SIEMENS

Édition 01/2022

Manuel de configuration

SIMATIC NET

Commutateurs Ethernet robustes

RUGGEDCOM ROS v5.6

Pour RSG2488

https://www.siemens.com/ruggedcom

SIEMENS

SIMATIC NET

Commutateurs Ethernet robustes RUGGEDCOM ROS v5.6

Manuel de configuration

Pour RSG2488

Avant-propos

Introduction 1

Utilisation de ROS 2

Mise en route 3

Gestion de l'appareil 4

Administration système 5

Securité 6

Layer 2 (Couche 2) 7

Layer 3 (couche 3) 8

Redondance réseau 9

Contrôle et classification du trafic 10

Services d'horloge 11

Découverte et gestion du réseau 12

Affectation d'adresse IP 13

Dépannage 14

Référence 15

01/2022
C79000-G8977-1513-01

Mentions légales

Signalétique d'avertissement

Ce manuel donne des consignes que vous devez respecter pour votre propre sécurité et pour éviter des dommages matériels. Les avertissements servant à votre sécurité personnelle sont accompagnés d'un triangle de danger, les avertissements concernant uniquement des dommages matériels sont dépourvus de ce triangle. Les avertissements sont représentés ci-après par ordre décroissant de niveau de risque.

⚠ **DANGER**
signifie que la non-application des mesures de sécurité appropriées **entraîne** la mort ou des blessures graves.

⚠ **AVERTISSEMENT**
signifie que la non-application des mesures de sécurité appropriées **peut entraîner** la mort ou des blessures graves.

⚠ **ATTENTION**
signifie que la non-application des mesures de sécurité appropriées peut entraîner des blessures légères.

⚠ **NOTA**
signifie que la non-application des mesures de sécurité appropriées peut entraîner un dommage matériel.

En présence de plusieurs niveaux de risque, c'est toujours l'avertissement correspondant au niveau le plus élevé qui est reproduit. Si un avertissement avec triangle de danger prévient des risques de dommages corporels, le même avertissement peut aussi contenir un avis de mise en garde contre des dommages matériels.

Personnes qualifiées

L'appareil/le système décrit dans cette documentation ne doit être manipulé que par du **personnel qualifié** pour chaque tâche spécifique. La documentation relative à cette tâche doit être observée, en particulier les consignes de sécurité et avertissements. Les personnes qualifiées sont, en raison de leur formation et de leur expérience, en mesure de reconnaître les risques liés au maniement de ce produit / système et de les éviter.

Utilisation des produits Siemens conforme à leur destination

Tenez compte des points suivants:

⚠ **AVERTISSEMENT**
Les produits Siemens ne doivent être utilisés que pour les cas d'application prévus dans le catalogue et dans la documentation technique correspondante. S'ils sont utilisés en liaison avec des produits et composants d'autres marques, ceux-ci doivent être recommandés ou agréés par Siemens. Le fonctionnement correct et sûr des produits suppose un transport, un entreposage, une mise en place, un montage, une mise en service, une utilisation et une maintenance dans les règles de l'art. Il faut respecter les conditions d'environnement admissibles ainsi que les indications dans les documentations afférentes.

Marques de fabrique

Toutes les désignations repérées par ® sont des marques déposées de Siemens Canada Ltd.. Les autres désignations dans ce document peuvent être des marques dont l'utilisation par des tiers à leurs propres fins peut enfreindre les droits de leurs propriétaires respectifs.

Exclusion de responsabilité

Nous avons vérifié la conformité du contenu du présent document avec le matériel et le logiciel qui y sont décrits. Ne pouvant toutefois exclure toute divergence, nous ne pouvons pas nous porter garants de la conformité intégrale. Si l'usage de ce manuel devait révéler des erreurs, nous en tiendrons compte et apporterons les corrections nécessaires dès la prochaine édition.

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8977-1513-01
© 01/2022 Modifications possibles

Copyright © Siemens 2022
Tous droits réservés

Table des matières

Avant-propos xiii
Note relative à la sécurité xiii
Modèle d'assistance de firmware/logiciel xiv
Syntaxe de commande CLI xiv
Documents liés xv
Configuration requise xvii
Accès à la documentation xvii
Marques déposées xvii
Garantie xvii
Formation xviii
Assistance client xviii
Contacter Siemens xix

1 Introduction 1

1.1 Fonctionnalités et avantages 1
1.2 Recommandations relatives à la sécurité 5
1.3 Évènements de sécurité enregistrés 8
1.4 Contrôlé ou non contrôlé 11
1.5 Normes de réseau prises en charge 11
1.6 Prise en charge de protocole Internet 12
1.6.1 Fonctionnalités prises en charge par IPv4 et/ou IPv6 12
1.6.2 Adresse IPv4 13
1.6.3 Adresse IPv6 13
1.7 Schéma de numérotation de ports 13
1.8 Services disponibles par port 14
1.9 Mémoire amovible 16

2 Utilisation de ROS 19

2.1 Ouverture de session 20
2.2 Fermeture de session 21
2.3 Utilisation de l'interface Web 22
2.4 Utilisation de l'interface de console 23
2.5 Utilisation de l'interface de ligne de commande 25
2.5.1 Commandes CLI disponibles 26
2.5.2 Traçage d'événements 34
2.5.3 Exécution distante de commandes via RSH 35
2.5.4 Utilisation de commandes SQL 35
2.5.4.1 Recherche du tableau correct 36
2.5.4.2 Récupération d'informations 36

2.5.4.3 Modification de valeurs dans un tableau 38
2.5.4.4 Réinitialisation d'un tableau 39
2.5.4.5 Utilisation de RSH et SQL 39

2.6 Sélection de ports dans RUGGEDCOM ROS 40

2.7 Gestion du système de fichiers flash 40
2.7.1 Affichage d'une liste de fichiers Flash 40
2.7.2 Affichage de détails de fichier Flash 41
2.7.3 Défragmentation du système de fichiers flash 41

2.8 Accès en mode BIST 42

2.9 Gestion de l'accès à l'interface du chargeur de démarrage (Boot Loader) 43
2.9.1 Activation/désactivation de l'accès à l'interface du chargeur de démarrage (Boot Loader) 43
2.9.2 Accès à l'interface du chargeur de démarrage (Boot Loader) 44
2.9.3 Réglage de la source de démarrage 45

2.10 Activation/désactivation de l'accès automatique à la mémoire amovible 45

2.11 Activation/désactivation du service de console 46

3 Mise en route 49

3.1 Connexion à ROS 49
3.1.1 Adresse IP par défaut 49
3.1.2 Connexion directe 49
3.1.3 Connexion à distance 51

3.2 Configuration d'un réseau de base 52

4 Gestion de l'appareil 53

4.1 Affichage d'informations produit 53

4.2 Affichage de diagnostics de la CPU 54

4.3 Affichage de l'état des alimentations 55

4.4 Restauration des valeurs par défaut 55

4.5 Chargement/téléchargement de fichiers 57
4.5.1 Chargement/téléchargement de fichiers à l'aide de XMODEM 58
4.5.2 Chargement/téléchargement de fichiers à l'aide d'un client TFTP 59
4.5.3 Chargement/téléchargement de fichiers à l'aide d'un serveur TFTP 60
4.5.4 Chargement/téléchargement de fichiers à l'aide d'un serveur SFTP 60
4.5.5 Chargement/téléchargement de fichiers à l'aide de la carte microSD/microSDHC ... 61

4.6 Gestion de journaux 62
4.6.1 Affichage de journaux locaux et système 62
4.6.2 Effacement de journaux locaux et système 63
4.6.3 Configuration du journal système local 63
4.6.4 Gestion de la journalisation distante 63
4.6.4.1 Format du journal système 64
4.6.4.2 Configuration du client Syslog distant 65
4.6.4.3 Affichage d'une liste de serveurs Syslog distants 66
4.6.4.4 Ajout d'un serveur Syslog distant 66

4.6.4.5 Suppression d'un serveur Syslog distant 67
4.7 Gestion de ports Ethernet 67
4.7.1 Protection du contrôleur via l'indication de défaillance de liaison (Link Fault Indication, LFI) 68
4.7.2 Affichage de l'état de ports Ethernet 69
4.7.3 Affichage des statistiques pour tous les ports Ethernet 70
4.7.4 Affichage de statistiques pour des ports Ethernet spécifiques 70
4.7.5 Effacement de statistiques pour des ports Ethernet spécifiques 73
4.7.6 Configuration d'un port Ethernet 73
4.7.7 Configuration de la limitation du débit de port 76
4.7.8 Configuration de la détection de liaison 77
4.7.9 Mise en miroir du trafic 79
4.7.9.1 Comprendre la mise en miroir du trafic à distance (Remote Traffic Mirroring, RTM) 79
4.7.9.2 Configuration de la mise en miroir du trafic 80
4.7.9.3 Exemple : configuration de Remote Traffic Mirroring 83
4.7.10 Gestion d'émetteurs-récepteurs SFP 86
4.7.10.1 Exigences pour les émetteurs-récepteurs SFP 87
4.7.10.2 Surveillance d'un port SFP 87
4.7.10.3 Affichage d'informations pour un port SFP 88
4.7.10.4 Définition de l'intervalle d'interrogation SFP 89
4.7.10.5 Affichage de diagnostics de SFP 89
4.7.11 Détection de défauts de câble 92
4.7.11.1 Affichage des résultats de diagnostics de câbles 93
4.7.11.2 Exécution de diagnostics de câble 94
4.7.11.3 Effacement de diagnostics de câble 95
4.7.11.4 Détermination de la distance estimée au défaut (Estimated Distance To Fault (DTF) 95
4.7.12 Réinitialisation de ports Ethernet 96
4.8 Gestion d'interfaces IP 96
4.8.1 Configuration de l'interface IP de gestion 97
4.8.2 Gestion d'interfaces IP de commutateur 98
4.8.2.1 Affichage d'une liste d'interfaces IP de commutateur 98
4.8.2.2 Ajout d'une interface IP de commutateur 99
4.8.2.3 Suppression d'une interface IP de commutateur 100
4.9 Gestion de passerelles IP 101
4.9.1 Affichage d'une liste de passerelles IP 101
4.9.2 Ajout d'une passerelle IP 101
4.9.3 Suppression d'une passerelle IP 102
4.10 Configuration des services IP 102
4.11 Gestion de la surveillance à distance 104
4.11.1 Gestion des RMON History Controls 104
4.11.1.1 Affichage d'une liste de contrôles d'historique RMON 104
4.11.1.2 Ajout d'un contrôle d'historique RMON 104
4.11.1.3 Suppression d'un contrôle d'historique RMON 105
4.11.2 Gestion des alarmes RMON 105
4.11.2.1 Affichage d'une liste d'alarmes RMON 107

4.11.2.2 Ajout d'une alarme RMON 107
4.11.2.3 Suppression d'une alarme RMON 109
4.11.3 Gestion des événements RMON 109
4.11.3.1 Affichage d'une liste d'événements RMON 109
4.11.3.2 Ajout d'un événement RMON 110
4.11.3.3 Suppression d'un événement RMON 110
4.12 Mise à niveau/rétrogradage du firmware 111
4.12.1 Vérification de la somme de contrôle de hachage 111
4.12.2 Mise à niveau du firmware 111
4.12.3 Rétrogradation du firmware 112
4.13 Réinitialisation de l'appareil 114
4.14 Désactivation de l'appareil 114
5 Administration système 117
5.1 Configuration du système d'information 117
5.2 Personnalisation de l'écran d'ouverture de session 117
5.3 Activation/désactivation de l'interface Web 118
5.4 Gestion des alarmes 118
5.4.1 Affichage d'une liste d'alarmes préconfigurées 119
5.4.2 Affichage et effacement d'alarmes verrouillées 119
5.4.3 Configuration d'une alarme 119
5.4.4 Alarmes de sécurité pour l'authentification de connexions 121
5.4.5 Liste des alarmes 123
5.5 Gestion du fichier de configuration 126
5.5.1 Configuration du chiffrage des données 126
5.5.2 Mise à jour du fichier de configuration 128
5.6 Gestion de MMS 128
5.6.1 Comprendre MMS 128
5.6.1.1 Rapport MMS 129
5.6.1.2 Rapports/jeux de données 129
5.6.1.3 Nœuds logiques pris en charge 130
5.6.2 Affichage d'une liste de rapports MMS préconfigurés 130
5.6.3 Configuration d'un rapport MMS 131
5.6.4 Exemple : configuration de rapports MMS 132
6 Securité 135
6.1 Configuration de mots de passe 135
6.2 Effacement de données privées 137
6.3 Gestion de l'authentification utilisateur 138
6.3.1 Méthodes d'authentification 138
6.3.2 Configuration d'extensions de nom d'utilisateur 140
6.3.3 Gestion de l'authentification RADIUS 141
6.3.3.1 Configuration du serveur RADIUS 142
6.3.3.2 Configuration du client RADIUS sur l'appareil 142
6.3.4 Gestion de l'authentification TACACS+ 144

6.3.4.1 Configuration de TACACS+ 144
6.3.4.2 Configuration des droits d'utilisateur 145

6.4 Gestion de la sécurité des ports (Port security) 146
6.4.1 Concepts de sécurité de port 146
6.4.1.1 Authentification basée sur des adresses MAC statiques 146
6.4.1.2 Authentification basée sur des adresses MAC statiques dans un anneau MRP 147
6.4.1.3 Authentification IEEE 802.1X. 147
6.4.1.4 Authentification IEEE 802.1X avec authentification basée sur l'adresse MAC 148
6.4.1.5 VLAN restreints 149
6.4.1.6 Affectation de VLAN avec attributs Tunnel 150
6.4.2 Affichage d'une liste d'adresses MAC autorisées 151
6.4.3 Configuration de la sécurité du port 151
6.4.4 Configuration d'IEEE 802.1X 153

6.5 Gestion des clés et des certificats SSH/SSL 154
6.5.1 Certificats SSL 156
6.5.2 Clé d'hôte SSH 157
6.5.3 Gestion de clés publiques SSH 157
6.5.3.1 Exigences en matière de clés publiques 158
6.5.3.2 Ajout d'une clé publique 159
6.5.3.3 Affichage d'une liste de clés publiques 159
6.5.3.4 Mise à jour d'une clé publique 160
6.5.3.5 Suppression d'une clé publique 161
6.5.4 Exemples de certificats et de clés 161

7 Layer 2 (Couche 2) 163

7.1 Gestion de LAN virtuels 163
7.1.1 Concepts VLAN 163
7.1.1.1 Trames balisées ou trames non balisées 163
7.1.1.2 VLAN natif 164
7.1.1.3 VLAN de gestion 164
7.1.1.4 VLAN de gestion auxiliaires 164
7.1.1.5 Types de port périphérie et de liaison 165
7.1.1.6 Règles d'entrée et de sortie 166
7.1.1.7 Liste Forbidden Ports 166
7.1.1.8 Modes compatible VLAN et non-compatible VLAN 167
7.1.1.9 GARP VLAN Registration Protocol (GVRP) 167
7.1.1.10 Périphérie PVLAN 169
7.1.1.11 QinQ 169
7.1.1.12 Avantages du VLAN 171
7.1.2 Affichage d'une liste de VLAN 173
7.1.3 Configuration globale de VLAN 173
7.1.4 Configuration de VLAN pour des ports Ethernet spécifiques 174
7.1.5 Gestion de VLAN statiques 176
7.1.5.1 Affichage d'une liste de VLAN statiques 176
7.1.5.2 Ajout d'un VLAN statique 176
7.1.5.3 Suppression d'un VLAN statique 178
7.1.6 Exemple : configuration du support de gestion sur plusieurs VLAN 178

7.2 Gestion des adresses MAC 180

7.2.1 Affichage d'une liste d'adresses MAC 180
7.2.2 Configuration des options d'apprentissage d'adresses MAC 181
7.2.3 Configuration des options d'avalanche d'adresses MAC 181
7.2.4 Gestion des adresses MAC statiques 182
7.2.4.1 Affichage d'une liste d'adresses MAC statiques 182
7.2.4.2 Ajout d'une adresse MAC statique 183
7.2.4.3 Suppression d'une adresse MAC statique 184
7.2.5 Purge de toutes les adresses MAC dynamiques 184

7.3 Gestion du filtrage de multidiffusion 184
7.3.1 Gestion d'IGMP 184
7.3.1.1 Concepts IGMP 185
7.3.1.2 Affichage d'une liste d'appartenances à des groupes de multidiffusion 189
7.3.1.3 Affichage d'informations de transmission pour des groupes de multidiffusion 190
7.3.1.4 Configuration d'IGMP 191
7.3.2 Gestion de GMRP 192
7.3.2.1 Concepts GMRP 193
7.3.2.2 Affichage d'un résumé de groupes de multidiffusion 195
7.3.2.3 Configuration globale du GMRP 196
7.3.2.4 Configuration de GMRP pour des ports Ethernet spécifiques 196
7.3.2.5 Affichage d'une liste de groupes de multidiffusion statiques 197
7.3.2.6 Ajout d'un groupe multidiffusion statique 197
7.3.2.7 Suppression d'un groupe de multidiffusion statique 198

8 Layer 3 (couche 3) 199

8.1 Gestion de Layer 3 Switching (commutation de couche 3) 199
8.1.1 Comprendre la commutation de couche 3 (Layer 3 Switching) 199
8.1.1.1 Tableau Forwarding Layer 3 Switch 199
8.1.1.2 Règles statiques Layer 3 Switching (commutation de couche 3) 200
8.1.1.3 Apprentissage dynamique des règles Layer 3 Switching (commutation de couche 3) 201
8.1.1.4 Interaction entre IP Forwarding et Layer 3 Switching 201
8.1.1.5 Tableau ARP Layer 3 Switch 202
8.1.1.6 Interfaces routables Layer 3 Switch 204
8.1.2 Configuration de la commutation de couche 3 (Layer 3 Switching) 205
8.1.3 Configuration des options de commutation de couche 3 (Layer 3 Switching) 205
8.1.4 Gestion des règles de monodiffusion statiques 206
8.1.4.1 Affichage des règles de monodiffusion statiques 206
8.1.4.2 Ajout d'une règle de monodiffusion statique 206
8.1.4.3 Suppression d'une règle de monodiffusion statique 207
8.1.5 Gestion des entrées de tableau Static ARP 207
8.1.5.1 Affichage d'une liste d'entrées de tableau ARP 207
8.1.5.2 Ajout d'une entrée de tableau Static ARP 208
8.1.5.3 Suppression d'une entrée de tableau Static ARP 208
8.1.6 Affichage des règles de routage 209
8.1.7 Suppression de règles de routage de matériel dynamiques 209
8.1.8 Exemple : configuration de la commutation de couche 3 (Layer 3 Switching) 210
8.1.9 Exemple : configuration de Layer 3 Switching à l'aide de plusieurs commutateurs . 212

9 Redondance réseau 215

9.1 Gestion du Spanning Tree Protocol 215
9.1.1 Fonctionnement RSTP 215
9.1.1.1 États et rôles RSTP 216
9.1.1.2 Ports de périphérie 218
9.1.1.3 Liaisons point à point et multipoint 218
9.1.1.4 Chemin et coûts de port 219
9.1.1.5 Diamètre de pont 220
9.1.1.6 eRSTP 220
9.1.1.7 Fast Root Failover 220
9.1.2 Applications RSTP 222
9.1.2.1 RSTP dans des configurations de câblage structuré 222
9.1.2.2 RSTP dans des configurations de structure en anneau 224
9.1.2.3 Redondance des ports RSTP 225
9.1.3 Opérations MSTP 226
9.1.3.1 Régions MSTP et interopérabilité 226
9.1.3.2 Rôles de pont et port MSTP 228
9.1.3.3 Avantages de MSTP 229
9.1.3.4 Mise en œuvre de MSTP sur un réseau ponté 230
9.1.4 Configuration globale de STP 231
9.1.5 Configuration de STP pour des ports Ethernet spécifiques 233
9.1.6 Configuration d'eRSTP 235
9.1.7 Affichage de statistiques globales concernant STP 238
9.1.8 Affichage de statistiques STP pour des ports Ethernet 239
9.1.9 Gestion de Multiple Spanning Tree Instances 241
9.1.9.1 Affichage des statistiques pour des MSTI globales 241
9.1.9.2 Affichage des statistiques pour des MSTI de ports 242
9.1.9.3 Configuration de l'identificateur de région MST 243
9.1.9.4 Configuration d'une MSTI globale 244
9.1.9.5 Configuration d'une MSTI pour un port Ethernet 245
9.1.10 Effacement de statistiques de Spanning Tree Protocol 246

9.2 Gestion du Media Redundancy Protocol (MRP) 246
9.2.1 Comprendre MRP 246
9.2.1.1 Appareils MRM ou MRC 246
9.2.1.2 Appareils MRA 247
9.2.1.3 États de ports d'anneau 247
9.2.1.4 Anneau fermé ou anneau ouvert 247
9.2.2 Configuration globale du MRP 248
9.2.3 Affichage de l'état des instances MRP 249
9.2.4 Ajout d'une instance MRP 250
9.2.5 Suppression d'une instance MRP 252
9.2.6 Exemple : configuration d'un anneau MRP 253

9.3 Gestion de l'agrégation de liens 254
9.3.1 Concepts d'agrégation de liens 255
9.3.1.1 Agrégation de lien statique ou dynamique 255
9.3.1.2 Règles et limitations 256
9.3.1.3 Agrégation de liens et fonctionnalités de couche 2 257
9.3.1.4 Agrégation de liens et fonctionnalités de couche physique 258
9.3.2 Configuration de l'agrégation de liens 258

9.3.3 Gestion des groupes d'agrégation de liens 258
9.3.3.1 Affichage d'une liste de groupes d'agrégation de liens 259
9.3.3.2 Ajouter un groupe d'agrégation de liens 259
9.3.3.3 Suppression d'un groupe d'agrégation de liens (Link Aggregation Group) 260
9.3.3.4 Affichage de l'état des Link Aggregation Groups 261
9.3.4 Gestion du Link Aggregation Control Protocol 261
9.3.4.1 Affichage des informations sur le partenaire LACP 262
9.3.4.2 Configuration des réglages globaux LACP 262
9.3.4.3 Configuration de LACP par port 263
9.3.4.4 Affichage des statistiques LACP 264
9.3.5 Effacement des statistiques d'agrégation de liens 265

10 Contrôle et classification du trafic 267

10.1 Gestion des classes de service 267
10.1.1 Configuration globale de classes de service 269
10.1.2 Configuration de classes de service pour des ports Ethernet spécifiques 269
10.1.3 Configuration de la priorité pour le mappage CoS 270
10.1.4 Configuration du mappage DSCP sur CoS 271

11 Services d'horloge 273

11.1 Configuration de la date et de l'heure 273
11.2 Configuration d'IRIG-B 275
11.3 Gestion du PTP (Precision Time Protocol) 276
11.3.1 Configuration de PTP 277
11.3.2 Configuration globale de PTP 278
11.3.3 Configuration d'une Ordinary Clock 279
11.3.4 Configuration d'une Transparent Clock 282
11.3.5 Configuration globale d'une Boundary Clock 284
11.3.6 Configuration d'un groupe de ports Boundary Clock 285
11.3.7 Affichage des statistiques PTP 288
11.3.8 Configuration d'un VLAN pour le trafic PTP 290
11.3.9 Exemple : configuration de PTP sur plusieurs VLAN 290
11.4 Configuration de la source de temps 293
11.5 Gestion de NTP 294
11.5.1 Activation/désactivation du service NTP 295
11.5.2 Configuration de serveurs NTP 295
11.6 Affichage de l'état de sous-systèmes de synchronisation d'horloge 296

12 Découverte et gestion du réseau 299

12.1 Activation/désactivation du RCDP 299
12.2 Gestion de LLDP 301
12.2.1 Configuration globale du LLDP 302
12.2.2 Configuration de LLDP pour un port Ethernet 302
12.2.3 Affichage de statistiques globales et d'informations système annoncées 303
12.2.4 Affichage des statistiques pour des voisins LLDP 304
12.2.5 Affichage des statistiques pour les ports LLDP 304

12.3 Gestion de SNMP 305
12.3.1 Gestion des utilisateurs SNMP 306
12.3.1.1 Affichage d'une liste d'utilisateurs SNMP 306
12.3.1.2 Ajout d'un utilisateur SNMP 306
12.3.1.3 Suppression d'un utilisateur SNMP 308
12.3.2 Gestion du mappage sécurité sur groupe 309
12.3.2.1 Affichage d'une liste de mappages sécurité sur groupe 309
12.3.2.2 Ajout d'un mappage sécurité sur groupe 309
12.3.2.3 Suppression d'un mappage sécurité sur groupe 310
12.3.3 Gestion de groupes SNMP 310
12.3.3.1 Affichage d'une liste de groupes SNMP 310
12.3.3.2 Ajout d'un groupe SNMP 310
12.3.3.3 Suppression d'un groupe SNMP 311

12.4 Prise en charge de la gestion de ModBus 311
12.4.1 Codes de fonction Modbus 312
12.4.2 Mappage de la mémoire ModBus 313
12.4.3 Formats de mémoire Modbus 319
12.4.3.1 Texte 319
12.4.3.2 Cmd 319
12.4.3.3 Uint16 320
12.4.3.4 Uint32 320
12.4.3.5 PortCmd 320
12.4.3.6 Alarme 321
12.4.3.7 PSStatusCmd 321
12.4.3.8 TruthValues 322

13 Affectation d'adresse IP 325

13.1 Gestion de DHCP 325
13.1.1 Concepts DHCP 325
13.1.1.1 Espionnage DHCP (DHCP Snooping) 325
13.1.1.2 Ports fiables et non fiables 325
13.1.1.3 DHCP Relay Agent (Option 82) (Agent de relais DHCP) 326
13.1.1.4 Inspection ARP dynamique 326
13.1.1.5 Tableau DHCP Binding 327
13.1.1.6 Attaques de réseau évitables 327
13.1.2 Configuration du DHCP Relay Agent (agent de relais DHCP) 331
13.1.3 Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques 331
13.1.4 Configuration de l'espionnage DHCP 332
13.1.5 Configuration de ports fiables/non fiables 333
13.1.6 Gestion de l'inspection ARP dynamique 333
13.1.6.1 Activation/désactivation de l'inspection ARP dynamique. 334
13.1.6.2 Affichage des statistiques d'inspection ARP 334
13.1.6.3 Effacement des statistiques d'inspection ARP 334
13.1.7 Gestion du tableau DHCP Binding 335
13.1.7.1 Ajout d'entrées au tableau DHCP Binding 335
13.1.7.2 Affichage du tableau DHCP Binding 335
13.1.7.3 Enregistrement du tableau DHCP Binding 336
13.1.7.4 Exemple : configuration de l'appareil comme Relay Agent 336

14 Dépannage 341
14.1 Généralités 341
14.2 Ports Ethernet 342
14.3 Spanning Tree 343
14.4 VLAN 345
15 Référence 347
15.1 MIB standard prises en charge 347
15.2 MIB RUGGEDCOM propriétaires prises en charge 425
15.3 Fonctionnalités d'agent prises en charge 463
15.4 Traps SNMP 464

Avant-propos

Ce manuel décrit la version v5.6 de ROS (Rugged Operating System) sur le RUGGEDCOM RSG2488. 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.

Remarque
Ce document est mis à jour pour correspondre à la version RUGGEDCOM ROS V5.6 disponible au moment de la publication, y compris les versions mineures (par exemple 5.6.1, 5.6.2, etc.). Pour déterminer la version actuelle RUGGEDCOM ROS V5.6, reportez-vous à Siemens Industrial Online Support :

- **Informations produit**

  https://support.industry.siemens.com/cs/search?search=ROS&type=ProductNote&o=0

- **Téléchargements**

  https://support.industry.siemens.com/cs/search?search=ROS&type=Download&o=0

Les utilisateurs peuvent également configurer une notification par e-mail quotidienne ou hebdomadaire pour les informer des dernières versions/mises à jour. Pour plus d'informations, voir le site Web Siemens Industrial Online Support [https://support.industry.siemens.com].

Remarque
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 manuel doit être utilisé en accompagnement des textes d'aide inclus dans le logiciel.

Note relative à la sécurité

Siemens commercialise des produits et solutions comprenant des fonctions de sécurité industrielle qui contribuent à une exploitation sûre des installations, systèmes, machines et réseaux.

Pour garantir la sécurité des installations, systèmes, machines et réseaux contre les cybermenaces, il est nécessaire de mettre en œuvre - et de maintenir en permanence

- un concept de sécurité industrielle global et de pointe. Les produits et solutions de Siemens constituent une partie de ce concept.

Il incombe aux clients d'empêcher tout accès non autorisé à ses installations, systèmes, machines et réseaux. Ces systèmes, machines et composants doivent uniquement être connectés au réseau d'entreprise ou à Internet si et dans la mesure où cela est nécessaire et seulement si des mesures de protection adéquates (ex : pare-feu et/ou segmentation du réseau) ont été prises.

Pour plus d'informations sur les mesures de protection pouvant être mises en œuvre dans le domaine de la sécurité industrielle, rendez-vous sur https://www.siemens.com/industrialsecurity.

Les produits et solutions Siemens font l'objet de développements continus pour être encore plus sûrs. Siemens recommande vivement d'effectuer des mises à jour dès que celles-ci sont disponibles et d'utiliser la dernière version des produits. L'utilisation de versions qui ne sont plus prises en charge et la non-application des dernières mises à jour peut augmenter le risque de cybermenaces pour nos clients.

Pour être informé des mises à jour produit, abonnez-vous au flux RSS Siemens Industrial Security à l'adresse suivante: https://www.siemens.com/industrialsecurity.

Modèle d'assistance de firmware/logiciel

Siemens L'assistance logiciel ne prend en charge que les failles de sécurité de la dernière version de firmware. Par conséquent, les corrections de bogues et de sécurité ne sont fournies que pour la dernière version du firmware.

Syntaxe de commande CLI

Ce document détaille les commandes CLI. Une commande CLI est constituée d'une commande par touches, de paramètres, d'options et/ou de variables utilisateur.

Éléments d'une commande CLI

Dans la commande CLI suivante, `interface` est la commande par touches, { *name* } est une valeur personnalisée, `vlan` et `type` sont des paramètres et `access` et `trunk` sont des options fixes.

```
interface { name } vlan type [ access | trunk ]
```

Mise en forme de la commande

Des commandes CLI sont affichées dans ce document selon les règles de syntaxe suivantes :

Convention	Description	Exemple
Police	Toutes les commandes, tous les paramètres et toutes les options sont affichés dans une police monospace.	`command parameter`
Valeurs personnalisées	Certains paramètres requièrent une valeur personnalisée. Les valeurs que	`command parameter { value }`

Convention	Description	Exemple
	vous devez définir sont entourées par des accolades (parenthèses bouclées). La valeur peut être une chaîne de caractères, telle qu'un nom ou une description. La valeur peut être un composant du système, tel qu'un ID ou une interface. Dans tous les cas, le mot-clé entre les accolades indique le type de valeur à entrer.	
Plages de nombres	Si la valeur d'un paramètre est un nombre compris dans une plage spécifique, la plage est entourée par des accolades (parenthèses bouclées).	`command parameter { 0 - 10 }`
Options	Si des choix multiples sont disponibles pour la valeur d'un paramètre, tous les choix sont entourés par des crochets. Les choix sont souvent composés de valeurs fixes mais ils peuvent également comprendre des valeurs personnalisées et/ou des plages de nombres.	`command parameter [ option1 | option2 | { value } | { 0 - 10 } ]`

Documents liés

Les documents suivants liés à ce produit peuvent présenter un intérêt. Sauf indication contraire, chaque document est disponible sur le site Web Siemens Industry Online Support (SIOS) [https://support.industry.siemens.com].

Les documents listés sont ceux qui sont disponibles à la date de publication. Des versions plus récentes de ces documents ou de leurs produits associés peuvent être disponibles. Pour plus d'informations, visitez SIOS ou consultez un agent du support client Siemens.

Informations produit

Les informations produit sont disponibles en ligne via SIOS [https://support.industry.siemens.com/cs/ca/en/ps/16008/pm].

Manuels de configuration

Titre du document	Lien
Guide utilisateur pour Windows RUGGEDCOM NMS v2.1	https://support.industry.siemens.com/cs/ww/en/view/109737564
Guide utilisateur pour Linux RUGGEDCOM NMS v2.1	https://support.industry.siemens.com/cs/ww/en/view/109737563
Manuel de configuration RUGGEDCOM DIRECTOR v1.5	https://support.industry.siemens.com/cs/ww/en/view/97691648

Titre du document	Lien
Manuel de configuration RUGGEDCOM EXPLORER v1.5	https://support.industry.siemens.com/cs/ww/en/view/109480804
Guide utilisateur RUGGEDCOM PING v1.2	https://support.industry.siemens.com/cs/ww/en/view/97674073

Instructions de service

Titre du document	Lien
Instructions de service SINEC PNI	https://support.industry.siemens.com/cs/de/en/view/109804190

Catalogues

Titre du document	Lien
Catalogue des modules RUGGEDCOM pour le RUGGEDCOM RSG2488	https://support.industry.siemens.com/cs/ww/en/view/109757282
Catalogue des émetteurs-récepteurs RUGGEDCOM SFP	https://support.industry.siemens.com/cs/ww/en/view/109482309

FAQ

Titre du document	Lien
Marche à suivre pour configurer la fonction SNMP dans un commutateur RUGGEDCOM avec RUGGEDCOM ROS	https://support.industry.siemens.com/cs/ww/en/view/109474615
Marche à suivre pour sécuriser les appareils RUGGEDCOM ROS avant et après le déploiement sur le terrain	https://support.industry.siemens.com/cs/ww/en/view/99858806
Marche à suivre pour implémenter des réseaux en anneau robustes avec RSTP et eRSTP	https://support.industry.siemens.com/cs/ww/en/view/109738240
Marche à suivre pour implémenter une connexion sécurisée sans surveillance dans ROS	https://support.industry.siemens.com/cs/ww/en/view/109756843
Marche à suivre pour contrôler le trafic bidirectionnel en utilisant la mise en miroir de ports	https://support.industry.siemens.com/cs/ww/en/view/109759351
Sommes de contrôle de hachage RUGGEDCOM ROS	https://support.industry.siemens.com/cs/ww/en/view/109779935
Les commutateurs Ethernet RUGGEDCOM prennent-ils en charge les messages non standard et surdimensionnés (trames jumbo) ?	https://support.industry.siemens.com/cs/ww/en/view/109782417

Livres blancs

Titre du document	Lien
Performance du Rapid Spanning Tree Protocol dans la topologie de réseau en anneau	https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf

Manuels de référence

Titre du document	Lien
Manuel de référence sur les fonctionnalités de synchronisation d'horloge	https://support.industry.siemens.com/cs/us/en/view/109780448

Manuels d'installation

Titre du document	Lien
Guide d'installation RUGGEDCOM RSG2488	https://support.industry.siemens.com/cs/ww/en/view/82169156

Configuration requise

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

- Une interface Ethernet fonctionnelle, compatible avec au moins l'un des types de port sur l'appareil RUGGEDCOM doit être disponible
- 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 v5.6 est disponible en ligne sur https://support.industry.siemens.com. Pour toute demande ou renseignement à propos d'un document utilisateur, contactez l'Assistance client Siemens.

Marques déposées

RUGGEDCOM®, ROS®, RCDP®et RUGGEDCOM Discovery Protocol® 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.

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 ou contactez un représentant du service client de 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.

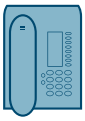
Pour plus d'informations sur les services de formation et les disponibilités des cours, rendez-vous sur https://www.siemens.com ou contactez un représentant commercial Siemens.

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 :

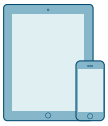
En ligne

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 Web https://w3.siemens.com/aspa_app/?lang=fr.



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

Contacter Siemens

Adresse	Siemens Canada Ltd. Industrie numérique Automatisation du processus 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
Courriel	info.ruggedcom@siemens.com
Site Web	https://www.siemens.com

1 Introduction

Bienvenue dans le Manuel de configuration du logiciel RUGGEDCOM ROS v5.6 pour les appareils RUGGEDCOM RSG2488. Ce manuel décrit la large gamme de fonctionnalités de type transporteur disponibles avec RUGGEDCOM ROS (Rugged Operating System).

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

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 et 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* 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.

- **Surveillance et configuration à distance avec SINEC NMS**

  SINEC NMS 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.

  SINEC NMS est particulièrement adapté pour la surveillance et la configuration à distance de routeurs Siemens, d'interrupteurs, de serveurs série et d'équipement réseau sans fil WiMAX. Pour plus d'informations, voir https://www.siemens.com/sinec.

- **Device Management avec SINEC PNI**

  Les appareils RUGGEDCOM ROS sont compatibles avec SINEC PNI (Primary Network Initialization), un outil de mise en service des routeurs et des commutateurs RUGGEDCOM. Utilisez SINEC PNI pour ajouter rapidement un ou plusieurs appareils au réseau.

  Les fonctionnalités proposées par SINEC PNI incluent :

  - Gestion des appareils en masse
  - Modification, chargement ou téléchargement des configurations d'appareils
  - Mise à niveau ou rétrogradage du firmware
  - Gestion des adresses IP

- **SNMP (Simple Network Management Protocol)**

  SNMP fournit une méthode standardisée pour les stations de gestion de réseau afin d'interroger les appareils de différents fournisseurs. Les versions SNMP prises en charge incluent 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. Les nombreuses MIB (Management Information Base) permettent une intégration facile dans tout système de gestion de réseau (NMS). Une fonctionnalité de SNMP prise en charge par RUGGEDCOM ROS est la capacité de générer des *traps* en cas d'événements système. SINEC 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.

- **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 liens**

  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, l'autonégociation, 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 de pointe.

- **Filtrage de 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.

- **Prise en charge d'IPv4/IPv6**

  RUGGEDCOM ROS prend en charge les adresses IPv4 et IPv6 (pour des fonctionnalités sélectionnées). Pour plus d'informations sur la prise en charge de chaque protocole, voir "Prise en charge de protocole Internet (Page 12)".

- **Layer 3 Switching (commutation de couche 3)**

  L'appareil peut fonctionner comme commutateur de couche 3. Pour plus d'informations sur les règles Layer 3 Switching (commutation de couche 3) dans RUGGEDCOM ROS, voir "*Layer 3 (couche 3)* (Page 199)".

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 :

Remarque
Notez que les signaux GPS peuvent potentiellement être falsifiés ou bloqués par une tierce personne malveillante.

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 "Configuration de mots de passe (Page 135)".
- 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 "Gestion des clés et des certificats SSH/SSL (Page 154)".
- Utilisez une authentification avec clé publique SSH. Pour plus d'informations, voir "Gestion de clés publiques SSH (Page 157)".
- PAP (Password Authentication Protocol) n'est pas considéré comme un protocole sécurisé et, dans la mesure du possible, doit être utilisé dans un environnement réseau protégé.
- Soyez conscient de tous les protocoles de couche de liaison qui ne fournissent aucune authentification inhérente entre les points de terminaison, tels qu'ARP dans IPv4, découverte de voisins/DAD dans IPv6 et Wi-Fi dans des réseaux sans fil. Une entité malveillante peut exercer des faiblesses dans ces protocoles pour attaquer les hôtes, les commutateurs et les routeurs connectés à votre réseau de couche 2, par exemple, en empoisonnant les caches ARP des systèmes du sous-réseau et en interceptant ensuite le trafic. Des garanties appropriées contre des protocoles L2 non sécurisés, telles que la sécurisation de l'accès physique au réseau local et l'utilisation de protocoles sécurisés de couche supérieure, doivent être prises pour empêcher tout accès non autorisé au réseau.

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.
- Sauf indication contraire, l'accès automatique à la mémoire amovible doit être désactivé pour éviter des accès non autorisés. Pour plus d'informations sur la désactivation de l'accès à une mémoire amovible, voir "Activation/désactivation de l'accès automatique à la mémoire amovible (Page 45)".
- 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 non autorisé potentiel au chargeur de démarrage RUGGEDCOM ROS, qui comprend des outils pouvant être utilisés pour obtenir un accès complet à l'appareil. Pour plus d'informations sur la restriction d'accès au chargeur de démarrage (Boot Loader), voir "Gestion de l'accès à l'interface du chargeur de démarrage (Boot Loader) (Page 43)".
- 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 de l'appareil.
- Les ports miroir permettent le trafic bidirectionnel, c.-à-d. que l'appareil ne bloque pas le trafic entrant vers le(s) port(s) miroir. Pour une sécurité accrue, configurez le filtrage à l'entrée pour contrôler le flux de trafic lorsque la mise en miroir de ports est activée. Pour plus d'informations sur l'activation de la fonction miroir pour les ports, voir "Configuration de la mise en miroir du trafic (Page 80)". Pour plus d'informations sur l'activation du filtrage à l'entrée, voir "Configuration globale de VLAN (Page 173)".
- Pour une sécurité accrue, activez le filtrage à l'entrée sur tous les ports par défaut. Pour plus d'informations sur l'activation du filtrage à l'entrée, voir "Configuration globale de VLAN (Page 173)".
- 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 "Gestion de SNMP (Page 305)".
- 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.
- Désactivez RCDP si son utilisation n'est pas prévue.
- 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, référez-vous à "Gestion de journaux (Page 62)" et à la FAQ "How to Implement Secure, Unattended Logging in ROS (Comment implémenter une connexion sécurisée

sans surveillance dans ROS)" (https://support.industry.siemens.com/cs/ww/en/view/109756843).

- 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 par 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 comme HTTP, MMS, Telnet et RSH 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 "Gestion de la sécurité des ports (Port security) (Page 146)".

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, visitez le site Web Industrial Security [https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html] ou le site Web ProductCERT Security Advisories [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.
- 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 manuel et de configurer l'environnement en fonction des meilleures pratiques de défense en profondeur.

- Évitez 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 "Configuration de mots de passe (Page 135)".
- 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.

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.

1.3 Évènements de sécurité enregistrés

Les messages sont des messages d'événements de sécurité pouvant être générés par RUGGEDCOM ROS.

Catégorie	Message d'événement	Infrastructure	Degré de gravité	Condition
SE_LOCAL_SUCCESSFUL_LOGON	{date} {time} INFO {temperature} Console user '{username}' logged in with admin level	local0	Info	Un utilisateur connecté avec succès à l'appareil via une interface locale.
SE_LOCAL_UNSUCCESSFUL_LOGON	{date} {time} INFO {temperature} Failed Console user '{username}' login attempt	local0	Info	Échec de tentative de connexion à l'appareil via une interface locale.
SE_NETWORK_SUCCESSFUL_LOGON	{date} {time} INFO {temperature} {protocol} user '{username}' logged in with admin level {ip address}	local0	Info	Un utilisateur connecté avec succès à l'appareil via une interface réseau.
SE_NETWORK_UNSUCCESSFUL_LOGON	{date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address}	local0	Info	Échec de tentative de connexion à l'appareil via une interface réseau.
SE_LOGOFF	{date} {time} INFO {temperature} console user '{username}, cmd: Logged out	local0	Info	Un utilisateur connecté manuellement ou automatiquement en raison d'un timeout via une interface locale.
	{date} {time} INFO {temperature} {protocol} user	local0	Info	Un utilisateur connecté manuellement ou automatiquement en

Catégorie	Message d'événement	Infrastructure	Degré de gravité	Condition
	'{username}' ({ip address}), cmd: Logged out			raison d'un timeout via une interface réseau.
SE_USER_AUTH_RADIUS_SERVER_NOT_AVAILABLE	{date} {time} INFO {temperature} RADIUS Primary server is unreachable	local0	Info	Échec d'accès au serveur RADIUS ou aucune réponse de RADIUS.
SE_ACCESS_PWD_CHANGED	{date} {time} INFO {temperature} 'admin' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Admin Password - MODIFIED.	local0	Info	Un utilisateur authentifié a modifié son propre mot de passe.
	{date} {time} INFO {temperature} 'guest' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Guest Password - MODIFIED.	local0	Info	Un utilisateur authentifié a modifié le mot de passe d'un autre utilisateur.
SE_USER_ACCOUNT_CHANGED	{date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {guest}, new: {new username} - MODIFIED.	local0	Info	Compte utilisateur modifié ou affecté à un autre rôle.
SE_USER_ACCOUNT_DELETED	date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {username}, new:- MODIFIED.	local0	Info	Compte utilisateur supprimé.
SE_ACCOUNT_LOCKED_TEMP	{date} {time} WARN {temperature} Excessive failed {protocol} access/login attempts, service locked.	local0	Avertissement	Protection contre les attaques par force brute via un compte utilisateur temporairement verrouillé.
SE_SESSION_LOCKED_INACTIVITY	{date} {time} INFO 37C Console user 'admin' , cmd: Logged out	local0	Info	La session a été verrouillée après une période d'inactivité.
SE_RAS_SESSION_TERMINATED_INACTIVITY	{date} {time} INFO 37C HTTPS user 'admin' logged out (IP:192.168.0.200).	local0	Info	La session distante a été fermée après une période d'inactivité.
SE_UNSUCCESSFUL_RAS_LOGON	{date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address}	local0	Info	Échec de connexion de l'appareil d'accès à distance par un utilisateur à accès distant.
SE_RAS_LOGOFF	{date} {time} INFO {temperature} {protocol} user '{username}' {ip address}, cmd: loggd out	local0	Info	L'utilisateur à accès distant s'est déconnecté de

Catégorie	Message d'événement	Infrastructure	Degré de gravité	Condition
				l'appareil d'accès à distance.
SE_RAS_CONNECTION_CLOSED	{date} {time} INFO {protocol} user {'username'} closing connection {(ip address)}	local0	Info	Connexion d'accès à distance fermée.
SE_SUCCESSFUL_DEVICE_ IDENTIFICATION	{date} {time} INFO {temperature} {protocol} port 1 authorized addr {MAC address}, {VLAN ID} {date} {time} INFO{temperature} Secure port 1 learned addr {MAC address}, {VLAN ID}	local0	Info	Accès à l'appareil accordé en raison d'une authentification 802.1X Port réussie.
SE_UNSUCCESSFUL_DEVICE_ IDENTIFICATION	{date} {time}WARN 43C 802.1X port 1 auth failed, addr {MAC address}, {VLAN ID}	local0	Avertissement	Accès à l'appareil refusé en raison d'un échec d'authentification 802.1X Port.
SE_SUCCESSFUL_DEVICE_ AUTHENTICATION	{date} {time} INFO {temperature}{protocol} user {username} (pub id 1 fingerprint:{value}) logged in with {role} access {ip address}	local0	Info	Appareil authentifié avec succès via une authentification basée sur des certificats.
SE_AUDIT_LOG_CLEARED	{date} {time}INFO {temperature} Console user 'admin' , cmd: clearlogs {date} {time} INFO {temperature} clearlogs	local0	Info	L'utilisateur a supprimé la mémoire tampon de connexion locale.
SE_CONFIG_CHANGE	{date} {time} INFO {temperature} Console user '{username}', IP Services Inactivity Timeout, old: 5 min, new: Disable - MODIFIED {date} {time} INFO {temperature} Configuration changed	local0	Info	L'utilisateur a modifié des détails de configuration définis.
	{date} {time} INFO {temperature} Console user '{username}', Load Factory Defaults Defaults Choice, old: None, new: All - MODIFIED.	local0	Info	L'utilisateur a lancé une réinitialisation aux paramètres d'usine.
SE_SOFTWARE_INTEGRITY_CHECK_ FAILED	{date} {time} NOTE {temperature} SFTP put file main.bin from {ip address} by user {date} {time} INFO Console user '{username}', cmd: xmodem receive main.bin {date} {time} ERRO Downloaded file main.bin is invalid: Bad signature {date} {time} NOTE Downloaded file with invalid signature (-7711) {date} {time} Downloaded file main.bin is invalid: Body CRC invalid	local0	Erreur	Le contrôle d'intégrité du firmware/logiciel a détecté une erreur d'intégrité.

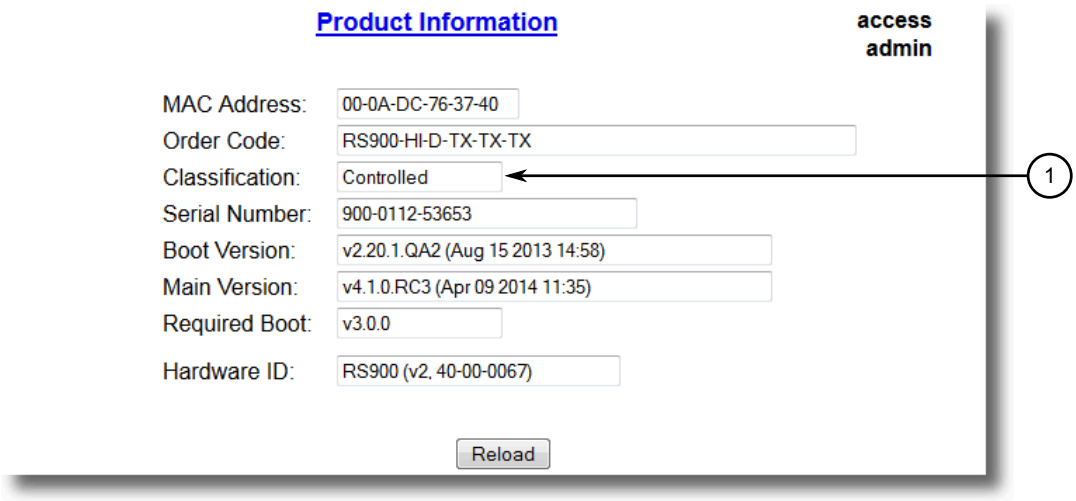
Catégorie	Message d'événement	Infrastructure	Degré de gravité	Condition
SE_BACKUP_SUCCESSFULLY_DONE	{date} {time} NOTE {temperature} config.csv copied to A:\config.csv	local0	Nota	Le système a créé une sauvegarde avec succès en cas de montage d'une mémoire externe.

1.4 Contrôlé ou non contrôlé

Les appareils RUGGEDCOM ROS sont disponibles en version contrôlée (C) ou non contrôlée (NC).

- Les commutateurs **contrôlés** possèdent plusieurs fonctionnalités de chiffrage.
- Les commutateurs **non contrôlés** ont des fonctionnalités de chiffrage limitées.

Pour déterminer si un appareil est classé comme contrôlé ou non contrôlé, accédez à ***Diagnostics » View Product Information***. Le paramètre **Classification** sur le formulaire **Product Information** indique si l'appareil est contrôlé ou non contrôlé.



① Zone Classification

Figure 1.1 Formulaire Product Information (exemple)

1.5 Normes de 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

Norme	Ports 10 Mbit/s	Ports 100 Mbit/s	Ports 1 000 Mb/s	Remarques
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

1.6 Prise en charge de protocole Internet

RUGGEDCOM ROS prend en charge les adresses IPv4 et les adresses de monodiffusion globales IPv6 pour certaines fonctionnalités. Pour plus d'informations, voir "Fonctionnalités prises en charge par IPv4 et/ou IPv6 (Page 12)".

1.6.1 Fonctionnalités prises en charge par IPv4 et/ou IPv6

Le tableau suivant indique les fonctionnalités prises en charge par les adresses IPv4 et/ou IPv6

Fonctionnalité	IPv4	IPv6
Ping	•	•
Telnet Server	•	•
SSH Server	•	•
SFTP Server	•	•
Web Server Access	•	•
SNMP Client (v1, v2c, v3)	•	•
Radius Client	•	•
TACACS+ Client	•	•
TFTP	•	•
NTP Server/Client	•	•
Client DHCP	•	
Remote Syslog Server	•	•
RSH	•	•
Serial Protocol	•	
ARP	•	
Network Discovery Messages[a]		•

[a] Prend en charge la sollicitation réseau et l'annonce réseau.

1.6.2 Adresse IPv4

Une adresse IPv4 a une longueur de 32 bits et est écrite en notation décimale avec points consistant en quatre octets séparés par des points. Chaque nombre est compris dans la plage allant de 0 à 255.

Exemple : 192.168.0.1

1.6.3 Adresse IPv6

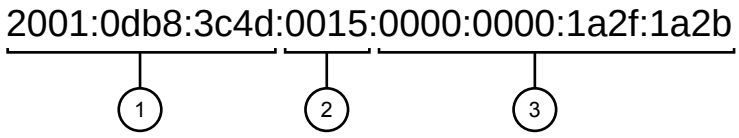
RUGGEDCOM ROS prend en charge les adresses de monodiffusion globales IPv6 pour la gestion.

Une adresse IPv6 a une longueur de 128 bits et est constituée de huit octets de 16 bits séparés par des double-points.

Les adresses IPv6 contiennent souvent des champs hexadécimaux consécutifs de zéros. Le double double-point *(::)* peut être utilisé pour comprimer des zéros dans une adresse. Par exemple, l'adresse IPv6 FF00:5402:0:0:0:0:0:32 peut être représentée sous la forme FF00:5402::32.

Une adresse IPv6 a la structure suivante :

- Les trois champs les plus à gauche (48 bits) contiennent le préfixe de site. Le préfixe décrit la topologie publique typiquement allouée à un site par un ISP.
- Le champ central est l'ID de sous-réseau de 16 bits allouée à un site spécifique. L'ID de sous-réseau décrit la topologie privée, aussi nommée topologie de site, car elle est interne au site.
- Les quatre champs les plus à droite (64 bits) contiennent l'ID d'interface.



① Préfixe de site
② ID de sous-réseau
③ ID d'interface

Figure 1.2 Exemple d'adresse de monodiffusion globale IPv6

1.7 Schéma de numérotation de ports

Pour une identification rapide, un numéro au format [emplacement]/[numéro] est affecté à chaque port sur un appareil RUGGEDCOM RSG2488. Les emplacements et les ports de la ligne supérieure sont numérotés de gauche à droite. Les emplacements et les ports de la ligne inférieure sont numérotés de droite à gauche. Par conséquent, le troisième port dans le premier emplacement serait étiqueté 1/3,

1 représentant l'emplacement et 3 le numéro de port. Tous les numéros de port sont sérigraphiés sur l'appareil.

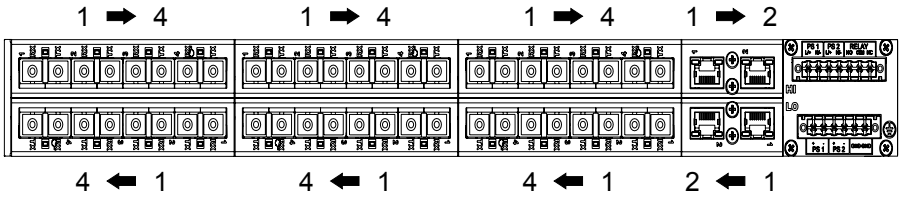


Figure 1.3 Numérotation de ports RUGGEDCOM RSG2488 (typique)

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

1.8 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, redirection vers 443	—	Uniquement redirection vers 443 sur des versions contrôlées

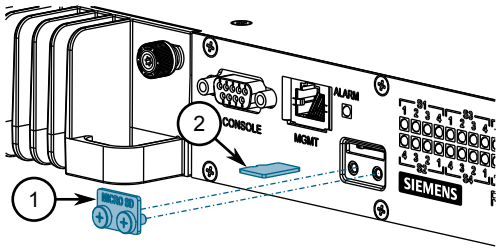
Services	Numéro de port	Service activé/ désactivé	Accès autorisé	Remarque
HTTPS	TCP/443	Activé (configurable)	Oui	Applicable uniquement à des versions contrôlées.
RSH	TCP/514	Désactivé (configurable)	Oui	Disponible uniquement via des interfaces de gestion.
TFTP	UDP/69	Désactivé (configurable)	Non	Disponible 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	
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	
PTP (IEEE 1588)	UDP/319 UDP/320	Désactivé (configurable)	Non	

1.9 Mémoire amovible

RSG2488 est doté d'un emplacement pour mémoire accessible par l'utilisateur prenant en charge un système de fichiers FAT16 ou FAT32 (File Allocation Table) standard compatible ISO/IEC 9293 sur une carte flash microSD/microSDHC.

Un avantage important de l'utilisation d'un système de fichiers basé sur FAT pour la mémoire amovible est que son contenu peut être modifié sur tout ordinateur à usage général comportant une interface microSD/microSDHC.

Remarque
La carte microSD/microSDHC est automatiquement formatée sur le système de fichiers FAT16 ou FAT32 si un système de fichiers autre que FAT16 ou FAT32 est chargé sur la carte.



① Plaque d'accès
② Carte Flash microSD/microSDHC

Figure 1.4 Emplacement de mémoire

Le but principal de la carte microSD/microSDHC amovible est de fournir un emplacement pour sauvegarder automatiquement l'image du firmware principal et la base de données de la configuration de l'appareil, ainsi que la possibilité de restaurer automatiquement l'image du firmware et/ou la configuration depuis la sauvegarde.Il peut également être utilisé pour récupérer l'accès à l'appareil si les données dans la mémoire flash interne sont corrompues.

Pendant un fonctionnement normal, l'appareil synchronise automatiquement les fichiers `main.bin` et `config.csv` sur l'appareil et la carte microSD/microSDHC. Si un fichier de firmware valide (`main.bin`) existe sur la carte microSD/microSDHC, RUGGEDCOM ROS charge et exécute le firmware depuis la carte microSD/microSDHC.

Lorsque l'appareil est redémarré, il compare les fichiers `main.bin` et `config.csv` sur l'appareil et la carte microSD/microSDHC. Si les fichiers sur l'appareil diffèrent de ceux sur la carte, l'appareil charge les fichiers depuis la carte dans le système de fichiers et les applique.

Il est possible d'utiliser la carte microSD/microSDHC amovible pour d'autres applications, notamment :

- Récupération rapide en cas de défaillance matérielle sur site
- Sauvegarde et restauration du firmware et des données de configuration
- Copie du firmware et de la configuration d'un appareil à un autre

- Exécution d'une mise à niveau automatique du firmware
- Récupération après un échec de mise à niveau du firmware ou de la reconfiguration
- Sauvegarde automatique des journaux système

Outre le fait qu'il est en mesure de sauvegarder automatiquement et de restaurer le firmware et la configuration à l'aide de la mémoire amovible, RUGGEDCOM ROS prend en charge un ensemble étendu d'utilitaires de ligne de commande pour manipuler les fichiers sur le système. La mémoire amovible présente un paradigme de disque avec lequel les utilisateurs de systèmes de fichiers basés sur FAT sont familiers, complété par des commandes CLI (Command Line Interface) telles que `dir`, `copy` et `move`. Pour une liste exhaustive des commandes CLI disponibles, voir "Commandes CLI disponibles (Page 26)".

Remarque
Pour obtenir des instructions sur la désactivation de l'accès automatique à la carte microSD/microSDHC, voir "Activation/désactivation de l'accès automatique à la mémoire amovible (Page 45)".

2 Utilisation de ROS

Ce chapitre décrit comment utiliser RUGGEDCOM ROS.

2.1 Ouverture de session

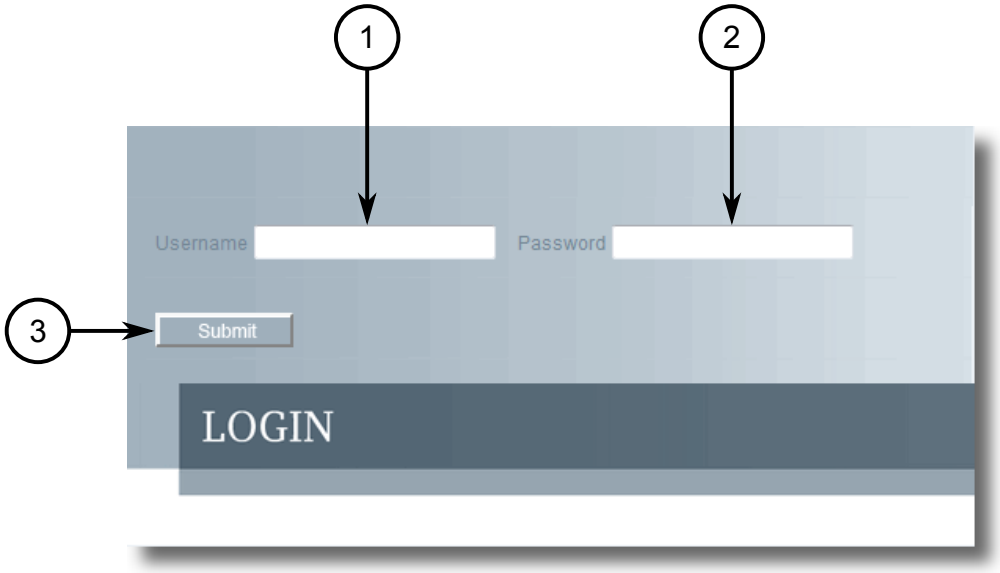
Procédez comme suit pour ouvrir une session sur l'appareil :

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 "Connexion à ROS (Page 49)".

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

① Zone User Name
② Zone Password

Figure 2.1 Écran d'ouverture de session SSH (interface de console)



① Zone Username
② Zone Password
③ Bouton Submit

Figure 2.2 Écran d'ouverture de session (interface web)

Remarque
Les nom d'utilisateur et mot de passe par défaut suivants sont définis sur l'appareil :

User Name	Password
admin	admin

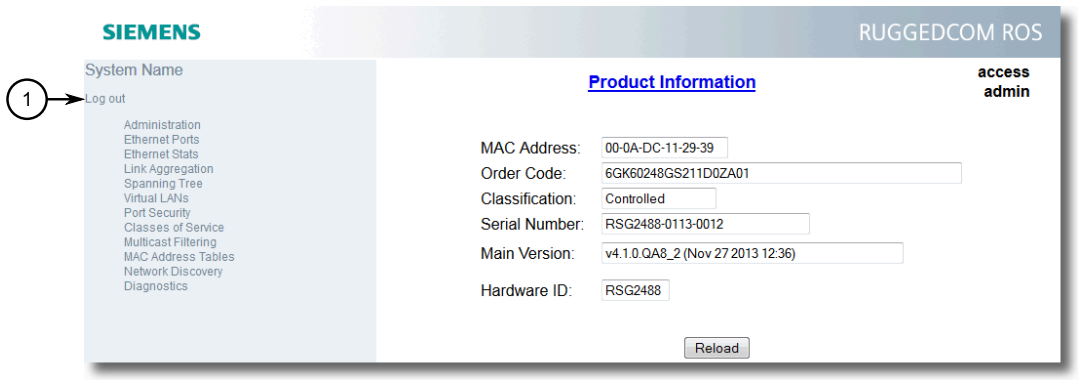
> **⚠ NOTA**
>
> **Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés**
>
> Pour éviter un accès non autorisé à l'appareil, assurez-vous de modifier le mot de passe administrateur par défaut avant de mettre l'appareil en service.
>
> Pour plus d'informations sur la modification de mots de passe, voir "Configuration de mots de passe (Page 135)".

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).

2.2 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**.



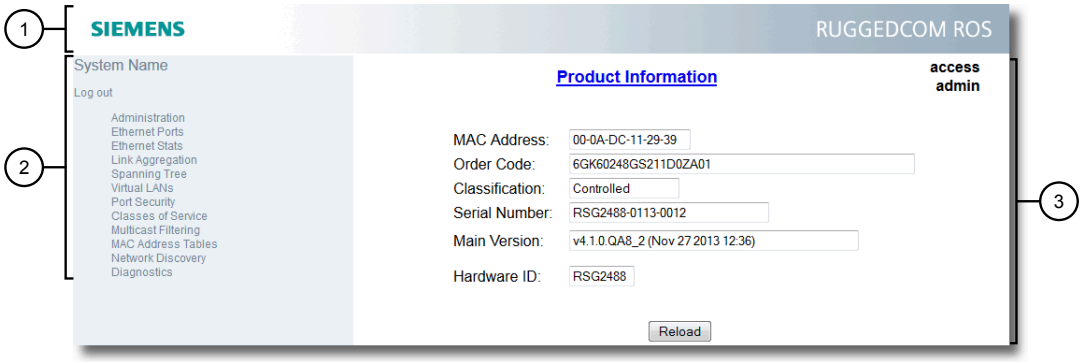
① Fermeture de session

Figure 2.3 Interface Web (exemple)

Remarque
S'il existe des modifications de 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.

2.3 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.



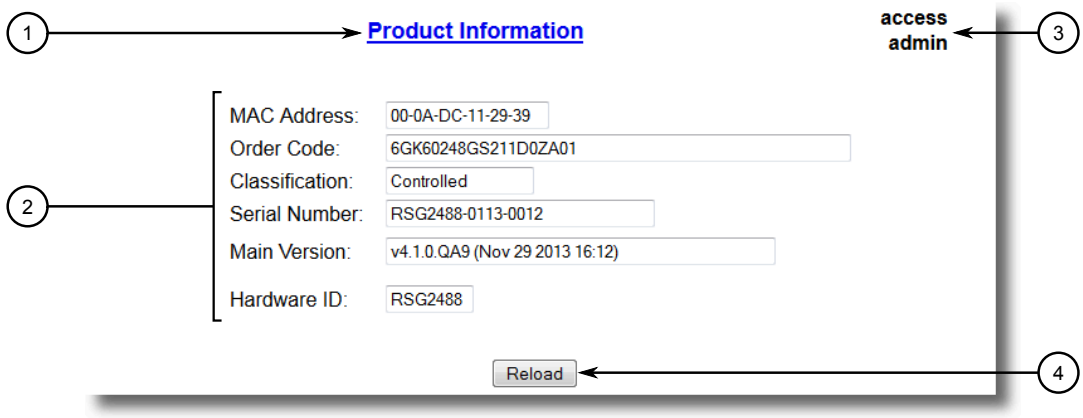
① Cadre supérieur
② Cadre latéral
③ Cadre principal

Figure 2.4 Exemple de disposition de l'interface Web

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 la déconnexion de RUGGEDCOM ROS, voir "Fermeture de session (Page 21)".
Principal	Le cadre principal affiche les paramètres et/ou les données liés à la fonctionnalité sélectionnée.

Chaque écran est composé d'un titre, du niveau d'accès de l'utilisateur, de paramètres et/ou de 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 "Gestion des alarmes (Page 118)".



① Titre
② Paramètres et/ou données
③ Niveau d'accès ou notification d'alarme
④ Bouton Reload

Figure 2.5 Exemple d'éléments d'un écran typique

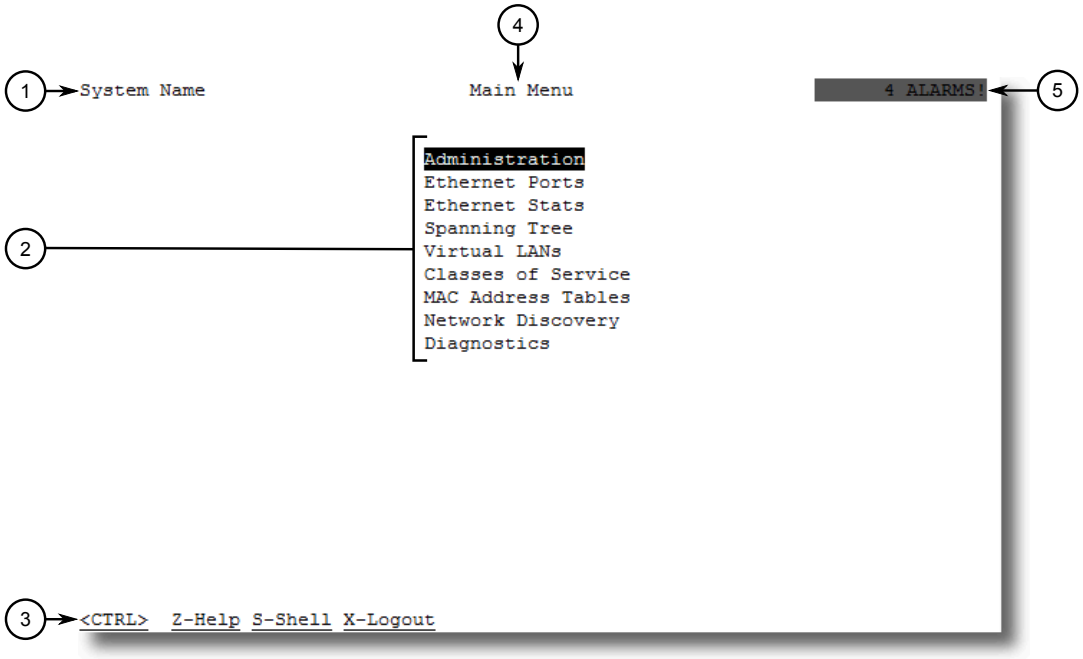
Remarque
Le cas échéant, l'interface Web peut être désactivée. Pour plus d'informations, voir "Activation/désactivation de l'interface Web (Page 118)".

2.4 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 "Configuration des services IP (Page 102)".

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.



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

Figure 2.6 Interface de console (exemple)

Remarque
L'identificateur système est configurable par l'utilisateur. Pour plus d'informations sur la définition du nom du système, voir "Configuration du système d'information (Page 117)".

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 à 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. **Remarque** Si la mémoire amovible (c.-à-d. la carte microSD/microSDHC) est présente, le changement de configuration mettra à jour les deux `config.csv` sur la mémoire flash et sur la mémoire amovible.
Ctrl + I	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.

2.5 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**.

