire, le résultat est un réseau entièrement et simplement connecté, mais, au mieux, le résultat est le même qu'avec un réseau utilisant uniquement RSTP. Pour tirer pleinement parti des fonctionnalités offertes par MSTP, un nombre potentiellement important de variables de configuration est nécessaire. Elles peuvent être dérivées d'une analyse de trafic de données sur le réseau ponté et des exigences de partage de charge, de redondance et d'optimisation de chemin. Une fois ces paramètres tous dérivés, il est également important de les appliquer et de les gérer de manière cohérente au sein de tous les ponts dans une région MST.

De par sa conception, le temps de traitement MSTP est proportionnel au nombre d'instances STP actives. Cela signifie que MSTP sera probablement largement plus lent que RSTP. Par conséquent, RSTP doit être considéré comme une meilleure solution de redondance du réseau que MSTP pour des applications critiques.

SOMMAIRE

- Section 5.2.3.1, « Régions MSTP et interopérabilité »
- Section 5.2.3.2, « Rôles de pont et port MSTP »
- Section 5.2.3.3, « Avantages de MSTP »
- Section 5.2.3.4, « Mise en œuvre de MSTP sur un réseau ponté »

Section 5.2.3.1

Régions MSTP et interopérabilité

Outre la prise en charge de plusieurs Spanning Trees dans un réseau de ponts compatibles MSTP, MSTP est en mesure d'interagir avec des ponts prenant en charge uniquement RSTP ou STP hérité sans avoir besoin d'une configuration spéciale.

Une région MST peut être définie comme le jeu de ponts interconnectés dont l'identification de région MST est identique. L'interface entre les ponts MSTP et les ponts non-MSTP (ou entre des ponts MSTP avec différentes informations d'identification de région MSTT) devient partie intégrante d'une limite de région MST.

Les ponts en dehors d'une région MST voient la région entière comme s'il s'agissait d'un unique pont (R)STP. Le détail interne de la région MST est masqué du reste du réseau ponté. Dans ce contexte, MSTP comprend des *compteurs de sauts* séparés pour des informations de Spanning Tree échangées à la limite de la région MST contre celles propagées à l'intérieur de la région. Pour les informations reçues à la limite de la région MST, l'âge du message (R)STP est incrémenté une seule fois. À l'intérieur de la région, des comptages de sauts restants sont effectués, un par instance de Spanning Tree. Le paramètre Message Age externe dépend du délai de vieillissement maximum (R)STP, alors que les comptages de sauts restants sont comparés à un paramètre de sauts maximum MST à l'échelle de la région.

» MSTI

Une Multiple Spanning Tree Instance (MSTI) est l'une des seize instances de Spanning Tree indépendantes pouvant être définies dans une région MST (sans inclure l'IST – voir ci-dessous). Une MSTI est créée en mappant un ensemble de VLAN (dans RUGGEDCOM ROS, via la configuration de VLAN) sur un ID MSTI donné. Le même mappage doit être configuré sur tous les ponts qui sont censés faire partie de la MSTI. En outre, tous les VLAN et les mappages MSTI doivent être identiques pour tous les ponts et une région MST.

RUGGEDCOM ROS prend en charge 16 MSTI en plus de l'IST.

Chaque MSTI a une topologie indépendante. Pour cette raison, le trafic de données provenant de la même source et lié à la même destination mais sur différents VLAN sur différentes MSTI peut être transporté sur un chemin différent au sein du même réseau.

IST

Une région MST définit toujours un IST (Interne Spanning Tree). L'IST s'étend sur toute la région MST et transporte tout le trafic de données non spécifiquement affecté (par VLAN) à une MSTI spécifique. L'IST est toujours calculé et défini sur une MSTI zéro.

L'IST est également l'extension au sein de la région MST du CIST (voir ci-dessous), qui s'étend sur le réseau ponté entier, à l'intérieur et à l'extérieur de la région MST et tous les autres ponts RSTP et STP, ainsi que de toute autre région MST.

CST

Le CST (Common Spanning Tree) s'étend sur tout le réseau ponté, notamment les régions MST et tout pont STP ou RSTP connecté. Une région MST est considérée par le CST comme un pont individuel avec un coût unique associé à sa traversée.

CIST

Le CIST (Common and Internal Spanning Tree) est l'union des CST et IST dans toutes les régions MST. Le CIST s'étend pour cette raison sur le réseau ponté complet et atteint chaque région MST via l'IST de cette dernière pour atteindre chaque pont du réseau.

Section 5.2.3.2

Rôles de pont et port MSTP

MSTP prend en charge les rôles de pont et de port suivants :

Rôles de pont

Rôle	Description
Racine CIST	La racine est le pont racine choisi de CIST (Common and Internal Spanning Tree), qui s'étend sur tous les ponts STP et RSTP connectés et toutes les régions MSTP.
Racine CIST régionale	Le pont racine de l'IST au sein d'une région MSTP. La racine régionale CIST est le pont au sein d'une région MSTP avec le chemin de coût le plus bas vers la racine CIST. Notez que la racine régionale CIST se trouvera à la limite d'une région MSTP. Notez également qu'il est possible que la racine régionale CIST soit la racine CIST.
Racine MSTI régionale	Le pont racine d'une MSTI au sein d'une région MSTP. Un pont racine est choisi de manière indépendante pour chaque MSTI dans une région MSTP.

Rôles de port

Chaque port sur un pont MSTP peut avoir plus d'un rôle CIST selon le nombre d'instances de Spanning Tree définies sur le port et leur topologie.

Rôle	Description
Rôles de port CIST	• Le port racine fournit le chemin de coût minimum du pont vers la racine CIST via la racine régionale CIST. Si le pont lui-même est une racine régionale CIST, le port racine est également le port maître

Rôle	Description
	pour toutes les MSTI et fournit le chemin de coût minimum pour une racine CIST située en dehors de la région. • Un port racine désigné fournit le chemin de coût minimum depuis un LAN attaché vers la racine régionale CIST via le pont. • Les ports alternatifs et de sauvegarde fonctionnent de la même manière que dans RSTP, mais en fonction de la racine régionale CIST.
Rôles de port MSTI	Pour chaque MSTI sur un pont : • Le port racine fournit le chemin de coût minimum du pont vers la racine régionale CIST, si le pont lui-même n'est pas la racine régionale CIST. • Un port racine désigné fournit le chemin de coût minimum d'un LAN attaché vers la racine régionale MSTI via le pont. • Les ports alternatifs et de sauvegarde fonctionnent de la même manière que dans RSTP, mais en fonction de la racine régionale MSTI. Si le port maître, qui est unique dans une région MSTP, est le port racine CIST de la racine régionale CIST et fournit le chemin de coût minimum pour la racine CIST pour toutes les MSTI.
Ports limites	Un port limite est un port sur un pont dans une région MSTP qui peut se connecter à un pont appartenant à une région MSTP différente ou à un pont prenant uniquement en charge RSTP ou STP hérité. Un port limite bloque et transmet tous les VLAN de la même manière depuis toutes les MSTI et tous les CIST. Un port limite peut être : • Le port racine CIST sur la racine régionale CIST (et donc également le port maître MSTI). • Un port CIST désigné, un port alternatif/de sauvegarde ou désactivé. À la limite de la région MSTP, le rôle de port MSTI est le même que le rôle de port CIST. Un port limite connecté à un pont STP envoie uniquement des BPDU STP. Un port connecté à un pont RSTP ne doit pas s'abstenir d'envoyer des BPDU MSTP. Cela est possible en raison du fait que le MSTP comprend l'identificateur de racine régionale CIST dans le champ que RSTP analyse en tant qu'identificateur de pont désigné.

Section 5.2.3.3

Avantages de MSTP

Outre le fait que MSTP est configuré par défaut de manière à arriver automatiquement dans une solution de Spanning Tree pour chaque MSTI configurée, des avantages peuvent être obtenus en influençant la topologie des MSTI dans une région MST. Le fait que la priorité de pont (Bridge Priority) et que le coût de chaque port sont configurables par MST rend possible le contrôle de la topologie pour chaque MSTI au sein d'une région.

Equilibrage de charge

MSTP peut être utilisé pour équilibrer la charge de trafic de données dans un ensemble de VLAN, permettant ainsi une utilisation plus optimale d'un réseau ponté à interconnexions multiples.

Un réseau ponté contrôlé par un Spanning Tree unique bloque des liens redondants afin d'éviter des boucles nuisibles. Avec MSTP, cependant, tout lien donné peut avoir un état de blocage différent pour MSTI conformément au MSTP. Pour cette raison, tout lien donné peut être à l'état de blocage pour certains VLAN et à un état de transmission pour d'autres VLAN selon le mappage des VLAN sur des MSTI.

Il est possible de contrôler la solution de Spanning Tree pour chaque MSTI, notamment le jeu de liens actifs pour chaque arbre, en manipulant (par MSTI) la priorité de pont et les coûts de port de liaisons dans le réseau. Si un trafic est affecté de manière judicieuse à plusieurs VLAN, les interconnexions redondantes dans un réseau ponté qui seraient restées inutilisées avec un Spanning Tree unique peuvent maintenant transporter le trafic.

Isolation de la reconfiguration du Spanning Tree.

Une défaillance de lien dans une région MSTP qui n'affecte pas les rôles de ports limites n'entraîne pas la reconfiguration de CST, et la modification n'affecte pas d'autres régions MSTP. La raison est que les informations MSTP ne se propagent pas au-delà des limites de la région.

MSTP contre PVST

Un avantage de MSTP par rapport au protocole propriétaire PVST de Cisco Systems Inc. est la capacité de mapper plusieurs VLAN sur une unique MSTI. Comme chaque Spanning Tree requiert un traitement et de la mémoire, les coûts entraînés par le suivi d'un nombre croissant de VLAN augmentent beaucoup plus rapidement avec PVST qu'avec MSTP.

Compatibilité avec STP et RSTP

Aucune configuration spécifique n'est requise pour les ponts d'une région MST pour établir une connexion complète en toute simplicité à des ponts non-MST sur le même réseau ponté. Une planification et une configuration soignées sont cependant recommandées pour créer un réseau optimal.

Section 5.2.3.4

Mise en œuvre de MSTP sur un réseau ponté

Il est recommandé de suivre la séquence présentée ci-dessous pour la configuration de MSTP pour un réseau.

Naturellement, il est également recommandé que l'analyse et la planification du réseau informent sur les étapes de configuration du VLAN et des paramètres MSTP en particulier.

À commencer par un ensemble de ponts Ethernet compatibles avec MSTP et la désactivation de MSTP. Pour chaque pont dans le réseau :

REMARQUE
MSTP n'a pas besoin d'être activé pour mapper un VLAN à une MSTI. Cependant, le mappage doit être identique pour chaque pont appartenant à la région MSTP.

1. Configurez et désactivez STP globalement et/ou pour des ports Ethernet spécifiques Pour plus d'informations, voir Section 5.2.4, « Configuration globale du STP » ou Section 5.2.5, « Configuration du STP pour des ports Ethernet spécifiques ».

   REMARQUE
   Des VLAN statiques doivent être utilisés dans une configuration MSTP. GVRP n'est pas pris en charge

2. Ajoutez des VLAN statiques et mappez-les à des MSTI. Pour plus d'informations, voir Section 5.1.5.2, « Ajout d'un VLAN statique ».

> **REMARQUE**
> *L'identification de région et le niveau de révision doivent être les mêmes pour chaque pont dans la région MST.*

3. Configurez le niveau de révision pour l'identificateur de région MST. Pour plus d'informations, voir Section 5.2.9.3, « Configuration de l'identificateur de région MST ».
4. Assurez-vous que le résumé en lecture seule pour l'identificateur de région MST est identique pour chaque point dans la région MST. Si le résumé est différent, l'ensemble de mappages pour les VLAN et le MSTI diffèrent.
5. Configurez la priorité de pont pour le MSTI global. Pour plus d'informations, voir Section 5.2.9.4, « Configuration d'une MSTI globale ».
6. Configurez le coût de port et la priorité par port pour chaque MSTI. Pour plus d'informations, voir Section 5.2.9.5, « Configuration d'une MSTI pour un port Ethernet ».
7. Définissez la version de protocole STP sur MSTP et activez STP. Pour plus d'informations, voir Section 5.2.4, « Configuration globale du STP ».

Section 5.2.4

Configuration globale du STP

Procédez comme suit pour configurer des réglages globaux du STP (Spanning Tree Protocol) :

1. Accédez à ***Spanning Tree » Configure Bridge RSTP Parameters***. Le formulaire **Bridge RSTP Parameters** s'affiche.

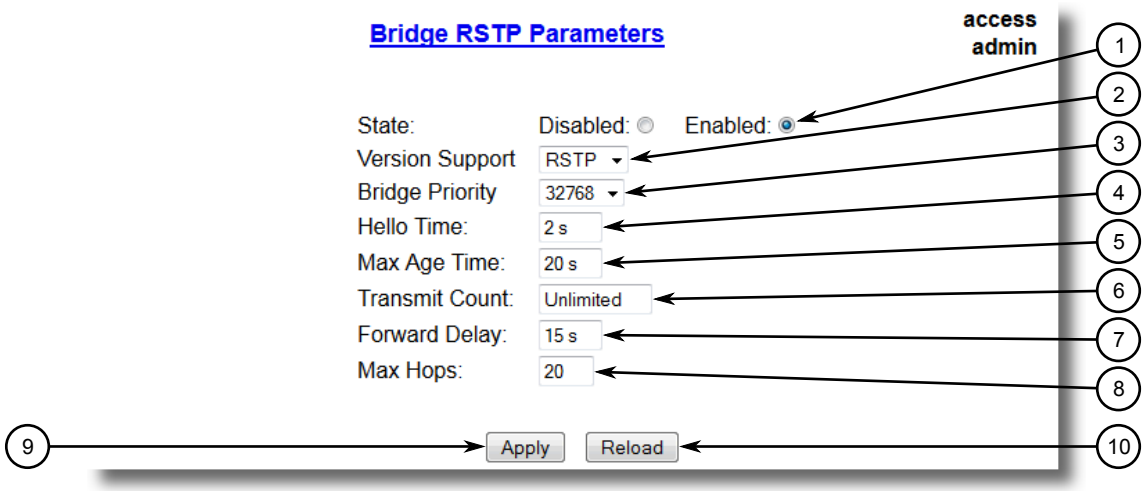


Figure 100 : Formulaire Bridge RSTP Parameters

1. Options State **2.** Liste Version Support **3.** Liste Bridge Priority **4.** Zone Hello Time **5.** Zone Max Age Time **6.** Zone Transmit Count **7.** Zone Forward Delay **8.** Zone Max Hops **9.** Bouton Apply **10.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
State	**Synopsis :** { Disabled, Enabled } **Par défaut :** Enabled Activer STP/RSTP/MSTP pour le pont globalement. Notez que STP/RSTP/MSTP est activé sur un port lorsqu'il est activé globalement avec le réglage de l'activation par port.
Version Support	**Synopsis :** { STP, RSTP, MSTP } **Par défaut :** RSTP Sélectionne la version du protocole Spanning Tree à prendre en charge, STP uniquement, Rapid STP ou Multiple STP.
Bridge Priority	**Synopsis :** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Par défaut :** 32768 Bridge Priority (priorité de pont) fournit une manière de contrôler la topologie du réseau connecté via STP. Les points racine et désigné peuvent être configurés pour une topologie spécifique. Le pont avec la priorité la plus basse devient la racine. En cas de défaillance du pont racine, le pont avec la priorité la plus basse suivante devient la racine. Les ponts désignés qui alimentent un LAN commun (à des fins de redondance) utilisent également une priorité pour déterminer le pont actif. De cette manière, une sélection minutieuse des priorités de point peut établir le chemin de flux de trafics dans des conditions normales et anormales.
Hello Time	**Synopsis :** 1 à 10 s **Par défaut :** 2 s Temps entre les messages de configuration générés par le pont source. Les temps Hello réduits entraînent une détection plus rapide de modifications de la topologie au détriment d'un trafic STP plus intense.
Max Age Time	**Synopsis :** 6 à 40 s **Par défaut :** 20 s Temps pendant lequel un message de configuration reste valide après avoir été généré par le pont source. Configurez ce paramètre avec précaution lorsque de nombreuses couches de pont existent, ou si des liaisons à basse vitesse (telles que celles utilisées dans des WAN) font partie du réseau.
Transmit Count	**Synopsis :** 3 à 100 ou { Unlimited } **Par défaut :** Unlimited Nombre maximum de BPDU sur chaque port pouvant être envoyées en une seconde. Une valeur plus élevée permet au réseau de récupérer en cas de liaisons défaillantes/ponts défaillantes plus rapidement.
Forward Delay	**Synopsis :** 4 à 30 s **Par défaut :** 15 s Le temps dont un pont a besoin pour apprendre des adresses MAC sur un pont montant avant de commencer à transmettre le trafic. Des valeurs plus basses permettent au port d'atteindre l'état de transmission plus rapidement, mais au détriment d'une avalanche d'adresses non apprises vers tous les ports.
Max Hops	**Synopsis :** 6 à 40 **Par défaut :** 20 Applicable uniquement au MSTP. Diamètre de pont maximum possible au sein d'une région MST. Les BPDU MSTP propagées au sein d'une région MST spécifient une durée de vie décrémentée par chaque commutateur qui propage les BPDU. Si le nombre de tronçons au sein de la région dépasse le nombre maximum configuré, les BPDU peuvent être rejetées en raison de leur durée de vie paramétrée.

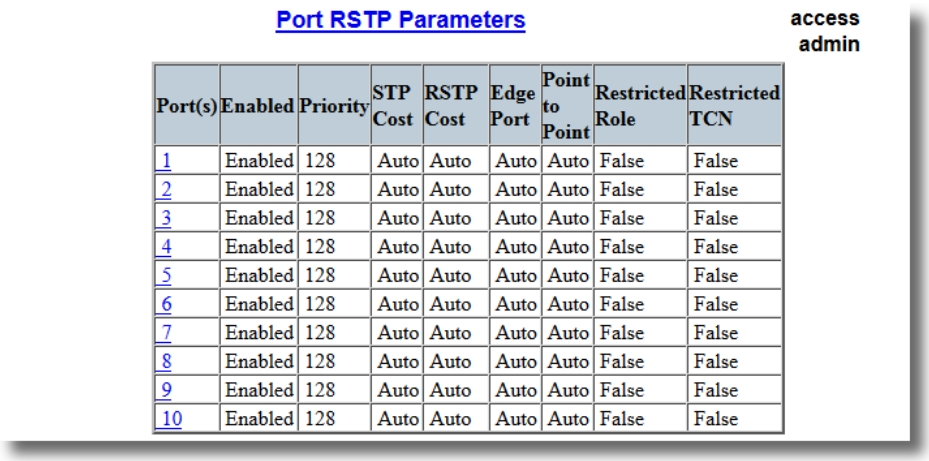
3. Cliquez sur **Apply**.

Section 5.2.5

Configuration du STP pour des ports Ethernet spécifiques

Procédez comme suit pour configurer le STP (Spanning Tree Protocol) pour un port Ethernet spécifique :

1. Accédez à ***Spanning Tree » Configure Port RSTP Parameters***. Le tableau **Port RSTP Parameters** s'affiche.



Port RSTP Parameters

access admin

Port(s)	Enabled	Priority	STP Cost	RSTP Cost	Edge Port	Point to Point	Restricted Role	Restricted TCN
1	Enabled	128	Auto	Auto	Auto	Auto	False	False
2	Enabled	128	Auto	Auto	Auto	Auto	False	False
3	Enabled	128	Auto	Auto	Auto	Auto	False	False
4	Enabled	128	Auto	Auto	Auto	Auto	False	False
5	Enabled	128	Auto	Auto	Auto	Auto	False	False
6	Enabled	128	Auto	Auto	Auto	Auto	False	False
7	Enabled	128	Auto	Auto	Auto	Auto	False	False
8	Enabled	128	Auto	Auto	Auto	Auto	False	False
9	Enabled	128	Auto	Auto	Auto	Auto	False	False
10	Enabled	128	Auto	Auto	Auto	Auto	False	False

Figure 101 : Tableau Port RSTP Parameters

2. Sélectionnez un port Ethernet. Le formulaire **Port RSTP Parameters** s'affiche.

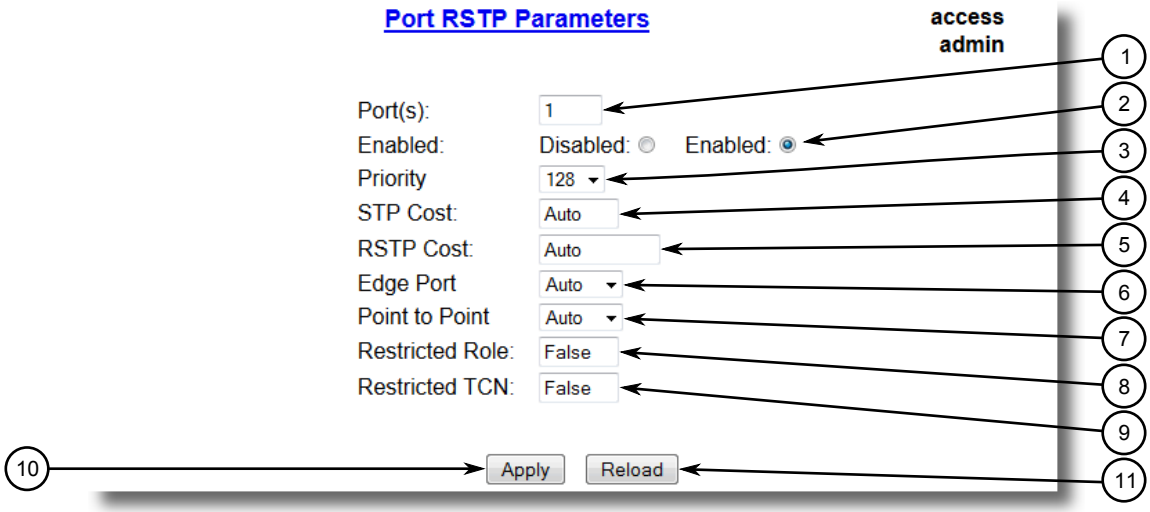


Figure 102 : Formulaire Port RSTP Parameters

1. Zone Port(s) **2.** Options Enabled **3.** Liste Priority **4.** Zone STP Cost **5.** Zone RSTP Cost **6.** Liste Edge Port **7.** Liste Point to Point **8.** Zone Restricted Role **9.** Zone Restricted TNC **10.** Bouton Apply **11.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
Enabled	**Synopsis :** { Disabled, Enabled } **Par défaut :** Enabled L'activation de STP active le protocole STP ou RSTP pour ce port en fonction de la configuration dans le menu STP Configuration. STP peut être désactivé pour le port UNIQUEMENT si le port n'est aucunement attaché à un pont STP. Le non-respect de cette exigence entraînera une boucle de trafic non détectable. Une meilleure alternative à la désactivation du port consiste à garder STP activé tout en configurant le port en tant que port de périphérie. Un candidat approprié pour une déconnexion de STP peut être un port alimentant uniquement un seul ordinateur hôte.
Priority	**Synopsis :** { 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 194, 208, 224, 240 } **Par défaut :** 128 Sélectionne la priorité du port STP. Les ports ayant le même coût attachés à un LAN commun sélectionnent le port à utiliser en fonction de la priorité.
STP Cost	**Synopsis :** 0 à 65535 ou { Auto } **Par défaut :** Auto Sélectionne le coût à appliquer dans le calcul de coûts lorsque le paramètre Cost Style est défini sur STP dans la configuration des paramètres Bridge RSTP. La définition manuelle du coût fournit la capacité à sélectionner de manière préférentielle des ports spécifiques pour transmettre le trafic à d'autres. Laissez ce champ défini sur "auto" pour utiliser les coûts de port STP standard négociés (4 pour 1 Gbit/s, 19 pour des liaisons 100 Mbit/s et 100 pour des liaisons 10 Mbit/s). Pour MSTP, ce paramètre s'applique au coût de chemin externe et interne.
RSTP Cost	**Synopsis :** 0 à 2147483647 ou { Auto } **Par défaut :** Auto Sélectionne le coût à appliquer dans le calcul de coûts lorsque le paramètre Cost Style est défini sur RSTP dans la configuration des paramètres Bridge RSTP. La définition manuelle du coût fournit la capacité à sélectionner de manière préférentielle des ports spécifiques pour transmettre le trafic à d'autres. Laissez ce champ défini sur "auto" pour utiliser les coûts de port RSTP standard négociés (20 000 pour 1 Gbit/s, 200 000 pour des liaisons 100 Mbit/s et 2 000 000 pour des liaisons 10 Mbit/s). Pour MSTP, ce paramètre s'applique au coût de chemin externe et interne.
Edge Port	**Synopsis :** { False, True, Auto } **Par défaut :** Auto Les ports de périphérie sont des ports qui ne participent pas au Spanning Tree mais envoient malgré tout des messages de configuration. Ils passent directement au transfert de trame sans écoute ni délai d'apprentissage. Les tableaux MAC des ports de périphérie n'ont pas besoin d'être vidés lorsque des modifications de la topologie se produisent dans le réseau STP. Au contraire d'un port désactivé avec STP, une connexion accidentelle d'un port de périphérie à un autre port dans le Spanning Tree entraîne une boucle détectable. Le port est alors désactivé en tant que port de périphérie et les règles RSTP standard sont appliquées (jusqu'à la prochaine défaillance de liaison).
Point to Point	**Synopsis :** { False, True, Auto } **Par défaut :** Auto RSTP utilise un protocole pair à pair qui fournit une transition rapide sur des liaisons point à point. Le protocole est désactivé automatiquement si plusieurs ponts STP communiquent via un LAN partagé (non point à point). Le pont considère automatiquement le point à point comme vrai lorsque la liaison est reconnue comme fonctionnant en mode duplex intégral. Ce comportement est annulé par le paramètre point à point qui est forcé sur True ou False. Le paramètre est forcé sur True lorsque le port traite une liaison point à point mais ne peut pas exécuter cette dernière en mode duplex intégral. Le paramètre est forcé sur False lorsque le port traite la liaison en mode

Paramètre	Description
	duplex intégral, mais n'est pas un port point à point (c'est-à-dire une liaison en duplex intégral vers un commutateur non managé qui concentre deux autres ponts STP).
Restricted Role	**Synopsis :** { True ou False } **Par défaut :** False Valeur booléenne définie par l'administration. Si TRUE est défini, le port n'est pas sélectionné comme port racine pour le CIST ou toute MSTI, même s'il a le meilleur vecteur de priorité de Spanning Tree. Il est alors sélectionné comme port alternatif une fois le port racine sélectionné. Ce paramètre doit être réglé sur FALSE par défaut. S'il est activé, il peut entraîner un manque de connectivité du Spanning Tree. Il est défini par un administrateur réseau de manière à éviter que des ponts externes à une région de base du réseau influencent la topologie active du Spanning Tree. Cela peut être nécessaire, par exemple, si ces ponts ne sont pas entièrement contrôlés par l'administrateur.
Restricted TCN	**Synopsis :** { True ou False } **Par défaut :** False Valeur booléenne définie par l'administration. Si TRUE est défini, le port ne propage pas de notifications de modification de topologie reçues ni les modifications de topologie vers d'autres ports. Si le paramètre est activé, il peut entraîner une perte temporaire de la connectivité après des modifications de la topologie active du Spanning Tree en raison d'informations d'emplacement de station persistantes et non correctement apprises. Il est défini par un administrateur réseau de manière à éviter que des ponts externes à une région de base du réseau entraînent un vidage d'adresse dans cette région. Cela peut être nécessaire, par exemple, si ces ponts ne sont pas entièrement contrôlés par l'administrateur ou si le paramètre d'état MAC_Operational pour les LAN attachés effectue des transitions fréquentes.

4. Cliquez sur **Apply**.

Section 5.2.6

Configuration d'eRSTP

Procédez comme suit pour configurer l'eRSTP :

1. Accédez à ***Spanning Tree » Configure eRSTP Parameters***. Le formulaire **eRSTP Parameters** s'affiche.

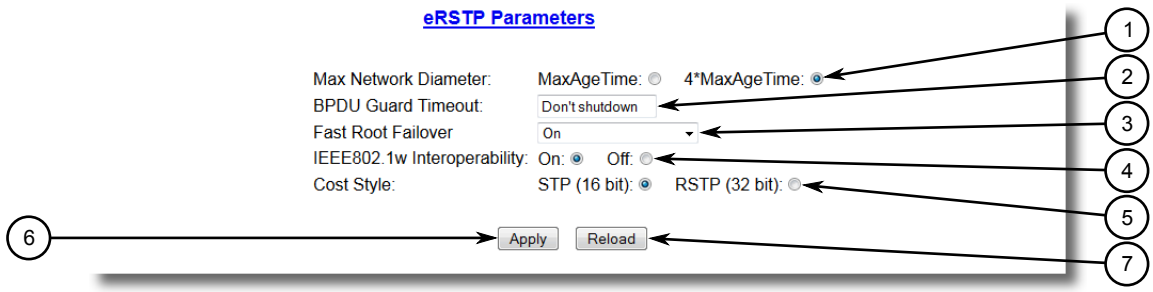


Figure 103 : Formulaire eRSTP Parameters

1. Options Max Network Diameter **2.** Zone BPDU Guart Timeout **3.** Liste Fast Root Failover **4.** Options IEEE802.1w Interoperability **5.** Options Cost Style **6.** Bouton Apply **7.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Max Network Diameter	**Synopsis :** { MaxAgeTime, 4*MaxAgeTime } **Par défaut :** 4*MaxAgeTime La norme RSTP définit une limite de la taille maximum du réseau pouvant être contrôlée par le protocole RSTP. La taille du réseau est décrite par le terme 'maximum network diameter' (diamètre du réseau maximum), qui est le nombre de commutateurs comprenant le chemin le plus long que les BPDU RSTP doivent traverser. Le diamètre du réseau standard maximum pris en charge est égal à la valeur du paramètre de configuration RSTP 'MaxAgeTime'. eRSTP offre un RSTP optimisé lui permettant de couvrir des réseaux plus importants que ceux définis par la norme. Ce paramètre de configuration sélectionne la taille réseau maximum prise en charge.
BPDU Guard Timeout	**Synopsis :** 1 à 86400 s ou { Until reset, Don't shutdown } **Par défaut :** Don't shutdown Le protocole RSTP ne tient pas compte de la sécurité du réseau. RSTP doit traiter chaque BPDU reçue et intervenir de manière appropriée. Ceci peut permettre à un pirate d'influence la topologie RSTP en injectant des BPDU RSTP dans le réseau. BPDU Guard est une fonctionnalité protégeant le réseau de BPDU reçues par un port où des appareils compatibles avec RSTP ne sont pas sensés être attachés. Si une BPDU est reçue par un port pour lequel le paramètre 'Edge' est défini sur 'TRUE' ou RSTP est désactivé, le port est fermé pendant la période spécifiée par ce paramètre. • DON'T SHUTDOWN - BPDU Guard est désactivé • UNTIL RESET - le port reste fermé jusqu'à ce que la commande de réinitialisation du port soit lancée par l'utilisateur
Fast Root Failover	**Synopsis :** { On, On with standard root, Off } **Par défaut :** On Dans des topologies de réseau en maillage, l'algorithme RSTP standard ne garantit pas la récupération de réseau déterministe en cas de défaillance d'un commutateur racine. Un tel délai de récupération est difficile à calculer et peut être différent (et éventuellement relativement long) pour toute topologie en maillage. Ce paramètre de configuration active le RSTP amélioré de Siemens, qui détecte une défaillance du commutateur racine et exécute des étapes de traitement RSTP supplémentaires, réduisant ainsi le temps de récupération du réseau et le rendant déterministe. **REMARQUE** • *Cette fonctionnalité est uniquement disponible en mode RSTP. En mode MSTP, le paramètre de configuration est ignoré.* • *Dans une topologie en anneau unique, cette fonctionnalité n'est pas nécessaire et doit être désactivée afin d'éviter des délais de récupération de réseau plus longs en raison d'un traitement RSTP supplémentaire.* L'algorithme Fast Root Failover (commutation rapide de racine) doit être pris en charge par tous les commutateurs dans le réseau, notamment la racine, pour garantir une performance optimale. Cependant, il n'est pas inhabituel d'affecter le rôle de racine à un commutateur d'un fournisseur différent du reste des commutateurs dans le réseau. En d'autres termes, il est possible que la racine ne prenne pas en charge l'algorithme Fast Root Failover Dans un tel cas, un algorithme "souple" tolérant le manque de prise en charge dans le commutateur racine doit être utilisé. Les options de configuration prises en charge sont les suivantes : • Off - l'algorithme Fast Root Failover est désactivé, et une défaillance du commutateur racine peut donc entraîner un temps de récupération de connectivité excessif. • On - l'algorithme Fast Root Failover est activé et l'algorithme le plus robuste est utilisé, ce qui requiert une prise en charge appropriée dans le commutateur racine. • On with standard root - Fast Root Failover est activé mais un algorithme "souple" est utilisé, permettant ainsi l'utilisation d'un commutateur standard pour le rôle racine.
IEEE802.1w Interoperability	**Synopsis :** { On, Off }

Paramètre	Description
	Par défaut : On Le protocole RSTP original défini dans la norme IEEE 802.1w comprend des différences minimes par rapport à des normes optimisées plus récentes. Ces différences entraînent des problèmes d'interopérabilité qui, même s'ils n'interrompent pas entièrement le fonctionnement du RSTP, peuvent provoquer un temps de récupération plus élevé en cas de défaillance dans le réseau. eRSTP propose des améliorations du protocole, qui permettent aux commutateurs d'interagir complètement avec des commutateurs d'autres fournisseurs pouvant exécuter le RSTP IEEE 802.2w. Ces améliorations n'affectent pas l'interopérabilité avec des éditions plus récentes du RSTP. Ce paramètre de configuration active le mode d'interopérabilité mentionné ci-dessus.
Cost Style	**Synopsis :** { STP (16 bit), RSTP (32 bit) } **Par défaut :** STP (16 bit) Le standard RSTP définit deux styles de valeur de coût du chemin. STP utilise des coûts de chemin 16 bits basés sur 1x10E9/vitesse de liaison (4 pour 1 Gbit/s, 19 pour 100 Mbit/s et 100 pour 10 Mbit/s), alors que RSTP utilise des coûts 32 bits basés sur 2x10E13/vitesse de liaison (20 000 pour 1 Gbit/s, 200 000 pour 100 Mbit/s et 2 000 000 pour 10 Mbit/s). Cependant, les commutateurs de certains fournisseurs continuent à utiliser le type de coût de chemin STP même en mode RSTP, ce qui peut entraîner une confusion et des problèmes d'interopérabilité. Ce paramètre de configuration sélectionne le style de coût de liaison à employer. Notez que les coûts de liaison RSTP sont utilisés uniquement lorsque la prise en charge de version de pont est définie de manière à autoriser RSTP et le port ne migre pas vers STP.