2.5.1 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. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `all` indique toutes les alarmes disponibles	Invité, opérateur, administrateur
`arp`	Affiche le tableau de résolution d'adresse IP à MAC.	Administrateur
`attrib { filename } [ + | - ] [ W | H ]`	Définit et supprime des attributs de fichier.	Administrateur
`banner { -? } { -c } { -l } { -f } { -s <enter>{ text } | -s { text } } -e { line_number } -d { line_number }`	Modifie le fichier de bannière `banner.txt`. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *-?* } Affiche l'aide des options de commande. • { *-c* } efface le contenu du fichier de bannière. • { *-l* } affiche le fichier de bannière avec indexation des numéros de ligne. • { *-f* } restaure la bannière aux paramètres d'usine. • `-s <enter> { text }` entre le texte dans le fichier de bannière. Le texte de bannière existant est effacé et remplacé par le nouveau texte. Autorise jusqu'à 8 190 caractères et prend en charge des jeux de caractères de contrôle pour éditer le texte. • `-s { text }` entre le texte dans le fichier de bannière. Peut être utilisé pour modifier le fichier via terminal. Le texte de bannière existant est effacé et remplacé par le nouveau texte. Autorise jusqu'à 500 caractères et 250 mots au maximum. • `-e { line_number }` édite la ligne sélectionnée du fichier de bannière. • `-d { line_number }` supprime la ligne sélectionnée du fichier de bannière.	Administrateur
`chkdsk`	Vérifie si le système de fichiers contient des erreurs de disque.	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 suivants sont compris : • `all` efface les statistiques pour tous les ports • { *port* } est une liste séparée par des virgules de numéros de port (p. 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 suivants sont compris : • `all` efface les statistiques pour tous les ports • { *port* } est une liste séparée par des virgules de numéros de port (p. ex. 1,3-5,7)	Administrateur

Commande	Description	Utilisateurs autorisés
`clrstpstats`	Efface toutes les statistiques Spanning Tree (arbre couvrant).	Opérateur, administrateur
`cls`	Efface l'écran.	Invité, opérateur, administrateur

`copy`	Copie un fichier cible sur la mémoire interne ou amovible.
	Exemples :
	• Copie d'un fichier d'une mémoire amovible vers la mémoire interne
	`copy a:\config.csv config.csv`
	• Copie d'un fichier de la mémoire interne vers la mémoire amovible
	`copy config.csv a:\config.csv`
		Administrateur

`delete { filename }`	Supprime le fichier spécifié de la carte mémoire amovible.	Administrateur
`dir`	Imprime la liste de répertoires de la mémoire interne.	Invité, opérateur, administrateur
`dir { A: }`	Imprime la liste de répertoires de la carte mémoire amovible, si présente.	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. **⚠ NOTA** **Risque pour la configuration - risque de corruption du firmware** 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 { info { filename } | 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 suivants sont compris : • `info { filename }` 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`, voir "Gestion du système de fichiers flash (Page 40)".	Administrateur
`flashleds { timeout }`	Fait clignoter les indicateurs LED sur l'appareil pendant un nombre de secondes spécifié. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *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).	Administrateur

Commande	Description	Utilisateurs autorisés
`format { disk }`	Formate le disque spécifié (par exemple A:).	Administrateur
`fpgacmd`	Fournit un accès à l'outil de gestion FPGA pour la synchronisation du temps de dépannage.	Administrateur
`help { command }`	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 suivants sont compris : • { *command* } 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.	Invité, opérateur, administrateur
`label { disk } { string }`	Applique une étiquette au disque spécifié (par exemple A:).	Administrateur
`loaddflts`	Charge la configuration usine 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
`passwd { user_name } { new_password }`	Modifie le mot de passe utilisateur sélectionné. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *user_name* } est un user_name existant dans RUGGEDCOM ROS. • { *new_password* } est le nouveau mot de passe qui remplacera le mot de passe existant de l'utilisateur sélectionné. Cette commande n'est pas disponible dans les sessions Telnet.	Administrateur
`ping { address } { { count } | { 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 commandes ping avec un délai d'attente de réponse paramétré. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *address* } est l'adresse IP cible. • { *count* } 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 5 000 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	Invité, opérateur, administrateur

Commande	Description	Utilisateurs autorisés
	une commande Ping à cet appareil, la passerelle par défaut doit être programmée.	
`purgemac`	Purge le tableau d'adresses MAC.	Opérateur, administrateur
`random`	Affiche des valeurs initiales ou des nombres quelconques.	Administrateur
`rename { source } { destination }`	Renomme le fichier spécifié. Ajoutez un chemin au nouveau nom de fichier pour déplacer le ficher simultanément.	Administrateur
`reset`	Exécute 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 le partenaire de liaison a été verrouillé dans un état inapproprié. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `all` réinitialise tous les ports • { *port* } est une liste séparée par des virgules de numéros de port (p. ex. 1,3-5,7)	Opérateur, administrateur
`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 suivants sont compris : • { *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 suivants sont compris : • `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	Administrateur

Commande	Description	Utilisateurs autorisés
	• `insert` permet l'insertion de nouveaux enregistrements dans un tableau • `save` enregistre la base de données dans le stockage en mémoire non 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 "Utilisation de commandes SQL (Page 35)".	
`sshdigest`	Affiche les empreintes de clé hôte de l'appareil.	Administrateur
`sshkeygen [ rsa | dsa ] [ 1024 | 2048 | 3072 ] { N }`	Génère de nouvelles clés RSA ou DSA dans `ssh.keys`. Les clés peuvent avoir une longueur de 1 024, 2 048 ou 3 072 bits.	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 dans `ssl.crt`. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *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 256, 384 ou 521.	Administrateur
`svcmod -s { snmpaccess } { -i { GroupName } | -d { GroupName } } -sm { SecurityModel } -sl { SecurityLevel } -rv { ReadViewName } -wv { WriteViewName } -nv { NotifyViewName }`	Modifie les groupes d'accès SNMP. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `-i { GroupName }` crée un nouveau groupe d'accès avec un nom de groupe spécifié ou modifie les paramètres associés à un groupe d'accès spécifié, s'il existe déjà. • `-d { GroupName }` supprime un groupe d'accès spécifié • `-sm { SecurityModel }` spécifie le modèle de sécurité à utiliser • `-sl { SecurityLevel }` spécifie le niveau de sécurité SNMP à attribuer au groupe d'accès spécifié. Les valeurs autorisées sont 'authPriv' (c.-à-d. communication avec authentification et confidentialité), 'authNoPriv' (c.-à-d. communication avec authentification et sans confidentialité), ou 'noAuthnoPriv' (c.-à-d. communication sans authentification ni confidentialité). • `-rv { ReadViewName }` identifie les arborescences MIB auxquelles cette entrée donne un accès en lecture. Les valeurs autorisées sont 'noView', 'V1Mib', ou 'allOfMib'. • `-wv { WriteViewName }` identifie les arborescences MIB auxquelles cette entrée donne un accès en écriture. Les valeurs autorisées sont 'noView', 'V1Mib', ou 'allOfMib'. • `-nv { NotifyViewName }` identifie les arborescences MIB auxquelles cette entrée donne un accès à des	Administrateur

Commande	Description	Utilisateurs autorisés
	notifications. Les valeurs autorisées sont 'noView', 'V1Mib', ou 'allOfMib'.	
`svcmod -s { snmp group } { -i { User Name } | -d { User Name } } -sm { SecurityModel } -g { group }`	Modifie les mappages sécurité sur groupe (security-to-group maps) SNMP. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `-i { UserName } -sm { SecurityModel }` crée un nouveau nom d'utilisateur et un nouveau profil de sécurité comme spécifié ou modifie les paramètres associés à un nom d'utilisateur et un profil de sécurité donnés, s'ils existent déjà. • `-d { UserName } -sm { SecurityModel }` supprime un nom d'utilisateur et un profil de sécurité spécifiés • `-g { group }` spécifie le groupe auquel le nom d'utilisateur et le profil de sécurité appartiennent	Administrateur
`svcmod -s { snmpuser } { -i { User Name } | -d { User Name } } -c { Community } -ip { IP } -ap { protocol } -ak { key } -pp { protocol } -pk { key }`	Modifie les utilisateurs SNMP. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `-i { UserName }` crée un nouveau nom d'utilisateur comme spécifié ou modifie les paramètres associés à un nom d'utilisateur donné, s'il existe déjà. • `-d { UserName }` supprime un nom d'utilisateur spécifié. • `-c { Community }` spécifie la chaîne de communauté SNMP (pour SNMPv1 ou SNMPv2c). • `-ip { IP }` configure une adresse IP à utiliser pour l'authentification SNMP. • `-ap { protocol }` configure une authentification SNMP via un protocole d'authentification spécifié. Les valeurs autorisées sont 'noAuth', 'HMACMD5', ou 'HMACSHA'. • `-ak { key }` définit une clé secrète (de 0 ou 6+ caractères) à utiliser pour l'authentification SNMP • `-pp { protocol }` configure le chiffrement des données via un protocole de confidentialité spécifié. Les valeurs autorisées sont 'noPriv' or 'CBC-DES.' • `-ak { key }` définit une clé secrète (de 0 ou 6+ caractères) à utiliser pour le chiffrement des données	Administrateur
`svcmod -s { radius } { -ip { 1 } | -ip { 2 } } -ip { IP } -ak { AuthKey } -pt { Port } -ux { UserNameExtension } -mr { MaxRetries } -to { timeout }`	Modifie le serveur de sécurité RADIUS. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `-ip { 1 }` définit le serveur spécifié comme serveur RADIUS principal • `-ip { 2 }` définit le serveur spécifié comme serveur RADIUS de sauvegarde • `-ip { 2 } -ip` supprime le serveur RADIUS principal • `-ip { 1 } -ip` supprime le serveur RADIUS de sauvegarde • `-ip { IP }` spécifie l'adresse IP du serveur RADIUS	Administrateur

Commande	Description	Utilisateurs autorisés
	• `-ak { AuthKey }` spécifie une clé d'authentification à partager avec le serveur RADIUS • `-pt { Port }` spécifie le numéro de port du port IP sur le serveur RADIUS • `-ux { UsernameExtension }` définit un affixe à ajouter lorsqu'un nom d'utilisateur est envoyé au serveur RADIUS pour authentification. Les valeurs peuvent comprendre des mots-clés prédéfinis (entre délimiteurs %) ou des chaînes de caractères définies par l'utilisateur. Les mots clés prédéfinis sont '%Username%' (c.-à-d. le nom associé au profil utilisateur), '%IPaddr%' (c.-à-d. l'adresse IP de gestion du Network Access Server), '%SysName%' (c.-à-d. le nom système donné à l'appareil), et '%SysLocation%' (c.-à-d. l'emplacement physique de l'appareil). • `-mr { MaxRetries }` spécifie le nombre maximum de tentatives par l'authentificateur d'authentification de l'utilisateur en cas de défaillance. En cas de dépassement de la valeur spécifiée, l'authentification échoue. • `-to { timeout }` spécifie le délai d'attente en millisecondes (ms) pendant lequel l'authentificateur attend une réponse du serveur RADUS avant de tenter à nouveau une authentification.	
`svcmod -s { tacacs plus } { -ip { 1 } | -ip { 2 } } -ip { IP } -ak { Auth Key } -pt { Port } -ux { UsernameExten sion } -mr { Max Retries } -to { ti meout } -apl { Ad minPrivilege } -opl { OperPrivilege } -gpl { GuestPrivi lege }`	Modifie le serveur de sécurité TACACS+. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `-ip { 1 }` définit le serveur spécifié comme serveur TACACS+ principal • `-ip { 2 }` définit le serveur spécifié comme serveur TACACS+ de sauvegarde • `-ip { 2 } -ip` supprime le serveur TACACS+ principal • `-ip { 1 } -ip` supprime le serveur TACACS+ de sauvegarde • `-ip { IP }` spécifie l'adresse IP du serveur TACACS+ • `-ak { AuthKey }` spécifie une clé d'authentification à partager avec le serveur TACACS+ • `-pt { Port }` spécifie le numéro de port du port IP sur le serveur TACACS+ • `-ux { UsernameExtension }` définit un affixe à ajouter lorsqu'un nom d'utilisateur est envoyé au serveur TACACS+ pour authentification. Les valeurs peuvent comprendre des mots-clés prédéfinis (entre délimiteurs %) ou des chaînes de caractères définies par l'utilisateur. Les mots clés prédéfinis sont '%Username%' (c.-à-d. le nom associé au profil utilisateur), '%IPaddr%' (c.-à-d. l'adresse IP de gestion du Network Access Server), '%SysName%' (c.-à-d. le nom système donné à l'appareil), et '%SysLocation%' (c.-à-d. l'emplacement physique de l'appareil). • `-mr { MaxRetries }` spécifie le nombre maximum de tentatives par l'authentificateur d'authentification de l'utilisateur en cas de défaillance. En cas de dépassement de la valeur spécifiée, l'authentification échoue.	Administrateur

Commande	Description	Utilisateurs autorisés
	• `-to { timeout }` spécifie le délai d'attente en millisecondes (ms) pendant lequel l'authentificateur attend une réponse du serveur TACACS+ avant d'effectuer une nouvelle tentative d'authentification. • `-apl { AdminPrivilege }` définit le niveau auquel les utilisateurs administrateurs peuvent configurer le serveur TACACS+. Les valeurs doivent correspondre à une ou plusieurs options définies numériquement (entre 0 et 15) dans le fichier de configuration TACACS+. • `-opl { OperPrivilege }` définit le niveau auquel les utilisateurs opérateurs peuvent configurer le serveur TACACS+. Les valeurs doivent correspondre à une ou plusieurs options définies numériquement (entre 0 et 15) dans le fichier de configuration TACACS+. • `-gpl { GuestPrivilege }` définit le niveau auquel les utilisateurs invités peuvent configurer le serveur TACACS+. Les valeurs doivent correspondre à une ou plusieurs options définies numériquement (entre 0 et 15) dans le fichier de configuration TACACS+.	
`telnet { dest }`	Ouvre une session telnet. Utilisez **Ctrl-C** pour fermer la session. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *dest* } est l'adresse IP du serveur	Invité, opérateur, administrateur
`tftp { address } [ put | get ] { source } { target }`	Ouvre une session TFTP. Utilisez **Ctrl-C** pour fermer la session. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *address* } est l'adresse IP du serveur TFTP distant • `put` indique que TFTP chargera le fichier source pour remplacer le fichier de destination • `get` indique que TFTP téléchargera le fichier source pour remplacer le fichier de destination • { *source* } est le nom du fichier source • { *target* } est le nom du fichier à remplacer	Administrateur
`trace`	Démarre le traçage des événements. Exécutez `trace ?` pour obtenir plus d'aide.	Opérateur, administrateur
`type { filename }`	Affiche le contenu d'un fichier texte. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • { *filename* } est le nom du fichier à lire	Invité, opérateur, administrateur
`usermod { -b | -r { username } | { old_user_name } { new_user_name } }`	Un jeu de commandes permettant d'afficher, supprimer et modifier des noms d'utilisateur existants. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `-b` navigue dans les noms d'utilisateur existants dans RUGGEDCOM ROS. • `-r { username }` supprime un nom d'utilisateur pour désactiver le compte • { *old_user_name* } et { *new_user_name* } définissent le nom d'utilisateur à modifier	Administrateur

Commande	Description	Utilisateurs autorisés
	Cette commande n'est pas disponible dans les sessions Telnet.	
`version`	Imprime la version logicielle	Invité, opérateur, administrateur
`xmodem { send | receive } { filename }`	Ouvre une session XModem. Les paramètres optionnels facultatifs et/ou obligatoires suivants sont compris : • `send` envoie le fichier au client. • `receive` reçoit le fichier du client. • { *filename* } est le nom du fichier à lire.	Opérateur, administrateur

2.5.2 Traçage d'événements

La commande CLI trace représente un moyen de tracer le fonctionnement de différents protocoles pris en charge par l'appareil. 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 "Utilisation de l'interface de ligne de commande (Page 25)".
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
   ```

2.5.3 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.

2.5.4 Utilisation de commandes SQL

RUGGEDCOM ROS fournit un utilitaire de commandes *similaires 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 "Commandes CLI disponibles (Page 26)".

Remarque
L'accès en lecture/écriture à des tableaux contenant des mots de passe ou des phrases secrètes partagées n'est pas disponible à l'aide de commandes SQL.

2.5.4.1 Recherche du tableau correct

De nombreuses commandes SQL fonctionnent dans des tableaux spécifiques de 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 tableau de la 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
```

2.5.4.2 Récupération d'informations

La présente rubrique décrit les différentes méthodes permettant de récupérer des informations depuis 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 depuis un tableau

Utilisez la commande suivante pour récupérer des informations depuis 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
   1/1  Port 1          1/1             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/2  Port 2          1/2             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/3  Port 3          1/3             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/4  Port 4          1/4             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
   1/1  Port 1          1/1             1000T       Enabled  On    Auto  Auto  Off
   Off on
   1/2  Port 2          1/2             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/3  Port 3          1/3             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/4  Port 4          1/4             1000T       Enabled  On    Auto  Auto  Off
   Off On

4 records selected
```

2.5.4.3 Modification de valeurs dans un tableau

Utilisez la commande suivante pour modifier les valeurs 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
```

Des 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
```

2.5.4.4 Réinitialisation d'un tableau

Utilisez la commande suivante pour réinitialiser un tableau à ses valeurs par défaut :

```
sql default into  { table }
```

Où :

- { *table* } est le nom du tableau

2.5.4.5 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:\
```

2.6 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 ou un port dans un emplacement spécifique.

Sélectionnez un port unique en spécifiant l'emplacement et le numéro de port :

1/2

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

1/1-1/4

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

1/1,1/4,1/6,1/9

Seuls les ports au sein du même emplacement peuvent être sélectionnés dans un même groupe. Pour sélectionner un groupe de ports de différents emplacements, définissez une liste de groupes séparée par des virgules :

1/1-1/4,2/1-2/4,3/1-3/3

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.

2.7 Gestion du système de fichiers flash

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

2.7.1 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 "Utilisation de l'interface de ligne de commande (Page 25)".
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
------------------------------------------------------------------
main.bin                   0xFE959AE0   0x002C5493 (2905235)
syslog.txt                 0xFE100080   0x001BFF80 (1834880)
.
.
.

Free Space: 19792360
Used Space: 11664720
Fragmented Space: 5830423
------------------------------------------------------------------
```

2.7.2 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 "Utilisation de l'interface de ligne de commande (Page 25)".
2. Affichez les informations concernant un fichier en saisissant :

   ```
   flashfiles info  { filename }
   ```

   Où :

   - `{ filename }` 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-MPC83
   File name        : main.bin
   Firmware version : v5.6.0
   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
   ```

2.7.3 Défragmentation du système de fichiers flash

La mémoire flash est défragmentée automatiquement lorsque la mémoire disponible est insuffisante 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 les 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 "Utilisation de l'interface de ligne de commande (Page 25)".
2. Défragmentez la mémoire flash en saisissant :

   ```
   flashfiles defrag
   ```

2.8 Accès en mode BIST

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

⚠ NOTA

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 du support client Siemens.

Remarque
Le mode BIST est désactivé par défaut en usine. Toutes les entrées de console sont ignorées et les utilisateurs sont automatiquement dirigés vers l'interface utilisateur RUGGEDCOM ROS.

Procédez comme suit pour activer l'accès au mode BIST :

1. À l'aide d'un PC/d'un ordinateur portable, créez un fichier ayant pour nom `bootoption.txt` et incluez-y la ligne suivante :

   ```
   Security=no
   ```

2. Chargez le fichier dans l'appareil et redémarrez ce dernier.

Remarque
Accédez à BIST et le chargeur de démarrage (boot loader) peut être révoqué ultérieurement en reparamétrant `no` sur `yes`.

Procédez comme suit pour accéder au mode BIST :

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

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 "Connexion directe (Page 49)".
3. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".
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.

Il est également possible d'accéder aux fonctions BIST en mode factory. Pour plus d'informations sur le mode factory, voir "Commandes CLI disponibles (Page 26)".

2.9 Gestion de l'accès à l'interface du chargeur de démarrage (Boot Loader)

La section suivante décrit comment activer/désactiver l'interface du chargeur de démarrage et y accéder dans RUGGEDCOM ROS.

Remarque
L'accès à l'interface du chargeur de démarrage est désactivé en usine par défaut sur tous les appareils utilisant RUGGEDCOM ROS v5.6. Toutes les entrées de console sont ignorées et les utilisateurs sont automatiquement dirigés vers l'interface utilisateur RUGGEDCOM ROS.

Remarque
Siemens recommande de désactiver l'accès à l'interface du chargeur de démarrage après une mise à niveau depuis une version ancienne de RUGGEDCOM ROS ver RUGGEDCOM ROS v5.6. Pour plus d'informations sur la désactivation du chargeur de démarrage, voir "Activation/désactivation de l'accès à l'interface du chargeur de démarrage (Boot Loader) (Page 43)".

2.9.1 Activation/désactivation de l'accès à l'interface du chargeur de démarrage (Boot Loader)

Procédez comme suit pour activer ou désactiver l'accès à l'interface du chargeur de démarrage :

Création du fichier bootoption.txt

Pour activer ou désactiver l'accès à l'interface du chargeur de démarrage, le fichier `bootoption.txt` doit être disponible sur l'appareil.

Si ce n'est pas le cas, procédez comme suit :

1. À l'aide d'un PC/d'un ordinateur portable, créez un fichier appelé `bootoption.txt`.

   ⚠ NOTA

   Si le paramètre *Security* est commenté à l'aide du caractère dièse (#) ou n'existe pas dans le fichier, il est créé par RUGGEDCOM ROS avec sa valeur par défaut après le redémarrage.

2. Incluez la ligne suivante dans le fichier :

   ```
   Security = [No | Yes]
   ```

   - *Security = No* active l'accès à l'interface du chargeur de démarrage (Boot Loader).
   - *Security = Yes* désactive l'accès à l'interface du chargeur de démarrage (Boot Loader). Correspond à la valeur par défaut.
3. Chargez le fichier dans l'appareil et redémarrez ce dernier.

Activation du chargeur de démarrage

Procédez comme suit pour activer l'accès au chargeur de démarrage :

1. À l'aide d'un PC/ordinateur portable, accédez au fichier `bootoption.txt`.
2. Localisez la ligne suivante et modifiez-la de

   ```
   Security = Yes
   ```

   à

   ```
   Security = No
   ```
3. Chargez le fichier dans l'appareil et redémarrez ce dernier.

Désactivation du chargeur de démarrage

Procédez comme suit pour désactiver l'accès au chargeur de démarrage :

1. À l'aide d'un PC/ordinateur portable, accédez au fichier `bootoption.txt`.
2. Localisez la ligne suivante et modifiez-la de

   ```
   Security = No
   ```

   à

   ```
   Security = Yes
   ```
3. Chargez le fichier dans l'appareil et redémarrez ce dernier.

2.9.2 Accès à l'interface du chargeur de démarrage (Boot Loader)

Procédez comme suit pour accéder à l'interface du chargeur de démarrage :

1. Connectez-vous à RUGGEDCOM ROS via le raccordement de console RS-232 et une application de terminal. Pour plus d'informations, voir "Connexion directe (Page 49)".
2. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".
3. Dès que l'appareil commence à démarrer, appuyez sur **Ctrl-Z**. L'invite de commande pour Uboot s'affiche.

   ```
   =>
   ```

4. Saisissez `help` pour afficher une liste d'options disponibles sous Uboot.

2.9.3 Réglage de la source de démarrage

Par défaut, l'appareil démarre depuis sa mémoire flash interne. Cependant, RUGGEDCOM ROS prend en charge le démarrage depuis la carte microSD/microSDHC insérée si vous le souhaitez.

Procédez comme suit pour régler la source de démarrage :

⚠ NOTA

Pour autoriser le démarrage à partir de la carte microSD/microSDHC, l'accès automatique à la mémoire amovible doit être activé. Pour plus d'informations, voir "Activation/désactivation de l'accès automatique à la mémoire amovible (Page 45)".

1. À l'aide d'un PC/d'un ordinateur portable, créez un fichier appelé `bootoption.txt`.

   ⚠ NOTA

   Si le paramètre *BootOrderFirstRemovable* est soit commenté à l'aide du caractère dièse (#) soit n'existe pas dans le fichier, il est créé par RUGGEDCOM ROS avec sa valeur par défaut après le redémarrage.

2. Incluez la ligne suivante dans le fichier :

   ```
   BootOrderFirstRemovable = [No | Yes]
   ```

   - *BootOrderFirstRemovable = No* active le démarrage depuis la mémoire flash interne. Correspond à la valeur par défaut.
   - *BootOrderFirstRemovable = Yes* active le démarrage depuis la microSD/microSDHC card.

3. Chargez le fichier dans l'appareil et redémarrez ce dernier.

2.10 Activation/désactivation de l'accès automatique à la mémoire amovible

RUGGEDCOM ROS peut synchroniser automatiquement le firmware, la configuration et les fichiers-journaux entre un appareil et sa RUGGEDCOM ROS carte microSD/microSDHC.

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

Sauf indication contraire, l'accès automatique à la mémoire amovible doit être désactivé.

Procédez comme suit pour configurer l'accès automatique à la mémoire amovible :

1. À l'aide d'un PC/d'un ordinateur portable, créez un fichier appelé `bootoption.txt`.

   ⚠ NOTA

   Si le paramètre *DisableAutoAccessRemovable* est commenté à l'aide du caractère dièse (#) ou n'existe pas dans le fichier, il est créé par RUGGEDCOM ROS avec sa valeur par défaut après le redémarrage.

2. Pour désactiver l'accès automatique à la mémoire amovible, ajoutez la ligne suivante au fichier :

   ```
   DisableAutoAccessRemovable = Yes
   ```

   Remarque
   La commande `DisableAutoAccessRemovable` affecte uniquement des actions automatiques. Même lorsque l'accès automatique à la mémoire amovible est désactivé, les utilisateurs peuvent copier manuellement les fichiers entre un appareil et sa carte microSD/microSDHC.

3. Pour réactiver l'accès automatique à la mémoire amovible après l'avoir désactivé, ajoutez la ligne suivante au fichier :

   ```
   DisableAutoAccessRemovable = No.
   ```

   No est la valeur par défaut.

4. Chargez le fichier dans l'appareil.
5. Redémarrez l'appareil.

2.11 Activation/désactivation du service de console

le service de console local est activé par défaut dans RUGGEDCOM ROS. Pour plus de sécurité, un administrateur peut désactiver et réactiver l'accès à la console série RS-232 comme souhaité.

Remarque
L'activation/la désactivation du service de console n'est disponible qu'à l'aide de commandes SQL. Pour plus d'informations, voir "Utilisation de commandes SQL (Page 35)".

Procédez comme suit pour activer/désactiver l'accès au service de console :

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 "Utilisation de l'interface de ligne de commande (Page 25)".

2. Activez ou désactivez le service de console en saisissant soit :

   Enabling

   ```
   sql update consoleServices SET Local Console Service = En
   abled
   ```

   Disabling

   ```
   sql update consoleServices SET Local Console Service = Di
   sabled
   ```

Les modifications seront effectives à la prochaine connexion à la console locale.

3 Mise en route

Ce paragraphe décrit les tâches de démarrage à effectuer au cours de la première mise en service de l'appareil. Ces tâches comprennent la connexion à l'appareil et l'accès à la RUGGEDCOM ROS , ainsi que la configuration d'un réseau de base.

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

Siemens recommande de procéder comme suit avant la mise en service de l'appareil :

- Remplacez le certificat SSL auto-signé fourni en usine par un certificat signé par une autorité de certification (CA) de confiance.
- Configurez le client SSH pour qu'il utilise *diffie-hellman-group14-sha1* ou mieux

3.1 Connexion à ROS

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

3.1.1 Adresse IP par défaut

L'adresse IP par défaut pour l'appareil est comme suit :

Port	Adresse/masque IP
MGMT	10.0.0.1/8
Tous les autres ports Ethernet	192.168.0.1/24

3.1.2 Connexion directe

Il est possible d'accéder à RUGGEDCOM ROS via une connexion directe console série RS-232 ou Ethernet 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. Une connexion Ethernet fournit un accès à l'interface Web.

Pour plus de sécurité, le service de console peut être désactivé le cas échéant. Pour plus d'informations sur la désactivation du service de console, voir "Activation/désactivation du service de console (Page 46)".

Utilisation du port console série RS-232

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 "manuel d'installation RSG2488".
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 "Ouverture de session (Page 20)".

Utilisation d'un port Ethernet

Procédez comme suit pour établir une connexion Ethernet directe à l'appareil :

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.

   Par défaut, l'appareil a une adresse IP et un sous-réseau différents pour deux types d'interface IP, chacun mappé sur un ou plusieurs ports physiques :

Port	Adresse/masque IP
MGMT	10.0.0.1/8
Tous les autres ports Ethernet	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. Lancez le client SSH sur le poste de travail et connectez-vous à admin@{adresse ip}, l'{adresse ip} étant l'adresse IP pour le port connecté au réseau. L'invite de connexion s'affiche :

   ```
   Using username "admin".
   admin@192.168.0.2's password:
   ```
3. Connectez-vous à RUGGEDCOM ROS. Pour plus d'informations sur la connexion à RUGGEDCOM ROS, voir "Ouverture de session (Page 20)".

3.1.3 Connexion à distance

Vous pouvez accéder àRUGGEDCOM ROS de façon sûre et à distance 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, il 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 défaut, l'appareil a une adresse IP et un sous-réseau différents pour deux types d'interface IP, chacun mappé sur un ou plusieurs ports physiques :

Port	Adresse/masque IP
MGMT	10.0.0.1/8
Tous les autres ports Ethernet	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 (Page xvii)".

   ⚠ NOTA

   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 configurer le navigateur pour qu'il accepte le certificat en toute sécurité. Une fois le certificat accepté, toutes les communications avec le serveur Web via ce navigateur sont sécurisées.

   ⚠ NOTA

   Les adresses IPv6 doivent être mises entre crochets (p. ex. **https://[2001:db8:123::2228]**).

3. Dans la barre d'adresse, saisissez l'adresse IP pour le port connecté au réseau. 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 "Ouverture de session (Page 20)". Pour plus d'informations sur l'interface Web, voir "Utilisation de l'interface Web (Page 22)".

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 "Configuration des services IP (Page 102)".

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 "Ouverture de session (Page 20)".

3.2 Configuration d'un réseau de base

Procédez comme suit pour configurer un réseau de base :

1. Connectez un ordinateur à l'interface de gestion de l'appareil et configurez l'ordinateur pour qu'il soit sur le même sous-réseau que le port.
2. Configurez l'ordinateur pour utiliser l'adresse du port MGMT comme passerelle par défaut.
3. Connectez l'un des ports commutés d'un module disponible à un commutateur connecté à un LAN.
4. Assurez-vous que l'ordinateur connecté à un commutateur est sur le même sous-réseau que le commutateur.
5. Configurez le commutateur et tous les ordinateurs en aval de manière à ce qu'ils utilisent l'adresse IP VLAN1 comme passerelle par défaut. L'adresse IP par défaut est 192.168.0.1.
6. Assurez-vous que tous les ordinateurs connectés à l'appareils peuvent s'envoyer des messages ping.

4 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.

4.1 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.

Cet écran affiche les informations suivantes :

Paramètre	Description
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF Indique l'adresse MAC unique de l'appareil.
`Order Code`	**Synopsis :** Chaîne de 57 caractères Affiche le code de commande de l'appareil.
`Classification`	**Synopsis :** Chaîne de 15 caractères Fournit la classification système. La valeur`Controlled`indique que le firmware principal est une version contrôlée. La valeur`Non-Controlled`indique que le firmware principal est une version non-contrôlée. 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 :** Chaîne de 31 caractères Indique le numéro de série de l'appareil.
`Main Version`	**Synopsis :** Chaîne de 47 caractères Indique la version et la date de version du système d'exploitation principal.
`Hardware ID`	Indique le type, le numéro de pièce et le niveau de révision du matériel. Exemple :RSG2488,RSG2488v2

Paramètre	Description
`Descr`	**Synopsis :** Chaîne de 57 caractères Description de produit basée sur l'ID matériel, le code de commande et la classification.

4.2 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.

Cet écran affiche les informations suivantes :

Paramètre	Description
`Running Time`	**Synopsis :** DDDD days, HH:MM:SS Temps écoulé depuis la dernière mise sous tension de l'appareil.
`CPU Usage`	**Synopsis :** Un entier compris entre 0.0 et 100.0 Pourcentage de cycles de CPU disponibles utilisés pour le fonctionnement de l'appareil mesuré pour la dernière seconde.
`RAM Total`	**Synopsis :** Un entier compris entre 0 et 4294967295 Taille totale de la mémoire RAM dans le système.
`RAM Free`	**Synopsis :** Un entier compris entre 0 et 4294967295 Taille totale de la mémoire RAM encore disponible.
`RAM Low Watermark`	**Synopsis :** Un entier compris entre 0 et 4294967295 Taille de la mémoire RAM qui n'a jamais été utilisée pendant l'exécution du système.
`DMA RAM Free`	**Synopsis :** Un entier compris entre 0 et 4294967295 Taille totale de la mémoire RAM DMA encore disponible.
`DMA RAM Low Watermark`	**Synopsis :** Un entier compris entre 0 et 4294967295 Taille de la mémoire RAM DMA qui n'a jamais été utilisée pendant l'exécution du système.
`Temperature`	**Synopsis :** Un entier compris entre -32768 et 32767 Température de la carte CPU.
`Free Rx Bufs`	**Synopsis :** Un entier compris entre 0 et 4294967295 Tampons Rx libres.
`Free Tx Bufs`	**Synopsis :** Un entier compris entre 0 et 4294967295 Tampons Tx libres.

4.3 Affichage de l'état des alimentations

Pour afficher l'état actuel des alimentations, accédez à ***Diagnostics » Power Supply Status***. Le tableau **Power Supply Status** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`ID`	**Synopsis :** Un entier compris entre 1 et 2 ID de l'alimentation.
`Voltage`	**Synopsis :** Un entier compris entre 0 et 4294967295 Tension de sortie en millivolts.
`Current`	**Synopsis :** Un entier compris entre 0 et 4294967295 Courant de sortie en milliampères.
`Temperature`	**Synopsis :** Un entier compris entre -32768 et 32767 Température de l'alimentation.
`InStatus`	**Synopsis :** [---- | Out of range | Good] Spécifie si la tension d'entrée de l'alimentation se trouve dans la plage ou non. Pour les alimentations doubles CC/CC, la plage de tension d'entrée se trouve entre 36 et 72 V. Pour les alimentations doubles CA/CC, la plage de tension d'entrée se trouve entre 85 et 264 V CA pour le courant alternatif et entre 95 et 300 V CC pour le courant continu.
`OutStatus`	**Synopsis :** [---- | Out of range | Good] Spécifie si la tension de sortie de l'alimentation se trouve dans la plage ou non. La plage de tension de sortie est 12 V +/- 1%.
`Calibration`	**Synopsis :** [---- | Bad | Good] Indique si l'alimentation est étalonnée correctement ou non.

4.4 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

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

- Time Zone
- DST Offset
- DST Rule

Remarque
Les MRM ou les MRA faisant fonction de Gestionnaire doivent être déconnectés physiquement ou leur port d'anneau doit être désactivé (c.-à-d. que l'anneau MRP doit être ouvert) avant la restauration des paramètres d'usine, sinon, les configurations par défaut peuvent ne pas être restaurées pour le paramètres suivants :

- Port RSTP Parameters
- Global MRP Parameters
- MRP Instances

Pour plus d'informations les anneaux MRP, voir "Gestion du Media Redundancy Protocol (MRP) (Page 246)".

Pour plus d'informations sur la configuration des paramètres de port, voir "Configuration d'un port Ethernet (Page 73)".

Procédez comme suit pour restaurer les paramètres par défaut :

1. Accédez à ***Diagnostics » Load Factory Defaults***. Le formulaire **Load Factory Defaults** s'affiche.
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`, régler **Defaults Choice** sur `Selected` la met automatiquement 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**.

4.5 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, SSH 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
- Carte microSD/microSDHC

Remarque
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 simultanées 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.

RUGGEDCOM ROS génèrera un trap SNMP et journalisera un message dans le syslog pour indiquer les détails et l'état du transfert lorsque les fichiers sont transférés vers ou depuis un ordinateur distant ou un support externe.

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

- `main.bin` – image de firmware principal d'application RUGGEDCOM ROS
- `fpga2488.bin` – 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
- `ssl.crt` – certificat SSL. Contient le certificat SSL et le fichier de clé privée RSA correspondant.
- `ssh.keys` – clés SSH pour l'appareil

Remarque
Plusieurs versions des fichiers standard peuvent être enregistrées sur la carte microSD/microSDHC. Cependant, si l'un de ces fichiers se trouve dans le répertoire

racine de la carte microSD/microSDHC et a le même nom de fichier qu'un fichier dans la mémoire interne, RUGGEDCOM ROS charge automatiquement le fichier lors du démarrage suivant.

4.5.1 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 "Connexion à ROS (Page 49)".
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 "Utilisation de l'interface de ligne de commande (Page 25)".
3. Dans l'invite de commande de la CLI, saisissez :

   `xmodem [ send | receive ]  { filename }`

   Où :

   - `send` envoie le fichier à l'ordinateur hôte
   - `receive` récupère le fichier de l'ordinateur hôte
   - { *filename* } 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 la 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.

   Remarque
   Lorsque SSH est utilisé pour établir une connexion entre l'appareil RSG2488 et l'ordinateur hôte, XMODEM peut prendre un temps important pour télécharger une image.

   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 "Réinitialisation de l'appareil (Page 114)".

4.5.2 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 :

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

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 "Connexion à ROS (Page 49)".
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 "Utilisation de l'interface de ligne de commande (Page 25)".
4. Dans l'invite de commande de la CLI, saisissez :

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

   Où :

   - `get` copie des fichiers de l'ordinateur hôte vers l'appareil
   - `put` copie des fichiers de l'appareil vers l'ordinateur hôte
   - `{ address }` est l'adresse IP de l'ordinateur exécutant le serveur TFTP
   - `{ source-filename }` est le nom du fichier à transférer
   - `{ destination-filename }` 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 TFTP client réussi :

   ```
   >tftp 10.0.0.1 get ROS-MPC83_Main_v5.6.0.zb 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 "Réinitialisation de l'appareil (Page 114)".

4.5.3 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 :

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

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

1. Établissez une connexion entre l'appareil et l'ordinateur hôte. Pour plus d'informations, voir "Connexion à ROS (Page 49)".
2. Initialisez le serveur TFTP sur l'appareil 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-MPC83_Main_v5.6.0.zb 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 "Réinitialisation de l'appareil (Page 114)".

4.5.4 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-MPC83_Main_v5.6.0.zb main.bin
   Uploading ROS-MPC83_Main_v5.6.zb to /main.bin
   ROS-MPC83_Main_v5.6.0.zb 100% 2139KB 48.6KB/s 00:44
   ```

```
sftp>
```

3. Si le fichier a été chargé, réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

4.5.5 Chargement/téléchargement de fichiers à l'aide de la carte microSD/ microSDHC

La carte microSD/microSDHC amovible peut être utilisée pour transférer des fichiers entre l'appareil, un ordinateur hôte et/ou un autre appareil à des fins diverses. Pour plus d'informations sur la carte microSD/microSDHC amovible et son utilisation, voir "Mémoire amovible (Page 16)".

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

Avant de partager un fichier de configuration chiffré avec un autre appareil, assurez-vous que les deux appareils partagent le même mot de passe/la même phrase secrète pour déchiffrer des fichiers de configuration chiffrés. Pour plus d'informations sur la manière d'activer le chiffrement de données, voir "Configuration du chiffrage des données (Page 126)".

⚠ NOTA

Risque pour la configuration - risque de perte de données.

Après le chargement ou le téléchargement d'un fichier, attendez au moins vingt secondes avant de retirer la carte microSD/microSDHC pour être certain que les données sont complètement transférées.

Remarque
Les fichiers sur la carte microSD/microSDHC et l'appareil peuvent être renommés pendant le transfert. Ceci est utile, par exemple, lorsque plusieurs versions d'un fichier binaire de firmware sont disponibles sur la carte microSD/microSDHC. La version correcte peut être transférée vers l'appareil et renommée en `main.bin` pour remplacer la version se trouvant actuellement sur l'appareil.

Remarque
Le fichier `bootoption.txt` me peut pas être chargé/téléchargé à l'aide de la carte microSD/microSDHC.

Procédez comme suit pour charger un fichier dans l'appareil ou télécharger un fichier de l'appareil :

1. Insérez la carte microSD/microSDHC dans l'appareil. Pour plus d'informations, voir le "manuel d'installation" de l'appareil.
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 "Utilisation de l'interface de ligne de commande (Page 25)".

3. Dans l'invite de commande de la CLI, saisissez :
   - **Chargement**

     `copy a:\{ sourceFile }  { destinationFile }`
   - **Téléchargement**

     `copy  { sourceFile }  a:\{ destinationFile }`
4. Si le fichier a été chargé, réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

4.6 Gestion de journaux

Les fichiers journaux d'incidents (`crashlog.txt`) et système (`syslog.txt`) contiennent des 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.

Remarque
Les fichiers Syslog sauvegardés sur la carte microSD/microSDHC sont horodatés au format année, mois et date (par ex. syslog.txt.20140101). Cela permet de sauvegarder plusieurs fichiers Syslog sur la même carte.

4.6.1 Affichage de journaux locaux et système

Les journaux d'incidents et système locaux peuvent être téléchargés depuis l'appareil et affichés dans un éditeur de texte. Pour plus d'informations sur le téléchargement de fichiers-journaux, voir "Chargement/téléchargement de fichiers (Page 57)".

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

4.6.2 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.
2. Cliquez sur **Confirm**.

4.6.3 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 "Gestion de la journalisation distante (Page 63)".

1. Accédez à ***Administration » Configure Syslog » Configure Local Syslog***. Le formulaire **Local Syslog** s'affiche.
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 le degré de gravité minimum pour le système. Par exemple, si ERROR est sélectionné, le système envoie les messages syslog générés par Error, Critical, Alert et Emergency.

3. Cliquez sur **Apply**.

4.6.4 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 client Syslog se trouve sur l'appareil et prend en charge jusqu'à 5 collecteurs (ou serveurs Syslog).

Le protocole de journal système distant est un transport basé sur UDP/IP qui permet à l'appareil d'envoyer des messages de notification d'événement dans des réseaux IP 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).

4.6.4.1 Format du journal système

RUGGEDCOM ROS prend en charge les formats de journal système RFC 3164 et RFC 5424 utilisés pour transmettre les messages de notification d'événement.

RFC 3164 ayant été remplacé par RFC 5424, cette section se concentre sur le format RFC 5424.

Chaque message syslog distant conforme à RFC 5424 est divisé en trois parties, comme suit :

- En-tête
- Élément structuré
- Message

En-tête

L'en-tête du message comprend les champs suivants :

Figure 4.1 Champs d'en-tête du message

Champ	Description
PRI	La valeur de priorité (PRIVAL) représente à la fois l'infrastructure et la gravité. PRIVAL = (Infrastructure * 8) + Degré de gravité.
VERSION	Version du protocole syslog RFC 5424 (par ex. "1").
SP	Ce champ est utilisé pour représenter un espace ASCII.
TS	Horodatage, au format AAAA-MM-JJTHH-MM-SSuZ. Exemple : "2020-10-06T20:14:47.476406-5:00" représente le 6 octobre 2020 à 20h 14 min 47 s, 476 406 microsecondes dans la seconde suivante. L'horodatage indique que son heure locale est décalée de -5 heures par rapport à UTC.
HN	Nom de l'hôte. Il est défini sur l'adresse IP statique ou dynamique de l'appareil (selon le type d'adresse IP sélectionné par l'utilisateur lors de la configuration de l'interface). Lorsqu'aucune adresse dynamique n'est attribuée à l'appareil, une valeur NIL (c'est-à-dire "-") est utilisée pour désigner le champ.
AN	Nom de l'application. Le type de châssis de l'appareil est utilisé pour ce champ. Par exemple, "RSG2488".
PID	ID de processus.
MID	ID de message.

Élément structuré

Un élément structuré se compose d'un nom et de paires paramètre-valeur au format "["SD-ID SP SD-PARAM)"]". Le nom est appelé SD-ID. Les paires paramètre-valeur sont appelées "SD-PARAM".

Dans RUGGEDCOM ROS, les informations de qualité temporelle sont envoyées à l'aide du SD-ID "timeQuality" et de 2 paires paramètre-valeur :

- **tzKnown** : indique si le créateur connaît ou non son fuseau horaire. Comme RUGGEDCOM ROS tient compte du fuseau horaire, tzKnown est toujours défini sur "1".
- **isSynced** : indique si le créateur est synchronisé ou non avec une source de temps externe fiable. La valeur "1" indique qu'une horloge maître externe a été sélectionnée comme source de temps et que la synchronisation entre le maître et l'esclave a été réalisée. La valeur "0" indique que l'horloge locale a été sélectionnée comme source de temps.

Message

Le message contient un message au format libre qui fournit des informations sur l'événement.

Exemples

Le message suivant indique que la source de temps est configurée sur l'horloge locale :

```
<190>1 2020-10-08T23:48:57.582209-5:00 192.168.2.102 RSG2488 - - [timeQuality
  tzKnown="1" isSynced="0"] RemoteSyslog update collector 192.168.2.101
```

Le message suivant indique que la source de temps est configurée sur l'horloge externe :

```
<190>1 2020-10-08T23:40:31.534206-5:00 192.168.2.102 RSG2488R - - [timeQuality
  tzKnown="1" isSynced="1"] RemoteSyslog update collector 192.168.2.101
```

Pour plus d'informations sur la configuration du format du journal système, voir "Ajout d'un serveur Syslog distant (Page 66)".

4.6.4.2 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.

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

Paramètre	Description
`UDP Port`	**Synopsis :** Un entier compris entre 1025 et 65535 ou [514] **Par défaut :** 514 Port UDP local via lequel le client envoie des informations au(x) serveur(s).

3. Cliquez sur **Apply**.

4.6.4.3 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.

Si aucun serveur Syslog distant n'a été configuré, ajoutez des serveurs en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un serveur Syslog distant (Page 66)".

4.6.4.4 Ajout d'un serveur Syslog distant

RUGGEDCOM ROS prend en charge jusqu'à 5 serveurs (ou collecteurs) 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 sécurité égal ou supérieur au niveau de sécurité spécifié sont écrits dans le journal.

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

1. Accédez à ***Administration » Configure Syslog » Configure Remote Syslog Server***. Le tableau **Remote Syslog Server** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **Remote Syslog Server** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`IP Address`	**Synopsis :** Any valid IP address Adresse IP du serveur Syslog.
`UDP Port`	**Synopsis :** Un entier compris entre 1025 et 65535 ou [514] **Par défaut :** 514 Numéro de port UDP sur lequel le serveur distant écoute.

Paramètre	Description
`Facility`	**Synopsis :** [USER | LOCAL0 | LOCAL1 | LOCAL2 | LOCAL3 | LOCAL4 | LOCAL5 | LOCAL6 | LOCAL7] **Par défaut :** LOCAL7 Composant d'application ou de système d'exploitation qui génère un message de journal. RUGGEDCOM ROS mappe toutes les informations de journalisation syslog sur une seule installation, configurable par l'utilisateur.
`Severity`	**Synopsis :** [EMERGENCY | ALERT | CRITICAL | ERROR | WARNING | NOTICE | INFORMATIONAL | DEBUGGING] **Par défaut :** DEBUGGING Degré de gravité du message généré. Le degré de gravité sélectionné est considéré comme le degré de gravité minimum pour le système. Par exemple, si 'ERROR' est sélectionné, le système envoie tout message syslog ayant le degré de gravité ERROR, CRITICAL, ALERT et EMERGENCY.
`Format`	**Synopsis :** [RFC3164 | RFC5424] **Par défaut :** RFC3164 Format des messages syslog envoyés au serveur syslog distant.

4. Cliquez sur **Apply**.

4.6.4.5 Suppression d'un serveur Syslog distant

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

1. Accédez à ***Administration » Configure Syslog » Configure Remote Syslog Server***. Le tableau **Remote Syslog Server** s'affiche.
2. Sélectionnez le serveur dans le tableau. Le formulaire **Remote Syslog Server** s'affiche.
3. Cliquez sur **Delete**.

4.7 Gestion de ports Ethernet

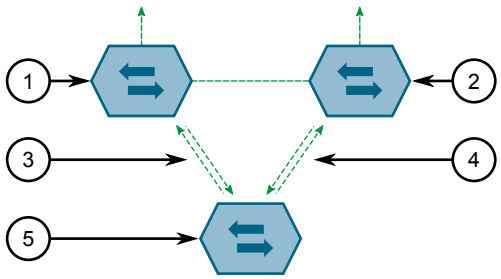
Cette section décrit la manière de gérer des ports Ethernet.

Remarque
Pour plus d'informations sur la configuration de la surveillance à distance de ports Ethernet, voir "Gestion de la surveillance à distance (Page 104)".

4.7.1 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.



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

Figure 4.2 Exemple

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 d'autonégociation intégrée (par exemple une balise spéciale appelée Remote Fault Indication est définie dans le signal d'autonégociation 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 : • **Transmissions de FEFI** 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).

	• **Détection de FEFI** 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 sur 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.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

Si les deux partenaires de liaison sont dotés de la fonctionnalité LFI, elle ne *doit pas* être activée 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 vider 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).

4.7.2 Affichage 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.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`Name`	**Synopsis :** Chaîne de 15 caractères 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.

Paramètre	Description
`Duplex`	**Synopsis :** [---- | Half | Full] État de duplex actuel du port.

4.7.3 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.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`State`	**Synopsis :** [---- | Down | Up] État de connexion du port.
`InOctets`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre d'octets dans des paquets bons (monodiffusion +multidiffusion+diffusion) et abandonnés reçus.
`OutOctets`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre d'octets dans les paquets bons transmis.
`InPkts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de paquets bons (monodiffusion+multidiffusion+diffusion) et abandonnés reçus.
`OutPkts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de paquets bons transmis.
`ErrorPkts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de types quelconques de paquets erronés.

4.7.4 Affichage de statistiques pour des ports Ethernet spécifiques

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

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.

Paramètre	Description
`InOctets`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre d'octets dans des paquets bons (monodiffusion +multidiffusion+diffusion) et abandonnés reçus.
`OutOctets`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre d'octets dans les paquets bons transmis.
`InPkts`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre de paquets bons (monodiffusion+multidiffusion+diffusion) et abandonnés reçus.
`OutPkts`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre de paquets bons transmis.
`TotalInOctets`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 18446744073709551615 Nombre de bons paquets de diffusion reçus.
`InMulticasts`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre de bons paquets multidiffusion reçus.
`CRCAlignErrors`	**Synopsis :** Un entier compris entre 0 et 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 Collision n'a été détecté • Aucun événement Late Collision n'a été détecté
`OversizePkts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de paquets reçus avec une longueur de données supérieure à 1 536 octets et un CRC valide.
`Fragments`	**Synopsis :** Un entier compris entre 0 et 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 Collision n'a été détecté • Aucun événement Late Collision n'a été détecté

Paramètre	Description
	• Le paquet a un CRC invalide
`Jabbers`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 4294967295 Nombre de paquets reçus pour lesquels l'événement Collision a été détecté.
`LateCollisions`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de paquets reçus pour lesquels l'événement Late Collision a été détecté.
`Pkt64Octets`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 4294967295 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 :** Un entier compris entre 0 et 4294967295 Nombre de paquets reçus abandonnés en raison d'un manque de tampons de réception.

Paramètre	Description
`OutMulticasts`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre de paquets multidiffusion transmis. Cela n'inclut pas les paquets de diffusion.
`OutBroadcasts`	**Synopsis :** Un entier compris entre 0 et 18446744073709551615 Nombre de paquets de diffusion transmis.
`UndersizePkts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de paquets reçus répondant à toutes les conditions suivantes : • La longueur de données du paquet est inférieure à 64 octets • Aucun événement Collision n'a été détecté • Aucun événement Late Collision n'a été détecté • Le paquet a un CRC valide

4.7.5 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.
2. Sélectionnez un ou plusieurs ports Ethernet.
3. Cliquez sur **Apply**.

4.7.6 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 "Exigences pour les émetteurs-récepteurs SFP (Page 87)".

1. Accédez à ***Ethernet Ports » Configure Port Parameters***. Le tableau **Port Parameters** s'affiche.
2. Sélectionnez un port Ethernet. Le formulaire **Port Parameters** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Numéro de port.

Paramètre	Description
`Name`	**Synopsis :** Chaîne de 15 caractères **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 de toutes les trames sur ce port. De plus, en cas de désactivation, le signal d'intégrité de liaison n'est pas envoyé et la LED de liaison/d'activité n'est jamais allumée. Vous pouvez désactiver un port pour le dépannage ou la sécurisation contre des connexions non autorisées. **Remarque** La désactivation dont le type de support est défini sur`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 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

Paramètre	Description
	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 :** Off 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 du port est désactivé. le paramètre State doit être mis sur Enabled (Activé) avant que la liaison puisse être restaurée.

Paramètre	Description
`Downshift`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Enabled Activez ou désactivez la négociation automatique sur un port gigabit (1000BASE-T) avec un câble à double paire torsadée. Si cette option est activée, l'appareil est capable de négocier automatiquement avec un autre partenaire de liaison 1000BASE-T à l'aide d'un câble à double paire et d'établir une liaison à 100Mbps ou 10Mbps.

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**.

4.7.7 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.
2. Sélectionnez un port Ethernet. Le formulaire **Port Rate Limiting** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Numéro de port.
`Ingress Limit`	**Synopsis :** Un entier compris entre 64 et 1000000 ou [Disabled] **Par défaut :** 1000 Débit auquel des trames reçues (du type décrit par le paramètre Ingress Frames) sont rejetées par le commutateur.

Paramètre	Description
`Ingress Frames`	**Synopsis :** [Broadcast | Multicast | Mcast&FloodUcast | Bcast&FloodUcast | FloodUcast | Bcast&Mcast | Bcast&Mcast&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`– Seules les trames de diffusion sont limitées • `Multicast`– Seules les trames multicast (multidiffusion) sont limitées • `Bcast&Mcast`– Les trames de diffusion et multidiffusion sont limitées • `Bcast&FloodUcast`– Les trames de diffusion et de monodiffusion en écoulement sont limitées • `Mcast&FloodUcast`– Les trames de multidiffusion et de monodiffusion en écoulement sont limitées • `FloodUcast`– Seules les trames de monodiffusion en écoulement sont limitées
`Egress Limit`	**Synopsis :** Un entier compris entre 64 et 1000000 ou [Disabled] **Par défaut :** Disabled 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**.

4.7.8 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.
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 le Port Guard n'est pas utilisé, il est possible que pratiquement toutes les ressources

disponibles de la CPU 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 changements d'états de liaison continues peuvent être signalées dans un intervalle de temps réduit. Ce grand nombre de faux changements d'état de liaison peut 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 : • `Off`– La désactivation de ce paramètre désactive complètement 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. • `On`– Dans des cas spéciaux dans lesquels des changements d'état de liaison excessifs prolongés 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 continuer d'affecter le temps de réponse du système. Ce réglage doit être utilisé avec prudence. • `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 a désactivé la FAST LINK DETECTION sur un port spécifique, l'utilisateur peut l'activer de nouveau sur le port en effaçant l'alarme.

Paramètre	Description
`Link Detection Time`	**Synopsis :** Un entier compris entre 100 et 1000 **Par défaut :** 100 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 quand il est branché ou débranché.)

3. Cliquez sur **Apply**.

4.7.9 Mise en miroir du trafic

La mise en miroir du trafic est une fonctionnalité de couche 2 qui permet la duplication d'un ou plusieurs flux de trafic à des fins de surveillance et d'analyse du trafic. Le trafic en miroir est transmis à un analyseur/renifleur de paquets externe. Les administrateurs réseau et les ingénieurs analysent le trafic pour détecter les intrusions, dépanner/déboguer les erreurs et surveiller les performances globales du réseau.

RUGGEDCOM ROS prend en charge la surveillance du trafic local et distant (RTM).

4.7.9.1 Comprendre la mise en miroir du trafic à distance (Remote Traffic Mirroring, RTM)

Cette section décrit certains concepts importants de RTM :

Mise en miroir du trafic locale ou à distance

La mise en miroir de ports *locale* nécessite la configuration du ou des ports de mise en miroir source et d'un port de mise en miroir cible sur un seul appareil. Le trafic Ethernet entrant et sortant du ou des ports de mise en miroir source peut être surveillé via le port de mise en miroir cible.

La mise en miroir du trafic *à distance* permet de configurer le(s) port(s) de mise en miroir source et le(s) port(s) de mise en miroir cible sur différents appareils. Sur l'appareil sur lequel un port de mise en miroir source a été configuré, le trafic Ethernet entrant et sortant du port de mise en miroir source peut être mis en miroir sur un VLAN spécifique, appelé VLAN miroir. Le trafic Ethernet en miroir peut transiter par plusieurs commutateurs de couche 2, lorsque le VLAN miroir est configuré sur ces commutateurs.

Sessions de mise en miroir du trafic à distance

Une session de mise en miroir du trafic à distance définit plusieurs sources de trafic (c'est-à-dire des ports de pont) et un VLAN miroir vers lequel le trafic mis en miroir est transmis.

Sources de trafic

Lorsqu'un port pont est la source de trafic, la mise en miroir peut être isolée du trafic circulant dans une direction spécifique (entrée ou sortie) ou de tout le trafic traversant le port.

Appareil source

Commutateur, routeur ou appareil sur lequel les trames de trafic entrantes ou sortantes sont mises en miroir.

Port source

Port spécifique sur l'appareil source sur lequel les trames de trafic sont mises en miroir.

Appareil distant

Pour la mise en miroir du trafic à distance, appareil du réseau auquel le trafic mis en miroir est destiné.

Port distant

Port spécifique sur l'appareil distant sur lequel le trafic mis en miroir sort.

Appareil intermédiaire

Tout appareil d'un réseau Ethernet qui transmet le trafic en miroir. La RTM doit être activée sur tous les appareils intermédiaires.

4.7.9.2 Configuration de la mise en miroir du trafic

La mise en miroir du trafic 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.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

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.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

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

⚠ NOTA

Avant de configurer la mise en miroir du trafic, tenez compte des points suivants :

- Les ports miroir permettent le trafic bidirectionnel, c.-à-d. que l'appareil ne bloque pas le trafic entrant vers le(s) port(s) miroir. Pour une sécurité accrue, configurez le filtrage à l'entrée pour contrôler le flux de trafic lorsque la mise en miroir du trafic est activée. Pour plus d'informations sur l'activation du filtrage à l'entrée, voir "Configuration globale de VLAN (Page 173)".
- Le port cible de la fonction de mise en miroir de ports locale ne peut pas être utilisé pour authentifier les appareils connectés via 802.1x ou gérer un appareil RUGGEDCOM ROS via SSH, Telnet, RSH ou Web UI.
- Le trafic est mis en miroir sur le port cible indépendamment de 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 (comme Telnet, HTTP, SNMP, etc.) ne peuvent pas être mises en miroir.

⚠ NOTA

Avant de configurer Remote Traffic Mirroring (RTM), tenez compte des points suivants :

- Toutes les adresses MAC de monodiffusion configurées de manière statique sur tous les VLAN miroir doivent être supprimées pour garantir la réussite de la mise en miroir du trafic.
- Les adresses IP ne doivent pas être affectées à un VLAN statique configuré en tant que VLAN miroir.
- Le même VLAN miroir doit être configuré de manière statique sur l'appareil source, les appareils intermédiaires et les appareils de destination.
- La mise en miroir du trafic doit être configurée sur un VID cible identique au VLAN miroir statique configuré sur les appareils intermédiaires et de destination.
- Évitez d'utiliser des fonctionnalités de contrôle de réseau dépendantes du VLAN telles que l'espionnage IGMP (IGMP Snooping) ou l'espionnage DHCP (DHCP

Snooping) sur le VLAN de mise en miroir, car elles peuvent ne pas fonctionner comme prévu.

- Sur un appareil source, si un port trunk VLAN est utilisé pour envoyer le trafic en miroir vers le côté distant, mais est également configuré en tant que port source de sortie, la mise en miroir du trafic à distance ne fonctionne pas. Aucun trafic en miroir n'est envoyé aux commutateurs voisins via ce port.
- Une tempête de trafic en miroir peut se produire dans un réseau lorsque RTM est activé sur plusieurs appareils sources utilisant le même VID cible ou des VID cibles différents, et que les ports Trunk connectant ces appareils source RTM sont configurés en tant que ports source d'entrée sur deux appareils source ou plus. Pour éviter une telle tempête, ne configurez pas les ports Trunk en tant que ports source d'entrée sur plusieurs appareils source.
- Un port ne doit pas être configuré en tant que port source pour le RTM d'entrée si le port peut être mis en état de rejet par un protocole de contrôle réseau tel que RSTP, MRP ou LACP. Si un port est déjà configuré pour un tel protocole de contrôle réseau, assurez-vous de choisir un port différent comme port de mise en miroir d'entrée source. L'utilisation du même port peut entraîner une tempête de trafic.
- RTM n'est pas pris en charge en mode non compatible VLAN. Si RTM est activé en mode compatible VLAN, le paramètre **Port Mirroring** est automatiquement défini sur **Disabled** et **Target VID** est défini sur **None** dans le formulaire **Traffic Mirroring** lors du passage du mode VLAN global de compatible VLAN à non compatible VLAN.
- Les VID de quarantaine et d'invité ne peuvent pas agir également en tant que VLAN 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 du trafic :

1. Accédez à ***Ethernet Ports » Configure Traffic Mirroring***. Le formulaire **Traffic Mirroring** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port Mirroring`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Si la mise en miroir de ports est activée, toutes les trames reçues et/ou transmises par le(s) port(s) source sont envoyées hors du port cible, ou sont à nouveau balisées sur le VID cible puis à nouveau commutées sur le VID cible (si cela est pris en charge par l'appareil).

Paramètre	Description
`Source Ports Egr`	**Synopsis :** Comma-separated list of ports **Par défaut :** None Le trafic sortant de ces ports est surveillé.
`Source Ports Ingr`	**Synopsis :** Comma-separated list of ports **Par défaut :** None Le trafic entrant dans ces ports est surveillé.
`Target Port`	**Synopsis :** 1/1 to maximum port number or { None } **Par défaut :** None Le trafic surveillé est envoyé hors de ce port, où un appareil de surveillance doit être connecté. Lorsque le VID cible est configuré (c'est-à-dire lorsque la mise en miroir du trafic à distance (Remote Traffic Mirroring) est activée), la signification de ce paramètre change. La mise en miroir du trafic à distance nécessite l'utilisation d'un port d'appareil pour baliser à nouveau les trames mises en miroir. Lorsqu'elle est configurée, aucun trafic n'entre ou ne sort de l'interface physique. Ce paramètre identifie le port utilisé à cette fin.
`Target VID`	**Synopsis :** 1 to 4094 or { None } **Par défaut :** None ID VLAN vers lequel le trafic surveillé doit être transféré.

3. Cliquez sur **Apply**.

4.7.9.3 Exemple : configuration de Remote Traffic Mirroring

Cet exemple montre comment configurer le Remote Traffic Mirroring (RTM) à l'aide d'un appareil source RTM, d'un ou plusieurs appareils intermédiaires et d'un appareil de destination.

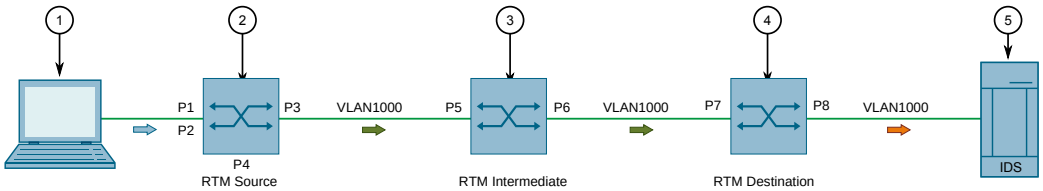
Dans la topologie, le trafic est envoyé d'une source de trafic vers un appareil source compatible RTM. Ce trafic est représenté par une flèche bleue.

Le trafic est ensuite balisé avec un ID de VLAN miroir et envoyé à un appareil de destination via un appareil intermédiaire (flèches vertes). Dans la topologie, un appareil intermédiaire est représenté, mais plusieurs appareils intermédiaires sont possibles.

Enfin, le trafic est capturé en tant que trafic en miroir (flèche orange) sur le système de détection d'intrusion (Intrusion Detection System, IDS) connecté à l'appareil de destination.

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① Source du trafic
② Appareil source RTM
③ Appareil intermédiaire RTM
④ Appareil de destination RTM
⑤ Système de détection d'intrusion (IDS)

Figure 4.3 Topologie RTM

Procédez comme suit pour répliquer la topologie :

Remarque
un VLAN miroir ne doit être utilisé que pour la mise en miroir. Il est recommandé d'éviter de configurer le VLAN 1 en tant que VLAN miroir, car il s'agit du VLAN par défaut.

Remarque
Tous les appareils participant à une session RTM doivent être compatibles RTM.

1. Configurez un VLAN statique en tant que **Mirror VLAN** sur les appareils source, intermédiaires et de destination RTM participant à la session RTM.

   Pour plus d'informations sur la configuration des VLAN statiques, voir "Ajout d'un VLAN statique (Page 176)".

   Dans la topologie, VID 1000 est configuré en tant que VLAN miroir sur les appareils source, intermédiaire et de destination.

2. Sur l'appareil source RTM, configurez les éléments suivants :

   a. Configurez **Port Mirroring** sur **Enabled**.

      Pour plus d'informations, voir "Configuration de la mise en miroir du trafic (Page 80)".

   b. Configurez **Source Ports Ingr** et **Source Ports Egr** selon les besoins.

      Dans la topologie, **Source Ports Ingr** est configuré en tant que port 1 et **Source Ports Egr** est configuré en tant que port 2.

      Remarque
      La mise en miroir du trafic à distance nécessite l'utilisation d'un port d'appareil pour baliser à nouveau les trames mises en miroir. Lorsqu'elle

est configurée, aucun trafic n'entre ou ne sort de l'interface physique. Le paramètre **Target Port** identifie le port utilisé à cette fin.

c. Configurez le **Target Port** comme l'un des ports de commutateur inutilisés.

Remarque
Lorsque RTM est désactivé, la configuration précédente du port désigné comme port cible est restaurée.

Dans la topologie, **Target Port** est configuré en tant que port 4.

d. Configurez **Target VID**. La valeur doit correspondre au VID configuré en tant que VLAN miroir sur l'appareil source, l'appareil/les appareils intermédiaire(s) et l'appareil de destination dans Étape 1.

Dans la topologie, **Target VID** est configuré sur 1000.

3. Configurez le VLAN **Type** pour les ports connectant l'appareil source aux appareils intermédiaires en tant que **Trunk** ou **Edge** sur le VLAN miroir selon les besoins.

Pour plus d'informations sur la configuration du trunk et des ports de périphérie, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".

Dans la topologie, le port 3 de l'appareil source est connecté au port 5 de l'appareil intermédiaire.

4. Configurez le VLAN **Type** pour les ports connectant les appareils intermédiaires à l'appareil de destination en tant que **Trunk** ou **Edge** sur le VLAN miroir selon les besoins.

Pour plus d'informations sur la configuration du trunk et des ports de périphérie, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".

Dans la topologie, le port 6 de l'appareil intermédiaire est connecté au port 7 de l'appareil de destination.

Remarque
Si un port connecté à l'IDS est configuré en tant que port VLAN **Edge**, le PVID du port doit être configuré avec l'ID VLAN miroir de la session pour recevoir le trafic mis en miroir. Dans ce cas, le format PVID du port contrôle si le trafic mis en miroir est balisé ou non balisé.

Remarque
Si un port connecté à l'IDS est configuré en tant que port VLAN **Trunk**, le trafic normal et le trafic mis en miroir sont reçus. Si le PVID du port est configuré avec l'ID de VLAN miroir de la session, le format PVID du port contrôle si le trafic mis en miroir est balisé ou non balisé. Sinon, le trafic mis en miroir est toujours balisé avec l'ID de VLAN miroir.

5. Configurez les paramètres Port VLAN pour les ports connectant l'appareil de destination à l'IDS soit comme **Edge** (avec le VID miroir de la session) soit comme **Trunk**.

   Pour plus d'informations sur la configuration du trunk et des ports de périphérie, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".

   Dans la topologie, le port 8 de l'appareil de destination est connecté à l'IDS.

4.7.10 Gestion d'émetteurs-récepteurs SFP

RUGGEDCOM ROS prend en charge les émetteurs-récepteurs Small Form Factor Pluggable (SFP).

La surveillance de diagnostic numérique (Digital Diagnostic Monitoring, DDM) est prise en charge sur les appareils équipés de ports SFP. La DDM est désactivée par défaut et peut être activée en configurant l'intervalle d'interrogation. Lorsqu'elle est activée, les émetteurs-récepteurs SFP installés sont surveillés en termes de température, tension, courant de polarisation Tx, puissance Rx et puissance Tx. Une alarme est générée lorsqu'un paramètre mesuré spécifique dépasse son seuil.

Pour plus d'informations sur les alarmes, voir "Gestion des alarmes (Page 118)".

Remarque
Les émetteurs-récepteurs 1000Base-X SFP en fibres étant normalisés, RUGGEDCOM ROS prend en charge la plupart des modèles de ce type. Pour plus d'informations, voir le Catalogue des émetteurs-récepteurs SFP RUGGEDCOM [https://support.industry.siemens.com/cs/ww/en/view/109482309].

Il est vivement recommandé d'utiliser uniquement des modèles d'émetteurs-récepteurs SFP approuvés par Siemens. Siemens soumet les émetteurs-récepteurs à des essais approfondis pour s'assurer qu'ils peuvent supporter 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 d'autonégociation 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 l'autonégociation réglée sur *On*.

Remarque
Du fait d'une latence éventuelle introduite par la couche physique intégrée, la précision temporelle d'IEEE 1588 peut être significativement dégradée sur un port SFP en cuivre.

4.7.10.1 Exigences pour les émetteurs-récepteurs SFP

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

- Pour les liaisons 100Base-FX ou 100Base-TX, la vitesse doit être définie sur 100 Mbit/s.
- Pour les liaisons 1000Base-X ou 1000Base-T, la vitesse du port SFP doit être définie sur 1 Gbit/s.
- L'autonégociation 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 "Configuration d'un port Ethernet (Page 73)".

4.7.10.2 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 l'autonégociation sur *Off*	Accepter
100 Mbit/s	Acceptez et définissez automatiquement la	Accepter	Comparez le modèle d'émetteur-récepteur

Vitesse configurée	Type SFP détecté : 1000Base-X	Type SFP détecté : 100Base-FX	Type SFP détecté : 1000Base-T
	vitesse sur 1 Gbit/s et définissez l'autonégociation sur *On*		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 l'autonégociation 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
```

4.7.10.3 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 "Utilisation de l'interface de ligne de commande (Page 25)".
2. Saisissez la commande suivante :

   `sfp { port }`

   Où :

   - `{ port }` est le numéro de port

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

```
>sfp
           1/1

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
>
```

4.7.10.4 Définition de l'intervalle d'interrogation SFP

Pour définir l'intervalle d'interrogation SFP, accédez à ***Ethernet Ports » Configure SFP DDM Options***. Le tableau **SFP DDM Options** s'affiche.

Remarque
Pour plus d'informations sur l'affichage de l'état de SFP actifs, voir "Affichage de diagnostics de SFP (Page 89)".

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Polling Interval`	**Synopsis :** Un entier compris entre 1 et 30 ou [Disabled] **Par défaut :** Disabled Ce paramètre configure l'intervalle de temps d'attente du système entre deux lectures consécutives d'émetteurs-récepteurs SFP/SFP+.

4.7.10.5 Affichage de diagnostics de SFP

Pour afficher l'état d'un SFP, accédez à ***Ethernet Ports » View SFP Diagnostics***. Le tableau **SFP Diagnostics** s'affiche.

Remarque
Pour plus d'informations sur la définition d'un intervalle d'interrogation, voir "Définition de l'intervalle d'interrogation SFP (Page 89)".

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.

Paramètre	Description
`DDM Status`	**Synopsis :** [N/A | OK | Warning | Alarm] État DDM du SFP.
`Temperature`	**Synopsis :** Un entier compris entre -128.000 et 128.000 **Par défaut :** 0.000 Température actuelle de l'émetteur-récepteur SFP, en degrés Celsius.
`Temp Alarm Low`	**Synopsis :** Un entier compris entre -128.000 et 128.000 **Par défaut :** 0.000 Seuil d'alarme de température basse de l'émetteur-récepteur SFP, en degrés Celsius.
`Temp Warn Low`	**Synopsis :** Un entier compris entre -128.000 et 128.000 **Par défaut :** 0.000 Seuil d'avertissement de température basse de l'émetteur-récepteur SFP, en degrés Celsius.
`Temp Warn High`	**Synopsis :** Un entier compris entre -128.000 et 128.000 **Par défaut :** 0.000 Seuil d'avertissement de température élevée de l'émetteur-récepteur SFP, en degrés Celsius.
`Temp Alarm High`	**Synopsis :** Un entier compris entre -128.000 et 128.000 **Par défaut :** 0.000 Seuil d'alarme de température élevée de l'émetteur-récepteur SFP, en degrés Celsius.
`Voltage`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Tension d'alimentation actuelle de l'émetteur-récepteur SFP, en volts.
`Volt Alarm Low`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'alarme de tension faible de l'émetteur-récepteur SFP, en volts.
`Volt Warn Low`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'avertissement de tension faible de l'émetteur-récepteur SFP, en volts.
`Volt Warn High`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'avertissement de tension élevée de l'émetteur-récepteur SFP, en volts.

Paramètre	Description
`Volt Alarm High`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'alarme de tension élevée de l'émetteur-récepteur SFP, en volts.
`Tx Bias`	**Synopsis :** Un entier compris entre 0.000 et 131.070 **Par défaut :** 0.000 Courant de polarisation Tx actuel de l'émetteur-récepteur SFP, en milliampères.
`TxBias Alarm Low`	**Synopsis :** Un entier compris entre 0.000 et 131.070 **Par défaut :** 0.000 Seuil d'alarme de courant de polarisation Tx faible de l'émetteur-récepteur SFP, en milliampères.
`TxBias Warn Low`	**Synopsis :** Un entier compris entre 0.000 et 131.070 **Par défaut :** 0.000 Seuil d'avertissement de courant de polarisation Tx faible de l'émetteur-récepteur SFP, en milliampères.
`TxBias Warn High`	**Synopsis :** Un entier compris entre 0.000 et 131.070 **Par défaut :** 0.000 Seuil d'avertissement de courant de polarisation Tx élevé de l'émetteur-récepteur SFP, en milliampères.
`TxBias Alarm High`	**Synopsis :** Un entier compris entre 0.000 et 131.070 **Par défaut :** 0.000 Seuil d'alarme de courant de polarisation Tx élevé de l'émetteur-récepteur SFP, en milliampères.
`Rx Power`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Puissance d'entrée Rx de l'émetteur-récepteur SFP, en microwatts.
`RxPower Alarm Low`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'alarme de puissance Rx faible de l'émetteur-récepteur SFP, en microwatts.
`RxPower Warn Low`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'avertissement de puissance Rx faible de l'émetteur-récepteur SFP, en microwatts.
`RxPower Warn High`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'avertissement de puissance Rx élevée de l'émetteur-récepteur SFP, en microwatts.

Paramètre	Description
`RxPower Alarm High`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'alarme de puissance Rx élevée de l'émetteur-récepteur SFP, en microwatts.
`Tx Power`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Puissance de sortie Tx actuelle de l'émetteur-récepteur SFP, en milliwatts.
`TxPower Alarm Low`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'alarme de puissance Tx faible de l'émetteur-récepteur SFP, en milliwatts.
`TxPower Warn Low`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'avertissement de puissance Tx faible de l'émetteur-récepteur SFP, en milliwatts.
`TxPower Warn High`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'avertissement de puissance Tx élevée de l'émetteur-récepteur SFP, en milliwatts.
`TxPower Alarm High`	**Synopsis :** Un entier compris entre 0.000 et 65.535 **Par défaut :** 0.000 Seuil d'alarme de puissance Tx élevée de l'émetteur-récepteur SFP, en milliwatts.
`Alarm Flags`	**Synopsis :** Un entier compris entre 0 et 4294967295 **Par défaut :** 00000000 Bits d'indicateur d'alarme actuels de l'émetteur-récepteur SFP.
`Warning Flags`	**Synopsis :** Un entier compris entre 0 et 4294967295 **Par défaut :** 00000000 Bits d'indicateur d'avertissement actuels de l'émetteur-récepteur SFP.

4.7.11 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.

4.7.11.1 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 "Exécution de diagnostics de câble (Page 94)".

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`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 S/O.
`Runs`	**Synopsis :** Un entier compris entre 0 et 65535 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 :** Un entier compris entre -100.0 et 100.0 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 : 1. Choisissez un port spécifique pour lequel un étalonnage est nécessaire. 2. Connectez un câble Ethernet avec une longueur connue (par ex. 50 m) au port. 3. NE connectez PAS l'autre extrémité du câble à un partenaire de liaison quelconque. 4. Exécutez quelques fois les diagnostics de câble sur le port. Un défaut d'ouverture doit être détecté. 5. Déterminez la distance moyenne avec 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. 6. Saisissez la valeur d'étalonnage et exécutez à nouveau quelques fois les diagnostics de câble. 7. La distance avec le défaut d'ouverture doit maintenant être similaire à la longueur du câble. 8. La distance avec le défaut pour le port sélectionné est maintenant étalonnée.
`Good`	**Synopsis :** Un entier compris entre 0 et 65535 Nombre de détections d'arrêts bons (GOOD, sans erreur) sur les paires de câbles du port sélectionné.

Paramètre	Description
`Open`	**Synopsis :** Un entier compris entre 0 et 65535 Nombre de détections d'ouvertures (OPEN) sur les paires de câbles du port sélectionné.
`Short`	**Synopsis :** Un entier compris entre 0 et 65535 Nombre de détections de courts-circuits (SHORT) sur les paires de câbles du port sélectionné.
`Imped`	**Synopsis :** Un entier compris entre 0 et 65535 Nombre de détections de discordances d'impédance (IMPEDANCE MISMATCH) sur les paires de câbles du port sélectionné.
`Pass /Fail /Total`	**Synopsis :** Chaîne de 19 caractères Ce champ résume les résultats des diagnostics de câble exécutés jusqu'ici. • `Pass (OK)` – 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 diagnostic 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 100Base-T, qui comprend deux paires de câbles, le nombre est incrémenté de deux. Pour un port 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 câbles, la défaillance détectée et la valeur de la distance au défaut. Pour plus d'informations sur le journal système, voir "Affichage de journaux locaux et système (Page 62)".

4.7.11.2 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.

⚠ NOTA
Le port Ethernet sélectionné et son port partenaire peuvent être configurés de manière à s'exécuter en mode *Enabled* avec autonégociation 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.
4. Sélectionnez un port Ethernet. Le formulaire **Cable Diagnostics Parameters** s'affiche.
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 "Détermination de la distance estimée au défaut (Estimated Distance To Fault (DTF) (Page 95)".
7. Sélectionnez **Started**.

⚠ NOTA

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** une fois le test terminé. Pour plus d'informations sur la manière de surveiller le test et d'afficher les résultats, voir "Affichage des résultats de diagnostics de câbles (Page 93)".

4.7.11.3 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.
2. Sélectionnez un ou plusieurs ports Ethernet.
3. Cliquez sur **Apply**.

4.7.11.4 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 à l'appareil. 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 "Exécution de diagnostics de câble (Page 94)". 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 "Affichage de journaux locaux et système (Page 62)".
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.

4.7.12 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.
2. Sélectionnez un ou plusieurs ports Ethernet à réinitialiser.
3. Cliquez sur **Apply**. Les ports Ethernet sélectionnés sont réinitialisés.

4.8 Gestion d'interfaces IP

Deux types d'interface IP peuvent être configurés dans RUGGEDCOM ROS:

- Interfaces IP de gestion
- Interfaces de commutateur IP

L'interface IP de gestion représente le port de gestion sur l'appareil. Une seule interface IP de gestion peut être configurée.

Les interfaces IP de commutateur représentent les interfaces VLAN où une adresse IP doit être affectée à chaque interface avec un sous-réseau unique. Une interface VLAN doit être marquée comme interface de gestion .Par défaut, l'interface de gestion est la seule interface capable d'utiliser des services IP tels que DHCP, IEEE1588, Serial Server et LLDP qui affectent l'appareil RUGGEDCOM ROS. Cependant, RUGGEDCOM

ROS peut être configuré pour permettre à des interfaces de gestion auxiliaires d'utiliser les services suivants :

- MMS
- Modbus
- Radius/TacPlus
- Shell distant
- Syslog distant
- SNMP
- SNTP
- SSH
- TFTP
- Telnet
- Serveur Web

Pour plus d'informations, voir "Configuration des services IP (Page 102)".

4.8.1 Configuration de l'interface IP de gestion

Procédez comme suit pour configurer l'interface IP de gestion :

1. Accédez à ***Administration » Configure IP Interfaces » Configure Mgmt IP Interfaces***. Le formulaire **Mgmt IP Interfaces** s'affiche.
2. 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 par défaut comme ID de VLAN. Les modifications de l'adresse IP sont effectives immédiatement. Toutes les connexions IP mises en œuvre au moment de la modification d'une adresse IP sont perdues.

Paramètre	Description
`IP Address Type`	**Synopsis :** [Static | Dynamic | DHCP | BOOTP] **Par défaut :** Static Spécifie si l'adresse IP est statique ou affectée de dynamiquement via DHCP ou BOOTP. L'option DYNAMIC est un exemple commun d'adresse IP affectée dynamiquement. Elle commute entre BOOTP et DHCP jusqu'à recevoir la réponse du serveur approprié. Elle doit être statique pour les interfaces qui ne sont pas des interfaces de gestion.

Paramètre	Description
`IP Address`	**Synopsis :** Any valid IP address **Par défaut :** 192.168.0.1 Spécifie l'adresse Internet Protocol de cette interface. Une adresse IP est un nombre 128 bits noté en utilisant huit champs de quatre nombres hexadécimaux pour lesquels les zéros de début peuvent être omis, délimités par des doubles points. Consultez la documentation hors-ligne pour plus d'informations. Une adresse de version 4 peut être encodée avec quatre nombres décimaux de 0 à 255, séparés par des points. Seule une adresse IP de monodiffusion ne commençant pas par "FF" ou se trouvant dans une plage de 1.0.0.0 à 233.255.255.255 est autorisée pour la version 4.
`Subnet`	**Synopsis :** Un entier compris entre 0 et 128 **Par défaut :** 24 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. **⚠ NOTA** Chaque interface IP doit avoir une adresse réseau unique.

3. Cliquez sur **Apply**.

4.8.2 Gestion d'interfaces IP de commutateur

Les interfaces IP de commutateur représentent les interfaces VLAN où une adresse IP doit être affectée à chaque interface avec un sous-réseau unique. Les sous-paragraphes suivants décrivent la façon de visualiser une liste d'interfaces IP de commutateur, ainsi que la manière de les ajouter/supprimer.

4.8.2.1 Affichage d'une liste d'interfaces IP de commutateur

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

Si aucune interface IP de commutateur n'a été configurée, ajoutez des interfaces IP en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".

4.8.2.2 Ajout d'une interface IP de commutateur

Procédez comme suit pour ajouter une interface IP de commutateur :

1. Accédez à ***Administration » Configure IP Interfaces » Configure Switch IP Interfaces***. Le tableau **Switch IP Interfaces Table** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **Switch IP Interfaces** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

Les interfaces IP appartenant à un VLAN de gestion ou de gestion auxiliaire doivent être connectées à un réseau de confiance.

⚠ NOTA

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.

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 par défaut comme ID de VLAN. Les modifications de l'adresse IP sont effectives immédiatement. Toutes les connexions IP mises en œuvre au moment de la modification d'une adresse IP sont perdues.

Remarque
Pour IPv4, si une notation décimale avec séparation par point est configurée pour le préfixe de sous-réseau (p. ex. 255.255.255.0), elle sera automatiquement convertie au nombre équivalent de bits (p. ex. 24 bits).

Paramètre	Description
`Type`	**Synopsis :** [VLAN] **Par défaut :** VLAN Spécifie le type d'interface pour lequel cette interface IP est créée.
`ID`	**Synopsis :** Un entier compris entre 1 et 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 | Aux] **Par défaut :** No Spécifie si l'interface IP peut prendre en charge des fonctions de gestion. • `Aux`– Prend en charge des fonctions de gestion

Paramètre	Description
	• `Oui`– Prend en charge des fonctions de gestion et l'affectation dynamique des adresses comme DHCP • `Non`– Ne prend pas en charge les fonctions de gestion ni l'affectation dynamique des adresses
`IP Address Type`	**Synopsis :** [Static | Dynamic | DHCP | BOOTP] **Par défaut :** Static Spécifie si l'adresse IP est statique ou affectée de dynamiquement via DHCP ou BOOTP. L'option DYNAMIC est un exemple commun d'adresse IP affectée dynamiquement. Elle commute entre BOOTP et DHCP jusqu'à recevoir la réponse du serveur approprié. Elle doit être statique pour les interfaces qui ne sont pas des interfaces de gestion.
`IP Address`	**Synopsis :** Any valid IP address **Par défaut :** 192.168.0.1 Spécifie l'adresse Internet Protocol de cette interface. Une adresse IP est un nombre 128 bits noté en utilisant huit champs de quatre nombres hexadécimaux pour lesquels les zéros de début peuvent être omis, délimités par des doubles points. Consultez la documentation hors-ligne pour plus d'informations. Une adresse de version 4 peut être encodée avec quatre nombres décimaux de 0 à 255, séparés par des points. Seule une adresse IP de monodiffusion ne commençant pas par "FF" ou se trouvant dans une plage de 1.0.0.0 à 233.255.255.255 est autorisée pour la version 4.
`Subnet Prefix`	**Synopsis :** Un entier compris entre 0 et 128 **Par défaut :** 24 Spécifie le nombre de bits d'ordre le plus élevé contigus qui comprennent le masque de sous-réseau de l'interface courante. Par exemple, 24 serait équivalent à un masque de sous-réseau IPv4 255.255.255.0, tandis que 64 spécifierait un masque de sous-réseau constitué des 64 bits d'ordre le plus élevé (valable pour IPv6). **⚠ NOTA** Chaque interface IP doit avoir une adresse réseau unique.

4. Cliquez sur **Apply**.

4.8.2.3 Suppression d'une interface IP de commutateur

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

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

2. Sélectionnez l'interface IP dans le tableau. Le formulaire **Switch IP Interfaces** s'affiche.
3. Cliquez sur **Delete**.

4.9 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 passerelle par défaut n'est pas modifiée si la configuration d'usine par défaut sélectionnée est rechargée.

4.9.1 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.

Si aucune passerelle IP n'a été configurée, ajoutez des passerelles IP en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'une passerelle IP (Page 101)".

4.9.2 Ajout d'une passerelle IP

Remarque
Les adresses de passerelle IP 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.
2. Cliquez sur **InsertRecord**. Le formulaire **IP Gateways** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Destination`	**Synopsis :** Any valid IP address 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 :** Un entier compris entre 0 et 128 **Par défaut :** 0 Spécifie le masque de sous-réseau IP de destination. Pour la passerelle par défaut, la destination et le sous-réseau sont 0.

Paramètre	Description
`Gateway`	**Synopsis :** Any valid IP address Spécifie la passerelle à utiliser pour atteindre la destination.

4. Cliquez sur **Apply**.

4.9.3 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.
2. Sélectionnez la passerelle IP dans le tableau. Le formulaire **IP Gateways** s'affiche.
3. Cliquez sur **Delete**.

4.10 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.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Inactivity Timeout`	**Synopsis :** Un entier compris entre 1 et 60 ou [Disabled] **Par défaut :** 5 Spécifie l'expiration de la console et affiche l'écran de connexion si l'utilisateur n'est pas actif. La valeur zéro désactive les délais d'expiration. La valeur de délai d'expiration maximum pour les utilisateurs de serveur Web est limitée à 30 minutes.
`Telnet Sessions Allowed`	**Synopsis :** Un entier compris entre 1 et 4 ou [Disabled] **Par défaut :** Disabled Limite le nombre de sessions Telnet. La valeur zéro empêche tout accès Telnet.
`Web Server Users Allowed`	**Synopsis :** Un entier compris entre 1 et 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 Comme il s'agit d'un protocole non sécurisé, ce paramètre permet à l'utilisateur de limiter ou de désactiver le service. `Disabled`– désactive l'accès en lecture et écriture pour tout ce service

Paramètre	Description
	`Get Only`– autorise uniquement la lecture des fichiers pour tout ce service `Enabled`– autorise la lecture et l'écriture de fichiers pour tout ce service
`ModBus Address`	**Synopsis :** Un entier compris entre 1 et 255 ou [Disabled] **Par défaut :** Disabled Détermine l'adresse Modbus à utiliser pour la gestion via Modbus.
`SSH Sessions Allowed (Controlled Version Only)`	**Synopsis :** Un entier compris entre 1 et 4 **Par défaut :** 4 Limite le nombre de sessions SSH.
`MMS Sessions Allowed`	**Synopsis :** Un entier compris entre 1 et 4 **Par défaut :** Disabled Limite le nombre de sessions MMS. "Disabled" empêche tout accès MMS.
`RSH Server`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Active/désactive l'accès Shell distant.
`IP Forward`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Contrôle la capacité de transfert IP entre des VLAN dans un serveur série ou des segments IP. **Remarque** Lorsque la commutation de couche 3 (Layer 3 Switching) est activée et**que le mode Monodiffusion**est défini sur "Auto", le transfert IP (IP forwarding) doit être activé.
`Max Failed Attempts`	**Synopsis :** Un entier compris entre 1 et 20 **Par défaut :** 10 Nombre maximum d'échecs de tentatives d'accès par service au sein de la Failed Attempts Window avant le blocage du service. Le nombre maximal de tentatives d'accès est autorisé pour chaque service, avant blocage. Ce paramètre est réinitialisé à la valeur par défaut lorsque la configuration d'usine par défaut est rechargée. Cependant, le compteur d'échecs de tentatives d'accès sur un service particulier n'est pas remis à zéro.
`Failed Attempts Window`	**Synopsis :** Un entier compris entre 1 et 30 **Par défaut :** 5 Temps en minutes (min) pendant lequel le nombre maximum d'échecs de tentatives de connexion doit être dépassé avant le blocage d'un service. Le compteur d'échecs de tentatives est remis à 0 lorsque la temporisation expire. Ce paramètre est réinitialisé à la valeur par défaut lorsque la configuration d'usine par défaut est rechargée.

Paramètre	Description
`Lockout Time`	**Synopsis :** Un entier compris entre 1 et 120 **Par défaut :** 60 Temps en minutes (min) pendant lequel le service reste bloqué lorsque le nombre maximum d'échecs de tentatives d'accès a été atteint. À l'exception de l'interface de gestion de l'appareil, ce paramètre est réinitialisé à la valeur par défaut lorsque la configuration d'usine par défaut est rechargée.

3. Cliquez sur **Apply**.

4.11 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.

4.11.1 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.

4.11.1.1 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.

Si aucun contrôle d'historique n'a été configuré, ajoutez des contrôles en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un contrôle d'historique RMON (Page 104)".

4.11.1.2 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.
2. Cliquez sur **InsertRecord**. Le formulaire **RMON History Controls** s'affiche.

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

Paramètre	Description
`Index`	**Synopsis :** Un entier compris entre 1 et 65535 **Par défaut :** 1 Index de cet enregistrement RMON History Contol.
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Numéro de port.
`Requested Buckets`	**Synopsis :** Un entier compris entre 1 et 5000 **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 :** Un entier compris entre 0 et 65535 Nombre de compartiments accordés pour cet historique de collecte RMON. Le champ ne peut pas être édité.
`Interval`	**Synopsis :** Un entier compris entre 1 et 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 :** Chaîne de 127 caractères **Par défaut :** Monitor Propriétaire de cet enregistrement. Nous recommandons de démarrer cette chaîne avec le mot 'monitor'.

4. Cliquez sur **Apply**.

4.11.1.3 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.
2. Sélectionnez le contrôle d'historique dans le tableau. Le formulaire **RMON History Controls** s'affiche.
3. Cliquez sur **Delete**.

4.11.2 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 "Affichage et effacement d'alarmes verrouillées (Page 119)".

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.

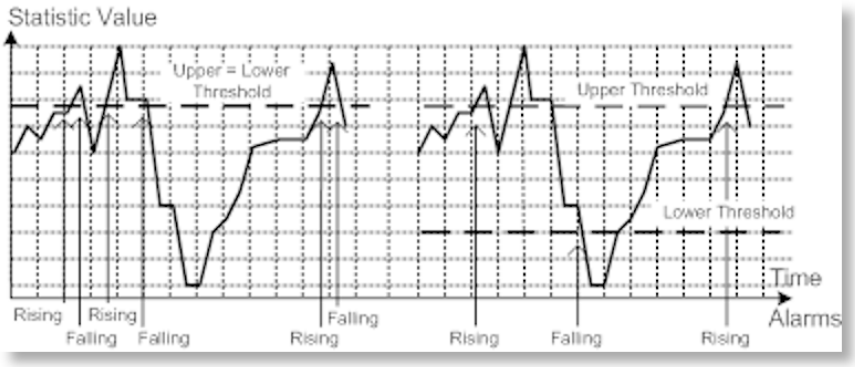


Figure 4.4 Le processus d'alarme

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 lorsque le nombre total ou absolu d'événements dépasse un seuil. Dans ce cas, définissez le type d'intervalle de mesure sur *absolu*.

4.11.2.1 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.

Si aucune alarme n'a été configurée, ajoutez des alarmes en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'une alarme RMON (Page 107)".

4.11.2.2 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.
2. Cliquez sur **InsertRecord**. Le formulaire **RMON Alarms** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Index`	**Synopsis :** Un entier compris entre 1 et 65535 **Par défaut :** 1 Index de cet enregistrement RMON Alarm.
`Variable`	**Synopsis :** Un entier 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'. Format OID : objectName.index1.index2... où le format d'index dépend du type d'objet d'index.
`Rising Thr`	**Synopsis :** Un entier compris entre -2147483647 et 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

Paramètre	Description
	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 :** Un entier compris entre -2147483647 et 2147483647 **Par défaut :** 0 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 avant que la valeur échantillonnée passe au-dessus de ce seuil et atteigne la valeur de RisingThreshold.
`Value`	**Synopsis :** Un entier compris entre -2147483647 et 2147483647 Valeur de l'objet de surveillance pendant la dernière période d'échantillonnage. La présentation de la valeur dépend du type d'échantillon ('absolute' ou '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 :** Un entier compris entre 0 et 2147483647 **Par défaut :** 60 Nombre de secondes pendant lesquelles les données sont échantillonnées et comparées 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 :** Un entier compris entre 0 et 65535 **Par défaut :** 0 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 associé n'est généré en particulier si la valeur est zéro.

Paramètre	Description
`Falling Event`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 0 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 associé n'est généré en particulier si la valeur est zéro.
`Owner`	**Synopsis :** Chaîne de 127 caractères **Par défaut :** Monitor Propriétaire de cet enregistrement. Nous recommandons de démarrer cette chaîne avec le mot 'monitor'.

4. Cliquez sur **Apply**.

4.11.2.3 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.
2. Sélectionnez l'alarme dans le tableau. Le formulaire **RMON Alarms** s'affiche.
3. Cliquez sur **Delete**.

4.11.3 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 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.

4.11.3.1 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.

Si aucun événement n'a été configuré, ajoutez des événements en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un événement RMON (Page 110)".

4.11.3.2 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.
2. Cliquez sur **InsertRecord**. Le formulaire **RMON Events** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Index`	**Synopsis :** Un entier compris entre 1 et 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 :** Chaîne de 31 caractères **Par défaut :** public Si le trap SNMP doit être envoyé, il est envoyé à la communauté SNMP spécifiée par cette chaîne.
`Last Time Sent`	**Synopsis :** DDDD days, 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 :** Chaîne de 127 caractères **Par défaut :** EV2-Rise Commentaire décrivant cet événement.
`Owner`	**Synopsis :** Chaîne de 127 caractères **Par défaut :** Monitor Propriétaire de cet enregistrement d'événement. Nous recommandons de démarrer cette chaîne avec le mot 'monitor'.

4. Cliquez sur **Apply**.

4.11.3.3 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.
2. Sélectionnez l'événement dans le tableau. Le formulaire **RMON Events** s'affiche.

3. Cliquez sur **Delete**.

4.12 Mise à niveau/rétrogradage du firmware

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

4.12.1 Vérification de la somme de contrôle de hachage

Avant d'installer un nouveau firmware pour RUGGEDCOM ROS, il est recommandé de vérifier la somme de contrôle de hachage pour garantir que le firmware est authentique et n'est pas défaillant.

Pour des instructions sur la manière de vérifier la somme de contrôle de hachage, y compris une liste de sommes de contrôle de hachage pour tous les appareils et versions RUGGEDCOM ROS, voir la FAQ "Sommes de contrôle de hachage RUGGEDCOM" (https://support.industry.siemens.com/cs/ww/en/view/109779935).

4.12.2 Mise à niveau du firmware

Une mise à niveau du firmware RUGGEDCOM ROS (notamment le firmware principal, du chargeur de démarrage et FPGA) peut être nécessaire pour tirer parti des nouvelles fonctionnalités ou des correctifs. 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.

⚠ **NOTA**
Si une carte microSD/microSDHC est installée pendant la mise à niveau, le nouveau firmware est stocké dans la mémoire flash interne et sur la carte microSD/microSDHC.

Remarque
Si le processus de mise à niveau est interrompu, par exemple en raison d'une interruption de courant, RUGGEDCOM ROS est en mesure de récupérer si une carte microSD/microSDHC avec une image de firmware valide (`main.bin`) est installée avant le redémarrage suivant. RUGGEDCOM ROS copie l'image de firmware dans la mémoire interne et démarre à partir de cette dernière.

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

Remarque
Il est recommandé d'activer l'accès à l'interface du chargeur de démarrage pendant cette procédure si une récupération d'urgence est nécessaire (c'est-à-dire une interruption de courant pendant la mise à niveau). Pour augmenter la sécurité, Siemens recommande de désactiver l'accès au chargeur de démarrage une fois la mise à niveau terminée. Pour plus d'informations sur la gestion de l'accès au chargeur de démarrage, voir "Activation/désactivation de l'accès à l'interface du chargeur de démarrage (Boot Loader) (Page 43)".

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

1. Activez l'accès à l'interface du chargeur de démarrage. Pour plus d'informations, voir "Activation/désactivation de l'accès à l'interface du chargeur de démarrage (Boot Loader) (Page 43)".
2. Chargez une version différente de l'image de firmware binaire dans l'appareil ou insérez une carte microSD/microSDHC contenant l'image. Pour plus d'informations sur le chargement de fichiers, voir "Chargement/téléchargement de fichiers (Page 57)".
3. Réinitialisez l'appareil pour terminer l'installation. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".
4. 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-MPC83 Main Software v5.6.0 (Jan 01 5.6 00:01)
   ```

5. Désactivez l'accès à l'interface du chargeur de démarrage. Pour plus d'informations, voir "Activation/désactivation de l'accès à l'interface du chargeur de démarrage (Boot Loader) (Page 43)".

4.12.3 Rétrogradation du firmware

La rétrogradation du firmware RUGGEDCOM ROS n'est généralement pas recommandée car il peut avoir des effets non prévisibles. Cependant, procédez comme suit si une rétrogradation est requise :

Remarque
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.

Remarque
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 "Ouverture de session (Page 20)".
3. Effectuez une copie locale du fichier de configuration actuel. Pour plus d'informations, voir "Chargement/téléchargement de fichiers (Page 57)".

   ⚠ NOTA

   Risque pour la configuration - risque d'interruption de la communication.

   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 "Restauration des valeurs par défaut (Page 55)".
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 "Mise à niveau du firmware (Page 111)".
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
   ```

   ⚠ NOTA

   Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

   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 rétrogradation 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 la rétrogradation.

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

4.13 Réinitialisation de l'appareil

Procédez comme suit pour réinitialiser l'appareil :

1. Accédez à ***Diagnostics » Reset Device***. Le formulaire **Reset Device** s'affiche.
2. Cliquez sur **Confirm**.

4.14 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 "Connexion directe (Page 49)".
3. Restaurez tous les réglages par défaut pour l'appareil. Pour plus d'informations, voir "Restauration des valeurs par défaut (Page 55)".
4. Accédez à la CLI. Pour plus d'informations, voir "Utilisation de l'interface de ligne de commande (Page 25)".
5. Effacez le fichier de bannière existant en saisissant :

   ```
   banner -c
   ```

6. Confirmez l'effacement de la bannière en saisissant :

   ```
   type banner.txt
   ```

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

   ```
   clearlogs
   ```

8. Générez un certificat SSL quelconque en saisissant :

   ```
   sslkeygen ecc 256
   ```

   Le message *ssl.crt generation is now pending* apparaît, indiquant que le processus de génération du certificat SSL a commencé.

   Remarque
   Le processus de génération du certificat SSL peut prendre plusieurs minutes.

   Pour plus d'informations sur les certificats SSL, y compris les conditions requises et les exemples, voir "Gestion des clés et des certificats SSH/SSL (Page 154)".

9. Vérifiez que le certificat a été généré en saisissant :

   ```
   type syslog.txt
   ```

   Le syslog affiche des messages similaires à ceux présentés ci-dessous :

   ```
   21/08/30 15:36:57.958 INFO 35C Generation pending for ssl.crt: SSL Certificate
   21/08/30 15:36:58.186 INFO 35C Started generating ssl.crt: SSL Certificate
   21/08/30 15:36:58.489 INFO 35C Successfully generated ssl.crt: SSL Certificate
   21/08/30 15:36:59.059 INFO 35C Flashing ssl.crt started
   21/08/30 15:36:59.066 INFO 35C Flashing ssl.crt done
   21/08/30 15:36:59.066 INFO 35C Successfully updated ssl.crt.
   21/08/30 15:36:59.067 INFO 35C Generated ssl.crt was saved
   21/08/30 15:36:59.068 INFO 35C Key generation task finished for ssl.crt
   ```

10. Générez des clés SSH aléatoires en saisissant :

    ```
    sshkeygen rsa 1024
    ```

    Le message *ssh.key generation is now pending* apparaît, indiquant que le processus de génération des clés SSH a commencé.

    Remarque
    Le processus de génération des clés SSH peut prendre plusieurs minutes.

    Pour plus d'informations sur les clés SSH, y compris les conditions requises et les exemples, voir "Gestion des clés et des certificats SSH/SSL (Page 154)".

11. Vérifiez que les clés SSH ont été générées en saisissant :

    ```
    type syslog.txt
    ```

    Le syslog affiche des messages similaires à ceux présentés ci-dessous :

    ```
    21/08/30 15:33:37.179 INFO 35C Generation pending for ssh.keys: SSH Keys
    21/08/30 15:33:37.860 INFO 35C Started generating ssh.keys: SSH Keys21/08/30
     15:34:52.098 INFO 35C Successfully generated ssh.keys: SSH Keys
    21/08/30 15:34:53.266 INFO 35C SSH host key installed, MD5#
     BD:BD:07:E5:9F:83:E3:4A:48:DA:F8:93:6E:37:D6:A6
    21/08/30 15:34:53.268 INFO 35C Flashing ssh.keys started
    21/08/30 15:34:53.280 INFO 35C Flashing ssh.keys done
    21/08/30 15:34:53.280 INFO 35C Successfully updated ssh.keys.
    21/08/30 15:34:53.281 INFO 35C Generated ssh.keys was saved
    21/08/30 15:34:53.283 INFO 35C Key generation task finished for ssh.keys
    ```

    Pour plus d'informations sur les clés SSH, y compris les conditions requises et les exemples, voir "Gestion des clés et des certificats SSH/SSL (Page 154)".

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

    ```
    flashfile defrag
    ```

    Remarque
    Ce processus peut prendre plusieurs minutes.

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

    ```
    clearlogs
    ```

5 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.

5.1 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.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`System Name`	**Synopsis :** Chaîne de 24 caractères Le nom du système est affiché dans tous lesRUGGEDCOM ROSécrans de menu. 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 :** Chaîne de 49 caractères 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 :** Chaîne de 49 caractères 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**.

5.2 Personnalisation de l'écran d'ouverture de session

Pour afficher un message de bienvenue personnalisé, des informations sur l'appareil ou toute autre information sur 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 "Chargement/téléchargement de fichiers (Page 57)".

Vous pouvez également mettre à jour le fichier `banner.txt` à l'aide de la commande CLI `banner`. Pour plus d'informations, voir "Commandes CLI disponibles (Page 26)".

5.3 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 form**. Pour plus d'informations, voir "Configuration des services IP (Page 102)".

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 "Utilisation de l'interface de ligne de commande (Page 25)".
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.

5.4 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 "Gestion des alarmes RMON (Page 105)".

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.

5.4.1 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.

Remarque
Cette liste d'alarmes (configurables et non-configurables) est accessible via l'interface de ligne de commande (CLI) à l'aide de la commande `alarms`. Pour plus d'informations, voir "Commandes CLI disponibles (Page 26)".

Pour plus d'informations sur la modification d'une alarme préconfigurée, voir "Configuration d'une alarme (Page 119)".

5.4.2 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.

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.
2. Cliquez sur **Confirm**.

5.4.3 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 :

⚠ NOTA

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.
2. Sélectionnez une alarme. Le formulaire **Alarms** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Name`	**Synopsis :** Chaîne de 34 caractères ou [sys_alarm] **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 : • `EMRG`– L'appareil a rencontré une défaillance sérieuse qui a entraîné un redémarrage du système. • `ALRT`– L'appareil a rencontré une défaillance sérieuse qui n'a pas entraîné un redémarrage du système. • `CRIT`– L'appareil a rencontré un problème sérieux irrécupérable. • `ERRO`– L'appareil a rencontré un problème récupérable qui n'affecte pas sérieusement le fonctionnement. • `WARN`– Problème éventuellement sérieux affectant le fonctionnement général du système. • `NOTE`– 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. • `DEBG`– 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 :** Un entier compris entre 0 et 60 **Par défaut :** 60 Délai d'actualisation pour cette alarme.

4. Cliquez sur **Apply**.

5.4.4 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 "Configuration d'une alarme (Page 119)".

Weak Password Configured

RUGGEDCOM ROS génère cette alarme et consigne un message dans le syslog 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 syslog lorsque des clés par défaut sont utilisées. Pour plus d'informations sur les clés par défaut, voir "Gestion des clés et des certificats SSH/SSL (Page 154)".

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 syslog lorsque des tentatives de connexion réussissent et échouent. Un message est également consigné dans le syslog 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 syslog 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 syslog 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 syslog 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 syslog 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 syslog 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

5.4.5 Liste des alarmes

Le tableau suivant répertorie toutes les alarmes possibles dans RUGGEDCOM ROS et identifie si l'alarme est configurable par l'utilisateur.

Pour plus d'informations sur la configuration d'alarmes, voir "Configuration d'une alarme (Page 119)".

Nom	Niveau	Verrouillage	Trap	Journal	LED & relais	Configurable par l'utilisateur
Admin Level Password Changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
ARP security notification	Avertissement	Activé	Activé	Activé	Activé	Oui
Bootp - cfg transfer failed	Erreur	Activé	Activé	Activé	Activé	Non
Bootup error	Critique	Activé	Désactivé	Activé	Activé	Non
Bouncing link	Critique	Activé	Activé	Activé	Activé	Non

Nom	Niveau	Verrouillage	Trap	Journal	LED & relais	Configurable par l'utilisateur
BPDU Guard activated	Erreur	Activé	Activé	Activé	Activé	Oui
Bundle port inconsistent speed	Erreur	Activé	Activé	Activé	Activé	Non
ClkMgr Out of Resources	Avertissement	Activé	Non	Activé	Activé	Non
ClkMgr PrimarySource Failed	Avertissement	Activé	Désactivé	Activé	Activé	Non
Configuration changed	Info	Désactivé	Activé	Activé	Désactivé	Oui
Crashlog created	Critique	Activé	Désactivé	Non	Activé	Non
Data Storage passphrase changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
Daughter card reading failed	Critique	Activé	Activé	Activé	Activé	Non
Device Error	Critique	Activé	Activé	Désactivé	Activé	Non
DHCP security notification	Avertissement	Activé	Activé	Activé	Activé	Oui
Excessive failed login attempts	Avertissement	Activé	Activé	Activé	Activé	Oui
Fast link detection disabled	Critique	Activé	Activé	Activé	Activé	Non
File Transfer Happened	Remarque	Désactivé	Activé	Activé	Désactivé	Non
GMRP cannot learn more addresses	Avertissement	Activé	Activé	Activé	Activé	Oui
GPS/IRIGB error	Erreur	Activé	Activé	Activé	Désactivé	Oui
GPS/IRIGB status	Remarque	Activé	Activé	Activé	Désactivé	Oui
Guest Level Password Changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
GVRP cannot learn more VLANs	Avertissement	Activé	Activé	Activé	Activé	Oui
Heap error	Alerte	Activé	Désactivé	Activé	Activé	Non
IEEE1588 BMC Error	Avertissement	Activé	Activé	Désactivé	Désactivé	Oui
IEEE1588 Holdover State	Avertissement	Activé	Activé	Désactivé	Désactivé	Oui
IGMP Group Membership table full	Avertissement	Activé	Activé	Activé	Activé	Oui
IGMP Mcast Forwarding table full	Avertissement	Activé	Activé	Activé	Activé	Oui
Inconsistent speed/dpx in trunk	Erreur	Activé	Activé	Activé	Activé	Oui
Intermittent link	Erreur	Activé	Activé	Activé	Activé	Non
Invalid configuration	Critique	Activé	Désactivé	Désactivé	Activé	Non
Link up/down	Avertissement	Activé	Activé	Activé	Activé	Oui
LLDP remote table changed	Info	Désactivé	Activé	Activé	Désactivé	Non
Local Console Disabled	Remarque	Désactivé	Activé	Activé	Désactivé	Non
Local Console Enabled	Remarque	Désactivé	Activé	Activé	Désactivé	Non
Échec de connexion	Info	Activé	Activé	Activé	Désactivé	Oui
Login information	Info	Activé	Activé	Activé	Désactivé	Oui
MAC address authorization failed	Erreur	Activé	Désactivé	Activé	Activé	Oui
MAC address not learned	Avertissement	Activé	Activé	Activé	Activé	Oui
Mcast CPU filtering table full	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 1 ring multiple MRM error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 1 ring One Side Rx error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 1 ring multiple MRM error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 1 ring port down	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 2 ring multiple MRM error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 2 ring One Side Rx error	Avertissement	Activé	Activé	Activé	Activé	Oui

Nom	Niveau	Verrouillage	Trap	Journal	LED & relais	Configurable par l'utilisateur
MRP Inst 2 ring open	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 2 ring port down	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 3 ring multiple MRM error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 3 ring One Side Rx error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 3 ring open	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 3 ring port down	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 4 ring multiple MRM error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 4 ring One Side Rx error	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 4 ring open	Avertissement	Activé	Activé	Activé	Activé	Oui
MRP Inst 4 ring port down	Avertissement	Activé	Activé	Activé	Activé	Oui
New active STP topology	Info	Désactivé	Activé	Désactivé	Désactivé	Non
New STP root	Info	Désactivé	Désactivé	Désactivé	Désactivé	Oui
NTP service status changed	Info	Activé	Activé	Activé	Désactivé	Oui
Operator Level Password Changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
Port placed in Quarantined VLAN	Remarque	Activé	Désactivé	Activé	Activé	Oui
Port security violated	Avertissement	Activé	Activé	Activé	Activé	Oui
Power supply failed	Avertissement	Activé	Activé	Activé	Activé	Oui
PTP clock offset exceeds limit	Info	Désactivé	Activé	Activé	Désactivé	Non
PTP grandmaster changed	Info	Désactivé	Activé	Activé	Désactivé	Non
PTP master time step changed	Info	Désactivé	Activé	Activé	Désactivé	Non
PTP service started	Info	Désactivé	Activé	Activé	Désactivé	Non
PTP service stopped	Info	Désactivé	Activé	Activé	Désactivé	Non
RADIUS authenticate key changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
RADIUS service status changed	Info	Activé	Activé	Activé	Désactivé	Oui
Real Time Clock failed	Erreur	Activé	Désactivé	Activé	Activé	Non
Received looped back BPDU	Erreur	Activé	Activé	Activé	Activé	Oui
RMON alarm	Info	Activé	Désactivé	Activé	Activé	Non
ROS FPGA compatibility alarm	Avertissement	Activé	Désactivé	Activé	Désactivé	Non
Rx Buffer Low	Remarque	Activé	Désactivé	Activé	Activé	Non
SFP Alarm	Erreur	Activé	Activé	Activé	Activé	Non
SFP DDM Alarm	Avertissement	Activé	Activé	Activé	Activé	Oui
SFP DDM Warning	Avertissement	Activé	Activé	Activé	Activé	Oui
SNMP authenticate key changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
SNMP Authentication Failure	Avertissement	Activé	Activé	Activé	Désactivé	Oui
SNMP community changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
SNMP private Key changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui
SSH user pub key add failed	Avertissement	Activé	Activé	Activé	Activé	Oui
Stack overflow	Alerte	Activé	Désactivé	Activé	Activé	Non
STP events	Info	Désactivé	Désactivé	Activé	Désactivé	Oui
STP topology change	Info	Désactivé	Désactivé	Désactivé	Désactivé	Oui
Tacacs+ authenticate key changed	Remarque	Désactivé	Activé	Activé	Désactivé	Oui

Nom	Niveau	Verrouillage	Trap	Journal	LED & relais	Configurable par l'utilisateur
TACACS+ response invalid	Avertissement	Activé	Activé	Activé	Activé	Oui
TACACS+ service status changed	Info	Activé	Activé	Activé	Désactivé	Oui
Unable to obtain IP address	Critique	Activé	Activé	Activé	Activé	Non
Unknown privKey from SNMPv3 user	Avertissement	Activé	Activé	Activé	Désactivé	Oui
Unresolved speed	Erreur	Activé	Activé	Activé	Activé	Non
Watchdog reset	Alerte	Activé	Désactivé	Activé	Activé	Non
WeakPswdAdmin	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakPswdGuest	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakPswdOper	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakRadiusBackupKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakRadiusPrimaryKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakSnmpAuthKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakSnmpPrivKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakSSHKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakSSLKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakTacacsBackupKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui
WeakTacacsPrimaryKey	Avertissement	Activé	Activé	Activé	Désactivé	Oui

5.5 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.

Si une carte microSD/microSDHC contenant un fichier de configuration complet ou partiel est chargée dans l'emplacement de carte mémoire amovible, ce fichier est prioritaire sur les fichiers de configuration complets ou partiels stockés dans la mémoire interne.

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).

5.5.1 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 le support client.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

Ne rétrogradez jamais la version logicielle de RUGGEDCOM ROS au-delà de RUGGEDCOM ROS V5.6 lorsque le chiffrement est activé. Assurez-vous que les paramètres par défaut de l'appareil ont été restaurés avant la restauration d'une version antérieure.

1. Accédez à ***Administration » Configure Data Storage***. Le formulaire **Data Storage** s'affiche.
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 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.
`Confirm Passphrase`	**Synopsis :** Chaîne de 31 caractères 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**.

5.5.2 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 "Chargement/téléchargement de fichiers (Page 57)".

- Tout programme de traitement de texte capable de lire et d'écrire des fichiers ASCII.
- Outils de différenciation/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)

⚠ NOTA

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,
```

5.6 Gestion de MMS

RUGGEDCOM ROS prend en charge le protocole IEC 61850 Manufacturing Message Specification (MMS).

5.6.1 Comprendre MMS

RUGGEDCOM ROS prend en charge la norme IEC 61850, un protocole de gestion et de surveillance pour les appareils électroniques intelligents (IED) sur les sous-stations électriques. La norme utilise Manufacturing Message Specification (MMS) comme protocole de transport, tandis que le modèle d'objet de pont définit les objets à interroger ou à configurer.

MMS spécifie des services pour l'échange de données en temps réel entre des appareils en réseau et des applications informatiques. Il fournit un système de messages générique pour la communication entre des appareils industriels.

Le modèle de données utilisé par MMS est basé sur des nœuds logiques contenant un ensemble d'objets de données. Ces objets de données contiennent un ensemble d'attributs de données.

5.6.1.1 Rapport MMS

La fonctionnalité de rapport IEC 61850 est utilisée pour agréger un groupe d'objets de données de nœuds logiques. Ces objets de données peuvent être envoyés au client comme un rapport non sollicité piloté par événement ou comme un rapport basé sur le temps initié par le client.

Le rapport MMS est basé sur le paramètre *MMS Sessions Allowed (Sessions MMS autorisées)* qui contrôle combien de clients peuvent établir des connexions MMS simultanément à l'appareil pont RUGGEDCOM ROS. Pour plus d'informations sur la configuration de rapports MMS, voir "Configuration des services IP (Page 102)".

5.6.1.2 Rapports/jeux de données

RUGGEDCOM ROS prend en charge les types de jeux de données/rapports suivants :

- **LLDPStatus**

  Rapport basé sur le temps appartenant au nœud logique LPLD indiquant l'état LLDP de l'appareil. Il comprend trois objets de données : LPLD.RemPortId (identificateur de port distant), LPLD.RemChsId (identificateur de châssis de port distant) et LPLD.RemAddr (adresse de gestion de système distant).

- **PortLinkStatus**

  Rapport déclenché par événement appartenant au nœud logique LPCP indiquant l'état MAU du port physique de l'appareil. Il comprend l'objet de données LPCP.Mau (medium attachment unit link status).

- **PortStatistics**

  Rapport basé sur le temps appartenant au nœud logique LPCP indiquant l'état de fonctionnement du port physique de l'appareil. Il comprend quatre objets de données : LPCP.AutoNgt (si vrai, le port est en autonégociation), LPCP.RxCnt (nombre de messages reçus depuis la dernière réinitialisation), LPCP.TxCnt (nombre de messages envoyés depuis la dernière réinitialisation) et LPCP.FerPort (taux d'erreur de trame sur le port).

- **RSTPStatus**

  Rapport déclenché par événement appartenant au nœud logique LBRI indiquant l'état RSTP de l'appareil. Il comprend trois objets de données : LBRI.RstpRoot (device is RSTP root or not), LBRI.RstpTopoCnt (RSTP topology change count) et LBSP.RstpSt (RSTP port state).

- **SystemStatus**

  Rapport déclenché par événement appartenant au nœud logique LPHD indiquant l'état de fonctionnement de l'appareil. Il comprend deux objets de données :

LPHD.PhyHealth (état de santé de l'appareil) et LPHD.PwrSupAlm (état de l'alarme d'alimentation de l'appareil).

Remarque
Les fichiers `ruggedcom.icd` (IEC61850 IED fonctionnalité de description sur l'appareil) et `ruggedcom.iid` (IEC61850 description IED instanciée de l'appareil) indiquent les nœuds logiques pris en charge par RUGGEDCOM ROS. Pour plus d'informations sur le téléchargement de ces fichiers, voir "Chargement/téléchargement de fichiers (Page 57)".

5.6.1.3 Nœuds logiques pris en charge

RUGGEDCOM ROS prend en charge les nœuds logiques suivants :

Nœud logique	Description
LLN0	Nœud logique courant fournissant des informations génériques sur l'appareil dans son ensemble, telles que le nom du fournisseur ou la version logicielle.
LPHD (appareil physique)	Nœud logique contenant des informations de niveau système sur un appareil logique, telles que le nom du système et sa description.
LBRI (pont)	Nœud logique fournissant des informations relatives au spanning tree lorsque l'appareil fonctionne comme pont, telles que RSTP priority et RSTP hello time.
LPCP (port de communication physique)	Nœud logique fournissant des informations spécifiques pour chaque interface physique sur l'appareil, telles que l'état admin du port et son état d'auto-négociation.
LPLD (découverte de liaison de port)	Nœud logique fournissant des informations spécifiques liées à LLDP (Link Layer Discovery Protocol) pour chaque interface physique sur l'appareil, telles que l'ID de port local et l'ID de port distant.
LBSP (port Bridge Spanning tree)	Nœud logique fournissant des informations spécifiques liées au spanning tree pour chaque interface physique sur l'appareil, telles que l'état RSTP du port et l'état RSTP du port de périphérie.
LCMF (filtrage MAC de la voie de communication)	Nœud logique contenant des informations de filtrage relatives aux adresses MAC multidiffusion, telles que la liste blanche des adresses MAC multidiffusion et les ID de VLAN liés.
LCVF (filtrage VLAN de la voie de communication)	Nœud logique fournissant des informations spécifiques relatives à la configuration VLAN, telles que l'ID de port VLAN et la priorité CoS.

5.6.2 Affichage d'une liste de rapports MMS préconfigurés

Pour afficher une liste de rapports MMS préconfigurés pour l'appareil, accédez à ***Administration » Configure MMS***. Le tableau **MMS Report Configuration** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Name`	**Synopsis :** Chaîne de 32 caractères ou [SysStatus] **Par défaut :** SysStatus Nom de rapport MMS (c.-à-d. le nom du jeu de données).
`Status`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled État de rapport MMS initié ou modifié par l'application client. Si une application client active une fonctionnalité de rapport d'un jeu de données, l'état de ce jeu de données est 'Enabled'. Si aucune application client n'active la fonctionnalité de rapport d'un jeu de données, l'état de ce jeu de données est 'Disabled'.
`EventDriven`	**Synopsis :** [False | True] **Par défaut :** True Critères de rapport : • `True`– Le rapport est piloté par événement • `False`– Le rapport est basé sur le temps
`Period`	**Synopsis :** Un entier compris entre 30 et 10800 ou [Disabled] **Par défaut :** 300 Intervalle de rapport, en secondes, pour les rapports basés sur le temps. Ce paramètre est 'Disabled' pour les rapports pilotés par événement.

Pour plus d'informations sur la modification d'un rapport MMS, voir "Configuration d'un rapport MMS (Page 131)".

5.6.3 Configuration d'un rapport MMS

Si tous les rapports MMS sont préconfigurés sur l'appareil, certains rapports peuvent être modifiés en fonction de l'application. Cela comprend l'activation/la désactivation de certains rapports et la modification de l'intervalle de rapport.

Procédez comme suit pour configurer un rapport MMS :

1. Accédez à ***Administration » Configure MMS***. Le tableau **MMS Report Configuration** s'affiche.
2. Sélectionnez un rapport. Le formulaire **MMS Report Configuration** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

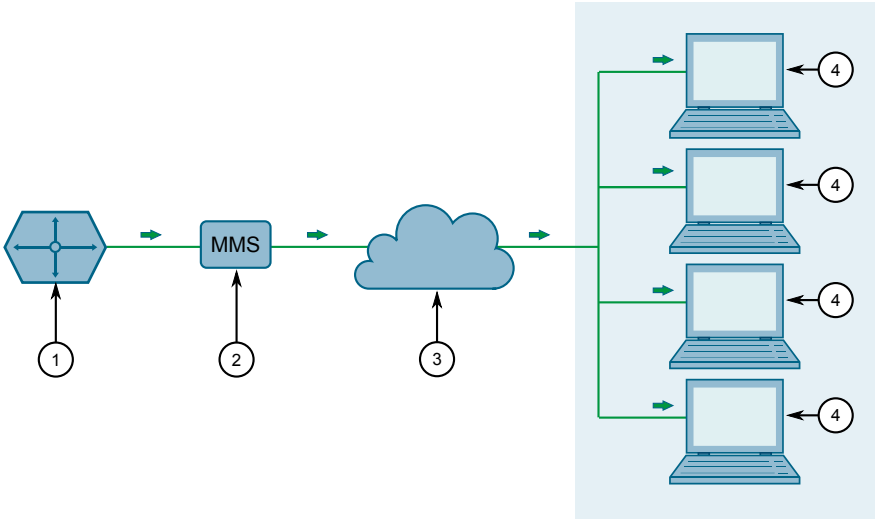
Paramètre	Description
`Period`	**Synopsis :** Un entier compris entre 30 et 10800 ou [Disabled] **Par défaut :** 300 Intervalle de rapport, en secondes, pour les rapports basés sur le temps. Ce paramètre est 'Disabled' pour les rapports pilotés par événement.

4. Cliquez sur **Apply**.

5.6.4 Exemple : configuration de rapports MMS

Cet exemple illustre la façon de configurer l'appareil pour générer des rapports MMS.

La topologie suivante décrit un scénario où des rapports MMS sont envoyés depuis RUGGEDCOM ROS à quatre clients sur un LAN.



① RSG2488
② Rapport MMS
③ LAN
④ Client

Figure 5.1 Topologie – MMS

Procédez comme suit pour configurer l'appareil afin qu'il reçoive des rapports MMS :

1. Côté client, procédez comme suit :

   Remarque
   La configuration du client dépend du client MMS utilisé. Veuillez consulter les instructions d'utilisation OEM pour des détails de configuration spécifiques.

   a. Activez ou désactivez des rapports MMS spécifiques comme souhaité. Pour obtenir une liste des rapports disponibles dans RUGGEDCOM ROS, voir "Rapports/jeux de données (Page 129)".

   b. Configurez l'appareil pour qu'il fournisse des rapports basés événement ou basés temps selon vos besoins.

2. Dans RUGGEDCOM ROS, procédez comme suit :

   a. Configurez le nombre de sessions MMS autorisé pour spécifier le nombre de clients qui reçoivent des rapports. 4 sessions sont autorisées par la

topologie. Pour plus d'informations sur la configuration des sessions MMS, voir "Configuration des services IP (Page 102)".

b. Si les rapports basés temps sont sélectionnés côté client, configurez l'intervalle de temps de rapport comme souhaité. Pour plus d'informations, voir "Configuration d'un rapport MMS (Page 131)".

3. Pour vérifier la configuration, assurez-vous que chaque client reçoive des rapports MMS de l'appareil par la configuration.

6 Securité

Ce chapitre décrit comment configurer et gérer les fonctionnalités de RUGGEDCOM ROS liées à la sécurité.

6.1 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.

   Remarque
   RUGGEDCOM ROS requiert que tous les mots de passe utilisateur 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 de 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*. *net-25admin* 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 "Gestion des alarmes (Page 118)".

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

Paramètre	Description
`Auth Type`	**Synopsis :** [Local | RADIUS | TACACS+ | RADIUSorLocal | TACACS+orLocal | RADIUSandLocal | TACACS+andLocal] **Par défaut :** Local Le mot de passe peut être authentifié à l'aide de valeurs configurées localement ou du serveur RADIUS ou TACACS

Paramètre	Description
	+ distant. La définition de la valeur sur une combinaison quelconque comprenant RADIUS ou TACACS+ requiert la configuration du tableau Security Server. Réglages : • `Local`– Authentification depuis le tableau des mots de passe local • `RADIUS`– Authentification à l'aide d'un serveur RADIUS pour l'accès réseau uniquement (HTTP/HTTPS, SSH, RSH, Telnet). Pour l'accès console, authentifiez-vous depuis le tableau des mots de passe local. Si l'authentification locale échoue, authentifiez-vous à l'aide du serveur RADIUS. • `TACACS+`– Authentification à l'aide d'un serveur TACACS+ pour l'accès réseau uniquement (HTTP/HTTPS, SSH, RSH, Telnet). Pour l'accès console, authentifiez-vous depuis le tableau des mots de passe local. Si l'authentification locale échoue, authentifiez-vous à l'aide du serveur TACACS+. • `RADIUSOrLocal`– Authentification à l'aide de RADIUS. Si le serveur n'est pas accessible, authentifiez-vous depuis le tableau des mots de passe local. • `TACACS+OrLocal`– Authentification à l'aide de TACACS+. Si le serveur n'est pas accessible, authentifiez-vous depuis le tableau des mots de passe local. • `RADIUSandLocal`– Authentification à l'aide de RADIUS. En cas d'échec, authentifiez-vous depuis le tableau des mots de passe local. • `TACACS+andLocal`– Authentification à l'aide de TACACS+. En cas d'échec, authentifiez-vous depuis le tableau des mots de passe local.
`Guest Username`	**Synopsis :** Chaîne de 15 caractères **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 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 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 :** Chaîne de 15 caractères **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.

Paramètre	Description
`Operator Password`	**Synopsis :** Chaîne de 19 caractères Le nom d'utilisateur correspondant se trouve dans le champ Operator Username ; ne peut pas modifier des réglages ; peut réinitialiser des alarmes, des statistiques, des journaux, etc.
`Confirm Operator Password`	**Synopsis :** Chaîne de 19 caractères Le nom d'utilisateur correspondant se trouve dans le champ Operator Username ; ne peut pas modifier des réglages ; peut réinitialiser des alarmes, des statistiques, des journaux, etc.
`Admin Username`	**Synopsis :** Chaîne de 15 caractères **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 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 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 :** Un entier compris entre 1 et 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**.

6.2 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 usine 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 "Connexion directe (Page 49)".

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.

6.3 Gestion de l'authentification utilisateur

Cette section décrit les différentes méthodes d'authentification des utilisateurs.

6.3.1 Méthodes d'authentification

RUGGEDCOM ROS prend en charge les authentifications Local, RADIUS, TACACS+, RADIUS or Local, et TACAS+ or Local server. La méthode peut être sélectionnée à l'aide du paramètre **Auth Type**.

Pour plus d'informations sur la configuration du paramètre **Auth Type**, voir "Configuration de mots de passe (Page 135)".

Le tableau suivant montre les accès pour différents scénarios basés sur les méthodes d'authentification prises en charge.

Type d'authentification	Méthode/scénario d'authentification	Informations d'identification pour accès de connexion	Méthode d'accès	
			Console locale	Réseau (SSH/ Telnet/WebUI)
Local	Authentification locale	Local	✓	✓
	Authentification pour serveur RADIUS	RADIUS	×	×
RADIUS	Authentification pour serveur RADIUS	RADIUS	✓	✓
	Authentification locale	Local	✓	✓
	Serveur inaccessible	Local	✓	×
		RADIUS	×	×

Type d'authentification	Méthode/scénario d'authentification	Informations d'identification pour accès de connexion	Méthode d'accès	
			Console locale	Réseau (SSH/ Telnet/WebUI)
	Clé partagée erronée	Local	✓	×
		RADIUS	×	×
	Port cible erroné	Local	✓	×
		RADIUS	×	×
TACACS+	Authentification pour serveur TACACS+	TACACS+	✓	✓
	Authentification locale	Local	✓	✓
	Serveur inaccessible	Local	✓	×
		TACACS+	×	×
	Clé partagée erronée	Local	✓	×
		TACACS+	×	×
	Port cible erroné	Local	✓	×
		TACACS+	×	×
RADIUSorLocal	Authentification pour serveur RADIUS	RADIUS	✓	✓
	Authentification locale	Local	✓	×
	Serveur inaccessible	Local	✓	✓
		RADIUS	×	×
	Clé partagée erronée	Local	×	×
		RADIUS	×	×
	Port cible erroné	Local	✓	✓
		RADIUS	×	×
TACACS+orLocal	Authentification pour serveur TACACS+	TACACS+	✓	✓
	Authentification locale	Local	✓	×
	Serveur inaccessible	Local	✓	✓
		TACACS+	×	×
	Clé partagée erronée	Local	×	×
		TACACS+	×	×
	Port cible erroné	Local	✓	✓
		TACACS+	×	×
RADIUSandLocal	Authentification pour serveur RADIUS	RADIUS	✓	✓
	Authentification locale	Local	✓	✓

Type d'authentification	Méthode/scénario d'authentification	Informations d'identification pour accès de connexion	Méthode d'accès	
			Console locale	Réseau (SSH/ Telnet/WebUI)
	Serveur inaccessible	Local	✓	✓
		RADIUS	×	×
	Clé partagée erronée	Local	✓	✓
		RADIUS	×	×
	Port cible erroné	Local	✓	✓
		RADIUS	×	×
TACACS+andLocal	Authentification pour serveur TACACS+	TACACS+	✓	✓
	Authentification locale	Local	✓	✓
	Serveur inaccessible	Local	✓	✓
		TACACS+	×	×
	Clé partagée erronée	Local	✓	✓
		TACACS+	×	×
	Port cible erroné	Local	✓	✓
		TACACS+	×	×

6.3.2 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 autre 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 est activée. RUGGEDCOM ROS reste transparent et n'apporte aucune modification au nom d'utilisateur. Pour plus d'informations sur l'authentification IEEE 802.1x, voir "Concepts de sécurité de port (Page 146)".

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.

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

Paramètre	Description
`Username Extension`	**Synopsis :** Chaîne de 127 caractères 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% : nom associé au profil utilisateur (par exemple admin, opérateur, etc.) %IPaddr% : adresse IP de gestion du commutateur agissant comme Network Access Server (NAS). %SysName% : nom système donné à l'appareil. %SysLocation% : 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'authentification.

3. Cliquez sur **Apply**.

6.3.3 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).

Remarque
Les messages RADIUS sont envoyés comme messages UDP. Le commutateur et le serveur RADIUS doivent utiliser la même clé d'authentification et de chiffrement.

Remarque
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].

6.3.3.1 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 requête 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 :

Attribut	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.

6.3.3.2 Configuration du client RADIUS sur l'appareil

Le client RADIUS peut être configuré de manière à utiliser deux serveurs RADIUS : un serveur principal et un serveur de sauvegarde. Si le serveur principal n'est pas disponible, l'appareil tente automatiquement de se connecter au serveur de sauvegarde.

⚠ NOTA
Le client RADIUS utilise le PAP (Password Authentication Protocol) pour vérifier l'accès. Aucun autre protocole d'authentification n'est pris en charge.

Pour les commandes CLI relatives à la configuration du client RADIUS sur l'appareil, voir "Commandes CLI disponibles (Page 26)".

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 Table** s'affiche.
2. Sélectionnez **Primary** ou **Backup** dans le tableau. Le formulaire **RADIUS Server** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Server`	**Synopsis :** Chaîne de 8 caractères ou [Primary] **Par défaut :** Primary Ce champ indique si cette configuration est valable pour un serveur principal ou de sauvegarde.
`IP Address`	**Synopsis :** Any valid IP address Adresse IP du serveur.
`Auth UDP Port`	**Synopsis :** Un entier compris entre 1 et 65535 **Par défaut :** 1812 Port IP sur le serveur.
`Max Retry`	**Synopsis :** Un entier compris entre 1 et 10 **Par défaut :** 2 Nombre maximum de tentatives par l'authentificateur de contact avec le serveur d'authentification pour authentifier l'utilisateur en cas de défaillance quelconque.
`Timeout`	**Synopsis :** Un entier compris entre 1000 et 120000 **Par défaut :** 10000 Délai d'attente en millisecondes pendant lequel l'authentificateur attend une réponse du serveur d'authentification.
`Reachable`	**Synopsis :** [No | Yes] État du serveur.
`Auth Key`	**Synopsis :** Chaîne de 31 caractères Clé d'authentification à partager avec le serveur.
`Confirm Auth Key`	**Synopsis :** Chaîne de 31 caractères Clé d'authentification à partager avec le serveur.

4. Cliquez sur **Apply**.

6.3.4 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.

6.3.4.1 Configuration de TACACS+

RUGGEDCOM ROS peut être configuré de manière à utiliser deux serveurs TACACS + : un serveur principal et un serveur de sauvegarde. Si le serveur principal n'est pas disponible, l'appareil tente automatiquement de se connecter au serveur de sauvegarde.

Pour les commandes CLI relatives à la configuration de TACACS+, voir "Commandes CLI disponibles (Page 26)".

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 Table** s'affiche.
2. Sélectionnez **Primary** ou **Backup** dans le tableau. Le formulaire **TACACS Plus Server** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Server`	**Synopsis :** Chaîne de 8 caractères ou [Primary] **Par défaut :** Primary Ce champ indique si cette configuration est valable pour un serveur principal ou de sauvegarde.
`IP Address`	**Synopsis :** Any valid IP address Adresse IP du serveur.
`Auth TCP Port`	**Synopsis :** Un entier compris entre 1 et 65535 **Par défaut :** 49 Port IP sur le serveur.
`Max Retry`	**Synopsis :** Un entier compris entre 1 et 10 **Par défaut :** 3 Nombre maximum de tentatives par l'authentificateur de contact avec le serveur d'authentification pour authentifier l'utilisateur en cas de défaillance quelconque.

Paramètre	Description
`Timeout`	**Synopsis :** Un entier compris entre 1000 et 120000 **Par défaut :** 10000 Délai d'attente en millisecondes pendant lequel l'authentificateur attend une réponse du serveur d'authentification.
`Reachable`	**Synopsis :** [No | Yes] État du serveur.
`Auth Key`	**Synopsis :** Chaîne de 31 caractères ou [mySecret] **Par défaut :** mySecret Clé d'authentification à partager avec le serveur.
`Confirm Auth Key`	**Synopsis :** Chaîne de 31 caractères 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 "Configuration des droits d'utilisateur (Page 145)".
5. Cliquez sur **Apply**.

6.3.4.2 Configuration des droits d'utilisateur

Chaque demande d'authentification TACACS+ comprend un attribut *priv_lvl* utilisé pour accorder l'accès à l'appareil. Par défaut, l'attribut utilise les plages suivantes définies dans le fichier de configuration TACACS+ :

- **15** représente le niveau d'accès *administrateur*
- **2-14** représente le niveau d'accès *opérateur*
- **1** représente le niveau d'accès *invité*

La commande CLI **svcmod** est utilisée pour configurer les droits d'utilisateur. Les valeurs saisies doivent correspondre à une ou plusieurs options définies numériquement (entre 0 et 15) dans le fichier de configuration TACACS+ situé dans le serveur TACACS+.

Pour plus d'informations sur la commande CLI **svcmod**, voir "Commandes CLI disponibles (Page 26)".

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.

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

Paramètre	Description
`Admin Priv`	**Synopsis :** Un entier compris entre 0 et 15 ou a range (e.g. 2-14) **Par défaut :** 15 Niveau de privilège à affecter à l'utilisateur.
`Oper Priv`	**Synopsis :** Un entier compris entre 0 et 15 ou a range (e.g. 2-14) **Par défaut :** 2-14 Niveau de privilège à affecter à l'utilisateur.
`Guest Priv`	**Synopsis :** Un entier compris entre 0 et 15 ou a range (e.g. 2-14) **Par défaut :** 1 Niveau de privilège à affecter à l'utilisateur.

3. Cliquez sur **Apply**.

6.4 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.

6.4.1 Concepts de sécurité de port

Cette section décrit certains concepts importants de la mise en œuvre de la sécurité de port dans RUGGEDCOM ROS.

6.4.1.1 Authentification basée sur des adresses MAC statiques

Avec cette méthode, le commutateur valide les adresses MAC source de trames reçues 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 des premières adresses MAC source 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.

6.4.1.2 Authentification basée sur des adresses MAC statiques dans un anneau MRP

Lorsque la sécurité de port est configurée sur un MRC, l'adresse MAC des ports d'anneau du MRM doit être configurée dans le tableau des **Static MAC Addresses** pour que l'anneau reste à l'état fermé.

Pour permettre la communication (c.-à-d. le ping) entre les appareils MRP dans un anneau, chaque appareil dont la sécurité de port est activée sur les ports MRP doit contenir les adresses MAC de tous les appareils de l'anneau dans son tableau **Static MAC Addresses**.