3. Cliquez sur **Apply**.

Section 5.2.7

Affichage de statistiques globales concernant STP

Pour afficher des statistiques globales concernant STP, accédez à ***Spanning Tree » View Bridge RSTP Statistics***. Le formulaire **Bridge RSTP Statistics** s'affiche.

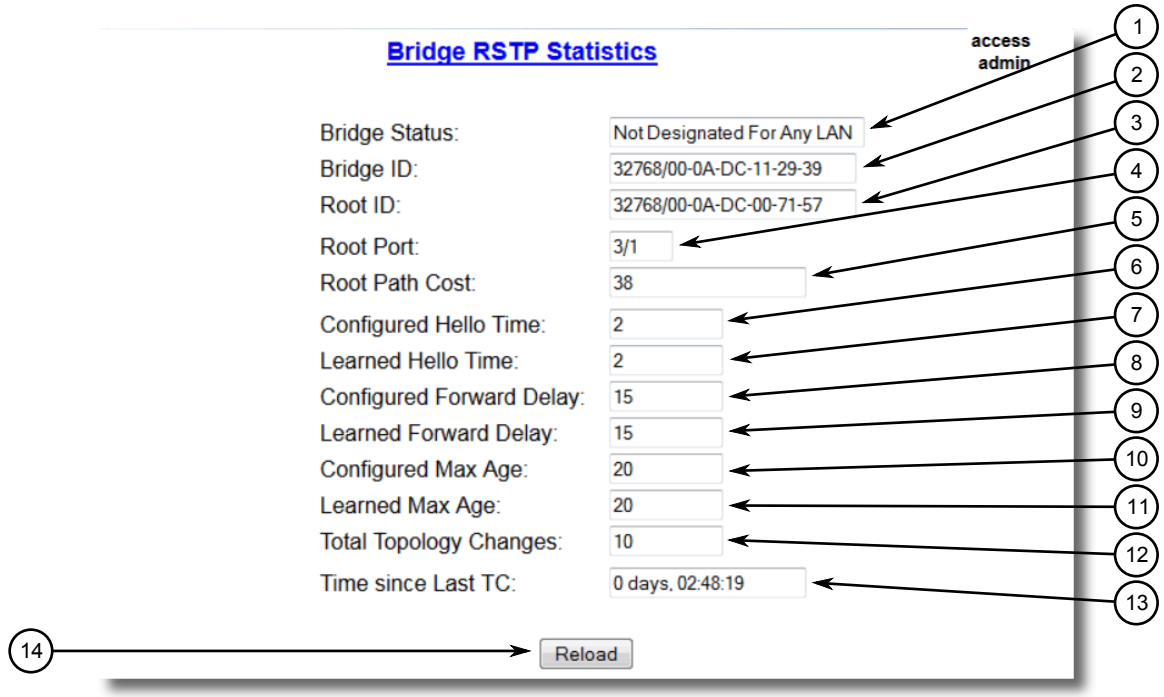


Figure 104 : Formulaire Bridge RSTP Statistics

1. Zone Bridge Status **2.** Zone Bridge ID **3.** Zone Root ID **4.** Zone Root Port **5.** Zone Root Path Cost **6.** Zone Configure Hello Time **7.** Zone Learned Hello Time **8.** Zone Configured Forward Delay **9.** Zone Learned Forward Delay **10.** Zone Configured Max Age **11.** Zone Learned Max Age **12.** Zone Total Topology Changes **13.** Zone Time since Last TC **14.** Bouton Reload

Ce tableau affiche les informations suivantes :

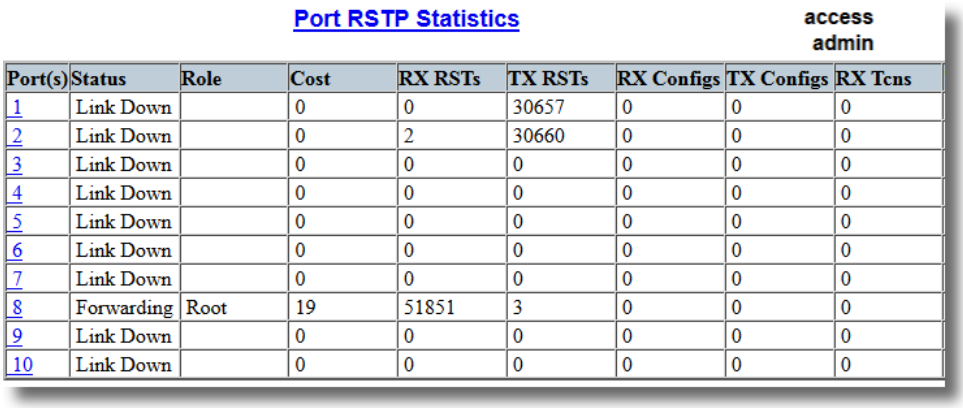
Paramètre	Description
Bridge Status	**Synopsis :** { , Designated Bridge, Not Designated For Any LAN, Root Bridge } État Spanning Tree du pont. L'état peut être racine ou désigné. Ce champ peut indiquer Not Designated For Any LAN pour tout LAN si le pont n'est désigné pour aucun de ses ports.
Bridge ID	**Synopsis :** $$ / ##-##-##-##-##-## où $$ a une plage de 0 à 65535 et ## de 0 à FF Identificateur de ce pont.
Root ID	**Synopsis :** $$ / ##-##-##-##-##-## où $$ a une plage de 0 à 65535 et ## de 0 à FF Identificateur du pont racine.
Port racine	**Synopsis :** 1 au numéro de port maximum ou { <chaîne vide> } Si le pont est désigné, il s'agit du port qui fournit la connectivité au pont racine du réseau.
Root Path Cost	**Synopsis :** 0 à 4294967295 Coût total du chemin au pont racine composé de la somme des coûts de chaque liaison dans le chemin. Si des coûts personnalisés n'ont pas été configurés. Les ports 1 Gbit/s ajoutent 4, les ports 100 Mbit/s ajoutent 19 et les ports 10 Mbit/s ajoutent 100 à ce chiffre. Pour l'instance CIST de MSTP, il s'agit d'un coût de chemin racine externe, qui correspond au coût du chemin du pont racine IST (c'est-à-dire la racine régionale) au pont racine CST (c'est-à-dire la racine réseau "globale").
Configured Hello Time	**Synopsis :** 0 à 65535 Délai Hello Time configuré dans le menu Bridge RSTP Parameters.

Paramètre	Description
Learned Hello Time	**Synopsis :** 0 à 65535 Délai Hello Time effectif fourni par le pont racine comme il a été appris dans des messages de configuration. Ce délai est utilisé dans des ponts désignés.
Configured Forward Delay	**Synopsis :** 0 à 65535 Délai de transmission (Forward Delay) configuré dans le menu Bridge RSTP Parameters.
Learned Forward Delay	**Synopsis :** 0 à 65535 Forward Delay effectif fourni par le pont racine comme il a été appris dans des messages de configuration. Ce délai est utilisé dans des ponts désignés.
Configured Max Age	**Synopsis :** 0 à 65535 Délai de vieillissement maximum configuré dans le menu Bridge RSTP Parameters.
Learned Max Age	**Synopsis :** 0 à 65535 Délai de vieillissement effectif fourni par le pont racine comme il a été appris dans des messages de configuration. Ce délai est utilisé dans des ponts désignés.
Total Topology Changes	**Synopsis :** 0 à 65535 Nombre de modifications de topologie dans le réseau, comme détecté sur ce pont via des défaillances de liaison ou signalé depuis d'autres ponts. Un nombre excessivement élevé ou croissant rapidement signale des problèmes réseau.
Time since Last TC	**Synopsis :** DDDD jours, HH:MM:SS Temps depuis la dernière détection d'une modification de topologie par le pont.

Section 5.2.8

Affichage de statistiques STP pour des ports Ethernet

Pour afficher des statistiques STP pour des ports Ethernet, accédez à ***Spanning Tree » View Port RSTP Statistics***. Le tableau **Port RSTP Statistics** s'affiche.



Port RSTP Statistics

access admin

Port(s)	Status	Role	Cost	RX RSTs	TX RSTs	RX Configs	TX Configs	RX Tcns
1	Link Down		0	0	30657	0	0	0
2	Link Down		0	2	30660	0	0	0
3	Link Down		0	0	0	0	0	0
4	Link Down		0	0	0	0	0	0
5	Link Down		0	0	0	0	0	0
6	Link Down		0	0	0	0	0	0
7	Link Down		0	0	0	0	0	0
8	Forwarding	Root	19	51851	3	0	0	0
9	Link Down		0	0	0	0	0	0
10	Link Down		0	0	0	0	0	0

Figure 105 : Tableau Port RSTP Statistics

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre

Paramètre	Description
	Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
Status	**Synopsis :** { Disabled, Listening, Learning, Forwarding, Blocking, Link Down, Discarding } État de ce port dans le Spanning Tree. Réglages possibles : • **Disabled** - STP est désactivé sur ce port. • **Link Down** - STP est activé sur ce port, mais la liaison désactivée. • **Discarding** - la liaison n'est pas utilisée dans la topologie STP mais est en réserve. • **Learning** - le port apprend les adresses MAC pour éviter une avalanche quand il commence à transmettre le trafic. • **Forwarding** - le port transmet le trafic.
Rôle	**Synopsis :** { , Root, Designated, Alternate, Backup, Master } Rôle de ce port dans le Spanning Tree. Réglages possibles : • **Designated** -le port est désigné pour (c'est-à-dire transfère le trafic vers la racine pour) le LAN auquel il est connecté. • **Root** - le port unique sur le pont, qui fournit la connectivité vers le pont racine. • **Backup** - le port est attaché à un LAN alimenté par un autre port sur le pont. Il n'est pas utilisé mais est en réserve. • **Alternate** - le port est attaché à un pont qui fournit la connectivité au pont racine. Il n'est pas utilisé mais est en réserve. • **Master** - existe uniquement dans le MSTP. Le port est un port limite de région MST et l'unique port sur le pont qui fournit la connectivité pour la Multiple Spanning Tree Instance vers le port racine Common Spanning Tree (c'est-à-dire que ce port est le port racine pour la Common Spanning Tree Instance).
Cost	**Synopsis :** 0 à 4294967295 Coût offert par ce port. Si le style de coût des paramètres Bridge RSTP est défini sur STP, les ports 1 Gbit/s ajoutent 4 au coût, les ports 100 Mbit/s 19 et les ports 10 Mbit/s 100. Si le style de coût est défini sur STP, les ports 1 Gbit/s ajoutent 20.000 au coût, les ports 100 Mbit/s 200.000 et les ports 10 Mbit/s 2.000.000. Notez que, même si le style de coût est défini sur RSTP, un port qui migre vers STP verra son coût limité à un maximum de 65535.
RX RSTs	**Synopsis :** 0 à 4294967295 Nombre de messages de configuration RSTP reçus sur ce port.
TX RSTs	**Synopsis :** 0 à 4294967295 Nombre de messages de configuration RSTP transmis sur ce port.
RX Configs	**Synopsis :** 0 à 4294967295 Nombre de messages de configuration STP reçus sur ce port.
TX Configs	**Synopsis :** 0 à 4294967295 Nombre de messages de configuration STP transmis sur ce port.
RX Tcns	**Synopsis :** 0 à 4294967295 Nombre de messages de notification de modification de topologie STP reçus sur ce port. Un nombre excessivement élevé ou croissant rapidement signale des problèmes réseau.
TX Tcns	**Synopsis :** 0 à 4294967295 Nombre de messages de notification de modification de topologie STP transmis sur ce port.
Desig Bridge ID	**Synopsis :** $$ / ##-##-##-##-##-## où $$ a une plage de 0 à 65535 et ## de 0 à FF Bridge Identifier du pont auquel ce port est connecté, fourni sur les ports racine des ponts désignés.
operEdge	**Synopsis :** True ou False Le port fonctionne ou non en tant que port de périphérie.

Section 5.2.9

Gestion de Multiple Spanning Tree Instances

Cette section décrit la configuration et la gestion des MSTI (Multiple Spanning Tree Instances).

SOMMAIRE

- Section 5.2.9.1, « Affichage des statistiques pour des MSTI globales »
- Section 5.2.9.2, « Affichage des statistiques pour des MSTI de ports »
- Section 5.2.9.3, « Configuration de l'identificateur de région MST »
- Section 5.2.9.4, « Configuration d'une MSTI globale »
- Section 5.2.9.5, « Configuration d'une MSTI pour un port Ethernet »

Section 5.2.9.1

Affichage des statistiques pour des MSTI globales

Pour afficher les statistiques pour des MSTI globales, accédez à ***Spanning Tree » View Bridge MSTI Statistics***. Le formulaire **Bridge MSTI Statistics** s'affiche.

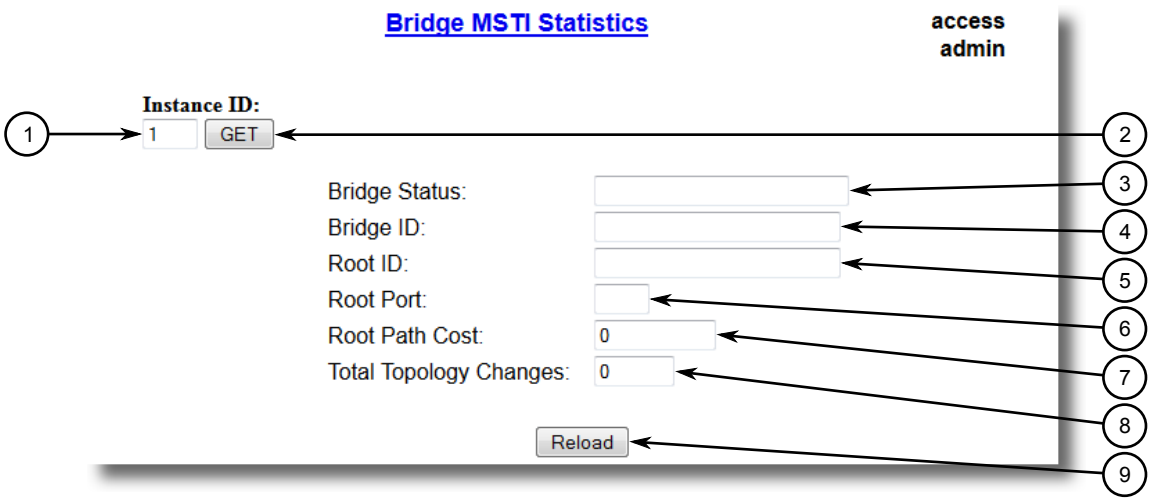


Figure 106 : Formulaire Bridge MSTI Statistics

1. Zone Instance **2.** Bouton Get **3.** Zone Bridge Status **4.** Zone Bridge ID **5.** Zone Root ID **6.** Zone Root Port **7.** Zone Root Path Cost **8.** Zone Total Topology Changes **9.** Bouton Reload

Ce tableau affiche les informations suivantes :

Paramètre	Description
Bridge Status	**Synopsis :** { , Designated Bridge, Not Designated For Any LAN, Root Bridge } État Spanning Tree du pont. L'état peut être racine ou désigné. Ce champ peut indiquer Not Designated For Any LAN pour tout LAN si le pont n'est désigné pour aucun de ses ports.
Bridge ID	**Synopsis :** $$ / ##-##-##-##-##-## où $$ a une plage de 0 à 65535 et ## de 0 à FF Identificateur de ce pont.

Paramètre	Description
Root ID	**Synopsis :** $$ / ##-##-##-##-##-## où $$ a une plage de 0 à 65535 et ## de 0 à FF Identificateur du pont racine.
Port racine	**Synopsis :** 1 au numéro de port maximum ou { <chaîne vide> } Si le pont est désigné, il s'agit du port qui fournit la connectivité au pont racine du réseau.
Root Path Cost	**Synopsis :** 0 à 4294967295 Coût total du chemin au pont racine composé de la somme des coûts de chaque liaison dans le chemin. Si des coûts personnalisés n'ont pas été configurés. Les ports 1 Gbit/s ajoutent 4, les ports 100 Mbit/s ajoutent 19 et les ports 10 Mbit/s ajoutent 100 à ce chiffre. Pour l'instance CIST de MSTP, il s'agit d'un coût de chemin racine externe, qui correspond au coût du chemin du pont racine IST (c'est-à-dire la racine régionale) au pont racine CST (c'est-à-dire la racine réseau "globale").
Total Topology Changes	**Synopsis :** 0 à 65535 Nombre de modifications de topologie dans le réseau, comme détecté sur ce pont via des défaillances de liaison ou signalé depuis d'autres ponts. Un nombre excessivement élevé ou croissant rapidement signale des problèmes réseau.

Section 5.2.9.2

Affichage des statistiques pour des MSTI de ports

Pour afficher les statistiques pour des MSTI de ports, accédez à ***Spanning Tree » View Port MSTI Statistics***. Le formulaire **Port MSTI Statistics** s'affiche.

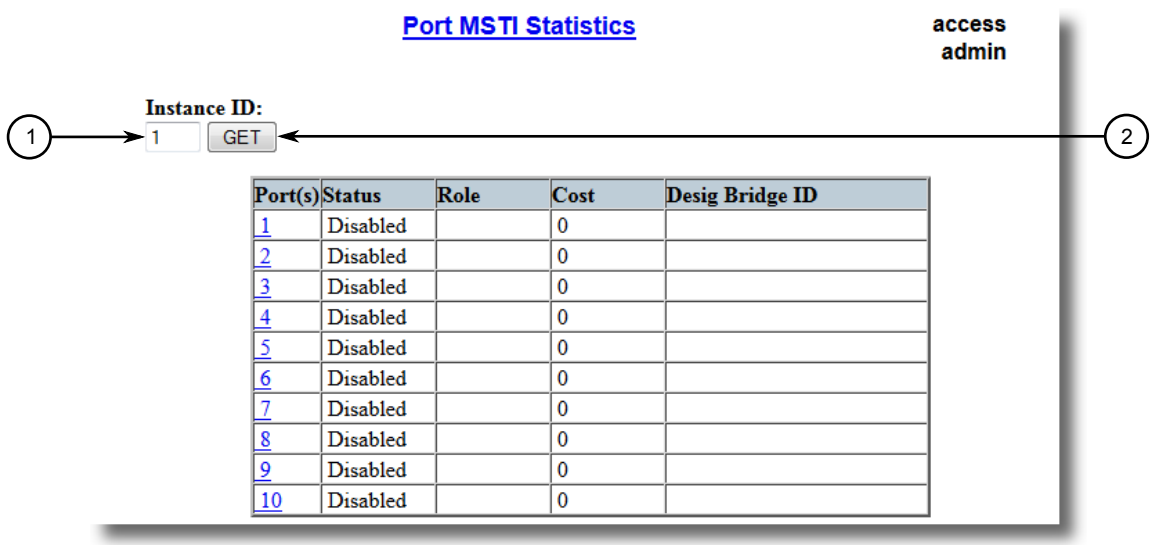


Figure 107 : Formulaire Port MSTI Statistics

1. Zone Instance ID **2.** Bouton Get

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre

Paramètre	Description
	Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
Status	**Synopsis :** { Disabled, Listening, Learning, Forwarding, Blocking, Link Down, Discarding } État de ce port dans le Spanning Tree. Réglages possibles : • **Disabled** - STP est désactivé sur ce port. • **Link Down** - STP est activé sur ce port, mais la liaison désactivée. • **Discarding** - la liaison n'est pas utilisée dans la topologie STP mais est en réserve. • **Learning** - le port apprend les adresses MAC pour éviter une avalanche quand il commence à transmettre le trafic. • **Forwarding** - le port transmet le trafic.
Rôle	**Synopsis :** { , Root, Designated, Alternate, Backup, Master } Rôle de ce port dans le Spanning Tree. Réglages possibles : • **Designated** -le port est désigné pour (c'est-à-dire transfère le trafic vers la racine pour) le LAN auquel il est connecté. • **Root** - le port unique sur le pont, qui fournit la connectivité vers le pont racine. • **Backup** - le port est attaché à un LAN alimenté par un autre port sur le pont. Il n'est pas utilisé mais est en réserve. • **Alternate** - le port est attaché à un pont qui fournit la connectivité au pont racine. Il n'est pas utilisé mais est en réserve. • **Master** - existe uniquement dans le MSTP. Le port est un port limite de région MST et l'unique port sur le pont qui fournit la connectivité pour la Multiple Spanning Tree Instance vers le port racine Common Spanning Tree (c'est-à-dire que ce port est le port racine pour la Common Spanning Tree Instance).
Cost	**Synopsis :** 0 à 4294967295 Coût offert par ce port. Si le style de coût des paramètres Bridge RSTP est défini sur STP, les ports 1 Gbit/s ajoutent 4 au coût, les ports 100 Mbit/s 19 et les ports 10 Mbit/s 100. Si le style de coût est défini sur STP, les ports 1 Gbit/s ajoutent 20.000 au coût, les ports 100 Mbit/s 200.000 et les ports 10 Mbit/s 2.000.000. Notez que, même si le style de coût est défini sur RSTP, un port qui migre vers STP verra son coût limité à un maximum de 65535.
Desig Bridge ID	**Synopsis :** $$ / ##-##-##-##-##-## où $$ a une plage de 0 à 65535 et ## de 0 à FF Bridge Identifier du pont auquel ce port est connecté, fourni sur les ports racine des ponts désignés.

Section 5.2.9.3

Configuration de l'identificateur de région MST

La configuration de l'identificateur de région et du niveau de révision place le pont MSTP dans un groupe défini. D'autres ponts qui ont le même identificateur et le même niveau de révision sont interconnectés au sein de cette région. Pour plus d'informations, voir Section 5.2.3.1, « Régions MSTP et interopérabilité ».

Procédez comme suit pour configurer l'identificateur de région MST (Multiple Spanning Tree) :

1. Accédez à ***Spanning Tree » Configure MST Region Identifier***. Le formulaire **MST Region Identifier** s'affiche.

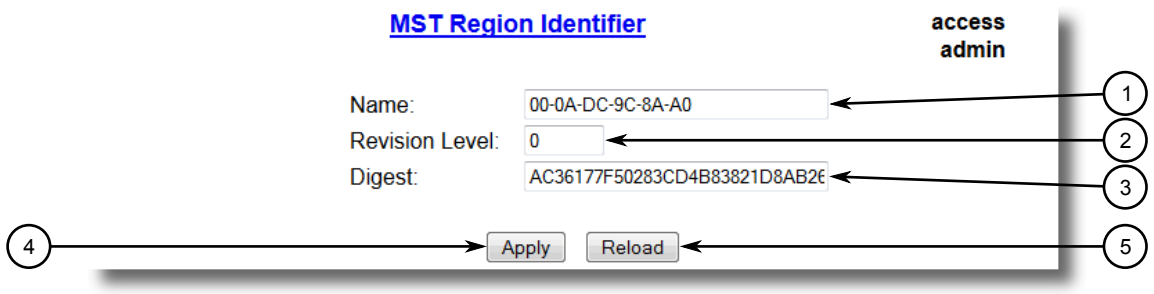


Figure 108 : Formulaire MST Region Identifier

1. Zone Name **2.** Zone Revision Level **3.** Zone Digest **4.** Bouton Apply **5.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Name	**Synopsis :** 32 caractères quelconques **Par défaut :** 00-0A-DC-92-00-00 Nom de la région MST. Tous les appareils dans la même région MST doivent avoir le même nom de région configuré.
Revision Level	**Synopsis :** 0 à 65535 **Par défaut :** 0 Niveau de révision pour la configuration MST. Généralement, tous les appareils dans la même région MST sont configurés avec le même niveau de révision. Cependant, différents niveaux de révision peuvent être utilisés pour créer des sous-régions sous le même nom de région.
Digest	**Synopsis :** 32 caractères quelconques **Par défaut :** 0 Il s'agit d'un paramètre en lecture seule qui doit être utilisé uniquement pour le dépannage du réseau. Pour garantir un mappage VLAN à instance cohérent, il est nécessaire pour le protocole de pouvoir identifier exactement les limites des régions MST. À cet effet, les caractéristiques de la région sont incluses dans les BPDU. Il n'est pas nécessaire de propager le mappage VLAN à instance exact dans les BPDU car les commutateurs ont uniquement besoin de savoir s'ils se trouvent dans la même région que leur voisin. Par conséquent, seul ce digesteur de 16 octets créé avec le mappage VLAN à instance est envoyé aux BPDU.

3. Cliquez sur **Apply**.

Section 5.2.9.4

Configuration d'une MSTI globale

Procédez comme suit pour configurer une MSTI (Multiple Spanning Tree Instance) globale pour le STP (Spanning Tree Protocol) :

1. Accédez à ***Spanning Tree » Configure Bridge MSTI Parameters***. Le formulaire **Bridge MSTI Parameters** s'affiche.

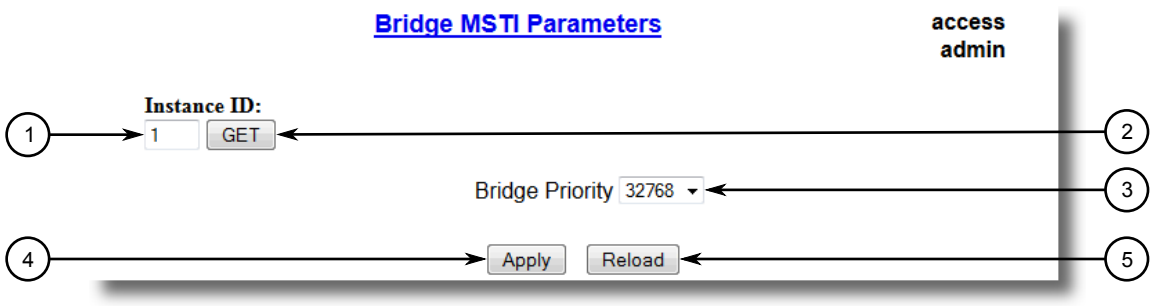


Figure 109 : Formulaire Bridge MSTI Parameters

1. Zone Instance ID **2.** Bouton Get **3.** Liste Bridge Priority **4.** Bouton Apply **5.** Bouton Reload

2. Sous**Instance ID**, saisissez un numéro d'ID pour une MSTI (Multiple Spanning Tree Instance), puis cliquez sur **GET**. Les réglages de la MSTI sont affichés. Toute modification de la configuration est appliquée spécifiquement à cet ID d'instance.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Bridge Priority	**Synopsis :** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Par défaut :** 32768 Bridge Priority (priorité de pont) fournit une manière de contrôler la topologie du réseau connecté via STP. Les points racine et désigné peuvent être configurés pour une topologie spécifique. Le pont avec la priorité la plus basse devient la racine. En cas de défaillance du pont racine, le pont avec la priorité la plus basse suivante devient la racine. Les ponts désignés qui alimentent un LAN commun (à des fins de redondance) utilisent également une priorité pour déterminer le pont actif. De cette manière, une sélection minutieuse des priorités de point peut établir le chemin de flux de trafics dans des conditions normales et anormales.

4. Cliquez sur **Apply**.

Section 5.2.9.5

Configuration d'une MSTI pour un port Ethernet

Procédez comme suit pour configurer une MSTI (Multiple Spanning Tree Instance) pour un port Ethernet :

1. Accédez à ***Spanning Tree » Configure Port MSTI Parameters***. Le tableau **Port MSTI Parameters** s'affiche.

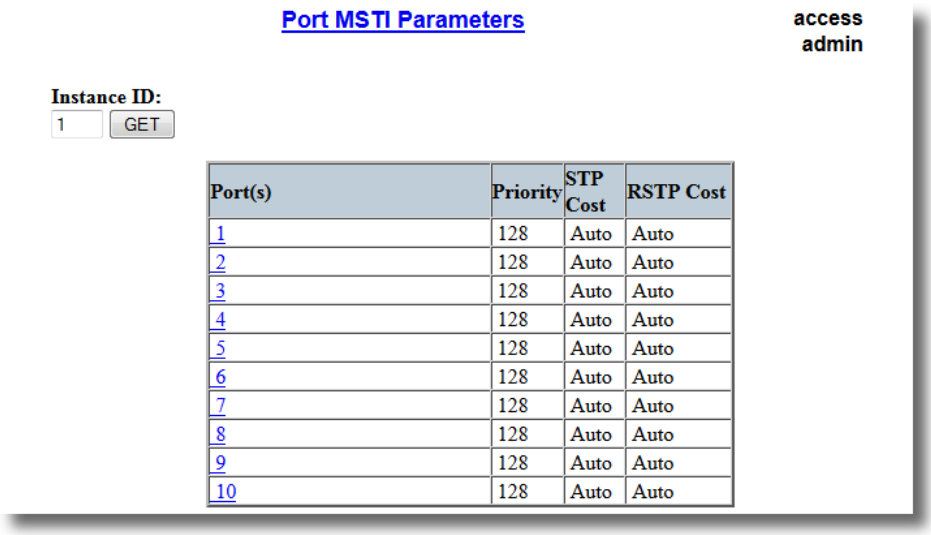


Figure 110 : Tableau Port MSTI Parameters

2. Sélectionnez un port Ethernet. Le formulaire **Port MSTI Parameters** s'affiche.

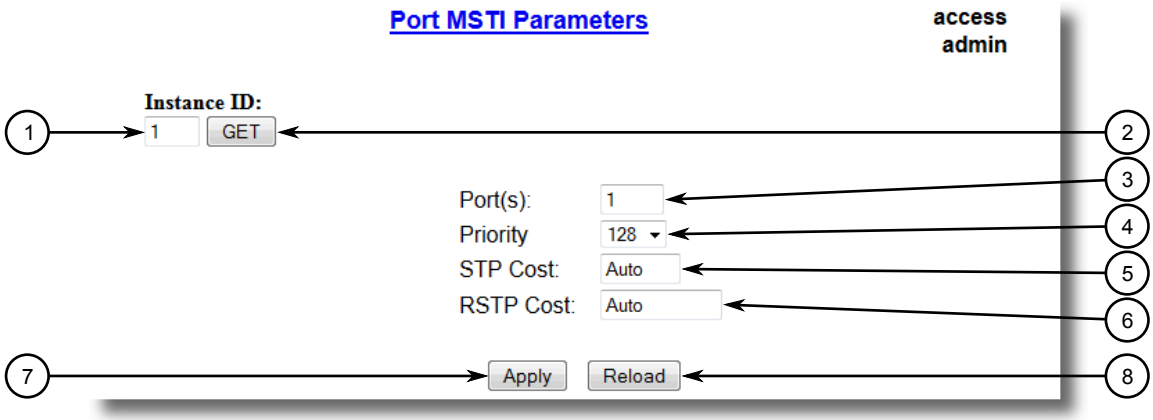


Figure 111 : Formulaire Port MSTI Parameters

1. Zone Instance ID **2.** Bouton Get **3.** Zone Port(s) **4.** Liste Priority **5.** Zone STP Cost **6.** Zone RSTP Cost **7.** Bouton Apply **8.** Bouton Reload

3. Sous**Instance ID**, saisissez un numéro d'ID pour une MSTI (Multiple Spanning Tree Instance), puis cliquez sur **GET**. Les réglages de la MSTI sont affichés. Toute modification de la configuration est appliquée spécifiquement à cet ID d'instance.
4. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).

Paramètre	Description
Priority	**Synopsis :** { 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } **Par défaut :** 128 Sélectionne la priorité du port STP. Les ports ayant le même coût attachés à un LAN commun sélectionnent le port à utiliser en fonction de la priorité.
STP Cost	**Synopsis :** 0 à 65535 ou { Auto } **Par défaut :** Auto Sélectionne le coût à appliquer dans le calcul de coûts lorsque le paramètre Cost Style est défini sur STP dans la configuration des paramètres Bridge RSTP. La définition manuelle du coût fournit la capacité à sélectionner de manière préférentielle des ports spécifiques pour transmettre le trafic à d'autres. Laissez ce champ défini sur "auto" pour utiliser les coûts de port STP standard négociés (4 pour 1 Gbit/s, 19 pour des liaisons 100 Mbit/s et 100 pour des liaisons 10 Mbit/s). Pour MSTP, ce paramètre s'applique au coût de chemin externe et interne.
RSTP Cost	**Synopsis :** 0 à 2147483647 ou { Auto } **Par défaut :** Auto Sélectionne le coût à appliquer dans le calcul de coûts lorsque le paramètre Cost Style est défini sur RSTP dans la configuration des paramètres Bridge RSTP. La définition manuelle du coût fournit la capacité à sélectionner de manière préférentielle des ports spécifiques pour transmettre le trafic à d'autres. Laissez ce champ défini sur "auto" pour utiliser les coûts de port RSTP standard négociés (20 000 pour 1 Gbit/s, 200 000 pour des liaisons 100 Mbit/s et 2 000 000 pour des liaisons 10 Mbit/s). Pour MSTP, ce paramètre s'applique au coût de chemin externe et interne.

5. Cliquez sur **Apply**.

Section 5.2.10

Effacement de statistiques de protocole Spanning Tree

Procédez comme suit pour effacer les statistiques de protocole Spanning Tree :

1. Accédez à ***Spanning Tree » Clear Spanning Tree Statistics***. Le formulaire **Clear Spanning Tree Statistics** s'affiche.

Figure 112 : Formulaire Clear Spanning Tree Statistics

1. Bouton Confirm

2. Cliquez sur **Confirm**.

Section 5.3

Gestion des classes de service

Les classes de service (Classes of Service (CoS)) donnent la possibilité d'expédier la transmission d'un certain trafic de trames et de ports avant d'autres. La CoS d'une trame peut être définie sur Normal, Medium, High, ou Critical. Par défaut, contrairement aux trames de contrôle, RUGGEDCOM ROS applique une CoS normale pour tout trafic entrant reçu sans balise de priorité.

IMPORTANT !
Utilisez la CoS la plus élevée prise en charge avec prudence, car elle est toujours utilisée par le commutateur pour transmettre le trafic de gestion du réseau, notamment les BPDU RSTP.