Pour plus d'informations sur la configuration de MRP, voir "Gestion du Media Redundancy Protocol (MRP) (Page 246)".

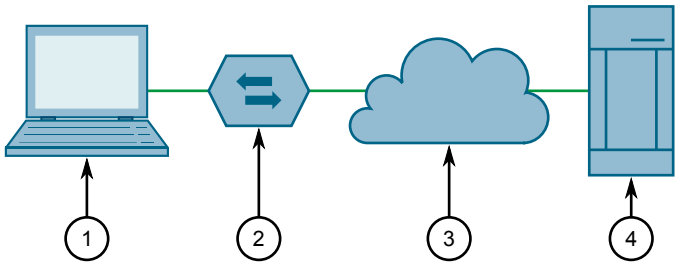
Pour plus d'informations sur la configuration d'une adresse MAC statique, voir "Ajout d'une adresse MAC statique (Page 183)".

6.4.1.3 Authentification IEEE 802.1X.

La 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.



① Demandeur
② Commutateur d'authentification
③ LAN
④ Serveur d'authentification

Figure 6.1 Topologie générale de IEEE 802.1x

⚠ NOTA

RUGGEDCOM ROS prend en charge le PEAP (Protected Extensible Authentication Protocol), EAP Transport Layer Security (EAP-TLS) et EAP-MD5. PEAP et EAP-TLS sont plus sécurisés et sont recommandés s'ils sont disponibles 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.

6.4.1.4 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.

6.4.1.5 VLAN restreints

RUGGEDCOM ROS permet aux utilisateurs de configurer des ports 802.1X en mode *Guest VLAN* ou *Quarantine VLAN* pour limiter les services aux clients lorsque l'authentification IEEE 802.1x ou 802.1x/MAC-Auth échoue. Par exemple, un administrateur peut choisir de restreindre l'accès uniquement à des imprimantes, Internet ou des téléchargements spécifiques pour des utilisateurs authentifiés.

Si l'authentification d'un client échoue après un nombre de tentatives défini, le port configuré sera commuté automatiquement sur le Quarantine VLAN ou le Guest VLAN en fonction du mode de sécurité et de la configuration de sécurité du client :

- Si un appareil connecté prend en charge la sécurité 802.1x, le port sera commuté sur le Quarantine VID en cas d'échec de son authentification.
- Si un appareil connecté est incompatible avec 802.1X et la sécurité de port est définie sur 802.1X, le port deviendra membre du Guest VLAN après expiration de l'authentification.

Un trap SNMP sera généré si un appareil client est placé dans le Quarantine VLAN ou le Guest VLAN. Une alarme avertit l'utilisateur du changement d'état du port.

Si un port est un membre du Quarantine VLAN, ROS tentera d'authentifier de nouveau le client à des intervalles configurés. Des clients dont l'authentification a échoué restent dans le Quarantine VLAN jusqu'à ce qu'ils soient de nouveau authentifiés avec succès, ou jusqu'à ce que la liaison physique soit coupée. Si la réauthentification échoue, le port reste membre du Quarantine VLAN.

Aucune tentative de réauthentification n'est effectuée pour les clients dans des Quarantine VLAN. Lorsque la trame EAPOL Start est reçue du client, le port est commuté à l'état non authentifié et l'accès client depuis le Guest VLAN est supprimé pour continuer le processus d'identification.

Le tableau suivant montre le comportement du port en mode Quarantine et Guest en cas d'échec d'authentification :

Mode de sécurité de port	Sécurité client	Mode en cas d'échec d'authentification
802.1x	compatible 802.1x	Quarantine VLAN
	non compatible 802.1x	Guest VLAN
802.1x/MAC-Auth	compatible 802.1x	Quarantine VLAN
	non compatible 802.1x	Quarantine VLAN

Pour plus d'informations sur la configuration d'un Guest/Quarantine VLAN, voir "Configuration de la sécurité du port (Page 151)".

6.4.1.6 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.

6.4.2 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 autorisées avec IEEE 802.1X ne sont pas affichées.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Port sur lequel l'adresse MAC a été apprise.
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF Adresse MAC autorisée apprise par le commutateur.
`VID`	**Synopsis :** Un entier compris entre 0 et 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 "Configuration de la sécurité du port (Page 151)".
- Configurez IEEE 802.1X. Pour plus d'informations, voir "Configuration d'IEEE 802.1X (Page 153)".

6.4.3 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.
2. Sélectionnez un port Ethernet. Le formulaire **Ports Security** s'affiche.

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

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Numéro de port.
`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 que la liaison soit 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.
`Quarantine VID`	**Synopsis :** Un entier compris entre 1 et 4096 ou [None] **Par défaut :** None Identificateur VLAN du VLAN de quarantaine. Applicable uniquement si le champ 'Security' a été défini sur '802.1x' ou '802.1x/MAC-Auth'. Le port est placé dans le VLAN de quarantaine si l'authentification d'un client échoue.
`Guest VID`	**Synopsis :** Un entier compris entre 1 et 4096 ou [None] **Par défaut :** None Identificateur VLAN du VLAN invité. Applicable uniquement si le champ 'Security' a été défini sur '802.1x'. Le port est placé dans le VLAN invité si un client ne prend pas en charge la norme 802.1x.
`Autolearn`	**Synopsis :** Un entier compris entre 1 et 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.

Paramètre	Description
`Sticky`	**Synopsis :** [No | Yes] **Par défaut :** Yes 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.
`Shutdown Time`	**Synopsis :** Un entier compris entre 1 et 86400 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 :** Chaîne de 31 caractères 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 à partir de ou vers un port sécurisé *non-sticky*

Remarque
Le trafic est perdu jusqu'à ce que l'adresse MAC source du trafic entrant soit autorisée par rapport au tableau Static MAC address.

4. Cliquez sur **Apply**.

6.4.4 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.
2. Sélectionnez un port Ethernet. Le formulaire **802.1X Parameters** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Numéro de port.

Paramètre	Description
`txPeriod`	**Synopsis :** Un entier compris entre 1 et 65535 **Par défaut :** 30 Temps d'attente du paquet de requête/d'identité EAP du demandeur avant la retransmission d'un paquet de requête/d'identité EAP.
`quietPeriod`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 60 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 :** Un entier compris entre 60 et 86400 **Par défaut :** 3600 Intervalle entre les réauthentifications périodiques du demandeur.
`reAuthMax`	**Synopsis :** Un entier compris entre 1 et 10 **Par défaut :** 2 Nombre de tentatives de réauthentification admissible avant que le port ne soit plus autorisé.
`suppTimeout`	**Synopsis :** Un entier compris entre 1 et 300 **Par défaut :** 30 Temps d'attente de la réponse du demandeur pour le paquet EAP du serveur d'authentification.
`serverTimeout`	**Synopsis :** Un entier compris entre 1 et 300 **Par défaut :** 30 Temps d'attente de la réponse du serveur d'authentification pour le paquet EAP du demandeur.
`maxReq`	**Synopsis :** Un entier compris entre 1 et 10 **Par défaut :** 2 Nombre maximum de retransmissions du paquet de requête EAP du serveur d'authentification au demandeur avant l'expiration de la session d'authentification.

4. Cliquez sur **Apply**.

6.5 Gestion des clés et des certificats SSH/SSL

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

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

Siemens recommande de procéder comme suit avant la mise en service de l'appareil :

- Remplacez le certificat SSL auto-signé fourni en usine par un certificat signé par une autorité de certification (CA) de confiance.
- Configurez le client SSH pour qu'il utilise *diffie-hellman-group14-sha1* ou mieux

Remarque
Seuls les administrateurs peuvent écrire des certificats et des clés pour l'appareil.

Chaque appareil RUGGEDCOM ROS est livré avec un certificat SSL auto-signé unique ECC 256 et une paire de clés d'hôte RSA 2048 SSH 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. 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`.

6.5.1 Certificats SSL

RUGGEDCOM ROS prend en charge les certificats SSL 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 NIST P-256, P-384 ou P-521
- Pour les versions non contrôlées (NC) de RUGGEDCOM ROS : Paire de clés RSA, 512 ou 2 048 bits

Remarque
Les clés courbe elliptique d'une longueur inférieure à P-256 bits ne sont pas recommandées.

Remarque
Les clés RSA d'une longueur inférieure à 2 048 bits ne sont pas recommandées.

Deux fichiers PEM standard sont requis : le certificat SSL et le fichier de clé privée RSA correspondant. Ils sont concaténés dans le fichier `ssl.crt` résultant, qui peut être chargé dans RUGGEDCOM ROS : Pour plus d'informations sur le transfert de fichiers entre l'appareil et un ordinateur hôte, voir "Chargement/téléchargement de fichiers (Page 57)".

Même si RUGGEDCOM ROS est capable d'utiliser des certificats auto-signés créés à l'aide de la commande `sslkeygen`, Siemens recommande d'utiliser un

certificat X.509 émis par l'autorité de certification (Certificate Authority, CA) d'une organisation.

6.5.2 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) suivant utilise l'utilitaire de 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
```

Pour obtenir un exemple de clé SSH générée par RUGGEDCOM ROS, voir "Exemples de certificats et de clés (Page 161)".

6.5.3 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.

6.5.3.1 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
- Type d'entrée : UserKey
- Niveau d'accès : (administrateur, opérateur ou invité)
- État de révocation : actif/inactif (toujours actif pour les clés)
- Nom d'utilisateur : 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/GR24NrRJa0Lc7scNsWR
gi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uLJe0Su3RvyNYz1jkdSwHq2h
SZCpukJxJ6CK95Po/sVa5Gq2gMaHowiYDSkcx+AJywzK/eM6i/jc125lRxFPdfkj74u+ob3PCvmIWz5z3WAJ
BrQU1IDPHDets511WMu8O9/mAPZRwjqrWhRsqmcXZuv5oo54wIopCAZ
So20SPzM2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/oMFFn934cbO5N6etsJSvplY
Q4pMCw6Ok8Q/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

6.5.3.2 Ajout d'une clé publique

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

Il existe 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 existantes du fichier *sshpub.keys*.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

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 "Chargement/téléchargement de fichiers (Page 57)".
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 "Utilisation de l'interface de ligne de commande (Page 25)".
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 ""Affichage de journaux locaux et système (Page 62)"".

6.5.3.3 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 "Utilisation de l'interface de ligne de commande (Page 25)".
2. Dans l'invite de commande de la CLI, saisissez :

   ```
   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.

6.5.3.4 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 "Utilisation de l'interface de ligne de commande (Page 25)".
2. Dans l'invite de commande de la CLI, saisissez :

   ```
   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 (administrateur, opérateur ou invité) 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

6.5.3.5 Suppression d'une clé publique

Les administrateurs peuvent supprimer une ou plusieurs clé(s) publique(s).

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 "Utilisation de l'interface de ligne de commande (Page 25)".
2. Dans l'invite de commande de la CLI, saisissez :

   ```
   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 la ou les clé(s) publique(s) :

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

6.5.4 Exemples de certificats et de clés

Pour SSL, les certificats doivent satisfaire aux exigences énoncées dans "Certificats SSL (Page 156)".

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
A1UEChMJUnVnZ2VkY29tMRkwFwYDVQQLExBDdXN0b21liciBTdXBwb3J0MSYwJAYD
VQQDEx1XUy1NSUxBTkdPVkFOLlJVR0dFRENPTS5MT0NBTDEkMCIGCSqGSIb3DQEJ
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-----
MIIEpQIBAAKCAQEAn3UT94ZjlmBjygLXaA21ULum7EDmgsvFvg2tKYyaMj1en5UW
x172GvlDLUm5EwGmcG9u6DyuO3wOyv/taD1OUFkZA1W7cPu9NjeTtZjIQCx33xSU
1d6INMi2oOzwJmWzqwqIkIgy0uMdw78be4n7359U0UOOEtCStOmUfdw34jv6c38J
8sb+lC/FktX8Eilka4mDr07tf/ivC2kdwpPlGZIKt/xjcwjOsNHIBSfqbEbg5mO3
9OAPqsPRWKhBQZ6rM8aqEQjGPlrSTTNHrxO/CYVxAh0gtz+6qUytL3zi7Z9P7EzD
H8V8qNdXRNN0w5hsh2A5ZJj6+cbQJm0JHQeOowIDAQABAoIBAH2zXqUfBLyTibbC
3KoDPG7DLwhI9S4gkuaKg3ogg6GdLU2hys4p9to2qxU1a7cm8tzpi0V6KGNuHX87
```

```
lxw4T9cZFZXCbLvZR0RJNaDPKvUj2O87m0SpYzgxDX74qSuruqHX8OX26BHExj78
FR8jHDIhuUwp9AKy9yO0isFY65jkLov6tdRpNy5A+QrGyRVBilCIT6YFYKSzEEI8
6+29FkLtX+ERjqxJs+aGHyEPDWE4Zy7dBsuTk1Fwz8F6/rOz4PS2pNQXc2sWmomn
muQXv0hwKY5gMcovCkC3y/op3kNuc/3qeBHjeCBYEMLR0o25hZHGrKOrQahFsy+R
V48sgIECgYEA0H66Ijfcc7NpgKOQwyvCt9/uhRZ3RkeABoSBLb/wYfQjw4pMadqr
RMMzVPzOLC459Giv4m8GeikNPl53rYdTCRmd/t1nZClU/UQKhgj+RRt4xY2cJNsg
j2CTZDr5SJO8H957K1IbvN5mxdsWZuDc5dtf0wBMIaCJoXR/iDMcf2MCgYEAw8oK
Dkpz9PdhGkbTE0ARLeUv7okelBkfDIGgucXBFHUElHAGe+XLF5dMppmzRDHXi2NG
gSNPJsDOlgSyLJjKX7HapYeAJWm91w5kJEX+oERr1EnEPWPvOHI+OW5DjM6eR1s9
xRJ87e3ymgLIF7G5rmf0p3OlnVvCaQvIVYTB98ECgYEAl+sPI2nCp0eeY05LZ/rV
6fcwLCdfh4UHwzf/jF9j/2vON2fpH+RmkTcOiymd7NFOB0nUhtBRTufkr4JT/8wv
89yHpDKdaH05YUWXyWx6Ic7PpFr34F8OjYpYO1tBUuHa3PnWk41Dis4e4qIt446L
Rq0fWHbKAmKghlWFq69aX3MCgYEArKU2JM/mXHbfe0pEyk7OV0gn8hGbk0Brrp2H
2wjUb3OYbEQ0k4BYjB7wimAyQcoppVIPU8SNAUE3afYOH2FD4wp0IU7Q4yzRKBga
mhnWpABxjSrXDsNWqNGkqQPgMQPpcka0u1jILQ6LxN77Dlm7wF0O0bIash292t92
8mI0oIECgYEAql8/uRHGtwSk64rXWXI+uq+x4ewwZkVc+mMmJ0yCMuQsOzbQTxhx
v9GEi3xsFbNazGCx4b56+/6Bi6gf7aH+NeK2+7C4ddlpHGEawoEcW1CW8hRQ2brp
vWgC+m5nmQ2SaYGzlilzZVK3JE6qOZ/AG8k+ZEG9tsvakMliG1SoJXk=
-----END RSA PRIVATE KEY-----
```

Pour SSH, DSA ou RSA, les paires de clés hôtes doivent satisfaire aux exigences énoncées dans "Clé d'hôte SSH (Page 157)".

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
sml/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```

7 Layer 2 (Couche 2)

Ce paragraphe décrit les fonctionnalités Layer 2 (Couche 2) ou Data Link Layer (DLL) de RUGGEDCOM ROS.

7.1 Gestion de LAN 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 deux manières :

- **Explicitement**

  Les VLAN statiques peuvent être créés dans le commutateur. Pour plus d'informations sur les VLAN statiques, voir "Gestion de VLAN statiques (Page 176)".

- **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.

Pour plus d'informations sur les VLAN, voir "Concepts VLAN (Page 163)".

7.1.1 Concepts VLAN

Cette section décrit certains concepts importants de la mise en œuvre de VLAN dans RUGGEDCOM ROS.

7.1.1.1 Trames balisées ou 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 égal à 0, elle est considérée comme trame non balisée.

7.1.1.2 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.

7.1.1.3 VLAN de gestion

Par défaut, tout le trafic de gestion appartient au VLAN de gestion. Des VLAN de gestion auxiliaires peuvent être configurés pour déplacer le trafic de gestion. Cependant, les trafics BOOTP, DHCP et LLDP ne peuvent appartenir qu'au VLAN de gestion.

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. Le VLAN de gestion peut être modifié pour restreindre l'accès de gestion à un groupe spécifique d'utilisateurs.

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

Les interfaces IP appartenant au VLAN de gestion doivent être connectées à un réseau de confiance.

7.1.1.4 VLAN de gestion auxiliaires

En plus du VLAN de gestion, des VLAN de gestion auxiliaires peuvent transmettre le trafic de gestion associé aux services suivants :

- MMS
- Modbus
- Radius/TacPlus
- Shell distant
- Syslog distant
- SNMP
- SNTP

- SSH
- TFTP
- Telnet
- Serveur Web

Cependant, contrairement au VLAN de gestion, les VLAN de gestion auxiliaires ne peuvent pas transmettre le trafic BOOTP, DHCP ou LLDP.

Aucun VLAN de gestion auxiliaire n'est configuré par défaut. Un maximum de 254 VLAN de gestion auxiliaires peuvent être configurés. La configuration des VLAN de gestion auxiliaires peut être utilisée pour restreindre ou étendre l'accès de gestion à un groupe d'utilisateurs.

⚠ NOTA

Risque de sécurité – risque d'accès et/ou d'exploitation non autorisés

Les interfaces IP appartenant à un VLAN de gestion auxiliaire doivent être connectées à un réseau de confiance.

7.1.1.5 Types de port périphérie et de liaison

Chaque port peut être configuré comme port de périphérie ou de liaison.

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 de liaison font partie du réseau et acheminent le trafic pour tous les VLAN entre des commutateurs. Les ports de liaison 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 de liaison d'un autre port de liaison. Les ports de liaison 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 de liaison 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 "Liste Forbidden Ports (Page 166)".

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.

7.1.1.6 Règles d'entrée et de sortie

Les règles d'entrée et de sortie déterminent la façon dont 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 :

- Si une trame entrante n'est pas balisée ou a un VID de 0 (balisée avec une priorité), la trame est associée au PVID du port d'entrée
- Si une trame entrante est balisée, elle est autorisée à passer, tout en conservant son VID
- Les trames entrantes sont abandonnées uniquement si le filtrage à l'entrée est activé et que la trame est balisée avec un VID qui ne correspond à aucun VLAN dont le port d'entrée est membre

Les règles de sortie sont appliquées comme suit à toutes les trames lorsqu'elles sont transmises par le commutateur.

- Si la balisage PVID est activé, les trames sortantes sont balisées si elles sont associées au VLAN natif du port de sortie, indépendamment du type d'appartenance du port de sortie (edge ou trunk)
- Les trames sortantes sur une interface edge sont abandonnées si elles sont associées à un VLAN autre que le VLAN natif du port de sortie
- Les trames sortantes sur une interface trunk sont balisées si elles sont associées à un VLAN dont le port de sortie est membre

7.1.1.7 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 "Ajout d'un VLAN statique (Page 176)".

7.1.1.8 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)

7.1.1.9 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 doit 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 compatible GVRP (par ex. un PC ou un appareil électronique intelligent) configurée pour un VID spécifique peut être connectée à un trunk sur un commutateur compatible GVRP et faire automatiquement partie du VLAN souhaité.

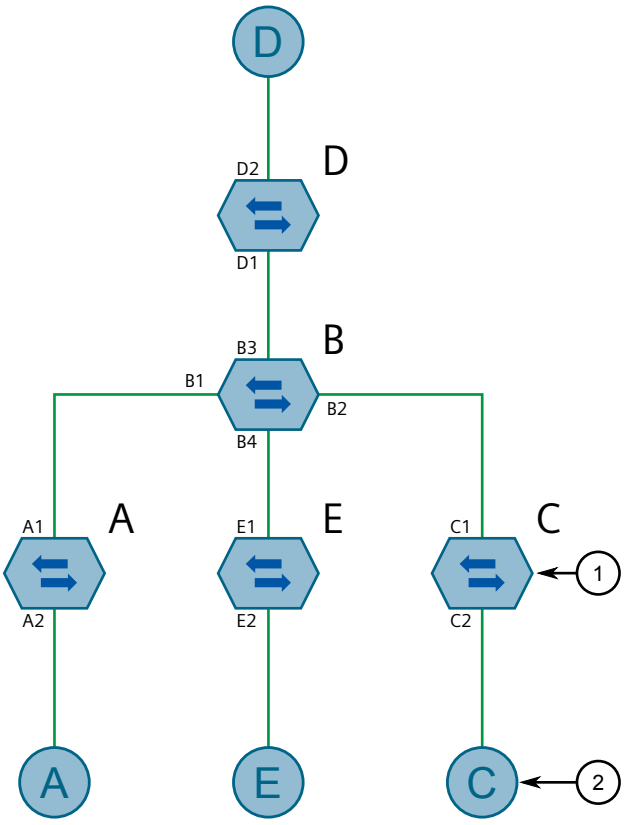
Lorsqu'un commutateur envoie des BPDU (bridge protocol data units) de tous les ports compatibles GVRP, les BPDU GVRP annoncent tous les VLAN connus de ce

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 compatibles 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 :



① Commutateur
② Nœud terminal

Figure 7.1 Utilisation de GVRP

- 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 "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".

7.1.1.10 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 de s'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 "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".

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.

7.1.1.11 QinQ

QinQ, également appelé VLAN empilés, pontage de ports, 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 de la trame (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 donc 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.

Le fournisseur de services supprime la trame sortante du VID externe, laissant la trame avec sa balise d'ID VLAN originale. Ces trames sont ensuite transmises aux VLAN appropriés.

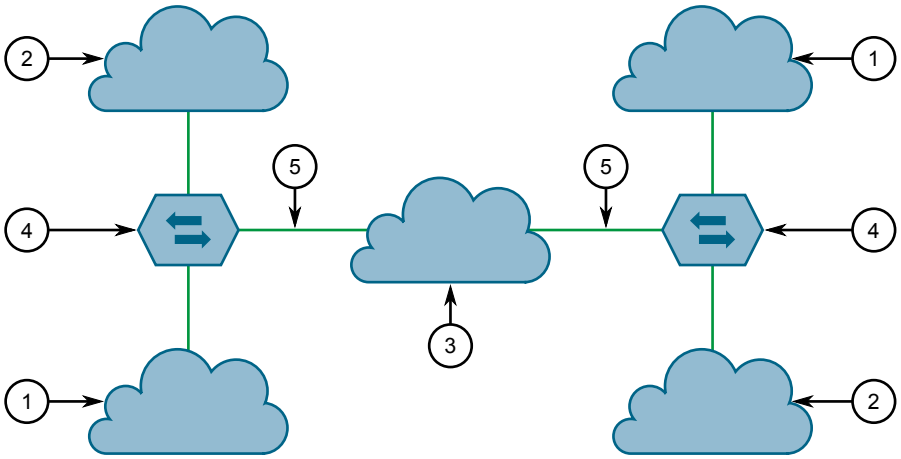
La figure suivante montre un exemple de flux de trafic avec QinQ.

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.



① Client 1 (PVID est X)
② Client 2 (PVID est Y)
③ Infrastructure du prestataire de services de réseau
④ Commutateur
⑤ QinQ

Figure 7.2 Utilisation de QinQ

Remarque
Selon le matériel installé, certains modèles de commutateur permettent uniquement la configuration d'un port de 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.

7.1.1.12 Avantages du VLAN

Vous trouverez ci-après quelques avantages offerts par les VLAN.

Isolation du domaine de trafic

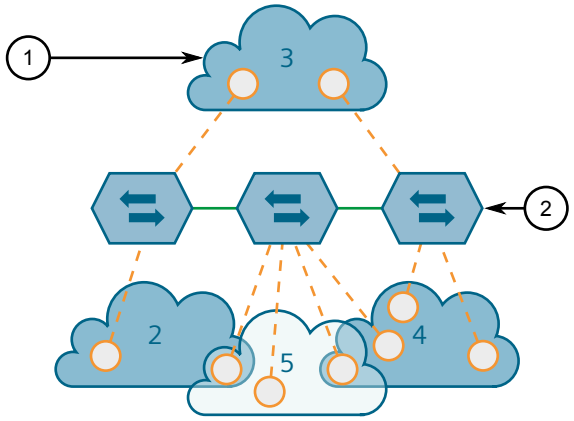
Les VLAN sont le plus souvent utilisés pour leur capacité à réduire les flux de trafic entre des groupes d'appareils.

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 des 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.



① VLAN
② Commutateur

Figure 7.3 VLAN multiples se chevauchant

Commodité administrative

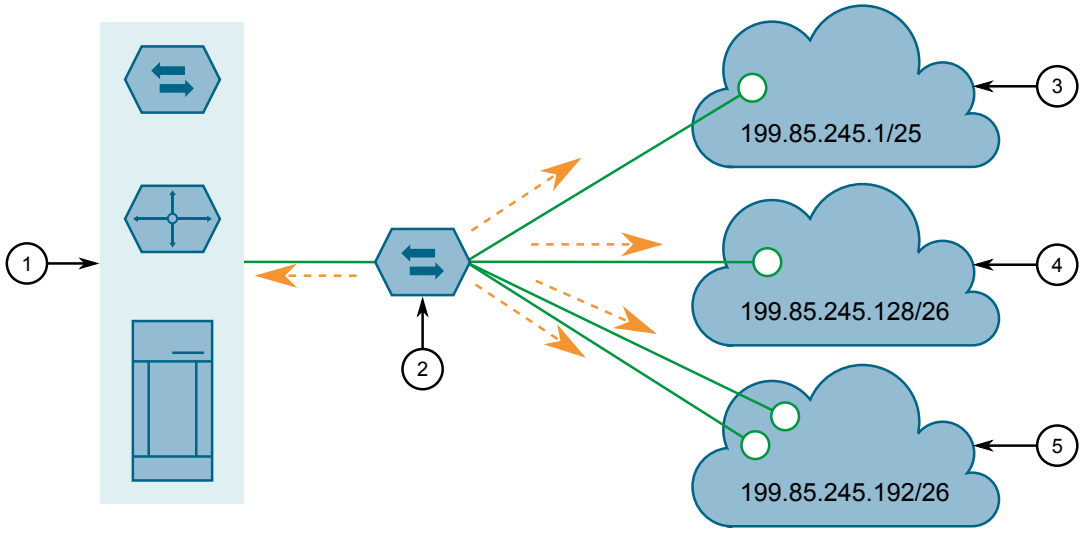
Les VLAN permettent un traitement des déplacements d'équipements par reconfiguration logicielle et non par gestion des câbles physiques. Lorsque l'emplacement physique d'un hôte est modifié, son point de connexion est souvent également modifié. Avec des VLAN, l'appartenance de l'hôte au VLAN et la priorité 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.



① Serveur, routeur ou commutateur de couche 3
② Commutateur
③ VLAN 2
④ VLAN 3
⑤ VLAN 4

Figure 7.4 Communications inter-VLAN

7.1.2 Affichage d'une liste de VLAN

Pour afficher une liste de tous les VLAN, qu'ils aient été créés de manière statique ou implicite, accédez à ***Virtual LANs » View VLAN Summary***. Le tableau **VLAN Summary** s'affiche.

Si aucun VLAN n'est répertorié, ajoutez des VLAN statiques en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".

7.1.3 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.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`VLAN-aware`	**Synopsis :** [No | Yes] **Par défaut :** Yes Sélectionnez un mode de fonctionnement compatible ou non-compatible VLAN.

Paramètre	Description
`Ingress Filtering`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Active ou désactive le filtrage à l'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 à l'entrée n'a pas d'effet lorsque des ports sont en mode non-compatible 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 lorsque QinQ est activé. Les trames entrant dans un port QinQ VLAN sont identifiées comme VLAN externe balisé 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**.

7.1.4 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.
2. Sélectionnez un port. Le formulaire **Port VLAN Parameters** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port(s)`	**Synopsis :** Any combination of numbers valid for this parameter Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).

Paramètre	Description
`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 : • `Périphérie`– Le port est uniquement membre d'un VLAN (son VLAN natif spécifié par le paramètre PVID). • `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 à d'autres ports PVLANedge dans le 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 de commutateur en mode QinQ à la fois.
`PVID`	**Synopsis :** Un entier compris entre 1 et 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 de 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.
`PVID Format`	**Synopsis :** [Untagged | Tagged] **Par défaut :** Untagged Spécifie si les trames transmises depuis le port vers son VLAN natif (spécifié par le paramètre**PVID**) sont balisées ou non balisées.

Paramètre	Description
	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 : • `Adv&Learn`– Le port déclare tous les VLAN existants dans le commutateur (configurés ou appris) et peut apprendre des VLAN de manière dynamique. • `Adv Only`– Le port déclare tous les VLAN existants dans le commutateur (configurés ou appris) mais n'apprend aucun VLAN. • `Disabled`– Le port n'est capable d'aucun traitement GVRP. Seuls les ports Trunk sont compatibles GVRP.

4. Cliquez sur **Apply**.

7.1.5 Gestion de VLAN statiques

Cette section décrit la configuration et la gestion de VLAN statiques.

7.1.5.1 Affichage d'une liste de VLAN statiques

Pour afficher une liste de VLAN statiques, accédez à ***Virtual LANs » Configure Static VLANs***. Le tableau **Static VLANs** s'affiche.

Si aucun VLAN statique n'est répertorié, ajoutez le VLAN. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".

7.1.5.2 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.
2. Cliquez sur **InsertRecord**. Le formulaire **Static VLANs** s'affiche.

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 de multidiffusion sont transmis directement à tous les membres du VLAN. Si un membre quelconque du VLAN rejoint un groupe de multidiffusion, tous les membres du VLAN recevront le trafic de multidiffusion.

Paramètre	Description
`VID`	**Synopsis :** Un entier compris entre 1 et 4094 **Par défaut :** 1 L'identificateur de VLAN est utilisé pour identifier le VLAN dans les trames Ethernet balisées selon IEEE 802.1Q.
`VLAN Name`	**Synopsis :** Chaîne de 19 caractères Le nom de VLAN fournit une description de l'utilisation du VLAN (par exemple, Engineering VLAN).
`Forbidden Ports`	**Synopsis :** Any combination of numbers valid for this parameter ou [None] 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.
`DHCP`	**Synopsis :** [Off | On] **Par défaut :** Off Ce paramètre active ou désactive l'espionnage DHCP sur le VLAN.
`MSTI`	**Synopsis :** Un entier compris entre 0 et 16 **Par défaut :** 0 Ce paramètre est valide uniquement pour le Multiple Spanning Tree Protocol (MSTP) et n'a pas d'effet si le MSTP n'est pas utilisé. Le paramètre spécifie la Multiple Spanning Tree Instance (MSTI) sur laquelle le VLAN doit être mappé.
`Mirror VLAN`	**Synopsis :** [No | Yes] **Par défaut :** No Ce paramètre spécifie si ce VLAN transporte ou non le trafic mis en miroir pour une session de mise en miroir du trafic à distance (Remote Traffic Mirroring).

4. Cliquez sur **Apply**.

7.1.5.3 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.
2. Sélectionnez le VLAN statique dans le tableau. Le formulaire **Static VLANs** s'affiche.
3. Cliquez sur **Delete**.

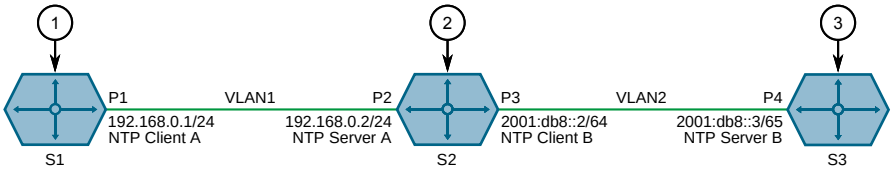
7.1.6 Exemple : configuration du support de gestion sur plusieurs VLAN

Cet exemple illustre la façon de déplacer le trafic de gestion sur plusieurs VLAN.

La topologie suivante décrit un scénario où l'heure système est synchronisée sur trois appareils RUGGEDCOM ROS et sur deux VLAN. Les paquets SNTP sont échangés entre les appareils RUGGEDCOM ROS dans un modèle client-serveur.

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① Commutateur S1
② Commutateur S2
③ Commutateur S3

Figure 7.5 Topologie – Support de gestion sur plusieurs VLAN

Procédez comme suit pour répliquer la topologie :

1. Configurez le commutateur S1 comme suit :
   a. Connectez le port P1 au port P2 sur le commutateur S2.
   b. Affectez l'adresse IP *192.168.0.1/24* au port P1.
   c. Configurez le port P1 comme interface de gestion. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   d. Affectez le port P1 à VLAN 1. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
   e. Définissez la source de l'heure du commutateur S1 sur *NTP SERVER*. Pour plus d'informations, voir "Configuration de la source de temps (Page 293)".
   f. Configurez le serveur NTP sur le commutateur S1 comme suit :

Serveur	Primary
IP Address	192.168.0.2
Update Period	1 min

   Pour plus d'informations, voir "Configuration de serveurs NTP (Page 295)".
2. Configurez le commutateur S2 comme suit :
   a. Connectez le port P3 au port P4 sur le commutateur S3.
   b. Affectez l'adresse IP *192.168.0.2/24* au port P2.
   c. Affectez l'adresse IP *2001:db8::2/64* au port P3.
   d. Configurez le port P2 comme interface de gestion auxiliaire. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   e. Configurez le port P3 comme interface non-gestion. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   f. Affectez le port P2 à VLAN 1. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
   g. Affectez le port P3 à VLAN 2. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
   h. Définissez la source de l'heure du commutateur S2 sur *NTP SERVER*. Pour plus d'informations, voir "Configuration de la source de temps (Page 293)".
   i. Configurez le serveur NTP sur le commutateur S2 comme suit :

Serveur	Primary
IP Address	2001:db8::3
Update Period	1 min

   Pour plus d'informations, voir "Configuration de serveurs NTP (Page 295)".

3. Configurez le commutateur S3 comme suit :
   a. Affectez l'adresse IP *2001:db8::3/64* au port P4.
   b. Configurez le port P4 comme interface non-gestion. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   c. Affectez le port P4 à VLAN 2. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
   d. Définissez la source de l'heure du commutateur S3 sur *LOCAL CLK*. Pour plus d'informations, voir "Configuration de la source de temps (Page 293)".
   e. Activez SNTP sur le commutateur S3. Pour plus d'informations, voir "Activation/désactivation du service NTP (Page 295)".
4. Vérifiez les points suivants :
   a. L'horloge locale du commutateur S1 est synchronisée avec l'horloge locale du commutateur S2. Pour plus d'informations, voir "Gestion de NTP (Page 294)".
   b. L'horloge locale du commutateur S2 *n'est pas* synchronisée avec l'horloge locale du commutateur S3. Pour plus d'informations, voir "Gestion de NTP (Page 294)".
   c. Le serveur SNTP sur le commutateur S2 n'est pas joignable depuis le serveur NTP (car VLAN 2 est un VLAN non-gestion). Pour plus d'informations, voir "Gestion de NTP (Page 294)".

7.2 Gestion des adresses MAC

Cette section décrit la manière de gérer des adresses MAC.

7.2.1 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.

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 d'autres appareils sur le réseau. Pour plus d'informations, voir "Configuration des options d'apprentissage d'adresses MAC (Page 181)".
2. Configurez l'adresse sur l'appareil en tant qu'adresse MAC statique. Pour plus d'informations, voir "Ajout d'une adresse MAC statique (Page 183)".

7.2.2 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 adresses individuelles sont supprimées 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.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Aging Time`	**Synopsis :** Un entier compris entre 15 et 800 **Par défaut :** 300 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 :** Yes 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**.

7.2.3 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.
2. Sélectionnez un port. Le formulaire **Flooding Options** s'affiche.

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

Paramètre	Description
`Port(s)`	**Synopsis :** Comma-separated list of ports Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).
`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**.

7.2.4 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.Il peut également être nécessaire de les configurer 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.

7.2.4.1 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.

Si aucune adresse MAC statique n'a été configurée, ajoutez des adresses en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'une adresse MAC statique (Page 183)".

7.2.4.2 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.
2. Cliquez sur **InsertRecord**. Le formulaire **Static MAC Addresses** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF 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-**-**-** désigne l'espace d'adresses MAC complet de RuggedCom. • 00-0A-DC-12-3*-** désigne la plage 00-0A-DC-12-30-00 à 00-0A-DC-12-3F-FF.
`VID`	**Synopsis :** Un entier compris entre 1 et 4094 ou [ANY] **Par défaut :** 1 Identificateur VLAN du VLAN sur la base duquel l'adresse MAC est exécutée. 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 :** 1/1 to maximum port number ou [Learn] **Par défaut :** Learn Saisissez le numéro de port dans lequel l'appareil avec cette adresse est située. 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'.
`Priority`	**Synopsis :** Un entier compris entre 0 et 7 ou [N/A] **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**.

7.2.4.3 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.
2. Sélectionnez l'adresse MAC dans le tableau. Le formulaire **Static MAC Addresses** s'affiche.
3. Cliquez sur **Delete**.

7.2.5 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.
2. Cliquez sur **Confirm**.

7.3 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).

7.3.1 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 spécifiques, les flux ou le trafic sont dirigés vers cet hôte ou retenus depuis celui-ci.

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.

⚠ NOTA

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

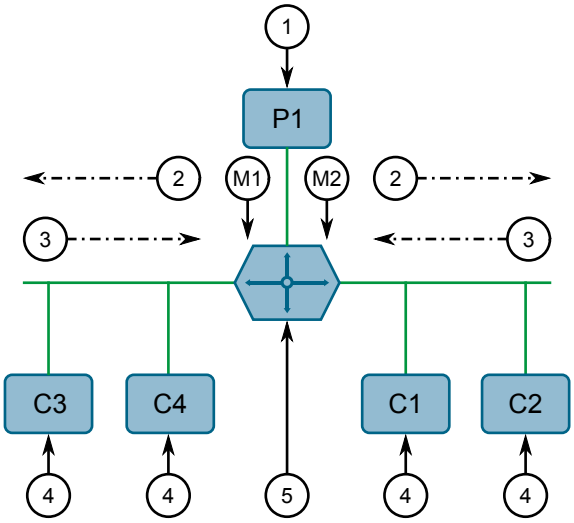
Ces adresses sont réservées pour les protocoles d'acheminement et IEEE 1588. Si un rapport d'appartenance IGMP contient l'une de ces adresses, le rapport est transmis par le commutateur sans apprentissage de l'hôte.

7.3.1.1 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.



① Producteur
② Demande d'appartenance
③ Rapports d'appartenance
④ Consommateur
⑤ Routeur de multidiffusion

Figure 7.6 Exemple - Fonctionnement d'IGMP

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 des 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 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.

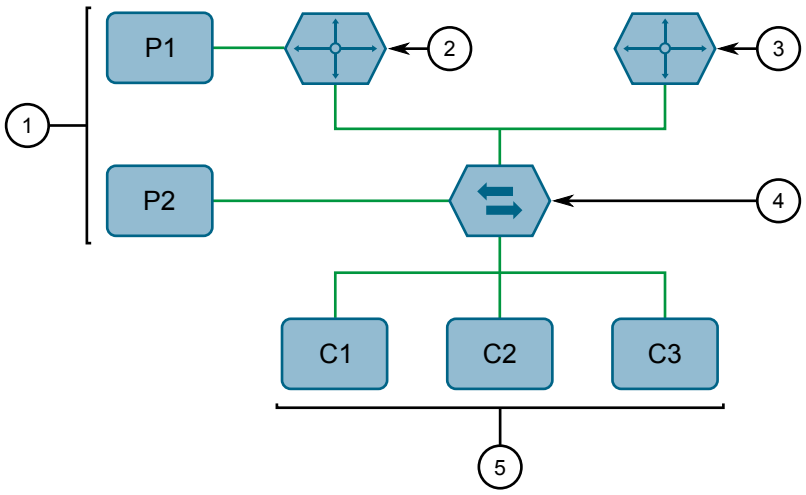
Si RSTP détecte une modification dans la topologie de réseau, IGMP prend des mesures pour éviter la perte de la connectivité de multidiffusion et réduire le temps de convergence du réseau :

- 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 lui-même.



① Producteur
② Routeur de multidiffusion 1
③ Routeur de multidiffusion 2
④ Commutateur
⑤ Hôte

Figure 7.7 Exemple - Fonctionnement combiné du routeur et du commutateur IGM

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 au routeur de multidiffusion 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.

7.3.1.2 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 **IGMP Group Membership** s'affiche.

Ce tableau fournit les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`VID`	**Synopsis :** Un entier compris entre 0 et 65535 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
`Group`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 Adresse du groupe de multidiffusion.
`Ver`	**Synopsis :** [v3 | v2 | v1] Spécifie la version IGMP du groupe de multidiffusion appris.
`Reporter`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 Spécifie l'adresse IP source qui rapporte l'inscription au groupe de multidiffusion.
`Age`	**Synopsis :** Un entier compris entre 0 et 7210 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 "Configuration d'IGMP (Page 191)".

7.3.1.3 Affichage d'informations de transmission pour des groupes de multidiffusion

Les informations de transmission en multidiffusion pour chaque combinaison de source, groupe et VLAN apprise par RUGGEDCOM ROS sont enregistrées dans le tableau IGMP Multicast Forwarding.

Pour afficher le tableau IGMP Multicast Forwarding, accédez à ***Multicast Filtering » View IGMP Multicast Forwarding***. Le tableau **IGMP Multicast Forwarding** s'affiche.

Ce tableau fournit les informations suivantes :

Paramètre	Description
`VID`	**Synopsis :** Un entier compris entre 0 et 65535 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
`Group`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 Adresse du groupe de multidiffusion.
`Source`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 ou [*] Adresse source. * signifie toutes les adresses source possibles.

Paramètre	Description
`Joined Ports`	**Synopsis :** Comma-separated list of ports Tous les ports recevant actuellement le trafic de multidiffusion pour le groupe de multidiffusion spécifié.
`Router Ports`	**Synopsis :** Comma-separated list of ports 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 de 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 "Configuration d'IGMP (Page 191)".

7.3.1.4 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 "Gestion de VLAN statiques (Page 176)".
2. Accédez à ***Multicast Filtering » Configure IGMP Parameters***. Le formulaire **IGMP Parameters** s'affiche.
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 : • `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,

Paramètre	Description
	et le trafic est réduit en fonction de l'adresse de groupe de multidiffusion uniquement.
`Query Interval`	**Synopsis :** Un entier compris entre 10 et 3600 **Par défaut :** 60 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 :** Comma-separated list of ports **Par défaut :** None Ce paramètre spécifie les ports se connectant à des routeurs de 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 de multidiffusion.
`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**.

7.3.2 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.

7.3.2.1 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 GMRP

GMRP étant une application de GARP, les transactions s'effectuent à l'aide du protocole GARP. GMRP définit les deux types d'attribut 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 :

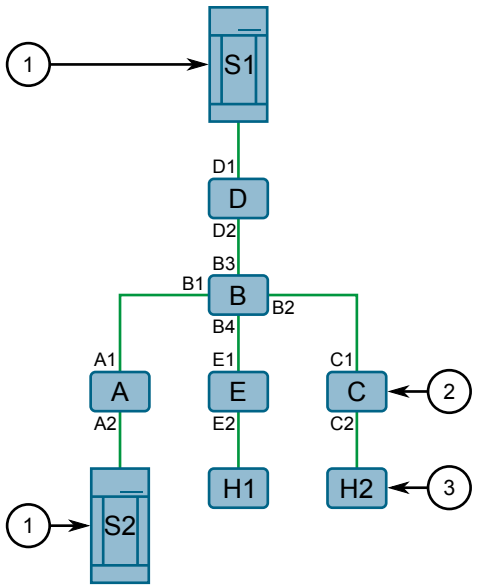
- transmettant tout le trafic de groupe de multidiffusion dans le VLAN ou
- transmettant tout le trafic inconnu (groupes de multidiffusion) pour lequel aucun membre n'est enregistré dans l'appareil dans un VLAN.

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.

Établissement d'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.



① Source de multidiffusion
② Commutateur
③ Hôte de multidiffusion

Figure 7.8 Exemple - Établissement d'une appartenance à un groupe avec GMRP

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.

7.3.2.2 Affichage d'un résumé de groupes de multidiffusion

Pour afficher un résumé de tous les groupes de multidiffusion, accédez à ***Multicast Filtering » View Multicast Group Summary***. Le tableau **Multicast Group Summary** s'affiche.

Ce tableau fournit les informations suivantes :

Paramètre	Description
`VID`	**Synopsis :** Un entier compris entre 0 et 65535 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF Adresse MAC de groupe de multidiffusion.
`Static Ports`	**Synopsis :** Any combination of numbers valid for this parameter 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.

Paramètre	Description
`GMRP Dynamic Ports`	**Synopsis :** Any combination of numbers valid for this parameter Ports ayant joint ce groupe dynamiquement via une application GMRP vers lesquels le trafic du groupe de multidiffusion est transmis.

7.3.2.3 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.
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 :** Un entier compris entre 600 et 300000 **Par défaut :** 4000 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**.

7.3.2.4 Configuration de GMRP pour des ports Ethernet spécifiques

Procédez comme suit pour configurer GMRP pour un port Ethernet spécifique :

1. Assurez-vous que les réglages globaux pour GMRP ont été configurés. Pour plus d'informations, voir "Configuration globale du GMRP (Page 196)".

2. Accédez à ***Multicast Filtering » Configure Port GMRP Parameters***. Le tableau **Port GMRP Parameters** s'affiche.
3. Sélectionnez un port Ethernet. Le formulaire **Port GMRP Parameters** s'affiche.
4. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port(s)`	**Synopsis :** Any combination of numbers valid for this parameter Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).
`GMRP`	**Synopsis :** [Disabled | Adv Only | Adv&Learn] **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. • `Adv Only`– Le port déclare toutes les adresses MCAST existantes dans le commutateur (configuré ou appris) mais n'apprend aucune adresse MACST. • `Adv&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**.

7.3.2.5 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.

Si aucun groupe de multidiffusion statique n'est répertorié, ajoutez le groupe. Pour plus d'informations, voir "Ajout d'un groupe multidiffusion statique (Page 197)".

7.3.2.6 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.
2. Cliquez sur **InsertRecord**. Le formulaire **Static Multicast Groups** s'affiche.

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

Paramètre	Description
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF **Par défaut :** 00-00-00-00-00-00 Adresse MAC de groupe de multidiffusion.
`VID`	**Synopsis :** Un entier compris entre 1 et 4094 **Par défaut :** 1 Identificateur VLAN du VLAN sur la base duquel le groupe de multidiffusion est exécuté.
`Priority`	**Synopsis :** Un entier compris entre 0 et 7 ou [N/A] **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 :** Any combination of numbers valid for this parameter **Par défaut :** None Une liste de ports séparés par des virgules vers lesquels le trafic du groupe de multidiffusion est transmis. Si un port fait partie d'un Link Aggregation Group (LAG), ou port trunk, spécifiez tous les ports du LAG.

4. Cliquez sur **Apply**.

7.3.2.7 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.
2. Sélectionnez le groupe dans le tableau. Le formulaire **Static Multicast Groups** s'affiche.
3. Cliquez sur **Delete**.

8 Layer 3 (couche 3)

Ce chapitre décrit les fonctionnalités Layer 3 (couche 3) ou couche réseau de RUGGEDCOM ROS.

8.1 Gestion de Layer 3 Switching (commutation de couche 3)

Cette section décrit la manière de gérer Layer 3 switching.

Remarque
Layer 3 Switching prend en charge uniquement les adresses IPv4 (pas les adresses IPv6).

Remarque
Layer 3 Switching prend en charge uniquement le trafic monodiffusion. Layer 3 Switching pour le trafic de multidiffusion et de diffusion n'est pas prise en charge.

8.1.1 Comprendre la commutation de couche 3 (Layer 3 Switching)

La commutation traditionnelle s'effectue au niveau de la couche 2 du modèle OSI, où les paquets sont envoyés à un port de commutateur spécifique, sur la base des adresses MAC de destination et des VLAN. Le routage s'effectue au niveau de la couche 3, où les paquets sont envoyés à une adresse IP du saut suivant, sur la base de l'adresse IP de destination.

RUGGEDCOM ROS prend en charge la configuration des règles Layer 3 Switching, permettant ainsi la commutation du trafic IP entre deux VLAN existants via le matériel de l'appareil.

Cette section décrit certains concepts importants de la mise en œuvre de la commutation de couche 3 (Layer 3 Switching) dans RUGGEDCOM ROS.

8.1.1.1 Tableau Forwarding Layer 3 Switch

Pour router un paquet avec une adresse IP de destination spécifique, un appareil a besoin des informations suivantes :

- **Interface de sortie (sous-réseau)**

  Cette information est stockée dans la table de routage de l'appareil.

  Remarque
  Dans un segment de réseau commuté de couche 2, un VLAN constitue un sous-réseau IP.

- **Prochain saut ou adresse Media Access Control (MAC) de la passerelle**

  Ces informations sont stockées dans un tableau ARP spécifique à la commutation de couche 3 (Layer 3 switching).

  Remarque
  Si le prochain saut est vers le sous-réseau cible lui-même, l'adresse MAC de l'hôte cible est requise.

La commutation de couche 3 (Layer 3 switching) traduit ces informations de routage en règles Layer 3 switching. Ces règles sont dénommées *Layer 3 Switch Forwarding Information Base (FIB)* ou *Layer 3 Switch Forwarding Table*. Une règle Layer 3 switching définit la façon de commuter un flux de trafic spécifique.

L'Application-Specific Integrated Circuits (ASICs) Layer 3 switching stocke les règles Layer 3 switching dans des tableaux Ternary Content Addressable Memory (TCAM) pour les hôtes et les sous-réseaux. Les règles Layer 3 switching peuvent être configurées de façon statique ou apprises de façon dynamique (ou *auto-apprises*).

Remarque
Les règles Layer 3 switching peuvent être uniquement apprises de façon dynamique pour les hôtes voisins. Les règles doivent être configurées de façon statique pour les hôtes et les sous-réseaux distants.

Remarque
Le nombre maximal de règles Layer 3 switching est 288, y compris 256 pour les hôtes et 32 pour les sous-réseaux.

8.1.1.2 Règles statiques Layer 3 Switching (commutation de couche 3)

Lors de la création d'une route statique dans la gestion de commutateur, l'accélération matérielle peut être configurée de manière explicite. Si l'accélération matérielle est sélectionnée, une règle Layer 3 Switching est installée dans TCAM ASIC et n'expire jamais.

Remarque
Seuls les flux de trafic ICMP, TCP et UDP sont accélérés par l'IP/Layer 3 Switching ASIC.

Remarque
Pour utiliser les règles Layer 3 Switching configurées de façon statique, le transfert IP peut être activé ou désactivé. Pour plus d'informations sur la configuration du transfert IP, voir "Configuration des services IP (Page 102)".

8.1.1.3 Apprentissage dynamique des règles Layer 3 Switching (commutation de couche 3)

Pour les routes statiques sans accélération matérielle ou pour les routes dynamiques, les règles Layer 3 Switching (commutation de couche 3) peuvent être apprises de façon dynamique en se fondant sur des décisions de routeur basées logiciel.

Après un routage réussi d'une certaine quantité de trafic avec le même flux, le Layer 3 Switching ASIC commence la commutation du reste des paquets appartenant au même flux. Un flux est un trafic unidirectionnel entre deux hôtes. Par exemple, le trafic entre des ports d'un hôte vers un autre est considéré comme un flux. Le trafic dans la direction opposée entre les mêmes ports est considéré comme un autre flux.

RUGGEDCOM ROS prend en charge la méthode orientée hôte auto-apprenante, où l'appareil utilise les adresses IP source et de destination pour identifier un flux de trafic.

Chaque flux représente une règle.

Le commutateur de couche 3 surveille en permanence l'activité (si le trafic est présent) pour les règles apprises de façon dynamique. Pour cette raison, les règles apprises de façon dynamique peuvent être supprimées après un temps configurable d'inactivité.

8.1.1.4 Interaction entre IP Forwarding et Layer 3 Switching

Pour utiliser les règles statiques Layer 3 Switching, IP forwarding peut être activé ou désactivé. Cependant, pour utiliser les règles Layer 3 Switching apprises de façon dynamique, IP forwarding doit être désactivé. Pour plus d'informations sur la configuration d'IP Forwarding, voir "Configuration des services IP (Page 102)".

Ce qui suit montre l'interaction d'IP forwarding avec Layer 3 switching dans RUGGEDCOM ROS.

IP Forwarding	L3 Switching désactivé	L3 Switching statique	L3 Switching dynamique
Désactivé	Les deux fonctionnalités sont désactivées	Layer 3 Switching statique	Impossible
Activé	Pas d'accélération matérielle	Layer 3 Switching statique	Layer 3 Switching statique et dynamique

8.1.1.5 Tableau ARP Layer 3 Switch

Un routeur a besoin de connaître l'adresse MAC de l'hôte cible ou de la passerelle du prochain saut pour transmettre un paquet sur un autre sous-réseau. À cette fin, le logiciel gère un tableau Address Resolution Protocol (ARP) qui fait correspondre les adresses IP avec les adresses MAC. Les mêmes informations sont aussi requises par Layer 3 switching ASIC en cas de commutation de paquets IP entre des sous-réseaux.

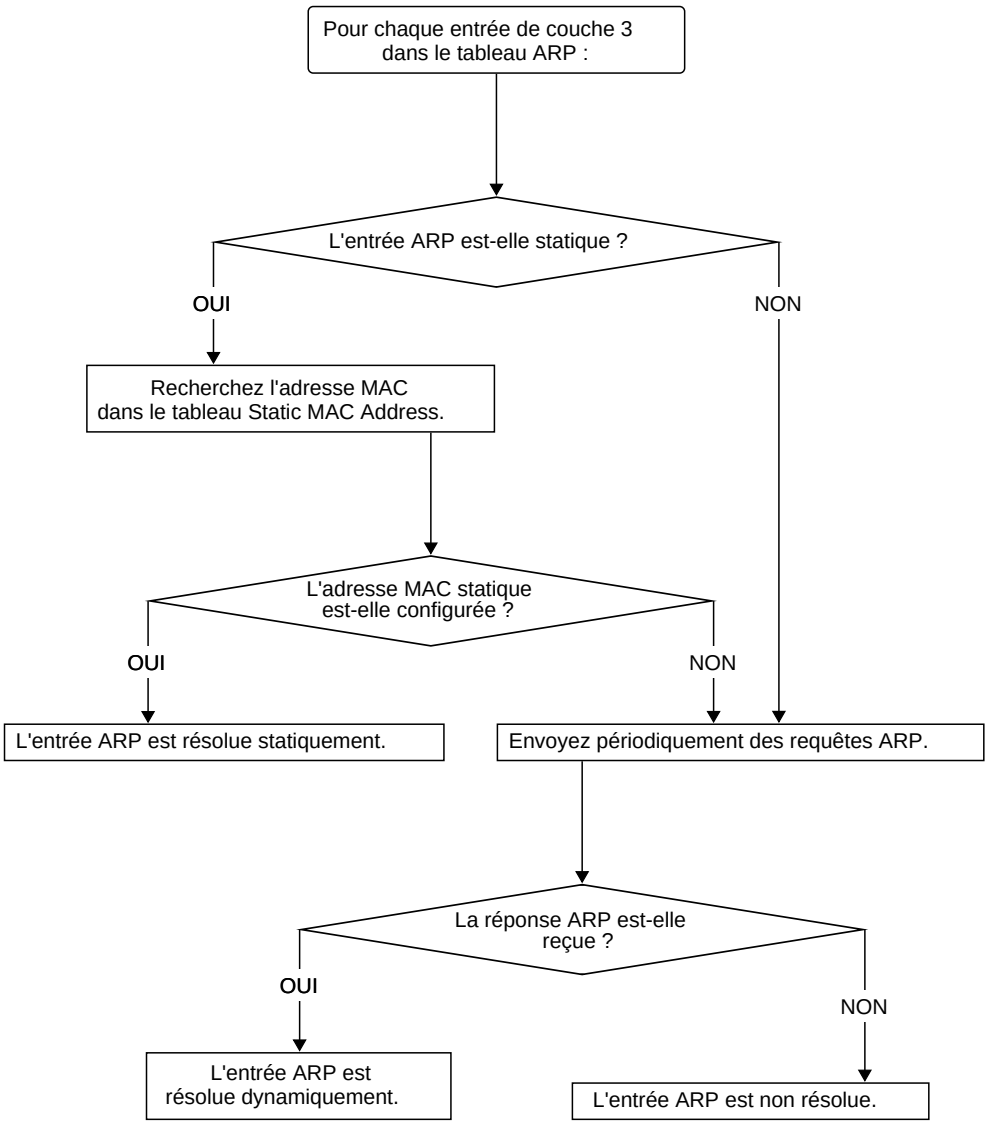
Remarque
Les entrées ARP peuvent être configurées de façon statique et résolues si les adresses MAC auxquelles elles correspondent sont configurées dans le **Static MAC Address Table**. Sinon, les entrées ARP sont résolues de façon dynamique toutes les 60 secondes (s).

L'adresse MAC de destination ou de passerelle est généralement obtenue par ARP. Cependant, les entrées ARP peuvent aussi être configurées de façon statique dans le commutateur de couche 3 (Layer 3 Switch), afin qu'elles n'expirent pas. Lors de la configuration d'une entrée ARP statique, si aucune valeur n'est entrée pour le paramètre d'adresse MAC, l'adresse est automatiquement résolue via ARP, puis enregistrée de façon statique. Elle est préservée au cours des redémarrages de l'appareil.

Si aucune entrée ARP statique n'est configurée pour une cible spécifique, une entrée ARP dynamique est créée et l'adresse MAC de destination sera résolue automatiquement.

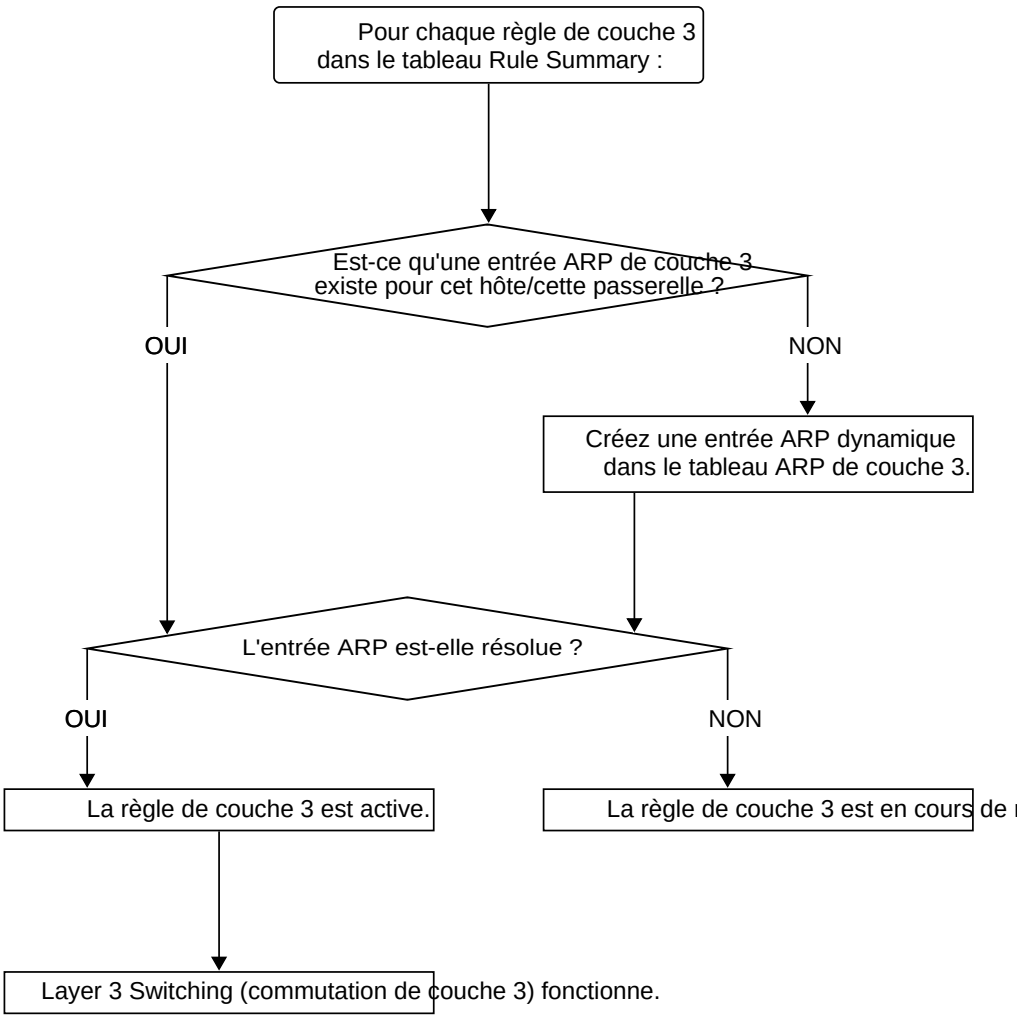
Comportement de résolution ARP Layer 3

L'organigramme suivant montre la façon dont les entrées ARP sont résolues dans RUGGEDCOM ROS.



Comportement de résolution de règle Layer 3 Switching

L'organigramme suivant montre la façon dont les règles Layer 3 switching sont résolues dans RUGGEDCOM ROS.



8.1.1.6 Interfaces routables Layer 3 Switch

RUGGEDCOM ROS permet la configuration d'un maximum de 255 interfaces (VLANs). Pour rendre une interface routable pour le trafic IPv4 en monodiffusion, une adresse IPv4 doit être configurée de façon statique ou affectée via DHCP à l'interface. Pour plus d'informations, voir "Gestion d'interfaces IP (Page 96)".

8.1.2 Configuration de la commutation de couche 3 (Layer 3 Switching)

Procédez comme suit pour configurer Layer 3 Switching :

Remarque
Évitez de configurer des Link Aggregation Groups (LAG) lorsque Layer 3 Switching est activée. Pour plus d'informations, voir "Gestion des groupes d'agrégation de liens (Page 258)".

1. Ajoutez les VLAN comme requis. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".
2. Affectez des adresses IP aux VLAN configurés. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
3. Affectez les ports souhaités aux VLAN configurés. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
4. Configurez le mode monodiffusion et le délai de vieillissement. Pour plus d'informations, voir "Configuration des options de commutation de couche 3 (Layer 3 Switching) (Page 205)".
5. Si le mode monodiffusion statique est sélectionné, ajoutez des adresses IP de destination, puis sautez les passerelles selon les besoins. Pour plus d'informations, voir "Gestion des règles de monodiffusion statiques (Page 206)".
6. Si le mode monodiffusion statique est sélectionné, ajoutez des entrées de tableau ARP en fonction des besoins. Pour plus d'informations, voir "Gestion des entrées de tableau Static ARP (Page 207)".
7. Testez la configuration en envoyant du trafic et vérifiez les points suivants :
   a. Les entrées ARP sont résolues dans le tableau **ARP Table**. Pour plus d'informations, voir "Affichage d'une liste d'entrées de tableau ARP (Page 207)".
   b. Les règles sont actives dans le tableau **Rule Summary Table**. Pour plus d'informations, voir "Affichage des règles de routage (Page 209)".
   c. Le trafic est envoyé et reçu. Pour plus d'informations, voir "Affichage de statistiques pour des ports Ethernet spécifiques (Page 70)".

Pour des exemples de configuration, voir "Exemple : configuration de la commutation de couche 3 (Layer 3 Switching) (Page 210)" et "Exemple : configuration de Layer 3 Switching à l'aide de plusieurs commutateurs (Page 212)".

8.1.3 Configuration des options de commutation de couche 3 (Layer 3 Switching)

Procédez comme suit pour configurer les options Layer 3 Switching :

1. Accédez à ***Layer 3 Switching » Configure Switch Options***. Le formulaire **Switch Options** s'affiche.

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

Paramètre	Description
`Unicast Mode`	**Synopsis :** [Disabled | Static | Auto] **Par défaut :** Disabled Disabled - Layer 3 switching (commutation de couche 3) est désactivé. Static - Seules les règles Layer 3 switching définies de façon statique sont utilisées. Auto - Les règles Layer 3 switching configurées de façon statique et celles apprises de façon dynamique sont utilisées. Dans ce mode, l'accélération matérielle de routage maximale est utilisée.
`Aging Time`	**Synopsis :** Un entier compris entre 16 et 600 **Par défaut :** 32 Ce paramètre configure le temps durant lequel une règle apprise de façon dynamique pour un flux de trafic, devenue inactive est conservée avant d'être supprimée du tableau de transmission Layer 3 Switch.

3. Cliquez sur **Apply**.

8.1.4 Gestion des règles de monodiffusion statiques

Cette section décrit la manière de gérer les règles de monodiffusion statiques.

8.1.4.1 Affichage des règles de monodiffusion statiques

Pour afficher une liste des entrées de règle de monodiffucion statiques, accédez à ***Layer 3 Switching » Configure Static Unicast Rules***. Si des entrées de tableau ont été configurées, le tableau **Static Unicast Rules** s'affiche.

Les règles de monodiffusion statiques peuvent être configurées comme requis. Pour plus d'informations sur l'ajout de règles de monodiffusion statiques, voir "Ajout d'une règle de monodiffusion statique (Page 206)".

8.1.4.2 Ajout d'une règle de monodiffusion statique

Procédez comme suit pour ajouter une règle de monodiffusion statique :

1. Accédez à ***Layer 3 Switching » Configure Static Unicast Rules***. Le tableau **Static Unicast Rules Table** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **Static Unicast Rules** s'affiche.

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

Paramètre	Description
`Destination`	**Synopsis :** ###.###.###.###/## where ### ranges from 0 to 255 and ## ranges from 0 to 32 **Par défaut :** ANY Adresse IP de destination ou sous-réseau. Pour être conforme à la règle, l'adresse IP de destination du paquet entrant doit appartenir au sous-réseau.
`Gateway`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 L'adresse IP du prochain saut à laquelle les paquets de monodiffusion correspondants vont être transmis. **Remarque** Si la**destination**est un voisin directement connecté, aucune valeur ne doit être fournie pour le**paramètre**de passerelle.

4. Cliquez sur **Apply**.

8.1.4.3 Suppression d'une règle de monodiffusion statique

Procédez comme suit pour supprimer une règle de monodiffusion statique :

1. Accédez à ***Layer 3 Switching » Configure Static Unicast Rules***. Le tableau **Static Unicast Rules** s'affiche.
2. Sélectionnez l'enregistrement à supprimer. Le formulaire **Static Unicast Rules** s'affiche.
3. Cliquez sur **Delete**.

8.1.5 Gestion des entrées de tableau Static ARP

Cette section décrit la manière de gérer les entrées de tableau Static ARP.

8.1.5.1 Affichage d'une liste d'entrées de tableau ARP

Pour afficher une liste d'entrées de tableau ARP Layer 3 Switching, accédez à ***Layer 3 Switching » Configure/View ARP Table***. Si des entrées de tableau ont été configurées, le tableau **ARP Table** s'affiche.

Lorsque des règles de monodiffusion sont configurées, le tableau ARP Layer 3 Switching est renseigné à mesure que les entrées ARP sont apprises de façon dynamique. Des entrées de tableau ARP statiques peuvent aussi être ajoutées selon les besoins. Pour plus d'informations sur l'ajout d'entrées de tableau ARP statiques, voir "Ajout d'une entrée de tableau Static ARP (Page 208)".

8.1.5.2 Ajout d'une entrée de tableau Static ARP

Procédez comme suit pour ajouter une entrée de tableau Static ARP :

1. Accédez à ***Layer 3 Switching » Configure/View ARP Table***. Le formulaire **ARP Table** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **ARP Table** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`IP Address`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 Adresse IP de l'appareil réseau décrit par l'entrée.
`VID`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** N/A Identificateur VLAN du VLAN sur la base duquel l'adresse MAC est exécutée.
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF **Par défaut :** 00-00-00-00-00-00 Adresse MAC de l'appareil réseau spécifiée par l'adresse IP.
`Static`	**Synopsis :** [True | False] **Par défaut :** True Indique si l'entrée est statique ou dynamique. Les entrées statiques sont configurées comme résultat de l'activité de gestion. Les entrées dynamiques sont automatiquement apprises par l'appareil et peuvent être désapprises.
`Status`	**Synopsis :** [Unresolved | Resolved] État de résolution d'entrée ARP : Resolved - La paire d'adresses MAC-IP est résolue et opérationnelle. Unresolved - L'appareil n'a pas résolu la paire d'adresses MAC-IP et continue d'envoyer périodiquement des requêtes ARP.

4. Cliquez sur **Apply**.

8.1.5.3 Suppression d'une entrée de tableau Static ARP

Procédez comme suit pour supprimer une entrée de tableau Static ARP :

1. Accédez à ***Layer 3 Switching » Configure/View ARP Table***. Le formulaire **ARP Table** s'affiche.
2. Sélectionnez l'enregistrement à supprimer. Le formulaire **ARP Table** s'affiche.
3. Cliquez sur **Delete**.

8.1.6 Affichage des règles de routage

Pour afficher une liste des règles de routage, accédez à ***Layer 3 Switching » View Rule Summary***. Si des règles de monodiffusion statiques ou dynamiques sont configurées, le tableau **Rule Summary Table** s'affiche.

Ce tableau fournit les informations suivantes :

Paramètre	Description
`Destination`	**Synopsis :** Chaîne de 20 caractères Adresse IP de destination ou sous-réseau. Pour être conforme à la règle, l'adresse IP de destination du paquet entrant doit appartenir au sous-réseau.
`Out-VLAN(s)`	**Synopsis :** Comma separated list of up to 2 numbers ranging from 1 to 4095 VLAN(s) de sortie. Les paquets monodiffusion et multidiffusion correspondants sont envoyés à un ou plusieurs VLAN.
`Gateway`	**Synopsis :** ###.###.###.### where ### ranges from 0 to 255 Adresse IP du prochain saut à laquelle les paquets de monodiffusion correspondants sont transmis.
`Static`	**Synopsis :** [True | False] Indique si la règle est statique ou dynamique. Les règles statiques sont configurées comme résultat de l'activité de gestion. Les règles dynamiques sont automatiquement apprises par l'appareil et peuvent être désapprises en fonction du temps de vieillissement.
`Status`	**Synopsis :** [Active | Resolving] Indique si la règle est actuellement opérationnelle ou non : Active - La règle est pleinement opérationnelle et peut être appliquée, donc l'accélération matérielle est effectuée. Resolving - La règle n'est pas opérationnelle en raison de la non-résolution de certaines informations, comme l'adresse MAC ARP ou de la passerelle dans le tableau des adresses MAC. L'accélération matérielle n'est pas effectuée.

8.1.7 Suppression de règles de routage de matériel dynamiques

La suppression de règles de routage de matériel dynamiques supprime toutes les règles apprises de façon dynamique du tableau **Layer 3 Switch Forwarding Table**.

Remarque
Seules les règles dynamiques peuvent être supprimées. Les règles dynamiques configurées dans le tableau **Layer 3 Switch Forwarding Table** ne vieillissent

jamais. Pour plus d'informations sur l'activation de l'accélération matérielle, voir "Comprendre la commutation de couche 3 (Layer 3 Switching) (Page 199)".

Pour supprimer les règles de routage de matériel dynamiques, procédez comme suit :

1. Accédez à ***Layer 3 Switching*** et cliquez sur **Flush Learned Rules**. Le formulaire **Flush Learned Rules** s'affiche.
2. Cliquez sur **Confirm**.

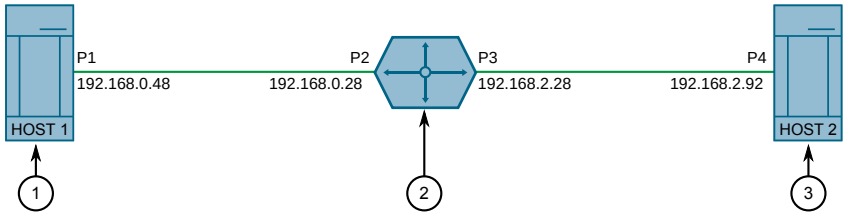
8.1.8 Exemple : configuration de la commutation de couche 3 (Layer 3 Switching)

Cet exemple illustre la configuration de la commutation de couche 3 (Layer 3 Switching)

La topologie suivante décrit un scénario où deux hôtes sur des réseaux distincts sont connectés à un appareil RUGGEDCOM ROS configuré comme commutateur de couche 3. Un trafic bidirectionnel est envoyé entre les deux hôtes via RUGGEDCOM ROS.

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① Hôte 1
② Appareil RUGGEDCOM ROS
③ Hôte 2

Figure 8.1 Topologie de base de la commutation de couche 3 (Layer 3 Switching)

Procédez comme suit pour répliquer la topologie :

Remarque
L'hôte 1 et l'hôte 2 peuvent être un appareil de couche 2 ou un PC. Pour obtenir des instructions de configuration spécifiques, consultez la documentation OEM.

1. Configurez l'hôte 1 par la topologie comme suit :
   a. Connectez P1 à P2 de l'appareil RUGGEDCOM ROS.
   b. Affectez une adresse IP *192.168.0.48* à l'interface P1.
   c. Définissez la passerelle par défaut sur *192.168.0.28*.

2. Configurez l'hôte 2 par la topologie comme suit :
   a. Connectez P4 à P3 de l'appareil RUGGEDCOM ROS.
   b. Affecter une adresse IP *192.168.2.92* à l'interface P4.
   c. Définissez la passerelle par défaut sur *192.168.2.28*.
3. Configurez l'appareil RUGGEDCOM ROS comme commutateur de couche 3 :
   a. Ajoutez VLAN 1 et VLAN 2. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".
   b. Affectez une adresse IP *192.168.0.28* à VLAN 1 et l'adresse IP *192.168.2.28* à VLAN 2. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   c. Affectez P2 à VLAN1 et P3 à VLAN2. Consultez "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)" pour plus d'informations.
   d. Activez le mode monodiffusion. Pour plus d'informations, voir "Configuration des options de commutation de couche 3 (Layer 3 Switching) (Page 205)".
   e. Si *Auto* est sélectionné comme mode monodiffusion, passez à l'étape Étape 4. Sinon, configurez les règles statiques de monodiffusion de passerelle par défaut et de destination comme suit :

Destination	Passerelle
192.168.0.48	0.0.0.0
192.168.2.92	0.0.0.0

      Pour plus d'informations sur la configuration des règles statiques de monodiffusion, voir "Ajout d'une règle de monodiffusion statique (Page 206)".
   f. Envoyez de multiples requêtes/réponses ARP de l'hôte 1 et de l'hôte 2 à l'appareil RUGGEDCOM ROS.
4. Envoyez un trafic bidirectionnel (c.-à-d. UDP, TCP, ICMP) entre l'hôte 1 et l'hôte 2, puis vérifiez les points suivants :
   a. Les entrées ARP sont résolues dans le tableau **ARP Table**. Pour plus d'informations, voir "Affichage d'une liste d'entrées de tableau ARP (Page 207)".
   b. Les règles sont actives dans le tableau **Rule Summary Table**. Pour plus d'informations, voir "Affichage des règles de routage (Page 209)".
   c. Le trafic est envoyé et reçu entre les deux hôtes terminaux. Pour plus d'informations, voir "Affichage de statistiques pour des ports Ethernet spécifiques (Page 70)".

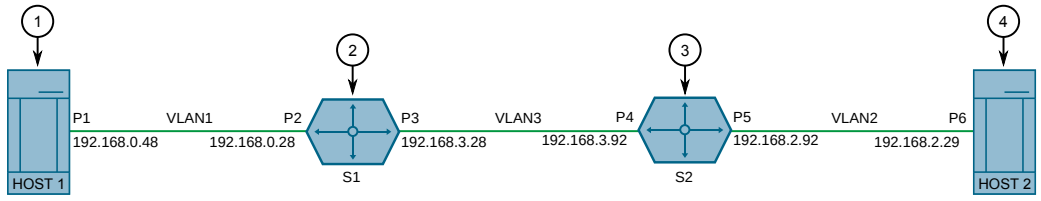
8.1.9 Exemple : configuration de Layer 3 Switching à l'aide de plusieurs commutateurs

Cet exemple illustre la configuration de commutation de couche 3 (Layer 3 Switching) à l'aide de commutateurs multiples

La topologie suivante décrit un scénario où deux hôtes sur des réseaux distincts sont connectés à deux appareils RUGGEDCOM ROS configurés comme commutateurs de couche 3. Un trafic bidirectionnel est envoyé entre les deux hôtes via les appareils RUGGEDCOM ROS.

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① Hôte 1
② S1
③ S2
④ Hôte 2

Figure 8.2 Topologie – Layer 3 Switching à l'aide de deux commutateurs

Procédez comme suit pour répliquer la topologie :

Remarque
L'hôte 1 et l'hôte 2 peuvent être un appareil de couche 2 ou un PC. Pour obtenir des instructions de configuration spécifiques, consultez la documentation OEM.

1. Configurez l'hôte 1 par la topologie comme suit :
   a. Connectez P1 à P2 de l'appareil 1 RUGGEDCOM ROS.
   b. Affectez une adresse IP *192.168.0.48* à l'interface P1.
   c. Définissez la passerelle par défaut sur *192.168.0.28*.
2. Configurez l'hôte 2 par la topologie comme suit :
   a. Connectez P6 à P5 de S2.
   b. Affectez une adresse IP *192.168.2.29* à l'interface P6.
   c. Définissez la passerelle par défaut sur *192.168.2.92*.

3. Configurez S1 comme commutateur de couche 3 :
   a. Connectez P3 à P4 de S2.
   b. Ajoutez VLAN 1 et VLAN 3. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".
   c. Affectez une adresse IP *192.168.0.28* à VLAN 1 et l'adresse IP *192.168.3.28* à VLAN 3. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   d. Affectez P2 à VLAN1 et P3 à VLAN3. Consultez "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)" pour plus d'informations.
   e. Réglez le mode monodiffusion sur *Auto*. Pour plus d'informations, voir "Configuration des options de commutation de couche 3 (Layer 3 Switching) (Page 205)".
   f. Configurez les règles statiques de monodiffusion de passerelle par défaut et de destination comme suit :

Destination	Passerelle
192.168.2.0/24	192.168.3.92

   Pour plus d'informations sur la configuration des règles statiques de monodiffusion, voir "Ajout d'une règle de monodiffusion statique (Page 206)".
4. Configurez S2 comme commutateur de couche 3 :
   a. Ajoutez VLAN 3 et VLAN 2. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".
   b. Affectez une adresse IP *192.168.3.92* à VLAN 3 et l'adresse IP *192.168.2.92* à VLAN 2. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   c. Réglez le mode monodiffusion sur *Auto*. Pour plus d'informations, voir "Configuration des options de commutation de couche 3 (Layer 3 Switching) (Page 205)".
   d. Configurez les règles statiques de monodiffusion de passerelle par défaut et de destination comme suit :

Destination	Passerelle
192.168.0.0/24	192.168.3.28

   Pour plus d'informations sur la configuration des règles statiques de monodiffusion, voir "Ajout d'une règle de monodiffusion statique (Page 206)".
5. Envoyez de multiples requêtes/réponses ARP de Host 1 à S1, et de Host 2 à S2.

6. Envoyez un trafic bidirectionnel (c.-à-d. UDP, TCP, ICMP) entre l'hôte 1 et l'hôte 2, puis vérifiez les points suivants :
   a. Les entrées ARP sont résolues dans le tableau **ARP Table**. Pour plus d'informations, voir "Affichage d'une liste d'entrées de tableau ARP (Page 207)".
   b. Les règles sont actives dans le tableau **Rule Summary Table**. Pour plus d'informations, voir "Affichage des règles de routage (Page 209)".
   c. Le trafic est envoyé et reçu entre les deux hôtes terminaux. Pour plus d'informations, voir "Affichage de statistiques pour des ports Ethernet spécifiques (Page 70)".

9 Redondance réseau

Ce chapitre décrit comment configurer et gérer les fonctionnalités de RUGGEDCOM ROS liées à la redondance.

9.1 Gestion du Spanning Tree Protocol

Cette section décrit la manière de gérer le Spanning Tree Protocol.

9.1.1 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.

9.1.1.1 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.

État

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 de transmission (Forwarding). Dans cet état, le port apprend des adresses et participe à la transmission de trames.

⚠ NOTA

RUGGEDCOM ROS introduit deux états supplémentaires : Disabled (désactivé) et Link Down (liaison interrompue). Ces états sont utiles pour la surveillance du réseau et le dépannage.

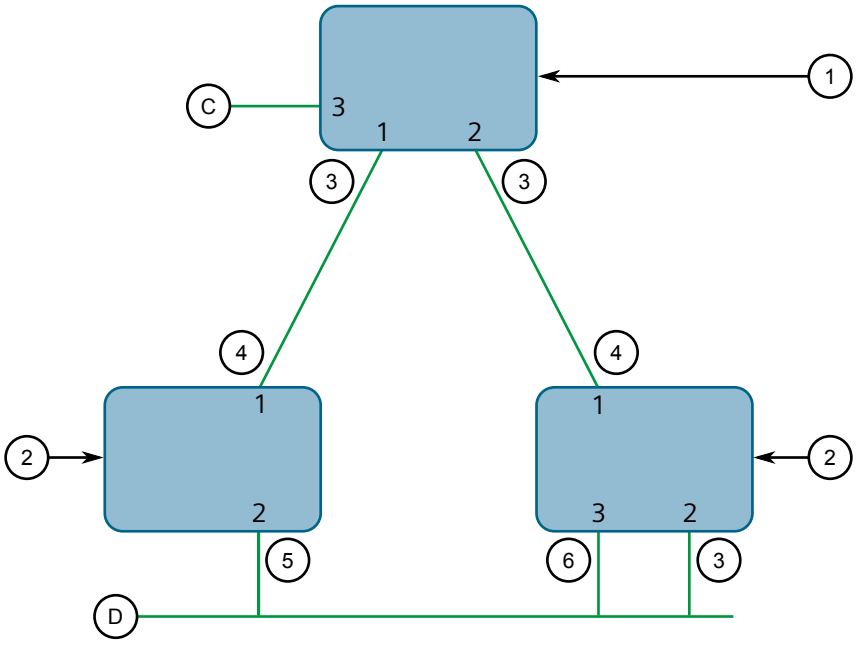
L'état Disabled (désactivé) se réfère à des liaisons pour lesquelles RSTP a été désactivé. à l'état Disabled, le port est toujours en mode de transmission.

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 racine. Les ports d'autres ponts sur le segment doivent devenir des ports racines, alternatifs ou de sauvegarde.



① Pont racine
② Pont désigné
③ Port désigné
④ Port racine
⑤ Port alternatif
⑥ Port de sauvegarde

Figure 9.1 Rôles de pont et port

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 et deviendra actif en cas de défaillance du port. Le port de sauvegarde ne participe pas au réseau.

9.1.1.2 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 donc 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.

9.1.1.3 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 du type point à point et il 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 semi-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.

9.1.1.4 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 l'autonégociation de liaison ou d'une configuration manuelle. Lorsque la méthode d'autonégociation 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 ou 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.

9.1.1.5 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.

⚠ NOTA

Augmentez la valeur du paramètre de vieillissement maximum si vous mettez en œuvre des réseaux pontés ou des anneaux de taille importante.

9.1.1.6 eRSTP

L'eRSTP (enhanced 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 160 commutateurs).

eRSTP est également compatible avec le RSTP standard pour une interopérabilité avec des commutateurs du commerce.

9.1.1.7 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.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

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 (Robust)** – 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 (Relaxed)** – 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.

9.1.2 Applications RSTP

Cette section décrit différentes applications de RSTP.

9.1.2.1 RSTP dans des configurations de câblage structuré

RSTP peut être utilisé pour construire des systèmes à câblage structuré où la connectivité est conservée en cas de défaillances de liaison. Par exemple, une seule défaillance de toute liaison entre A et N dans Figure 9.2, « Exemple - configuration de câblage structuré » maintient la connexion de tous les ports des ponts 555 à 888 au réseau.

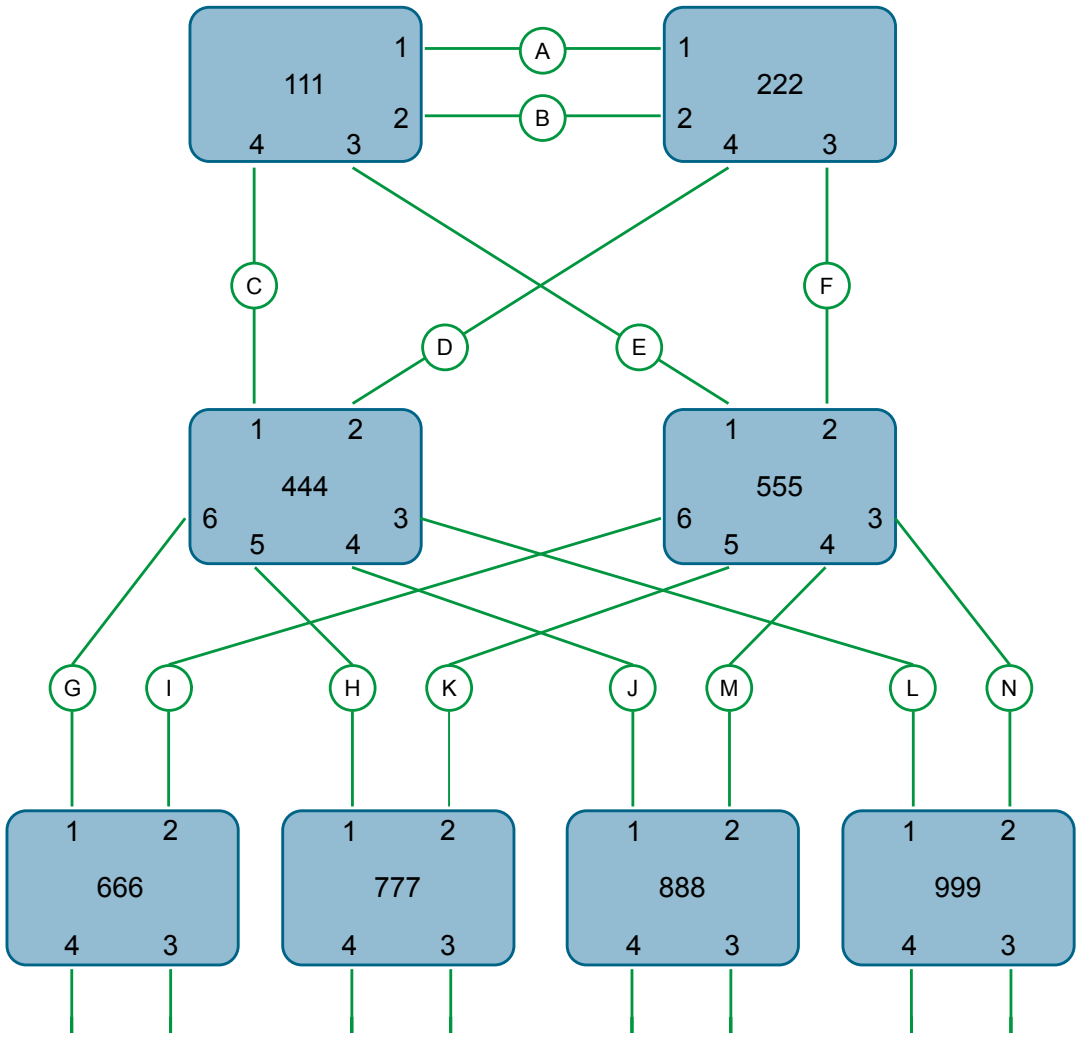


Figure 9.2 Exemple - configuration de câblage structuré

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 possible consiste à modifier la priorité de pont pour établir le pont racine et à 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 proposé 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.**

9.1.2.2 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 9.3, « Exemple - Configuration de structure en anneau ». 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.

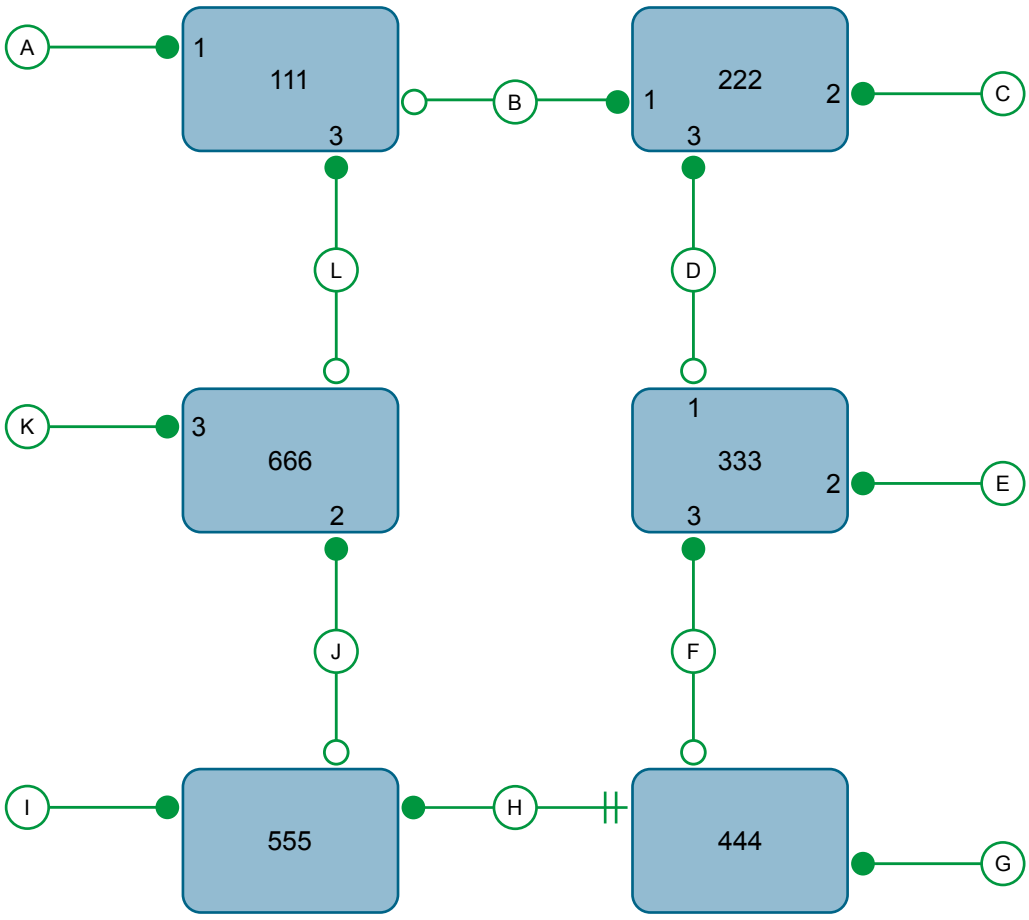


Figure 9.3 Exemple - Configuration de structure en anneau

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.**

   Pour plus d'informations, référez-vous au livre blanc RUGGEDCOM "Performance of the Rapid Spanning Tree Protocol in Ring Network Topology" disponible sous https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf.

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.**

9.1.2.3 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.

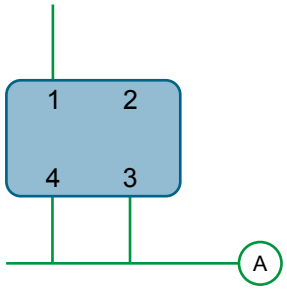


Figure 9.4 Exemple - Redondance de ports

9.1.3 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 et l'utilisation du Multiple Spanning Tree mis en œuvre 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.

9.1.3.1 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 mappages VLAN sur MSTI doivent être identiques pour tous les ponts dans 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 (Internal 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.

9.1.3.2 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 la solution 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 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.

Rôle	Description
	• Un port racine désigné fournit la solution de coût le plus bas 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 la solution de coût le plus bas 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.

9.1.3.3 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.

Équilibrage 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 ou PVST

Un des avantages de MSTP par rapport au protocole propriétaire Per-VLAN Spanning Tree (PVST) de Cisco Systems Inc. réside dans la capacité à 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.

9.1.3.4 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 sur une MSTI. Cependant, le mappage doit être identique pour chaque pont appartenant à la région MSTP.

1. Configurez et activez STP globalement et/ou pour des ports Ethernet spécifiques Pour plus d'informations, voir "Configuration globale de STP (Page 231)" ou "Configuration de STP pour des ports Ethernet spécifiques (Page 233)".

   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 "Ajout d'un VLAN statique (Page 176)".

   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 "Configuration de l'identificateur de région MST (Page 243)".
4. Assurez-vous que le résumé en lecture seule pour l'identificateur de région MST est identique pour chaque pont dans la région MST. Si le résumé est différent, l'ensemble de mappages des VLAN sur les MSTI diffère.
5. Configurez la priorité de pont pour la MSTI globale. Pour plus d'informations, voir "Configuration d'une MSTI globale (Page 244)".
6. Configurez le coût de port et la priorité par port pour chaque MSTI. Pour plus d'informations, voir "Configuration d'une MSTI pour un port Ethernet (Page 245)".
7. Définissez la version de protocole STP sur MSTP et activez STP. Pour plus d'informations, voir "Configuration globale de STP (Page 231)".

9.1.4 Configuration globale de STP

Procédez comme suit pour configurer des réglages globaux pour STP (Spanning Tree Protocol) :

1. Accédez à ***Network Redundancy » Spanning Tree » Configure Bridge RSTP Parameters***. Le formulaire **Bridge RSTP Parameters** s'affiche.
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.

Paramètre	Description
`Version Support`	**Synopsis :** [STP | RSTP | MSTP] **Par défaut :** RSTP Sélectionne la version du protocole Spanning Tree à prendre en charge, STP uniquement, Rapid STPou 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 ponts 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 pont peut établir le chemin de flux de trafics dans des conditions normales et anormales.
`Hello Time`	**Synopsis :** Un entier compris entre 1 et 10 **Par défaut :** 2 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 modérément plus intense.
`Max Age Time`	**Synopsis :** Un entier compris entre 6 et 40 **Par défaut :** 20 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 :** Un entier compris entre 3 et 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 plus rapidement en cas de liaisons défaillantes/ponts défaillants.
`Forward Delay`	**Synopsis :** Un entier compris entre 4 et 30 **Par défaut :** 15 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.

Paramètre	Description
`Max Hops`	**Synopsis :** Un entier compris entre 6 et 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 maximum 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**.

9.1.5 Configuration de STP pour des ports Ethernet spécifiques

Procédez comme suit pour configurer STP (Spanning Tree Protocol) pour un port Ethernet spécifique :

1. Accédez à ***Network Redundancy » Spanning Tree » Configure Port RSTP Parameters***. Le tableau **Port RSTP Parameters** s'affiche.
2. Sélectionnez un port Ethernet. Le formulaire **Port RSTP Parameters** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port(s)`	**Synopsis :** Comma-separated list of ports Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).
`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 dans le réseau. 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 et qui sont attachés à un LAN commun sélectionnent le port à utiliser en fonction de la priorité de port.

Paramètre	Description
`STP Cost`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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 autorisé ou 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	Description
	paramètre est forcé sur False lorsque le port traite la liaison en mode duplex intégral, mais n'est pas point à point (c'est-à-dire une liaison en duplex intégral vers un pont non managé qui concentre deux autres ponts STP).
`Restricted Role`	**Synopsis :** [True | 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 | False] **Par défaut :** False Valeur booléenne définie par l'administration. Si TRUE est défini, le port ne propage pas les 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**.

9.1.6 Configuration d'eRSTP

Procédez comme suit pour configurer eRSTP :

1. Accédez à ***Network Redundancy » Spanning Tree » Configure eRSTP Parameters***. Le formulaire **eRSTP Parameters** s'affiche.
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

Paramètre	Description
	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 :** Un entier compris entre 1 et 86400 ou [Until reset | Don't shutdown] **Par défaut :** Don't shutdown La norme 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'influencer 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 censés 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 temps de récupération est difficile à calculer et peut être différent (et éventuellement relativement long) pour toute topologie en maillage. Ce paramètre de configuration activeSiemensle RSTP amélioré qui détecte une défaillance du commutateur racine et exécute des étapes de traitement RSTP supplémentaires, réduisant ainsi de manière significative 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 temps 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

Paramètre	Description
	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 de racine.
`IEEE802.1w Interoperability`	**Synopsis :** [On | Off] **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 style 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.

Paramètre	Description
	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 si le port ne migre pas vers STP.

3. Cliquez sur **Apply**.

9.1.7 Affichage de statistiques globales concernant STP

Pour afficher des statistiques globales concernant STP, accédez à ***Network Redundancy » Spanning Tree » View Bridge RSTP Statistics***. Le formulaire **Bridge RSTP Statistics** s'affiche.

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 afficher du texte indiquant Not Designated For Any LAN si le pont n'est désigné pour aucun de ses ports.
`Bridge ID`	**Synopsis :** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Identificateur de ce pont.
`Root ID`	**Synopsis :** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Identificateur du pont racine.
`Root Port`	**Synopsis :** 1/1 to maximum port number ou [<empty string>] Si le pont est désigné, il s'agit du port qui fournit la connectivité au pont racine du réseau.
`Root Path Cost`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 65535 Délai Hello Time configuré dans le menu Bridge RSTP Parameters.
`Learned Hello Time`	**Synopsis :** Un entier compris entre 0 et 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.

Paramètre	Description
`Configured Forward Delay`	**Synopsis :** Un entier compris entre 0 et 65535 Délai de transmission (Forward Delay) configuré dans le menu Bridge RSTP Parameters.
`Learned Forward Delay`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 65535 Délai de vieillissement maximum configuré dans le menu Bridge RSTP Parameters.
`Learned Max Age`	**Synopsis :** Un entier compris entre 0 et 65535 Délai de vieillissement maximum 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 :** Un entier compris entre 0 et 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. Nombre excessivement élevé ou croissant rapidement signale des problèmes réseau.
`Time since Last TC`	**Synopsis :** DDDD days, HH:MM:SS Temps depuis la dernière détection d'une modification de topologie par le pont.

9.1.8 Affichage de statistiques STP pour des ports Ethernet

Pour afficher des statistiques STP pour des ports Ethernet, accédez à ***Network Redundancy » Spanning Tree » View Port RSTP Statistics***. Le tableau **Port RSTP Statistics** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port(s)`	**Synopsis :** Comma-separated list of ports Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).
`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. • `Listening`– Cet état n'est pas utilisé par . • `Learning`– Le port apprend les adresses MAC pour éviter l'écoulement quand il commence à transmettre le trafic. • `Forwarding`– Le port transmet le trafic. • `Blocking`– Le port bloque le trafic.

Paramètre	Description
	• `Link Down`– STP est activé sur ce port, mais la liaison est désactivée. • `Discarding`– La liaison n'est pas utilisée dans la topologie STP mais est en réserve.
`Role`	**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 :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 4294967295 Nombre de messages de configuration RSTP reçus sur ce port.
`TX RSTs`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de messages de configuration RSTP transmis sur ce port.
`RX Configs`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de messages de configuration STP reçus sur ce port.
`TX Configs`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de messages de configuration STP transmis sur ce port.
`RX Tcns`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de messages de notification de modification de topologie STP reçus sur ce port. Nombre excessivement élevé ou croissant rapidement signale des problèmes réseau.
`TX Tcns`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de messages de notification de modification de topologie STP transmis sur ce port.

Paramètre	Description
`Desig Bridge ID`	**Synopsis :** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier du pont auquel ce port est connecté, fourni sur les ports racine des ponts désignés.
`operEdge`	**Synopsis :** [True | False] Le port fonctionne ou non en tant que port de périphérie.

9.1.9 Gestion de Multiple Spanning Tree Instances

Cette section décrit la configuration et la gestion des MSTI (Multiple Spanning Tree Instances).

9.1.9.1 Affichage des statistiques pour des MSTI globales

Pour afficher les statistiques pour des MSTI globales, accédez à ***Network Redundancy » Spanning Tree » View Bridge MSTI Statistics***. Le formulaire **Bridge MSTI Statistics** s'affiche.

Pour afficher les statistiques pour des MSTI globales, accédez à ***Spanning Tree » View Bridge MSTI Statistics***. Le formulaire **Bridge MSTI Statistics** s'affiche.

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 afficher du texte indiquant Not Designated For Any LAN si le pont n'est désigné pour aucun de ses ports.
`Bridge ID`	**Synopsis :** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Identificateur de ce pont.
`Root ID`	**Synopsis :** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Identificateur du pont racine.
`Root Port`	**Synopsis :** 1/1 to maximum port number ou [<empty string>] Si le pont est désigné, il s'agit du port qui fournit la connectivité au pont racine du réseau.
`Root Path Cost`	**Synopsis :** Un entier compris entre 0 et 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.

Paramètre	Description
	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 :** Un entier compris entre 0 et 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. Nombre excessivement élevé ou croissant rapidement signale des problèmes réseau.

9.1.9.2 Affichage des statistiques pour des MSTI de ports

Pour afficher les statistiques pour des MSTI de ports, accédez à ***Network Redundancy » Spanning Tree » View Port MSTI Statistics***. Le formulaire **Port MSTI Statistics** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port(s)`	**Synopsis :** Comma-separated list of ports Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).
`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. • `Listening`– Cet état n'est pas utilisé par . • `Learning`– Le port apprend les adresses MAC pour éviter une avalanche quand il commence à transmettre le trafic. • `Forwarding`– Le port transmet le trafic. • `Blocking`– Le port bloque le trafic. • `Link Down`– STP est activé sur ce port, mais la liaison est désactivée. • `Discarding`– La liaison n'est pas utilisée dans la topologie STP mais est en réserve.
`Role`	**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.

Paramètre	Description
	• `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 :** Un entier compris entre 0 et 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 :** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier du pont auquel ce port est connecté, fourni sur les ports racine des ponts désignés.

9.1.9.3 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 "Régions MSTP et interopérabilité (Page 226)".

Procédez comme suit pour configurer l'identificateur de région MST (Multiple Spanning Tree) :

1. Accédez à ***Network Redundancy » Spanning Tree » Configure MST Region Identifier***. Le formulaire **MST Region Identifier** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Name`	**Synopsis :** Chaîne de 32 caractères **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 :** Un entier compris entre 0 et 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.

Paramètre	Description
`Digest`	**Synopsis :** Chaîne de 32 caractères **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 digest (cette synthèse) de 16 octets créé avec le mappage VLAN à instance est envoyé aux BPDU.

3. Cliquez sur **Apply**.

9.1.9.4 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 ***Network Redundancy » Spanning Tree » Configure Bridge MSTI Parameters***. Le formulaire **Bridge MSTI Parameters** s'affiche.
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 ponts 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 pont peut établir le chemin de flux de trafics dans des conditions normales et anormales.

4. Cliquez sur **Apply**.

9.1.9.5 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 ***Network Redundancy » Spanning Tree » Configure Port MSTI Parameters***. Le tableau **Port MSTI Parameters** s'affiche.
2. Sélectionnez un port Ethernet. Le formulaire **Port MSTI Parameters** s'affiche.
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 :** Comma-separated list of ports Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).
`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 et qui sont attachés à un LAN commun sélectionnent le port à utiliser en fonction de la priorité de port.
`STP Cost`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 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**.

9.1.10 Effacement de statistiques de Spanning Tree Protocol

Procédez comme suit pour effacer toutes les statistiques de Spanning Tree Protocol :

1. Accédez à ***Network Redundancy » Spanning Tree » Clear Spanning Tree Statistics***. Le formulaire **Clear Spanning Tree Statistics** s'affiche.
2. Cliquez sur **Confirm**.

9.2 Gestion du Media Redundancy Protocol (MRP)

RUGGEDCOM ROS prend en charge le Media Redundancy Protocol (MRP).

9.2.1 Comprendre MRP

Le MRP (Media Redundancy Protocol) est un protocole réseau conçu pour implémenter la redondance et la récupération dans une topologie en anneau comprenant jusqu'à 50 appareils. Il permet à des anneaux de commutateurs Ethernet de surmonter rapidement toute défaillance unique d'une liaison inter-commutateurs, d'un commutateur dans l'anneau MRP ou de la topologie d'interconnexion.

MRP fonctionne entre la couche 2 et la couche d'application et utilise les fonctions de ISO/IEC/IEEE 8802-3 (IEEE 802.3) et IEEE 802.1Q, y compris Filtering Database (FDB).

MRP est normalisé par l'International Electrotechnical Commission comme IEC 62439-2.

9.2.1.1 Appareils MRM ou MRC

Dans un anneau MRP, le Media Redundancy Manager (MRM) agit comme le gestionnaire d'anneau, tandis que les Media Redundancy Clients (MRCs) agissent comme nœuds membres de l'anneau.

Le MRM envoie périodiquement des messages de test MRP via ses deux ports d'anneau. Ces messages sont transmis par les MRC entre leurs ports d'anneau. Les commutateurs étant connectés dans un anneau, les messages de test MRP circulent dans l'anneau et retournent au MRM. Cela permet au MRM de déterminer l'état de l'anneau.

Lorsque les messages de test MRP sont retournés au MRM, la redondance est présente et l'anneau est déclaré fermé. Lorsque le retour des messages de test MRP échoue, la redondance est perdue et l'anneau est déclaré ouvert.

Lorsque l'anneau est fermé, le MRM bloque tous les paquets transmis sur un de ses deux ports d'anneau désignés, pendant que l'autre port transmet des paquets. Lorsqu'une défaillance de liaison se produit, le MRC envoie une notification de

défaillance de liaison au MRM qui débloque alors ses ports bloqués, permettant ainsi la communication entre tous les appareils.

9.2.1.2 Appareils MRA

Les appareils Media Redundancy Manager Auto (MRA) décident automatiquement quel appareil prendra le rôle de manager dans l'anneau. Ceci est réalisé via un processus d'élection entre tous les MRA de l'anneau. Une fois le manager élu, les autres MRA jouent le rôle de clients.

Lorsqu'un MRA est présent dans un anneau, tous les autres appareils de l'anneau doivent être soit MRA ou MRC (pas MRM).

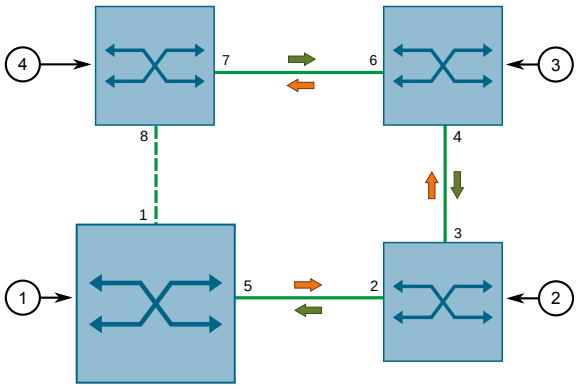
9.2.1.3 États de ports d'anneau

Les ports d'anneau MRM et MRC prennent en charge trois états : *disabled* (désactivé), *blocked* (bloqué), et *forwarding* (transmission) :

- Les ports d'anneau **désactivés** abandonnent tous les paquets reçus.
- Les ports d'anneau **bloqués** abandonnent tous les paquets reçus à l'exception des paquets de contrôle MRP.
- Les ports d'anneau en **transmission** transmettent tous les paquets reçus.

9.2.1.4 Anneau fermé ou anneau ouvert

En fonctionnement normal, le réseau fonctionne à l'état anneau fermé. Dans cet état, un des ports d'anneau MRM est bloqué, tandis que l'autre transmet. Les deux ports d'anneau de tous les MRC transmettent.

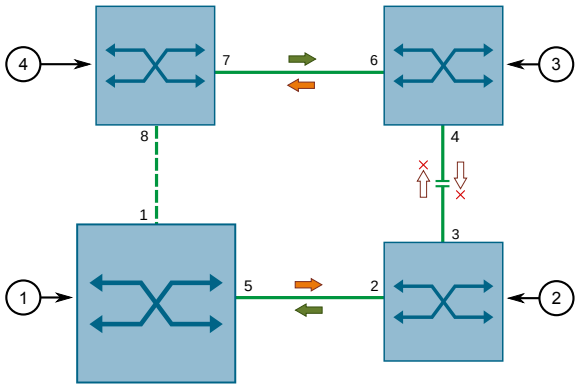


① MRM ou MRA fonctionnant comme Manager
② Client 1 MRP
③ Client 2 MRP

④ Client 3 MRP

Figure 9.5 État anneau fermé MRP

En cas de défaillance, le réseau fonctionne à l'état anneau ouvert. Dans cet état, lorsqu'une liaison entre deux appareils est défaillante, les deux ports d'anneau du MRM transmettent. Les MRC adjacents à la défaillance ont un port d'anneau bloqué et un qui transmet et les autres MRC ont les deux ports d'anneau qui transmettent.



① MRM ou MRA fonctionnant comme Manager
② Client 1 MRP
③ Client 2 MRP
④ Client 3 MRP

Figure 9.6 État MRP anneau ouvert

9.2.2 Configuration globale du MRP

Procédez comme suit pour configurer globalement le Media Redundancy Protocol :

1. Accédez à ***Network Redundancy » Ring Redundancy » Configure Global MRP Parameters***. Le formulaire **Global MRP Parameters** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`State`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Active/désactive MRP globalement. Remarquez que MRP peut être désactivé port par port.
`Auto Generate UUID`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Enabled Active/désactive la génération automatique de l'UUID (Universal Unique Identifier) MRP. Si activé, tout ID de domaine existant

Paramètre	Description
	configuré par l'utilisateur sera écrasé par l'UUID généré. L'UUID généré est le hachage MD5 du nom de domaine.

3. Cliquez sur **Apply**.

9.2.3 Affichage de l'état des instances MRP

Pour afficher l'état des instances MRP, accédez à ***Network Redundancy » Ring Redundancy » View MRP Instance Status***. Le tableau **MRP Instance Status** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Index`	Numéro d'instance MRP.
`Name`	**Synopsis :** Chaîne de 24 caractères ou [default-mrpdomain] **Par défaut :** default-mrpdomain Nom du domaine/de l'anneau MRP. Toutes les instances MRP appartenant au même anneau doivent avoir le même nom de domaine.
`Role`	Rôle assigné à l'instance MRP : • `Disabled`– Aucun rôle assigné. L'instance MRP est désactivée. • `Client`– Client MRP. • `Manager`– MRP Manager. • `ManagerAuto`– L'instance MRP détermine automatiquement le rôle.
`Ring Status`	État de l'anneau MRP. Les valeurs possibles sont : • `N/A`– L'état de l'anneau est inconnu. S'affiche lorsque l'appareil est un MRC. • `Open`– L'anneau MRP est ouvert. Les deux ports d'anneau transmettent des paquets. • `Fermé`– L'anneau MRP est fermé. Un port d'anneau transmet les paquets, tandis que l'autre bloque les paquets.
`PRM Port`	Numéro de port et état du port d'anneau MRP. Les valeurs possibles sont : • `{` *port* `}-OFF`– MRP désactivé. • `{` *port* `}-DWN`– Le port d'anneau est désactivé. • `{` *port* `}-BLK`– Le port d'anneau bloque les paquets. • `{` *port* `}-FWD`– Le port d'anneau transmet les paquets.
`SEC Port`	Numéro de port et état du port d'anneau MRP. Les valeurs possibles sont : • `{` *port* `}-OFF`– MRP désactivé. • `{` *port* `}-DWN`– Le port d'anneau est désactivé. • `{` *port* `}-BLK`– Le port d'anneau bloque les paquets.

Paramètre	Description
	• `{ port }-FWD`– Le port d'anneau transmet les paquets.
`Multi-MRM Err`	Erreur indiquée par un MRM lorsque plus d'un MRM est actif dans l'anneau MRP. Les valeurs possibles sont : • `false`– Pas d'erreur Multi-MRM. • `true`– Plus d'un MRM présent dans l'anneau.
`One Side Rx Err`	Erreur indiquée par un MRM lorsque les trames de test d'un MRM ont été vues, mais seulement sur un port d'anneau. Les valeurs possibles sont : • `false`– Pas d'erreur One Side Rx. • `true`– Trame test reçue uniquement sur un port d'anneau.

9.2.4 Ajout d'une instance MRP

Procédez comme suit pour configurer une instance MRP :

1. Accédez à ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. Le tableau **MRP Instances** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **MRP Instances** s'affiche.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

RUGGEDCOM ROS n'autorise les instances MRP multiples que si l'appareil est le gestionnaire d'anneau dans chaque instance. Un appareil peut posséder jusqu'à quatre instances de gestionnaire d'anneau.

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

Les MRM ou les MRA faisant fonction de gestionnaire doivent être déconnectés physiquement ou leur port d'anneau primaire doit être désactivé (c.-à-d. que l'anneau MRP doit être ouvert) avant que la configuration de l'instance MRM ne puisse être modifiée.

Pour plus d'informations sur la configuration des paramètres de port, voir "Configuration d'un port Ethernet (Page 73)".

Pour plus d'informations sur les anneaux MRP ouverts et fermés, voir "Gestion du Media Redundancy Protocol (MRP) (Page 246)".

Remarque
Pour éviter d'éventuels problèmes de configuration erronée pouvant entraîner une perte d'accès au réseau, Siemens recommande de désactiver le port d'anneau d'un MRC avant de le configurer. Pour plus d'informations sur la

configuration des paramètres de port, voir "Configuration d'un port Ethernet (Page 73)".

Remarque
Lorsque vous utilisez la sécurité de port dans un anneau MRP, les adresses MAC des appareils de l'anneau doivent être configurées pour permettre la communication entre eux. Par ailleurs, le port d'anneau du MRM doit être configuré dans le tableau **Static MAC Addresses** pour que l'anneau reste à l'état fermé. Pour plus d'informations, voir "Authentification basée sur des adresses MAC statiques dans un anneau MRP (Page 147)".

3. Configurez les paramètres suivants :

Paramètre	Description
`Index`	**Synopsis :** Un entier compris entre 1 et 4 **Par défaut :** 1 Numéro d'instance MRP.
`Name`	**Synopsis :** Chaîne de 24 caractères **Par défaut :** default-mrpdomain Nom du domaine/de l'anneau MRP. Toutes les instances MRP appartenant au même anneau doivent avoir le même nom de domaine.
`Role`	**Synopsis :** [Disabled | Client | Manager | ManagerAuto] **Par défaut :** Client Rôle assigné à l'instance MRP : • `Disabled`– Aucun rôle assigné. L'instance MRP est désactivée. • `Client`– Client MRP. • `Manager`– MRP Manager. • `ManagerAuto`– L'instance MRP détermine automatiquement le rôle.
`PRM Port`	**Synopsis :** 1 to maximum port number **Par défaut :** 1 Numéro de port d'anneau MRP. Numéro de port indiqué sur l'appareil.
`SEC Port`	**Synopsis :** 1 to maximum port number **Par défaut :** 1 Numéro de port d'anneau MRP. Numéro de port indiqué sur l'appareil.
`Priority`	**Synopsis :** Chaîne de 4 caractères **Par défaut :** 8000 Priorité affectée à l'instance MRP. Ceci est utilisé lors de la négociation avec d'autres appareils MRP pour déterminer lequel est le MRP Manager. Les valeurs possibles sont : • `0000`– Priorité la plus élevée (Manager)

Paramètre	Description
	• `1000`– 7000 – Priorité élevée (Manager) • `8000`– Priorité par défaut (Manager) • `9000 – E000`– Priorité basse (ManagerAuto) • `F000`– Priorité la plus basse (ManagerAuto) La priorité s'applique uniquement lorsque le rôle est défini sur Manager ou ManagerAuto.
`ID`	**Synopsis :** Chaîne de 32 caractères **Par défaut :** FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF Domaine 128 bits UUID univoque sur un domaine/anneau. Toutes les instances MRP appartenant au même anneau doivent avoir le même ID de domaine. Lorsque le paramètre Auto Generate UUID est activé, ROS génère automatiquement l'ID de domaine comme hachage MD5 du nom de domaine. Dans ce cas, toute tentative de modification de l'ID de domaine est rejetée. Lorsque le paramètre Auto Generate UUID est désactivé, l'ID de domaine peut être modifié par l'utilisateur.

4. Cliquez sur **Apply**.

9.2.5 Suppression d'une instance MRP

Procédez comme suit pour supprimer une instance MRP :

1. Accédez à ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. Le tableau **MRP Instances** s'affiche.
2. Cliquez sur l'enregistrement souhaité. Le formulaire **MRP Instances** s'affiche.

⚠ NOTA

Les MRM ou les MRA faisant fonction de gestionnaire doivent être déconnectés physiquement ou leur port d'anneau doit être désactivé (c.-à-d. que l'anneau MRP doit être ouvert) pour que la configuration de l'instance MRM puisse être modifiée.

Pour plus d'informations sur la configuration des paramètres de port, voir "Configuration d'un port Ethernet (Page 73)".

Pour plus d'informations sur les anneaux MRP ouverts et fermés, voir "Gestion du Media Redundancy Protocol (MRP) (Page 246)".

Remarque
Pour éviter d'éventuels problèmes de configuration erronée pouvant entraîner une perte d'accès au réseau, Siemens recommande de désactiver le port d'anneau d'un MRC avant de le configurer. Pour plus d'informations sur la configuration des paramètres de port, voir "Configuration d'un port Ethernet (Page 73)".

3. Cliquez sur **Delete**.

9.2.6 Exemple : configuration d'un anneau MRP

Cet exemple illustre la façon de configurer un anneau MRP à l'aide quatre appareils RUGGEDCOM ROS.

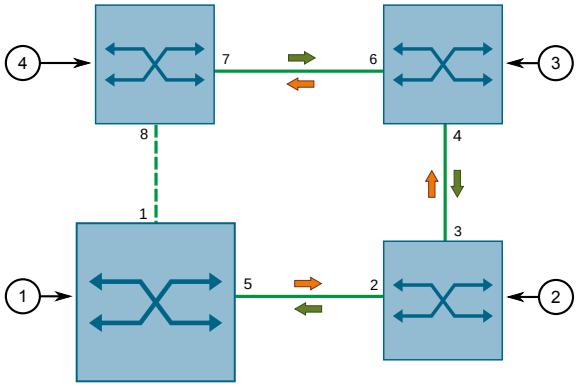
Dans la topologie suivante, l'anneau MRP fonctionne à l'état d'anneau fermé. L'appareil MRP Manager (MRM) sert de gestionnaire d'anneau, tandis que les appareils MRP Client (MRC) agissent comme nœuds membres de l'anneau. Chaque nœud MRM ou MRC possède deux ports participant à l'anneau.

Le MRM bloque tous les paquets transmis sur un de ses deux ports d'anneau désignés. Si l'un des deux liens sur autre nœud d'anneau détecte une défaillance, l'anneau MRP passe à l'état anneau ouvert. À cet état, le MRC envoie un message au MRM qui débloque alors ses ports bloqués, établissant la communication entre tous les commutateurs.

Pour plus d'informations sur les états anneau fermé et anneau ouvert, voir "Gestion du Media Redundancy Protocol (MRP) (Page 246)".

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① MRP Manager
② Client 1 MRP
③ Client 2 MRP
④ Client 3 MRP

Figure 9.7 Topologie – Anneau MRP

Procédez comme suit pour configurer un anneau MRP par la topologie :

1. Assurez-vous que RSTP est désactivé sur les ports agissant comme ports PRM et SEC ports dans l'anneau. Pour plus d'informations, voir "Configuration d'un port Ethernet (Page 73)".
2. Activez MRP sur le MRP Manager et tous les appareils MRP Client. Pour plus d'informations, voir "Configuration globale du MRP (Page 248)".

3. Configurez une instance MRP pour l'appareil MRP Manager comme suit :

Paramètre	Valeur
Name	{ name }
Role	Manager
PRM Port	5
SEC Port	1
Priority	1000

Pour plus d'informations sur la configuration d'instances MRP, voir "Ajout d'une instance MRP (Page 250)".

4. Configurez une instance MRP pour chaque appareil MRP Client comme suit :

Remarque
Dans cet exemple, trois appareils sont utilisés. MRP est pris en charge dans des topologies en anneau jusqu'à 50 appareils.

Appareil	Paramètre	Valeur
Client 1 MRP	Name	{ name }
	Role	Client
	PRM Port	2
	SEC Port	3
	Priority	A000
Client 2 MRP	Name	{ name }
	Role	Client
	PRM Port	4
	SEC Port	6
	Priority	A000
Client 3 MRP	Name	{ name }
	Role	Client
	PRM Port	7
	SEC Port	8
	Priority	A000

Pour plus d'informations sur la configuration d'instances MRP, voir "Ajout d'une instance MRP (Page 250)".

5. Pour vérifier la configuration, assurez-vous que l'ID d'instance MRP est générée automatiquement dans l'appareil MRP Manager et chaque appareil MRP Client. Pour plus d'informations sur l'ID d'instance MRP, référez-vous à "Ajout d'une instance MRP (Page 250)".

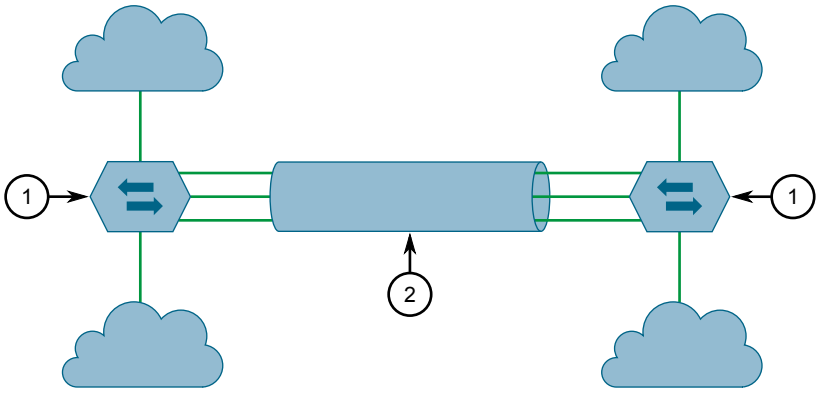
9.3 Gestion de l'agrégation de liens

L'agrégation de liens, également appelée *port trunking* ou *port bundling*, permet d'agréger ou de rassembler plusieurs ports Ethernet dans une liaison logique

(Link Aggregation Group) avec une largeur de bande 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 liens peut être utilisée 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.



① Appareil
② Link Aggregation Group (LAG)

Figure 9.8 Topographie basique de l'agrégation de liens

9.3.1 Concepts d'agrégation de liens

La présente rubrique décrit certains concepts importants de la mise en œuvre de l'agrégation de liens dans RUGGEDCOM ROS.