Si cette CoS est utilisée pour le trafic réseau normal, une perte de cadres de gestion de réseau peut se produire en cas de rafales de trafic, ce qui peut entraîner une perte de la connectivité sur le réseau.

Le processus de contrôle du trafic basé sur la CoS s'effectue en deux phases :

1. **Phase d'inspection**
   Dans la phase d'inspection, la priorité CoS d'une trame reçue est déterminée par l'un des éléments suivants :
   - Une CoS spécifique basée sur les adresses MAC source et de destination (définies dans le tableau Static MAC Address)
   - Le champ de priorité dans les balises IEEE 802.1Q.
   - Le composant Differentiated Services Code Point (DSCP) du champ Type-Of-Service (TOS) de l'en-tête IP si la trame est IP.
   - La CoS du port par défaut.

   Chaque CoS de trame est déterminée une fois que le premier paramètre examiné est trouvé dans la trame.

   REMARQUE
   *Pour plus d'informations sur la manière de configurer le paramètre**Inspect TOS**, voir Section 5.3.2, « Configuration de classes de service pour des ports Ethernet spécifiques ».*

   Les cadres reçus sont d'abord examinés pour déterminer si leur adresse MAC de destination ou source se trouve dans le tableau Static MAC Address. Si c'est le cas, la CoS configurée pour l'adresse MAC statique est utilisée. Si ni l'adresse MAC de destination, ni l'adresse MAC source dans le tableau Static MAC Address, la trame est ensuite examinée pour rechercher des balises 802.1Q et le champ de priorité est mappé sur une CoS. S'il n'existe aucune balise, la trame est examinée pour déterminer s'il s'agit d'une trame IP. Si la trame est une trame IP et**Inspect TOS** est activé dans RUGGEDCOM ROS, la CoS est déterminée dans le champ DSCP. Si la trame n'est pas une frame IP ou si**Inspect TOS** est désactivé, la CoS du port par défaut est utilisée.

   Après inspection, la trame est envoyée au port de sortie pour transmission.

2. **Phase de transmission**
   Une fois que la CoS de la trame est déterminée, la trame est transmise au port de sortie, où elle est collectée dans l'une des files d'attente de priorité en fonction de la CoS affectée.

   La pondération de CoS sélectionne le degré de traitement préférentiel lié à différentes files d'attente de priorité. Le ratio nombre de trames CoS élevées sur nombre de trames CoS basses transmises peut être configuré. Le cas échéant, les trames CoS basses peuvent être transmises uniquement après les trames CoS élevées.

SOMMAIRE

- Section 5.3.1, « Configuration globale de classes de service »
- Section 5.3.2, « Configuration de classes de service pour des ports Ethernet spécifiques »

- Section 5.3.3, « Configuration de la priorité pour le mappage CoS »
- Section 5.3.4, « Configuration du mappage DSCP sur CoS »

Section 5.3.1

Configuration globale de classes de service

Procédez comme suit pour configurer des réglages globaux pour la classe de service (CoS) :

1. Accédez à ***Classes of Service » Configure Global CoS Parameters***. Le formulaire **Global CoS Parameters** s'affiche.

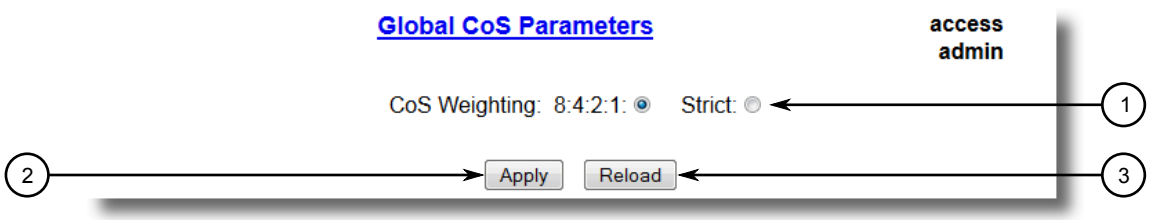


Figure 113 : Formulaire Global CoS Parameters

1. Options CoS Weighting **2.** Bouton Apply **3.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
CoS Weighting	**Synopsis :** { 8:4:2:1, Strict } **Par défaut :** 8:4:2:1 Pendant des rafales de trafic, les trames en attente dans le commutateur d'une transmission vers un port peuvent avoir différentes priorités CoS. Ce paramètre spécifie l'algorithme de pondération pour la transmission de trames CoS à priorités différentes. Exemples : • 8:4:2:1 - trame CoS à priorité 8 Critical, 4 High, 2 Medium et 1 Normal • Strict - les trames CoS à priorité basse ne sont transmises qu'une fois toutes les trames CoS à priorité plus élevées transmises.

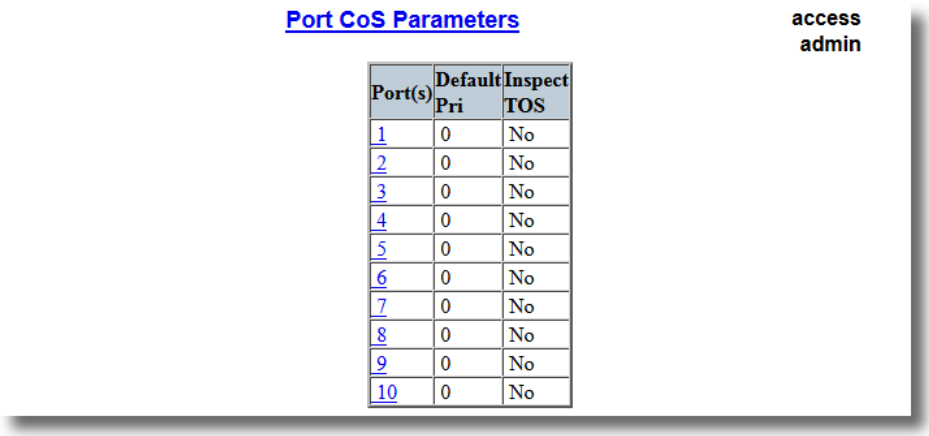
3. Cliquez sur **Apply**.
4. Si nécessaire, configurez le mappage CoS sur la base du champ IEEE 802.1p priority ou Differentiated Services (DS) défini dans l'en-tête IP pour chaque paquet. Pour plus d'informations, voir Section 5.3.3, « Configuration de la priorité pour le mappage CoS » ou Section 5.3.4, « Configuration du mappage DSCP sur CoS ».

Section 5.3.2

Configuration de classes de service pour des ports Ethernet spécifiques

Procédez comme suit pour configurer une classe de service (CoS) pour un ou plusieurs ports Ethernet :

1. Accédez à ***Classes of Service » Configure Port CoS Parameters***. Le tableau **Port CoS Parameters** s'affiche.



Port(s)	Default Pri	Inspect TOS
1	0	No
2	0	No
3	0	No
4	0	No
5	0	No
6	0	No
7	0	No
8	0	No
9	0	No
10	0	No

Figure 114 : Tableau Port CoS Parameters

2. Sélectionnez un port Ethernet. Le formulaire **Port CoS Parameters** s'affiche.

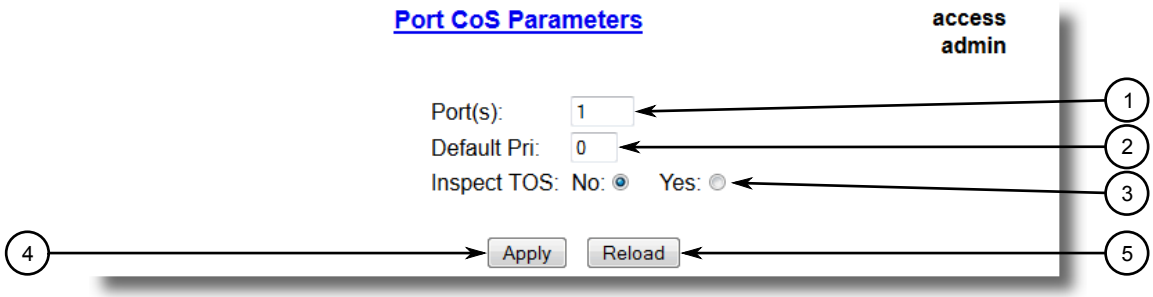


Figure 115 : Formulaire Port CoS Parameters

1. Zone Port(s) **2.** Zone Default Pri **3.** Options Inspect TOS **4.** Bouton Apply **5.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
Default Pri	**Synopsis :** 0 à 7 **Par défaut :** 0 Ce paramètre permet de prioriser les trames reçues sur ce port qui ne sont pas priorisées sur la base de leur contenu (par exemple, le champ de priorité dans la balise VLAN, le champ DiffServ dans l'en-tête IP, adresse MAC priorisée).
Inspect TOS	**Synopsis :** { No, Yes } **Par défaut :** No Ce paramètre active ou désactive le champ Type-Of-Service (TOS, type de service) dans l'en-tête IP des trames reçues pour déterminer la classe de service qui doit leur être affectée. Lorsque l'analyse TOS est activée, le commutateur utilise les bites de services différenties dans le champ TOS.

4. Cliquez sur **Apply**.

Section 5.3.3

Configuration de la priorité pour le mappage CoS

Une classe de service peut être automatiquement affectée aux trames reçues non balisées sur la base de leur niveau de priorité.

Procédez comme suit pour mapper un niveau de priorité sur une classe de service :

1. Accédez à ***Classes of Service » Configure Priority to CoS Mapping***. Le tableau **Priority to CoS Mapping** s'affiche.

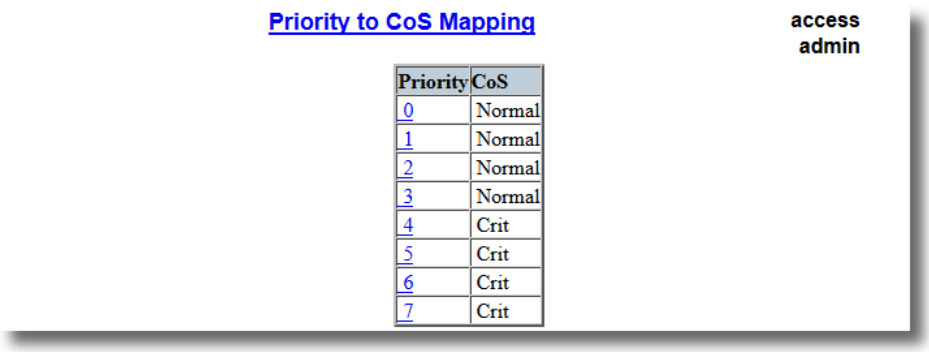


Figure 116 : Tableau Priority to CoS Mapping

2. Sélectionnez un niveau de priorité. Le formulaire **Priority to CoS Mapping** s'affiche.

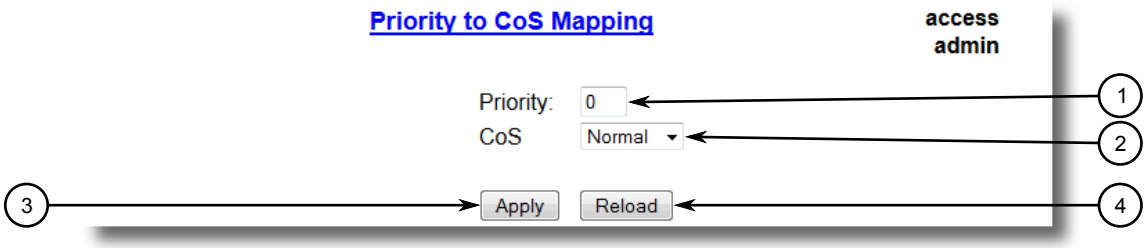


Figure 117 : Formulaire Priority to CoS Mapping

1. Zone Priority **2.** Liste CoS **3.** Bouton Apply **4.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Priority	**Synopsis :** 0 à 7 **Par défaut :** 0 Va de la priorité IEEE 802.1p.
CoS	**Synopsis :** { Normal, Medium, High, Crit } **Par défaut :** Normal

Paramètre	Description
	CoS affectée de manière à recevoir les trames balisées reçues avec la valeur de priorité IEEE 802.1p spécifiée.

4. Cliquez sur **Apply**.

Section 5.3.4

Configuration du mappage DSCP sur CoS

Le mappage de CoS sur le champ Differentiated Services (DS) défini dans l'en-tête IP pour chaque paquet est réalisé en définissant les Differentiated Services Code Points (DSCPs) dans la configuration CoS.

Procédez comme suit pour mapper un DSCP sur une classe de service :

1. Accédez à ***Classes of Service » Configure DSCP to CoS Mapping***. Le tableau **DSCP to CoS Mapping** s'affiche.

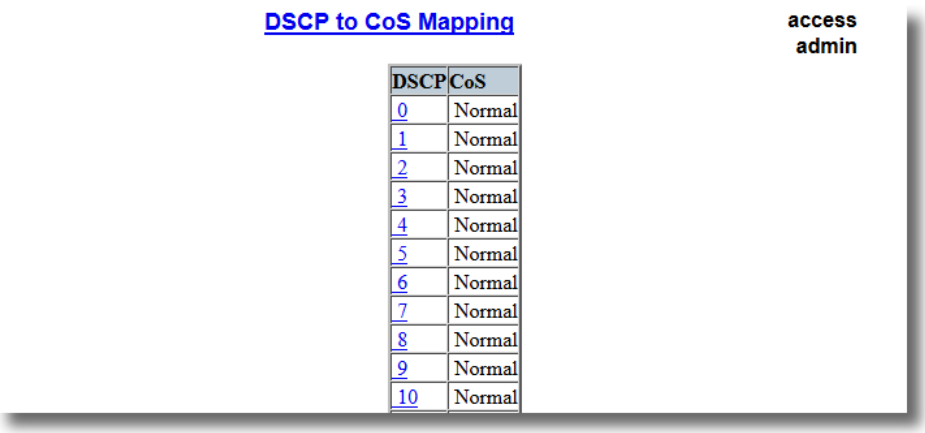


Figure 118 : Tableau DSCP to CoS Mapping

2. Sélectionnez un niveau DSCP. Le formulaire **DSCP to CoS Mapping** s'affiche.

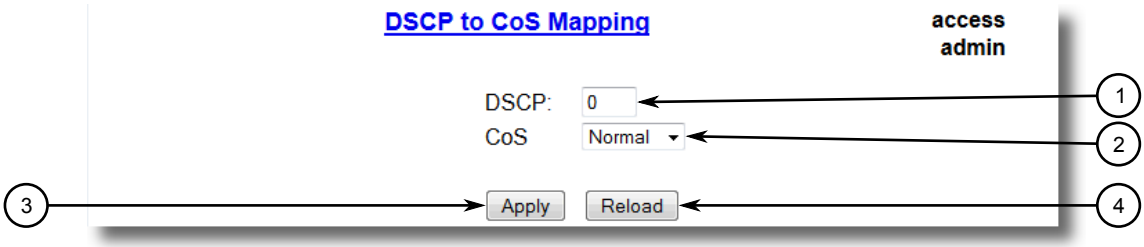


Figure 119 : Formulaire DSCP to CoS Mapping

1. Zone DSCP **2.** Liste CoS **3.** Bouton Apply **4.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
DSCP	**Synopsis :** 0 à 63 **Par défaut :** 0 Differentiated Services Code Point (DSCP) - valeur du champ DiffServ 6 bits dans le champ Type-Of-Service (TOS) de l'en-tête IP.
CoS	**Synopsis :** { Normal, Medium, High, Crit } **Par défaut :** Normal Classe de service affectée pour recevoir les trames reçues avec la valeur DSCP spécifiée.

4. Cliquez sur **Apply**.
5. Configurez les paramètres CoS sur les ports Ethernet commutés en fonction de vos besoins. Pour plus d'informations, voir Section 5.3.2, « Configuration de classes de service pour des ports Ethernet spécifiques ».

Section 5.4

Gestion des adresses MAC

Cette section décrit la manière de gérer des adresses MAC.

SOMMAIRE

- Section 5.4.1, « Affichage d'une liste d'adresses MAC »
- Section 5.4.2, « Configuration des options d'apprentissage d'adresses MAC »
- Section 5.4.3, « Configuration des options d'avalanche d'adresses MAC »
- Section 5.4.4, « Gestion des adresses MAC statiques »
- Section 5.4.5, « Purge de toutes les adresses MAC dynamiques »

Section 5.4.1

Affichage d'une liste d'adresses MAC

Pour afficher une liste de toutes les adresses MAC statiques et apprises de manière dynamique, accédez à ***MAC Address Tables » View MAC Addresses***. Le tableau **MAC Addresses** s'affiche.

MAC Addresses

access
admin

MAC Address	VID	Port	Type	CoS
00-01-6C-4A-60-1A	1	8	Dynamic	N/A
00-01-C0-0B-B8-42	1	8	Dynamic	N/A
00-01-C0-0C-0B-B7	1	8	Dynamic	N/A
00-06-B5-64-92-75	1	8	Dynamic	N/A
00-0A-DC-00-1E-CA	1	8	Dynamic	N/A
00-0A-DC-11-33-40	1	8	Dynamic	N/A
00-0A-DC-2D-A6-E3	1	8	Dynamic	N/A
00-0A-DC-E5-86-FF	1	8	Dynamic	N/A
00-0A-DC-E5-A4-FF	1	8	Dynamic	N/A
00-0A-DC-F1-7A-FF	1	8	Dynamic	N/A
00-0A-DC-F1-7B-FF	1	8	Dynamic	N/A
00-0A-DC-F1-84-FD	1	8	Dynamic	N/A
00-0A-DC-F1-8C-FD	1	8	Dynamic	N/A
00-0A-DC-F1-D7-FF	1	8	Dynamic	N/A
00-0A-DC-F3-5D-FF	1	8	Dynamic	N/A

Figure 120 : Tableau MAC Address

Procédez comme suit si aucune adresse MAC n'est répertoriée :

1. Configurez les options d'apprentissage d'adresses MAC pour contrôler le vieillissement d'adresses MAC apprises de manière dynamique ou d'autres appareils sur le réseau. Pour plus d'informations, voir Section 5.4.2, « Configuration des options d'apprentissage d'adresses MAC ».
2. Configurez l'adresse sur l'appareil en tant qu'adresse MAC statique. Pour plus d'informations, voir Section 5.4.4.2, « Ajout d'une adresse MAC statique ».

Section 5.4.2

Configuration des options d'apprentissage d'adresses MAC

Les options d'apprentissage d'adresses MAC contrôlent comment et quand les adresses MAC sont automatiquement supprimées du tableau MAC Address. Les destinataires individuels sont supprimés lorsque la temporisation de vieillissement est dépassée. Les adresses peuvent également être supprimées en cas de défaillance de liaison ou de modifications de la topologie.

Procédez comme suit pour configurer les options d'apprentissage d'adresses MAC :

1. Accédez à ***MAC Address Tables » Configure MAC Address Learning Options***. Le formulaire **MAC Address Learning Options** s'affiche.

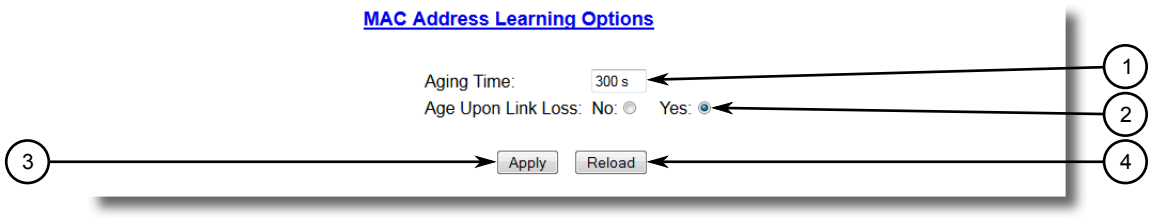


Figure 121 : Formulaire MAC Address Learning Options

1. Zone Aging Time **2.** Options Age Upon Link Loss **3.** Bouton Apply **4.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Aging Time	**Synopsis :** 15 à 800 **Par défaut :** 300 s Ce paramètre configure le temps pendant lequel une adresse MAC apprise est en attente avant d'atteindre la limite de vieillissement.
Age Upon Link Loss	**Synopsis :** { No, Yes } **Par défaut :** Oui Si ce paramètre est défini sur Yes, toutes les adresses MAC apprises sur un port défaillant sont immédiatement exclues en cas de détection de défaillance de liaison. Lorsqu'une défaillance de liaison se produit, le commutateur peut avoir des adresses MAC apprises auparavant sur le port défaillant. Tant que ces adresses n'ont pas dépassé la limite de vieillissement, le commutateur continue à transmette le trafic vers ce port, empêchant ainsi que ce trafic n'atteigne sa destination via la nouvelle topologie de réseau. Notez que, lorsqu'un protocole de redondance réseau comme RSTP/MSTP est activé sur le commutateur, ce protocole de redondance peut, en cas de défaillance de liaison, vider les adresses MAC apprises sur le port défaillant quel que soit le réglage de ce paramètre.

3. Cliquez sur **Apply**.

Section 5.4.3

Configuration des options d'avalanche d'adresses MAC

Procédez comme suit pour configurer les options d'avalanche d'adresses MAC :

1. Accédez à ***MAC Address Tables » Configure MAC Address Flooding Options***. Le tableau **Flooding Options** s'affiche.

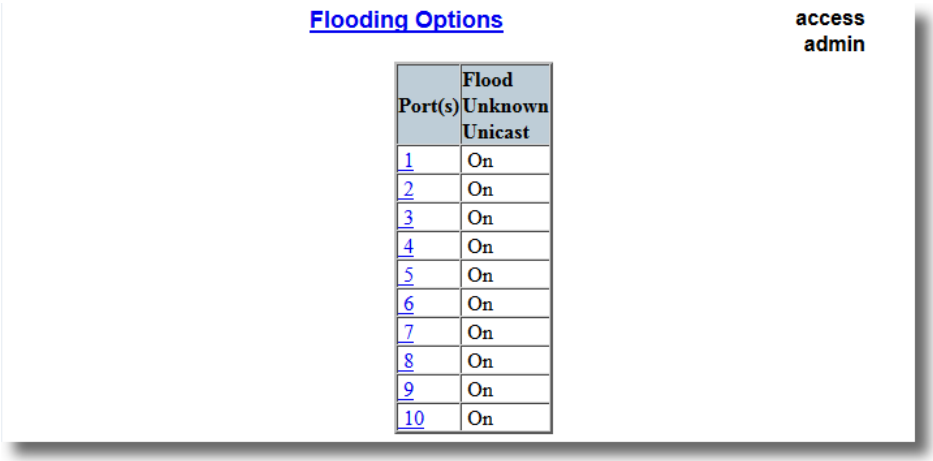


Figure 122 : Tableau Flooding Options

2. Sélectionnez un port. Le formulaire **Flooding Options** s'affiche.

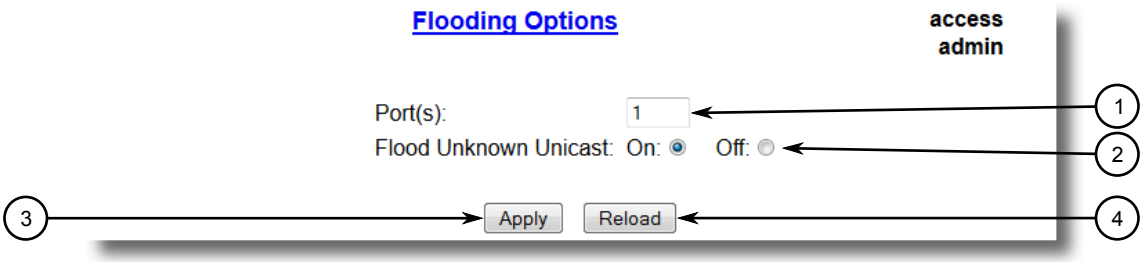


Figure 123 : Formulaire Flooding Options

1. Zone Port(s) **2.** Options Flood Unknown Unicast **3.** Bouton Apply **4.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port(s)	**Synopsis :** Liste de ports séparée par des virgules Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
Flood Unknown Unicast	**Synopsis :** { On, Off } **Par défaut :** On Normalement, le trafic monodiffusion avec une adresse de destination inconnue s'écoule depuis tous les ports. Lorsqu'un port est configuré de manière à désactiver ce genre d'avalanche, le trafic monodiffusion inconnu n'est pas envoyé depuis le port sélectionné.

4. Cliquez sur **Apply**.

Section 5.4.4

Gestion des adresses MAC statiques

Les adresses MAC statiques doivent être configurées lorsque l'appareil est uniquement en mesure de recevoir des trames et pas de les transmettre. Elles peuvent également devoir être configurées si la sécurité du port (si elle est prise en charge) doit être mise en œuvre.

Les adresses MAC priorisées sont configurées lorsqu'une priorité CoS supérieure à celle d'autres appareils doit être affectée au trafic vers ou issu d'un appareil spécifique sur un segment de LAN.

REMARQUE
Une adresse MAC ne peut pas être apprise sur un VLAN qui n'a pas été configuré dans le tableau Static VLAN. Si une trame avec une balise de VLAN inconnue arrive sur un port sécurisé, cela est considéré comme une violation de sécurité et RUGGEDCOM ROS génère une alarme de sécurité de port.

SOMMAIRE

- Section 5.4.4.1, « Affichage d'une liste d'adresses MAC statiques »
- Section 5.4.4.2, « Ajout d'une adresse MAC statique »
- Section 5.4.4.3, « Suppression d'une adresse MAC statique »

Section 5.4.4.1

Affichage d'une liste d'adresses MAC statiques

Pour afficher une liste d'adresses MAC statiques configurées sur l'appareil, accédez à ***MAC Address Tables » Configure Static MAC Addresses***. Le tableau **Static MAC Addresses** s'affiche.

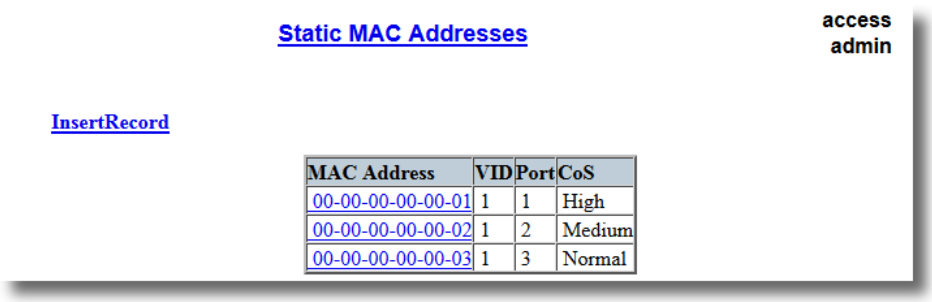


Figure 124 : Tableau Static MAC Addresses

Si aucune adresse MAC statique n'a été configurée, ajoutez des adresses en fonction de vos besoins. Pour plus d'informations, voir Section 5.4.4.2, « Ajout d'une adresse MAC statique ».

Section 5.4.4.2

Ajout d'une adresse MAC statique

Procédez comme suit pour ajouter une adresse MAC statique au tableau Static MAC Address :

1. Accédez à ***MAC Address Tables » Configure Static MAC Addresses***. Le tableau **Static MAC Addresses** s'affiche.

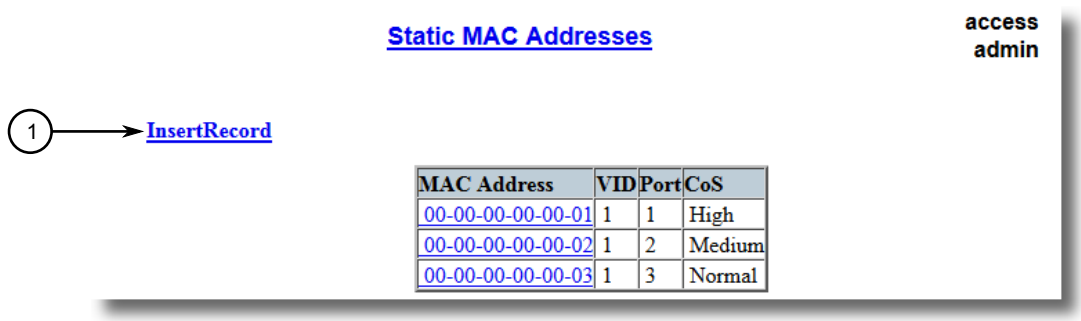


Figure 125 : Tableau Static MAC Addresses

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **Static MAC Addresses** s'affiche.

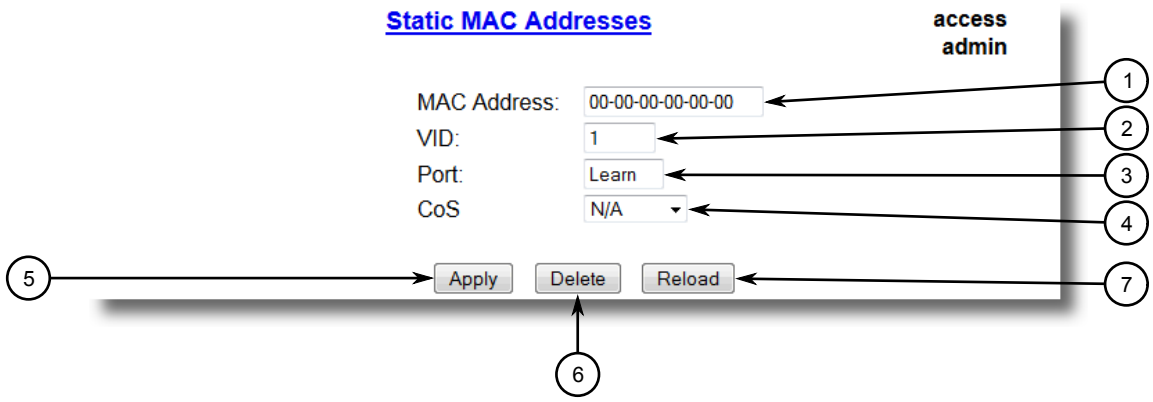


Figure 126 : Formulaire Static MAC Addresses

1. Zone MAC Address **2.** Zone VID **3.** Zone Port **4.** Liste CoS **5.** Bouton Apply **6.** Bouton Delete **7.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
MAC Address	**Synopsis :** ##-##-##-##-##-## avec une plage de 0 à FF pour ## Adresse MAC apprise par le commutateur. 6 caractères génériques peuvent être utilisés au maximum pour spécifier une plage d'adresses MAC pouvant être apprise par le module de sécurité du port (lorsque la sécurité du port est définie sur le mode 'Static MAC'). Les caractères génériques démarrent de la droite et sont continus. Exemples : • *00-0A-DC-**-**-** signifie l'espace d'adresses MAC complet de RuggedCom. • *00-0A-DC-12-3*-** signifie la plage 00-0A-DC-12-30-00 à 00-0A-DC-12-3F-FF.
VID	**Synopsis :** 1 à 4094 ou { ANY } **Par défaut :** 1 Identificateur VLAN du VLAN sur la base duquel l'adresse MAC est exécutée.

Paramètre	Description
	L'option ANY permet l'apprentissage d'une adresse MAC via le module de sécurité du port sur tout VLAN configuré sur le commutateur.
Port	**Synopsis :** 1 au numéro de port maximum ou { Learn } **Par défaut :** Learn Saisissez le numéro de port dans lequel l'appareil avec cette adresse est situé. Le mode de sécurité du port sélectionné ne doit pas être '802.1X'. Si le port doit être appris automatiquement, définissez ce paramètre sur 'Learn'. L'option 'Learn' est applicable pour la sécurité du port en mode 'Static MAC'.
CoS	**Synopsis :** { N/A, Normal, Medium, High, Crit } **Par défaut :** N/A Priorise le trafic pour l'adresse MAC spécifiée. Si le trafic ne doit pas être priorisé sur la base de l'adresse, sélectionnez N/A.

4. Cliquez sur **Apply**.

Section 5.4.4.3

Suppression d'une adresse MAC statique

Procédez comme suit pour supprimer une adresse MAC statique du tableau Static MAC Address :

1. Accédez à ***MAC Address Tables » Configure Static MAC Addresses***. Le tableau **Static MAC Addresses** s'affiche.

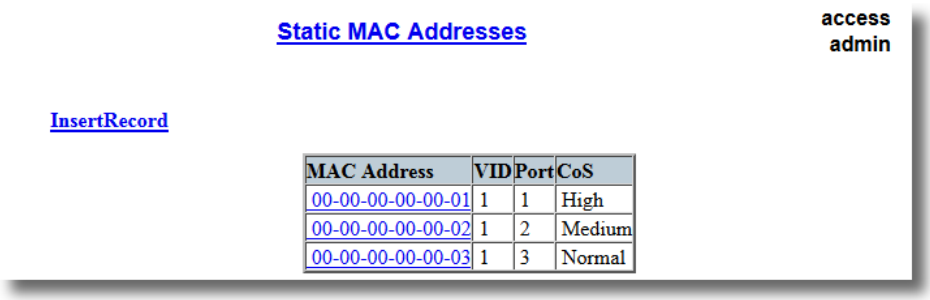


Figure 127 : Tableau Static MAC Addresses

2. Sélectionnez l'adresse MAC dans le tableau. Le formulaire **Static MAC Addresses** s'affiche.

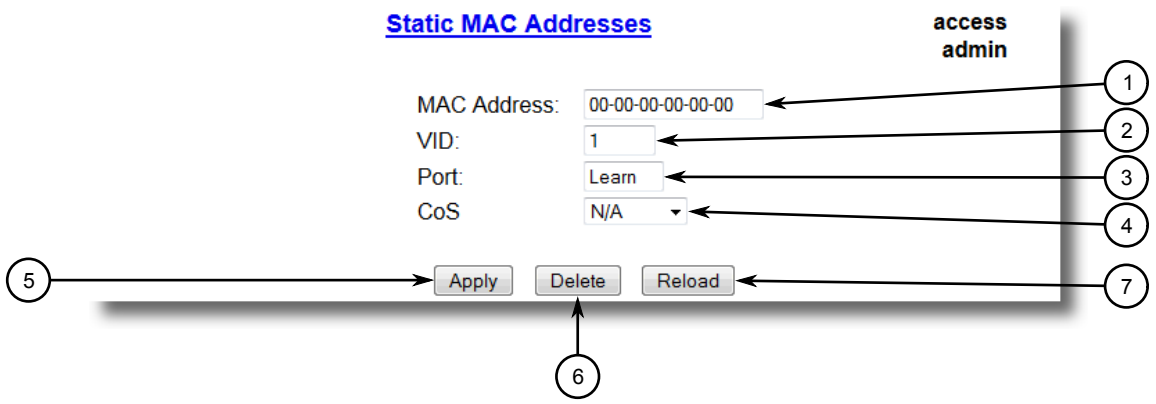


Figure 128 : Formulaire Static MAC Addresses

1. Zone MAC Address **2.** Zone VID **3.** Zone Port **4.** Liste CoS **5.** Bouton Apply **6.** Bouton Delete **7.** Bouton Reload

3. Cliquez sur **Delete**.

Section 5.4.5

Purge de toutes les adresses MAC dynamiques

Procédez comme suit pour vider la liste d'adresses MAC dynamiques de toutes ses entrées :

1. Accédez à ***MAC Address Tables » Purge MAC Address Table***. Le formulaire **Purge MAC Address Table** s'affiche.

Figure 129 : Formulaire Purge MAC Address Table

1. Bouton Confirm

2. Cliquez sur **Confirm**.

Section 5.5

Gestion des services de temps

Le System Time Manager offre les fonctionnalités suivantes de chronométrage et de synchronisation d'horloge

- Chronométrage matériel local et gestion des fuseaux horaires

- Client et serveur SNTP (Simple Network Time Protocol)

SOMMAIRE

- Section 5.5.1, « Configuration de la date et de l'heure »
- Section 5.5.2, « Gestion de NTP »

Section 5.5.1

Configuration de la date et de l'heure

Procédez comme suit pour définir la date, l'heure et d'autres paramètres relatifs à la comptabilisation du temps

1. Accédez à ***Administration » System Time Manager » Configure Time and Date***. Le formulaire **Time and Date** s'affiche.

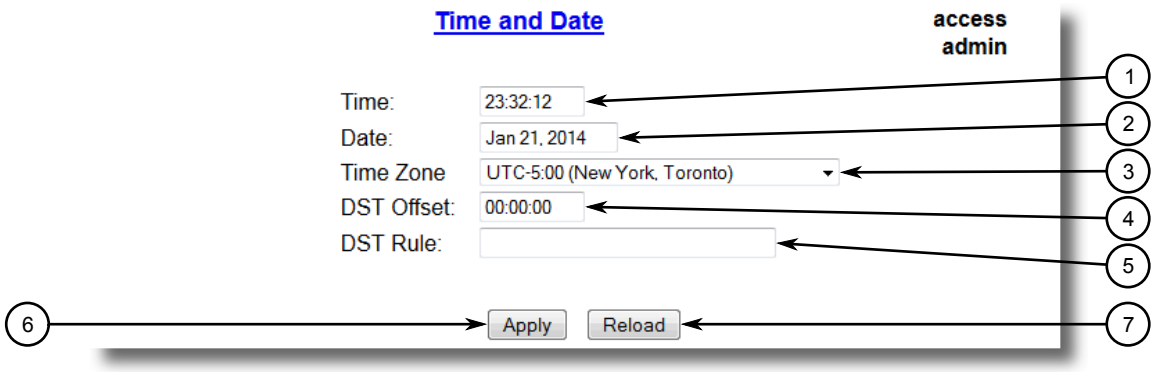


Figure 130 : Formulaire Time and Date

1. Time **2.** Date **3.** Time Zone **4.** DST Offset **5.** DST Rule **6.** Bouton Apply **7.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Time	**Synopsis :** HH:MM:SS Ce paramètre permet l'affichage et le réglage de l'heure locale.
Date	**Synopsis :** MMM JJ, AAAA Ce paramètre permet l'affichage et le réglage de la date locale.
Time Zone	**Synopsis :** { UTC-12:00 (Eniwetok, Kwajalein), UTC-11:00 (Midway Island, Samoa), UTC-10:00 (Hawaii), UTC-9:00 (Alaska), UTC-8:00 (Los Angeles, Vancouver), UTC-7:00 (Calgary, Denver), UTC-6:00 (Chicago, Mexico City), UTC-5:00 (New York, Toronto), UTC-4:30 (Caracas), UTC-4:00 (Santiago), UTC-3:30 (Newfoundland), UTC-3:00 (Brasilia, Buenos Aires), UTC-2:00 (Mid Atlantic), UTC-1:00 (Azores), UTC-0:00 (Lisbon, London), UTC+1:00 (Berlin, Paris, Rome), ... } **Par défaut :** UTC-5:00 (New York, Toronto) Ce réglage permet la conversion de l'UTC (Universal Coordinated Time) en heure locale.
DST Offset	**Synopsis :** HH:MM:SS **Par défaut :** 00:00:00 Ce paramètre spécifie la durée à avancer/reculer lorsque DTS (heure d'été/hiver) démarre ou s'arrête. Par exemple, sur la plupart du territoire des USA et du Canada, le décalage

Paramètre	Description
	de l'heure DST (heure d'été/hiver) est 1 heure (01:00:00) vers l'avant lorsque l'heure DST commence et 1 heure vers l'arrière lorsque DST se termine.
DST Rule	**Synopsis :** mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS Ce paramètre spécifie une règle pour l'heure et la date au moment de la transition entre l'heure standard et l'heure DST (heure d'été/hiver). • mm - mois de l'année (01 - janvier, 12 - décembre) • n - nième jour du mois (1 - 1er jour, 5 - 5ème/dernier jour) • d - jour de la semaine (0 - dimanche, 6 - samedi) • HH - heure du jour (0 - 24) • MM - minutes de l'heure (0 - 59) • SS - secondes de la minute (0 - 59) Exemple : la règle suivante s'applique sur la plupart du territoire des USA et du Canada : `03.2.0/02:00:00 11.1.0/02:00:00` Le DST commence le 2ème dimanche de mars à 2:00 du matin. Le DST se termine le 1er dimanche de novembre à 2:00 du matin.

Section 5.5.2

Gestion de NTP

RUGGEDCOM ROS peut être configuré de manière à se référer périodiquement à un serveur NTP spécifié pour corriger le décalage dans l'horloge intégrée. RUGGEDCOM ROS indique également l'heure via le SNTP (Simple Network Time Protocol) à des hôtes qui la demandent.

Deux serveurs NTP (principal et de sauvegarde) peuvent être configurés pour l'appareil. Le serveur principal est contacté en premier pour chaque tentative de mise à jour de l'heure système. Si le serveur principal ne répond pas, le serveur de sauvegarde est contacté. Si ni le serveur principal ni le serveur de sauvegarde ne répond, une alarme est générée.

SOMMAIRE

• Section 5.5.2.1, « Activation/désactivation du service NTP »
• Section 5.5.2.2, « Configuration de serveurs NTP »

Section 5.5.2.1

Activation/désactivation du service NTP

Procédez comme suit pour activer ou désactiver le service NTP :

REMARQUE
Si l'appareil est exécuté comme serveur NTP, le service NTP doit être activé.

1. Accédez à ***Administration » System Time Manager » Configure NTP » Configure NTP Service***. Le formulaire **SNTP Parameters** s'affiche.

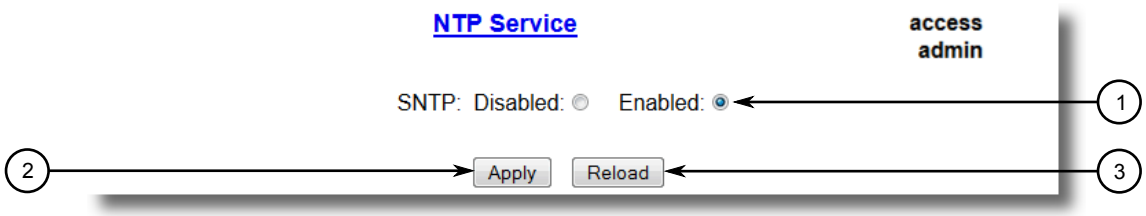


Figure 131 : Formulaire SNTP Parameters

1. Options SNTP **2.** Bouton Apply **3.** Bouton Reload

2. Sélectionnez**Enabled** pour activer SNTP ou**Disabled** pour désactiver SNTP.
3. Cliquez sur **Apply**.

Section 5.5.2.2

Configuration de serveurs NTP

Procédez comme suit pour configurer le serveur NTP principal (Primary) ou de sauvegarde (backup) :

1. Accédez à ***Administration » System Time Manager » Configure NTP » Configure NTP Servers***. Le tableau **NTP Servers** s'affiche.

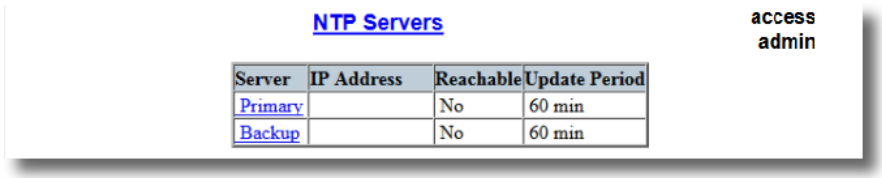


Figure 132 : Tableau NTP Servers

2. Sélectionnez**Primary** ou**Backup**. Le formulaire **NTP Servers** s'affiche.

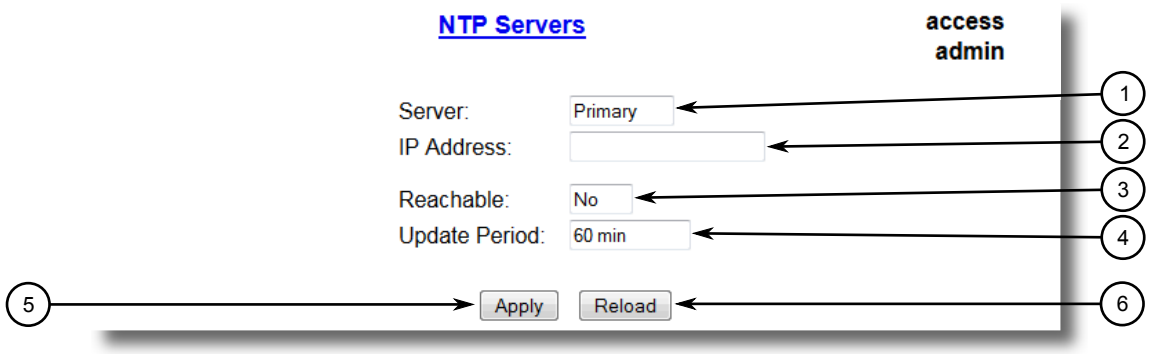


Figure 133 : Formulaire NTP Servers

1. Zone Server **2.** Zone IP Address **3.** Zone Reachable **4.** Zone Update Period **5.** Bouton Apply **6.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Server	**Synopsis :** 8 caractères quelconques **Par défaut :** Primary Ce champ indique si cette configuration est valable pour un serveur principal ou de sauvegarde.
IP Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### L'adresse IP du serveur.
Reachable	**Synopsis :** { No, Yes } Indique l'état du serveur.
Update Period	**Synopsis :** 1 à 1440 min **Par défaut :** 60 min Détermine la fréquence de l'interrogation du serveur (S)NTP pour une mise à jour de l'heure. Une alarme est générée si le serveur n'est pas accessible après trois tentatives effectuées à une minute d'intervalle.

4. Cliquez sur **Apply**.

Section 5.6

Gestion de SNMP

RUGGEDCOM ROS prend en charge les versions 1, 2 et 3 du SNMP (Simple Network Management Protocol), généralement appelées respectivement SNMPv1, SNMPv2c et SNMPv3. SNMPv3 fournit un accès sécurisé à des appareils via une combinaison de processus d'authentification et de chiffrement de paquets dans le réseau. Les fonctionnalités de sécurité pour ce protocole sont entre autres :

Fonctionnalité	Description
Intégrité des messages	S'assure qu'un paquet n'a pas été modifié au cours du transit.
Authentification	Détermine si le message provient d'une source valide.
Chiffrement	Chiffre le contenu d'un paquet afin d'éviter qu'il ne soit visible par une source non autorisée.

SNMPv3 fournit des modèles et des niveaux de sécurité. Un modèle de sécurité est une configuration de stratégie d'authentification pour un utilisateur et le groupe dans lequel il se trouve. Un niveau de sécurité est un niveau de sécurité autorisé au sein d'un modèle de sécurité. Une combinaison de modèle et de niveau de sécurité détermine le mécanisme de sécurité employé lors du traitement d'un paquet SNMP.

Avant de configurer SNMPv3, tenez compte des points suivants :

- Chaque utilisateur appartient à un groupe
- Un groupe définit la stratégie d'accès pour un ensemble d'utilisateurs
- Une stratégie d'accès définit les objets SNMP auxquels il est possible d'accéder (notamment lecture, écriture et création de notifications)
- Un groupe détermine la liste de notifications que ses utilisateurs peuvent recevoir
- Un groupe définit également le modèle et le niveau de sécurité pour ses utilisateurs

Une chaîne de communauté peut être configurée pour SNMPv1 et SNMPv2c. La chaîne est mappée sur le groupe et le niveau d'accès avec un nom de sécurité configuré en tant que**User Name**.

SOMMAIRE

- Section 5.6.1, « Gestion des utilisateurs SNMP »
- Section 5.6.2, « Gestion du mappage sécurité sur groupe »
- Section 5.6.3, « Gestion de groupes SNMP »

Section 5.6.1

Gestion des utilisateurs SNMP

Cette section décrit la manière de gérer les utilisateurs SNMP.

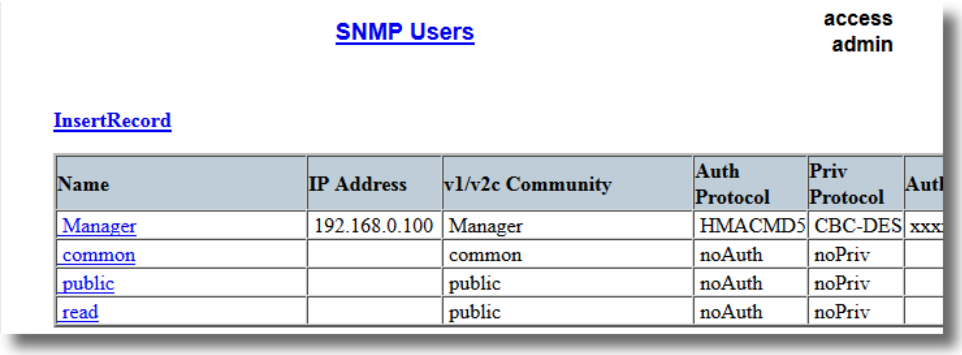
SOMMAIRE

- Section 5.6.1.1, « Affichage d'une liste d'utilisateurs SNMP »
- Section 5.6.1.2, « Ajout d'un utilisateur SNMP »
- Section 5.6.1.3, « Suppression d'un utilisateur SNMP »

Section 5.6.1.1

Affichage d'une liste d'utilisateurs SNMP

Pour afficher une liste d'utilisateurs SNMP configurés sur l'appareil, accédez à ***Administration » Configure SNMP » Configure SNMP Users***. Le tableau **SNMP Users** s'affiche.



Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 134 : Tableau SNMP Users

Si aucun utilisateur n'a été configuré, ajoutez des utilisateurs en fonction de vos besoins. Pour plus d'informations, voir Section 5.6.1.2, « Ajout d'un utilisateur SNMP ».

Section 5.6.1.2

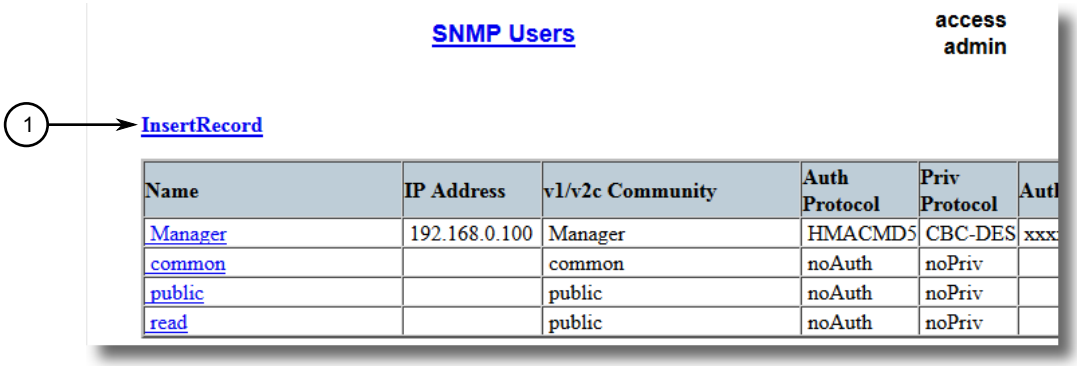
Ajout d'un utilisateur SNMP

Plusieurs utilisateurs (32 max.) peuvent être configurés pour le moteur SNMPv3 local, ainsi que pour les communités SNMPv1 et SNMPv2c.

REMARQUE
*En cas d'activation du niveau de sécurité SNMPv1 ou SNMPv2c, le paramètre**User Name** mappe le nom de communauté sur le groupe de sécurité et le niveau d'accès.*

Procédez comme suit pour ajouter un nouvel utilisateur SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Users***. Le tableau **SNMP Users** s'affiche.



Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 135 : Tableau SNMP Users

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **SNMP Users** s'affiche.

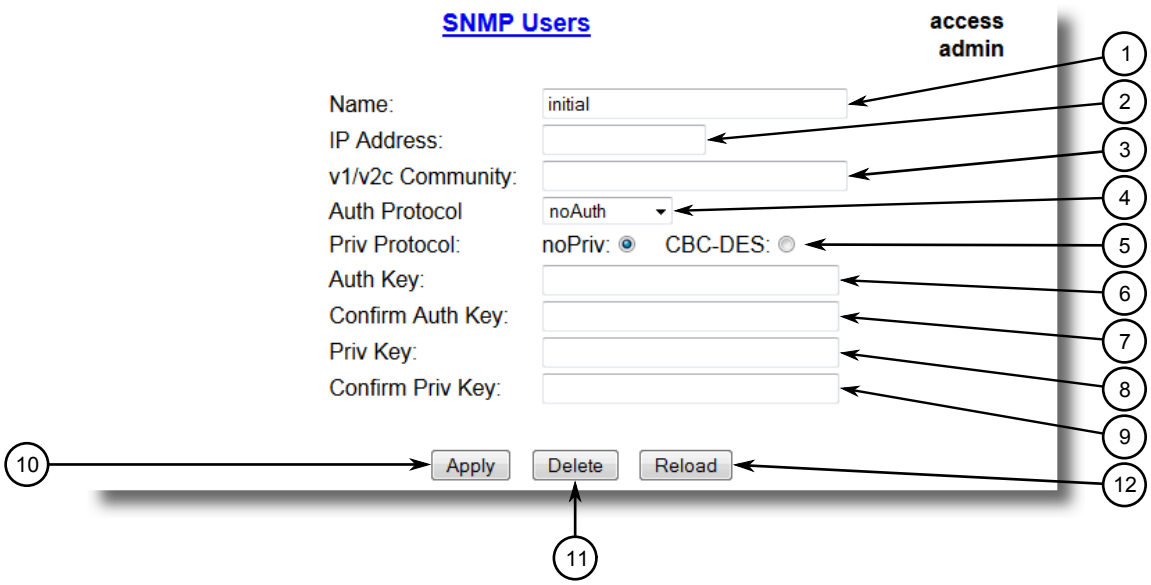


Figure 136 : Formulaire SNMP Users

1. Zone Name **2.** Zone IP Address **3.** Zone v1/v2c Community **4.** Zone Auth Protocol **5.** Zone Priv Protocol **6.** Zone Auth Key **7.** Zone Confirm Auth Key **8.** Zone Priv Key **9.** Zone Confirm Priv Key **10.** Bouton Apply **11.** Bouton Delete **12.** Bouton Reload

REMARQUE

RUGGEDCOM ROS requiert que tous les mots de passes répondent à des directives strictes afin d'éviter l'utilisation de mots de passe faibles. Lors de la création d'un nouveau mot de passe, assurez-vous que les règles suivantes sont respectées :

- *Sa longueur ne doit pas dépasser 6 caractères.*
- *Il ne doit pas inclure de nom d'utilisateur ou 4 caractères alphanumériques continus figurant dans le nom d'utilisateur. Par exemple, si le nom d'utilisateur est **Subnet25**, le mot de passe ne peut pas être **subnet25admin** ou **subnetadmin**. **net25admin** ou **Sub25admin** sont cependant autorisés.*
- *Il doit comprendre au moins un caractère alphabétique et un chiffre. Les caractères spéciaux ne sont pas autorisés.*
- *Il ne doit pas comprendre plus de 3 chiffres à incrémentation ou décrémentation continue. Par exemple, **Sub123** et **Sub19826** sont autorisés, mais pas **Sub12345**.*

Une alarme est générée si un mot de passe faible est configuré. L'alarme de mot de passe faible peut être désactivée par l'utilisateur. Pour plus d'informations sur la désactivation d'alarmes, voir *Section 4.6, « Gestion des alarmes »*.

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Name	**Synopsis :** 32 caractères quelconques **Par défaut :** initial Nom de l'utilisateur. Ce nom d'utilisateur représente également le nom de sécurité qui mappe cet utilisateur sur le groupe de sécurité.
IP Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ###

Paramètre	Description
	L'adresse IP de la station de gestion SNMP de l'utilisateur. Si l'adresse IP est configurée, les requêtes SNMP de cet utilisateur sont également vérifiées par l'adresse IP. Un trap d'authentification est généré pour piéger les destinataires sur la requête est reçue de cet utilisateur depuis une autre adresse IP quelconque. Si l'adresse IP est vide, les traps ne peuvent pas être générés pour cet utilisateur, mais les requêtes SNMP sont exécutées pour cet utilisateur à partir d'une adresse IP quelconque.
v1/v2c Community	**Synopsis :** 32 caractères quelconques La chaîne de communauté, mappée par cet utilisateur/cette sécurité sur le groupe de sécurité si le modèle de sécurité est SNMPv1 ou SNMPv2c. Si cette chaîne de caractères est vide, on supposera qu'elle est égale au nom d'utilisateur.
Auth Protocol	**Synopsis :** { noAuth, HMACMD5, HMACSHA } **Par défaut :** noAuth Indication si des messages envoyés au nom de cet utilisateur vers/depuis le moteur SNMP peuvent être authentifiés et, le cas échéant, le type de protocole d'authentification utilisé.
Priv Protocol	**Synopsis :** { noPriv, CBC-DES } **Par défaut :** noPriv Indication si des messages envoyés au nom de cet utilisateur vers/depuis le moteur SNMP peuvent être protégés contre la divulgation et, le cas échéant, le type de protocole de confidentialité utilisé.
Auth Key	**Synopsis :** chaîne de 31 caractères ASCII La clé d'authentification secrète (mot de passe) à partager avec le client SNMP. Si la clé n'est pas une chaîne vide, elle doit comprendre au moins 6 caractères.
Confirm Auth Key	**Synopsis :** chaîne de 31 caractères ASCII La clé d'authentification secrète (mot de passe) à partager avec le client SNMP. Si la clé n'est pas une chaîne vide, elle doit comprendre au moins 6 caractères.
Priv Key	**Synopsis :** chaîne de 31 caractères ASCII La clé de chiffrement secrète (mot de passe) à partager avec le client SNMP. Si la clé n'est pas une chaîne vide, elle doit comprendre au moins 6 caractères.
Confirm Priv Key	**Synopsis :** chaîne de 31 caractères ASCII La clé de chiffrement secrète (mot de passe) à partager avec le client SNMP. Si la clé n'est pas une chaîne vide, elle doit comprendre au moins 6 caractères.

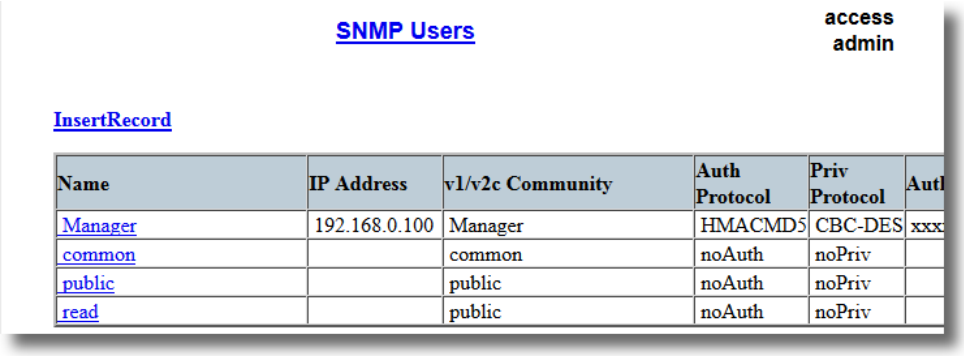
4. Cliquez sur **Apply**.

Section 5.6.1.3

Suppression d'un utilisateur SNMP

Procédez comme suit pour supprimer un utilisateur SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Users***. Le tableau **SNMP Users** s'affiche.



Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 137 : Tableau SNMP Users

2. Sélectionnez l'utilisateur dans le tableau. Le formulaire **SNMP Users** s'affiche.

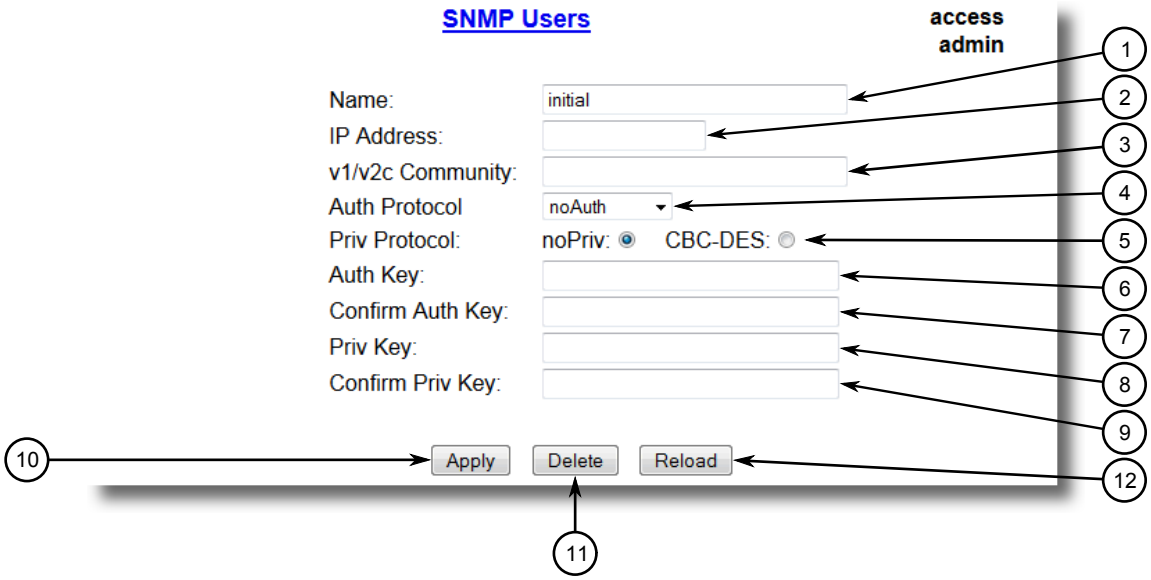


Figure 138 : Formulaire SNMP Users

1. Zone Name **2.** Zone IP Address **3.** Zone v1/v2c Community **4.** Zone Auth Protocol **5.** Zone Priv Protocol **6.** Zone Auth Key **7.** Zone Confirm Auth Key **8.** Zone Priv Key **9.** Zone Confirm Priv Key **10.** Bouton Apply **11.** Bouton Delete **12.** Bouton Reload

3. Cliquez sur **Delete**.

Section 5.6.2

Gestion du mappage sécurité sur groupe

Cette section décrit la configuration et la gestion des mappages sécurité sur groupe.

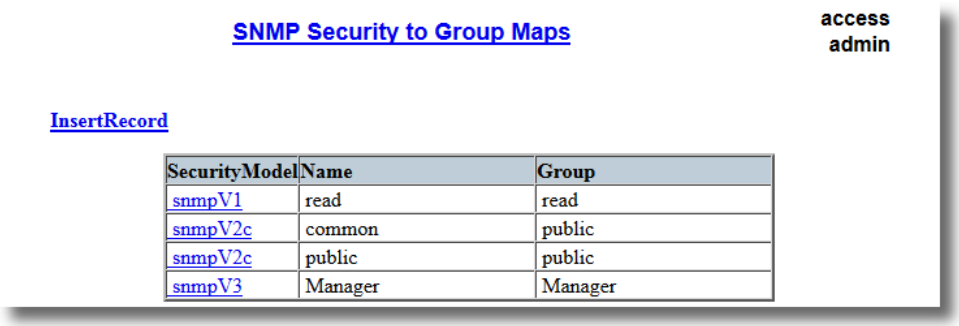
SOMMAIRE

- Section 5.6.2.1, « Affichage d'une liste de mappages sécurité sur groupe »
- Section 5.6.2.2, « Ajout d'un mappage sécurité sur groupe »
- Section 5.6.2.3, « Suppression d'un mappage sécurité sur groupe »

Section 5.6.2.1

Affichage d'une liste de mappages sécurité sur groupe

Pour afficher une liste de mappages sécurité sur groupe configurés sur l'appareil, accédez à ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. Le tableau **SNMP Security to Group Maps** s'affiche.



SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

Figure 139 : Tableau SNMP Security to Group Maps

Si aucun mappage sécurité sur groupe n'a été configuré, ajoutez des mappages en fonction de vos besoins. Pour plus d'informations, voir Section 5.6.2.2, « Ajout d'un mappage sécurité sur groupe ».

Section 5.6.2.2

Ajout d'un mappage sécurité sur groupe

Plusieurs combinations de modèles et de groupes de sécurité peuvent être mappées (32 max.) pour SNMP.

Procédez comme suit pour ajouter un mappage sécurité sur groupe :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. Le tableau **SNMP Security to Group Maps** s'affiche.

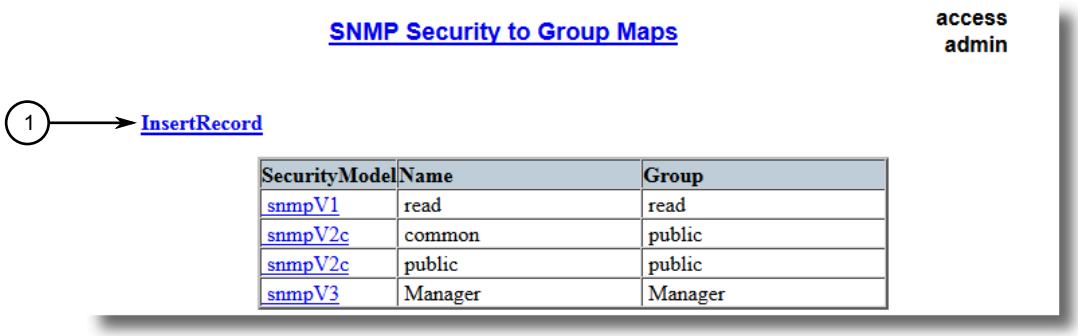


Figure 140 : Tableau SNMP Security to Group Maps

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **SNMP Security to Group Maps** s'affiche.

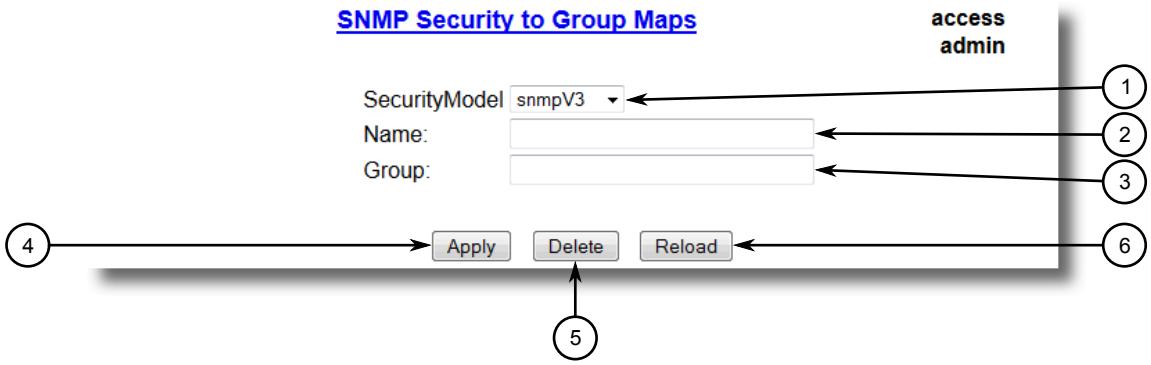


Figure 141 : Formulaire SNMP Security to Group Maps

1. Zone Security Model **2.** Zone Name **3.** Zone Group **4.** Bouton Apply **5.** Bouton Delete **6.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
SecurityModel	**Synopsis :** { snmpV1, snmpV2c, snmpV3 } **Par défaut :** snmpV3 Modèle de sécurité fournissant le nom référencé dans ce tableau.
Name	**Synopsis :** 32 caractères quelconques Le nom d'utilisateur mappé par cette entrée sur un nom de groupe spécifié.
Group	**Synopsis :** 32 caractères quelconques Nom du groupe auquel le modèle de sécurité et le nom appartiennent. Ce nom est utilisé comme index du tableau SNMPv3 VACM Access.

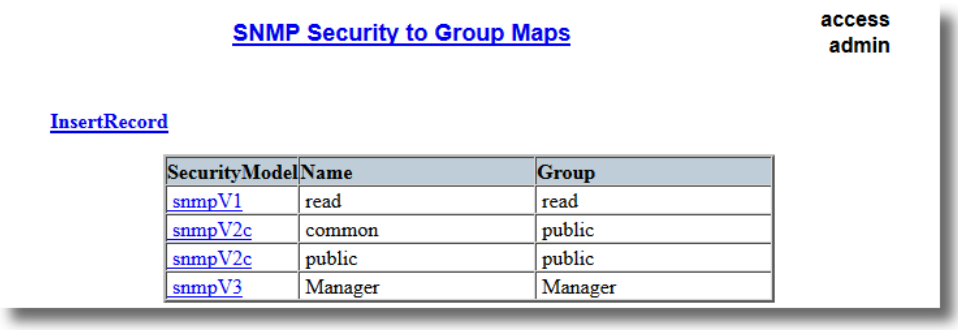
4. Cliquez sur **Apply**.