9.3.1.1 Agrégation de lien statique ou dynamique

RUGGEDCOM ROS prend en charge l'agrégation de lien statique ou dynamique. Dans l'agrégation de lien **statique**, un appareil est apparié avec un appareil partenaire spécifique partageant les mêmes fonctionnalités et la même configuration. Les exigences sont les mêmes pour l'agrégation de lien dynamique, mais avec moins d'interventions de l'utilisateur. Dans l'agrégation de lien **dynamique**, le Link Aggregation Control Protocol (LACP) recherche un partenaire adéquat par lui-même après avoir négocié avec ses pairs pour déterminer le meilleur candidat.

L'agrégation de lien statique est idéale pour les configurations switch-to-switch, mais ne dispose pas des fonctionnalités clés suivantes offertes par l'agrégation de lien dynamique :

- **Basculement**

  Dans l'agrégation de lien statique, les appareils sont incapables de communiquer l'état de leurs LAGs. Si tous les ports d'un LAG sont défaillants et qu'il y a un convertisseur de supports entre les deux appareils, l'appareil à l'autre extrémité le saura et continuera à transmettre le trafic à ses partenaires. L'agrégation de lien dynamique, quant à elle, détecte la liaison défaillante et arrête d'envoyer le trafic aux autres appareils.

- **Renégociation**

  Si tous les ports de l'appareil partenaire sont défaillants et/ou le rapport signal-bruit (Signal-to-Noise Ratio (SNR)) est trop élevé, LACP cherche automatiquement un autre appareil compatible LACP sur le réseau avec lequel former une nouvelle voie de port.

- **Réserve**

  Si un nombre de ports plus grand que ce que l'appareil peut prendre en charge est ajouté au LAG, LACP met automatiquement les ports en excès en réserve. Il détermine les ports à mettre en réserve sur la base de critères définis par l'utilisateur. Ces ports de réserve attendent jusqu'à ce qu'un port actif soit défaillant, puis prennent sa place.

- **Vérification de liaison**

  Dans l'agrégation de lien dynamique, les deux partenaires peuvent mutuellement vérifier la voie de port entre eux, ce qui facilite la confirmation de la configuration par l'utilisateur. L'agrégation de lien statique ne permet pas cette vérification.

Le choix entre l'agrégation de lien statique et dynamique dépend des fonctionnalités des appareils disponibles sur le réseau.

9.3.1.2 Règles et limitations

La mise en œuvre d'une d'agrégation de liaisons doit respecter les règles et limitations suivantes :

- Un port peut uniquement appartenir à un seul Link Aggregation Group (LAG) ou *port trunk* à la fois.
- Un port en miroir (le port cible) ne peut pas appartenir à un LAG. Cependant, tout port qui reçoit le trafic en miroir (le port source) peut appartenir à un LAG.
- Si seul un LAG QinQ est pris en charge par l'appareil, le port fonctionnant en mode QinQ ne peut pas être un membre secondaire d'un LAG.
- Le port client DHCP Relay Agent ne peut pas être membre d'une agrégation d'un LAG.
- 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 du LAG 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'un LAG.
- La norme d'agrégation de liens IEEE 802.1AX (anciennement IEEE 802.3ad) requiert que toutes les liaisons physiques dans le LAG s'exécutent à la même vitesse et en mode duplex intégral. Si cette condition n'est pas remplie, la performance du LAG diminue.

  Le commutateur génère une alarme correspondante en cas de détection d'une telle incompatibilité vitesse/duplex.
- Le Spanning Tree Protocol (STP) calcule de manière dynamique le coût de chemin du LAG 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.

9.3.1.3 Agrégation de liens et fonctionnalités de couche 2

Les fonctionnalités de couche 2 (par ex. STP, VLAN, CoS, filtrage de multidiffusion) traitent un Link Aggregation Group (LAG) comme une liaison unique.

- Si le Spanning Tree Protocol (STP) met l'état d'un port agrégé en mode `Blocking` or `Forwarding`, il le fait dans le LAG entier.
- Si l'un des ports agrégés joint ou quitte un groupe de multidiffusion (par ex. via GMRP), tous les autres ports dans le LAG 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 LAG.
- 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 utilisateur appropriées.
- Lorsqu'un port secondaire est ajouté à un LAG, il hérite de tous les réglages de configuration du port principal. Lorsque ce port secondaire est supprimé du LAG, les réglages qu'il avait avant l'agrégation sont restaurés.

9.3.1.4 Agrégation de liens 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 Link Aggregation Group (LAG) et sont affichés comme à l'accoutumée pour chaque port.
- Assurez-vous que seuls les ports avec la même vitesse et le même réglage de duplex sont agrégés. Si l'autonégociation est utilisée, assurez-vous qu'elle est résolue à la même vitesse pour tous les ports du groupe d'agrégation de liens.
- Pour obtenir une valeur de compteur de statistiques Ethernet pour le LAG, ajoutez les valeurs des compteurs pour tous les ports dans le LAG.

9.3.2 Configuration de l'agrégation de liens

Procédez comme suit pour configurer l'agrégation de liens statique ou dynamique :

1. Déconnectez ou désactivez chaque port à agréger. Pour plus d'informations sur la désactivation d'un port, voir "Configuration d'un port Ethernet (Page 73)".
2. Créez un ou plusieurs Link Aggregation Groups (LAG) composés de deux ports ou plus. Pour plus d'informations, voir "Ajouter un groupe d'agrégation de liens (Page 259)".
3. Connectez ou activez chaque port dans le LAG. Pour plus d'informations sur l'activation d'un port, voir "Configuration d'un port Ethernet (Page 73)".
4. Si l'agrégation de liens dynamique est requise, configurez les réglages LACP globaux et par port. Pour plus d'informations, voir "Configuration des réglages globaux LACP (Page 262)" et "Configuration de LACP par port (Page 263)".
5. Répétez Étape 1 à Étape 4 pour un appareil voisin qui possède les mêmes fonctionnalités (c.-à-d. vitesse de port, type de support, etc.), en veillant à consulter la documentation utilisateur de l'appareil pour plus de détails.

9.3.3 Gestion des groupes d'agrégation de liens

RUGGEDCOM ROS permet la configuration d'un maximum de 15 Link Aggregation Groups (LAG) ou *port trunks* sur un appareil unique, composés chacun d'un maximum de huit ports.

Remarque
Évitez de configurer les LAG lorsque Layer 3 switching est activé. Pour plus d'informations sur l'activation ou la désactivation de Layer 3 switching, voir "*Layer 3 (couche 3)* (Page 199)".

Remarque
Le nombre maximum de LAG pour chaque appareil dépend du nombre de ports disponibles. Au moins deux ports sont requis pour configurer un LAG.

Remarque
Le port agrégé avec le numéro de port le plus petit est appelé le port *principal*. Les autres ports dans le LAG sont dénommés ports *secondaires*.

9.3.3.1 Affichage d'une liste de groupes d'agrégation de liens

Pour afficher une liste de groupes d'agrégation de liens (LAG), ou *port trunks* configurés sur l'appareil, accédez à ***Link Aggregation » Configure Port Trunks***. Le tableau **Port Trunks** s'affiche.

Si aucun LAG n'a été configuré, ajoutez des LAG en fonction de vos besoins. Pour plus d'informations, voir "Ajouter un groupe d'agrégation de liens (Page 259)".

9.3.3.2 Ajouter un groupe d'agrégation de liens

Procédez comme suit pour ajouter un groupe d'agrégation de liens (LInk Aggregation Group ou (LAG)) ou un *port trunk* (agrégation de ports) :

⚠ NOTA

Risque pour la configuration - risque d'interruption de la communication.

Le groupe d'agrégation de liens doit être correctement configuré des deux côtés de la voie de port. 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'un groupe d'agrégation de liens est fortement recommandée :

1. Déconnectez ou désactivez tous les ports intervenant dans la configuration, c'est-à-dire qui sont en cours d'ajout ou de suppression du groupe d'agrégation de liens.
2. Configurez le groupe d'agrégation de liens sur les deux commutateurs.
3. Vérifiez le groupe d'agrégation de liens sur les deux commutateurs.
4. Reconnectez ou activez de nouveau les ports.

Si le groupe d'agrégation de liens est en cours de configuration alors que les ports ne sont pas déconnectés ou désactivés, ces derniers seront désactivés automatiquement pendant quelques secondes.

Remarque
Assurez-vous que seuls les ports avec la même vitesse et le même réglage de duplex sont agrégés. Si l'autonégociation est utilisée, assurez-vous qu'elle est résolue à la même vitesse pour tous les ports du groupe d'agrégation de liens.

1. Accédez à ***Link Aggregation » Configure Port Trunks***. Le tableau **Port Trunks** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **Port Trunks** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Trunk ID`	**Synopsis :** Un entier compris entre 1 et 5 **Par défaut :** 1 ID du Link Aggregation Group (LAG), ou port trunk (agrégation de ports).
`Trunk Name`	**Synopsis :** Chaîne de 19 caractères Nom du Link Aggregation Group (LAG), ou port trunk (agrégation de ports). Lorsque possible, incluez des détails qui identifient le motif de l'agrégation des liaisons.
`Mode`	**Synopsis :** [LACP | Static] **Par défaut :** Static Définit la façon dont l'agrégation de liaisons est effectuée. Options possibles : • `LACP`– L'agrégation de liaisons est effectuée de façon dynamique à l'aide de LACP pour les deux côtés du partenariat de l'agrégation de liaisons. • `Static`– Les paramètres d'agrégation de liaisons sont configurés manuellement sur les deux côtés du partenariat de l'agrégation de liaisons. LACP n'est pas utilisé.
`Ports`	Une liste séparée par des virgules ou une gamme de ports à agréger dans le Link Aggregation Group (LAG) ou port trunk.

4. Cliquez sur **Apply**.

9.3.3.3 Suppression d'un groupe d'agrégation de liens (Link Aggregation Group)

Procédez comme suit pour supprimer un Link Aggregation Group (LAG), ou *port trunk* :

1. Accédez à ***Link Aggregation » Configure Port Trunks***. Le tableau **Port Trunks** s'affiche.
2. Sélectionnez le LAG souhaité dans le tableau. Le formulaire **Port Trunks** s'affiche.
3. Cliquez sur **Delete**.

9.3.3.4 Affichage de l'état des Link Aggregation Groups

Pour afficher l'état de chaque Link Aggregation Group (LAG) ou *port trunk* configurés sur l'appareil, accédez à ***Link Aggregation » View Port Trunk Statistics***. Le tableau **Port Trunk Statistics** s'affiche.

Ce tableau affiche les informations suivantes sur chaque LAG :

Paramètre	Description
`Trunk ID`	ID du Link Aggregation Group (LAG), ou port trunk (agrégation de ports).
`Mode`	Mode d'agrégation de liaisons. Options possibles : • `LACP`– L'agrégation de liaisons est effectuée de façon dynamique à l'aide de LACP pour les deux côtés du partenariat de l'agrégation de liaisons. • `Static`– Les paramètres d'agrégation de liaisons sont configurés manuellement sur les deux côtés du partenariat de l'agrégation de liaisons. LACP n'est pas utilisé.
`State`	État opérationnel du Link Aggregation Group (LAG), ou port trunk.
`Ports Aggregated`	Une liste séparée par des virgules ou une gamme de ports qui sont agrégés et opérationnels dans le Link Aggregation Group (LAG) ou port trunk.

9.3.4 Gestion du Link Aggregation Control Protocol

Le Link Aggregation Control Protocol (LACP) permet aux appareils compatibles LACP d'apprendre de façon dynamique les uns des autres et de créer automatiquement des voies de port basées sur la vitesse maximale de port et l'état d'agrégation. Les fonctionnalités et configuration de chaque appareil n'ont pas besoin d'être expressément contrôlées comme avec une agrégation de liens statique.

Les fonctionnalités des appareils compatibles LACP sont apprises via l'échange de LACP Data Units (LACPDU). Les LACPDU sont distribuées initialement par les ports configurés pour utiliser LACP en mode `Active`. Quand ces LAPDU sont reçues par un appareil compatible LACP voisin, une LACPDU est retournée et les deux appareils négocient la création d'une voie de port. La voie est créée uniquement si les fonctionnalités de tous les appareils correspondent.

Remarque
Évitez de configurer LACP lorsque Layer 3 switching est activé. Pour plus d'informations sur l'activation ou la désactivation de Layer 3 switching, voir "*Layer 3 (couche 3)* (Page 199)".

⚠ NOTA

Au moins un appareil compatible LACP doit avoir un port configuré pour utiliser LACP en mode `Active`. Les ports configurés pour fonctionner en mode `Passive` participent au processus de négociation, mais ne l'initient pas.

Configurez LACP lorsque le paramètre **Mode** pour une agrégation de ports (port trunk) est défini sur `LACP`.

9.3.4.1 Affichage des informations sur le partenaire LACP

Pour afficher des détails sur le système partenaire LACP, accédez à ***Link Aggregation » View Partner LACP Information***. Le tableau **Partner LACP Information** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	Numéro de port.
`System Priority`	Priorité système LACP du système partenaire.
`System ID`	Adresse MAC du système partenaire.
`Port Priority`	Priorité de port LACP du port partenaire.
`Port Number`	Numéro de port LACP du port partenaire.
`Key`	Clé LACP affectée au port partenaire par le système partenaire.
`State`	État opérationnel LACP du port partenaire. L'état est exprimé sous la forme d'une chaîne de huit caractères. Par exemple : `ASAO----` De gauche à droite, chaque caractère de la chaîne a la signification suivante : 1. Activité LACP : A=Active LACP, P=Passive LACP 2. Timeout LACP : S=Short Timeout, L=Long Timeout 3. Agrégation : A=Aggregateable, I=Individual 4. Synchronisation : S=In Sync, O=Out Of Sync 5. Collecte : C=Collecting, -=Not Collecting 6. Distribution : D=Distributing, -=Not Distributing 7. En défaut : D=Defaulted Info, -=Received Info 8. Expiré : E=Expired, -=Not Expired
`Version`	**Synopsis :** Un entier compris entre 0 et 255 Numéro de version des paquets LACP envoyés par le système partenaire.

9.3.4.2 Configuration des réglages globaux LACP

Procédez comme suit pour configurer les réglages globaux pour Link Aggregation Control Protocol (LACP) :

1. Accédez à ***Link Aggregation » Configure Global LACP Parameters***. Le formulaire **Global LACP Parameters** s'affiche.

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

Paramètre	Description
`Bridge LACP Priority`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 32768 Priorité système LACP. Elle est combinée avec l'adresse MAC de l'appareil pour former l'ID système LACP utilisée dans les négociations avec les autres appareils à LACP activé.
`LAG Ports Selection Rule`	**Synopsis :** [ActivePartner | LinkSpeed | LinkPriority] **Par défaut :** ActivePartner Définit l'ordre dans lequel les ports dans le Link Aggregation Group (LAG) ou port trunk sont sélectionnés par LACP pour l'agrégation. Ce paramètre s'applique lorsque les ports du LAG sont connectés à deux autres LAG ou plus. Options possibles : • `ActivePartner`– Sélectionner des ports en fonction du moment où des ports partenaires deviennent actifs. • `LinkSpeed`– Sélectionner des ports en fonction de la vitesse de transmission. Le port avec la vitesse de transmission la plus élevée prévaut. • `LinkPriority`– Sélectionner des ports en fonction de la priorité de liaison LACP. Le port avec la priorité de liaison LACP la plus élevée prévaut.

3. Cliquez sur **Apply**.

9.3.4.3 Configuration de LACP par port

Procédez comme suit pour configurer les réglages de Link Aggregation Control Protocol (LACP) pour un port spécifique :

1. Accédez à ***Link Aggregation » Configure Port LACP Parameters***. Le tableau **Port LACP Parameters** s'affiche.
2. Sélectionnez le port souhaité. Le formulaire **Port LACP Parameters** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`Mode`	**Synopsis :** [Active | Passive] **Par défaut :** Passive Définit le mode LACP pour le port. Options possibles : • `Active`– Le port envoie de façon active des paquets LACP, indépendamment du mode du port partenaire. • `Passive`– Le port n'envoie pas de paquets LACP, à moins que le port partenaire ne soit en mode Actif.

Paramètre	Description
	Remarque Pour chaque liaison physique dans le Link Aggregation Group (LAG), ou port trunk, un port partenaire doit être en mode Actif.
`Timeout`	**Synopsis :** [Short | Long] **Par défaut :** Short Définit le temps en secondes (s) d'attente des paquets LACP du port partenaire. Si un paquet LACP n'est pas reçu dans l'intervalle de temps requis, les informations du port partenaire sont invalidées. Options possibles : Options possibles : • `Short`– 3 s • `Long`– 90 s **Remarque** Les paramètres de Timeout doivent être les mêmes pour tous les ports d'un Link Aggregation Group (LAG), ou port trunk.
`Individual`	**Synopsis :** [False | True] **Par défaut :** False Active ou désactive le mode Individual pour le port. Les ports en mode Individual ne peuvent pas être agrégés dans un Link Aggregation Group (LAG), ou port trunk.
`Priority`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 32768 Priorité de port LACP. Elle est combinée avec le numéro de port pour former l'identificateur de port LACP. La priorité de port est prise en compte lorsqu'il faut déterminer si le port doit être en attente.

4. Cliquez sur **Apply**.

9.3.4.4 Affichage des statistiques LACP

Pour afficher les statistiques collectées sur les ports gérés par LACP (Link Aggregation Control Protocol), accédez à ***Link Aggregation » View Port LACP Statistics***. Le tableau **Port LACP Statistics** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	Numéro de port.
`Link`	État de connexion du port.

Paramètre	Description
`State`	**Synopsis :** Un entier compris entre 0 et 255 État opérationnel LACP du port. L'état est exprimé sous la forme d'une chaîne de huit caractères. Par exemple : `ASAO----` De gauche à droite, chaque caractère de la chaîne a la signification suivante : 1. Activité LACP : A=Active LACP, P=Passive LACP 2. Timeout LACP : S=Short Timeout, L=Long Timeout 3. Agrégation : A=Aggregateable, I=Individual 4. Synchronisation : S=In Sync, O=Out Of Sync 5. Collecte : C=Collecting, -=Not Collecting 6. Distribution : D=Distributing, -=Not Distributing 7. En défaut : D=Defaulted Info, -=Received Info 8. Expiré : E=Expired, -=Not Expired
`Tx`	Nombre de paquets LACP transmis par le port.
`Rx`	Nombre de bons paquets LACP reçus par le port.
`RxUnknown`	Nombre de paquets LACP inconnus reçus par le port.
`RxIllegal`	Nombre de paquets LACP illégaux reçus par le port.

9.3.5 Effacement des statistiques d'agrégation de liens

Procédez comme suit pour effacer toutes les statistiques d'agrégation de liens de l'appareil :

1. Accédez à ***Link Aggregation » Clear Link Aggregation Statistics***. Le formulaire **Clear Link Aggregation Statistics** s'affiche.
2. Cliquez sur **Confirm**.

10 Contrôle et classification du trafic

Utilisez les sous-systèmes de contrôle et de classification du trafic pour contrôler le flux des paquets de données vers les interfaces réseau connectées.

10.1 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.

⚠ NOTA

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 trames de gestion de réseau peut se produire en cas de rafales de trafic, ce qui peut entraîner une perte de la connectivité 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 "Configuration de classes de service pour des ports Ethernet spécifiques (Page 269)".

   L'en-tête de chaque trame reçue est d'abord examiné afin de déterminer si la trame est un paquet IP et si **Inspect TOS** est activé dans RUGGEDCOM ROS. La CoS est déterminée dans le champ DSCP.

   Si la trame n'est pas un paquet IP ou si **Inspect TOS** est désactivé, la trame est examinée afin de déterminer si son 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 ne se trouve 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. Si aucune balise n'est présente, 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 haute priorité sur nombre de trames CoS basse priorité transmises peut être configuré. Le cas échéant, les trames CoS basse priorité peuvent être transmises uniquement après les trames CoS élevées.

10.1.1 Configuration globale de classes de service

Procédez comme suit pour configurer des réglages globaux pour les classes de service (CoS) :

1. Accédez à ***Classes of Service » Configure Global CoS Parameters***. Le formulaire **Global CoS Parameters** s'affiche.
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 "Configuration de la priorité pour le mappage CoS (Page 270)" ou "Configuration du mappage DSCP sur CoS (Page 271)".

10.1.2 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.
2. Sélectionnez un port Ethernet. Le formulaire **Port CoS Parameters** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port(s)`	**Synopsis :** Any combination of numbers valid for this parameter Numéro de port de l'appareil (ou liste de ports s'ils sont agrégés dans un port trunk).

Paramètre	Description
`Default Pri`	**Synopsis :** Un entier compris entre 0 et 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, l'adresse MAC priorisée).
`Inspect TOS`	**Synopsis :** [No | Yes] **Par défaut :** No Ce paramètre active ou désactive l'analyse du 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 bits de services différentiés dans le champ TOS.

4. Cliquez sur **Apply**.

10.1.3 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.
2. Sélectionnez un niveau de priorité. Le formulaire **Priority to CoS Mapping** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Priority`	**Synopsis :** Un entier compris entre 0 et 7 **Par défaut :** 0 Valeur de la priorité IEEE 802.1p.
`CoS`	**Synopsis :** [Normal | Medium | High | Crit] **Par défaut :** Normal CoS affectée de manière à recevoir les trames balisées reçues avec la valeur de priorité IEEE 802.1p spécifiée.

4. Cliquez sur **Apply**.

10.1.4 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.
2. Sélectionnez un niveau DSCP. Le formulaire **DSCP to CoS Mapping** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`DSCP`	**Synopsis :** Un entier compris entre 0 et 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.
`Priority`	**Synopsis :** Un entier compris entre 0 et 7 **Par défaut :** 0 Priorité affectée aux 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 "Configuration de classes de service pour des ports Ethernet spécifiques (Page 269)".

11 Services d'horloge

Ce chapitre décrit les fonctionnalités de chronométrage et de synchronisation d'horloge de RUGGEDCOM ROS.

11.1 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.
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 DD, YYYY 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) | UTC+2:00 (Athens, Cairo, Helsinki) | ...] **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 l'heure DTS (heure d'été/hiver) démarre ou s'arrête. Par exemple, sur la plupart du territoire des USA et du Canada, le décalage 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 l'heure DST se termine.

Paramètre	Description
`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 (d) du mois (1 = 1er jour (d), 5 = 5ème/dernier jour (d)) • `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` L'heure DST commence le 2ème dimanche de mars à 2h00 du matin. L'heure DST se termine le 1er dimanche de novembre à 2h00 du matin.
`Current UTC Offset`	**Synopsis :** Un entier compris entre 0 et 1000 **Par défaut :** 36 Le Coordinated Universal Time (UTC) est l'heure standard basée sur le temps atomique international (TAI) avec des secondes intercalaires ajoutées à intervalles irréguliers pour compenser le ralentissement de la rotation de la Terre. Le paramètre Current UTC Offset permet à l'utilisateur d'ajuster la différence entre UTC et TAI. Le Service international de la rotation terrestre et des systèmes de référence (IERS) observe la rotation de la Terre. Un message Bulletin-C est envoyé environ 6 mois à l'avance (janvier et juillet) pour indiquer si une seconde intercalaire doit être ajoutée ou non fin juin et fin décembre. Notez qu'une modification du paramètre Current UTC Offset provoque une interruption temporaire du réseau de synchronisation.
`Leap Second Pending`	**Synopsis :** [No | Yes] **Par défaut :** No Ce paramètre permet à l'utilisateur de gérer l'événement Seconde intercalaire. Une seconde intercalaire est une seconde ajoutée au Coordinated Universal Time (UTC) afin de garantir la synchronisation avec le temps astronomique. Le Service international de la rotation terrestre et des systèmes de référence (IERS) observe la rotation de la Terre. Un message Bulletin-C est envoyé environ 6 mois à l'avance (janvier et juillet) pour indiquer si une seconde intercalaire doit être ajoutée ou non fin juin et fin décembre. Ce paramètre doit être défini au moins 5 minutes avant l'occurrence de l'événement Seconde intercalaire.

11.2 Configuration d'IRIG-B

La sortie TTL peut exécuter différentes fonctions, notamment la transmission du signal de temps de référence IRIG-B ou d'un signal de référence utility Pulse Per Second (PPS) ou Pulse per x Seconds (PPx).

Procédez comme suit pour configurer IRIG-B :

1. Accédez à ***Administration » System Time Manager » Configure IRIGB***. Le formulaire **IRIGB** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`TTL Output`	**Synopsis :** [Off | PWM | PPS | PPx] **Par défaut :** PWM Sélectionne le mode de fonctionnement pour le port de sortie TTL. Le mode PWM est conforme à la norme IRIG 200-04. PPx fournit une impulsion générique par interface de X secondes pour synchroniser des appareils externes.
`PPx Pulse Interval`	**Synopsis :** Un entier compris entre 1 et 86400 **Par défaut :** 1 Sélectionne l'intervalle d'impulsion pour le port de sortie TTL. Ce paramètre est utilisé en combinaison avec PPx afin de fournir une impulsion générique par interface de X secondes pour synchroniser des appareils externes.
`PPx Pulse Width`	**Synopsis :** Un entier compris entre 1 et 200 **Par défaut :** 1 Sélectionne la largeur d'impulsion en millisecondes pour le port de sortie TTL. Ce paramètre est utilisé en combinaison avec PPx afin de contrôler la largeur de l'impulsion.
`PPx Start Time`	**Synopsis :** YYYY/MM/DD HH:MM:SS **Par défaut :** 1970/01/01 00:00:00 Ce paramètre est utilisé en combinaison avec PPx pour définir l'heure de lancement du premier événement PPx. Notez que ce paramètre doit être défini sur au moins 15 secondes avant le démarrage du PPx souhaité. Le premier événement PPx pourrait sinon être perdu.
`AM Output`	**Synopsis :** [Off | AM] **Par défaut :** AM Sélectionne le mode AM (modulation d'amplitude) du port IRIGB. Le mode AM est conforme à la norme IRIG 200-04.
`Time Code`	**Synopsis :** [Bxx0 | Bxx1 | Bxx2 | Bxx3 | Bxx4 | Bxx5 | Bxx6 | Bxx7] **Par défaut :** Bxx4 Cet appareil utilise la convention suivante pour décoder le code horaire IRIGB : la lettre [B] représente le format IRIG-B, [xx] représente [00] pour le mode de fonctionnement PWM/TTL et [12] pour le mode de fonctionnement AM. Par exemple, Bxx7 représente B007 pour le mode de fonctionnement PWM/TTL et

Paramètre	Description
	B127 pour le mode de fonctionnement AM. Veuillez noter que seuls les codes horaires Bxx0, Bxx1, Bxx4 et Bxx5 prennent en charge les extensions IRIGB.
`IRIGB Ext`	**Synopsis :** [Off | IEEE1344 | C37.118-2005 | C37.118-2011] **Par défaut :** Off Les extensions IRIGB utilisent des bits supplémentaires de la portion fonctions de contrôle (Control Functions (CF)) du code horaire IRIGB. Dans cette partie du code horaire, des bits sont désignés pour des fonctionnalités supplémentaires, notamment : année civile, secondes intercalaires, secondes intercalaires en attente, Daylight Saving Time (DST), DST en attente, décalage horaire local et qualité du temps. Veuillez noter que seuls les codes horaires Bxx0, Bxx1, Bxx4 et Bxx5 prennent en charge les extensions IRIGB.
`IRIGB Input`	**Synopsis :** [Off | PWM | AM] **Par défaut :** PWM Sélectionne le mode de fonctionnement pour le port d'entrée IRIGB. Le module IRIGB est en mesure d'interpréter des extensions IRIGB telles que C37.118-2011, C37.118-2005 et IEEE1344.

3. Cliquez sur **Apply**.
4. Si **IRIGB Ext** a été modifié, réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

11.3 Gestion du PTP (Precision Time Protocol)

Le Precision Time Protocol (PTP) est une méthode standard de synchronisation des horloges réseau via Ethernet. RUGGEDCOM ROS prend en charge la version PTP v2 définie par le groupe de travail IEEE 1588 dans la norme IEEE 1588-2008.

PTP est un protocole distribué permettant la synchronisation entre elles de plusieurs horloges dans un réseau. Ces horloges sont organisées au sein d'une hiérarchie de synchronisation maître-esclave avec une horloge *grandmaster* au sommet de la hiérarchie déterminant l'heure de référence pour le système complet. La synchronisation est réalisée via l'échange de messages de synchronisation PTP. Les horloges *esclaves* utilisent les informations de synchronisation dans les messages PTP pour ajuster leur heure sur celle du *maître* dans leur partie de la hiérarchie.

Le protocole PTP s'exécute au sein d'un champ logique appelé *domaine*. L'heure établie via le protocole au sein d'un domaine ne dépend pas de l'heure dans d'autres domaines.

Un système PTP v2 peut consister en une combinaison d'appareils compatibles PTP et non-compatibles PTP. Il existe cinq types d'appareils PTP de base définis dans la norme IEEE 1588-2008 :

- Ordinary Clocks
- Boundary Clocks

- End-to-End Transparent Clocks
- Peer-to-Peer Transparent Clocks
- Management Nodes

RUGGEDCOM ROS prend en charge les modes *Ordinary Clock*, *Peer-to-Peer Transparent Clock*, *Boundary Clock* et *End-to-End Transparent Clock* :

- L'*Ordinary Clock* peut être configurée comme Grandmaster ou comme Slave Clock au sein de la hiérarchie maître-esclave. La sélection d'horloges Grandmaster et Slave est basée sur l'algorithme Best Master Clock (BMC) défini dans la norme IEEE 1588-2008.
- Une *Peer-to-Peer Transparent Clock* transmet tous les messages comme un pont, un routeur ou un répéteur normal. La différence est que la Peer-to-Peer Transparent Clock calcule également la période de rétention (heure de l'envoi du message - heure d'arrivée du message) et le délai de liaison (délai de propagation du paquet entre des ports pairs) et ajoute ces informations au message d'événement PTP (qui comprend des horodatages). Les ports Ethernet sur une Peer-to-Peer Transparent Clock utilisent le mécanisme de délai de pair pour calculer le délai de propagation du paquet entre des ports pairs.
- Une *Boundary Clock* peut être considérée comme passerelle IEEE 1588. Une Boundary Clock transfère les messages PTP entre des régions PTP en mettant en œuvre différents protocoles de transport et de messagerie ou différents profils PTP. Par exemple, un appareil en mode Boundary Clock peut agir en tant que synchronisation d'horloge (esclave PTP) depuis un réseau de télécommunication et en tant que source de distribution de l'heure (maître PTP) dans un environnement de sous-station électrique.
- La *End-to-End Transparent Clock* prend en charge l'utilisation du mécanisme de mesure de délai de bout en bout entre les horloges esclave et maître. Elle transmet tous les messages comme un pont, un routeur ou un répéteur normal. La différence est que la End-to-End Transparent Clock calcule la période de rétention (heure de l'envoi du message - heure d'arrivée du message) et ajoute cette information au message d'événement PTP (qui comprend un horodatage).

Pour plus d'informations sur les fonctionnalités PTP, référez-vous au "Manuel de référence sur les fonctionnalités de synchronisation d'horloge des appareils RUGGEDCOM" disponible à l'adresse https://support.industry.siemens.com/cs/us/en/view/109780448.

11.3.1 Configuration de PTP

Procédez comme suit pour configurer PTP :

1. Définissez le type d'horloge.

   Pour plus d'informations, voir "Configuration globale de PTP (Page 278)".

2. Assurez-vous qu'un VLAN est configuré pour le trafic PTP

   Pour plus d'informations, voir "Configuration d'un VLAN pour le trafic PTP (Page 290)".

3. Configurez les paramètres pour le type d'horloge sélectionné :
   - Pour une **Ordinary Clock**, voir "Configuration d'une Ordinary Clock (Page 279)".
   - Pour une **Transparent Clock**, voir "Configuration d'une Transparent Clock (Page 282)".
   - Pour une **OC and TC clock**, voir "Configuration d'une Ordinary Clock (Page 279)" et "Configuration d'une Transparent Clock (Page 282)".
   - Pour une **Boundary Clock**, voir "Configuration globale d'une Boundary Clock (Page 284)" et "Configuration d'un groupe de ports Boundary Clock (Page 285)".
4. Assurez-vous que le service PTP est activé globalement.

   Pour plus d'informations, voir "Configuration globale de PTP (Page 278)".

11.3.2 Configuration globale de PTP

Procédez comme suit pour configurer des réglages globaux pour PTP :

1. Accédez à ***Administration » System Time Manager » Precision Time Protocol » Configure Global Parameters***. Le formulaire **Global Parameters** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`PTP Enable`	**Synopsis :** [No | Yes] **Par défaut :** No Active le protocole PTP (Precision Time Protocol).
`Clock Type`	**Synopsis :** [Ordinary Clock | Boundary Clock | Transparent Clock | OC and TC] **Par défaut :** Transparent Clock Sélectionne le type d'horloge PTP (Precision Time Protocol).
`Startup Wait`	**Synopsis :** Un entier compris entre 0 et 3600 **Par défaut :** 10 Normalement, le délai de démarrage pour une horloge maître non GPS est inférieure à un maître avec GPS activé (c'est-à-dire le temps nécessaire pour acquérir un verrou GPS). Ce paramètre fournit la possibilité d'amorcer le réseau PTP d'une manière ordonnée.
`Network Class`	**Synopsis :** [IEEE1588 network | Non-IEEE1588 network] **Par défaut :** IEEE1588 network La stabilité du servomécanisme de l'horloge dépend largement de la personnalité du réseau. Ce paramètre permet à l'utilisateur de configurer une personnalité du réseau pour refléter un environnement réseau spécifique. Cela peut signifier, par exemple, que tous les appareils dans la temporisation sont compatibles IEEE1588 (réseau IEEE1588) ou que la

Paramètre	Description
	temporisation comprend également des appareils non-IEEE1588 (réseau non-IEEE1588). Notez que le réseau IEEE1588 est indépendant de la charge de trafic. Seul le mécanisme E2E est applicable à des réseaux non-IEEE1588.
`P2P Request Interval`	**Synopsis :** [1 s | 2 s | 4 s | 8 s | 16 s | 32 s] **Par défaut :** 1 s Sélectionne l'intervalle de demande de délai PTP (intervalle moyen entre des messages de demande de délai successifs) en secondes. Le mécanisme de délai de pair (peer delay) mesure le délai de propagation port à port, tel que le délai de liaison, entre deux ports communicants prenant en charge le mécanisme de délai de pair (peer delay).
`E2E Request Interval`	**Synopsis :** [1 s | 2 s | 4 s | 8 s | 16 s | 32 s] **Par défaut :** 1 s Sélectionne l'intervalle de demande de délai PTP (intervalle moyen entre des messages de demande de délai successifs) en secondes. Le mécanisme de délai E2E (également appelé demande-réponse) mesure le délai de propagation de messages entre des horloges maître et esclave.
`1 Step`	**Synopsis :** [No | Yes] **Par défaut :** Yes Ce paramètre permet à l'utilisateur de configurer la fonctionnalité d'horloge maître à 1 étape ou 2 étapes.

3. Cliquez sur **Apply**.
4. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

11.3.3 Configuration d'une Ordinary Clock

Procédez comme suit pour configurer les réglages d'une Ordinary Clock PTP :

1. Accédez à ***Administration » System Time Manager » Precision Time Protocol » Configure Ordinary Clock Parameters***. Le formulaire **Ordinary Clock Parameters** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Ethernet Ports`	**Synopsis :** Comma-separated list of ports **Par défaut :** 2/1-2/3,4/1-4/3,5/1-5/4,7/1,8/1-8/2 Sélectionne le(s) port(s) Ethernet prenant part aux échanges de messages PTP (Precision Time Protocol). Notez que seuls les modes P2P (Peer-to-Peer) Transparent Clock (TClock), E2E (End-to-End) Transparent Clock et P2P Grandmaster Clock sont pris en charge sur les ports 2/4, 4/4, 6/4 et 7/2.

Paramètre	Description
`PTP Profile`	**Synopsis :** [Power Profile | Default P2P Profile | Utility Profile Level 1 | Default E2E Profile | Custom Profile | Power Profile v2] **Par défaut :** Power Profile Sélectionne le profil d'horloge PTP (Precision Time Protocol). Le profil PTP représente un ensemble de fonctionnalités PTP autorisées applicables à un secteur industriel spécifique. **Remarque** `Profil d'alimentation électrique`représente C37.238.2011. **Remarque** `Profil d'alimentation électrique v2`représente C37.238.2017. **Remarque** `Profile de niveau utilitaire 1`représente IEC/IEEE 61850-9-3 Ed.1.
`Domain Number`	**Synopsis :** Un entier compris entre 0 et 127 ou [254] **Par défaut :** 0 Sélectionne le numéro de domaine PTP (Precision Time Protocol). Un domaine PTP est un regroupement logique d'horloges PTP synchronisées à l'aide du protocole PTP.
`Transport Protocol`	**Synopsis :** [Layer 2 Multicast | Layer 3 Multicast] **Par défaut :** Layer 2 Multicast Sélectionne le protocole de transport réseau pour les messages PTP (Precision Time Protocol).
`Path Delay Mechanism`	**Synopsis :** [Disabled | Peer-to-Peer | End-to-End] **Par défaut :** Peer-to-Peer Sélectionne le mécanisme de délai PTP (Precision Time Protocol). Deux mécanismes sont utilisés dans PTP pour mesurer le délai de propagation entre des ports PTP : le mécanisme de délai P2P (Peer-to-Peer) mesure le délai de propagation port à port, tel que le délai de liaison et la durée de rétention de trame. Le mécanisme P2P est indépendant de l'état de maître ou d'esclave du port PTP. Le mécanisme de délai E2E (End-to-End) mesure le délai de propagation de messages entre des horloges maître et esclave au sein du réseau concerné entier. Notez que le mécanisme P2P n'interagit pas avec les mesures de délai de chemin basées sur le mécanisme de délai E2E (également appelé demande-réponse)
`Desired Clock Accuracy`	**Synopsis :** [50 ns | 100 ns | 250 ns | 1 us | 2.5 us | 10 us | 25 us | 100 us | 250 us | 1 ms | 2.5 ms | 10 ms | 25 ms | 100 ms | 250 ms] **Par défaut :** 1 us Ce paramètre permet à l'utilisateur de configurer la précision d'horloge souhaitée. Cela représente la valeur instantanée du

Paramètre	Description
	décalage d'horloge entre les horloges maître et esclave. Le système génère une alarme si le décalage d'horloge par rapport au maître dépasse la précision souhaitée.
`Priority1`	**Synopsis :** Un entier compris entre 0 et 255 **Par défaut :** 128 Sélectionne la priorité d'horloge PTP (Precision Time Protocol) priority1 pendant l'exécution de l'algorithme BMC (Best Master Clock). Une valeur moins élevée correspond à une priorité plus élevée. L'algorithme BMC sélectionne des horloges parmi celles dont la priority1 a une valeur moins élevée avant celles ayant une valeur plus élevée.
`Priority2`	**Synopsis :** Un entier compris entre 0 et 255 **Par défaut :** 128 Sélectionne la priorité d'horloge PTP (Precision Time Protocol) priority2 pendant l'exécution de l'algorithme BMC (Best Master Clock). Une valeur moins élevée correspond à une priorité plus élevée. Si l'algorithme BMC ne peut pas ordonner les horloges en fonction de la valeur de leur priority1, clockClass, clockAccuracy et scaledOffsetLogVariance, l'attribut priority2 permet la création de jusqu'à 256 priorités à évaluer avant le disjoncteur de couplage. Le disjoncteur de couplage est basé sur l'identité de l'horloge.
`PTP Port Type`	**Synopsis :** [Auto | SlaveOnly | MasterOnly] **Par défaut :** Auto Cette option peut être utilisée pour forcer un port PTP à être un esclave uniquement qui ne passe jamais à l'état de maître. Les fonctionnalités Slave only et Transparent Clock peuvent être combinées.
`Sync Interval`	**Synopsis :** [125 ms | 250 ms | 500 ms | 1 s | 2 s] **Par défaut :** 1 s Sélectionne l'intervalle de synchronisation PTP (Precision Time Protocol) (intervalle moyen entre des messages de synchronisation successifs) en secondes. Les messages de synchronisation sont envoyés de manière périodique par l'horloge maître pour fournir l'heure du jour à des horloges esclave PTP.
`Announce Interval`	**Synopsis :** [1 s | 2 s | 4 s | 8 s | 16 s | 32 s] **Par défaut :** 1 s Sélectionne l'intervalle d'annonce PTP (Precision Time Protocol) (intervalle moyen entre des messages d'annonce successifs) en secondes. Les messages d'annonce sont envoyés de manière périodique par l'horloge maître pour fournir son état et sa caractéristique. Les messages d'annonce sont utilisés pour établir une hiérarchie de synchronisation à l'aide de l'algorithme BMC (Best Master Clock).
`Announce Receipt Timeout`	**Synopsis :** Un entier compris entre 2 et 4 **Par défaut :** 3 Sélectionne le délai d'expiration de la réception de l'annonce PTP (Precision Time Protocol). Ce paramètre spécifie le nombre

Paramètre	Description
	d'intervalles pouvant s'écouler sans réception d'un message d'annonce. Il fait partie de l'algorithme BMC (Best Master Clock). Veuillez noter qu'une modification de ce paramètre peut avoir un effet perturbant.
`Grandmaster ID`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 255 Ce paramètre est spécifique au profil d'alimentation électrique (IEEE C37.238-2011) ou au profil d'alimentation électrique v2 (IEEE C37.238-2017) en fonction de la sélection. Tous les appareils compatibles PTP doivent configurer une instance unique au niveau du réseau de ce paramètre avec une plage de 3 à 254 pour un fonctionnement correct.
`VID`	**Synopsis :** 1 to 4094 or { PVID, Priority tagged, Untagged } **Par défaut :** PVID Identificateur VLAN. Options possibles : • `PVID`– Rejette les trames PTP reçues associées à tout VLAN sauf PVID. Les trames Tx PTP sont balisées avec un PVID. • `Untagged`– Accepte toutes les trames PTP reçues, quel que soit le format de balise ou l'association VLAN. Les trames PTP non balisées sont transmises. • `Priority tagged`– Accepte toutes les trames PTP reçues, quel que soit le format de balise ou l'association VLAN. Les trames PTP balisées avec une priorité sont transmises. • `1 à 4094`– Rejette les trames PTP reçues associées à tout VLAN à l'exception de ce PVID. Les trames Tx PTP sont balisées avec ce PVID si le port est un membre de ce VLAN
`802.1Q Priority`	**Synopsis :** [0 to 7] **Par défaut :** 4 Sélectionne la priorité de message PTP (Precision Time Protocol) sur la base de la spécification IEEE 802.1Q. IEEE 802.1Q définit 8 classes de service différentes, généralement exprimées à l'aide du champ de priorité 3 bits dans un en-tête IEEE 802.1Q ajouté à la trame Ethernet.

3. Cliquez sur **Apply**.
4. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

11.3.4 Configuration d'une Transparent Clock

Procédez comme suit pour configurer les réglages d'une Transparent Clock PTP :

1. Accédez à ***Administration » System Time Manager » Precision Time Protocol » Configure Transparent Clock Parameters***. Le formulaire **Transparent Clock Parameters** s'affiche.

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

Paramètre	Description
`Ethernet Ports`	**Synopsis :** Comma-separated list of ports ou [All] **Par défaut :** All Sélectionne le(s) port(s) Ethernet prenant part aux échanges de messages PTP (Precision Time Protocol). Notez que seuls les modes P2P (Peer-to-Peer) Transparent Clock (TClock), E2E (End-to-End) Transparent Clock et P2P Grandmaster Clock sont pris en charge sur les ports 2/4, 4/4, 6/4 et 7/2.
`PTP Profile`	**Synopsis :** [Power Profile | Default P2P Profile | Utility Profile Level 1 | Default E2E Profile | Custom Profile | Power Profile v2] **Par défaut :** Power Profile Sélectionne le profil d'horloge PTP (Precision Time Protocol). Le profil PTP représente un ensemble de fonctionnalités PTP autorisées applicables à un secteur industriel spécifique. **Remarque** `Profil d'alimentation électrique`représente C37.238.2011. **Remarque** `Profil d'alimentation électrique v2`représente C37.238.2017. **Remarque** `Profile de niveau utilitaire 1`représente IEC/IEEE 61850-9-3 Ed.1.
`Domain Number`	**Synopsis :** Un entier compris entre 0 et 127 **Par défaut :** 0 Sélectionne le numéro de domaine PTP (Precision Time Protocol). Un domaine PTP est un regroupement logique d'horloges PTP synchronisées à l'aide du protocole PTP.
`Transport Protocol`	**Synopsis :** [Layer 2 Multicast | Layer 3 Multicast] **Par défaut :** Layer 2 Multicast Sélectionne le protocole de transport réseau pour les messages PTP (Precision Time Protocol).
`Path Delay Mechanism`	**Synopsis :** [Disabled | Peer-to-Peer | End-to-End] **Par défaut :** Peer-to-Peer Sélectionne le mécanisme de délai PTP (Precision Time Protocol). Deux mécanismes sont utilisés dans PTP pour mesurer le délai de propagation entre des ports PTP : le mécanisme de délai P2P (Peer-to-Peer) mesure le délai de propagation port à port, tel que le délai de liaison et la durée de rétention de trame. Le mécanisme P2P est indépendant de l'état de maître ou d'esclave du port PTP.

Paramètre	Description
	Le mécanisme de délai E2E (End-to-End) mesure le délai de propagation de messages entre des horloges maître et esclave au sein du réseau concerné entier. Notez que le mécanisme P2P n'interagit pas avec les mesures de délai de chemin basées sur le mécanisme de délai E2E (également appelé demande-réponse)
`802.1Q Priority`	**Synopsis :** [0 to 7] **Par défaut :** 4 Sélectionne la priorité de message PTP (Precision Time Protocol) sur la base de la spécification IEEE 802.1Q. IEEE 802.1Q définit 8 classes de service différentes, généralement exprimées à l'aide du champ de priorité 3 bits dans un en-tête IEEE 802.1Q ajouté à la trame Ethernet.

3. Cliquez sur **Apply**.
4. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

11.3.5 Configuration globale d'une Boundary Clock

Procédez comme suit pour configurer les réglages globaux d'une Boundary Clock PTP :

1. Accédez à ***Administration » System Time Manager » Precision Time Protocol » Configure Boundary Clock Parameters » Configure BC Common Parameters***. Le formulaire **BC Common Parameters** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Desired Clock Accuracy`	**Synopsis :** [50 ns | 100 ns | 250 ns | 1 us | 2.5 us | 10 us | 25 us | 100 us | 250 us | 1 ms | 2.5 ms | 10 ms | 25 ms | 100 ms | 250 ms] **Par défaut :** 1 us Ce paramètre permet à l'utilisateur de configurer la précision d'horloge souhaitée. Cela représente la valeur instantanée du décalage d'horloge entre les horloges maître et esclave. Le système génère une alarme si le décalage d'horloge par rapport au maître dépasse la précision souhaitée.
`Priority1`	**Synopsis :** Un entier compris entre 0 et 255 **Par défaut :** 128 Sélectionne la priorité d'horloge PTP (Precision Time Protocol) priority1 pendant l'exécution de l'algorithme BMC (Best Master Clock). Une valeur moins élevée correspond à une priorité plus élevée. L'algorithme BMC sélectionne des horloges parmi celles dont la priority1 a une valeur moins élevée avant celles ayant une valeur plus élevée.

Paramètre	Description
`Priority2`	**Synopsis :** Un entier compris entre 0 et 255 **Par défaut :** 128 Sélectionne la priorité d'horloge PTP (Precision Time Protocol) priority2 pendant l'exécution de l'algorithme BMC (Best Master Clock). Une valeur moins élevée correspond à une priorité plus élevée. Si l'algorithme BMC ne peut pas ordonner les horloges en fonction de la valeur de leur priority1, clockClass, clockAccuracy et scaledOffsetLogVariance, l'attribut priority2 permet la création de jusqu'à 256 priorités à évaluer avant le disjoncteur de couplage. Le disjoncteur de couplage est basé sur l'identité de l'horloge.

3. Cliquez sur **Apply**.
4. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

11.3.6 Configuration d'un groupe de ports Boundary Clock

Procédez comme suit pour configurer les paramètres de Boundary Clock PTP par port :

1. Accédez à ***Administration » System Time Manager » Precision Time Protocol » Configure Boundary Clock Parameters » Configure BC Port Groups***. Le formulaire **BC Port Groups** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Ethernet Ports`	**Synopsis :** Comma-separated list of ports **Par défaut :** None Sélectionne le(s) port(s) Ethernet prenant part aux échanges de messages PTP (Precision Time Protocol). Notez que seuls les modes P2P (Peer-to-Peer) Transparent Clock (TClock), E2E (End-to-End) Transparent Clock et P2P Grandmaster Clock sont pris en charge sur les ports 2/4, 4/4, 6/4 et 7/2.
`Group Name`	**Synopsis :** Any 19 characters Le nom du groupe de ports Boundary Clock identifie uniquement chaque groupe de port.
`PTP Profile`	**Synopsis :** [Power Profile | Default P2P Profile | Utility Profile Level 1 | Default E2E Profile | Custom Profile | Power Profile v2] **Par défaut :** Power Profile Sélectionne le profil d'horloge PTP (Precision Time Protocol). Le profil PTP représente un ensemble de fonctionnalités PTP autorisées applicables à un secteur industriel spécifique.

Paramètre	Description
	Remarque `Profil d'alimentation électrique`représente C37.238.2011. **Remarque** `Profil d'alimentation électrique v2`représente C37.238.2017. **Remarque** `Profile de niveau utilitaire 1`représente IEC/IEEE 61850-9-3 Ed.1.
`Domain Number`	**Synopsis :** Un entier compris entre 0 et 127 ou [254] **Par défaut :** 0 Sélectionne le numéro de domaine PTP (Precision Time Protocol). Un domaine PTP est un regroupement logique d'horloges PTP synchronisées à l'aide du protocole PTP.
`Transport Protocol`	**Synopsis :** [Layer 2 Multicast | Layer 3 Multicast | Layer 3 Unicast] **Par défaut :** Layer 2 Multicast Sélectionne layer 2 (Ethernet) multicast transport, layer 3 (UDP/IP) multicast transport ou layer 3 (UDP/IP) unicast transport pour les messages PTP (Precision Time Protocol).
`Path Delay Mechanism`	**Synopsis :** [Disabled | Peer-to-Peer | End-to-End] **Par défaut :** Peer-to-Peer Sélectionne le mécanisme de délai PTP (Precision Time Protocol). Deux mécanismes sont utilisés dans PTP pour mesurer le délai de propagation entre des ports PTP : le mécanisme de délai P2P (Peer-to-Peer) mesure le délai de propagation port à port, tel que le délai de liaison et la durée de rétention de trame. Le mécanisme P2P est indépendant de l'état de maître ou d'esclave du port PTP. Le mécanisme de délai E2E (End-to-End) mesure le délai de propagation de messages entre des horloges maître et esclave au sein du réseau concerné entier. Notez que le mécanisme P2P n'interagit pas avec les mesures de délai de chemin basées sur le mécanisme de délai E2E (également appelé demande-réponse)
`PTP Port Type`	**Synopsis :** [Auto | SlaveOnly | MasterOnly] **Par défaut :** Auto Cette option peut être utilisée pour forcer un port PTP à être un esclave uniquement qui ne passe jamais à l'état de maître. Les fonctionnalités Slave only et Transparent Clock peuvent être combinées.
`Sync Interval`	**Synopsis :** [125 ms | 250 ms | 500 ms | 1 s | 2 s] **Par défaut :** 1 s Sélectionne l'intervalle de synchronisation PTP (Precision Time Protocol) (intervalle moyen entre des messages de

Paramètre	Description
	synchronisation successifs) en secondes. Les messages de synchronisation sont envoyés de manière périodique par l'horloge maître pour fournir l'heure du jour à des horloges esclave PTP.
`Announce Interval`	**Synopsis :** [1 s | 2 s | 4 s | 8 s | 16 s | 32 s] **Par défaut :** 1 Sélectionne l'intervalle d'annonce PTP (Precision Time Protocol) (intervalle moyen entre des messages d'annonce successifs) en secondes. Les messages d'annonce sont envoyés de manière périodique par l'horloge maître pour fournir son état et sa caractéristique. Les messages d'annonce sont utilisés pour établir une hiérarchie de synchronisation à l'aide de l'algorithme BMC (Best Master Clock).
`Announce Receipt Timeout`	**Synopsis :** Un entier compris entre 2 et 4 **Par défaut :** 3 Sélectionne le délai d'expiration de la réception de l'annonce PTP (Precision Time Protocol). Ce paramètre spécifie le nombre d'intervalles pouvant s'écouler sans réception d'un message d'annonce. Il fait partie de l'algorithme BMC (Best Master Clock). Veuillez noter qu'une modification de ce paramètre peut avoir un effet perturbant.
`Auto Registration`	**Synopsis :** [No | Yes] **Par défaut :** Yes Ce paramètre est spécifique au transport en monodiffusion. Il permet à l'utilisateur d'enregistrer automatiquement l'horloge esclave dans l'horloge maître de monodiffusion comme spécifié dans l'attribut 'Master IP Address'.
`Master IP Address`	**Synopsis :** Any valid IP address Ce paramètre est spécifique au transport en monodiffusion et représente l'adresse IP de l'horloge maître PTP (Precision Time Protocol) de monodiffusion.
`Backup Master IP Address`	**Synopsis :** Any valid IP address Ce paramètre est spécifique au transport en monodiffusion et représente l'adresse IP de l'horloge maître PTP (Precision Time Protocol) de monodiffusion de sauvegarde.
`Grandmaster ID`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 0 Ce paramètre est spécifique au profil d'alimentation électrique (IEEE C37.238-2011) ou au profil d'alimentation électrique v2 (IEEE C37.238-2017) en fonction de la sélection. Tous les appareils compatibles PTP doivent configurer une instance unique au niveau du réseau de ce paramètre avec une plage de 3 à 254 pour un fonctionnement correct.
`VID`	**Synopsis :** 1 to 4094 or { PVID, Priority tagged, Untagged } **Par défaut :** PVID Identificateur VLAN. Options possibles :

Paramètre	Description
	• `PVID`– Rejette les trames PTP reçues associées à tout VLAN sauf PVID. Les trames Tx PTP sont balisées avec un PVID. • `Untagged`– Accepte toutes les trames PTP reçues, quel que soit le format de balise ou l'association VLAN. Les trames PTP non balisées sont transmises. • `Priority tagged`– Accepte toutes les trames PTP reçues, quel que soit le format de balise ou l'association VLAN. Les trames PTP balisées avec une priorité sont transmises. • `1 à 4094`– Rejette les trames PTP reçues associées à tout VLAN à l'exception de ce PVID. Les trames Tx PTP sont balisées avec ce PVID si le port est un membre de ce VLAN
`802.1Q Priority`	**Synopsis :** [0 to 7] **Par défaut :** 4 Sélectionne la priorité de message PTP (Precision Time Protocol) sur la base de la spécification IEEE 802.1Q. IEEE 802.1Q définit 8 classes de service différentes, généralement exprimées à l'aide du champ de priorité 3 bits dans un en-tête IEEE 802.1Q ajouté à la trame Ethernet.

3. Cliquez sur **Apply**.
4. Réinitialisez l'appareil. Pour plus d'informations, voir "Réinitialisation de l'appareil (Page 114)".

11.3.7 Affichage des statistiques PTP

Pour afficher les statistiques d'une horloge PTP (Precision Time Protocol), accédez à ***Administration » System Time Manager » Precision Time Protocol » View PTP Statistics » View PTP Statistics***. Le formulaire **PTP Statistics** s'affiche.

Ce formulaire affiche les informations suivantes :

Remarque
Des paramètres sont disponibles en fonction de l'état de l'appareil.

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`State`	**Synopsis :** Any 31 characters **Par défaut :** None Affiche l'état du nœud PTP (Precision Time Protocol). Si l'appareil est configuré comme Ordinary Clock, ce champ affiche l'état PTP tel que MASTER, SLAVE, LISTENING. Si l'appareil est configuré en tant que Transparent Clock, ce champ reflète simplement le réglage de configuration.

Paramètre	Description
`Current Offset`	**Synopsis :** Un entier compris entre -2147483647 et 2147483647 **Par défaut :** 0 Affiche le temps de décalage actuel en nanosecondes entre les horloges maître et esclave et est calculé comme suit <heure à l'horloge esclave> - <heure à l'horloge maître> selon les spécifications IEEE1588-2008. Veuillez noter que ce paramètre reflète la valeur approximative et peut ignorer l'asymétrie de liaison.
`Servo Status`	**Synopsis :** Chaîne de 15 caractères Affiche l'état du servomécanisme de l'horloge. Le servomécanisme de l'horloge permet de discipliner l'horloge système. Si la précision de l'horloge se trouve dans les limites souhaitées, l'état est défini sur`lock`. Notez qu'une alarme peut être générée en cas de convergence du servomécanisme de l'horloge.
`GM ID`	**Synopsis :** Chaîne de 31 caractères Affiche l'ID Grandmaster PTP (Precision Time Protocol). Notez que l'horloge maître (Master Clock) peut être la même que la Grandmaster Clock.
`Master ID`	**Synopsis :** Chaîne de 31 caractères Affiche l'identité de l'horloge maître PTP (Precision Time Protocol). Notez que l'horloge maître (Master Clock) peut être la même que la Grandmaster Clock.
`Path Delay Mechanism`	**Synopsis :** [Disabled | Peer-to-Peer | End-to-End | ---] **Par défaut :** Peer-to-Peer Sélectionne le mécanisme de délai PTP (Precision Time Protocol). Deux mécanismes sont utilisés dans PTP pour mesurer le délai de propagation entre des ports PTP : le mécanisme de délai P2P (Peer-to-Peer) mesure le délai de propagation port à port, tel que le délai de liaison et la durée de rétention de trame. Le mécanisme P2P est indépendant de l'état de maître ou d'esclave du port PTP. Le mécanisme de délai E2E (End-to-End) mesure le délai de propagation de messages entre des horloges maître et esclave au sein du réseau concerné entier. Notez que le mécanisme P2P n'interagit pas avec les mesures de délai de chemin basées sur le mécanisme de délai E2E (également appelé demande-réponse)
`PeerDelay`	**Synopsis :** Un entier compris entre 0 et 2147483647 **Par défaut :** 0 Affiche le délai de pair (peer delay) en nanosecondes. Le mécanisme de délai de pair (peer delay) mesure le délai de propagation port à port, tel que le délai de liaison, entre deux ports communicants prenant en charge le mécanisme de délai de pair (peer delay).

11.3.8 Configuration d'un VLAN pour le trafic PTP

Procédez comme suit pour configurer un VLAN spécifiquement pour le trafic PTP :

Remarque
Voici les étapes de base pour configurer un VLAN pour le trafic PTP. Certaines configurations réseau peuvent nécessiter une configuration supplémentaire.

1. [Facultatif] Ajouter un VLAN statique Pour plus d'informations sur la configuration d'un VLAN statique, voir "Ajout d'un VLAN statique (Page 176)".
2. Pour chaque port Ethernet transportant le trafic PTP, configurez le PVID de manière à ce qu'il corresponde à l'ID de VLAN configuré dans Étape 1, sinon configurez un port trunk. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
3. Configurez le format PVID pour chaque port Ethernet affecté pour contrôler si le trafic PTP est transporté ou non sous forme de trames balisées ou non balisées. Pour plus d'informations, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".
4. Si le type d'horloge est **Boundary Clock**, affectez un ou plusieurs ID de VLAN uniques ou différents au(x) groupe(s) de ports PTP en fonction du nombre de réseaux PTP utilisés. Pour plus d'informations, voir "Configuration globale d'une Boundary Clock (Page 284)" et "Configuration d'un groupe de ports Boundary Clock (Page 285)".
5. Si le type d'horloge est **Ordinary Clock** ou **OC and TC** , affectez l'ID de VLAN configuré dans Étape 1. Pour plus d'informations, voir "Configuration d'une Ordinary Clock (Page 279)".
6. Assurez-vous que PTP est activé globalement. Pour plus d'informations, voir "Configuration globale de PTP (Page 278)".

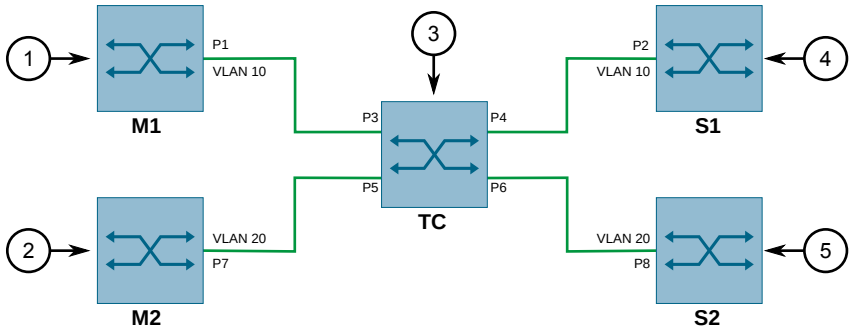
11.3.9 Exemple : configuration de PTP sur plusieurs VLAN

Cet exemple illustre la configuration de plusieurs VLAN pour prendre en charge le trafic PTP.

La topologie suivante décrit un scénario dans lequel le trafic PTP est dirigé via un appareil Transparent Clock (TC) de l'appareil maître 1 (M1) vers l'appareil esclave 1 (S1) sur VLAN 10, et de l'appareil maître 2 (M2) vers l'appareil esclave 2 (S2) sur VLAN 20. Toutes les trames PTP balisées avec un VLAN différent sont abandonnées par les appareils esclaves.

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① Maître 1 (M1)
② Maître 2 (M2)
③ Transparent Clock (TC)
④ Esclave 1 (S1)
⑤ Esclave 2 (S2)

Figure 11.1 Topologie - PTP sur plusieurs VLAN

Procédez comme suit pour configurer des appareils par la topologie :

1. Connectez les ports de l'appareil de la manière suivante :
   - Connectez le port P1 de l'appareil M1 au port P3 de l'appareil TC.
   - Connectez le port P7 de l'appareil M2 au port P5 de l'appareil TC.
   - Connectez le port P2 de l'appareil S1 au port P4 de l'appareil TC.
   - Connectez le port P8 de l'appareil S2 au port P6 de l'appareil TC.
2. Configurez les types de port et les affectations VLAN pour les ports connectant les appareils maître et esclave à la Transparent Clock comme suit :

Appareil	Port(s)	Type	PVID
M1	P1	Trunk	10
S1	P2	Trunk	10
TC	P3, P4	Périphérie	10
M2	P7	Trunk	20
S2	P8	Trunk	20
TC	P5, P6	Périphérie	20

   Pour plus d'informations sur la configuration des types de port, voir "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)".

   Pour plus d'informations sur la configuration des VLAN statiques, voir "Ajout d'un VLAN statique (Page 176)".
3. Configurez les appareils maîtres avec les paramètres suivants :

Paramètre	Valeur	
	M1	M2
Ethernet Ports	1	7
PTP Profile	Power Profile v2	Power Profile v2

Paramètre	Valeur	
	M1	**M2**
Domain Number	254	254
Transport Protocol	Layer 2 Multicast	Layer 2 Multicast
Path Delay Mechanism	Peer-to-Peer	Peer-to-Peer
Desired Clock Accuracy	1 us	1 us
Priority 1	10	10
Priority 2	200	200
PTP Port Type	Auto	Auto
Sync Interval	1 s	1 s
Announce Interval	1 s	1 s
Announce Receipt Timeout	3	3
Grandmaster ID	10	10
VID	PVID	20
802.1Q Priority	4	4

Remarque
Dans ce scénario, le paramètre **VID** peut être soit **PVID** soit le numéro VLAN spécifique. Le paramètre **802.1Q Priority** peut être n'importe quelle valeur entre 0 et 7.

Pour plus d'informations, voir "Configuration d'une Ordinary Clock (Page 279)".

4. Configurez les appareils esclaves avec les paramètres suivants :

Paramètre	Valeur	
	S1	**S2**
Ethernet Ports	2	8
PTP Profile	Power Profile v2	Power Profile v2
Domain Number	254	254
Transport Protocol	Layer 2 Multicast	Layer 2 Multicast
Path Delay Mechanism	Peer-to-Peer	Peer-to-Peer
Desired Clock Accuracy	1 us	1 us
Priority 1	128	128
Priority 2	128	128
PTP Port Type	Auto	Auto
Sync Interval	1 s	1 s
Announce Interval	1 s	1 s
Announce Receipt Timeout	3	3
Grandmaster ID	10	10
VID	10	20

Paramètre	Valeur	
	S1	S2
802.1Q Priority	4	4

Remarque
Dans ce scénario, le paramètre **VID** peut être soit **PVID** soit le numéro VLAN spécifique. Le paramètre **802.1Q Priority** peut être n'importe quelle valeur entre 0 et 7.

Pour plus d'informations, voir "Configuration d'une Ordinary Clock (Page 279)".

5. Configurez l'appareil Transparent Clock (TC) avec les paramètres suivants :

Paramètre	Valeur
Ethernet Ports	3-6
PTP Profile	Power Profile v2
Domain Number	0
Transport Protocol	Layer 2 Multicast
Path Delay Mechanism	Peer-to-Peer
802.1Q Priority	4

Pour plus d'informations, voir "Configuration d'une Transparent Clock (Page 282)".

6. Pour vérifier la configuration, assurez-vous que la Transparent Clock transfère le trafic vers VLAN 10 et VLAN 20 comme configuré et abandonne toutes les trames PTP mal balisées comme suit :
   - L'esclave 1 traite les trames PTP balisées sur VLAN 10 et se verrouille sur l'appareil M1. Les messages PTP de VLAN 20 sont rejetés.
   - L'esclave 2 traite les trames PTP balisées sur VLAN 20 et se verrouille sur l'appareil M2. Les messages PTP de VLAN 10 sont rejetés.

11.4 Configuration de la source de temps

Procédez comme suit pour configurer une source de temps de référence que l'appareil doit utiliser pour l'horloge locale et toutes les sorties de synchronisation d'horloge qui en dépendent :

1. Accédez à ***Administration » System Time Manager » Configure Time Source***. Le formulaire **Time Source** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Primary Time Source`	**Synopsis :** [LOCAL CLK | IRIGB | IEEE1588 | NTP Server | GPS] **Par défaut :** LOCAL CLK Pour sélectionner la source de temps qui disciplinera l'horloge locale. Notez qu'une modification de la source de temps peut

Paramètre	Description
	entraîner une modification d'étape dans l'heure indiquée via l'une quelconque des sorties d'horloges.
`GPS/IRIGB Lock Interval`	**Synopsis :** Un entier compris entre 1 et 120 ou [Forever] **Par défaut :** Forever Intervalle de temps pendant lequel le récepteur GPS/IRIG-B doit acquérir un verrouillage de la source de temps. Normalement, le récepteur GPS (ou IRIG-B) a besoin d'un court intervalle de l'ordre de quelques minutes pour verrouiller le signal. Si l'intervalle de temps expire sans acquisition du verrouillage, le système démarre la distribution de l'heure à l'aide de l'horloge locale.
`GPS Cable Compensation`	**Synopsis :** Un entier compris entre 1 et 50000 ou [none] **Par défaut :** none La compensation de câble peut servir à compenser une longueur de câble importante afin de minimiser l'inexactitude horaire.
`IRIGB Cable Compensation`	**Synopsis :** Un entier compris entre 1 et 50000 ou [none] **Par défaut :** none La compensation de câble peut servir à compenser une longueur de câble importante afin de minimiser l'inexactitude horaire.
`GPS Antenna Power`	**Synopsis :** [On | Off] **Par défaut :** On Le récepteur GPS requiert une antenne active. Une antenne active comprend un préamplificateur qui filtre et amplifie les signaux GPS avant de l'envoyer au récepteur. Cette option permet à l'utilisateur d'activer ou de désactiver l'alimentation de l'antenne GPS. Si l'antenne GPS est partagée entre plusieurs appareils, tous les appareils sauf un doivent l'alimenter.

3. Cliquez sur **Apply**.

11.5 Gestion de NTP

RUGGEDCOM ROS peut être configuré de manière à se référer périodiquement à un serveur NTP spécifié pour corriger le décalage accumulé 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 répondent, une alarme est générée.

11.5.1 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.
2. Sélectionnez **Enabled** pour activer SNTP ou **Disabled** pour désactiver SNTP.
3. Cliquez sur **Apply**.

11.5.2 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.
2. Sélectionnez **Primary** ou **Backup**. Le formulaire **NTP Servers** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Server`	**Synopsis :** Chaîne de 8 caractères **Par défaut :** Primary Ce champ indique si cette configuration est valable pour un serveur principal ou de sauvegarde.
`IP Address`	**Synopsis :** Any valid IP address Adresse IP du serveur.
`Reachable`	**Synopsis :** [No | Yes] État du serveur.
`Update Period`	**Synopsis :** Un entier compris entre 1 et 1440 **Par défaut :** 60 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**.

11.6 Affichage de l'état de sous-systèmes de synchronisation d'horloge

Pour afficher l'état actuel de chaque sous-système de synchronisation d'horloge, accédez à ***Administration » System Time Manager » View Time Sync Status***. Le formulaire **Time Sync Status** s'affiche. Ce formulaire varie en fonction de la source d'heure configurée.

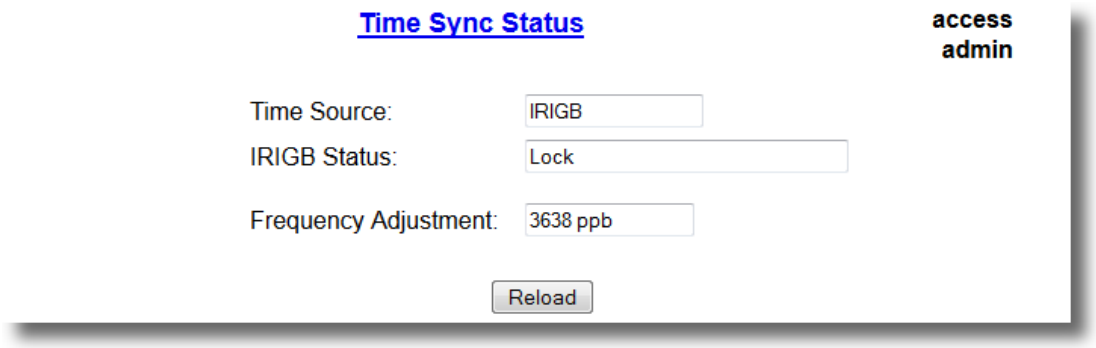


Figure 11.2 Formulaire Time Sync Status (source d'heure IRIG-B)

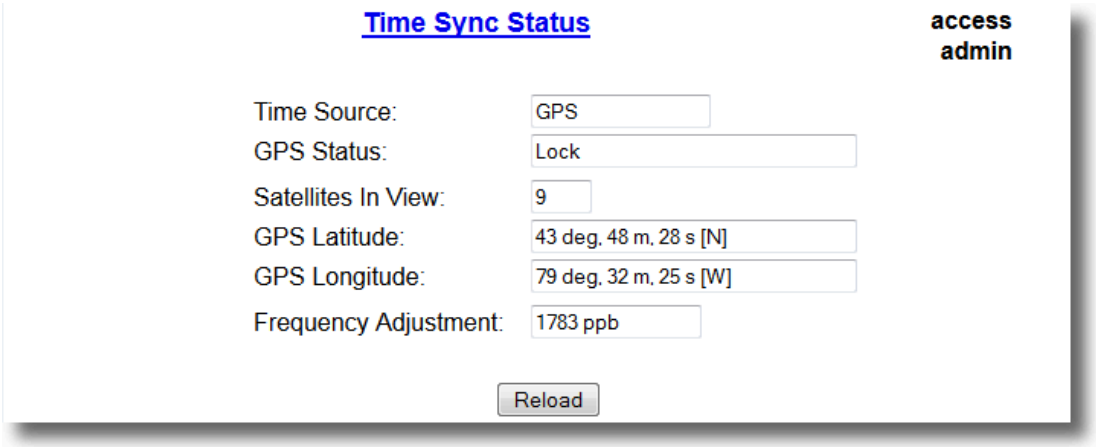


Figure 11.3 Formulaire Time Sync Status (source d'heure GPS)

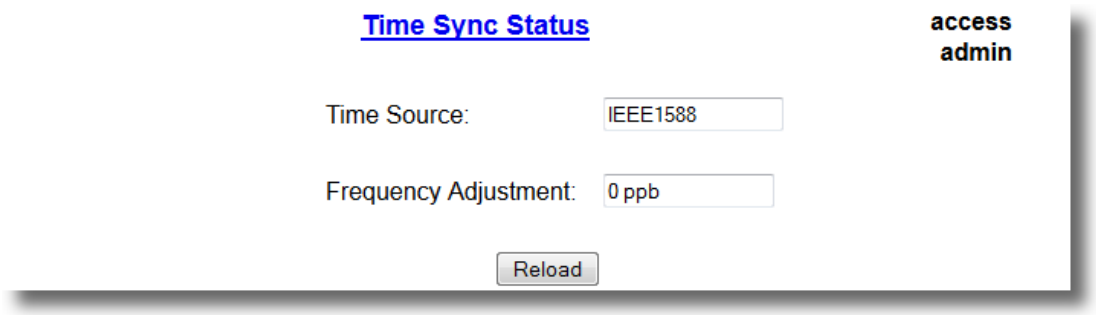


Figure 11.4 Formulaire Time Sync Status (source d'heure IEEE 1588)

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Time Source`	**Synopsis :** [LOCAL CLK | IRIGB | IEEE1588 | NTP Server | GPS] Une source de temps pilotant l'horloge locale.
`GPS Status`	**Synopsis :** [NULL | NotPresent | Disabled | Locked | Searching | Acquiring | Holdover | ParityError | SignalDecodingError | ReceiverShortCircuit | DeviceConfigFailure] État de synchronisation du système par rapport à la source de temps principale sélectionnée.
`IRIGB Status`	**Synopsis :** [NULL | NotPresent | Disabled | Locked | Searching | Acquiring | Holdover | ParityError | SignalDecodingError | ReceiverShortCircuit | DeviceConfigFailure] État de synchronisation du système par rapport à la source de temps principale sélectionnée.
`Satellites in View`	**Synopsis :** Un entier compris entre 0 et 24 Le nombre de satellites (Number of Satellites) indique le nombre de satellites actuellement suivis par le module GPS.
`GPS Latitude`	**Synopsis :** Chaîne de 31 caractères Les champs Latitude et Longitude indiquent la position actuelle de l'antenne GPS. La distance d'une position au nord ou sud de l'Équateur, mesurée en degrés de 0 à 90. Une minute de latitude correspond à un mille marin. La latitude est souvent mesurée en degrés, avec des minutes et des secondes pour affiner les mesures. Un degré est divisé en 60 minutes. Une minute peut être elle-même divisée en 60 secondes.
`GPS Longitude`	**Synopsis :** Chaîne de 31 caractères Les champs Latitude et Longitude indiquent la position actuelle de l'antenne GPS. Distance à l'est ou à l'ouest du premier méridien (mesurée en degrés). Le premier méridien s'étend du pôle nord au pôle sud via Greenwich, en Angleterre. Il s'agit d'une mesure angulaire exprimée en degrés, minutes et secondes.
`SNTP Offset`	**Synopsis :** Un entier compris entre -2147483647 et 2147483646 ou [Acquiring | Holdover] Affiche le décalage horaire actuel entre le serveur (S)NTP et les horloges client, calculé comme "–" .
`Frequency Adjustment`	**Synopsis :** Un entier compris entre -2147483647 et 2147483646 Affiche la quantité de discipline appliquée à la référence de fréquence locale (TCXO) ; c'est-à-dire la quantité de corrections requises sur ce système pour synchroniser la référence actuelle.

12 Découverte et gestion du réseau

RUGGEDCOM ROS prend en charge les protocoles suivants pour la découverte de réseau, la surveillance et la gestion d'appareil automatiques :

- **RUGGEDCOM Discovery Protocol (RCDP)**

  Utiliser RCDP pour découvrir les appareils basés RUGGEDCOM ROS via un réseau de couche 2.

- **LLDP (Link Layer Device Protocol)**

  Utiliser LLDP pour diffuser les fonctionnalités réseau et la configuration aux autres appareils du réseau, ainsi que pour recevoir des diffusions des autres appareils.

- **SNMP (Simple Network Management Protocol)**

  Utiliser SNMP pour notifier des utilisateurs ou des groupes sélectionnés de certains événements qui se produisent durant le fonctionnement de l'appareil, tels que des changements de topologie réseau, l'état de liaison, la racine spanning tree, etc.

12.1 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.

RUGGEDCOM EXPLORER et SINEC PNI de Siemens sont des applications Windows légères et autonomes prenant en charge RCDP. Ils sont 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.
- Mises à jour du firmware.

Remarque
Pour plus d'informations sur l'utilisation de RUGGEDCOM EXPLORER, voir le "manuel de configuration de RUGGEDCOM EXPLORER".

Pour plus d'informations sur l'utilisation de SINEC PNI, voir les "Instructions de service SINEC PNI".

Pour les liens vers ces manuels, voir "Documents liés (Page xv)".

Pour des raisons de sécurité, RUGGEDCOM ROS tente de désactiver RCDP ou de mettre tous les appareils en mode *Get Only* lorsque RUGGEDCOM EXPLORER est fermé.

De plus, RUGGEDCOM ROS met tous les appareils en mode *Get Only* dans les conditions suivantes :

- 60 minutes après la réception de la dernière trame RCDP.
- 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.

⚠ NOTA

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 requêtes 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 » RuggedCom Discovery Protocol » Configure RCDP Parameters***. Le formulaire **RCDP Parameters** s'affiche.

2. Sous **RCDP Discovery**, sélectionnez l'une des options suivantes :

   ⚠ NOTA

   L'option `Enabled` est uniquement disponible pour les appareils chargés avec les paramètres d'usine par défaut. Cette option ne sera plus disponible une fois l'appareil configuré.

   - `Disabled` – Désactive l'accès en lecture et écriture
   - `Get Only` – Active l'accès en lecture seule
   - `Enabled` – Active l'accès en lecture et écriture

3. Cliquez sur **Apply**.

12.2 Gestion de LLDP

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)) contenant 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.

12.2.1 Configuration globale du LLDP

Procédez comme suit pour configurer les réglages globaux pour LLDP :

1. Accédez à ***Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters***. Le formulaire **Global LLDP Parameters** s'affiche.
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 lorsqu'il est activé globalement avec le réglage de l'activation par port dans le menu Port LLDP Parameters.
`Tx Interval`	**Synopsis :** Un entier compris entre 5 et 32768 **Par défaut :** 30 Intervalle auquel les trames LLDP sont transmises au nom de cet agent LLDP.
`Tx Hold`	**Synopsis :** Un entier compris entre 2 et 10 **Par défaut :** 4 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 :** Un entier compris entre 1 et 10 **Par défaut :** 2 Délai en secondes pendant lequel la valeur du paramètre Admin Status d'un port spécifique est 'Disabled' jusqu'à une nouvelle tentative de réinitialisation.
`Tx Delay`	**Synopsis :** Un entier compris entre 1 et 8192 **Par défaut :** 2 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**.

12.2.2 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.
2. Sélectionnez un port. Le formulaire **Port LLDP Parameters** s'affiche.

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

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Numéro de port.
`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 ne peut ni transmettre ni recevoir des trames LLDP.
`Notifications`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled La désactivation des notifications empêche l'envoi de notifications et la génération d'alarmes pour un port spécifique depuis l'agent LLDP.

4. Cliquez sur **Apply**.

12.2.3 Affichage de statistiques globales et d'informations système annoncées

Pour afficher des statistiques globales concernant LLDP 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.

Ce formulaire affiche les informations suivantes :

Paramètre	Description
`Inserts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre d'insertions de l'entrée dans le tableau LLDP Neighbor Information.
`Deletes`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de suppressions de l'entrée du tableau LLDP Neighbor Information.
`Drops`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre de suppressions d'une entrée du tableau LLDP Neighbor Information en raison de l'expiration de l'intervalle d'exactitude de l'information.

Paramètre	Description
`Ageouts`	**Synopsis :** Un entier compris entre 0 et 4294967295 Compteur de toutes les TLV rejetées.

12.2.4 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.

Ce formulaire affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Port local associé à cette entrée.
`ChassisId`	**Synopsis :** Chaîne de 45 caractères Information d'ID de châssis reçue de l'agent LLDP distant.
`PortId`	**Synopsis :** Chaîne de 45 caractères Information d'ID de port reçue de l'agent LLDP distant.
`SysName`	**Synopsis :** Chaîne de 45 caractères Information de nom du système reçue de l'agent LLDP distant.
`SysDesc`	**Synopsis :** Chaîne de 45 caractères Information de descripteur du système reçue de l'agent LLDP distant.

12.2.5 Affichage des statistiques pour les ports LLDP

Pour afficher les statistiques pour les ports LLDP, accédez à ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics***. Le tableau **LLDP Statistics** s'affiche.

Ce tableau affiche les informations suivantes :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`FrmDrop`	**Synopsis :** Un entier compris entre 0 et 4294967295 Compteur de toutes les trames LLDP rejetées.
`ErrFrm`	**Synopsis :** Un entier compris entre 0 et 4294967295 Compteur de toutes les LLDPDU reçues avec erreurs détectables.

Paramètre	Description
`FrmIn`	**Synopsis :** Un entier compris entre 0 et 4294967295 Compteur de toutes les LLDPDU reçues.
`FrmOut`	**Synopsis :** Un entier compris entre 0 et 4294967295 Compteur de toutes les LLDPDU transmises.
`Ageouts`	**Synopsis :** Un entier compris entre 0 et 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 :** Un entier compris entre 0 et 4294967295 Compteur de toutes les TLV rejetées.
`TLVsUnknown`	**Synopsis :** Un entier compris entre 0 et 4294967295 Compteur de toutes les TLV reçues sur le port non reconnues par l'agent local LLDP.

12.3 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**.

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 et de trap de fonctionnalités d'agent, toutes pour SNMP (Simple Network Management Protocol).

Pour plus d'informations sur les MIB, les fonctionnalités d'agent et les traps pris en charge, voir "*Référence* (Page 347)".

12.3.1 Gestion des utilisateurs SNMP

Cette section décrit la manière de gérer les utilisateurs SNMP.

12.3.1.1 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.

Si aucun utilisateur n'a été configuré, ajoutez des utilisateurs en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un utilisateur SNMP (Page 306)".

12.3.1.2 Ajout d'un utilisateur SNMP

Plusieurs utilisateurs (32 max.) peuvent être configurés pour le moteur SNMPv3 local, ainsi que pour les communautés 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.

Pour les commandes CLI liées à l'ajout d'un utilisateur SNMP, reportez-vous à "Commandes CLI disponibles (Page 26)".

Procédez comme suit pour ajouter un nouvel utilisateur SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Users***. Le tableau **SNMP Users Table** s'affiche.

2. Cliquez sur **InsertRecord**. Le formulaire **SNMP Users** s'affiche.

Remarque
RUGGEDCOM ROS requiert que tous les mots de passe utilisateur 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 être inférieure à 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 "Gestion des alarmes (Page 118)".

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

Paramètre	Description
`Name`	**Synopsis :** Chaîne de 32 caractères **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 :** Any valid IP address 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 SNMP est généré pour piéger les destinataires si la requête est reçue de cet utilisateur mais 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 :** Chaîne de 32 caractères Chaîne de communauté, mappée par cet utilisateur/ce nom de 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.

Paramètre	Description
`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 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 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 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 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**.

12.3.1.3 Suppression d'un utilisateur SNMP

Pour les commandes CLI liées à la suppression d'un utilisateur SNMP, reportez-vous à "Commandes CLI disponibles (Page 26)".

Procédez comme suit pour supprimer un utilisateur SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Users***. Le tableau **SNMP Users Table** s'affiche.
2. Sélectionnez l'utilisateur dans le tableau. Le formulaire **SNMP Users** s'affiche.
3. Cliquez sur **Delete**.

12.3.2 Gestion du mappage sécurité sur groupe

Cette section décrit la configuration et la gestion des mappages sécurité sur groupe.

12.3.2.1 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.

Si aucun mappage sécurité sur groupe n'a été configuré, ajoutez des mappages en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un mappage sécurité sur groupe (Page 309)".

12.3.2.2 Ajout d'un mappage sécurité sur groupe

Plusieurs combinations de modèles et de groupes de sécurité peuvent être mappées (32 max.) pour SNMP.

Pour les commandes CLI liées à l'ajout d'un mappage sécurité sur groupe SNMP, reportez-vous à "Commandes CLI disponibles (Page 26)".

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 Table** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **SNMP Security to Group Maps** s'affiche.
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 :** Chaîne de 32 caractères Nom d'utilisateur mappé par cette entrée sur le nom de groupe spécifié.
`Group`	**Synopsis :** Chaîne de 32 caractères 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**.

12.3.2.3 Suppression d'un mappage sécurité sur groupe

Pour les commandes CLI liées à la suppression d'un mappage sécurité sur groupe SNMP, reportez-vous à "Commandes CLI disponibles (Page 26)".

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 Table** s'affiche.
2. Sélectionnez le mappage dans le tableau. Le formulaire **SNMP Security to Group Maps** s'affiche.
3. Cliquez sur **Delete**.

12.3.3 Gestion de groupes SNMP

Plusieurs groupes SNMP (jusqu'à 32) peuvent être configurés pour avoir un accès au SNMP.

12.3.3.1 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.

Si aucun groupe SNMP n'a été configuré, ajoutez des groupes en fonction de vos besoins. Pour plus d'informations, voir "Ajout d'un groupe SNMP (Page 310)".

12.3.3.2 Ajout d'un groupe SNMP

Pour les commandes CLI liées à l'ajout d'un groupe SNMP, reportez-vous à "Commandes CLI disponibles (Page 26)".

Procédez comme suit pour ajouter un groupe SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Access***. Le tableau **SNMP Access Table** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **SNMP Access** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Group`	**Synopsis :** Chaîne de 32 caractères Nom du groupe auquel le modèle de sécurité et le nom appartiennent. Ce nom est utilisé comme index du tableau SNMPv3 VACM Access.

Paramètre	Description
`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 à des notifications n'est accordé.

4. Cliquez sur **Apply**.

12.3.3.3 Suppression d'un groupe SNMP

Pour les commandes CLI liées à la suppression d'un groupe SNMP, reportez-vous à "Commandes CLI disponibles (Page 26)".

Procédez comme suit pour supprimer un groupe SNMP :

1. Accédez à ***Administration » Configure SNMP » Configure SNMP Access***. Le tableau **SNMP Access Table** s'affiche.
2. Sélectionnez le groupe dans le tableau. Le formulaire **SNMP Access** s'affiche.
3. Cliquez sur **Delete**.

12.4 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 connus 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

12.4.1 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] 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*[a]

Valeur de registres	*N*[a] x 2 octets	Valeur du registre

[a] 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)

12.4.2 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 de référence 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
0042	1	Nombre d'alarmes	L	Uint16
0043	1	État de l'alimentation	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 de référence dans l'interface utilisateur)	L/E	Format
0080	1	Effacer les alarmes	O	Cmd
0081	2	Réinitialiser les ports Ethernet	O	PortCmd
0083	2	Effacer les statistiques Ethernet	O	PortCmd

Alarmes

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

Adresse	Nombre de registres	Description (tableau de référence dans l'interface utilisateur)	L/E	Format
0100	64	Alarme 1	L	Alarme
0140	64	Alarme 2	L	Alarme
0180	64	Alarme 3	L	Alarme

Adresse	Nombre de registres	Description (tableau de référence dans l'interface utilisateur)	L/E	Format
01C0	64	Alarme 4	L	Alarme
0200	64	Alarme 5	L	Alarme
0240	64	Alarme 6	L	Alarme
0280	64	Alarme 7	L	Alarme
02C0	64	Alarme 8	L	Alarme

État des ports Ethernet

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

Adresse	Nombre de registres	Description (tableau de référence 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 de référence 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

Adresse	Nombre de registres	Description (tableau de référence dans l'interface utilisateur)	L/E	Format
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
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

Adresse	Nombre de registres	Description (tableau de référence dans l'interface utilisateur)	L/E	Format
0452	2	Statistiques du port s3/p2 - Paquets Ethernet sortants	L	Uinst32
0454	2	Statistiques du port s3/p3 - Paquets Ethernet sortants	L	Uinst32
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 de référence 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
04B6	2	Statistiques du port s8/p2 - Paquets Ethernet entrants	L	Uinst32
04C0	2	Statistiques du port s1/p1 - Paquets Ethernet sortants	L	Uinst32

Adresse	Nombre de registres	Description (tableau de référence dans l'interface utilisateur)	L/E	Format
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
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

Adresse	Nombre de registres	Description (tableau de référence dans l'interface utilisateur)	L/E	Format
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

12.4.3 Formats de mémoire Modbus

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

12.4.3.1 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).

12.4.3.2 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, on envisage 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

12.4.3.3 Uint16

Le format Uint16 décrit un registre 16 bits Modbus standard.

12.4.3.4 Uint32

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

12.4.3.5 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

12.4.3.6 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.

12.4.3.7 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)

Valeur des bits	Description
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.

12.4.3.8 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.

13 Affectation d'adresse IP

Ce chapitre décrit les fonctionnalités relatives à l'affectation d'adresses IP.

13.1 Gestion de DHCP

Le Dynamic Host Configuration Protocol (DHCP) est un protocole de communication qui permet aux administrateurs réseau de gérer et d'automatiser de manière centralisée la configuration réseau d'appareils attachés à un réseau Internet Protocol (IP).

13.1.1 Concepts DHCP

La section suivante décrit des concepts importants de configuration et d'application de DHCP.

13.1.1.1 Espionnage DHCP (DHCP Snooping)

L'espionnage DHCP est une fonctionnalité de sécurité réseau qui protège le réseau de serveurs DHCP et de clients non fiables en surveillant les ports sur lesquels les clients et serveurs DHCP se trouvent. Ces informations sont suivies par la création d'un tableau DHCP Binding qui contient toutes les associations MAC-IP que le commutateur a apprises en espionnant les communications client et serveur DHCP. Le tableau de liaison contient les informations MAC-IP qui peuvent être également utilisées par des applications d'espionnage DHCP. RUGGEDCOM ROS consigne des messages dans le journal système et/ou génère une alarme en cas de détection de violations DHCP.

Remarque
L'espionnage DHCP est activé sur l'appareil par VLAN. Pour plus d'informations sur l'activation de l'espionnage DHCP sur des VLAN individuels, voir "Gestion de VLAN statiques (Page 176)".

13.1.1.2 Ports fiables et non fiables

L'espionnage DHCP classe les ports en fiables et non fiables. Cette classification de ports détermine la manière dont un message DHCP est traité par le commutateur. Les messages DHCP reçus sur des ports fiables sont transmis sans vérification supplémentaire, alors que des messages reçus de ports non fiables sont vérifiés

afin de déterminer si le message est légitime. L'utilisateur doit configurer les ports comme fiables ou non fiables.

Du point de vue du déploiement, l'utilisateur doit configurer les ports du réseau comme fiables. Les ports du réseau se connectent généralement à un autre commutateur ou routeur. Cela est nécessaire car un serveur DHCP peut ne pas être connecté directement à un port de commutateur.

Pour plus d'informations sur la configuration de ports comme fiables ou non fiables, voir "Configuration de ports fiables/non fiables (Page 333)".

13.1.1.3 DHCP Relay Agent (Option 82) (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 requête 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 requêtes 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.

Par exemple, l'ID de circuit pour un client connecté au VLAN 1 sur le port 3/1 à l'aide de la formule suivante est `00:01:00:09`.