Section 5.6.2.3

Suppression d'un mappage sécurité sur groupe

Procédez comme suit pour supprimer un mappage sécurité sur groupe :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. Le tableau **SNMP Security to Group Maps** s'affiche.



SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

Figure 142 : Tableau SNMP Security to Group Maps

2. Sélectionnez le mappage dans le tableau. Le formulaire **SNMP Security to Group Maps** s'affiche.

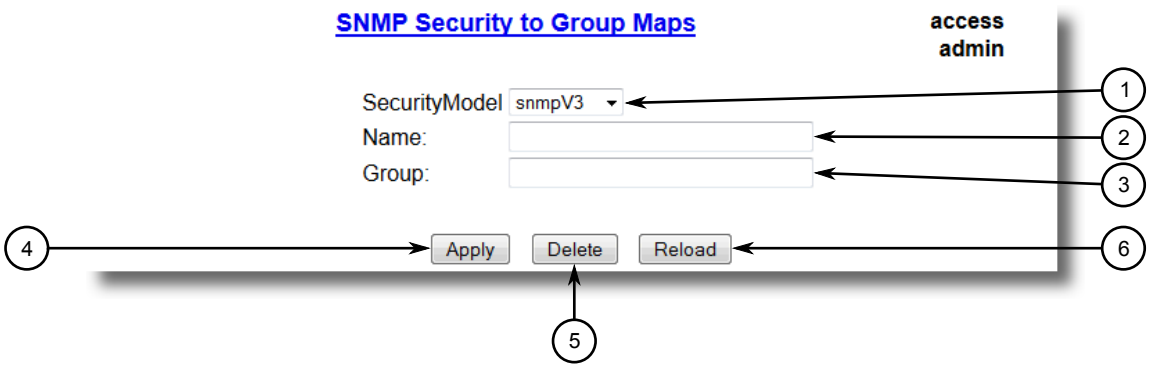


Figure 143 : Formulaire SNMP Security to Group Maps

1. Zone Security Model **2.** Zone Name **3.** Zone Group **4.** Bouton Apply **5.** Bouton Delete **6.** Bouton Reload

3. Cliquez sur **Delete**.

Section 5.6.3

Gestion de groupes SNMP

Plusieurs groupes SNMP (jusqu'à 32) peuvent être configurés pour avoir un accès au SNMP.

SOMMAIRE

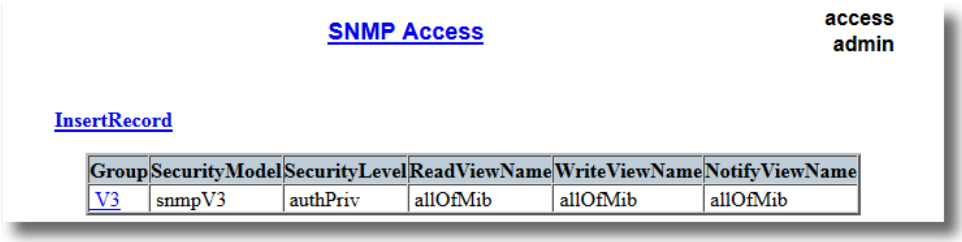
- Section 5.6.3.1, « Affichage d'une liste de groupes SNMP »
- Section 5.6.3.2, « Ajout d'un groupe SNMP »

- Section 5.6.3.3, « Suppression d'un groupe SNMP »

Section 5.6.3.1

Affichage d'une liste de groupes SNMP

Pour afficher une liste de groupes SNMP configurés sur l'appareil, accédez à ***Administration » Configure SNMP » Configure SNMP Access***. Le tableau **SNMP Access** s'affiche.



Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 144 : Tableau SNMP Access

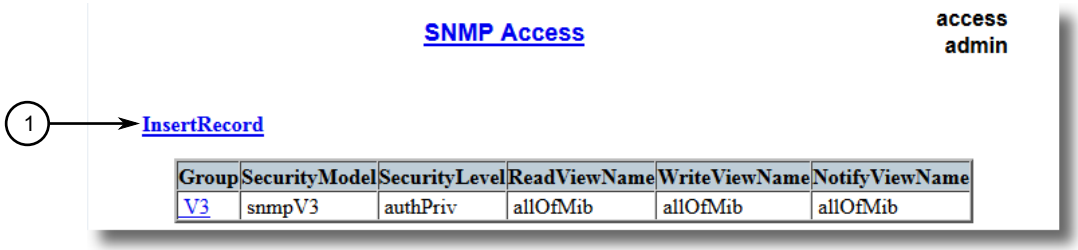
Si aucun groupe SNMP n'a été configuré, ajoutez des groupes en fonction de vos besoins. Pour plus d'informations, voir Section 5.6.3.2, « Ajout d'un groupe SNMP ».

Section 5.6.3.2

Ajout d'un groupe SNMP

Procédez comme suit pour ajouter un groupe SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Access***. Le tableau **SNMP Access** s'affiche.



Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 145 : Tableau SNMP Access

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **SNMP Access** s'affiche.

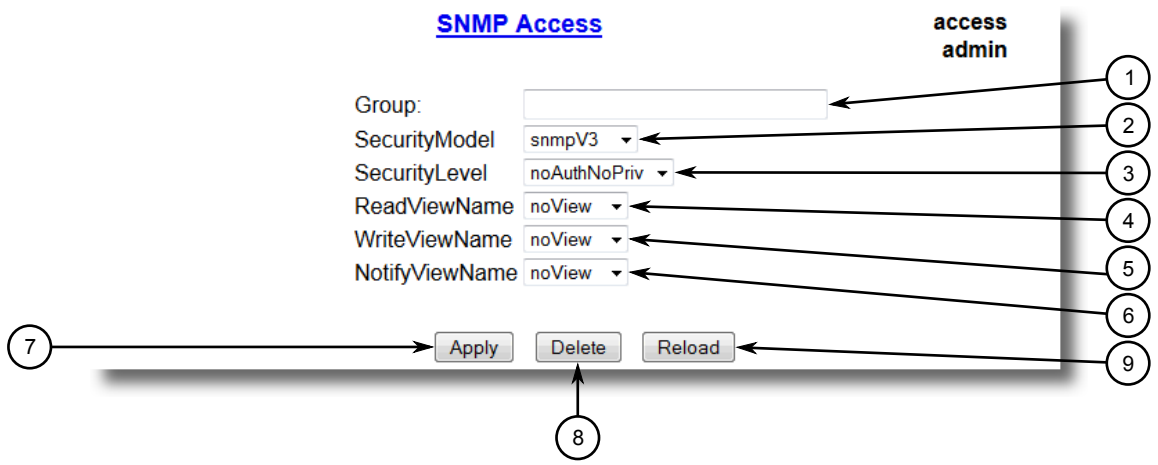


Figure 146 : Formulaire SNMP Access

1. Zone Group **2.** Zone Security Model **3.** Zone Security Level **4.** Zone ReadViewName **5.** Zone WriteViewName **6.** Zone NotifyViewName **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Group	**Synopsis :** 32 caractères quelconques Nom du groupe auquel le modèle de sécurité et le nom appartiennent. Ce nom est utilisé comme index du tableau SNMPv3 VACM Access.
SecurityModel	**Synopsis :** { snmpV1, snmpV2c, snmpV3 } **Par défaut :** snmpV3 Pour obtenir des droits d'accès liés à cette entrée, un modèle de sécurité configuré doit être utilisé.
SecurityLevel	**Synopsis :** { noAuthNoPriv, authNoPriv, authPriv } **Par défaut :** noAuthNoPriv Niveau de sécurité minimum requis pour obtenir des droits d'accès liés à cette entrée. Le niveau de sécurité noAuthNoPriv est inférieur à authNoPriv, qui est inférieur à authPriv.
ReadViewName	**Synopsis :** { noView, V1Mib, allOfMib } **Par défaut :** noView Ce paramètre identifie les arborescences MIB auxquelles cette entrée donne un accès en lecture. Si la valeur est noView, aucun accès en lecture n'est accordé.
WriteViewName	**Synopsis :** { noView, V1Mib, allOfMib } **Par défaut :** noView Ce paramètre identifie les arborescences MIB auxquelles cette entrée donne un accès en écriture. Si la valeur est noView, aucun accès en écriture n'est accordé.
NotifyViewName	**Synopsis :** { noView, V1Mib, allOfMib } **Par défaut :** noView Ce paramètre identifie les arborescences MIB auxquelles cette entrée donne un accès à des notifications. Si la valeur est noView, aucun accès en écriture n'est accordé à des notifications.

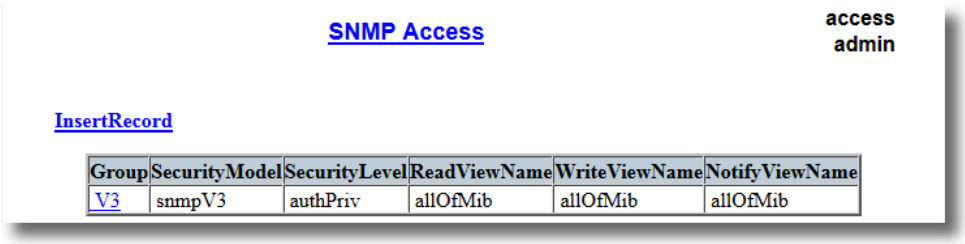
4. Cliquez sur **Apply**.

Section 5.6.3.3

Suppression d'un groupe SNMP

Procédez comme suit pour supprimer un groupe SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Access***. Le tableau **SNMP Access** s'affiche.



Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 147 : Tableau SNMP Access

2. Sélectionnez le groupe dans le tableau. Le formulaire **SNMP Access** s'affiche.

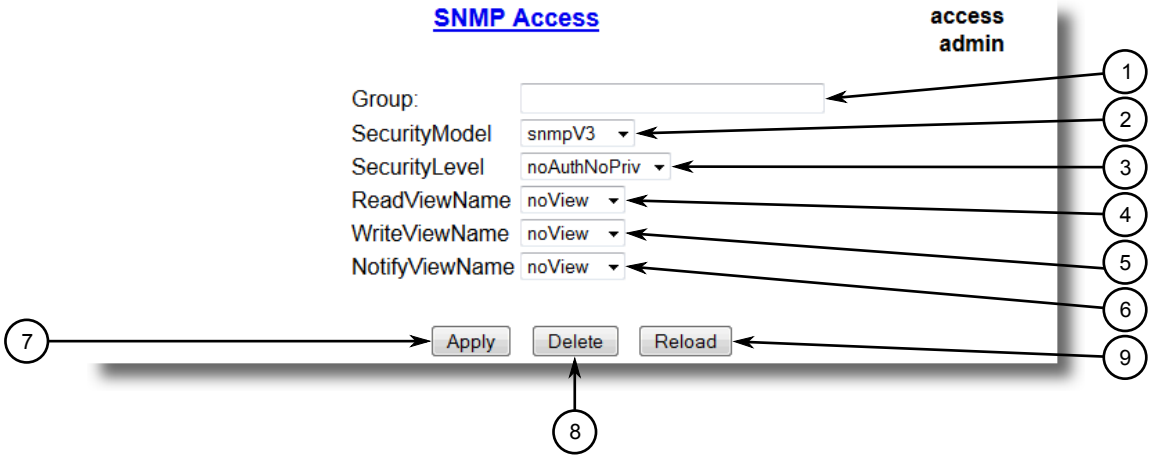


Figure 148 : Formulaire SNMP Access

1. Zone Group **2.** Zone Security Model **3.** Zone Security Level **4.** Zone ReadViewName **5.** Zone WriteViewName **6.** Zone NotifyViewName **7.** Bouton Apply **8.** Bouton Delete **9.** Bouton Reload

3. Cliquez sur **Delete**.

Section 5.7

Gestion de la découverte de réseau

RUGGEDCOM ROS prend en charge le LLDP (Link Layer Discovery Protocol) et RUGGEDCOM le RCDP (Discovery Protocol), les deux étant des protocoles de couche 2 pour la découverte de réseau automatisée.

SOMMAIRE

- Section 5.7.1, « Activation/désactivation du RCDP »
- Section 5.7.2, « LLDP (Link Layer Discovery Protocol) »

Section 5.7.1

Activation/désactivation du RCDP

RUGGEDCOM ROS prend en charge le RCDP (RUGGEDCOM Discovery Protocole). RCDP prend en charge le déploiement d'appareils basés sur RUGGEDCOM ROS qui n'ont pas été configurés depuis la sortie d'usine. Les appareils RUGGEDCOM ROS qui n'ont pas été configurés ont tous l'adresse IP par défaut (couche 3). Connecter plusieurs de ces appareils sur un réseau de couche 2 signifie qu'il est impossible d'utiliser des outils de configuration standard basés sur IP pour les configurer. Le comportement des mécanismes basés sur IP tels que l'interface Web, SSH, telnet ou SNMP n'est pas défini.

Le RCDP fonctionnant en couche 2, il peut être utilisé pour adresser de manière fiable et non-ambiguë plusieurs appareils, même s'ils ont la même configuration IP.

Le RUGGEDCOM Explorer de Siemens est une application Windows légère et autonome prenant en charge RCDP. Il est en mesure de découvrir, d'identifier et d'exécuter la configuration de base d'appareils basés sur RUGGEDCOM ROS via RCDP. Les fonctionnalités prises en charge par RCDP sont entre autres :

- Découverte d'appareils basés sur RUGGEDCOM ROS via un réseau de couche 2.
- Récupération de la configuration réseau de base, de la version RUGGEDCOM ROS, du code de commande et du numéro de série.
- Contrôle des LED d'appareil pour une identification physique aisée.
- Configuration de l'identification de base, de la mise en réseau et des paramètres d'authentification.

Pour des raisons de sécurité, RUGGEDCOM Explorer tente de désactiver RCDP sur tous les appareils lorsque l'Explorer est fermé. Si RUGGEDCOM Explorer n'est pas en mesure de désactiver RCDP sur un appareil, RUGGEDCOM ROS désactive automatiquement RCDP une heure après la réception de la dernière trame RCDP.

RUGGEDCOM ROS désactive automatiquement RCDP si l'adresse IP, le sous-réseau, la passerelle ou des mots de passe sont modifiés pour l'appareil via SSH, RSH, Telnet, la console série ou SNMP.

IMPORTANT !
Pour une sécurité accrue, Siemens recommande la désactivation de RCDP si son utilisation n'est pas prévue.

REMARQUE
RCDP n'est pas compatible avec des configurations réseau basées sur VLAN. Pour un fonctionnement correct de RUGGEDCOM Explorer, aucun VLAN (balisé ou non balisé) ne doit être configuré. Tous les éléments de configuration doivent être paramétrés sur leurs réglages par défaut.

REMARQUE
RUGGEDCOM ROS répond uniquement aux demandes RCDP. Il n'initie en aucun cas une communication basée sur RCDP.

Procédez comme suit pour activer ou désactiver RCDP :

1. Accédez à ***Network Discovery » Link Layer Discovery Protocol » Configure RCDP Parameters***. Le formulaire **RCDP Parameters** s'affiche.

Figure 149 : Formulaire RCDP Parameters

1. Liste RCDP Discovery **2.** Bouton Apply **3.** Bouton Reload

2. Sous**RCDP Discovery**, sélectionnez l'une des options suivantes :
   - `Disabled` – Désactive l'accès en lecture et écriture
   - `Get Only` – Active l'accès en lecture uniquement
   - `Enabled` – Active l'accès en lecture et écriture
3. Cliquez sur **Apply**.

Section 5.7.2

LLDP (Link Layer Discovery Protocol)

Le LLDP (Link Layer Discovery Protocol) défini par IEEE 802.11AB permet à un appareil mis en réseau d'annoncer ses propres capacités de mise en réseau de base et sa configuration.

LLDP permet à un appareil mis en réseau de découvrir ses voisins dans les liaisons réseau connectées à l'aide d'un mécanisme standard. Les appareils prenant en charge LLDP sont en mesure d'annoncer des informations les concernant, notamment leur capacité, leur configuration, les interconnexions et l'identification.

Le fonctionnement de l'agent LLDP est généralement mis en œuvre comme deux modules : le module de transmission LLDP et le module de réception LLDP. Le module de transmission LLDP, lorsqu'il est activé, envoie les informations de l'appareil local à intervalles réguliers au format standard IEEE 802.1AB. Lorsque le module de transmission est désactivé, il transmet une LLDPDU (LLDP data unit) avec un type-longueur-valeur (type-length-value (TLV)) de durée de vie (time-to-live (TTL)) de 0 dans le champ d'information Ceci permet aux appareils distants de supprimer les informations associées à l'appareil local dans leurs bases de données. Le module de réception LLDP, lorsqu'il est activé, reçoit des informations des appareils distants et met à jour sa base de données LLDP de systèmes distants. Lorsque des informations nouvelles ou mises à jour sont reçues, le module de réception lance une temporisation pour la durée valide indiquée par le TLV TTL dans la LLDPDU reçue. Les informations d'un système distant sont supprimées d'une base de données lorsqu'une LLDPDU est reçue de ce système avec un TLV TTL de 0 dans son champ d'information.

REMARQUE
LLDP est mis en œuvre pour suivre un seul appareil par port Ethernet. Par conséquent, si plusieurs appareils envoient des informations LLDP à un port de commutateur sur lequel LLDP est activé, les informations concernant le voisin sur ce port sont constamment modifiées.

SOMMAIRE

- Section 5.7.2.1, « Configuration globale du LLDP »
- Section 5.7.2.2, « Configuration de LLDP pour un port Ethernet »
- Section 5.7.2.3, « Affichage de statistiques globales et d'informations système annoncées »
- Section 5.7.2.4, « Affichage des statistiques pour des voisins LLDP »
- Section 5.7.2.5, « Affichage des statistiques pour des ports LLDP »

Section 5.7.2.1

Configuration globale du LLDP

Procédez comme suit pour configurer des réglages globaux pour LLDP :

1. Accédez à ***Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters***. Le formulaire **Global LLDP Parameters** s'affiche.

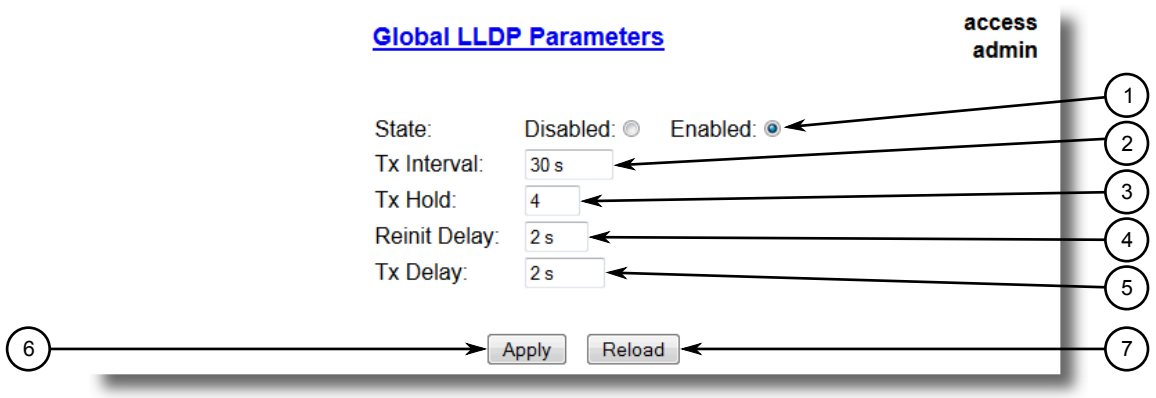


Figure 150 : Formulaire Global LLDP Parameters

1. Options State **2.** Zone Tx Interval **3.** Zone Tx Hold **4.** Zone Reinit Delay **5.** Zone Tx Delay **6.** Bouton Apply **7.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
State	**Synopsis :** { Disabled, Enabled } **Par défaut :** Enabled Active le protocole LLDP Notez que le LLDP est activé sur un port LLDP lorsqu'il est activé globalement avec le réglage de l'activation par port dans le menu Port LLDP Parameters.
Tx Interval	**Synopsis :** 5 à 32768 s **Par défaut :** 30 s L'intervalle auquel les trames LLDP sont transmises au nom de cet agent LLDP.

Paramètre	Description
Tx Hold	**Synopsis :** 2 à 10 **Par défaut :** 4 Le multiplicateur du paramètre Tx Interval qui détermine la durée de vie (time-to-live (TTL)) effective dans une LLDPDU. La valeur TTL effective peut être exprimée par la formule suivante : `TTL = MIN(65535, (Tx Interval * Tx Hold))`
Reinit Delay	**Synopsis :** 1 à 10 s **Par défaut :** 2 s Délai en secondes pendant lequel la valeur du paramètre Admin Status d'un port spécifique est 'Disbled' jusqu'à une nouvelle tentative de réinitialisation.
Tx Delay	**Synopsis :** 1 à 8192 s **Par défaut :** 2 s Délai en secondes entre des transmissions de trames LLDP successives initiées par une modification de valeur ou d'état. La valeur recommandée est définie avec la formule suivante : `1<= txDelay<= (0.25 * Tx Interval)`

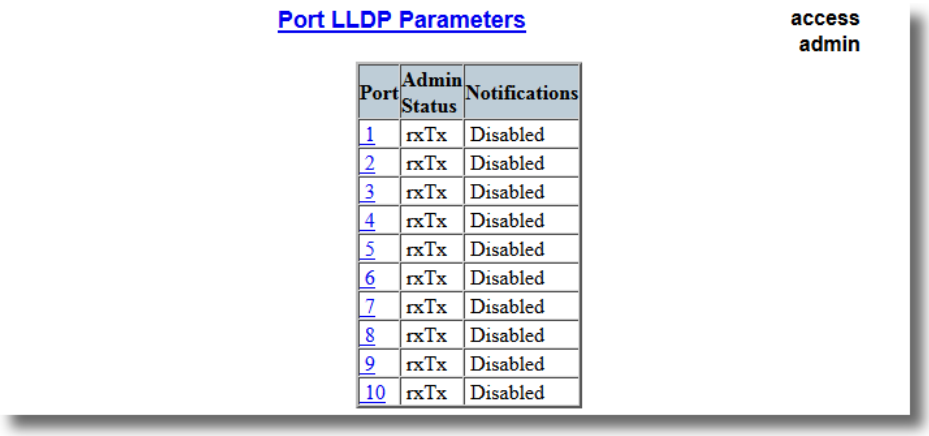
3. Cliquez sur **Apply**.

Section 5.7.2.2

Configuration de LLDP pour un port Ethernet

Procédez comme suit pour configurer LLDP pour un port Ethernet spécifique :

1. Accédez à ***Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters***. Le tableau **Port LLDP Parameters** s'affiche.



Port	Admin Status	Notifications
1	rxTx	Disabled
2	rxTx	Disabled
3	rxTx	Disabled
4	rxTx	Disabled
5	rxTx	Disabled
6	rxTx	Disabled
7	rxTx	Disabled
8	rxTx	Disabled
9	rxTx	Disabled
10	rxTx	Disabled

Figure 151 : Tableau Port LLDP Parameters

2. Sélectionnez un port. Le formulaire **Port LLDP Parameters** s'affiche.

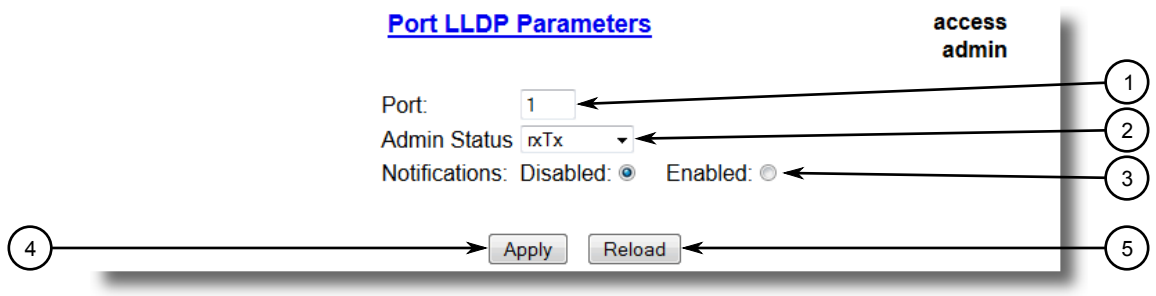


Figure 152 : Formulaire Port LLDP Parameters

1. Zone Port **2.** Liste Admin Status **3.** Options Notifications **4.** Bouton Apply **5.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Admin Status	**Synopsis :** { rxTx, txOnly, rxOnly, Disabled } **Par défaut :** rxTx rxTx : l'agent LLDP local peut transmettre et recevoir des trames LLDP via le port. txOnly : l'agent LLDP local peut uniquement transmettre des trames LLDP. rxOnly : l'agent LLDP local peut uniquement recevoir des trames LLDP. disabled : l'agent LLDP local peut ne peut ni transmettre ni recevoir des trames LLDP.
Notifications	**Synopsis :** { Disabled, Enabled } **Par défaut :** Disabled La désactivation de notifications empêche l'envoi de notifications et la génération d'alarmes pour un port particulier depuis l'agent LLDP.

4. Cliquez sur **Apply**.

Section 5.7.2.3

Affichage de statistiques globales et d'informations système annoncées

Pour afficher des statistiques globales concernant PPP et les informations système annoncées à des voisins, accédez à ***Network Discovery » Link Layer Discovery Protocol » View LLDP Global Remote Statistics***. Le formulaire **LLDP Global Remote Statistics** s'affiche.

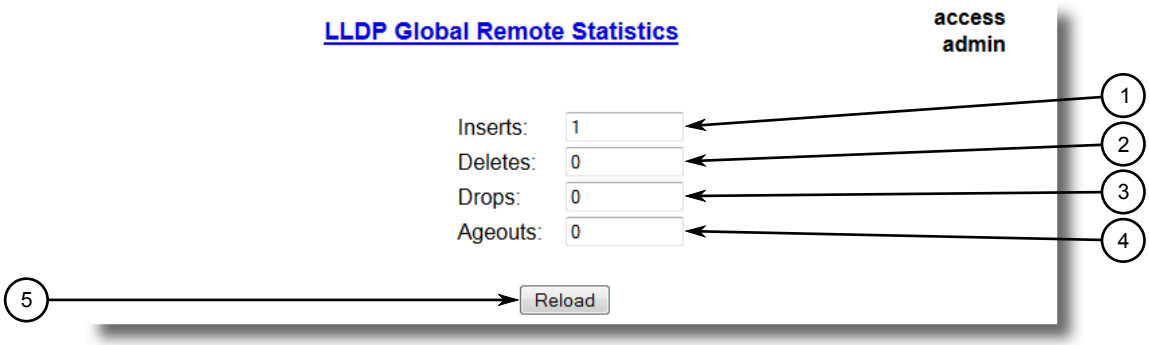


Figure 153 : Formulaire LLDP Global Remote Statistics

1. Zone Inserts **2.** Zone Deletes **3.** Zone Drops **4.** Zone Ageouts **5.** Bouton Reload

Ce formulaire affiche les informations suivantes :

Paramètre	Description
Inserts	**Synopsis :** 0 à 4294967295 Nombre d'insertions de l'entrée dans le tableau LLDP Neighbor Information.
Deletes	**Synopsis :** 0 à 4294967295 Nombre de suppressions de l'entrée dans le tableau LLDP Neighbor Information.
Drops	**Synopsis :** 0 à 4294967295 Nombre de suppressions d'une entrée dans le tableau LLDP Neighbor Information en raison de l'expiration de l'intervalle d'exactitude de l'information.
Ageouts	**Synopsis :** 0 à 4294967295 Compteur de toutes les TLV rejetées.

Section 5.7.2.4

Affichage des statistiques pour des voisins LLDP

Pour afficher les statistiques pour des voisins LLDP, accédez à ***Network Discovery » Link Layer Discovery Protocol » View LLDP Neighbor Information***. Le tableau **LLDP Neighbor Information** s'affiche.

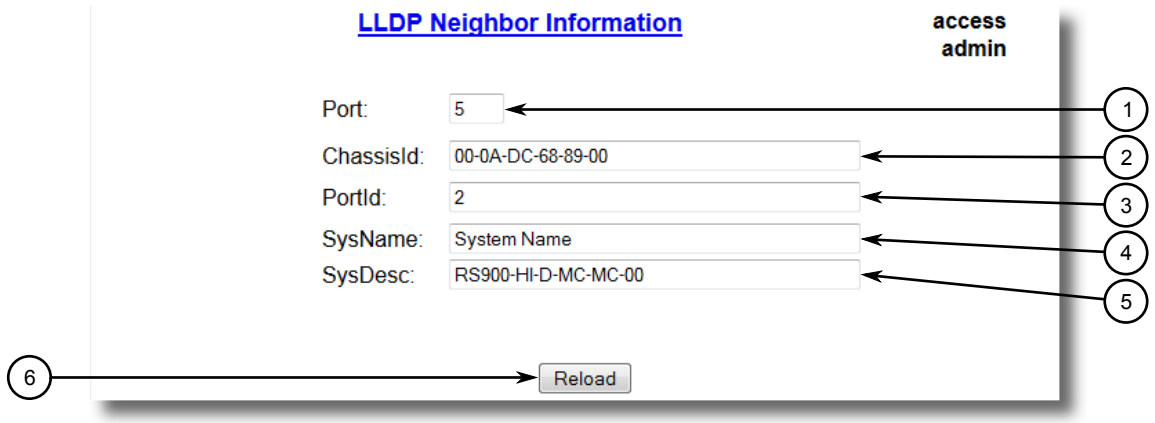


Figure 154 : Tableau LLDP Neighbor Information

1. Zone Port **2.** Zone ChassisId **3.** Zone PortId **4.** Zone SysName **5.** Zone SysDesc **6.** Bouton Reload

Ce formulaire affiche les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Port local associé à cette entrée.
ChassisId	**Synopsis :** 45 caractères quelconques Information d'ID de boîtier reçue de l'agent LLDP distant.
PortId	**Synopsis :** 45 caractères quelconques Information d'ID de port reçue de l'agent LLDP distant.
SysName	**Synopsis :** 45 caractères quelconques Information de nom du système reçue de l'agent LLDP distant.
SysDesc	**Synopsis :** 45 caractères quelconques Information de descripteur du système reçue de l'agent LLDP distant.

Section 5.7.2.5

Affichage des statistiques pour des ports LLDP

Pour afficher les statistiques pour des ports LLDP, accédez à ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics***. Le tableau **LLDP Statistics** s'affiche.

LLDP Statistics

access
admin

Port	FrmDrop	ErrFrm	FrmIn	FrmOut	Ageouts	TLVsDrop	TLVsUnknown
1	0	0	12274	2041	1	0	36822
2	0	0	2046	2041	1	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	1435	1433	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0

Figure 155 : Tableau LLDP Statistics

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
FrmDrop	**Synopsis :** 0 à 4294967295 Compteur de toutes les trames LLDP rejetées.
ErrFrm	**Synopsis :** 0 à 4294967295 Compteur de toutes les LLDPDU reçues avec erreurs détectables.
FrmIn	**Synopsis :** 0 à 4294967295 Compteur de toutes les LLDPDU reçues.
FrmOut	**Synopsis :** 0 à 4294967295 Compteur de toutes les LLDPDU transmises.
Ageouts	**Synopsis :** 0 à 4294967295 Compteur de suppressions d'une information de voisin du MIB du système distant LLDP en raison de l'expiration de la temporisation txinfoTTL.
TLVsDrop	**Synopsis :** 0 à 4294967295 Compteur de toutes les TLV rejetées.
TLVsUnknown	**Synopsis :** 0 à 4294967295 Compteur de toutes les TLV reçues sur le port non reconnues par l'agent local LLDP.

Section 5.8

Gestion du filtrage de multidiffusion

Le trafic de multidiffusion peut être filtré à l'aide de l'espionnage IGMP (Internet Group Management Protocol) ou GMRP (GARP Multicast Registration Protocol).

SOMMAIRE

- Section 5.8.1, « Gestion d'IGMP »
- Section 5.8.2, « Gestion de GMRP »

Section 5.8.1

Gestion d'IGMP

IGMP est utilisé par les hôtes IP pour signaler leurs appartenances à des groupes d'hôtes avec des routeurs de multidiffusion. Lorsque les hôtes joignent et quittent des groupes de multidiffusion, les flux ou le trafic sont dirigés ou retenus depuis cet hôte.

Le protocole IGMP fonctionne entre des routeurs de multidiffusion et des hôtes IP. Lorsqu'un commutateur non managé est placé entre des routeurs de multidiffusion et leurs hôtes, les flux de multidiffusion sont distribués à tous les ports. Cela peut impliquer un trafic important vers les ports qui n'en ont pas besoin et n'en tirent aucun avantage.

L'espionnage IGMP, lorsqu'il est activé, agit sur des messages IGMP envoyés depuis le routeur et l'hôte, réduisant ainsi les flux de trafic aux segments LAN appropriés.

IMPORTANT !
RUGGEDCOM ROS empêche les ports IGMP de s'inscrire aux adresses de multidiffusion spéciales suivantes :

- *224.0.0.0 à 224.0.0.255*
- *224.0.1.129*

Ces adresses sont réservées pour les protocoles d'acheminement et IEEE 1588. Si un rapport d'appartenance IGMP contient l'une de ces adresses, le rapport est transmis par le commutateur sans apprentissage de l'hôte.

SOMMAIRE

- Section 5.8.1.1, « Concepts IGMP »
- Section 5.8.1.2, « Affichage d'une liste d'appartenances à des groupes de multidiffusion »
- Section 5.8.1.3, « Affichage d'informations de transmission pour des groupes de multidiffusion »
- Section 5.8.1.4, « Configuration d'IGMP »

Section 5.8.1.1

Concepts IGMP

La présente rubrique décrit certains concepts importants de la mise en œuvre du filtrage de multidiffusion à l'aide d'IGMP :

Fonctionnement d'IGMP

Le diagramme de réseau suivant fournit un exemple simple de l'utilisation d'IGMP.

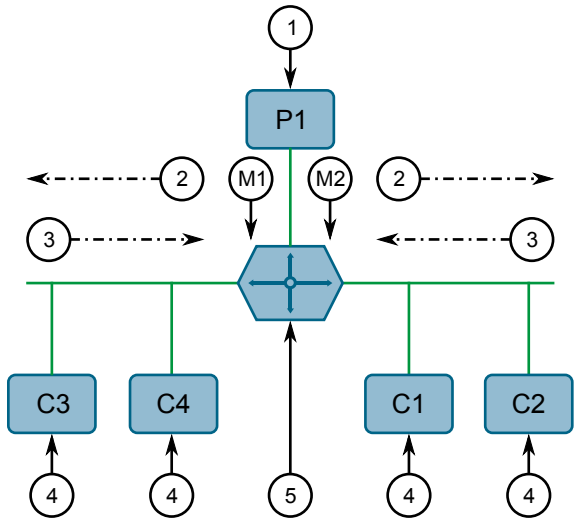


Figure 156 : Exemple - Fonctionnement d'IGMP

1. Producteur **2.** Demande d'appartenance **3.** Rapports d'appartenance **4.** Consommateur **5.** Routeur de multidiffusion

Un hôte IP *producteur* (P1) génère deux flux de multidiffusion, M1 and M2. Il existe quatre *consommateurs* potentiels dans ces flux, C1 à C4. Le routeur de multidiffusion découvre l'hôte souhaitant s'abonner et à quel flux en envoyant des demandes d'appartenance générales à chaque segment.

Dans cet exemple, la demande d'appartenance générale envoyée aux segments C1-C2 reçoit une réponse sous forme de rapport d'appartenance (ou *join*) indiquant le souhait d'une inscription au flux M2. Le routeur transmet le flux M2 aux segments C1-C2. D'une manière similaire, le routeur identifie qu'il doit transmettre le flux M1 aux segments C3-C4.

Un *consommateur* peut joindre un nombre quelconque de groupes de multidiffusion, générant alors un rapport d'appartenance pour chaque groupe. Lorsqu'un hôte génère un rapport d'appartenance, d'autres hôtes sur le même segment de réseau nécessitant également une appartenance au même groupe suppriment leurs propres demandes car elles seraient redondantes. De cette manière, le protocole IGMP garantit que le segment génère uniquement un rapport d'appartenance pour chaque groupe.

Le routeur interroge périodiquement chaque segment afin de déterminer si au moins un consommateur est toujours abonné à un flux donné. S'il ne reçoit aucune réponse pendant un intervalle de temps donné (généralement deux intervalles d'interrogation), le routeur réduit le flux de multidiffusion du segment donné.

Une méthode plus commune de réduction se produit lorsque les consommateurs souhaitant se désinscrire génèrent un message IGMP *leave group*. Le routeur génère immédiatement une appartenance au groupe spécifique pour déterminer si le segment comprend des abonnés restants de ce groupe. Une fois que le dernier consommateur d'un groupe s'est désinscrit, le routeur réduit le flux de multidiffusion du segment donné.

Fonctionnement du commutateur IGMP

La fonctionnalité d'espionnage IGMP fournit un moyen pour les commutateurs d'espionner (snoop) le fonctionnement des routeurs, de répondre avec des messages joins/leaves pour le compte des ports consommateurs et de réduire les flux de multidiffusion en conséquence. Le commutateur peut être configuré avec deux modes IGMP : actif et passif.

- **Mode actif**
  IGMP prend en charge un mode de fonctionnement *sans routeur*.

  Lorsqu'un tel commutateur est utilisé sans routeur de multidiffusion, il est en mesure de fonctionner de la même manière qu'un routeur de multidiffusion envoyant des demandes IGMP générales.
- **Mode passif**
  Lorsqu'un tel commutateur est utilisé dans un réseau avec un routeur de multidiffusion, il peut être configuré de manière à exécuter IGMP en mode passif. Ce mode empêche le commutateur d'envoyer des demandes pouvant perturber le routeur qui s'arrête alors d'envoyer des demandes IGMP.

REMARQUE
Un commutateur fonctionnant en mode passif requiert la présence d'un routeur de multidiffusion, sinon il n'est pas en mesure de transmettre des flux de multidiffusion si aucun routeur de multidiffusion n'est présent.

REMARQUE
Un commutateur d'espionnage IGMP au minimum doit être en mode actif pour que IGMP puisse fonctionner.

Règles d'espionnage IGMP

L'espionnage IGMP respecte les règles suivantes :

- Lorsqu'une source de multidiffusion démarre la multidiffusion, le flux de trafic est immédiatement bloqué sur les segments desquels aucun message Join n'a été reçu.
- S'il n'est pas configuré différemment, le commutateur transmet le trafic de multidiffusion complet aux ports auxquels les routeurs de multidiffusion sont attachés.
- Les paquets avec une adresse de multidiffusion IP de destination dans la plage 224.0.0.X qui ne sont pas IGMP sont toujours transmis à tous les ports. Ce comportement est basé sur le fait que de nombreux systèmes n'envoient pas de rapport d'appartenance pour les adresses de multidiffusion IP dans cette plage pendant qu'ils écoutent de tels paquets.
- Le commutateur met en œuvre le *reporting proxy* IGMPv2 (c'est-à-dire que les rapports d'appartenance reçus en aval sont résumés et utilisés par le commutateur pour que ce dernier génère ses propres rapports).
- Le commutateur envoie uniquement les rapports d'appartenance IGMP de ces ports dans lesquels des routeurs de multidiffusion sont attachés, car envoyer des rapports d'appartenance à des hôtes empêcherait de manière non intentionnelle les hôtes de joindre un groupe spécifique.
- Les routeurs de multidiffusion utilisent IGMP pour élire un routeur maître connu comme *demandeur*.
  Le *demandeur* est le routeur avec l'adresse IP la moins élevée. Tous les autres routeurs deviennent non-demandeurs et participent uniquement à la transmission du trafic de multidiffusion. Les commutateurs exécutés en mode actif participent à l'élection du demandeur comme les routeurs de multidiffusion.
- Lorsque le processus d'élection du demandeur est terminé, le commutateur relaie simplement les demandes IGMP reçues du demandeur.
- Lorsqu'il envoie des paquets IGMP, le commutateur utilise le cas échéant sa propre adresse IP pour le VLAN vers lequel les paquets sont envoyés, ou une adresse 0.0.0.0 si aucune adresse IP ne lui est affectée.

REMARQUE
Les commutateurs d'espionnage IGMP exécutent la réduction de la multidiffusion à l'aide de l'adresse de multidiffusion MAC de destination d'une trame de multidiffusion, qui dépend de l'adresse de multidiffusion IP du groupe. L'adresse IP W.X.Y.Z correspond à l'adresse MAC 01-00-5E-XX-YY-ZZ dans laquelle XX correspond aux 7 bits bas de X, et YY et ZZ sont simplement Y et Z codés en hexadécimal.

On peut noter que les adresses de multidiffusion IP, telles que 224.1.1.1 et 225.1.1.1, sont mappées sur la même adresse MAC 01-00-5E-01-01-01. C'est un problème pour lequel l'IETF Network Working Group n'apporte aucune solution. Il est recommandé aux utilisateurs d'éviter ce problème.

IGMP et RSTP

Une modification de la topologie RSTP peut faire que les routes sélectionnées acheminent le trafic de multidiffusion comme incorrect. Cela peut entraîner une perte de trafic de multidiffusion.

Si RSTP détecte une modification dans la topologie de réseau, IGMP prend des mesures pour éviter la perte de la connectivité de multidiffusion et réduire le temps de convergence du réseau :

- Le commutateur génère immédiatement des demandes IGMP (s'il est en mode IGMP actif) pour obtenir des informations potentielles sur les nouvelles appartenances à des groupes.
- Le commutateur peut être configuré pour écouler temporairement les flux de multidiffusion de tous les ports non configurés comme ports de périphérie RSTP.

Fonctionnement IGM combiné du routeur et du commutateur

L'exemple suivant illustre le défi que représentent plusieurs routeurs, la prise en charge du VLAN et la commutation.

Le producteur P1 réside sur le VLAN 2 alors que le P2 réside sur le VLAN 3. Le consommateur C1 réside sur les deux VLAN alors que C2 et C3 résident respectivement sur les VLAN 3 et 2. Le routeur 2 réside sur le VLAN 2, vraisemblablement pour transmettre le trafic vers un réseau distant ou agir lui-même comme source du trafic de multidiffusion.

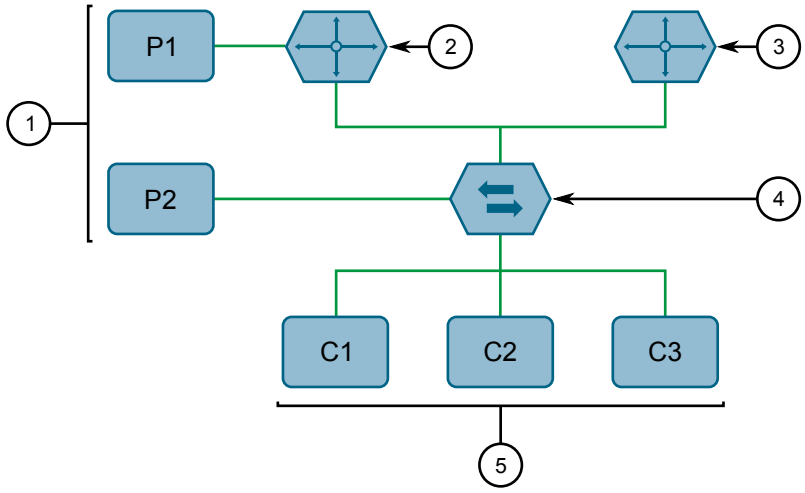


Figure 157 : Exemple - Fonctionnement combiné du routeur et du commutateur IGM

1. Producteur **2.** Routeur de multidiffusion 1 **3.** Routeur de multidiffusion 2 **4.** Commutateur **5.** Hôte

Dans cet exemple :

- P1, le routeur 1, le routeur 2 et C3 se trouvent sur VLAN 2
- P2 et C2 se trouvent sur VLAN 3
- C1 se trouve sur les VLAN 2 et 3

En supposant que le routeur 1 est le demandeur pour le VLAN 2 et que le routeur 2 est simplement non-demandeur, le commutateur reçoit périodiquement des demandes du routeur 1 et actualise les informations concernant le port lié au routeur de multidiffusion. Cependant, le port de commutateur lié au routeur 2 doit être configuré manuellement comme *port de routeur Port*. Sinon, le commutateur n'envoie ni les flux de multidiffusion ni les messages join/leave au routeur 2.

Notez que le VLAN 3 n'a pas de routeur de multidiffusion externe. Le commutateur doit être configuré de manière à fonctionner en mode *sans routeur* et générer des demandes d'appartenance générales comme s'il était le routeur.

- **Traitement des messages Join**
  Si l'hôte C1 veut s'inscrire aux flux de multidiffusion pour P1 et P2, il génère deux rapports d'appartenance. Le rapport d'appartenance de C1 sur le VLAN 2 entraînera l'initiation immédiate par le commutateur de son propre rapport d'appartenance pour le routeur 1 (et la génération de son propre rapport d'appartenance comme réponse à des demandes).

  Le rapport d'appartenance de l'hôte C1 pour VLAN3 a pour conséquence que le commutateur commence immédiatement à transmettre le trafic de multidiffusion du producteur P2 à l'hôte C2.
- **Traitement des messages Leave**
  Lorsque l'hôte C1 décide de quitter un groupe de multidiffusion, il génère une demande Leave au commutateur. Le commutateur interroge le port pour déterminer si l'hôte C1 est le dernier membre du groupe sur ce port. Si l'hôte C1 est le dernier (ou unique) membre, le groupe est immédiatement enlevé du port.

  Si l'hôte C1 doit quitter le groupe de multidiffusion sans générer un message Leave group et n'est pas ensuite en mesure de répondre à une demande d'appartenance générale, le commutateur arrête de transmettre le trafic après deux demandes.

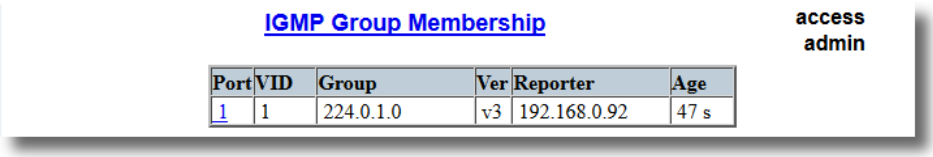
  Lorsque le dernier port dans un groupe de multidiffusion quitte le groupe (ou atteint sa limite de vieillissement), le commutateur génère un rapport Leave IGMP pour le routeur.

Section 5.8.1.2

Affichage d'une liste d'appartenances à des groupes de multidiffusion

À l'aide de l'espionnage IGMP, RUGGEDCOM ROS enregistre les informations d'appartenance à un groupe par port sur la base de rapports d'appartenance qu'il observe entre le routeur et l'hôte.

Pour afficher une liste d'appartenances à des groupes de multidiffusion, accédez à ***Multicast Filtering » View IGMP Group Membership***. Le tableau **View IGMP Group Membership** s'affiche.



Port	VID	Group	Ver	Reporter	Age
1	1	224.0.1.0	v3	192.168.0.92	47 s

Figure 158 : Tableau View IGMP Group Membership

Ce tableau fournit les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
VID	**Synopsis :** 0 à 65535

Paramètre	Description
	Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
Group	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Adresse du groupe de multidiffusion.
Ver	**Synopsis :** { v3, v2, v1 } Spécifie la version IGMP du groupe de multidiffusion appris.
Reporter	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Spécifie l'adresse IP source qui rapporte l'inscription au groupe de multidiffusion.
Age	**Synopsis :** 0 à 7210 s Spécifie l'âge actuel du groupe de multidiffusion IP appris sur le port en secondes.

Si le tableau est vide,procédez comme suit :

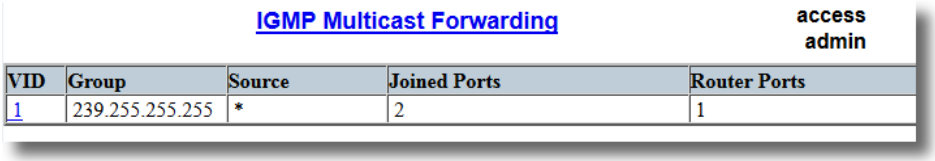
- Assurez-vous que le trafic est envoyé à l'appareil.
- Assurez-vous qu'IGMP est correctement configuré sur l'appareil. Pour plus d'informations, voir Section 5.8.1.4, « Configuration d'IGMP ».

Section 5.8.1.3

Affichage d'informations de transmission pour des groupes de multidiffusion

La transmission en multidiffusion d'informations pour chaque combinaison de source, groupe et VLAN apprise par RUGGEDCOM ROS est enregistrée dans le tableau IGMP Multicast Forwarding.

Pour afficher le tableau IGMP Multicast Forwarding table, accédez à ***Multicast Filtering » View IGMP Multicast Forwarding***. Le tableau **IGMP Multicast Forwarding** s'affiche.



VID	Group	Source	Joined Ports	Router Ports
1	239.255.255.255	*	2	1

Figure 159 : Tableau IGMP Multicast Forwarding

Ce tableau fournit les informations suivantes :

Paramètre	Description
VID	**Synopsis :** 0 à 65535 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
Group	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Adresse du groupe de multidiffusion.
Source	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### ou { * } Adresse source. * signifie toutes les adresses source possibles.
Joined Ports	**Synopsis :** Liste de ports séparée par des virgules Tous les ports recevant actuellement le trafic de multidiffusion pour le groupe de multidiffusion spécifié.

Paramètre	Description
Router Ports	**Synopsis :** Liste de ports séparée par des virgules Tous les ports ont été configurés manuellement ou découverts de manière dynamique (en observant le trafic spécifique au routeur) en tant que ports liés à des routeurs multidiffusion.

Si le tableau est vide,procédez comme suit :

- Assurez-vous que le trafic est envoyé à l'appareil.
- Assurez-vous qu'IGMP est correctement configuré sur l'appareil. Pour plus d'informations, voir Section 5.8.1.4, « Configuration d'IGMP ».

Section 5.8.1.4

Configuration d'IGMP

Procédez comme suit pour configurer l'IGMP :

1. Assurez-vous qu'un ou plusieurs VLAN statiques avec IGMP activé existent : Pour plus d'informations, voir Section 5.1.5, « Gestion de VLAN statiques ».
2. Accédez à ***Multicast Filtering » Configure IGMP Parameters***. Le formulaire **IGMP Parameters** s'affiche.

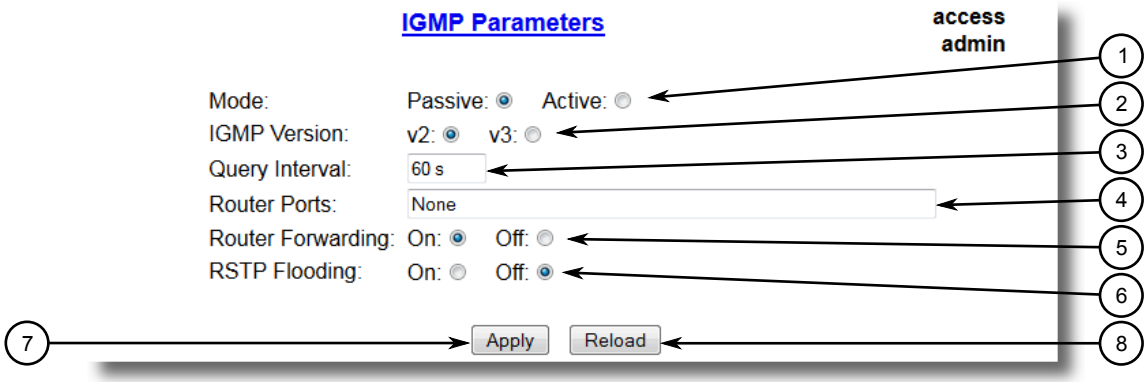


Figure 160 : Formulaire IGMP Parameters

1. Options Mode **2.** IGMP Version **3.** Zone Query Interval **4.** Zone Router Ports **5.** Options Router Forwarding **6.** Options RSTP Flooding **7.** Bouton Apply **8.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Mode	**Synopsis :** { Passive, Active } **Par défaut :** Passive Spécifie le mode IGMP. Options possibles : • `PASSIVE` – le commutateur espionne de manière passive le trafic IGMP et n'envoie jamais de requêtes IGMP • `ACTIVE` – le commutateur génère des requêtes IGMP si aucune requête d'un meilleur candidat demandeur n'est détectée pendant un certain temps.
IGMP Version	**Synopsis :** { v2, v3 } **Par défaut :** v2 Spécifie la version IGMP configurée pour le commutateur. Options possibles :

Paramètre	Description
	• `v2` – définit la version IGMP sur la version 2. Lorsqu'ils sont sélectionnés pour un commutateur espion, tous les rapports et toutes les requêtes IGMP dont la version est supérieure à v2 sont transmis, mais ils ne sont pas ajoutés au tableau IGMP Multicast Forwarding. • `v3` – définit la version IGMP sur la version 3. Les requêtes générales sont générées au format IGMPv3, toutes les versions des messages IGMP sont traitées par le commutateur, et le trafic est réduit en fonction de l'adresse de groupe multidiffusion uniquement.
Query Interval	**Synopsis :** 10 à 3600 **Par défaut :** 60 s L'intervalle de temps entre les requêtes IGMP générées par le commutateur. **REMARQUE** *Ce paramètre affecte également le Group Membership Interval (c'est-à-dire le temps de vieillissement d'abonné de groupe). Il prend donc effet même en mode PASSIVE.*
Router Ports	**Synopsis :** Liste de ports séparée par des virgules **Par défaut :** None Ce paramètre spécifie les ports se connectant aux routeurs multidiffusion. Si vous ne configurez pas de ports de routeur connus, le commutateur peut être en mesure de les détecter, mais il est recommandé de les préconfigurer.
Router Forwarding	**Synopsis :** { Off, On } **Par défaut :** On Ce paramètre spécifie si les flux multidiffusion sont toujours transmis vers des routeurs multicast.
RSTP Flooding	**Synopsis :** { Off, On } **Par défaut :** Off Ce paramètre spécifie si les flux multidiffusion s'écoulent hors de tous les ports non-périphériques RSTP en cas de détection d'une modification de la topologie. Une telle avalanche est souhaitée si la garantie d'un flux multidiffusion en cas de modification de la topologie est la priorité.

4. Cliquez sur **Apply**.

Section 5.8.2

Gestion de GMRP

Le GMRP est une application du GARP (Generic Attribute Registration Protocol) fournissant un mécanisme de couche 2 pour la gestion d'appartenances à des groupes de multidiffusion dans un réseau de couche 2 ponté. Il permet aux commutateurs Ethernet et aux stations terminales d'inscrire et de désinscrire une appartenance dans des groupes de multidiffusion avec d'autres commutateurs sur un LAN, et que ces informations soient diffusées sur tous les commutateurs dans le LAN qui prennent en charge les services de filtrage étendus.

GMRP est un protocole industriel standard défini dans IEEE 802.1D-1998 et étendu dans IEEE 802.1Q-2005. GARP a été défini dans IEEE 802.1D-1998 et mis à jour dans 802.1D-2004.

REMARQUE
GMRP fournit dans la couche 2 une fonctionnalité similaire à celle fournie par IGMP dans la couche 3.

SOMMAIRE

- Section 5.8.2.1, « Concepts GMRP »
- Section 5.8.2.2, « Affichage d'un résumé de groupes de multidiffusion »
- Section 5.8.2.3, « Configuration globale du GMRP »
- Section 5.8.2.4, « Configuration de GMRP pour des ports Ethernet spécifiques »
- Section 5.8.2.5, « Affichage d'une liste de groupes de multidiffusion statiques »
- Section 5.8.2.6, « Ajout d'un groupe multidiffusion statique »
- Section 5.8.2.7, « Suppression d'un groupe de multidiffusion statique »

Section 5.8.2.1

Concepts GMRP

La présente rubrique décrit certains concepts importants de la mise en œuvre du filtrage de multidiffusion à l'aide de GMRP :

Joindre un groupe de multidiffusion

Pour joindre un groupe de multidiffusion, une station terminale transmet un message GMRP *join*. Le commutateur qui reçoit le message *join* ajoute le port via lequel le message a été reçu au groupe de multidiffusion spécifié dans le message. Il propage ensuite le message *join* à tous les autres hôtes dans le VLAN, dont l'un devrait être la source de multidiffusion.

Lorsqu'un commutateur transmet des mises à jour GMRP (depuis des ports compatibles GMRP), tous les groupes connus du commutateur (qu'ils soient configurés manuellement ou appris dynamiquement via GMRP) sont annoncés au reste du réseau.

Tant qu'un hôte dans le réseau de couche 2 est enregistré pour un groupe de multidiffusion donné, le trafic provenant de la source de multidiffusion correspondante est transporté sur le réseau. Le trafic multidiffusion par la source est uniquement transmis par chaque commutateur dans le réseau aux ports desquels il a reçu le message Join pour le groupe de multidiffusion.

Quitter un groupe de multidiffusion

Périodiquement, le commutateur envoie des demandes GMRP sous la forme d'un message *leave all*. Si un hôte (commutateur ou station terminale) souhaite rester dans un groupe de multidiffusion, il réaffirme son appartenance au groupe en répondant avec une demande *join* appropriée. Sinon, il peut répondre avec un message *leave* ou simplement ne pas répondre. Si le commutateur reçoit un message *leave* ou ne reçoit aucune réponse de l'hôte pendant un certain délai, le commutateur supprime l'hôte du groupe de multidiffusion.

Remarques sur GM

GMRP étant une application de GARP, les transactions s'effectuent à l'aide du protocole GARP. GMRP définit les deux types d'attributs suivants :

- le type d'attribut de groupe, utilisé pour identifier les valeurs d'adresses MAC de groupes,
- le type d'attribut de condition de service, utilisé pour identifier les conditions de service pour le groupe.

Les attributs de condition de service sont utilisés pour modifier le comportement de filtrage de multidiffusion du port récepteur en :

- transmettre tout le trafic de groupe de multidiffusion dans le VLAN ou
- transmettre tout le trafic inconnu (groupes de multidiffusion) pour lequel aucun membre n'est enregistré dans l'appareil dans un VLAN.

Si GMRP est désactivé, les paquets GMRP reçus sont transmis comme tout autre trafic. Sinon, les paquets GMRP sont traités et ne sont pas transmis.

Établir une appartenance à un groupe avec GMRP

L'exemple suivant illustre comment un réseau d'hôtes et de commutateurs peut joindre dynamiquement deux groupes de multidiffusion à l'aide de GMRP.

Dans ce scénario, il existe deux sources de multidiffusion (S1 et S2), qui exécutent respectivement la multidiffusion vers les groupes de diffusion 1 et 2. Un réseau avec cinq commutateurs, notamment un commutateur principal (B), connecte les sources à deux hôtes, H1 et H2, qui reçoivent les flux de multidiffusion respectivement de S1 et S2.

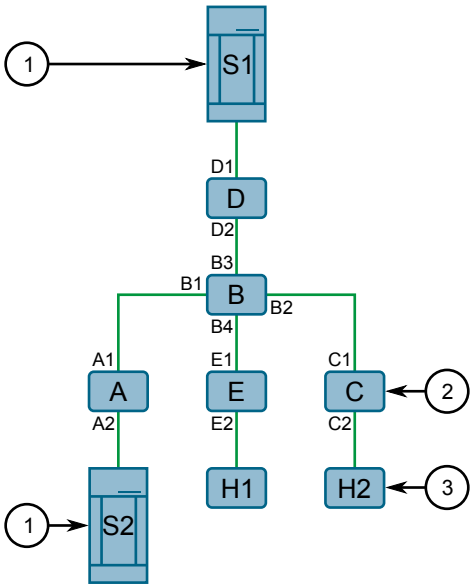


Figure 161 : Exemple - Établir une appartenance à un groupe avec GMRP

1. Source de multidiffusion **2.** Commutateur **3.** Hôte de multidiffusion

Les hôtes et les commutateurs établissent une appartenance aux groupes de multidiffusion 1 et 2 de la manière suivante :

1. L'hôte H1 ignore GMRP, mais doit voir le trafic du groupe de multidiffusion 1. Pour cette raison, le port E2 sur le commutateur E est configuré de manière statique de manière à transmettre le trafic du groupe de multidiffusion 1.
2. Le commutateur E annonce l'appartenance au groupe de multidiffusion 1 dans le réseau via le port E1, faisant ainsi du port B4 sur le commutateur B un membre du groupe de multidiffusion 1.

3. Le commutateur B propage le message *join*, et les ports A1, C1 et D1 deviennent alors des membres du groupe de multidiffusion 1.
4. L'hôte H2 tient compte de GMRP et envoie une demande *join* pour le groupe de multidiffusion 2 au port C2, qui devient alors membre du groupe de multidiffusion 2.
5. Le commutateur C propage le message *join*, et les ports A1, B2, D1 et E1 deviennent alors des membres du groupe de multidiffusion 2.

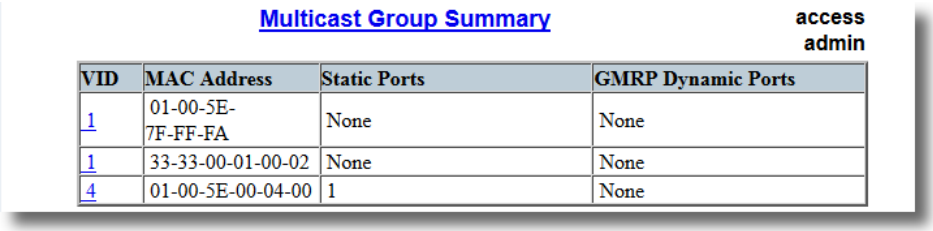
Une fois que l'inscription basée sur GMRP est propagée dans le réseau, le trafic de multidiffusion provenant de S1 et S2 peut atteindre sa destination de la manière suivante :

- La source S1 transmet le trafic de multidiffusion au port D2, qui est transmis via le port D1, lui-même devenu membre du groupe de multidiffusion 1.
- Le commutateur B transmet le groupe de multidiffusion 1 via le port B4 vers le commutateur E.
- Le commutateur E transmet le groupe de multidiffusion 1 via le port E2, qui a été configuré de manière statique pour appartenir au groupe de multidiffusion 1.
- L'hôte H1, qui est connecté au port E2, reçoit donc le groupe de multidiffusion 1.
- La source S2 transmet le trafic de multidiffusion au port A2, qui est transmis via le port A1, lui-même devenu membre du groupe de multidiffusion 2.
- Le commutateur B transmet le groupe de multidiffusion 2 via le port B2 vers le commutateur C.
- Le commutateur C transmet le groupe de multidiffusion 2 via le port C2, lui-même devenu membre du groupe 2.
- Enfin, l'hôte H2, qui est connecté au port C2, reçoit le groupe de multidiffusion 2.

Section 5.8.2.2

Affichage d'un résumé de groupes de multidiffusion

Pour afficher un résumé de groupes de multidiffusion, accédez à ***Multicast Filtering » View Multicast Group Summary***. Le tableau **Multicast Group Summary** s'affiche.



Multicast Group Summary

access admin

VID	MAC Address	Static Ports	GMRP Dynamic Ports
1	01-00-5E-7F-FF-FA	None	None
1	33-33-00-01-00-02	None	None
4	01-00-5E-00-04-00	1	None

Figure 162 : Tableau Multicast Group Summary

Ce tableau fournit les informations suivantes :

Paramètre	Description
VID	**Synopsis :** 0 à 65535 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
MAC Address	**Synopsis :** ##-##-##-##-##-## avec une plage de 0 à FF pour ## Adresse MAC de groupe multidiffusion.
Static Ports	**Synopsis :** toute combinaison de nombres valide pour ce paramètre

Paramètre	Description
	Ports ayant joint ce groupe statiquement via une configuration statique dans le tableau Static MAC vers lesquels le trafic du groupe de multidiffusion est transmis.
GMRP Dynamic Ports	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Ports ayant joint ce groupe dynamiquement via une application GMRP vers lesquels le trafic du groupe de multidiffusion est transmis.

Section 5.8.2.3

Configuration globale du GMRP

Procédez comme suit pour configurer des réglages globaux pour GMRP :

1. Accédez à ***Multicast Filtering » Configure Global GMRP Parameters***. Le formulaire **Global GMRP Parameters** s'affiche.

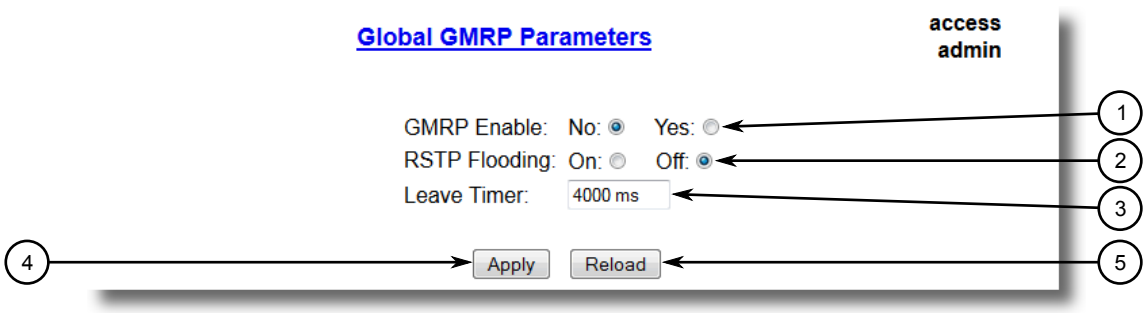


Figure 163 : Formulaire Global GMRP Parameters

1. Options GMRP Enable **2.** Options RSTP Flooding **3.** Zone Leave Timer **4.** Bouton Apply **5.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
GMRP Enable	**Synopsis :** { No, Yes } **Par défaut :** No Activer ou désactiver GMRP globalement. Lorsque GMRP est désactivé globalement, les configurations GMRP sur des ports individuels sont ignorées. Lorsque GMRP est activé globalement, chaque port peut être configuré individuellement.
RSTP Flooding	**Synopsis :** { On, Off } **Par défaut :** Off Ce paramètre spécifie si les flux multidiffusion s'écoulent hors de tous les ports non-périphériques RSTP en cas de détection d'une modification de la topologie. Une telle avalanche est souhaitée si la garantie d'un flux multidiffusion en cas de modification de la topologie est la priorité.
Leave Timer	**Synopsis :** 600 à 300000 ms **Par défaut :** 4000 ms Temps d'attente (en millisecondes) après la génération de la commande Leave ou LeaveAll avant la suppression de groupes de multidiffusion inscrits. Si des messages Join pour des adresses spécifiques sont reçus avant expiration de ce délai, les adresses restent enregistrées.

3. Cliquez sur **Apply**.

Section 5.8.2.4

Configuration de GMRP pour des ports Ethernet spécifiques

Procédez comme suit pour configurer GMRP pour un port Ethernet spécifique :

1. Assurez-vous que les paramètres globaux pour GMRP ont été configurés. Pour plus d'informations, voir Section 5.8.2.3, « Configuration globale du GMRP ».
2. Accédez à ***Multicast Filtering » Configure Port GMRP Parameters***. Le tableau **Port GMRP Parameters** s'affiche.