```
({slot} - 1)*4 + {port}
```

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).

Pour plus d'informations sur la configuration du DHCP Relay Agent, voir "Configuration du DHCP Relay Agent (agent de relais DHCP) (Page 331)".

13.1.1.4 Inspection ARP dynamique

L'inspection ARP dynamique (Dynamic ARP Inspection (DAI)) est une application d'espionnage DHCP qui valide les paquets ARP (Address Resolution Protocol) dans un réseau. DAI filtre les paquets ARP avec des liaisons d'adresse IP à MAC non valides. De

cette manière, le réseau est protégé d'attaques de type "intercepteur". L'inspection ARP dynamique garantit que seules les demandes et réponses ARP valides sont relayées.

Remarque
L'inspection ARP dynamique ne peut être activée que si l'espionnage DHCP est activé sur l'appareil.

Les paquets de demande et de réponse ARP entrant sur des ports non fiables sont interceptés par l'appareil et soumis à une validation. Les paquets ARP ne sont pas interceptés sur des ports configurés comme fiables. L'utilisateur doit configurer les ports réseau comme *fiables* afin que le trafic ARP entre les appareils ne soit pas soumis à une inspection.

Les champs de l'adresse MAC de l'émetteur et l'adresse IP de l'émetteur dans les paquets de demande/réponse ARP sont validés selon l'entrée de liaison MAC-IP présente dans le tableau de liaison DHCP Snooping. Si aucune entrée de liaison n'est présente dans le tableau, ou si les informations dans l'entrée ne correspondent pas, le paquet de demande/réponse ARP est abandonné.

Pour plus d'informations sur les statistiques d'inspection ARP, voir "Affichage des statistiques d'inspection ARP (Page 334)".

13.1.1.5 Tableau DHCP Binding

L'espionnage DHCP (DHCP Snooping) crée et actualise un tableau de liaison à l'aide d'informations extraites de messages DHCP interceptés. Le tableau contient une entrée pour chaque hôte non fiable avec une adresse IP louée du serveur DHCP. Le tableau ne contient pas d'entrées d'hôtes connectés via des interfaces fiables. La fonctionnalité d'espionnage DHCP met à jour le tableau lorsque le commutateur reçoit des messages DHCP spécifiques.

Lorsque l'appareil est réinitialisé, toutes les informations de liaison MAC-IP apprises par le commutateur sont perdues, à moins que les liaisons apprises ne soient enregistrées dans le fichier de configuration du commutateur.

Si une liaison de port de commutateur est défaillante, toutes les entrées de tableau de liaison apprises de manière dynamique sont supprimées du tableau.

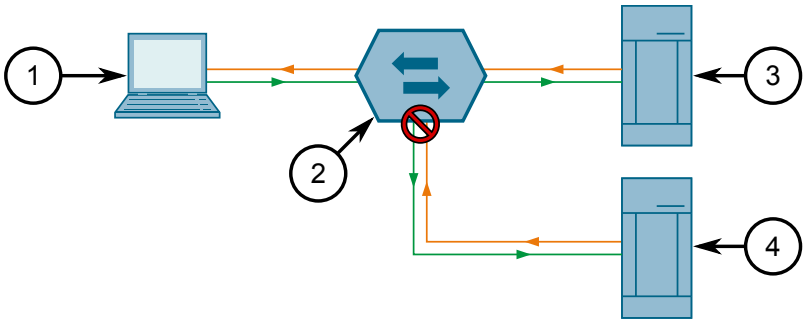
Les enregistrements saisis manuellement peuvent être également configurés à l'aide d'un tableau de liaison statique. Pour plus d'informations sur la configuration du tableau DHCP Binding statique, voir "Ajout d'entrées au tableau DHCP Binding (Page 335)".

13.1.1.6 Attaques de réseau évitables

Les attaques contre des réseaux suivantes peuvent être évitées en activant l'espionnage DHCP et l'inspection ARP dynamique sur le commutateur. Pour plus d'informations, voir "Configuration de l'espionnage DHCP (Page 332)".

- **Configuration erronée de l'hôte par un serveur DHCP non autorisé (Rogue DHCP Server)**

  Un serveur DHCP non autorisé peut affecter une adresse IP, une passerelle par défaut et/ou des paramètres de serveur DNS incorrects au client. Un client configuré de manière incorrecte est vulnérable à une potentielle attaque de réseau. Les commutateurs prenant en charge l'espionnage DHCP peut identifier des messages DHCP depuis un serveur DHCP non autorisé et bloquer ces messages dans le commutateur lui-même.



① Client DHCP
② Commutateur
③ Serveur DHCP
④ Serveur DHCP non autorisé

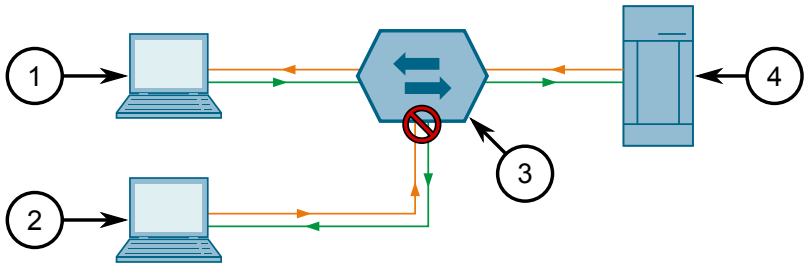
Figure 13.1 Configuration erronée par un serveur DHCP non autorisé

- **Attaque de client DHCP**

  Un client DHCP non autorisé, ou hôte pirate, peut annuler la location pour une adresse IP affectée à un autre client en envoyant un message DHCPRELEASE

au serveur DHCP. Il peut également refuser l'adresse IP pour un autre client en envoyant un message DHCPDECLINE.

L'espionnage DHCP crée un tableau DHCP Binding pour valider la légitimité des messages DHCPRELEASE et DHCPDECLINE. Si la validation de ces messages échoue, ils sont abandonnés par l'appareil.



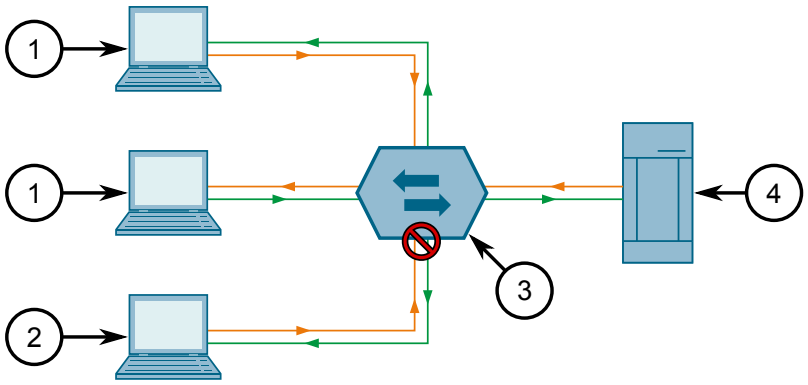
① Client DHCP
② Hôte pirate
③ Commutateur
④ Serveur DHCP

Figure 13.2 Attaque de client DHCP

- **Attaque par privation de DHCP (DHCP Starvation)**

  Une privation de DHCP (DHCP starvation) se produit lorsqu'un serveur DHCP déborde en raison de demandes DHCP depuis un unique client DHCP non autorisé qui a falsifié les adresses matérielles client d'autres clients. Cela épuise le pool d'adresses IP du serveur DHCP, et le serveur n'est plus en mesure de répondre et de fournir de nouvelles locations pour légitimer des clients DHCP. L'espionnage DHCP fournit aux utilisateurs une option permettant de vérifier

l'adresse matérielle client dans le message DHCP-REQUEST et donc d'éviter une attaque par privation (starvation attack).



① Client DHCP
② Pirate
③ Commutateur
④ Serveur DHCP

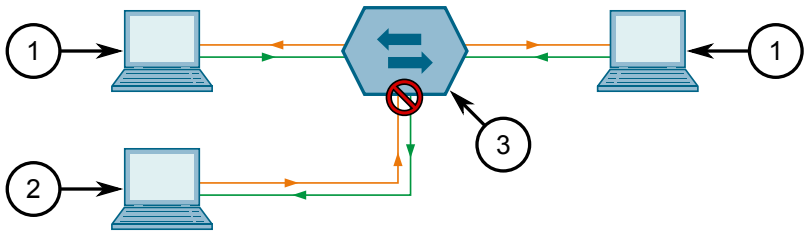
Figure 13.3 Attaque par privation/consommation de DHCP

- **Attaque par falsification d'ARP/Empoisonnement du cache ARP**

  Des attaques par falsification d'ARP et empoisonnement du cache ARP peuvent se produire car l'ARP permet une réponse gratuite par un hôte même si aucune demande ARP n'a été reçue. Après l'attaque, tout le trafic provenant de l'appareil piraté s'écoule vers l'ordinateur du pirate. Une attaque par falsification d'ARP peut cibler des hôtes, des commutateurs et des routeurs connectés à un réseau de couche 2 en empoisonnant les caches ARP de systèmes connectés au sous-réseau et en interceptant le trafic conçu pour d'autres hôtes sur le sous-réseau.

  Une attaque par falsification d'ARP peut être évitée en activant l'inspection ARP dynamique sur le commutateur. Pour plus d'informations sur l'activation de

l'inspection ARP dynamique, voir "Configuration de l'espionnage DHCP (Page 332)".



① Hôte
② Pirate
③ Commutateur

Figure 13.4 Empoisonnement du cache ARP

13.1.2 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.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`DHCP Server Address`	**Synopsis :** Any valid IP address 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 "Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques (Page 331)".

13.1.3 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) :

1. Accédez à ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. Le tableau **DHCP Port Parameters** s'affiche.
2. Sélectionnez un port. Le formulaire **DHCP Port Parameters** s'affiche.

   Remarque
   Le paramètre **Trusted** est configuré comme élément de la fonctionnalité d'espionnage DHCP. Pour plus d'informations, voir "Configuration de ports fiables/non fiables (Page 333)".

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

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`Option-82`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Insère l'option 82 DHCP.

4. Cliquez sur **Apply**.

13.1.4 Configuration de l'espionnage DHCP

Procédez comme suit pour configurer l'espionnage DHCP :

Remarque
L'espionnage DHCP est activé sur l'appareil par VLAN. Pour plus d'informations sur l'activation de l'espionnage DHCP sur des VLAN individuels, voir "Gestion de VLAN statiques (Page 176)".

1. Accédez à ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. Le formulaire **DHCP Parameters** s'affiche.

   Remarque
   Pour plus d'informations sur le paramètre **ARP Inspection**, voir "Activation/désactivation de l'inspection ARP dynamique. (Page 334)".

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

Paramètre	Description
`DHCP Server Address`	**Synopsis :** Any valid IP address 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.

Paramètre	Description
`Verify Hardware Address`	**Synopsis :** [No | Yes] **Par défaut :** Yes Vérifie si l'adresse matérielle du client présente dans le message DHCP reçu sur un port non fiable correspond à l'adresse MAC source.

3. Cliquez sur **Apply**.
4. Configurez les différents ports comme *fiables* ou *non fiables*. Pour plus d'informations, voir "Configuration de ports fiables/non fiables (Page 333)".

13.1.5 Configuration de ports fiables/non fiables

Une fois que l'espionnage DHCP (DHCP Snooping) a été activé, les différents ports doivent être marqués comme *fiables* ou *non fiables*. Les ports connectés au serveur DHCP doivent être *fiables* alors que les ports connectés au client ou à un serveur DHCP non fiable doivent être considérés comme *non fiables*.

Procédez comme suit pour configurer un port comme *fiable* ou *non fiable*.

1. Accédez à ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. Le tableau **DHCP Port Parameters** s'affiche.
2. Sélectionnez un port Ethernet. Le formulaire **DHCP Port Parameters** s'affiche.

Remarque
Le paramètre **Option-82** est configuré comme élément de la fonctionnalité DHCP Relay Agent. Pour plus d'informations, voir "Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques (Page 331)".

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

Paramètre	Description
`Trusted`	**Synopsis :** [No | Yes] **Par défaut :** No Réglage de fiabilité DHCP pour le port.

4. Cliquez sur **Apply**.

13.1.6 Gestion de l'inspection ARP dynamique

Cette section décrit la configuration et la gestion de l'inspection Address Resolution Protocol (ARP) dynamique.

13.1.6.1 Activation/désactivation de l'inspection ARP dynamique.

Procédez comme suit pour activer ou désactiver l'inspection ARP dynamique :

1. Accédez à ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. Le formulaire **DHCP Parameters** s'affiche.
2. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`ARP Inspection`	**Synopsis :** [Disabled | Enabled] **Par défaut :** Disabled Active ou désactive l'inspection ARP dynamique.

3. Cliquez sur **Apply**.

13.1.6.2 Affichage des statistiques d'inspection ARP

Procédez comme suit pour afficher les statistiques d'inspection ARP :

1. Accédez à ***Network Access Control » DHCP Snooping » View ARP Inspection Statistics***. Le tableau **ARP Inspection Statistics** s'affiche.
2. Sélectionnez un port Ethernet. Le formulaire **ARP Inspection Statistics** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`Port`	**Synopsis :** 1/1 to maximum port number Numéro de port.
`In Packets`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre total de paquets ARP entrants traités par l'inspection ARP dynamique sur ce port.
`Dropped Packets`	**Synopsis :** Un entier compris entre 0 et 4294967295 Nombre total de paquets ARP entrants abandonnés par l'inspection ARP dynamique sur ce port.

4. Cliquez sur **Apply**.

13.1.6.3 Effacement des statistiques d'inspection ARP

Procédez comme suit pour effacer les statistiques d'inspection ARP :

1. Accédez à ***Network Access Control » DHCP Snooping » Clear ARP Inspection Statistics***. Le formulaire **Clear ARP Inspection Statistics** s'affiche.
2. Cliquez sur **Confirm**.

13.1.7 Gestion du tableau DHCP Binding

Cette section décrit la configuration et la gestion du tableau DHCP Binding.

13.1.7.1 Ajout d'entrées au tableau DHCP Binding

Le tableau DHCP Binding est renseigné automatiquement avec les informations collectées par RUGGEDCOM ROS sur les hôtes non fiables. Des hôtes spécifiques peuvent également être ajoutés au tableau. Les entrées statiques n'expirent pas et ne sont pas supprimées lors de la désactivation de l'espionnage DHCP ou de la réinitialisation de l'appareil.

Procédez comme suit pour ajouter une entrée statique au tableau DHCP binding :

1. Accédez à ***Network Access Control » DHCP Snooping » Configure Static DHCP Binding Table***. Le tableau **Configure Static DHCP Binding Table** s'affiche.
2. Cliquez sur **InsertRecord**. Le formulaire **Static DHCP Binding Table** s'affiche.
3. Configurez le(s) paramètre(s) suivant(s) en fonction des besoins :

Paramètre	Description
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF **Par défaut :** 00-00-00-00-00-00 Adresse MAC de l'hôte DHCP.
`IP Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to 255 Adresse IP affectée à l'hôte DHCP.
`VID`	**Synopsis :** Un entier compris entre 0 et 65535 **Par défaut :** 1 VLAN dans lequel l'entrée de liaison IP-MAC a été enregistrée.
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Port sur lequel l'entrée de liaison IP-MAC a été enregistrée.

4. Cliquez sur **Apply**.

13.1.7.2 Affichage du tableau DHCP Binding

Procédez comme suit pour afficher le tableau DHCP Binding :

1. Accédez à ***Network Access Control » DHCP Snooping » View DHCP Binding Table***. Le tableau **View DHCP Binding Table** s'affiche.
2. Sélectionnez un port Ethernet. Le formulaire **DHCP Binding Table** s'affiche.

Le tableau DHCP Binding affiche les informations suivantes :

Paramètre	Description
`MAC Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to FF Adresse MAC de l'hôte DHCP.
`IP Address`	**Synopsis :** ##-##-##-##-##-## where ## ranges 0 to 255 Adresse IP affectée à l'hôte DHCP.
`VID`	**Synopsis :** Un entier compris entre 0 et 65535 VLAN dans lequel l'entrée de liaison IP-MAC a été enregistrée.
`Port`	**Synopsis :** 1/1 to maximum port number **Par défaut :** 1/1 Port sur lequel l'entrée de liaison IP-MAC a été enregistrée.
`Type`	**Synopsis :** [Static | Dynamic] Entrées de liaison DHCP IP-MAC dynamiques.
`Lease (secs)`	**Synopsis :** Un entier compris entre 0 et 4294967295 ou [–] Durée de bail affectée à une entrée de liaison dynamique en secondes. Si l'entrée est statique, la durée de bail est infinie et notée comme "– ".

Pour actualiser le tableau, cliquez sur **Reload**.

13.1.7.3 Enregistrement du tableau DHCP Binding

Les informations apprises de manière dynamique et ajoutées au tableau DHCP Binding sont supprimées automatiquement lorsque les événements suivants se produisent :

- La location expire
- L'espionnage DHCP est désactivé
- L'appareil est réinitialisé

Cependant, ces informations peuvent être enregistrées dans le fichier de configuration comme référence ou pour une utilisation future.

Procédez comme suit pour enregistrer le tableau DHCP Binding :

1. Accédez à ***Network Access Control » DHCP Snooping » Save DHCP Binding Table***. Le tableau **Save DHCP Binding Table** s'affiche.
2. Cliquez sur **Confirm**.

13.1.7.4 Exemple : configuration de l'appareil comme Relay Agent

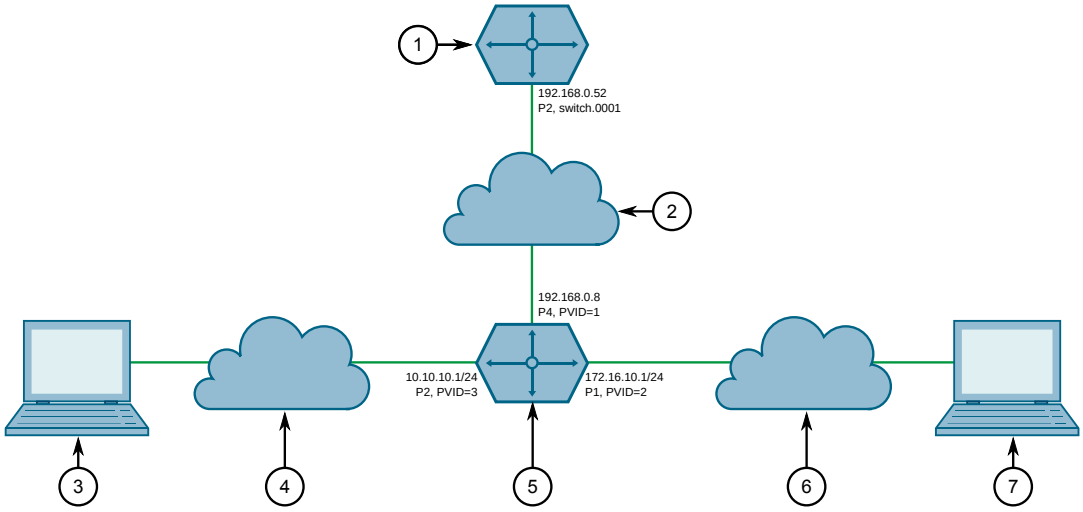
Cet exemple illustre la configuration de l'appareil comme DHCP Relay Agent.

La topologie suivante décrit un scénario où deux clients sur des LAN distincts requièrent des adresses IP sur des sous-réseaux différents d'un serveur DHCP. Chaque

client se connecte au DHCP Relay Agent à l'aide de différents VLAN. Le DHCP Relay Agent gère les requêtes et réponses entre les clients et le serveur DHCP.

⚠ NOTA

Les valeurs indiquées sont spécifiques à la topologie présentée. Les valeurs réelles peuvent varier en fonction de la configuration utilisateur.



① Serveur DHCP
② LAN A
③ Client 2
④ LAN B
⑤ DHCP Relay Agent (appareil RUGGEDCOM ROS)
⑥ LAN C
⑦ Client 1

Figure 13.5 Topologie – Appareil comme Relay Agent

Procédez comme suit pour configurer l'appareil comme DHCP Relay Agent par la topologie :

1. Configurez un appareil distinct comme serveur DHCP. Si le serveur DHCP utilisé est un appareil RUGGEDCOM ROX II, voir le manuel de configuration spécifique à l'appareil pour plus d'informations.

2. Configurez l'appareil RUGGEDCOM ROS comme DHCP Relay Agent :
   a. Ajoutez les VLAN 2 et VLAN 3. Pour plus d'informations, voir "Ajout d'un VLAN statique (Page 176)".
   b. Affecter une adresse IP *192.168.0.8* à VLAN 1. Pour plus d'informations, voir "Ajout d'une interface IP de commutateur (Page 99)".
   c. Modifiez le PVID du port 1 en PVID 2 et modifiez le PVID du port 2 en PVID 3. Consultez "Configuration de VLAN pour des ports Ethernet spécifiques (Page 174)" pour plus d'informations.
   d. Configurez *192.168.0.52* comme adresse de serveur DHCP. Consultez "Configuration du DHCP Relay Agent (agent de relais DHCP) (Page 331)" pour plus d'informations.
   e. Configurez les ports client et serveur DHCP comme suit :

Port	Option 82
1	Activé
2	Activé
4	Désactivé

   Pour plus d'informations sur la configuration du Relay Agent DHCP (Option 82) pour un port spécifique, voir "Activation de l'information de DHCP Relay Agent (Option 82) (Agent de relais DHCP) pour des ports spécifiques (Page 331)".
   f. Pour vérifier la configuration, assurez-vous que le client 1 a pour adresse IP 172.16.10.1/24 et que le client 2 a pour adresse IP 10.10.10.1/24.
3. [Facultatif] Configuration de l'espionnage DHCP :
   a. Activez l'espionnage DHCP sur le serveur DHCP. Si le serveur DHCP utilisé est un appareil RUGGEDCOM ROX II, voir le manuel de configuration spécifique à l'appareil pour plus d'informations.
   b. Assurez-vous que l'option DHCP est activée sur les VLAN 1, 2 et 3. Pour plus d'informations sur l'activation de DHCP pour un VLAN spécifique, voir "Ajout d'un VLAN statique (Page 176)".
   c. Configurer les ports client et serveur DHCP :

      Pour plus d'informations sur la configuration des paramètres de port DHCP, voir "Configuration de ports fiables/non fiables (Page 333)".

Port	Fiable
1	Non
2	Non
4	Oui

      Pour vérifier la configuration, assurez-vous que le client 1 a pour adresse IP 172.16.10.1/24 et que le client 2 a pour adresse IP 10.10.10.1/24.

      Dans le tableau Binding relay agent, assurez-vous que des enregistrements ont été ajoutés pour Port 1 and Port 2 et assurez-vous qu'aucun

enregistrement n'existe pour Port 4. Pour plus d'informations, voir "Affichage du tableau DHCP Binding (Page 335)".

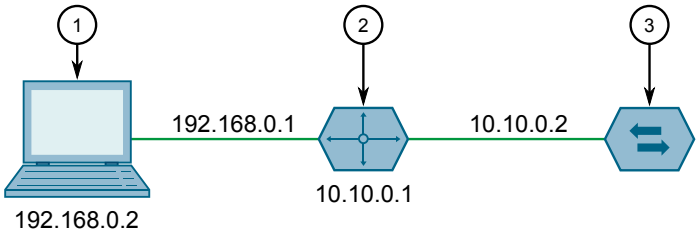
14 Dépannage

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.

⚠ NOTA
Pour obtenir de l'aide, contactez un représentant du service client.

14.1 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.  ① Poste de travail ② Routeur ③ Commutateur Figure 14.1 Utilisation d'un routeur comme passerelle 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. 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.

14.2 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 avec l'autonégociation désactivée 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 autonégociation 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 {destination} {count} {timeout}` peut être utilisée pour envoyer une commande ping au commutateur suivant avec un nombre de demandes d'écho spécifié, séparées par un nombre défini de millisecondes. Par exemple, `ping 192.168.0.1 500 2` génère 500 commandes ping séparé 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.
Des liaisons de port qui étaient stables rencontrent des événements d'activation/ désactivation lorsqu'un nouveau média est introduit.	Il s'agit d'une réaction normale en cas d'introduction d'appareils à fibres optiques. Lorsqu'un appareil à fibres optiques récemment intégré démarre, les ports fibre sont dans un état de transition et, ainsi, les systèmes adjacents activés observeront des événements d'activation/ désactivation de port jusqu'à ce que l'appareil ait terminé sa séquence de démarrage. Cela est dû au fait que les niveaux d'alimentation des émetteurs/récepteurs à fibres varient au cours de la transition de démarrage, faisant ainsi alterner l'état de la liaison connectée. L'installation de câbles à fibres optiques dans un réseau activé provoquera ces effets, tout spécialement pour les connecteurs conçus pour être "keyed" et "locked", tels que les connecteurs ST.
Le syslog distant apparaît pour sauter des événements ou les supprimer de la séquence.	C'est une réaction normale lorsqu'un nouveau commutateur Ethernet est introduit dans un réseau. Dans RUGGEDCOM ROS, la stabilité système et réseau est la première priorité. Lorsqu'un nouveau commutateur Ethernet est introduit dans un réseau, la reconfiguration du réseau a lieu de manière à empêcher la survenue de boucles qui pourraient produire des tempêtes de diffusion. Lorsque cette reconfiguration a lieu, la première priorité est donnée aux messages RSTP et aux opérations de reconfiguration, plutôt qu'aux activités de journalisation des événements.

14.3 Spanning Tree

La présente rubrique décrit les problèmes communs liés à 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 commutateurs 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.
Occasionnellement, les ports rencontrent un important débordement pendant un bref intervalle de temps.	Si le problème semble être de nature temporaire, il est possible que des 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." (Page 344). Une autre cause possible pour un fonctionnement intermittent est une discordance dans l'autonégociation. Si une extrémité de la liaison est fixe en mode duplex intégral alors que le pair exécute une autonégociation, l'extrémité exécutant une autonégociation 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. 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 commutateur a un comportement étrange lorsque le port racine saute entre deux ports de commutateur et ne se stabilise jamais.	
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.

Problème	Solution
	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 est 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 l'autonégociation 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 STP pour le port. Si le contrôleur est défaillant au moment où la liaison est coupée, il se peut que le problème soit causé par une désorganisation ou une duplication des trames. Essayez de définir le port racine du pont du contrôleur défaillant sur STP.
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

Problème	Solution
	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.

14.4 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 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 VLAN 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.

15 Référence

Ce chapitre fournit des informations supplémentaires qui peuvent être nécessaires pour comprendre et/ou configurer les fonctionnalités associées dans RUGGEDCOM ROS.

15.1 MIB standard prises en charge

RUGGEDCOM ROS prend en charge les MIB standard suivantes :

> **⚠ NOTA**
>
> Cette section répertorie toutes les MIB prises en charge par RUGGEDCOM ROS, et est destinée uniquement à des fins de référence. La prise en charge de chaque appareil peut varier.

- **BRIDGE-MIB**

  Pour plus d'informations, voir "BRIDGE-MIB".
- **IEC-62439-3-MIB**

  Pour plus d'informations, voir "IEC-62439-3-MIB".
- **IF-MIB**

  Pour plus d'informations, voir "IF-MIB".
- **IP-MIB**

  Pour plus d'informations, voir "IP-MIB".
- **LLDP-MIB**

  Pour plus d'informations, voir "LLDP-MIB".
- **Q-BRIDGE-MIB**

  Pour plus d'informations, voir "Q-BRIDGE-MIB".
- **RMON-MIB**

  Pour plus d'informations, voir "RMON-MIB".
- **RS-232-MIB**

  Pour plus d'informations, voir "RS-232-MIB".
- **RSTP-MIB**

  Pour plus d'informations, voir "RSTP-MIB".

- **SNMP-FRAMEWORK-MIB**

  Pour plus d'informations, voir "SNMP-FRAMEWORK-MIB".
- **SNMP-USER-BASED-SM-MIB**

  Pour plus d'informations, voir "SNMP-USER-BASED-SM-MIB".
- **SNMPv2-MIB**

  Pour plus d'informations, voir "SNMPv2-MIB".
- **SNMP-VIEW-BASED-ACM-MIB**

  Pour plus d'informations, voir "SNMP-VIEW-BASED-ACM-MIB".
- **TCP-MIB**

  Pour plus d'informations, voir "TCP-MIB".
- **UDP-MIB**

  Pour plus d'informations, voir "UDP-MIB".

BRIDGE-MIB

Groupe/objet	Description
Groupe : dot1dBaseBridgeGroup **Object :** dot1dBaseBridgeAddress	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.1.1.0 **Définition :** adresse MAC utilisée par ce pont lorsqu'il doit être désigné de manière unique. Il est recommandé qu'il s'agisse de l'adresse MAC numériquement la plus petite de tous les ports appartenant à ce pont. Cependant, la seule obligation est que cette adresse soit unique. Lorsqu'il est concaténé avec dot1dStpPriority, un BridgeIdentifier unique est formé, qui est utilisé dans le protocole Spanning Tree.
Groupe : dot1dBaseBridgeGroup **Trap :** dot1dBaseNumPorts	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.1.2.0 **Définition :** nombre de ports contrôlés par cette entité de pontage.
Groupe : dot1dBasePortGroup **Trap :** dot1dBasePort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.1.4.1.1.1 **Définition :** numéro du port pour lequel cette entrée contient des informations de gestion de pont.
Groupe : dot1dBasePortGroup **Trap :** dot1dBasePortCircuit	**Accès :** lecture seule **Syntaxe :** OID **OID :** .1.3.6.1.2.1.17.1.3.1 **Définition :** pour un port qui a (potentiellement) la même valeur de dot1dBasePortIfIndex qu'un autre port sur le même pont. Cet objet contient le nom d'une instance d'objet unique pour ce port. Par exemple, dans le cas où plusieurs ports correspondent un à un à plusieurs circuits virtuels X.25, cette valeur peut identifier une instance d'objet (par exemple, la première) associée au circuit virtuel X.25 correspondant à ce port. Pour un port qui a

Groupe/objet	Description
	une valeur unique de dot1dBasePortIfIndex, cet objet peut avoir la valeur { 0 0 }.
Groupe : dot1dBasePortGroup **Trap :** dot1dBasePortDelayExceededDiscards	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.1.4.1.4.1 **Définition :** nombre de trames rejetées par ce port en raison d'un délai de transit excessif à travers le pont. Il est incrémenté par les ponts de route transparents et source. **Remarque** Le commutateur n'a pas connaissance de la valeur de cet objet. Une valeur nulle est renvoyée en réponse à une requête get.
Groupe : dot1dBasePortGroup **Trap :** dot1dBasePortIfIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.1.4.1.2.1 **Définition :** valeur de l'instance de l'objet ifIndex défini dans IF-MIB, pour l'interface correspondant à ce port.
Groupe : dot1dBasePortGroup **Trap :** dot1dBasePortMtuExceededDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.1.4.1.5.1 **Définition :** nombre de trames rejetées par ce port en raison d'une taille excessive. Il est incrémenté par les ponts de route transparents et source.
Groupe : dot1dBaseBridgeGroup **Trap :** dot1dBaseType	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.1.3.0 **Définition :** indique quel type de pontage ce pont peut effectuer. Si un pont exécute réellement un certain type de pontage, cela sera indiqué par des entrées dans le tableau des ports pour le type donné.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpBridgeForwardDelay	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.14.0 **Définition :** valeur que tous les ponts utilisent pour ForwardDelay lorsque ce pont agit en tant que racine. Notez que 802.1D-1998 spécifie que la plage de ce paramètre est liée à la valeur de dot1dStpBridgeMaxAge. La granularité de cette temporisation est spécifiée par 802.1D-1998 à 1 seconde. Un agent peut renvoyer une erreur badValue si un réglage est tenté à une valeur qui n'est pas un nombre entier de secondes. **Remarque** La valeur de cet objet est arrondie au nombre de dixièmes de seconde le plus proche.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpBridgeHelloTime	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer

Groupe/objet	Description
	OID : .1.3.6.1.2.1.17.2.13.0 **Définition :** valeur que tous les ponts utilisent pour HelloTime lorsque ce pont agit en tant que racine. La granularité de cette temporisation est spécifiée par 802.1D-1998 à 1 seconde. Un agent peut renvoyer une erreur badValue si un réglage est tenté à une valeur qui n'est pas un nombre entier de secondes. **Remarque** La valeur de cet objet est arrondie au nombre de dixièmes de seconde le plus proche.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpBridgeMaxAge	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.12.0 **Définition :** valeur que tous les ponts utilisent pour MaxAge lorsque ce pont agit en tant que racine. Notez que 802.1D-1998 spécifie que la plage de ce paramètre est liée à la valeur de dot1dStpBridgeHelloTime. La granularité de cette temporisation est spécifiée par 802.1D-1998 à 1 seconde. Un agent peut renvoyer une erreur badValue si un réglage est tenté à une valeur qui n'est pas un nombre entier de secondes. **Remarque** La valeur de cet objet est arrondie au nombre de dixièmes de seconde le plus proche.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpDesignatedRoot	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.2.5.0 **Définition :** identificateur de pont de la racine du Spanning Tree, tel que déterminé par le protocole Spanning Tree, tel qu'il est exécuté par ce nœud. Cette valeur est utilisée comme paramètre Root Identifier dans toutes les PDU de pont de configuration créées par ce nœud.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpForwardDelay	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.11.0 **Définition :** cette valeur de temps, mesurée en unités de centièmes de seconde, contrôle la vitesse à laquelle un port change son état de couverture lorsqu'il passe à l'état de transmission (Forwarding). La valeur détermine la durée pendant laquelle le port reste dans chacun des états d'écoute et d'apprentissage, qui précèdent l'état de transmission. Cette valeur est également utilisée lorsqu'une modification de la topologie a été détectée et est en cours, pour vieillir toutes les entrées dynamiques dans la base de données de transmission. [Notez que cette valeur est celle que ce pont utilise actuellement, contrairement à dot1dStpBridgeForwardDelay, qui est la valeur que ce pont et tous les autres commenceraient à utiliser si ce pont devenait la racine.]
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpHelloTime	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.9.0

Groupe/objet	Description
	Définition : durée entre la transmission des PDU de pont de configuration par ce nœud sur un port quelconque lorsqu'il est la racine du Spanning Tree, ou tente de le devenir, en unités de centièmes de seconde. Il s'agit de la valeur réelle que ce pont utilise actuellement.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpHoldTime	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.10.0 **Définition :** cette valeur de temps détermine la durée de l'intervalle pendant lequel pas plus de deux PDU de pont de configuration doivent être transmises par ce nœud, en unités de centièmes de seconde.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpMaxAge	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.8.0 **Définition :** âge maximal des informations du protocole Spanning Tree apprises du réseau sur un port quelconque avant qu'elles ne soient rejetées, en unités de centièmes de seconde. Il s'agit de la valeur réelle que ce pont utilise actuellement.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.15.1.1.1 **Définition :** numéro du port pour lequel cette entrée contient des informations de gestion de protocole Spanning Tree.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortDesignatedBridge	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.2.15.1.8.1 **Définition :** identificateur du pont que ce port considère comme le pont désigné pour le segment de ce port.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortDesignatedCost	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.15.1.7.1 **Définition :** coût du chemin du port désigné du segment connecté à ce port. Cette valeur est comparée au champ Root Path Cost dans les PDU de pont reçues.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortDesignatedPort	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.2.15.1.9.1 **Définition :** identificateur du port sur le pont désigné pour le segment de ce port.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortDesignatedRoot	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.2.15.1.6.1 **Définition :** identificateur de pont unique du pont enregistré en tant que racine dans les BPDU de configuration transmises par le pont désigné pour le segment auquel le port est attaché.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortEnable	**Accès :** lecture et écriture **Syntaxe :** Integer

Groupe/objet	Description
	OID : .1.3.6.1.2.1.17.2.15.1.4.1 **Définition :** état activé/désactivé du port.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortForwardTransitions	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.2.15.1.10.1 **Définition :** nombre de passages de ce port de l'état d'apprentissage à l'état de transmission.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortPathCost	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.15.1.5.1 **Définition :** contribution de ce port au coût des chemins vers la racine du Spanning Tree qui incluent ce port. 802.1D-1998 recommande que la valeur par défaut de ce paramètre soit inversement proportionnelle à la vitesse du LAN attaché. Les nouvelles mises en œuvre doivent prendre en charge dot1dStpPortPathCost32. Si les coûts de chemin de port dépassent la valeur maximale de cet objet, ce dernier doit indiquer la valeur maximale, à savoir 65535. Les applications doivent essayer de lire l'objet dot1dStpPortPathCost32 si cet objet indique la valeur maximale.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortPriority	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.15.1.2.1 **Définition :** valeur du champ de priorité qui est contenue dans le premier octet (dans l'ordre des octets du réseau) de l'ID de port (long de 2 octets). L'autre octet de l'ID de port est donné par la valeur de dot1dStpPort. Sur les ponts prenant en charge IEEE 802.1t ou IEEE 802.1w, les valeurs autorisées sont comprises entre 0 et 240, par pas de 16. **Remarque** Les valeurs autorisées pour cet objet sont comprises entre 0 et 240 par pas de 16 conformément à RFC 4188.
Groupe : rstpPortGroup **Trap :** dot1dStpPortProtocolMigration	**Accès :** lecture et écriture **TruthValue** **OID :** .1.3.6.1.2.1.17.2.19.1.1 **Définition :** lors d'un fonctionnement en mode RSTP (version 2), écrire true(1) sur cet objet force ce port à transmettre des BPDU RSTP. Tout autre fonctionnement sur cet objet n'a aucun effet et renvoie toujours false(2) lors de la lecture.
Groupe : dot1dStpPortGroup **Trap :** dot1dStpPortState	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.15.1.3.1 **Définition :** état actuel du port, tel que défini par l'application du protocole Spanning Tree. Cet état contrôle l'action qu'un port effectue à la réception d'une trame. Si le pont a détecté un port défectueux, il place ce port à l'état broken(6). Pour les ports désactivés (voir dot1dStpPortEnable), cet objet a la valeur disabled(1).
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpPriority	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture et écriture

Groupe/objet	Description
	Syntaxe : Integer **OID :** .1.3.6.1.2.1.17.2.2.0 **Définition :** valeur de la partie inscriptible de l'ID de pont (c'est-à-dire les deux premiers octets de l'ID de pont (long de 8 octets)). Les 6 autres (derniers) octets de l'ID de pont sont donnés par la valeur de dot1dBaseBridgeAddress. Sur les ponts prenant en charge IEEE 802.1t ou IEEE 802.1w, les valeurs autorisées sont comprises entre 0 et 61440, par pas de 4096. **Remarque** Les valeurs autorisées pour cet objet sont comprises entre 0 et 61440 par pas de 4096 conformément à RFC 4188.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpProtocolSpecification	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.1.0 **Définition :** indication de la version du protocole Spanning Tree en cours d'exécution. La valeur `decLb100(2)` indique le protocole DEC LANbridge 100 Spanning Tree. Les mises en œuvre d'IEEE 802.1D renvoient `ieee8021d(3)`. Si les futures versions du protocole IEEE Spanning Tree incompatibles avec la version actuelle sont publiées, une nouvelle valeur est définie.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpRootCost	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.6.0 **Définition :** coût du chemin jusqu'à la racine vu depuis ce pont.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpRootPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.7.0 **Définition :** numéro du port qui offre le chemin de coût le plus faible entre ce pont et le pont racine.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpTimeSinceTopologyChange	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.17.2.3.0 **Définition :** temps (en centièmes de seconde) écoulé depuis la dernière détection d'une modification de topologie par l'entité de pont. Pour RSTP, cela indique le temps écoulé depuis que la temporisation tcWhile pour un port quelconque sur ce pont était différente de zéro. **Remarque** Temps écoulé depuis que la temporisation tcWhile pour un port quelconque sur ce pont était différente de zéro conformément à RFV 4188.
Groupe : dot1dStpBridgeGroup **Trap :** dot1dStpTopChanges	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.2.4.0 **Définition :** nombre total de modifications de la topologie détectées par ce pont depuis la dernière réinitialisation ou initialisation de l'entité de gestion.

Groupe/objet	Description
Groupe : dot1dTpBridgeGroup **Trap :** dot1dTpAgingTime	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.4.2.0 **Définition :** délai d'expiration en secondes pour l'expiration des informations de transmission apprises dynamiquement. 802.1D-1998 recommande une valeur par défaut de 300 secondes. **Remarque** La plage de valeurs valides est limitée à 15 à 800 secondes. La limite inférieure de 15 secondes est une limitation matérielle.
Groupe : dot1dTpFdbGroup **Trap :** dot1dTpFdbAddress	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.4.3.1.1.148.184.197.5.176.0 **Définition :** adresse MAC de monodiffusion pour laquelle le pont dispose d'informations de transmission et/ou de filtrage.
Groupe : dot1dTpFdbGroup **Trap :** dot1dTpFdbPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.4.3.1.2.148.184.197.5.176.0 **Définition :** soit la valeur `0`, soit le numéro du port sur lequel une trame ayant une adresse source égale à la valeur de l'instance correspondante de dot1dTpFdbAddress a été vue. La valeur `0` indique que le numéro de port n'a pas été appris, mais que le pont dispose d'informations de transmission/filtrage sur cette adresse (par exemple, dans dot1dStaticTable). Il est recommandé aux responsables de la mise en œuvre d'affecter la valeur de port à cet objet chaque fois qu'il est appris, même pour les adresses pour lesquelles la valeur correspondante de dot1dTpFdbStatus est not learned(3).
Groupe : dot1dTpFdbGroup **Trap :** dot1dTpFdbStatus	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.4.3.1.3.148.184.197.5.176.0 **Définition :** état de cette entrée. Voici les significations des valeurs : • other(1) - aucune des valeurs suivantes. Cela inclurait le cas où un autre objet MIB (pas l'instance correspondante de dot1dTpFdbPort, ni une entrée dans dot1dStaticTable) est utilisé pour déterminer si et comment les trames adressées à la valeur de l'instance correspondante de dot1dTpFdbAddress sont transmises. • invalid(2) - cette entrée n'est plus valide (par exemple, elle a été apprise mais a expiré depuis), mais n'a pas encore été supprimée du tableau. • learn(3) - la valeur de l'instance correspondante de dot1dTpFdbPort a été apprise et est utilisée. • self(4) - la valeur de l'instance correspondante de dot1dTpFdbAddress représente l'une des adresses du pont. L'instance correspondante de dot1dTpFdbPort indique le port du pont qui possède cette adresse. • mgmt(5) - la valeur de l'instance correspondante de dot1dTpFdbAddress est également la valeur d'une instance existante de dot1dStaticAddress.
Groupe : dot1dTpBridgeGroup **Trap :** dot1dTpLearnedEntryDiscards	**Capacité de l'agent :** RC-BRIDGE-MIB-AC **Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.4.1.0

Groupe/objet	Description
	Définition : nombre total d'entrées de la base de données de transmission qui ont été ou auraient été apprises, mais qui ont été rejetées en raison d'un manque d'espace de stockage dans la base de données de transmission. Si ce compteur est incrémenté, cela indique que la base de données de transmission est régulièrement pleine (une condition qui a des effets négatifs sur les performances du sous-réseau). Si ce compteur a une valeur significative mais n'augmente pas actuellement, cela indique que le problème s'est produit mais n'est pas persistant. **Remarque** Le commutateur n'a pas connaissance de la valeur de cet objet. Une valeur nulle est renvoyée en réponse à une requête get.
Groupe : dot1dTpGroup **Trap :** dot1dTpPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.4.4.1.1.1 **Définition :** numéro du port pour lequel cette entrée contient des informations de gestion de pontage transparent.
Groupe : dot1dTpGroup **Trap :** dot1dTpPortInDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.4.4.1.5.1 **Définition :** nombre de trames valides reçues qui ont été rejetées (c'est-à-dire filtrées) par le processus de transmission.
Groupe : dot1dTpGroup **Trap :** dot1dTpPortInFrames	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.4.4.1.3.1 **Définition :** nombre de trames reçues par ce port depuis son segment. Notez qu'une trame reçue sur l'interface correspondant à ce port n'est comptée par cet objet que si et seulement si c'est pour un protocole en cours de traitement par la fonction de pontage local, y compris les trames de gestion de pont.
Groupe : dot1dTpGroup **Trap :** dot1dTpPortMaxInfo	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.4.4.1.2.1 **Définition :** taille maximale du champ INFO (non-MAC) que ce port reçoit ou transmet.
Groupe : dot1dTpGroup **Trap :** dot1dTpPortOutFrames	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.4.4.1.4.1 **Définition :** nombre de trames transmises par ce port à son segment. Notez qu'une trame transmise sur l'interface correspondant à ce port n'est comptée par cet objet que si et seulement si c'est pour un protocole en cours de traitement par la fonction de pontage local, y compris les trames de gestion de pont.

IEC-62439-3-MIB

Groupe/objet	Description
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntDuplicateA	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.19.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port A pour lesquelles un seul doublon a été reçu.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntDuplicateB	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.20.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port B pour lesquelles un seul doublon a été reçu.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntDuplicateC	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.21.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port C pour lesquelles un seul doublon a été reçu.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntErrorsA	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.11.1 **Définition :** nombre de trames erronées reçues sur ce port LRE A. Valeur initiale = 0.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntErrorsB	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.12.1 **Définition :** nombre de trames erronées reçues sur ce port LRE B. Valeur initiale = 0.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntErrorsC	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.13.1 **Définition :** nombre de trames erronées reçues sur l'interface d'application d'un DANP ou DANH ou sur l'interconnexion d'une RedBox. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntErrWrongLanA	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.5.1 **Définition :** nombre de trames avec un identificateur LAN erroné reçues sur le port LRE A. Valeur initiale = 0. Applicable uniquement aux ports PRP.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntErrWrongLanB	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.6.1 **Définition :** nombre de trames avec un identificateur LAN erroné reçues sur le port LRE B. Valeur initiale = 0. Applicable uniquement aux ports PRP.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntErrWrongLanC	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32

Groupe/objet	Description
	OID : 1.0.62439.2.21.1.1.0.1.1.7.1 **Définition :** nombre de trames avec un identificateur LAN erroné reçues sur l'interconnexion d'une RedBox. Applicable uniquement aux RedBox HSR en configuration HSR-PRP.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntMultiA	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.22.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port A pour lesquelles plusieurs doublons ont été reçus.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntMultiB	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.23.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port B pour lesquelles plusieurs doublons ont été reçus.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntMultiC	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.24.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur l'interface d'application du DAN ou l'interconnexion de la RedBox pour lesquelles plusieurs doublons ont été reçus.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntNodes	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.1.1.0.1.1.14.1 **Définition :** nombre de nœuds dans le tableau de nœuds.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntOwnRxA	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.25.1 **Définition :** nombre de trames balisées HSR reçues sur le port A provenant de cet appareil. Les trames proviennent de cet appareil si le MAC source correspond au MAC de la LRE, ou si le MAC source apparaît dans le tableau de nœuds proxy (si mis en œuvre). Applicable uniquement à HSR. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntOwnRxB	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.26.1 **Définition :** nombre de trames balisées HSR reçues sur le port B provenant de cet appareil. Les trames proviennent de cet appareil si le MAC source correspond au MAC de la LRE, ou si le MAC source apparaît dans le tableau de nœuds proxy (si mis en œuvre). Applicable uniquement à HSR. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntProxyNodes	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.1.1.0.1.1.15.1

Groupe/objet	Description
	Définition : nombre de nœuds dans le tableau de nœuds proxy. Applicable uniquement à la RedBox. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntRxA	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.8.1 **Définition :** nombre de trames reçues sur un port LRE A. Seules les trames balisées HSR ou équipées d'un Redundancy Control Trailer PRP sont comptées. Les trames qui ne sont transmises nulle part (par exemple parce que l'émetteur de la trame se trouve dans le tableau de nœuds proxy) sont également comptées. Seules les trames reçues complètement et sans erreur sont comptées. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntRxB	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.9.1 **Définition :** nombre de trames reçues sur un port LRE B. Seules les trames balisées HSR ou équipées d'un Redundancy Control Trailer PRP sont comptées. Les trames qui ne sont transmises nulle part (par exemple parce que l'émetteur de la trame se trouve dans le tableau de nœuds proxy) sont également comptées. Seules les trames reçues complètement et sans erreur sont comptées. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntRxC	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.10.1 **Définition :** nombre de trames reçues de l'interface d'application d'un DANP ou DANH ou nombre de trames reçues sur l'interconnexion d'une RedBox. Les trames avec et sans balise PRP RCT ou HSR sont comptées, mais pas les trames linklocal. Seules les trames reçues complètement et sans erreur sont comptées. Valeur initiale = 0 **Remarque** Seules les trames reçues sur le port local sont comptées.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntTxA	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.2.1 **Définition :** nombre de trames envoyées sur le port A qui sont balisées HSR ou équipées d'un Redundancy Control Trailer PRP. Seules les trames qui sont balisées HSR ou qui ont un PRP RCT sont comptées. Une trame abandonnée pendant la transmission n'est pas comptée. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntTxB	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.3.1 **Définition :** nombre de trames envoyées sur le port B qui sont balisées HSR ou équipées d'un Redundancy Control Trailer PRP. Seules les trames qui sont balisées HSR ou qui ont un PRP RCT sont comptées. Une trame abandonnée pendant la transmission n'est pas comptée. Valeur initiale = 0
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntTxC	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule

Groupe/objet	Description
	Syntaxe : Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.4.1 **Définition :** nombre de trames envoyées vers l'interface d'application du DANP ou DANH ou sur l'interconnexion de la RedBox. Les trames avec et sans balise PRP RCT ou HSR sont comptées, mais pas les trames link-local. Une trame abandonnée pendant la transmission n'est pas comptée. Valeur initiale = 0 **Remarque** Seules les trames envoyées par le port local sont comptées.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntUniqueA	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.16.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port A pour lesquelles aucun doublon n'a été reçu.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntUniqueB	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.17.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port B pour lesquelles aucun doublon n'a été reçu.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreCntUniqueC	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Counter32 **OID :** 1.0.62439.2.21.1.1.0.1.1.18.1 **Définition :** nombre d'entrées dans le mécanisme de détection des doublons sur le port C pour lesquelles aucun doublon n'a été reçu.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreDuplicateDiscard	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.11.1 **Définition :** spécifie si un algorithme de suppression des doublons est utilisé à la réception. Par défaut : discard.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreEvaluateSupervision	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.16.1 **Définition :** True si la LRE évalue les trames de supervision reçues. False si elle abandonne les trames de supervision sans les évaluer. Remarque : les LRE doivent envoyer des trames de supervision, mais la réception est facultative. La valeur par défaut dépend de la mise en œuvre.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreHsrLREMode	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer

Groupe/objet	Description
	OID : 1.0.62439.2.21.0.1.0.1.1.13.1 **Définition :** cette énumération n'est applicable que si la LRE est un nœud de pontage HSR ou une RedBox. Elle montre le mode de la HSR LRE : • (1) : Mode par défaut : la HSR LRE est en mode h et ponte le trafic HSR balisé. • (2) : Mode facultatif : la HSR LRE est en mode n et le pontage entre ses ports HSR est désactivé. Le trafic est balisé HSR. • (3) : Mode facultatif : la HSR LRE est en mode t et ponte le trafic HSR non balisé entre ses ports HSR. • (4) : Mode facultatif : la HSR LRE est en mode u et se comporte comme en mode h, sauf qu'il ne supprime pas les messages de monodiffusion. • (5) : Mode facultatif : la HSR LRE est configurée en mode mixte. Les trames HSR sont traitées selon le mode h. Les trames non-HSR sont traitées selon les règles de pontage 802.1D. Lorsque le commutateur est en mode HSR, ce réglage de configuration est accessible mais en lecture seule. Valeur : modeh(1). Lorsque le commutateur est en mode PRP, ce réglage n'est pas accessible car il ne s'applique pas.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreInterfaceConfigEntry	**Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1 **Définition :** chaque entrée contient des informations de gestion applicables à une LRE spécifique.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreInterfaceConfigIndex	**Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.1 **Définition :** valeur unique pour chaque LRE.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreInterfaceConfigTable	**Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1 **Définition :** liste des LRE PRP/HSR. Chaque entrée correspond à une entité de redondance de liaison (Link Redundancy Entity, LRE) PRP/HSR, chacune représentant une paire de ports LAN A et B. Les appareils de base prenant en charge PRP/HSR peuvent n'avoir qu'une seule LRE et donc une seule entrée dans le tableau, tandis que des appareils plus complexes peuvent avoir plusieurs entrées pour plusieurs LRE.
Groupe : lreConfigurationGeneralGroup **Trap :** lreInterfaceCount	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.0.2.0 **Définition :** nombre total de LRE présentes dans ce système.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreInterfaceStatsEntry	**Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.1.1.0.1.1 **Définition :** entrée contenant des informations de gestion applicables à une LRE spécifique.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreInterfaceStatsIndex	**Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.1.1.0.1.1.1

Groupe/objet	Description
	Définition : valeur unique pour chaque LRE.
Groupe : lreStatisticsInterfaceGroup **Trap :** lreInterfaceStatsTable	**Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.1.1.0.1 **Définition :** liste des LRE PRP/HSR. Chaque entrée correspond à une entité de redondance de liaison (Link Redundancy Entity, LRE) PRP/HSR, chacune représentant une paire de ports LAN A et B et un port C vers l'application/ l'interconnexion. Les appareils de base prenant en charge PRP/HSR peuvent n'avoir qu'une seule LRE et donc une seule entrée dans le tableau, tandis que des appareils plus complexes peuvent avoir plusieurs entrées pour plusieurs LRE.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreLinkStatusA	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.9.1 **Définition :** indique l'état de connexion réel du port LRE A.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreLinkStatusB	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.10.1 **Définition :** indique l'état de connexion réel du port LRE B.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreMacAddress	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :**MacAddress **OID :** 1.0.62439.2.21.0.1.0.1.1.6.1 **Définition :** spécifie l'adresse MAC à utiliser par cette LRE. Les adresses MAC sont identiques pour tous les ports d'une même LRE.
Groupe : lreConfigurationGeneralGroup **Trap :** lreManufacturerName	**Accès :** lecture seule **Syntaxe :**DisplayString **OID :** 1.0.62439.2.21.0.0.1.0 **Définition :** spécifie le nom du fabricant de l'appareil LRE.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreNodeName	**Accès :** lecture et écriture **Syntaxe :**DisplayString **OID :** 1.0.62439.2.21.0.1.0.1.1.4.1 **Définition :** spécifie le nom de nœud de cette LRE.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreNodesTableClear	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.17.1 **Définition :** spécifie que le tableau de nœuds doit être effacé.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreNodeType	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.3.1 **Définition :** spécifie le mode de fonctionnement de la LRE : • mode PRP 1 (1) • mode HSR (2)

Groupe/objet	Description
	Remarque Le mode PRP 0 est considéré comme obsolète et n'est pas pris en charge par cette révision de la MIB.
Groupe : lreConfigurationInterfaceGroup **Trap :** lrePortAdminStateA	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.7.1 **Définition :** spécifie si le port A doit être actif (active) ou non actif (not Active) via une action administrative. Par défaut : active
Groupe : lreConfigurationInterfaceGroup **Trap :** lrePortAdminStateB	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.8.1 **Définition :** spécifie si le port B doit être actif (active) ou non actif (not Active) via une action administrative. Par défaut : active
Groupe : lreConfigurationInterfaceGroup **Trap :** lreProxyNodeTableClear	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.18 **Définition :** spécifie que le tableau de nœuds proxy doit être effacé.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreRedBoxIdentity	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** non utilisé **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.15 **Définition :** applicable à RedBox HSR-PRP A et RedBox HSR-PRP B. Un ID est utilisé par une paire de RedBox (une configurée A et une configurée B) couplant un anneau HSR à un réseau PRP. La valeur entière indique la valeur du champ de chemin qu'une RedBox insère dans chaque trame qu'elle reçoit de son interconnexion et injecte dans l'anneau HSR. Lorsqu'il est interprété comme des valeurs binaires, LSB désigne la configuration de la RedBox (A ou B), et les 3 bits suivants désignent l'identificateur d'une paire de RedBox.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreRowStatus	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :** RowStatus **OID :** 1.0.62439.2.21.0.1.0.1.1.2 **Définition :** indique l'état de l'entrée du tableau LRE.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreSwitchingEndNode	**Capacité de l'agent :** RC-IEC-62439-3-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.14.1 **Définition :** cette énumération montre la fonctionnalité activée dans cette LRE spécifique : • (1) : un nœud non spécifié qui n'est pas un nœud de pontage, par exemple SRP. • (2) : un nœud de pontage non spécifié, par exemple RSTP. • (3) : un nœud/une RedBox PRP.

Groupe/objet	Description
	• (4) : une RedBox HSR avec un trafic Ethernet régulier sur son interconnexion. • (5) : un nœud de commutation HSR. • (6) : une RedBox HSR avec un trafic balisé HSR sur son interconnexion. • (7) : une RedBox HSR avec un trafic PRP pour LAN A sur son interconnexion. • (8) : une RedBox HSR avec un trafic PRP pour LAN B sur son interconnexion.
Groupe : lreConfigurationInterfaceGroup **Trap :** lreTransparentReception	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.0.62439.2.21.0.1.0.1.1.12.1 **Définition :** si removeRCT est configuré, le RCT est supprimé lors de la transmission vers les couches supérieures, applicable uniquement à PRP LRE (par défaut : removeRCT).
Groupe : lreConfigurationInterfaceGroup **Trap :** lreVersionName	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** 1.0.62439.2.21.0.1.0.1.1.5.1 **Définition :** spécifie la version du logiciel de cette LRE.

IF-MIB

Groupe/objet	Description
Groupe : IfGeneralInformationGroup **Trap :** IfAdminStatus	**Capacité de l'agent :** RC-IEEEC37-238-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.2.1.7.1 **Définition :** état souhaité de l'interface. L'état testing(3) indique qu'aucun paquet opérationnel ne peut être transmis. Lorsqu'un système géré s'initialise, toutes les interfaces sont initialement réglées sur ifAdminStatus à l'état down(2). À la suite d'une action de gestion explicite ou d'informations de configuration conservées par le système géré, ifAdminStatus passe alors à l'état up(1) ou testing(3) (ou reste à l'état down(2)). **Remarque** La prise en charge de la valeur `testing(3)` n'est pas appliquée selon la déclaration de conformité RFC 2863.
Groupe : IfGeneralInformationGroup **Trap :** IfAlias	**Capacité de l'agent :** RC-IF-MIB-AC **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.31.1.1.1.18.1 **Définition :** cet objet est un nom `alias` de l'interface tel que spécifié par un gestionnaire de réseau, et fournit un `handle` non volatile à l'interface. Lors de la première instanciation d'une interface, la valeur d'ifAlias associée à cette interface est une chaîne de longueur nulle. Au fur et à mesure qu'une valeur est écrite dans une instance de ifAlias via une opération de réglage de gestion de réseau, l'agent doit conserver la valeur fournie dans l'instance d'ifAlias associée à la même interface aussi longtemps que cette interface reste instanciée, y compris lors de toutes les réinitialisations/tous les redémarrages du système de gestion de réseau, y compris celles ou

Groupe/objet	Description
	ceux qui entraînent une modification de la valeur d'ifIndex de l'interface. Un exemple de la valeur qu'un gestionnaire de réseau peut stocker dans cet objet pour une interface WAN est le numéro de circuit/l'identificateur de l'interface (de Telco). Certains agents peuvent prendre en charge l'accès en écriture uniquement pour les interfaces ayant des valeurs particulières d'ifType. Un agent qui prend en charge l'accès en écriture à cet objet doit conserver la valeur dans un stockage non volatil, mais il peut limiter la longueur des nouvelles valeurs en fonction du volume de stockage déjà occupé par les valeurs actuelles pour d'autres interfaces. **Remarque** La longueur de la chaîne est limitée à 15 caractères.
Groupe : IfGeneralInformationGroup **Trap :** IfConnectorPresent	**Capacité de l'agent :** RC-IF-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.31.1.1.1.17.1 **Définition :** cet objet a la valeur `true(1)` si la sous-couche d'interface a un connecteur physique et la valeur `false(2)` en cas contraire.
Groupe : IfCounterDiscontinuityGroup **Trap :** IfCounterDiscontinuityTime	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.31.1.1.1.19.1 **Définition :** valeur de sysUpTime la dernière fois qu'un ou plusieurs des compteurs de cette interface ont subi une discontinuité. Les compteurs pertinents sont les instances spécifiques associées à cette interface de tout Counter32 ou
Groupe : IfGeneralInformationGroup **Trap :** IfDescr	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.2.2.1.2.1 **Définition :** chaîne textuelle contenant des informations sur l'interface. Cette chaîne doit inclure le nom du fabricant, le nom du produit et la version du matériel/logiciel de l'interface.
Groupe : IfVHCPacketGroup **Trap :** IfHCInBroadcastPkts	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.9.1 **Définition :** objet Counter64 contenu dans l'ifTable ou l'ifXTable. Si aucune discontinuité de ce type ne s'est produite depuis la dernière réinitialisation du sous-système de gestion local, cet objet contient alors une valeur nulle.
Groupe : IfVHCPacketGroup **Trap :** IfHCInMulticastPkts	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.8.1 **Définition :** nombre de paquets, envoyés par cette sous-couche à une (sous-)couche supérieure, qui ont été adressés à une adresse de multidiffusion au niveau de cette sous-couche. Pour un protocole de couche MAC, cela inclut à la fois les adresses de groupe et fonctionnelles. Cet objet est une version 64 bits d'ifInMulticastPkts. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.

Groupe/objet	Description
Groupe : IfVHCPacketGroup **Trap :** IfHCInOctets	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.6.1 **Définition :** nombre total d'octets reçus sur l'interface, y compris les caractères de trame. Cet objet est une version 64 bits d'ifInOctets. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfHCInUcastPkts	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.7.1 **Définition :** nombre de paquets, envoyés par cette sous-couche à une (sous-)couche supérieure, qui n'ont pas été adressés à une adresse de multidiffusion ou de diffusion au niveau de cette sous-couche. Cet objet est une version 64 bits d'ifInUcastPkts. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfHCOutBroadcastPkts	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.13.1 **Définition :** nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui ont été adressés à une adresse de diffusion au niveau de cette sous-couche, y compris ceux qui ont été rejetés ou non envoyés. Cet objet est une version 64 bits d'ifOutBroadcastPkts. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfHCOutMulticastPkts	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.12.1 **Définition :** nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui ont été adressés à une adresse de multidiffusion au niveau de cette sous-couche, y compris ceux qui ont été rejetés ou non envoyés. Pour un protocole de couche MAC, cela inclut à la fois les adresses de groupe et fonctionnelles. Cet objet est une version 64 bits d'ifOutMulticastPkts. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfHCOutOctets	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.10.1 **Définition :** nombre total d'octets transmis hors de l'interface, y compris les caractères de trame. Cet objet est une version 64 bits d'ifOutOctets.
Groupe : IfVHCPacketGroup **Trap :** IfHCOutUcastPkts	**Accès :** lecture seule **Définition :** Counter64 **OID :** .1.3.6.1.2.1.31.1.1.1.11.1

Groupe/objet	Description
	Définition : nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui n'ont pas été adressés à une adresse de multidiffusion ou de diffusion au niveau de cette sous-couche, y compris ceux qui ont été rejetés ou non envoyés. Cet objet est une version 64 bits d'ifOutUcastPkts.
Groupe : IfGeneralInformationGroup **Trap :** IfHighSpeed	**Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.3.6.1.2.1.31.1.1.1.15.1 **Définition :** estimation de la largeur de bande actuelle de l'interface en unités de 1 000 000 bits par seconde. Si cet objet indique une valeur de `n`, alors la vitesse de l'interface se situe dans la plage de `n-500,000` à `n+499,999`. Pour les interfaces dont la largeur de bande ne varie pas ou pour celles pour lesquelles aucune estimation précise ne peut être faite, cet objet doit contenir la largeur de bande nominale. Pour une sous-couche qui n'a pas de concept de largeur de bande, cet objet doit être nul.
Groupe : IfVHCPacketGroup **Trap :** IfInBroadcastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.31.1.1.1.3.1 **Définition :** nombre de paquets, envoyés par cette sous-couche à une (sous-)couche supérieure, qui ont été adressés à une adresse de diffusion au niveau de cette sous-couche. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfGeneralInformationGroup **Trap :** IfIndex	**Capacité de l'agent :** RC-IEEEC37-238-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.2.1.1.1 **Définition :** valeur unique, supérieure à zéro, pour chaque interface. Il est recommandé d'affecter les valeurs de manière contiguë à partir de 1. La valeur de chaque sous-couche d'interface doit rester constante au moins d'une réinitialisation du système de gestion de réseau de l'entité à la réinitialisation suivante. **Remarque** La création et la suppression d'une entrée dans ifTable ne sont pas prises en charge.
Groupe : IfVHCPacketGroup **Trap :** IfInDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.13.1 **Définition :** nombre de paquets entrants choisis pour être rejetés même si aucune erreur n'a été détectée pour empêcher leur livraison à un protocole de couche supérieure. Une raison possible pour rejeter les paquets en question peut être de libérer de l'espace dans la mémoire tampon. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfInErrors	**Accès :** lecture seule **Syntaxe :** Counter32

Groupe/objet	Description
	OID : .1.3.6.1.2.1.2.2.1.14.1 **Définition :** pour les interfaces orientées paquets, nombre de paquets entrants contenant des erreurs les empêchant d'être transmis à un protocole de couche supérieure. Pour les interfaces orientées caractères ou les interfaces de longueur fixe, nombre d'unités de transmission entrantes contenant des erreurs les empêchant d'être transmises à un protocole de couche supérieure. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfInMulticastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.31.1.1.1.2.1 **Définition :** nombre de paquets, envoyés par cette sous-couche à une (sous-)couche supérieure, qui ont été adressés à une adresse de multidiffusion au niveau de cette sous-couche. Pour un protocole de couche MAC, cela inclut à la fois les adresses de groupe et fonctionnelles. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfInOctets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.10.1 **Définition :** nombre total d'octets reçus sur l'interface, y compris les caractères de trame. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfInUcastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.11.1 **Définition :** nombre de paquets, envoyés par cette sous-couche à une (sous-)couche supérieure, qui n'ont pas été adressés à une adresse de multidiffusion ou de diffusion au niveau de cette sous-couche. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfInUnknownProtos	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.15.1 **Définition :** pour les interfaces orientées paquets, nombre de paquets reçus via l'interface qui ont été rejetés en raison d'un protocole inconnu ou non pris en charge. Pour les interfaces orientées caractères ou les interfaces de longueur fixe qui prennent en charge le multiplexage de protocole, nombre d'unités de transmission reçues via l'interface qui ont été rejetées en raison d'un protocole inconnu ou non pris en charge. Pour toute interface qui ne prend pas en charge le multiplexage de protocole, ce compteur sera toujours 0. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfGeneralInformationGroup	**Accès :** lecture seule

Groupe/objet	Description
Trap : IfLastChange	**Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.2.2.1.9.1 **Définition :** valeur de sysUpTime au moment où l'interface est passée à son état opérationnel actuel. Si elle est passée à l'état actuel avant la dernière réinitialisation du sous-système de gestion de réseau local, cet objet contient une valeur nulle.
Groupe : IfGeneralInformationGroup **Trap :** IfLinkUpDownTrapEnable	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.31.1.1.1.14.1 **Définition :** indique si des traps linkUp/linkDown doivent être générés pour cette interface. Par défaut, cet objet doit avoir la valeur enabled(1) pour les interfaces qui ne fonctionnent sur le `top` d'aucune autre interface (comme défini dans ifStackTable), et disabled(2) en cas contraire.
Groupe : IfVHCPacketGroup **Trap :** IfMtu	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.2.1.4.1 **Définition :** taille du plus grand paquet pouvant être envoyé/reçu sur l'interface, spécifiée en octets. Pour les interfaces utilisées pour transmettre des datagrammes réseau, il s'agit de la taille du plus grand datagramme réseau pouvant être envoyé sur l'interface.
Groupe : IfGeneralInformationGroup **Trap :** IfName	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.31.1.1.1.1.1 **Définition :** nom textuel de l'interface. La valeur de cet objet doit être le nom de l'interface tel qu'affecté par l'appareil local et doit être compatible avec une utilisation dans les commandes entrées dans la `console` de l'appareil. Il peut s'agir d'un nom textuel, tel que `le0` ou d'un simple numéro de port, tel que `1`, selon la syntaxe de dénomination de l'interface de l'appareil. Si plusieurs entrées d'ifTable représentent ensemble une seule interface telle que nommée par l'appareil, elles auront chacune la même valeur d'ifName. Notez que, pour un agent qui répond aux requêtes SNMP concernant une interface sur un autre appareil (représenté), la valeur d'ifName pour l'interface en question est le nom local de l'appareil représenté pour celle-ci. En l'absence de nom local, ou si cet objet n'est pas applicable, cet objet contient une chaîne de longueur nulle.