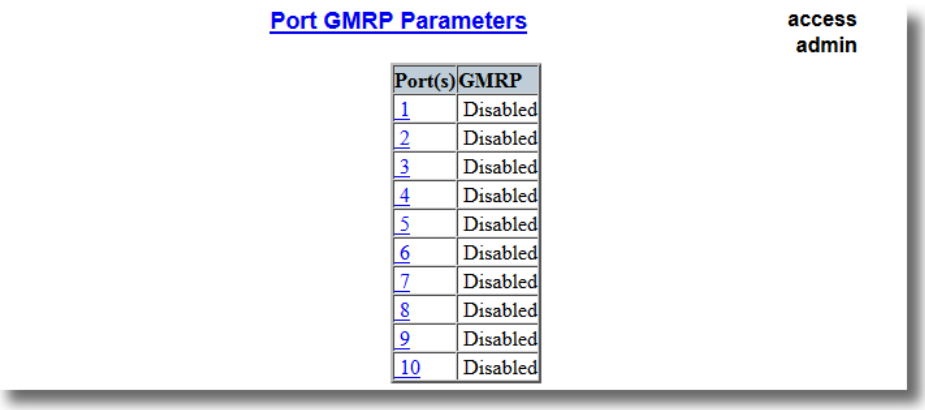


Figure 164 : Tableau Port GMRP Parameters

3. Sélectionnez un port Ethernet. Le formulaire **Port GMRP Parameters** s'affiche.

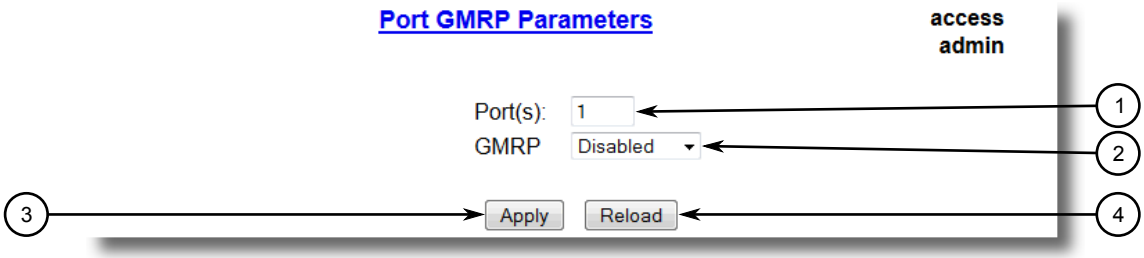


Figure 165 : Formulaire Port GMRP Parameters

1. Zone Port(s) **2.** Liste GMRP **3.** Bouton Apply **4.** Bouton Reload

4. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port(s)	**Synopsis :** toute combinaison de nombres valide pour ce paramètre Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur (comme une liste de ports s'ils sont agrégés).
GMRP	**Synopsis :** { Disabled, Adv Only, Adv&Learn }

Paramètre	Description
	Par défaut : Par défaut : Disabled Configure le fonctionnement de GMRP (GARP Multicast Registration Protocol) sur le port. Il existe plusieurs modes de fonctionnement GMRP : • DISABLED - le port n'est capable d'aucun traitement GMRP. • ADVERTISE ONLY - le port déclare toutes les adresses MCAST existantes dans le commutateur (configuré ou appris) mais n'apprend aucune adresse MACST. • ADVERTISE & LEARN - le port déclare toutes les adresses MCAST existantes dans le commutateur (configuré ou appris) et peut apprendre des adresses MCAST de manière dynamique.

5. Cliquez sur **Apply**.

Section 5.8.2.5

Affichage d'une liste de groupes de multidiffusion statiques

Pour afficher une liste de groupes de multidiffusion statiques, accédez à ***Multicast Filtering » Configure Static Multicast Groups***. Le tableau **Static Multicast Groups** s'affiche.

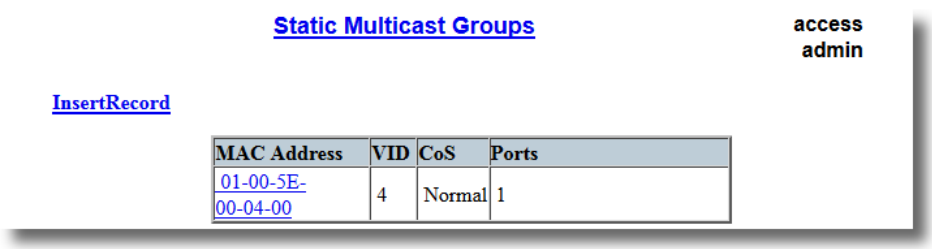


Figure 166 : Tableau Static Multicast Groups

Si aucun groupe de multidiffusion statique n'est répertorié, ajoutez le groupe. Pour plus d'informations, voir Section 5.8.2.6, « Ajout d'un groupe multidiffusion statique ».

Section 5.8.2.6

Ajout d'un groupe multidiffusion statique

Procédez comme suit pour ajouter un groupe multidiffusion statique depuis un autre appareil :

1. Accédez à ***Multicast Filtering » Configure Static Multicast Groups***. Le tableau **Static Multicast Groups** s'affiche.

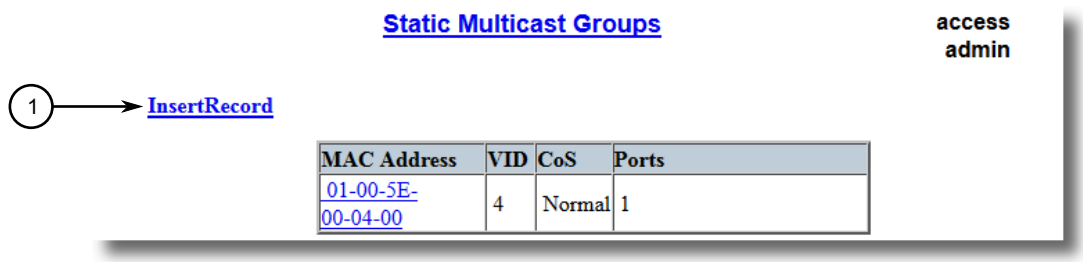


Figure 167 : Tableau Static Multicast Groups

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **Static Multicast Groups** s'affiche.

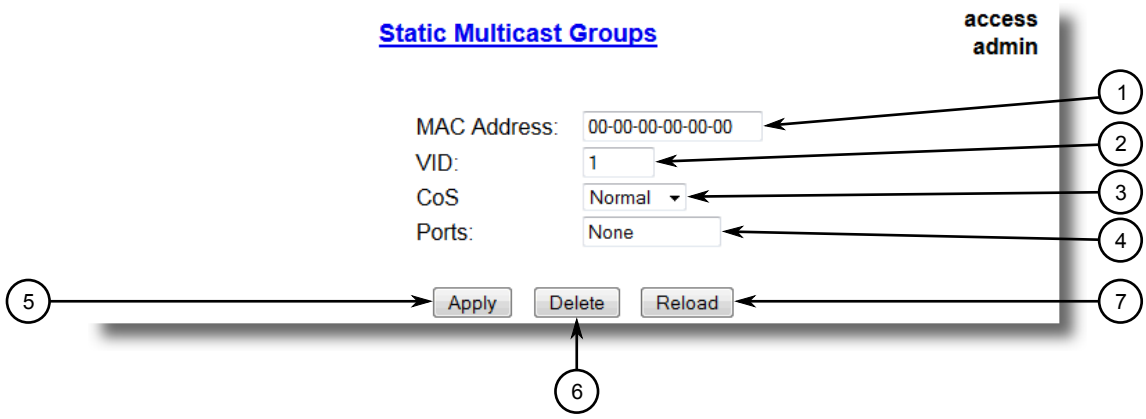


Figure 168 : Formulaire Static Multicast Groups

1. Zone MAC Address **2.** Zone VID **3.** Liste CoS **4.** Zone Ports **5.** Bouton Apply **6.** Bouton Delete **7.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
MAC Address	**Synopsis :** ##-##-##-##-##-## avec une plage de 0 à FF pour ## **Par défaut :** 00-00-00-00-00-00 Adresse MAC de groupe multidiffusion.
VID	**Synopsis :** 1 à 4094 **Par défaut :** 1 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
CoS	**Synopsis :** { N/A, Normal, Medium, High, Crit } **Par défaut :** N/A Priorise le trafic pour l'adresse MAC spécifiée. Si le trafic ne doit pas être priorisé sur la base de l'adresse, sélectionnez N/A.
Ports	**Synopsis :** toute combinaison de nombres valide pour ce paramètre **Par défaut :** None Ports vers lesquels le trafic du groupe multidiffusion est transmis.

4. Cliquez sur **Apply**.

Section 5.8.2.7

Suppression d'un groupe de multidiffusion statique

Procédez comme suit pour supprimer un groupe de multidiffusion statique :

1. Accédez à ***Multicast Filtering » Configure Static Multicast Groups***. Le tableau **Static Multicast Groups** s'affiche.

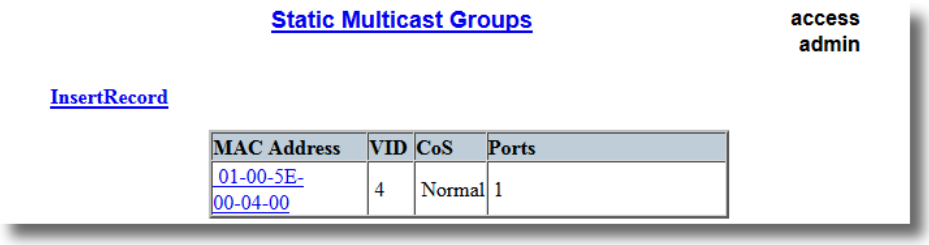


Figure 169 : Tableau Static Multicast Groups

2. Sélectionnez le groupe dans le tableau. Le formulaire **Static Multicast Groups** s'affiche.

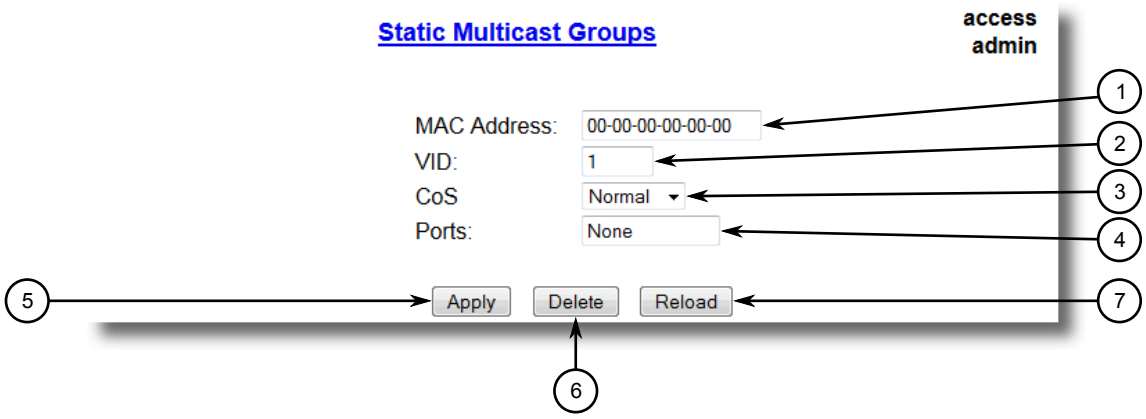


Figure 170 : Formulaire Static Multicast Groups

1. Zone MAC Address **2.** Zone VID **3.** Zone Priority **4.** Zone Ports **5.** Bouton Apply **6.** Bouton Delete **7.** Bouton Reload

3. Cliquez sur **Delete**.

Section 5.9

Gestion du DHCP Relay Agent (agent de relais DHCP)

Un DHCP Relay Agent (agent de relais DHCP) est un appareil qui transmet des paquets DHCP entre des clients et des serveurs lorsqu'ils ne se trouvent pas sur le même segment LAN physique ou le même sous-réseau IP. La fonctionnalité est activée si l'adresse IP du serveur DHCP et un ensemble de ports Ethernet sont configurés.

DHCP Option 82 fournit un mécanisme d'affectation d'une adresse IP basée sur l'emplacement de l'appareil client dans le réseau. Les informations concernant l'emplacement du client peuvent être envoyées avec la demande DHCP au serveur. En fonction de ces informations, le serveur DHCP prend une décision concernant une adresse IP à affecter.

Le DHCP Relay Agent prend les demandes de diffusion DHCP de clients reçues sur le port configuré et insère l'option d'information d'agent de relais (Option 82) dans le paquet. L'Option 82 contient l'ID de VLAN (2 octets) et le numéro de port du port client (2 octets : la sous-option ID de circuit), ainsi que l'adresse MAC de l'agent de relais (la sous-option ID distant). Ces informations définissent uniquement la position du client dans le réseau.

Le serveur DHCP prenant en charge l'Option 82 DHCP envoie une réponse de monodiffusion et répète l'Option 82. Le DHCP Relay Agent supprime le champ Option 82 et transmet le paquet vers le port duquel la demande originale a été reçue.

Ces paramètres permettent de configurer les informations sur la base du DHCP Relay Agent (Option 82) (Agent de relais DHCP).

SOMMAIRE

- Section 5.9.1, « Configuration du DHCP Relay Agent (agent de relais DHCP) »
- Section 5.9.2, « Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques »

Section 5.9.1

Configuration du DHCP Relay Agent (agent de relais DHCP)

Procédez comme suit pour configurer l'appareil comme DHCP Relay Agent (Option 82) :

1. Accédez à ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. Le formulaire **DHCP Parameters** s'affiche.

Figure 171 : Formulaire DHCP Parameters

1. Zone DHCP Server Address **2.** Bouton Apply **3.** Bouton Reload

2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
DHCP Server Address	**Synopsis :** ###.###.###.### avec une plage de 0 à 255 pour ### Adresse IP du serveur DHCP vers lequel les requêtes DHCP sont transmises. L'IP du serveur DHCP doit être configurée pour que l'agent de relais puisse fonctionner.

3. Cliquez sur **Apply**.
4. Activez le DHCP Relay Agent (Option 82) sur les ports connectés à un client DHCP. Pour plus d'informations, voir Section 5.9.2, « Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques ».

Section 5.9.2

Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques

Le DHCP Relay Agent (Option 82) peut être activé pour tout port Ethernet connecté à un client DHCP.

Procédez comme suit pour activer le DHCP Relay Agent (Option 82) (DHCP Relay Agent) :

1. Accédez à ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. Le tableau **DHCP Port Parameters** s'affiche.

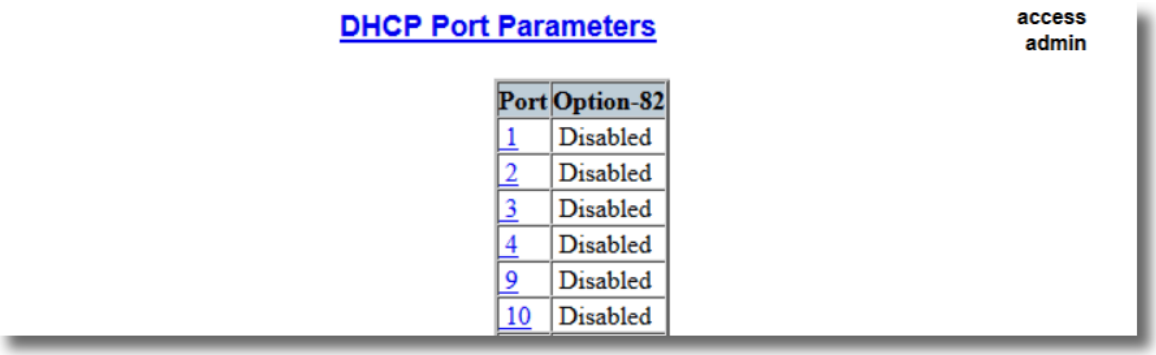


Figure 172 : Tableau DHCP Port Parameters

2. Sélectionnez un port. Le formulaire **DHCP Port Parameters** s'affiche.

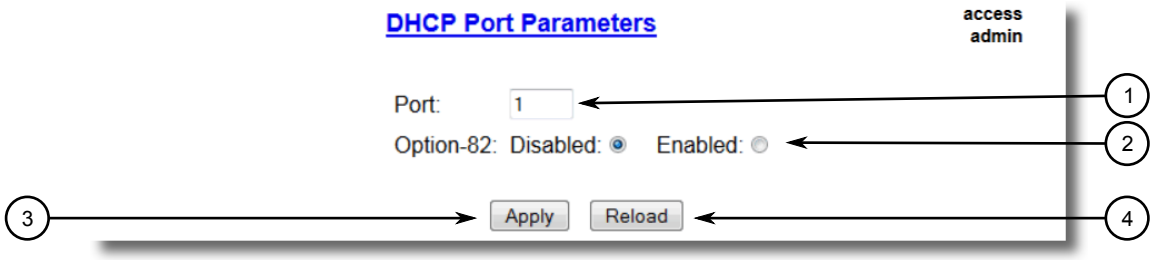


Figure 173 : Formulaire Port DCHP Parameters

1. Zone Port **2.** Options Option-82 **3.** Bouton Apply **4.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Option-82	**Synopsis :** { Disabled, Enabled } **Par défaut :** Disabled Insère l'option 82 DHCP.

4. Cliquez sur **Apply**.

Section 5.10

Gestion de la sécurité des ports (Port security)

Port security, ou le contrôle d'accès aux ports, donne la possibilité de filtrer ou d'accepter le trafic d'adresses MAC spécifiques.

Port security fonctionne en inspectant les adresses MAC source de trames reçues et en les validant sur la base de la liste d'adresses MAC autorisées par le port. Les trames non autorisées sont filtrées et, en option, la partie qui a reçu la trame peut être fermée de manière permanente ou pour un intervalle de temps spécifique. Une alarme est générée indiquant l'adresse MAC non autorisée détectée.

Les trames vers des adresses de destination inconnues s'écoulent vers des ports sécurisés.

SOMMAIRE

- Section 5.10.1, « Concept de sécurité de port »
- Section 5.10.2, « Affichage d'une liste d'adresses MAC autorisées »
- Section 5.10.3, « Configuration de la sécurité du port »
- Section 5.10.4, « Configuration d'IEEE 802.1X »

Section 5.10.1

Concept de sécurité de port

Cette section décrit certains concepts importants de la mise en œuvre de la sécurité de port dans RUGGEDCOM ROS :

SOMMAIRE

- Section 5.10.1.1, « Authentification basée sur des adresses MAC statiques »
- Section 5.10.1.2, « Authentification IEEE 802.1X. »
- Section 5.10.1.3, « Authentification IEEE 802.1X avec authentification basée sur l'adresse MAC »
- Section 5.10.1.4, « Affectation de VLAN avec attributs Tunnel »

Section 5.10.1.1

Authentification basée sur des adresses MAC statiques

Avec cette méthode, le commutateur valide les adresses MAC source de trames reçues en sur la base du contenu du tableau Static MAC Address.

RUGGEDCOM ROS prend également en charge une configuration de sécurité de ports hautement flexible qui fournit un moyen confortable aux administrateurs réseau d'utiliser la fonctionnalité dans différents scénarios de réseau.

Une adresse MAC statique peut être configurée sans que le numéro de port ne soit explicitement spécifié. Dans ce cas, l'adresse MAC configurée est automatiquement autorisée sur le port où elle est détectée. Cela permet aux appareils d'être connectés à tout port sécurisé sur le commutateur sans avoir besoin d'une reconfiguration.

Le commutateur peut également être programmé pour apprendre (et donc autoriser) un nombre préconfiguré de premières adresses MAC rencontrées sur un port sécurisé. Cela permet de capturer les adresses sécurisées appropriées lors de la première configuration de l'autorisation basée sur des adresses MAC sur un port. Ces adresses MAC sont automatiquement insérées dans le tableau Static MAC Address et y restent jusqu'à ce qu'elles soient explicitement supprimées par l'utilisateur.

Section 5.10.1.2

Authentification IEEE 802.1X.

Le norme IEEE 802.1x définit un mécanisme pour le contrôle d'accès au réseau basé sur des ports et fournit un moyen d'authentification et d'autorisation d'appareils attachés à des ports LAN.

Même si IEEE 802.1x est utilisé principalement dans des réseaux sans fil, cette méthode est également mise en œuvre dans des commutateurs câblés.

La norme IEEE 802.1x définit trois composants principaux de la méthode d'authentification : demandeur, authentificateur et serveur d'authentification. RUGGEDCOM ROS prend en charge le composant authentificateur.

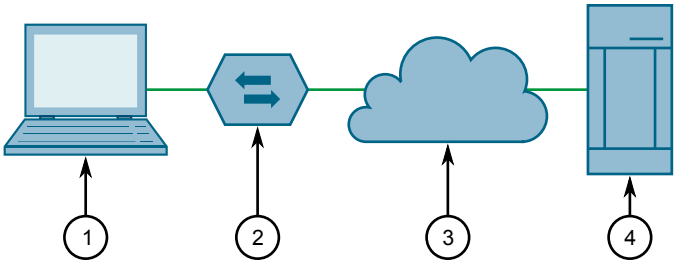


Figure 174 : Topologie générale de IEEE 802.1x

1. Demandeur **2.** Commutateur d'authentification **3.** LAN **4.** Serveur d'authentification

IMPORTANT !
RUGGEDCOM ROS prend en charge le PEAP (Protected Extensible Authentication Protocol) et EAP-MD5. PEAP est plus sécurisé et est recommandé s'il est disponible pour le demandeur.

IEEE 802.1x utilise l'EAP (Extensible Authentication Protocol), qui est un protocole d'authentification PPP générique prenant en charge différentes méthodes d'authentification. IEEE 802.1x définit un protocole pour la communication entre le demandeur et l'authentificateur, appelé EAP over LAN (EAPOL).

RUGGEDCOM ROS communique avec le serveur d'authentification à l'aide d'EAP over RADIUS.

REMARQUE
Le commutateur prend en charge l'authentification d'un hôte par port.

REMARQUE
Si l'adresse MAC de l'hôte est configurée dans le tableau Static MAC Address, elle est autorisée, même si l'authentification de l'hôte est rejetée par le serveur d'authentification.

Section 5.10.1.3

Authentification IEEE 802.1X avec authentification basée sur l'adresse MAC

Cette méthode, également appelée MAB (MAC-Authentication Bypass), est généralement utilisée pour des appareils tels que des téléphones VoIP et des imprimantes Ethernet ne prenant pas en charge le protocole 802.1x. Cette méthode permet à de tels appareils d'être authentifiés à l'aide de la même infrastructure de base de données que celle utilisée dans 802.1x.

IEEE 802.1X avec MAC-Authentication Bypass fonctionne de la manière suivante :

1. L'appareil se connecte à un port de commutateur.
2. Le commutateur apprend l'adresse MAC de l'appareil à la réception de la première trame de l'appareil (l'appareil envoie généralement un message de demande DHCP lors de la première connexion).
3. Le commutateur envoie un message de demande EAP à l'appareil et tente de démarrer l'authentification 802.1X.
4. Le commutateur est désactivé pendant l'attente de la réponse EAP car l'appareil ne prend pas en charge 802.1x.
5. Le commutateur envoie un message d'authentification au serveur d'authentification à l'aide de l'adresse MAC de l'appareil comme nom d'utilisateur et mot de passe.

6. Le commutateur authentifie ou rejette l'appareil en fonction de la réponse du serveur d'authentification.

Section 5.10.1.4

Affectation de VLAN avec attributs Tunnel

RUGGEDCOM ROS prend en charge l'affectation d'un VLAN au port autorisé à l'aide d'attributs de tunnel définis dans RFC 3580 [http://tools.ietf.org/html/rfc3580], lorsque le mode Port Security est réglé sur 802.1x ou 802.1x/MAC-Auth.

Dans certains cas, il est préférable d'autoriser le placement d'un port dans un VLAN spécifique sur la base du résultat de l'authentification. Par exemple :

- pour autoriser un appareil spécifique (sur la base de son adresse MAC) à rester sur le même VLAN pendant qu'il se déplace au sein d'un réseau, configurez les commutateurs pour le mode d'authentification 802.1X/MAC-Auth.
- Pour autoriser un utilisateur spécifique (sur la base de ses informations d'identification) à rester sur le même VLAN pendant qu'il se connecte depuis différents emplacements, configurez les commutateurs pour le mode 802.1X.

Si le serveur RADIUS souhaite utiliser cette fonctionnalité, il indique le VLAN souhaité en incluant des attributs de tunnel dans le message d'acceptation d'accès. Le serveur RADIUS utilise les attributs de tunnel suivants pour l'affectation de VLAN :

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Notez que le VLANID est 12 bits et a une valeur comprise entre 1 et 4094 inclus. Le Tunnel-Private-Group-ID est une chaîne de caractères définie dans RFC 2868 [http://tools.ietf.org/html/rfc2868], le nombre entier VLANID est donc codé en tant que chaîne de caractères.

Si les attributs de tunnel ne sont pas renvoyés par le serveur d'authentification, le VLAN affecté au port de commutation reste inchangé.

Section 5.10.2

Affichage d'une liste d'adresses MAC autorisées

Pour afficher une liste d'adresses MAC statiques apprises de ports sécurisés, accédez à ***Network Access Control » Port Security » View Authorized MAC Addresses***. Le tableau **Authorized MAC Addresses** s'affiche.

REMARQUE
Seules les adresses MAC autorisées sur des ports MAC statiques sont affichées. Les adresses MAC avec IEEE 802.1X ne sont pas affichées.

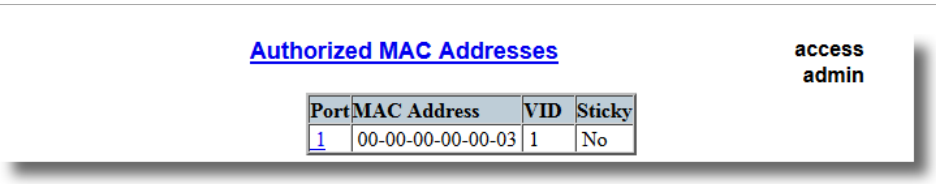


Figure 175 : Tableau Authorized MAC Addresses

Ce tableau affiche les informations suivantes :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum Port sur lequel l'adresse MAC a été apprise.
MAC Address	**Synopsis :** ##-##-##-##-##-## avec une plage de 0 à FF pour ## Adresse MAC autorisée apprise par le commutateur.
VID	**Synopsis :** 0 à 65535 Identificateur VLAN du VLAN sur la base duquel l'adresse MAC est exécutée.
Sticky	**Synopsis :** { No, Yes } Ce paramètre décrit si l'adresse MAC autorisée/l'appareil autorisé peut se déplacer vers un autre port ou non : • YES - l'adresse MAC autorisée/l'appareil autorisé ne peut pas se déplacer vers un autre port de commutateur • NO - l'adresse MAC autorisée/l'appareil autorisé peut se déplacer vers un autre port de commutateur

Procédez comme suit si aucune adresse MAC n'est répertoriée :

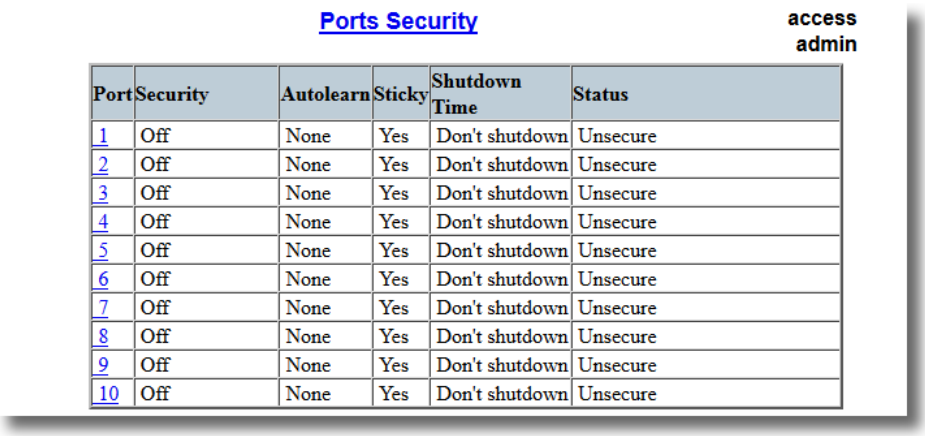
- Configurez la sécurité de port. Pour plus d'informations, voir Section 5.10.3, « Configuration de la sécurité du port ».
- Configurez IEEE 802.1X. Pour plus d'informations, voir Section 5.10.4, « Configuration d'IEEE 802.1X ».

Section 5.10.3

Configuration de la sécurité du port

Procédez comme suit pour configurer la sécurité du port :

1. Accédez à ***Network Access Control » Port Security » Configure Ports Security***. Le tableau **Ports Security** s'affiche.



Ports Security

access admin

Port	Security	Autolearn	Sticky	Shutdown Time	Status
1	Off	None	Yes	Don't shutdown	Unsecure
2	Off	None	Yes	Don't shutdown	Unsecure
3	Off	None	Yes	Don't shutdown	Unsecure
4	Off	None	Yes	Don't shutdown	Unsecure
5	Off	None	Yes	Don't shutdown	Unsecure
6	Off	None	Yes	Don't shutdown	Unsecure
7	Off	None	Yes	Don't shutdown	Unsecure
8	Off	None	Yes	Don't shutdown	Unsecure
9	Off	None	Yes	Don't shutdown	Unsecure
10	Off	None	Yes	Don't shutdown	Unsecure

Figure 176 : Tableau Ports Security

2. Sélectionnez un port Ethernet. Le formulaire **Ports Security** s'affiche.

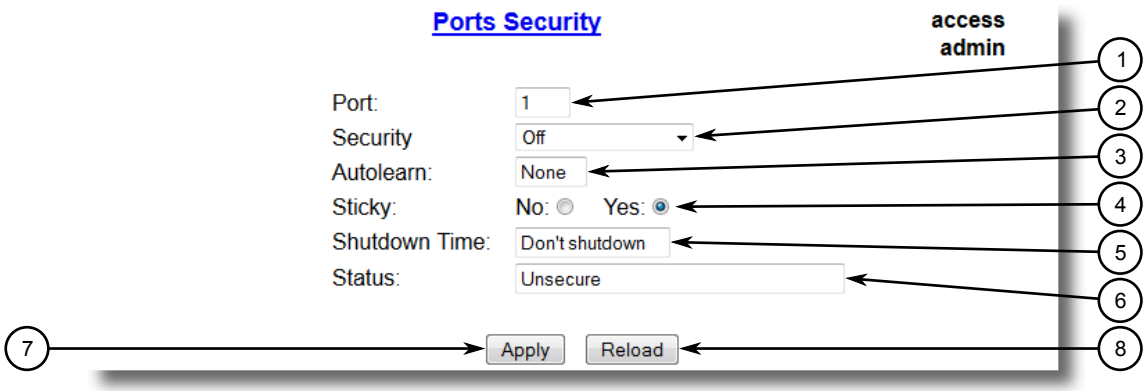


Figure 177 : Formulaire Ports Security

1. Zone Port **2.** Liste Security **3.** Zone Autolearn **4.** Options Sticky **5.** Zone Shutdown Time **6.** Zone Status **7.** Bouton Apply **8.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
Security	**Synopsis :** { Off, Static MAC, 802.1X, 802.1x/MAC-Auth } **Par défaut :** Off Active ou désactive la fonctionnalité de sécurité du port. Deux types de contrôle d'accès au port sont disponibles : • Basé sur l'adresse MAC statique. Avec cette méthode, les adresses MAC autorisées doivent être configurées dans le tableau Static MAC Address. Si certaines adresses MAC ne sont pas connues à l'avance (ou si l'utilisateur ne sait pas à quel port elles seront connectées), il est toujours possible de configurer le commutateur de manière à apprendre automatiquement un certain nombre d'adresses MAC. Une fois l'apprentissage terminé, elles ne vieillissent pas jusqu'à ce que l'unité soit réinitialisée ou si la liaison est défaillante. • Authentification standard IEEE 802.1X. • IEEE 802.1X avec authentification MAC, également appelée MAC-Authentication Bypass. Avec cette option, l'appareil peut authentifier des clients sur la base de leur adresse MAC si l'authentification IEEE 802.1X expire.
Autolearn	**Synopsis :** 1 à 16 ou { None } **Par défaut :** None Applicable uniquement si le champ 'Security' a été défini sur 'Static MAC'. Il spécifie le nombre maximum d'adresses MAC pouvant être apprises dynamiquement sur le port. Si des adresses statiques sont configurées sur le port, le nombre effectif d'adresses autorisées à être apprises est ce nombre moins le nombre d'adresses MAC statiques.
Sticky	**Synopsis :** { No, Yes } **Par défaut :** Oui Applicable uniquement si le champ 'Security' a été défini sur 'Static MAC'. Modifie le comportement du port afin qu'il soit 'sticky' ou 'non-sticky'. Si le paramètre est défini sur 'Yes', les MAC/appareils autorisés sur le port restent sur le port et le commutateur ne permet pas leur déplacement vers un autre port. Si le paramètre est défini sur 'No', les MAC/appareils autorisés sur le port peuvent être déplacés vers un autre port.

Paramètre	Description
Shutdown Time	**Synopsis :** 1 à 86400 s ou { Until reset, Don't shutdown } **Par défaut :** Don't shutdown Spécifie la durée d'arrêt du port en cas de violation de sécurité.
Status	**Synopsis :** 31 caractères quelconques Décrit l'état de sécurité du port.

REMARQUE
Il existe quelques cas dans lesquels des adresses MAC statiques peuvent être déplacées :

- *Lorsque la liaison est activée/désactivée sur un port sécurisé* ***non-sticky***
- *Lorsque le trafic commute sur un port sécurisé* ***non-sticky***

REMARQUE
Le trafic est perdu jusqu'à ce que l'adresse MAC source du trafic entrant soit autorisé par rapport au tableau Static MAC address.

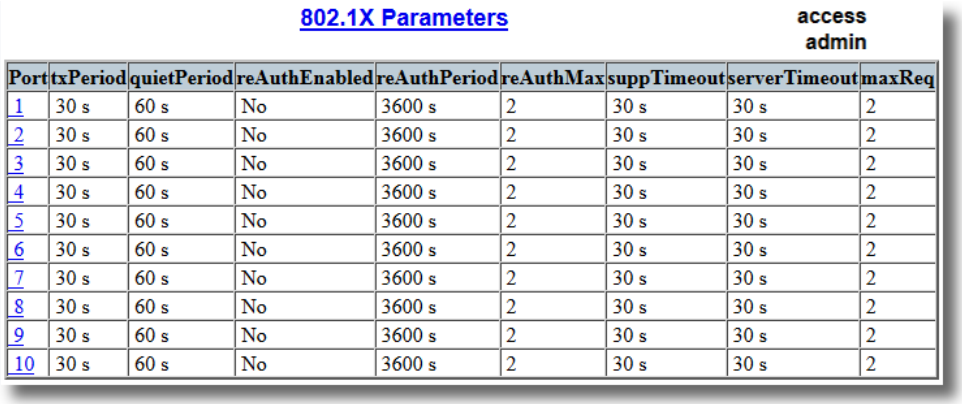
4. Cliquez sur **Apply**.

Section 5.10.4

Configuration d'IEEE 802.1X

Procédez comme suit pour configurer l'authentification IEEE 802.1X basée sur des ports :

1. Accédez à ***Network Access Control » Port Security » Configure 802.1X***. Le tableau **802.1X Parameters** s'affiche.



802.1X Parameters

access admin

Port	txPeriod	quietPeriod	reAuthEnabled	reAuthPeriod	reAuthMax	suppTimeout	serverTimeout	maxReq
1	30 s	60 s	No	3600 s	2	30 s	30 s	2
2	30 s	60 s	No	3600 s	2	30 s	30 s	2
3	30 s	60 s	No	3600 s	2	30 s	30 s	2
4	30 s	60 s	No	3600 s	2	30 s	30 s	2
5	30 s	60 s	No	3600 s	2	30 s	30 s	2
6	30 s	60 s	No	3600 s	2	30 s	30 s	2
7	30 s	60 s	No	3600 s	2	30 s	30 s	2
8	30 s	60 s	No	3600 s	2	30 s	30 s	2
9	30 s	60 s	No	3600 s	2	30 s	30 s	2
10	30 s	60 s	No	3600 s	2	30 s	30 s	2

Figure 178 : Tableau 802.1X Parameters

2. Sélectionnez un port Ethernet. Le formulaire **802.1X Parameters** s'affiche.

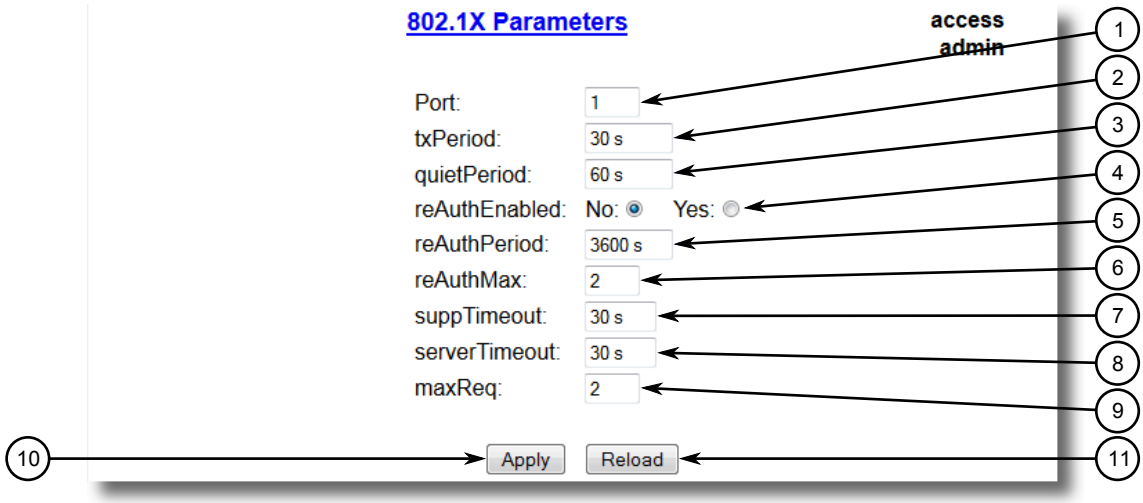


Figure 179 : Formulaire 802.1X Parameters

1. Zone Port **2.** Zone tX Period **3.** Zone quietPeriod **4.** Options reAuthEnabled **5.** Zone reAuthPeriod **6.** Zone reAuthMax **7.** Zone suppTimeout **8.** Zone serverTimeout **9.** Zone maxReq **10.** Bouton Apply **11.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Port	**Synopsis :** 1 au numéro de port maximum **Par défaut :** 1 Numéro de port indiqué par sérigraphie sur la plaque frontale du commutateur.
txPeriod	**Synopsis :** 1 à 65535 **Par défaut :** 30 s Temps d'attente avant la retransmission d'un paquet de réponse/identité EAP du demandeur.
quietPeriod	**Synopsis :** 0 à 65535 **Par défaut :** 60 s Intervalle de temps pendant lequel aucune tentative d'acquisition d'un demandeur n'est effectuée après l'échec d'une session d'autorisation.
reAuthEnabled	**Synopsis :** { No, Yes } **Par défaut :** No Active ou désactive la réauthentification périodique.
reAuthPeriod	**Synopsis :** 60 à 86400 **Par défaut :** 3600 s Intervalle entre les réauthentifications périodiques du demandeur.
reAuthMax	**Synopsis :** 1 à 10 **Par défaut :** 2 Nombre de tentatives de réauthentification admissible avant que le port ne soit plus autorisé.
suppTimeout	**Synopsis :** 1 à 300 **Par défaut :** 30 s Temps d'attente de la réponse du demandeur pour le paquet EAP du serveur d'authentification.

Paramètre	Description
serverTimeout	**Synopsis :** 1 à 300 **Par défaut :** 30 s Temps d'attente de la réponse du serveur d'authentification pour le paquet EAP du demandeur.
maxReq	**Synopsis :** 1 à 10 **Par défaut :** 2 Nombre maximum de retransmissions du paquet de demande EAP du serveur d'authentification au demandeur avant l'expiration de la session d'authentification.

4. Cliquez sur **Apply**.

Section 5.11

Gestion de l'agrégation de liaisons

L'agrégation de liaisons, également appelée port trunking ou port bundling, donne la possibilité d'agréger ou de rassembler plusieurs ports Ethernet dans une liaison logique (port trunk, agrégation de ports) avec une bande passante plus élevée. Cela permet un équilibrage de charge hautement aléatoire entre les liaisons agrégées sur la base des adresses MAC source et de destination des trames transmises.

L'agrégation de liaisons peut être utilisées dans deux buts :

- Pour obtenir une largeur de bande de liaison augmentée et linéairement incrémentielle.
- Pour améliorer la fiabilité du réseau en créant une redondance de liaisons. Si l'une des liaisons agrégées est défaillante, le commutateur répartit le trafic entre les liaisons restantes.

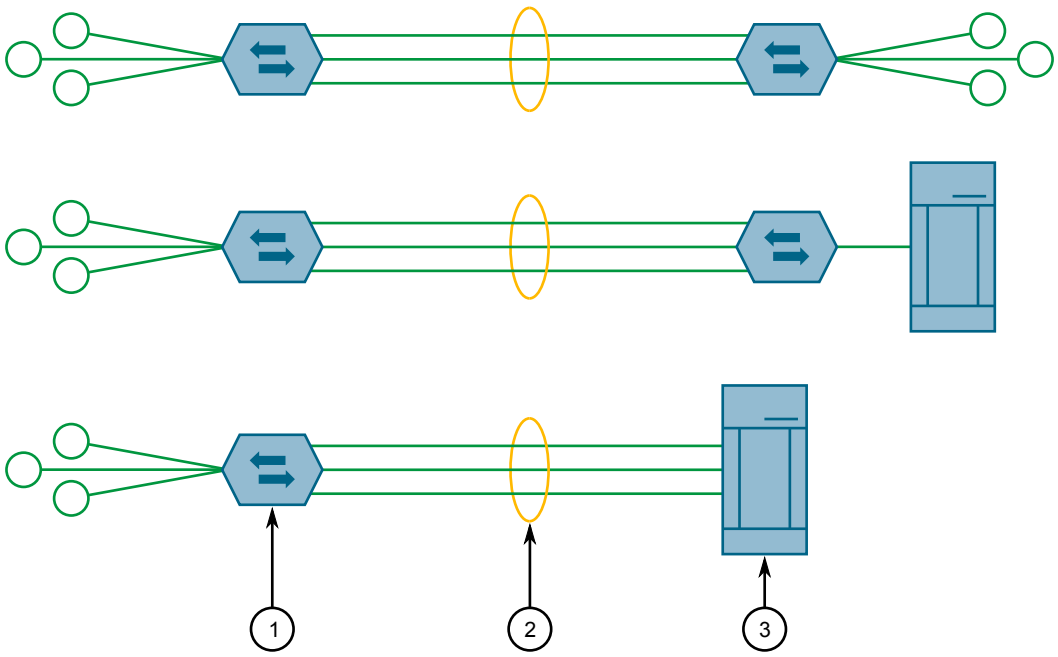


Figure 180 : Exemples d'agrégation de liaisons

1. Commutateur **2.** Serveur

RUGGEDCOM ROS permet la configuration de jusqu'à 15 agrégations de ports sur un appareil composées chacune de jusqu'à 8 ports.

REMARQUE
Le nombre maximum d'agrégations de ports pour chaque appareil dépend du nombre de ports disponibles. Au moins deux ports sont requis pour configurer une agrégation de ports.

REMARQUE
Le port agrégé avec le numéro de port le plus bas est appelé port principal de l'agrégation de ports. Les autres interfaces dans l'agrégation de ports sont appelées ports secondaires.

SOMMAIRE

- Section 5.11.1, « Concepts d'agrégation de liaisons »
- Section 5.11.2, « Gestion d'agrégations de ports »

Section 5.11.1

Concepts d'agrégation de liaisons

La présente rubrique décrit certains concepts importants de la mise en œuvre de l'agrégation de liaisons dans RUGGEDCOM ROS :

SOMMAIRE

- Section 5.11.1.1, « Règles et limitations »
- Section 5.11.1.2, « Agrégation de liaisons et fonctionnalités de couche 2 »
- Section 5.11.1.3, « Agrégation de liaisons et fonctionnalités de couche physique »

Section 5.11.1.1

Règles et limitations

La mise en œuvre d'une d'agrégation de liaisons doit respecter les règles et limitations suivantes :

- Chaque port ne peut appartenir qu'à une agrégation de ports à la fois.
- Un port cible de la mise en miroir de ports ne peut pas être membre de l'agrégation de ports. Cependant, un port source de la mise en miroir de ports peut être membre d'une agrégation de ports.
- Si seul un port QinQ est pris en charge par le commutateur, le port fonctionnant en mode QinQ ne peut pas être un membre secondaire d'une agréation de ports.
- Le port client DHCP Relay Agent (agent de relais DHCP) ne peut pas être membre d'une agrégation de ports.
- L'équilibrage de charge entre les liaisons d'un bundle est aléatoire et peut ne pas être optimal. Par exemple, si trois liaisons 100 Mbit/s sont agrégées, la largeur de bande résultant de l'agrégation de ports peut ne pas être précisément 300 Mbit/s.
- Une adresse MAC statique ne doit pas être configurée de manière à ce qu'elle se trouve sur un port agrégé - cela peut entraîner l'abandon de trames destinées à cette adresse.
- Un port sécurisé ne peut pas être membre d'une agrégation de ports.

- La norme d'agrégation de liens IEEE 802.3ad nécessite que toutes les liaisons physiques dans l'agrégation de ports s'exécutent à la même vitesse et en mode duplex intégral. Si cette condition n'est pas remplie, la performance de l'agrégation de ports diminue.

  Le commutateur génère une alarme correspondante en cas de détection d'une telle incompatibilité vitesse/duplex.
- STP calcule de manière dynamique le coût de chemin de l'agrégation de ports sur la base de sa largeur de bande agrégée. Cependant, si les ports agrégés fonctionnent à des vitesses différentes, le coût de chemin peut ne pas être calculé correctement.
- L'activation de STP est le meilleur moyen de traiter la redondance de liaisons dans des connexions commutateur à commutateur de plusieurs liaisons physiques. Si STP est activé et qu'une largeur de bande accrue n'est pas nécessaire, l'agrégation de liaisons ne doit pas être utilisée car elle entraîne une augmentation du temps de commutation.

Section 5.11.1.2

Agrégation de liaisons et fonctionnalités de couche 2

Les fonctionnalités de couche 2 (par ex. STP, VLAN, CoS, filtrage de multidiffusion) traitent une agrégation de ports comme une liaison unique.

- Si le Spanning Tree Protocol (STP) met un port agrégé en mode de blocage/transmission, il le fait dans l'agrégation de liaisons complète.
- Si l'un des ports agrégés joint/quitte un groupe de multidiffusion (par ex. viaIGMP ouGMRP), tous les autres ports dans le trunk joignent ou quittent également le groupe.
- Toute modification de paramètre de configuration de port (par ex. VLAN, CoS) est automatiquement appliquée à tous les ports du trunk.
- Les paramètres de configuration/d'état des ports secondaires ne sont pas affichés et leurs numéros de port sont simplement indiqués à côté du numéro de port principal dans les sessions d'interface de configuration/d'état appropriées.
- Lorsqu'un port secondaire et ajouté à une agrégation de ports, il hérite de tous les réglages de configuration du port principal. Lorsque ce port secondaire est supprimé de l'agrégation de ports, les réglages qu'il avait avant l'agrégation sont restaurés.

Section 5.11.1.3

Agrégation de liaisons et fonctionnalités de couche physique

Les fonctionnalités de couche physique (par exemple la configuration de liaisons physiques, l'état de liaisons, la limitation du débit, les statistiques Ethernet) traitent chaque port agrégé séparément.

- Les paramètres de configuration/d'état physiques ne sont PAS automatiquement appliqués à d'autres ports dans le trunk et sont affichés comme à l'accoutumée pour chaque port.
- Assurez-vous que seuls les ports avec la même vitesse et réglages de duplex sont agrégés. Si la négociation automatique est utilisée, assurez-vous qu'elle est résolue à la même vitesse pour tous les ports de l'agrégation de ports.
- Pour obtenir une valeur de compteur de statistiques Ethernet pour l'agrégation de ports, ajoutez les valeurs des compteurs pour tous les ports dans l'agrégation de ports.

Section 5.11.2

Gestion d'agrégations de ports

Cette section décrit la manière de gérer des agrégations de ports.

SOMMAIRE

- Section 5.11.2.1, « Affichage d'une liste d'agrégations de ports »
- Section 5.11.2.2, « Ajout d'une agrégation de ports »
- Section 5.11.2.3, « Suppression d'une agrégation de ports »

Section 5.11.2.1

Affichage d'une liste d'agrégations de ports

Pour afficher une liste d'agrégations de ports configurées sur l'appareil, accédez à ***Link Aggregation » Configure Port Trunks***. Le tableau **Port Trunks** s'affiche.

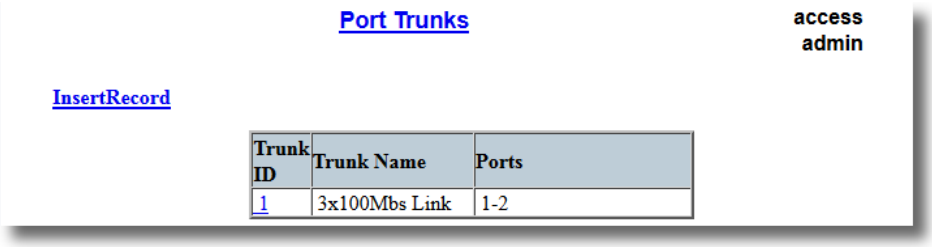


Figure 181 : Tableau Port Trunks

Si aucune agrégation de ports n'a été configurée, ajoutez des agrégations en fonction de vos besoins. Pour plus d'informations, voir Section 5.11.2.2, « Ajout d'une agrégation de ports ».

Section 5.11.2.2

Ajout d'une agrégation de ports

Procédez comme suit pour ajouter une agrégation de ports :

IMPORTANT !

L'agrégation de ports doit être correctement configurée des deux côtés du lien agrégé. Si la configuration ne correspond pas sur les deux côtés dans des connexions de commutateur à commutateur (c'est-à-dire que certains ports ne sont pas inclus dans l'agrégation de ports alors qu'ils devraient l'être), il en résultera une boucle. Par conséquent, la procédure de configuration suivante d'une agrégation de ports est recommandée :

a. Déconnectez ou désactivez tous les ports intervenant dans la configuration, c'est-à-dire qui sont en cours d'ajout ou de suppression dans l'agrégation de ports.

b. Configurez l'agrégation de ports sur les deux commutateurs.

c. Vérifiez l'agrégation de ports sur les deux commutateurs.

d. Reconnectez ou activez de nouveau les ports.

Si l'agrégation de ports est en cours de configuration alors que les ports ne sont pas déconnectés ou désactivés, ces derniers seront désactivés automatiquement pendant quelques secondes.

1. Accédez à ***Link Aggregation » Configure Port Trunks***. Le tableau **Port Trunks** s'affiche.

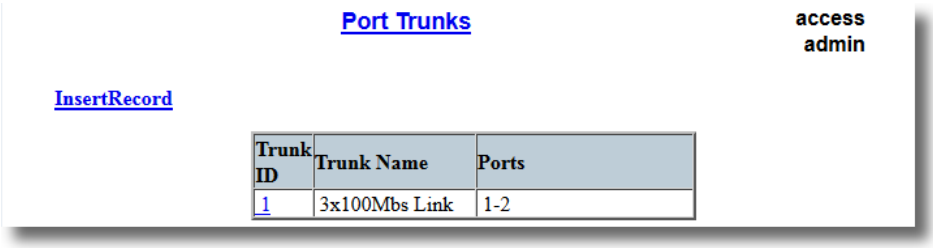


Figure 182 : Tableau Port Trunks

1. InsertRecord

2. Cliquez sur **InsertRecord**. Le formulaire **Port Trunks** s'affiche.

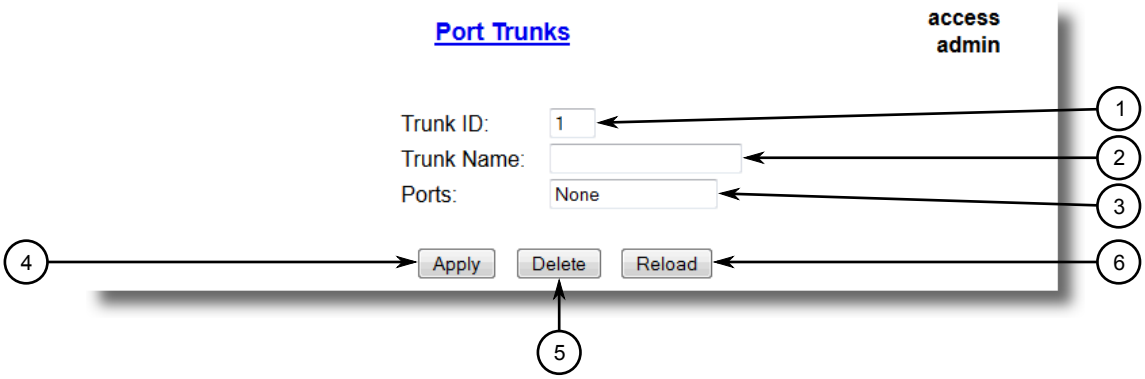


Figure 183 : Agrégations de ports

1. Zone Trunk ID **2.** Zone Trunk Name **3.** Zone Ports **4.** Bouton Apply **5.** Bouton Delete **6.** Bouton Reload

3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
Trunk ID	**Synopsis :** 1 à 2 **Par défaut :** 1 Numéro de compartiment. Il n'affecte pas le fonctionnement du compartiment de port et est utilisé uniquement à des fins d'identification.
Trunk Name	**Synopsis :** 19 caractères quelconques Fournit une description de l'utilisation de lien agrégé.
Ports	**Synopsis :** toute combinaison de nombres valide pour ce paramètre **Par défaut :** None Liste de ports agrégés dans le compartiment.

4. Cliquez sur **Apply**.

Section 5.11.2.3

Suppression d'une agrégation de ports

Procédez comme suit pour supprimer une agrégation de ports :

1. Accédez à ***Link Aggregation » Configure Port Trunks***. Le tableau **Port Trunks** s'affiche.

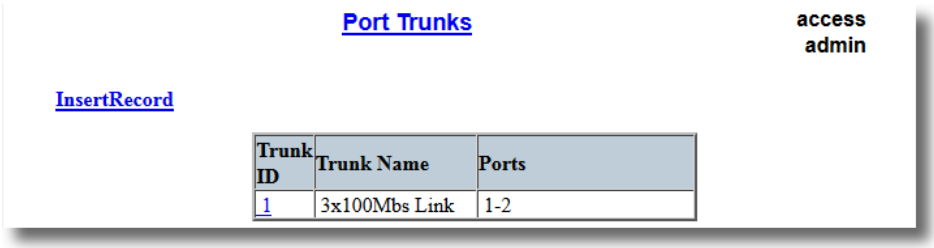


Figure 184 : Tableau Port Trunks

2. Sélectionnez l'agrégation de ports dans le tableau. Le formulaire **Port Trunks** s'affiche.

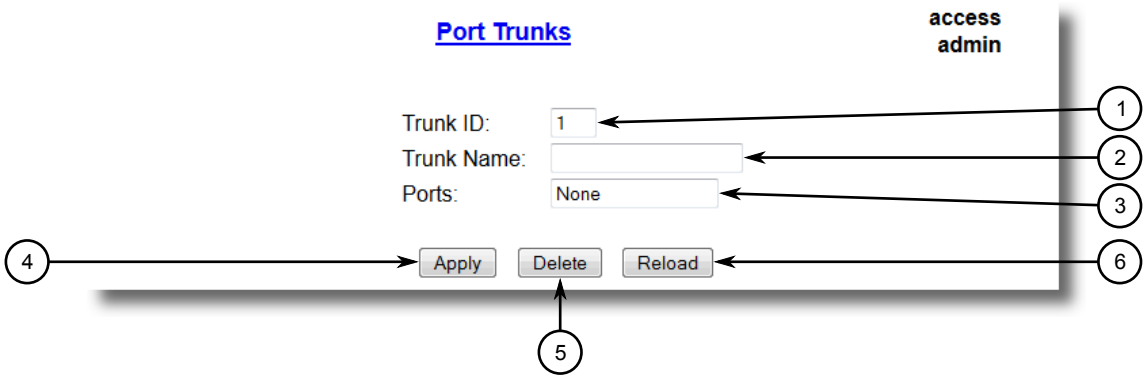


Figure 185 : Formulaire Port Trunks

1. Zone Trunk ID **2.** Zone Trunk Name **3.** Zone Ports **4.** Bouton Apply **5.** Bouton Delete **6.** Bouton Reload

3. Cliquez sur **Delete**.

6 Dépannage

Ce chapitre décrit les étapes de dépannage pour les problèmes communs rencontrés lors de l'utilisation de RUGGEDCOM ROS ou de la conception d'un réseau.

IMPORTANT !
Pour obtenir de l'aide, contactez un représentant du service client.

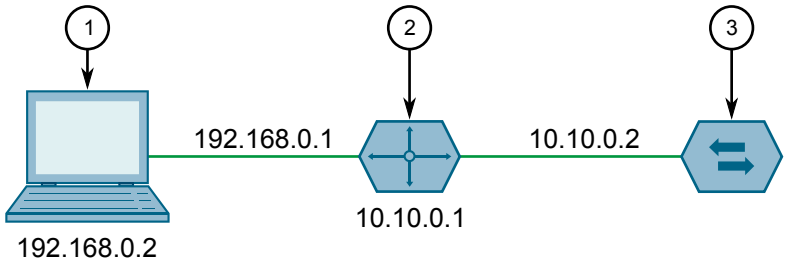
SOMMAIRE

- Section 6.1, « Généralités »
- Section 6.2, « Ports Ethernet »
- Section 6.3, « Spanning Tree »
- Section 6.4, « VLAN »

Section 6.1

Généralités

La présente rubrique décrit des problèmes communs.

Problème	Solution
Le commutateur ne répond pas aux tentatives de ping, même si l'adresse et la passerelle IP ont été configurées. Le commutateur reçoit la commande ping car les LED clignotent et les statistiques d'appareil journalisent les commandes ping. Que se passe-t-il ?	Le commutateur reçoit-il la commande ping via un routeur ? Si c'est le cas, l'adresse de la passerelle de commutateur doit être également configurée. La figure suivante illustre le problème.  **Figure 186 : Utilisation d'un routeur comme passerelle** **1.** Poste de travail **2.** Routeur **3.** Commutateur Le routeur est configuré avec les sous-réseaux IP appropriés et transmet la commande ping du poste de travail vers le commutateur. Lorsque le commutateur répond, il ne sait cependant pas laquelle de ses interfaces il doit utiliser pour accéder au poste de travail et abandonne la réponse. En cas de programmation d'une passerelle de 10.0.0.1, le commutateur envoie des trames ne pouvant être résolues au routeur.

Problème	Solution
	Ce problème se produit également si l'adresse de passerelle n'est pas configurée et si le commutateur tente de générer un trap SNMP vers un hôte qui ne se trouve pas sur le sous-réseau local.

Section 6.2

Ports Ethernet

La présente rubrique décrit les problèmes communs liés aux ports Ethernet.

Problème	Solution
Une liaison semble fonctionner correctement lorsque les niveaux de trafic sont peu élevés, mais est défaillante lorsque le débit augmente ou si une liaison est interrogée par une commande Ping mais rencontre des problèmes avec FTP/SQL/HTTP/etc.	Une cause possible pour un fonctionnement intermittent est une discordance du mode duplex. Si une extrémité de la liaison est fixe en duplex intégral alors que le pair exécute une négociation automatique, l'extrémité exécutant une négociation automatique repasse en mode semi-duplex. La liaison peut afficher quelques erreurs ou aucune si les volumes de trafic sont moins élevés. À mesure que le trafic devient plus intense, le côté négociation fixe commence à rencontrer des paquets abandonnés alors que le côté négociation automatique rencontre des collisions. Finalement, lorsque la charge de trafic approche les 100 %, la liaison devient entièrement inutilisable. La commande Ping avec options de débordement est un outil utile pour tester des liaisons établies. La commande **`ping`** `192.168.0.1 500 2` peut être utilisées pour générer 500 pings séparés chacun par deux millisecondes du commutateur suivant. Si la liaison utilisée est d'excellente qualité, aucune commande ping ne devrait être perdue et le temps d'exécution moyen devrait être peu élevé.
Les liaisons sont inaccessibles, même en cas d'utilisation de la fonctionnalité de protection LFI (Link Fault Indication).	Assurez-vous que la LFI n'est pas activée également sur le pair. Si la LFI est activée sur les deux extrémités de la liaison, elles s'empêchent mutuellement de générer des signaux de liaison.

Section 6.3

Spanning Tree

La présente rubrique décrit les problèmes communs liés au STP (Spanning Tree Protocol).

Problème	Solution
Le réseau est bloqué lorsqu'un nouveau port est connecté et que les LED d'état du port clignotent rapidement.	Est-il possible que STP soit désactivé sur l'un des ports dans le réseau ou l'un des ports sur un commutateur dans le réseau et se connecte accidentellement à un autre commutateur ? Si cela se produit, une boucle de trafic s'est créée. Si le problème semble être de nature temporaire, il est possible que de ports faisant partie du Spanning Tree aient été configurés comme ports de périphérie. Une fois les couches de liaison activées sur les ports de périphérie, STP les fait passer directement (peut-être de manière inappropriée) à l'état de transmission. Si un message de configuration RSTP est ensuite reçu, le port repasse à l'état bloqué. Une boucle de trafic peut se former pendant que le port est à l'état de transmission. Si l'un de commutateurs semble commuter la racine d'un port à un autre, le problème peut être lié à la priorisation du trafic. Pour plus d'informations, voir "The network becomes unstable when a specific application is started." Une autre cause possible pour un fonctionnement intermittent est une discordance dans la négociation automatique. Si une extrémité de la liaison est fixe en mode duplex intégral alors que le pair exécute une négociation automatique, l'extrémité exécutant une négociation automatique repasse en mode semi-duplex. La liaison peut afficher quelques erreurs ou aucune si les volumes de trafic sont moins élevés. À mesure que le trafic devient
Occasionnellement, les ports rencontrent un important débordement pendant un bref intervalle de temps.	
Un commutateur a un comportement étrange lorsque le port racine saute entre deux ports de commutateur et ne se stabilise jamais.	

Problème	Solution
	plus intense, le côté négociation fixe commence à rencontrer des paquets abandonnés alors que le côté négociation automatique rencontre des collisions. Finalement, lorsque la charge de trafic approche les 100 %, la liaison devient entièrement inutilisable. RSTP n'est alors pas en mesure de transmettre des messages de configuration via la liaison et la topologie Spanning Tree est désactivée. Si un trunk alternatif existe, RSTP l'active à la place du port surchargé. L'activation du port alternatif soulage souvent le port surchargé de son trafic, le port surchargé redevient fiable. RSTP est rapidement remis en service et le cycle recommence. Le port racine commute entre deux ports sur le commutateur.
Un ordinateur ou un appareil est connecté à un commutateur. Une fois le commutateur réinitialisé, il a besoin de beaucoup de temps pour être réactivé.	Est-il possible que le réglage de périphérie RSTP soit défini sur False ? Si la périphérie est définie sur False, le pont fait passer le port par deux délais de transmission avant que ce dernier ne puisse envoyer ou recevoir des trames. Si la périphérie est définie sur True, le pont fait passer le port directement à l'état de transmission à l'activation de la liaison. Une autre explication possible est que certaines liaisons dans le réseau s'exécutent en mode semi-duplex. RSTP utilise un protocole pair à pair appelé Proposal-Agreement pour assurer la transition en cas de défaillance de liaison. Ce protocole requiert un fonctionnement en mode duplex intégral. Lorsque RSTP détecte un port en mode non duplex intégral, il ne peut pas se fier au protocole Proposal-Agreement et doit faire en sorte que le port effectue une transition lente (c'est-à-dire STP). Si possible, configurez le port pour un fonctionnement en duplex intégral. Sinon, configurez le réglage point à point du port sur True. Ces deux solutions vous permettent d'utiliser le protocole Proposal-Agreement.
Lorsque le commutateur est testé à l'aide d'une défaillance de liaison délibérée, le système a besoin de beaucoup de temps avant que les appareils se trouvant après le commutateur ne puissent être interrogés.	Est-il possible que certains ports participant à la topologie aient été configurés en mode STP ou que le paramètre point à point du port soit défini sur False ? STP et les ports multipoint convergent lentement après des défaillances. Est-il possible que le port ait migré vers STP ? Si le port est connecté au segment LAN à l'aide d'un support partagé et que les ponts STP sont connectés à ce support, la convergence après une défaillance de liaison est lente. Des délais de l'ordre de dizaines ou de centaines de millisecondes peuvent se produire dans des circonstances dans lesquelles la liaison coupée est la seule liaison vers le pont racine et le pont racine secondaire n'a pas été choisi de manière optimale. Le pire cas se produit lorsque le pont racine secondaire est situé à la périphérie du réseau la plus éloignée de la racine. Dans ce cas, un message de configuration doit être propagé depuis cette périphérie et renvoyé pour rétablir la topologie.
Le réseau est composé d'un anneau de ponts, dont deux sont managés (connectés l'un à l'autre) et le reste ne sont pas managés. Pourquoi le protocole RSTP fonctionne-t-il rapidement lorsqu'une liaison est coupée entre les ponts managés, mais pas dans le pont non managé faisant partie de l'anneau ?	Un pont managé fonctionnant correctement est transparent aux messages de configuration STP. Les ponts managés échangent des messages de configuration via le pont non managé qui fait partie de l'anneau comme s'il n'existait pas. Lorsqu'une liaison dans la partie non managée de l'anneau est défaillante, cependant, les ponts managés sont uniquement en mesure de détecter une défaillance par l'expiration de messages Hello. Une connectivité complète requiert trois temps Hello et deux temps de transmission pour être restaurée.
Le réseau devient instable si une application spécifique et démarrée. Le réseau repasse en fonctionnement normal lorsque l'application est arrêtée.	RSTP envoie ses messages de configuration à l'aide du niveau de priorité le plus élevé possible. Si la CoS est configurée de manière à permettre des écoulements de trafic au niveau de priorité le plus élevé et que ces trafics s'écoulent continuellement en rafale à 100 % de la largeur de bande de ligne, il se peut que STP soit interrompu. Il est dont recommandé de ne pas utiliser la CoS la plus élevée.
Lorsqu'un nouveau port est rattaché, la racine se déplace vers ce port au lieu du port vers lequel elle devrait se déplacer ou sur lequel elle devrait rester.	Est-il possible que le coût de port soit programmé de manière incorrecte ou que la négociation automatique dérive vers une valeur non désirée ? Inspectez le port et les coûts de chemin avec chaque port activé comme racine.
Un IED (Intelligent Electronic Device) ou contrôleur ne fonctionne pas avec l'appareil.	Certains contrôleurs à largeur de bande de CPU peu élevée peuvent avoir un comportement non désiré lorsqu'ils reçoivent un trafic non attendu. Essayez de désactiver le port. Si le contrôleur est défaillant au moment où la liaison est coupée, il se peut que le problème soit causé par des trames désorganisées ou une duplication. Essayez de définir le port racine du pont du contrôleur défaillant sur STP.

Problème	Solution
Des interrogations d'autres appareils sont occasionnellement perdues.	Vérifiez les statistiques du réseau pour déterminer si le pont racine reçoit des TCN (Topology Change Notifications) au moment où une perte de trame a été détectée. Il se peut que des problèmes se soient produits dans les liaisons intermittentes du réseau.
La racine reçoit un grand nombre de TCN. D'où proviennent-elles ?	Examinez les statistiques du port RSTP pour déterminer le port depuis lequel les TCN sont envoyées. Connectez-vous au commutateur à l'autre extrémité de la liaison attachée à ce port. Répétez cette étape jusqu'à ce que le commutateur générant les TCN (c'est-à-dire le commutateur qui ne reçoit pas lui-même un grand nombre de TCN) soit trouvé. Identifiez le problème dans ce commutateur.

Section 6.4

VLAN

La présente rubrique décrit les problèmes communs liés aux VLAN.

Problème	Solution
Des VLAN ne sont pas nécessaires sur le réseau. Peuvent-ils être désactivés ?	Oui. Gardez simplement tous les ports configurés comme *périphérie* et maintenez le VLAN natif à 1. Il s'agit de la configuration par défaut pour le commutateur.
Deux VLAN ont été créés et un certain nombre de ports en sont devenus membres. Certains appareils dans un VLAN doivent alors envoyer des messages à des appareils dans d'autres VLAN.	Si les appareils doivent communiquer dans la couche d'adresse physique, ils doivent être membres du même VLAN. S'ils prennent en charge une communication de type couche 3 (c'est-à-dire à l'aide d'un protocole tel qu'IP ou IPX), utilisez un routeur. Le routeur traite chaque VLAN comme une interface séparée qui dispose de son propre espace d'adresses IP associé.
Sur un réseau de 30 commutateurs, le trafic de gestion doit être limité à un domaine séparé. Quelle est la meilleure méthode pour ce faire pour tout en restant en contact avec ces commutateurs ?	Dans le commutateur dans lequel la station de gestion est située, configurez un port pour utiliser le nouveau VLAN de gestion comme son VLAN natif. Configurez un ordinateur hôte agissant comme une station de gestion temporaire. À chaque commutateur, configurez le VLA de gestion sur sa nouvelle valeur. Le contact avec chaque commutateur est immédiatement perdu lorsqu'ils sont configurés, mais il peut être possible d'établir de nouveau la communication depuis la station de gestion temporaire. Une fois que tous les commutateurs font partie du nouveau VLAN de gestion, configurez les ports de tous les appareils de gestion attachés pour qu'ils utilisent le nouveau VLAN. **REMARQUE** *L'établissement d'un domaine de gestion s'accompagne souvent de l'établissement d'un sous-réseau IP spécifiquement pour les appareils managés.*