Groupe : IfGeneralInformationGroup **Trap :** IfNumber	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.1.0 **Définition :** nombre d'interfaces réseau (indépendamment de leur état actuel) présentes sur ce système.
Groupe : IfGeneralInformationGroup **Trap :** IfOperStatus	**Capacité de l'agent :** RC-IF-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.2.1.8.1 **Définition :** état opérationnel actuel de l'interface. L'état testing(3) indique qu'aucun paquet opérationnel ne peut être transmis. Si ifAdminStatus est à l'état down(2) alors ifOperStatus doit être à l'état down(2). Si ifAdminStatus passe à up(1) alors ifOperStatus doit passer à up(1) si l'interface est prête à transmettre et à recevoir du trafic réseau ; il doit passer à dormant(5) si

Groupe/objet	Description
	l'interface attend des actions externes (comme une ligne série attendant une connexion entrante) ; il doit rester à l'état down(2) si et seulement s'il y a un défaut qui l'empêche de passer à l'état up(1) ; il doit rester à l'état notPresent(6) s'il manque des composants à l'interface (généralement du matériel). **Remarque** Informations limitées par Rugged Switch Agent pour l'objet Read-Only (lecture seule).
Groupe : IfVHCPacketGroup **Trap :** IfOutBroadcastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.31.1.1.1.5.1 **Définition :** nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui ont été adressés à une adresse de diffusion au niveau de cette sous-couche, y compris ceux qui ont été rejetés ou non envoyés. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfOutDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.19.1 **Définition :** nombre de paquets sortants choisis pour être rejetés même si aucune erreur n'a été détectée, pour empêcher leur transmission. Une raison possible pour rejeter les paquets en question peut être de libérer de l'espace dans la mémoire tampon. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfOutErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.20.1 **Définition :** pour les interfaces orientées paquets, nombre de paquets sortants qui n'ont pas pu être transmis en raison d'erreurs. Pour les interfaces orientées caractères ou les interfaces de longueur fixe, nombre d'unités de transmission sortantes qui n'ont pas pu être transmises en raison d'erreurs. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfOutMulticastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.31.1.1.1.4.1 **Définition :** nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui ont été adressés à une adresse de multidiffusion au niveau de cette sous-couche, y compris ceux qui ont été rejetés ou non envoyés. Pour un protocole de couche MAC, cela inclut à la fois les adresses de groupe et fonctionnelles. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup	**Accès :** lecture seule

Groupe/objet	Description
Trap : IfOutOctets	**Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.16.1 **Définition :** nombre total d'octets transmis hors de l'interface, y compris les caractères de trame. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfVHCPacketGroup **Trap :** IfOutUcastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.2.2.1.17.1 **Définition :** nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui n'ont pas été adressés à une adresse de multidiffusion ou de diffusion au niveau de cette sous-couche, y compris ceux qui ont été rejetés ou non envoyés. Des discontinuités dans la valeur de ce compteur peuvent se produire lors de la réinitialisation du système de gestion, et à d'autres moments comme indiqué par la valeur d'ifCounterDiscontinuityTime.
Groupe : IfGeneralInformationGroup **Trap :** IfPhysAddress	**Accès :** lecture seule **Syntaxe :** PhysAddress **OID :** .1.3.6.1.2.1.2.2.1.6.1 **Définition :** adresse de l'interface au niveau de sa sous-couche de protocole. Par exemple, pour une interface 802.x, cet objet contient normalement une adresse MAC. La MIB spécifique au support de l'interface doit définir l'ordre des bits et des octets et le format de la valeur de cet objet. Pour les interfaces qui n'ont pas d'adresse de ce type (par exemple, une ligne série), cet objet doit contenir une chaîne d'octets de longueur nulle.
Groupe : IfVHCPacketGroup **Trap :** IfPromiscuousMode	**Capacité de l'agent :** RC-IF-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.31.1.1.1.16.1 **Définition :** cet objet a la valeur false(2) si cette interface n'accepte que les paquets/trames qui sont adressés à cette station. Cet objet a la valeur true(1) lorsque la station accepte tous les paquets/trames transmis sur le support. La valeur true(1) n'est légale que sur certains types de supports. Si c'est légal, le réglage de cet objet sur la valeur true(1) peut nécessiter la réinitialisation de l'interface avant de devenir effectif. La valeur de ifPromiscuousMode n'affecte pas la réception des paquets/trames de diffusion et de multidiffusion par l'interface. **Remarque** L'accès en écriture n'est pas appliqué selon la déclaration de conformité RFC 2863. Ce mode est toujours `false(1)`.
Groupe : IfGeneralInformationGroup **Trap :** IfSpeed	**Capacité de l'agent :** RC-IF-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.2.1.5.1 **Définition :** estimation de la largeur de bande actuelle de l'interface en bits par seconde. Pour les interfaces dont la largeur de bande ne varie pas ou pour celles pour lesquelles aucune estimation précise ne peut être faite, cet

Groupe/objet	Description
	objet doit contenir la largeur de bande nominale. Si la largeur de bande de l'interface est supérieure à la valeur maximale pouvant être indiquée par cet objet, cet objet doit indiquer sa valeur maximale (4 294 967 295) et ifHighSpeed doit être utilisé pour indiquer la vitesse de l'interface. Pour une sous-couche qui n'a pas de concept de largeur de bande, cet objet doit être nul.
Groupe : IfGeneralInformationGroup **Trap :** IfTableLastChange	**Capacité de l'agent :** RC-IF-MIB-AC **Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.31.1.5.0 **Définition :** valeur de sysUpTime au moment de la dernière création ou suppression d'une entrée dans l'ifTable. Si le nombre d'entrées est resté inchangé depuis la dernière réinitialisation du sous-système de gestion de réseau local, cet objet contient une valeur nulle.
Groupe : IfGeneralInformationGroup **Trap :** IfType	**Capacité de l'agent :** RC-IP-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.2.2.1.3.1 **Définition :** type d'interface. Des valeurs supplémentaires d'ifType sont affectées par l'IANA (Internet Assigned Numbers Authority), par la mise à jour de la syntaxe de la convention textuelle IANAifType.

IP-MIB

Groupe/objet	Description
Groupe : icmpGroup **Trap :** icmpInAddrMaskReps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.13 **Définition :** nombre de messages ICMP Address Mask Reply reçus.
Groupe : icmpGroup **Trap :** icmpInAddrMasks	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.12 **Définition :** nombre de messages ICMP Address Mask Request reçus.
Groupe : icmpGroup **Trap :** icmpInDestUnreachs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.3 **Définition :** nombre de messages ICMP Destination Unreachable reçus.
Groupe : icmpGroup **Trap :** icmpInEchoReps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.9 **Définition :** nombre de messages ICMP Echo Reply reçus.
Groupe : icmpGroup **Trap :** icmpInEchos	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.8 **Définition :** nombre de messages ICMP Echo (request) reçus.

Groupe/objet	Description
Groupe : icmpGroup **Trap :** icmpInErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.2 **Définition :** nombre de messages ICMP reçus par l'entité mais déterminés comme ayant des erreurs spécifiques à ICMP (sommes de contrôle ICMP erronées, longueur erronée, etc.).
Groupe : icmpGroup **Trap :** icmpInMsgs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.1 **Définition :** nombre total de messages ICMP reçus par l'entité. Notez que ce compteur inclut tous les messages comptés par icmpInErrors.
Groupe : icmpGroup **Trap :** icmpInParmProbs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.5 **Définition :** nombre de messages ICMP Parameter Problem reçus.
Groupe : icmpGroup **Trap :** icmpInRedirects	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.7 **Définition :** nombre de messages ICMP Redirect reçus.
Groupe : icmpGroup **Trap :** icmpInSrcQuenchs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.6 **Définition :** nombre de messages ICMP Time Exceeded reçus.
Groupe : icmpGroup **Trap :** icmpInTimeExcds	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.4 **Définition :** nombre de messages ICMP Timestamp Reply reçus.
Groupe : icmpGroup **Trap :** icmpInTimestampReps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.11 **Définition :** nombre de messages ICMP Timestamp Reply reçus.
Groupe : icmpGroup **Trap :** icmpInTimestamps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.10 **Définition :** nombre de messages ICMP Timestamp (request) reçus.
Groupe : icmpGroup **Trap :** icmpOutAddrMaskReps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.26 **Définition :** nombre de messages ICMP Address Mask Reply envoyés.
Groupe : icmpGroup **Trap :** icmpOutDestUnreachs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.16

Groupe/objet	Description
	Définition : nombre de messages ICMP Destination Unreachable envoyés.
Groupe : icmpGroup **Trap :** icmpOutEchoReps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.22 **Définition :** nombre de messages ICMP Echo Reply envoyés.
Groupe : icmpGroup **Trap :** icmpOutErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.15 **Définition :** nombre de messages ICMP que cette entité n'a pas envoyés en raison de problèmes découverts dans ICMP, tels qu'un manque de tampons. Cette valeur ne doit pas inclure les erreurs découvertes en dehors de la couche ICMP telles que l'incapacité d'IP à acheminer le datagramme résultant. Dans certaines mises en œuvre, il peut n'y avoir aucun type d'erreur qui contribue à la valeur de ce compteur.
Groupe : icmpGroup **Trap :** icmpOutMsgs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.14 **Définition :** nombre total de messages ICMP que cette entité a tenté d'envoyer. Notez que ce compteur inclut tous les messages comptés par icmpOutErrors.
Groupe : icmpGroup **Trap :** icmpOutParmProbs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.18 **Définition :** nombre de messages ICMP Parameter Problem envoyés.
Groupe : icmpGroup **Trap :** icmpOutRedirects	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.20 **Définition :** nombre de messages ICMP Redirect envoyés. Pour un hôte, cet objet est toujours égal à zéro, car les hôtes n'envoient pas de redirections.
Groupe : icmpGroup **Trap :** icmpOutSrcQuenchs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.19 **Définition :** nombre de messages ICMP Source Quench envoyés.
Groupe : icmpGroup **Trap :** icmpOutTimeExcds	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.17 **Définition :** nombre de messages ICMP Time Exceeded envoyés.
Groupe : icmpGroup **Trap :** icmpOutTimestampReps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.24 **Définition :** nombre de messages ICMP Timestamp Reply envoyés.
Groupe : icmpGroup **Trap :** icmpOutTimestamps	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.5.23

Groupe/objet	Description
	Définition : nombre de messages ICMP Timestamp (request) envoyés.
Groupe : ipGroup **Trap :** ipAdEntAddr	**Accès :** lecture seule **Syntaxe :** IpAddress **OID :** .1.3.6.1.2.1.4.20.1.1.192.168.0.180 **Définition :** adresse IP à laquelle se rapportent les informations d'adressage de cette entrée.
Groupe : ipGroup **Trap :** ipAdEntBcastAddr	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.20.1.4.192.168.0.180 **Définition :** valeur du bit le moins significatif de l'adresse de diffusion IP utilisée pour envoyer des datagrammes sur l'interface (logique) associée à l'adresse IP de cette entrée. Par exemple, lorsque l'adresse de diffusion standard Internet contenant uniquement des uns est utilisée, la valeur est égale à 1. Cette valeur s'applique à la fois aux adresses de diffusion de sous-réseau et de réseau utilisées par l'entité sur cette interface (logique).
Groupe : ipGroup **Trap :** ipAdEntIfIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.20.1.2.192.168.0.180 **Définition :** valeur d'index qui identifie de manière unique l'interface à laquelle cette entrée s'applique. L'interface identifiée par une valeur spécifique de cet index est la même interface que celle identifiée par la même valeur de l'ifIndex de RFC 1573.
Groupe : ipGroup **Trap :** ipAdEntNetMask	**Accès :** lecture seule **Syntaxe :** IpAddress **OID :** .1.3.6.1.2.1.4.20.1.3.192.168.0.180 **Définition :** masque de sous-réseau associé à l'adresse IP de cette entrée. La valeur du masque est une adresse IP avec tous les bits de réseau mis à 1 et tous les bits d'hôtes mis à 0.
Groupe : ipGroup **Trap :** ipAdEntReasmMaxSize	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.20.1.5.192.168.0.180 **Définition :** taille du plus grand datagramme IP que cette entité peut réassembler à partir des datagrammes fragmentés IP entrants reçus sur cette interface.
Groupe : ipGroup **Trap :** ipDefaultTTL	**Capacité de l'agent :** RC-IP-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.2.0 **Définition :** valeur par défaut insérée dans le champ Time-To-Live de l'en-tête IP des datagrammes provenant de cette entité, chaque fois qu'une valeur TTL n'est pas fournie par le protocole de la couche transport. **Remarque** L'accès en écriture n'est pas pris en charge.
Groupe : ipGroup **Trap :** ipForwarding	**Capacité de l'agent :** RC-IP-MIB-AC **Accès :** lecture et écriture

Groupe/objet	Description
	Syntaxe : Integer **OID :** .1.3.6.1.2.1.4.1.0 **Définition :** indique si cette entité agit en tant que routeur IP en ce qui concerne la transmission des datagrammes reçus par (mais non adressés à) cette entité. Les routeurs IP transmettent les datagrammes. Les hôtes IP ne le font pas (sauf ceux routés par la source via l'hôte). **Remarque** La prise en charge de la valeur `forwarding(1)` n'est pas appliquée selon RFC 2011.
Groupe : ipGroup **Trap :** ipForwDatagrams	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.6.0 **Définition :** nombre de datagrammes d'entrée pour lesquels cette entité n'était pas leur destination IP finale, ce qui a entraîné une tentative de trouver une route pour les transmettre à cette destination finale. Dans les entités qui n'agissent pas en tant que routeurs IP, ce compteur inclut uniquement les paquets qui ont été routés par la source via cette entité, et le traitement de l'option Source-Route a réussi.
Groupe : ipGroup **Trap :** ipFragCreates	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.19.0 **Définition :** nombre de fragments de datagramme IP qui ont été générés à la suite de la fragmentation au niveau de cette entité.
Groupe : ipGroup **Trap :** ipFragFails	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.18.0 **Définition :** nombre de datagrammes IP qui ont été rejetés parce qu'ils devaient être fragmentés au niveau de cette entité mais qui n'ont pas pu l'être, par exemple parce que leur indicateur Don't Fragment a été défini.
Groupe : ipGroup **Trap :** ipFragOKs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.17.0 **Définition :** nombre de datagrammes IP qui ont été fragmentés avec succès au niveau de cette entité.
Groupe : ipGroup **Trap :** ipInAddrErrors	**Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.5.0 **Définition :** nombre de datagrammes d'entrée rejetés parce que l'adresse IP dans le champ de destination de leur en-tête IP n'était pas une adresse valide pour la réception sur cette entité. Ce nombre inclut les adresses non valides (par exemple, 0.0.0.0) et les adresses de classes non prises en charge (par exemple, la classe E). Pour les entités qui ne sont pas des routeurs IP et ne transmettent donc pas de datagrammes, ce compteur inclut les datagrammes rejetés car l'adresse de destination n'était pas une adresse locale.
Groupe : ipGroup	**Accès :** lecture seule

Groupe/objet	Description
Trap : ipInDelivers	**Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.9.0 **Définition :** nombre total de datagrammes d'entrée dont l'envoi aux protocoles utilisateur IP (y compris ICMP) a réussi.
Groupe : ipGroup **Trap :** ipInDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.8.0 **Définition :** nombre de datagrammes IP d'entrée pour lesquels aucun problème n'a été rencontré pour empêcher leur traitement continu, mais qui ont été rejetés (par exemple, par manque d'espace dans la mémoire tampon). Notez que ce compteur n'inclut aucun datagramme rejeté en attendant le réassemblage.
Groupe : ipGroup **Trap :** ipInHdrErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.4.0 **Définition :** nombre de datagrammes d'entrée rejetés en raison d'erreurs dans leurs en-têtes IP, y compris les sommes de contrôle erronées, la non-concordance des numéros de version, d'autres erreurs de format, le dépassement de la durée de vie, les erreurs découvertes lors du traitement de leurs options IP, etc.
Groupe : ipGroup **Trap :** ipInReceives	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.3.0 **Définition :** nombre total de datagrammes d'entrée reçus en provenance des interfaces, y compris ceux reçus par erreur.
Groupe : ipGroup **Trap :** ipInUnknownProtos	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.7.0 **Définition :** nombre de datagrammes adressés localement dont la réception a réussi mais qui ont été rejetés en raison d'un protocole inconnu ou non pris en charge.
Groupe : ipGroup **Trap :** ipNetToMediaIfIndex	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.22.1.1.1002.192.168.0.254 **Définition :** interface sur laquelle l'équivalence de cette entrée est effective. L'interface identifiée par une valeur spécifique de cet index est la même interface que celle identifiée par la même valeur de l'ifIndex de RFC 1573.
Groupe : ipGroup **Trap :** ipNetToMediaNetAddress	**Accès :** Lecture et création **Syntaxe :** IpAddress **OID :** .1.3.6.1.2.1.4.22.1.3.1002.192.168.0.254 **Définition :** IpAddress correspondant à l'adresse `physical` dépendante du support.
Groupe : ipGroup **Trap :** ipNetToMediaPhysAddress	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.4.22.1.2.1002.192.168.0.254 **Définition :** adresse `physical` dépendante du support.

Groupe/objet	Description
Groupe : ipGroup **Trap :** ipNetToMediaType	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.22.1.4.1002.192.168.0.254 **Définition :** type de mappage. Définir cet objet sur la valeur invalid(2) a pour effet d'invalider l'entrée correspondante dans ipNetToMediaTable. C'est-à-dire qu'il dissocie efficacement l'interface identifiée avec ladite entrée du mappage identifié avec ladite entrée. Savoir si l'agent supprime une entrée invalidée du tableau est une question spécifique à la mise en œuvre. En conséquence, les stations de gestion doivent être prêtes à recevoir des informations tabulaires des agents qui correspondent aux entrées non utilisées actuellement. L'interprétation correcte de ces entrées nécessite l'examen de l'objet ipNetToMediaType pertinent.
Groupe : ipGroup **Trap :** ipOutDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.11.0 **Définition :** nombre de datagrammes IP de sortie pour lesquels aucun problème n'a été rencontré pour empêcher leur transmission vers leur destination, mais qui ont été rejetés (par exemple, par manque d'espace dans la mémoire tampon). Notez que ce compteur inclurait les datagrammes comptés dans ipForwDatagrams si des paquets de ce type remplissaient ce critère de suppression (discrétionnaire).
Groupe : ipGroup **Trap :** ipOutNoRoutes	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.12.0 **Définition :** nombre de datagrammes IP rejetés car aucune route n'a pu être trouvée pour les transmettre à leur destination. Notez que ce compteur inclut tous les paquets comptés dans ipForwDatagrams qui répondent à ce critère `no-route`. Notez que cela inclut tous les datagrammes qu'un hôte ne peut pas router car tous ses routeurs par défaut sont en panne.
Groupe : ipGroup **Trap :** ipOutRequests	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.10.0 **Définition :** nombre total de datagrammes IP que les protocoles utilisateur IP locaux (y compris ICMP) ont fournis à l'IP dans les demandes de transmission. Notez que ce compteur n'inclut aucun datagramme compté dans ipForwDatagrams.
Groupe : ipGroup **Trap :** ipReasmFails	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.16.0 **Définition :** nombre de défaillances détectées par l'algorithme de réassemblage IP (quelle qu'en soit la raison : expiration, erreurs, etc.). Notez qu'il ne s'agit pas nécessairement d'un nombre de fragments IP rejetés car certains algorithmes (notamment l'algorithme de RFC 815) peuvent perdre la trace du nombre de fragments en les combinant au fur et à mesure qu'ils sont reçus.
Groupe : ipGroup **Trap :** ipReasmOKs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.15.0 **Définition :** nombre de datagrammes IP dont le réassemblage a réussi.

Groupe/objet	Description
Groupe : ipGroup **Trap :** ipReasmReqds	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.14.0 **Définition :** nombre de fragments IP reçus qui devaient être réassemblés au niveau de cette entité.
Groupe : ipGroup **Trap :** ipReasmTimeout	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.4.13.0 **Définition :** nombre maximum de secondes pendant lesquelles les fragments reçus sont conservés en attendant d'être réassemblés au niveau de cette entité.
Groupe : ipGroup **Trap :** ipRoutingDiscards	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.4.23 **Définition :** nombre d'entrées de routage qui ont été choisies pour être rejetées même si elles sont valides. Une raison possible pour rejeter une telle entrée peut être de libérer de l'espace dans la mémoire tampon pour d'autres entrées de routage.

LLDP-MIB

Groupe/objet	Description
Groupe : lldpConfigTxGroup **Trap :** lldpConfigManAddrPortsTxEnable	**Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture et écriture **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.1.7.1.1.4 **Définition :** ensemble de ports identifiés par PortList dans lequel chaque port est représenté par un bit. L'instance d'adresse de gestion du système local correspondante est transmise sur les ports membres de lldpManAddrPortsTxEnable. La valeur par défaut de l'objet lldpConfigManAddrPortsTxEnable est une chaîne binaire vide, ce qui signifie qu'aucun port n'est spécifié pour l'annonce de l'instance d'adresse de gestion indiquée. L'accès en écriture n'est pas mis en œuvre.
Groupe : lldpLocSysGroup **Trap :** lldpLocChassisId	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.3.2.0 **Définition :** type de codage utilisé pour identifier le châssis associé au système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocChassisIdSubtype	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.3.1.0 **Définition :** type de codage utilisé pour identifier le châssis associé au système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocManAddrIfId	**Accès :** lecture seule **Syntaxe :** Integer

Groupe/objet	Description
	OID : .1.0.8802.1.1.2.1.3.8.1.5.192.168.0.180 **Définition :** valeur entière utilisée pour identifier le numéro d'interface concernant le composant d'adresse de gestion associé au système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocManAddrIfSubtype	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.3.8.1.4.192.168.0.180 **Définition :** valeur d'énumération qui identifie la méthode de numérotation d'interface utilisée pour définir le numéro d'interface, associée au système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocManAddrLen	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.3.8.1.3 **Définition :** longueur totale du sous-type d'adresse de gestion et des champs d'adresse de gestion dans les LLDPDU transmises par l'agent LLDP local. Le champ de longueur d'adresse de gestion est nécessaire pour que les systèmes récepteurs qui ne mettent pas en œuvre SNMP ne soient pas obligés de mettre en œuvre un tableau d'équivalence entre les numéros de famille iana et la longueur d'adresse afin de décoder l'adresse de gestion.
Groupe : lldpLocSysGroup **Trap :** lldpLocManAddrOID	**Accès :** lecture seule **Syntaxe :** OID **OID :** .1.0.8802.1.1.2.1.3.8.1.6.192.168.0.180 **Définition :** valeur OID utilisée pour identifier le type de composant matériel ou d'entité de protocole associé à l'adresse de gestion annoncée par l'agent du système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocPortDesc	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.3.7.1.4.1 **Définition :** valeur de chaîne utilisée pour identifier la description du port de la station LAN 802 associée au système local. Si l'agent local prend en charge IETF RFC 2863, l'objet lldpLocPortDesc doit avoir la même valeur que l'objet ifDescr.
Groupe : lldpLocSysGroup **Trap :** lldpLocPortId	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.3.7.1.3.1 **Définition :** valeur de chaîne utilisée pour identifier le composant de port associé à un port donné dans le système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocPortIdSubtype	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.3.7.1.2.1 **Définition :** type de codage d'identificateur de port utilisé dans l'objet `lldpLocPortId` associé.
Groupe : lldpLocSysGroup **Trap :** lldpLocSysCapEnabled	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.3.6.0 **Définition :** valeur bitmap utilisée pour identifier les fonctionnalités système activées sur le système local.

Groupe/objet	Description
Groupe : lldpLocSysGroup **Trap :** lldpLocSysCapSupported	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.3.5.0 **Définition :** valeur bitmap utilisée pour identifier les fonctionnalités système prises en charge sur le système local.
Groupe : lldpLocSysGroup **Trap :** lldpLocSysDesc	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.3.4.0 **Définition :** valeur de chaîne utilisée pour identifier la description du système local. Si l'agent local prend en charge IETF RFC 3418, l'objet lldpLocSysDesc doit avoir la même valeur que l'objet sysDesc.
Groupe : lldpLocSysGroup **Trap :** lldpLocSysName	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.3.3.0 **Définition :** valeur de chaîne utilisée pour identifier le nom système du système local. Si l'agent local prend en charge IETF RFC 3418, l'objet lldpLocSysName doit avoir la même valeur que l'objet sysName.
Groupe : lldpConfigTxGroup **Trap :** lldpMessageTxHoldMultiplier	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.2.0 **Définition :** valeur de durée de vie exprimée sous la forme d'un multiple de l'objet lldpMessageTxInterval. La valeur de durée de vie réelle utilisée dans les trames LLDP, transmise au nom de cet agent LLDP, peut être exprimée par la formule suivante : TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)). Par exemple, si la valeur de lldpMessageTxInterval est `30`, et si la valeur de lldpMessageTxHoldMultiplier est `4`, alors la valeur `120` est codée dans le champ TTL de l'en-tête LLDP. La valeur par défaut de l'objet lldpMessageTxHoldMultiplier est 4. La valeur de cet objet doit être restaurée à partir du stockage non volatil après une réinitialisation du système de gestion.
Groupe : lldpConfigTxGroup **Trap :** lldpMessageTxInterval	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.1.0 **Définition :** intervalle auquel les trames LLDP sont transmises au nom de cet agent LLDP. La valeur par défaut de l'objet lldpMessageTxInterval est 30 secondes. La valeur de cet objet doit être restaurée à partir du stockage non volatil après une réinitialisation du système de gestion.
Groupe : lldpConfigRxGroup **Trap :** lldpNotificationInterval	**Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.5.0 **Définition :** cet objet contrôle la transmission des notifications LLDP. L'agent ne doit pas générer plus d'un événement de notification lldpRemTablesChange dans la période indiquée, où un `notification-event` est la transmission d'un seul type de PDU de notification à une liste de destinations de notification. Si des modifications supplémentaires dans les groupes d'objets lldpRemoteSystemsData se produisent pendant la période de limitation indiquée, ces événements trap doivent être

Groupe/objet	Description
	supprimés par l'agent. Un NMS doit vérifier périodiquement la valeur de lldpStatsRemTableLastChangeTime pour détecter tout événement de notification lldpRemTablesChange manqué, par exemple en raison d'une limitation ou d'une perte de transmission. Si la transmission de la notification est activée pour des ports spécifiques, la période de limitation par défaut suggérée est de 5 secondes. La valeur de cet objet doit être restaurée à partir du stockage non volatil après une réinitialisation du système de gestion. **Remarque** L'accès en écriture n'est pas mis en œuvre.
Groupe : lldpConfigGroup **Trap :** lldpPortConfigAdminStatus	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.6.1.2.1 **Définition :** état administrativement souhaité de l'agent LLDP local. Si l'objet lldpPortConfigAdminStatus associé a la valeur `txOnly(1)`, alors l'agent LLDP transmet les trames LLDP sur ce port et il ne stocke aucune information sur les systèmes distants connectés. Si l'objet lldpPortConfigAdminStatus associé a la valeur `rxOnly(2)`, l'agent LLDP reçoit, mais ne transmet pas les trames LLDP sur ce port. Si l'objet lldpPortConfigAdminStatus associé a la valeur `txAndRx(3)`, l'agent LLDP transmet et reçoit les trames LLDP sur ce port. Si l'objet lldpPortConfigAdminStatus associé a la valeur `disabled(4)`, l'agent LLDP ne transmet et ne reçoit pas les trames LLDP sur ce port. Les informations vieillissent naturellement si des informations de systèmes distants sont reçues sur ce port et stockées dans d'autres tableaux, avant que le lldpPortConfigAdminStatus du port ne soit désactivé.
Groupe : lldpConfigRxGroup **Trap :** lldpPortConfigNotificationEnable	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.6.1.3.1 **Définition :** lldpPortConfigNotificationEnable contrôle, port par port, si les notifications de l'agent sont activées ou non. La valeur true(1) signifie que les notifications sont activées ; la valeur false(2) signifie qu'elles sont désactivées.
Groupe : lldpConfigTxGroup **Trap :** lldpPortConfigTLVsTxEnable	**Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture et écriture **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.1.6.1.4.1 **Définition :** lldpPortConfigTLVsTxEnable, défini comme un bitmap, inclut l'ensemble de base des LLDP TLV dont la transmission est autorisée sur l'agent LLDP local par la gestion du réseau. Chaque bit du bitmap correspond à un type de TLV associé à une TLV facultative spécifique. Il convient de noter que les TLV spécifiques à l'organisation sont exclus du bitmap lldpTLVsTxEnable. Les MIB d'extension d'informations spécifiques à l'organisation LLDP doivent avoir un objet de configuration similaire pour contrôler la transmission de leurs TLV définies par l'organisation. Le bit `portDesc(0)` indique que l'agent LLDP doit transmettre `Port Description TLV`. Le bit `sysName(1)` indique que l'agent LLDP doit transmettre `System Name TLV`. Le bit `sysDesc(2)` indique que l'agent LLDP doit transmettre `System Description TLV`. Le bit `sysCap(3)` indique que l'agent LLDP doit transmettre `System Capabilities TLV`. Aucun bit n'est réservé pour le type TLV d'adresse de gestion puisque la transmission des TLV d'adresse de gestion est contrôlée par un autre objet, lldpConfigManAddrTable. La valeur par défaut de l'objet

Groupe/objet	Description
	lldpPortConfigTLVsTxEnable est un ensemble vide, ce qui signifie qu'aucune valeur énumérée n'est définie. La valeur de cet objet doit être restaurée à partir du stockage non volatil après une réinitialisation du système de gestion. L'accès en écriture n'est pas mis en œuvre.
Groupe : lldpConfigTxGroup **Trap :** lldpReinitDelay	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.3.0 **Définition :** lldpReinitDelay indique le délai (en unités de secondes) à partir du moment où l'objet lldpPortConfigAdminStatus d'un port particulier devient `disabled` jusqu'à ce que la prochaine tentative de réinitialisation. La valeur par défaut de l'objet lldpReintDelay est deux secondes. La valeur de cet objet doit être restaurée à partir du stockage non volatil après une réinitialisation du système de gestion.
Groupe : lldpRemSysGroup **Trap :** lldpRemChassisId	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.4.1.1.5.3496.7.1 **Définition :** valeur de chaîne utilisée pour identifier le composant de châssis associé au système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemChassisIdSubtype	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.4.1.1.4.3496.7.1 **Définition :** type de codage utilisé pour identifier le châssis associé au système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemManAddrIfId	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.4.2.1.4.3496.7.1.1.4.192.168.0.20 **Définition :** valeur entière utilisée pour identifier le numéro d'interface concernant le composant d'adresse de gestion associé au système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemManAddrIfSubtype	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.4.2.1.3.3496.7.1.1.4.192.168.0.20 **Définition :** valeur d'énumération qui identifie la méthode de numérotation d'interface utilisée pour définir le numéro d'interface, associée au système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemManAddrOID	**Accès :** lecture seule **Syntaxe :** OID **OID :** .1.0.8802.1.1.2.1.4.2.1.5.6036.6.1.1.4.192.168.0.33 **Définition :** valeur OID utilisée pour identifier le type de composant matériel ou d'entité de protocole associée à l'adresse de gestion annoncée par l'agent du système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemOrgDefInfo	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.4.4.1.4 **Définition :** ce tableau contient une ou plusieurs lignes par connexion réseau physique qui annonce les informations définies par l'organisation. Notez que ce tableau contient une ou plusieurs lignes d'informations

Groupe/objet	Description
	définies par l'organisation qui ne sont pas reconnues par l'agent local. Si le système local est capable de reconnaître toute information définie par l'organisation, des MIB d'extension appropriées de l'organisation doivent être utilisées pour la récupération d'informations.
Groupe : lldpRemSysGroup **Trap :** lldpRemPortDesc	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.4.1.1.8 **Définition :** valeur de chaîne utilisée pour identifier la description du port donné associé au système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemPortId	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.4.1.1.7.3496.7.1 **Définition :** valeur de chaîne utilisée pour identifier le composant de port associé au système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemPortIdSubtype	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.4.1.1.6.3496.7.1 **Définition :** type de codage d'identificateur de port utilisé dans l'objet `lldpRemPortId` associé.
Groupe : lldpRemSysGroup **Trap :** lldpRemSysCapEnabled	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.4.1.1.12.3496.7.1 **Définition :** valeur bitmap utilisée pour identifier les fonctionnalités système activées sur le système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemSysCapSupported	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.0.8802.1.1.2.1.4.1.1.11.3496.7.1 **Définition :** valeur bitmap utilisée pour identifier les fonctionnalités système prises en charge sur le système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemSysDesc	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.4.1.1.10.3496.7.1 **Définition :** valeur de chaîne utilisée pour identifier la description du système distant.
Groupe : lldpRemSysGroup **Trap :** lldpRemSysName	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.0.8802.1.1.2.1.4.1.1.9.3496.7.1 **Définition :** valeur de chaîne utilisée pour identifier le nom du système distant.
Groupe : lldpNotificationsGroup **Trap :** lldpRemTablesChange	**Syntaxe :** Chaîne **OID :** 1.0.8802.1.1.2.0.0.1.0 **Définition :** une notification lldpRemTablesChange est envoyée lorsque la valeur de lldpStatsRemTableLastChangeTime change. Elle peut être utilisée par un NMS pour déclencher des interrogations de maintenance de tableaux de systèmes distants LLDP. Notez que la transmission des notifications

Groupe/objet	Description
	lldpRemTablesChange est limitée par l'agent, comme spécifié par l'objet `lldpNotificationInterval`.
Groupe : lldpRemSysGroup **Trap :** lldpRemUnknownTLVInfo	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** 1.0.8802.1.1.2.1.4.3.1.2 **Définition :** cet objet représente la valeur extraite du champ de valeur de la TLV.
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRemTablesLastChangeTime	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.0.8802.1.1.2.1.2.1.0 **Définition :** valeur de l'objet sysUpTime (définie dans IETF RFC 3418) au moment où une entrée est créée, modifiée ou supprimée dans les tableaux associés aux objets lldpRemoteSystemsData et à tous les objets d'extension LLDP associés aux systèmes distants. Un NMS peut utiliser cet objet pour réduire l'interrogation des objets lldpRemoteSystemsData.
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRxPortAgeoutsTotal	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.7.1.7.1 **Définition :** compteur qui représente le nombre de vieillissements qui se sont produits sur un port donné. Un vieillissement est le nombre de fois que l'ensemble complet d'informations annoncées par un MSAP particulier a été supprimé des tableaux contenus dans les objets lldpRemoteSystemsData et lldpExtensions parce que l'intervalle d'actualité des informations a expiré. Ce compteur est similaire à lldpStatsRemTablesAgeouts, sauf que le compteur est basé sur un port. Cela permet à NMS d'interroger les tableaux associés aux objets lldpRemoteSystemsData et tous les objets d'extension LLDP associés aux systèmes distants sur le port indiqué uniquement. Ce compteur doit être mis à zéro lors de l'initialisation de l'agent et sa valeur ne doit pas être enregistrée dans un stockage non volatil. Lorsque l'état d'administration d'un port passe de `disabled` à `rxOnly`, `txOnly` ou `txAndRx`, le compteur associé au même port doit être remis à 0. L'agent doit également vider toutes les informations du système distant associées au même port. Ce compteur ne doit être incrémenté qu'une seule fois lorsque l'ensemble complet d'informations est invalidé (a expiré) dans tous les tableaux associés sur un port particulier. Le vieillissement partiel n'est pas autorisé et ne doit donc pas modifier la valeur de ce compteur.
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRxPortFramesDiscardedTotal	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.7.1.2.1 **Définition :** nombre de trames LLDP reçues par cet agent LLDP sur le port indiqué, puis rejetées pour une raison quelconque. Ce compteur peut indiquer que des problèmes de formatage d'en-tête LLDP peuvent exister avec l'agent LLDP local dans le système émetteur ou que des problèmes de validation de LLDPDU peuvent exister avec l'agent LLDP local dans le système récepteur.
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRxPortFramesErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.7.1.3.1 **Définition :** nombre de trames LLDP non valides reçues par cet agent LLDP sur le port indiqué, alors que cet agent LLDP est activé.

Groupe/objet	Description
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRxPortFramesTotal	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.7.1.4.1 **Définition :** nombre de trames LLDP valides reçues par cet agent LLDP sur le port indiqué alors que cet agent LLDP est activé.
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRxPortTLVsDiscardedTotal	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.7.1.5.1 **Définition :** nombre de TLV LLDP rejetées pour une raison quelconque par cet agent LLDP sur le port indiqué.
Groupe : lldpStatsRxGroup **Trap :** lldpStatsRxPortTLVsUnrecognizedTotal	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.7.1.6.1 **Définition :** nombre de TLV LLDP reçues sur le port donné qui ne sont pas reconnues par cet agent LLDP sur le port indiqué. Une TLV non reconnu est appelée TLV dont la valeur de type se situe dans la plage des types de TLV réservés (000 1001 - 111 1110) dans le tableau 9.1 de la norme IEEE 802.1AB-2005. Une TLV non reconnue peut être une TLV de gestion de base d'une version ultérieure de LLDP.
Groupe : lldpStatsTxGroup **Trap :** lldpStatsTxPortFramesTotal	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.0.8802.1.1.2.1.2.6.1.2.1 **Définition :** nombre de trames LLDP transmises par cet agent LLDP sur le port indiqué.
Groupe : lldpConfigTxGroup **Trap :** lldpTxDelay	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.0.8802.1.1.2.1.1.4.0 **Définition :** lldpTxDelay indique le délai (en unités de secondes) entre les transmissions successives de trames LLDP initiées par des changements de valeur/d'état dans la MIB des systèmes locaux LLDP. La valeur recommandée pour lldpTxDelay est définie par la formule suivante : 1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval) La valeur par défaut de l'objet lldpTxDelay est deux secondes. La valeur de cet objet doit être restaurée à partir du stockage non volatil après une réinitialisation du système de gestion.

Q-BRIDGE-MIB

Groupe/objet	Description
Groupe : qBridgeFdbUnicastGroup **Trap :** dot1qFdbDynamicCount	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.7.1.2.1.1.2.255.148.184.197.5.176.0 **Définition :** nombre actuel d'entrées dynamiques dans cette base de données de filtrage.
Groupe : qBridgeServiceRequirementsGroup **Trap :** dot1qForwardAllForbiddenPorts	**Capacité de l'agent :** RC-Q-BRIDGE-MIB-AC **Accès :** lecture seule

Groupe/objet	Description
	Syntaxe : chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.2.4.1.3.22 **Définition :** ensemble de ports configurés par l'administration dans ce VLAN pour lequel l'attribut de condition de service Forward All Multicast Groups peut ne pas être enregistré dynamiquement par GMRP. Cette valeur est restaurée après la réinitialisation de l'appareil. Un port ne peut pas être ajouté à cet ensemble s'il fait déjà partie de l'ensemble de ports dans dot1qForwardAllStaticPorts. La valeur par défaut est une chaîne de zéros de longueur appropriée. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : qBridgeServiceRequirementsGroup **Trap :** dot1qForwardAllPorts	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.2.4.1.1.22 **Définition :** ensemble complet de ports de ce VLAN vers lesquels toutes les trames de multidiffusion adressées au groupe doivent être transmises. Cela inclut les ports pour lesquels ce besoin a été déterminé dynamiquement par GMRP ou configuré statiquement par l'administration.
Groupe : qBridgeServiceRequirementsGroup **Trap :** dot1qForwardAllStaticPorts	**Capacité de l'agent :** RC-Q-BRIDGE-MIB-AC **Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.2.4.1.2.22 **Définition :** ensemble de ports de ce VLAN configurés par l'administration vers lesquels toutes les trames de multidiffusion adressées au groupe doivent être transmises. Les ports entrés dans cette liste apparaissent également dans l'ensemble complet affiché par dot1qForwardAllPorts. Cette valeur est restaurée après la réinitialisation de l'appareil. Cela s'applique uniquement aux ports membres du VLAN définis par dot1qVlanCurrentEgressPorts. Un port ne peut pas être ajouté à cet ensemble s'il fait déjà partie de l'ensemble de ports dans dot1qForwardAllForbiddenPorts. La valeur par défaut est une chaîne de uns de longueur appropriée, pour indiquer le comportement standard d'utilisation des services de filtrage de base, c'est-à-dire transmettre toutes les multidiffusions à tous les ports. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : qBridgeServiceRequirementsGroup **Trap :** dot1qForwardUnregisteredForbiddenPorts	**Accès :** lecture et écriture **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.2.5.1.3.22 **Définition :** ensemble de ports configurés par l'administration dans ce VLAN pour lequel l'attribut de condition de service Forward Unregistered Multicast Groups peut ne pas être enregistré dynamiquement par GMRP. Cette valeur est restaurée après la réinitialisation de l'appareil. Un port ne peut pas être ajouté à cet ensemble s'il fait déjà partie de l'ensemble de ports dans dot1qForwardUnregisteredStaticPorts. La valeur par défaut est une chaîne de zéros de longueur appropriée. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : qBridgeServiceRequirementsGroup **Trap :** dot1qForwardUnregisteredPorts	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.2.5.1.1.22 **Définition :** ensemble complet de ports de ce VLAN vers lesquels sont transmises les trames adressées au groupe de multidiffusion pour lesquelles il n'existe plus d'informations de transmission spécifiques. Cela inclut les

Groupe/objet	Description
	ports pour lesquels ce besoin a été déterminé dynamiquement par GMRP ou configuré statiquement par l'administration.
Groupe : qBridgeServiceRequirementsGroup **Trap :** dot1qForwardUnregisteredStaticPorts	**Accès :** lecture et écriture **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.2.5.1.2.22 **Définition :** ensemble de ports configurés par l'administration, dans ce VLAN, vers lesquels les trames adressées au groupe de multidiffusion pour lesquelles il n'existe plus d'informations de transmission spécifiques doivent être transmises. Les ports entrés dans cette liste apparaissent également dans l'ensemble complet affiché par dot1qForwardUnregisteredPorts. Cette valeur est restaurée après la réinitialisation de l'appareil. Un port ne peut pas être ajouté à cet ensemble s'il fait déjà partie de l'ensemble de ports dans dot1qForwardUnregisteredForbiddenPorts. La valeur par défaut est une chaîne de zéros de longueur appropriée, bien que cela n'ait aucun effet sur la valeur par défaut de dot1qForwardAllStaticPorts. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : qBridgeBaseGroup **Trap :** dot1qGvrpStatus	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.1.5.0 **Définition :** état administratif demandé par l'administration pour GVRP. La valeur enabled(1) indique que GVRP doit être activé sur cet appareil, sur tous les ports pour lesquels il n'a pas été spécifiquement désactivé. Si cet objet a la valeur disabled(2), GVRP est désactivé sur tous les ports et tous les paquets GVRP sont transmis de manière transparente. Cet objet affecte toutes les machines d'état GVRP Applicant et Registrar. Le passage de disabled(2) à enabled(1) entraîne une réinitialisation de toutes les machines d'état GVRP sur tous les ports. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : qBridgeBaseGroup **Trap :** dot1qMaxSupportedVlans	**Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.3.6.1.2.1.17.7.1.1.3.0 **Définition :** nombre maximum de VLAN IEEE 802.1Q pris en charge par cet appareil.
Groupe : qBridgeBaseGroup **Trap :** dot1qMaxVlanId	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.1.2.0 **Définition :** ID VLAN IEEE 802.1Q maximum pris en charge par cet appareil.
Groupe : qBridgeVlanStaticGroup **Trap :** dot1qNextFreeLocalVlanIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.4.4.0 **Définition :** prochaine valeur disponible pour dot1qVlanIndex d'une entrée de VLAN local dans dot1qVlanStaticTable. Cela indiquera des valeurs >=4096 si un nouveau VLAN local peut être créé ou bien la valeur 0 si ce n'est pas possible. Une opération de création de ligne dans ce tableau pour une entrée avec une valeur VlanIndex locale peut échouer si la valeur actuelle de cet objet n'est pas utilisée comme index. Même si la valeur lue est utilisée, il n'y a aucune garantie qu'elle sera toujours l'index valide lorsque l'opération de création est tentée ; un autre gestionnaire est peut-être déjà entré dans l'intervalle de temps écoulé. Dans ce cas, dot1qNextFreeLocalVlanIndex doit être relu et la création est tentée de nouveau avec la nouvelle valeur. Cette

Groupe/objet	Description
	valeur change automatiquement lorsque la valeur actuelle est utilisée pour créer une nouvelle ligne.
Groupe : qBridgeBaseGroup **Trap :** dot1qNumVlans	**Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.3.6.1.2.1.17.7.1.1.4.0 **Définition :** nombre actuel de VLAN IEEE 802.1Q configurés dans cet appareil.
Groupe : qBridgePortGroup2 **Trap :** dot1qPortAcceptableFrameTypes	**Capacité de l'agent :** RC-Q-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.4.5.1.2.1 **Définition :** lorsque la valeur admitOnlyVlanTagged(2) est définie, l'appareil rejette les trames non balisées ou les trames balisées avec une priorité reçues sur ce port. Lorsque la valeur admitAll(1) est définie, les trames non balisées ou les trames balisées avec une priorité reçues sur ce port sont acceptées et affectées à un VID basé sur le PVID et le VID défini pour ce port. Ce contrôle n'affecte pas les trames BPDU (Bridge Protocol Data Unit) indépendantes du VLAN, telles que GVRP et Spanning Tree Protocol (STP). Cela affecte les trames BPDU dépendantes du VLAN, telles que GMRP. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion. **Remarque** La valeur de `admitOnlyVlanTagged(2)` n'est pas prise en charge.
Groupe : qBridgePortGroup2 **Trap :** dot1qPortGvrpStatus	**Capacité de l'agent :** RC-Q-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.4.5.1.4.1 **Définition :** état du fonctionnement GVRP sur ce port. La valeur enabled(1) indique que GVRP est activé sur ce port, tant que dot1qGvrpStatus est également activé pour cet appareil. Lorsque la valeur disabled(2) est définie mais que dot1qGvrpStatus est toujours activé pour l'appareil, GVRP est désactivé sur ce port : tous les paquets GVRP reçus sont rejetés en silence et aucun enregistrement GVRP n'est propagé à partir d'autres ports. Cet objet affecte toutes les machines d'état GVRP Applicant et Registrar sur ce port. Le passage de disabled(2) à enabled(1) entraîne une réinitialisation de toutes les machines d'état GVRP sur ce port. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion. **Remarque** La valeur par défaut est `disabled(2)`.
Groupe : qBridgePortGroup2 **Trap :** dot1qPortIngressFiltering	**Capacité de l'agent :** RC-Q-BRIDGE-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.4.5.1.3.1 **Définition :** lorsque la valeur true(1) est définie, l'appareil rejette les trames entrantes pour les VLAN qui n'incluent pas ce port dans son ensemble de membres. Si la valeur false(2) est définie, le port accepte toutes les trames entrantes. Ce contrôle n'affecte pas les trames BPDU indépendantes du

Groupe/objet	Description
	VLAN, telles que GVRP et STP. Cela affecte les trames BPDU dépendantes du VLAN, telles que GMRP. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion. **Remarque** La valeur `true(1)` n'est pas prise en charge.
Groupe : qBridgePortGroup2 **Trap :** dot1qPvid	**Accès :** lecture et écriture **Syntaxe :** Gauge32 **OID :** .1.3.6.1.2.1.17.7.1.4.5.1.1.1 **Définition :** PVID, VLAN-ID affecté aux trames non balisées ou aux trames balisées avec une priorité reçues sur ce port. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : qBridgeFdbUnicastGroup **Trap :** dot1qTpFdbPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.2.2.1.2.255.148.184.197.5.176.0 **Définition :** soit la valeur `0`, soit le numéro du port sur lequel une trame ayant une adresse source égale à la valeur de l'instance correspondante de dot1qTpFdbAddress a été vu(e). La valeur `0` indique que le numéro de port n'a pas été appris, mais que l'appareil dispose d'informations de transmission/filtrage sur cette adresse (par exemple, dans dot1qStaticUnicastTable). Les responsables de la mise en œuvre sont encouragés à affecter la valeur de port à cet objet chaque fois qu'il est appris, même pour les adresses pour lesquelles la valeur correspondante de dot1qTpFdbStatus est not learned(3).
Groupe : qBridgeFdbUnicastGroup **Trap :** dot1qTpFdbStatus	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.2.2.1.3.255.148.184.197.5.176.0 **Définition :** état de cette entrée. Voici les significations des valeurs : • other(1) - aucune des valeurs suivantes. Cela peut inclure le cas où un autre objet MIB (pas l'instance correspondante de dot1qTpFdbPort, ni une entrée dans dot1qStaticUnicastTable) est utilisé pour déterminer si et comment les trames adressées à la valeur de l'instance correspondante de dot1qTpFdbAddress sont transmises. • invalid(2) - cette entrée n'est plus valide (par exemple, elle a été apprise mais a expiré depuis), mais n'a pas encore été supprimée du tableau. • learn(3) - la valeur de l'instance correspondante de dot1qTpFdbPort a été apprise et est utilisée. • self(4) - la valeur de l'instance correspondante de dot1qTpFdbAddress représente l'une des adresses de l'appareil. L'instance correspondante de dot1qTpFdbPort indique le port de l'appareil qui possède cette adresse. • mgmt(5) - la valeur de l'instance correspondante de dot1qTpFdbAddress est également la valeur d'une instance existante de dot1qStaticAddress.
Groupe : qBridgeFdbMulticastGroup **Trap :** dot1qTpGroupEgressPorts	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.2.3.1.2 **Définition :** ensemble complet de ports, dans ce VLAN, vers lesquels les trames destinées à cette adresse MAC de groupe sont actuellement explicitement transmises. Cela n'inclut pas les ports pour lesquels cette adresse n'est transmise qu'implicitement dans la liste dot1qForwardAllPorts.

Groupe/objet	Description
Groupe : qBridgeFdbMulticastGroup **Trap :** dot1qTpGroupLearnt	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.2.3.1.3 **Définition :** sous-ensemble de ports dans dot1qTpGroupEgressPorts qui ont été appris par GMRP ou un autre mécanisme dynamique dans cette base de données de filtrage.
Groupe : qBridgeVlanGroup **Trap :** dot1qVlanCreationTime	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.17.7.1.4.2.1.7 **Définition :** valeur de sysUpTime lors de la création de ce VLAN.
Groupe : qBridgeVlanGroup **Trap :** dot1qVlanCurrentEgressPorts	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.4.2.1.4 **Définition :** ensemble de ports qui transmettent le trafic pour ce VLAN sous forme de trames balisées ou non balisées.
Groupe : qBridgeVlanGroup **Trap :** dot1qVlanCurrentUntaggedPorts	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** .1.3.6.1.2.1.17.7.1.4.2.1.5 **Définition :** ensemble de ports qui transmettent le trafic pour ce VLAN sous forme de trames non balisées.
Groupe : qBridgeVlanGroup **Trap :** dot1qVlanFdbId	**Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.3.6.1.2.1.17.7.1.4.2.1.3 **Définition :** base de données de filtrage utilisée par ce VLAN. Il s'agit de l'une des valeurs dot1qFdbId dans dot1qFdbTable. Cette valeur est attribuée automatiquement par l'appareil à chaque création du VLAN : soit dynamiquement par GVRP, soit par l'administration, dans dot1qVlanStaticTable. L'attribution de cette valeur suit les contraintes d'apprentissage définies pour ce VLAN dans dot1qLearningConstraintsTable.
Groupe : qBridgeVlanStaticGroup **Trap :** dot1qVlanForbiddenEgressPorts	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.17.7.1.4.3.1.3.22 **Définition :** ensemble de ports dont l'administration a interdit l'inclusion dans la liste de sorties pour ce VLAN. Les modifications apportées à cet objet qui entraînent l'inclusion ou l'exclusion d'un port affectent le contrôle du registraire par port et par VLAN pour l'enregistrement interdit pour la machine d'état GVRP appropriée sur chaque port. Un port ne peut pas être ajouté à cet ensemble s'il fait déjà partie de l'ensemble de ports dans dot1qVlanStaticEgressPorts. La valeur par défaut de cet objet est une chaîne de zéros de longueur appropriée, excluant tous les ports de l'ensemble interdit.
Groupe : qBridgeVlanGroup **Trap :** dot1qVlanNumDeletes	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.17.7.1.4.1 **Définition :** nombre de fois qu'une entrée VLAN a été supprimée de dot1qVlanCurrentTable (pour une raison quelconque). Si une entrée est

Groupe/objet	Description
	supprimée, puis insérée, et ensuite supprimée, ce compteur est incrémenté de 2.
Groupe : qBridgeVlanStaticGroup **Trap :** dot1qVlanStaticEgressPorts	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.17.7.1.4.3.1.2.22 **Définition :** ensemble de ports affectés en permanence à la liste de sorties pour ce VLAN par l'administration. Les modifications apportées à un bit dans cet objet affectent le contrôle du registraire par port et par VLAN pour l'enregistrement fixé pour la machine d'état GVRP appropriée sur chaque port. Un port ne peut pas être ajouté à cet ensemble s'il fait déjà partie de l'ensemble de ports dans dot1qVlanForbiddenEgressPorts. La valeur par défaut de cet objet est une chaîne de zéros de longueur appropriée indiquant non fixe.
Groupe : qBridgeVlanStaticGroup **Trap :** dot1qVlanStaticName	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.17.7.1.4.3.1.1.22 **Définition :** chaîne affectée administrativement, qui peut être utilisée pour identifier le VLAN.
Groupe : qBridgeVlanStaticGroup **Trap :** dot1qVlanStaticRowStatus	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.4.3.1.5.22 **Définition :** cet objet indique l'état de cette entrée.
Groupe : qBridgeVlanStaticGroup **Trap :** dot1qVlanStaticUntaggedPorts	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.17.7.1.4.3.1.4.22 **Définition :** ensemble de ports qui doivent transmettre les paquets de sortie pour ce VLAN sous forme non balisée. La valeur par défaut de cet objet pour le VLAN par défaut (dot1qVlanIndex = 1) est une chaîne de longueur appropriée incluant tous les ports. Aucune valeur par défaut n'est spécifiée pour les autres VLAN. Si un agent d'appareil ne peut pas prendre en charge l'ensemble de ports défini, il rejette l'opération de réglage en émettant une erreur. Par exemple, un gestionnaire peut tenter de définir que plus d'un VLAN n'est pas balisé à la sortie alors que l'appareil ne prend pas en charge cette option IEEE 802.1Q.
Groupe : qBridgeVlanGroup **Trap :** dot1qVlanStatus	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.4.2.1.6 **Définition :** cet objet indique l'état de cette entrée. • other(1) - Cette entrée est actuellement utilisée, mais les conditions dans lesquelles elle le restera diffèrent des valeurs suivantes. • permanent(2) - Cette entrée, correspondant à une entrée dans dot1qVlanStaticTable, est actuellement utilisée et le restera après la prochaine réinitialisation de l'appareil. Les listes de ports pour cette entrée incluent les ports de l'entrée dot1qVlanStaticTable équivalente et les ports appris dynamiquement. • dynamicGvrp(3) - Cette entrée est actuellement utilisée et le restera jusqu'à ce qu'elle soit supprimée par GVRP. Il n'existe pas d'entrée statique pour ce VLAN et il sera supprimé lorsque le dernier port quittera le VLAN.

Groupe/objet	Description
Groupe : qBridgeBaseGroup **Trap :** dot1qVlanVersionNumber	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.7.1.1.1.0 **Définition :** numéro de version d'IEEE 802.1Q pris en charge par cet appareil.

RMON-MIB

Groupe/objet	Description
Groupe : rmonAlarmGroup **Trap :** AlarmFallingEventIndex	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.10.1 **Définition :** index d'eventEntry utilisé lorsqu'un seuil descendant est dépassé. eventEntry identifié par une valeur spécifique de cet index est le même que celui identifié par la même valeur de l'objet eventIndex. S'il n'existe aucune entrée correspondante dans eventTable, aucune association n'existe. Aucun événement associé n'est généré en particulier si la valeur est zéro, car zéro n'est pas un index d'événement valide. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1).
Groupe : rmonAlarmGroup **Trap :** AlarmFallingThreshold	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.8.1 **Définition :** seuil de la statistique échantillonnée. Lorsque la valeur 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 après que cette entrée est devenue valide est inférieur ou égal à ce seuil et que l'alarmStartupAlarm associée est égale à fallingAlarm(2) ou risingOrFallingAlarm(3). Après la génération d'un événement descendant, un autre événement de ce type n'est pas généré tant que la valeur échantillonnée ne dépasse pas ce seuil et n'atteint pas alarmRisingThreshold. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1).
Groupe : rmonAlarmGroup **Trap :** AlarmIndex	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.1.1 **Définition :** index qui identifie de manière unique une entrée dans le tableau Alarms. Chacune de ces entrées définit un échantillon de diagnostic à un intervalle particulier pour un objet sur l'appareil. Quatre entrées par port en moyenne peuvent être créées dans alarmTable.
Groupe : rmonAlarmGroup **Trap :** AlarmInterval	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.2.1 **Définition :** intervalle en secondes pendant lequel les données sont échantillonnées et comparées avec les seuils montant et descendant. Lors de la définition de cette variable, des précautions doivent être prises

Groupe/objet	Description
	dans le cas de l'échantillonnage de deltaValue - l'intervalle défini doit être suffisamment court pour que la variable échantillonnée ne soit guère susceptible d'augmenter ou de diminuer de plus de 2^31 - 1 au cours d'un seul intervalle d'échantillonnage. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1). La valeur par défaut d'alarmInterval est de 60 secondes.
Groupe : rmonAlarmGroup **Trap :** AlarmOwner	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.3.1.1.11.1 **Définition :** entité qui a configuré cette entrée et utilise donc les ressources qui lui sont affectées. La valeur par défaut d'alarmOwner est une chaîne `Monitor`.
Groupe : rmonAlarmGroup **Trap :** AlarmRisingEventIndex	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.9.1 **Définition :** index d'eventEntry utilisé lorsqu'un seuil montant est dépassé. eventEntry identifié par une valeur spécifique de cet index est le même que celui identifié par la même valeur de l'objet eventIndex. S'il n'existe aucune entrée correspondante dans eventTable, aucune association n'existe. Aucun événement associé n'est généré en particulier si la valeur est zéro, car zéro n'est pas un index d'événement valide. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1).
Groupe : rmonAlarmGroup **Trap :** AlarmRisingThreshold	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.7.1 **Définition :** seuil de la statistique échantillonnée. Lorsque la valeur 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 après que cette entrée est devenue valide, est supérieur ou égal à ce seuil et que l'alarmStartupAlarm associée est égale à risingAlarm(1) ou risingOrFallingAlarm(3). Après la génération d'un événement montant, un autre événement de ce type n'est pas généré tant que la valeur échantillonnée ne descend pas en-dessous de ce seuil et n'atteint pas alarmFallingThreshold. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1).
Groupe : rmonAlarmGroup **Trap :** AlarmSampleType	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.4.1 **Définition :** méthode d'échantillonnage de la variable sélectionnée et de calcul de la valeur à comparer avec les seuils. Si la valeur de cet objet est absoluteValue(1), la valeur de la variable sélectionnée est directement comparée avec les seuils à la fin de l'intervalle d'échantillonnage. Si la valeur de cet objet est deltaValue(2), la valeur de la variable sélectionnée au dernier échantillon est soustraite de la valeur actuelle, et la différence est comparée avec les seuils. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1). La valeur par défaut d'alarmSampleType est `deltaValue(2)`.
Groupe : rmonAlarmGroup	**Capacité de l'agent :** RC-RMON-MIB-AC

Groupe/objet	Description
Trap : AlarmStartupAlarm	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.6.1 **Définition :** alarme pouvant être envoyée lorsque cette entrée est définie pour la première fois sur valide. Si le premier échantillon après que cette entrée est devenue valide est supérieur ou égal à risingThreshold et qu'alarmStartupAlarm est égale à risingAlarm(1) ou risingOrFallingAlarm(3), une alarme montante unique est générée. Si le premier échantillon après que cette entrée est devenue valide est inférieur ou égal à fallingThreshold et qu'alarmStartupAlarm est égale à fallingAlarm(2) ou risingOrFallingAlarm(3), une alarme descendante unique est générée. Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1). La valeur par défaut d'alarmStartupAlarm est `risingOrFallingAlarm(3)`.
Groupe : rmonAlarmGroup **Trap :** AlarmStatus	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.12.1 **Définition :** état de cette entrée d'alarme.
Groupe : rmonAlarmGroup **Trap :** AlarmValue	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.3.1.1.5.1 **Définition :** valeur de la statistique pendant la dernière période d'échantillonnage. Par exemple, si le type d'échantillon est deltaValue, cette valeur sera la différence entre les échantillons au début et à la fin de la période. Si le type d'échantillon est absoluteValue, cette valeur est la valeur échantillonnée à la fin de la période. Il s'agit de la valeur qui est comparée aux seuils montant et descendant. La valeur pendant la période d'échantillonnage en cours n'est pas mise à disposition tant que la période n'est pas terminée et reste disponible jusqu'à la fin de la période suivante.
Groupe : rmonAlarmGroup **Trap :** AlarmVariable	**Accès :** Lecture et création **Syntaxe :** OID **OID :** 1.3.6.1.2.1.16.3.1.1.3.1 **Définition :** identificateur d'objet 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. Étant donné que le contrôle d'accès SNMP est entièrement articulé en termes de contenu des vues MIB, il n'existe aucun mécanisme de contrôle d'accès qui puisse restreindre la valeur de cet objet pour identifier uniquement les objets qui existent dans une vue MIB spécifique. Puisqu'il n'y a donc aucun moyen acceptable de restreindre l'accès en lecture via le mécanisme d'alarme, la sonde ne doit accorder l'accès en écriture à cet objet que dans les vues qui ont un accès en lecture à tous les objets de la sonde. Lors d'une opération de réglage, une erreur badValue sera renvoyée si le nom de variable fourni n'est pas disponible dans la vue MIB sélectionnée. Si, à tout moment, le nom de la variable d'une alarmEntry établie n'est plus disponible dans la vue MIB sélectionnée, la sonde doit faire passer l'état de cette alarmEntry à invalid(4). Cet objet ne peut pas être modifié si l'objet alarmStatus associé est égal à valid(1).
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryBroadcastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.7.1

Groupe/objet	Description
	Définition : nombre de bons paquets reçus pendant cet intervalle d'échantillonnage qui ont été dirigés vers l'adresse de diffusion.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoriqueCollisions	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.14.1 **Définition :** meilleure estimation du nombre total de collisions sur ce segment Ethernet pendant cet intervalle d'échantillonnage. La valeur renvoyée dépend de l'emplacement de la sonde RMON. La section 8.2.1.3 (10BASE-5) et la section 10.3.1.3 (10BASE-2) de la norme IEEE 802.3 stipulent qu'une station doit détecter une collision en mode réception si trois stations ou plus émettent simultanément. Un port répéteur doit détecter une collision lorsque deux stations ou plus émettent simultanément. Ainsi, une sonde placée sur un port répéteur peut enregistrer plus de collisions qu'une sonde connectée à une station sur le même segment. L'emplacement de la sonde joue un rôle beaucoup moins important si l'on se base sur 10BASE-T. 14.2.1.4 (10BASE-T) de la norme IEEE 802.3 définit une collision comme la présence simultanée de signaux sur les circuits DO et RD (d'émission et de réception simultanément). Une station 10BASE-T ne peut détecter les collisions que lorsqu'elle émet. Ainsi les sondes placées sur une station et un répéteur devraient signaler le même nombre de collisions. Notez également qu'une sonde RMON à l'intérieur d'un répéteur devrait idéalement signaler les collisions entre le répéteur et un ou plusieurs autres hôtes (collisions de transmission telles que définies par IEEE 802.3k) ainsi que les collisions de récepteur observées sur tous les segments coaxiaux auxquels le répéteur est connecté.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryCRCAlignErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.9.1 **Définition :** nombre de paquets reçus au cours de cet intervalle d'échantillonnage dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 64 et 1518 octets inclus, mais qui avaient soit une séquence de contrôle de trame erronée (Frame Check Sequence, FCS) avec un nombre entier d'octets (erreur FCS) soit une FCS erronée avec un nombre d'octets non entier (erreur d'alignement).
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryDropEvents	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.4.1 **Définition :** nombre total d'événements au cours desquels des paquets ont été abandonnés par la sonde en raison d'un manque de ressources pendant cet intervalle d'échantillonnage. Notez que ce nombre ne correspond pas nécessairement au nombre de paquets abandonnés, il s'agit juste le nombre de fois que cette condition a été détectée.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryFragments	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.12.1 **Définition :** nombre total de paquets reçus au cours de cet intervalle d'échantillonnage dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était inférieure à 64 octets, et qui avaient soit une séquence de contrôle de trame erronée (Frame Check Sequence, FCS) avec un nombre entier d'octets (erreur FCS) soit une FCS erronée avec un nombre d'octets non entier (erreur d'alignement). Notez qu'il est tout à fait normal

Groupe/objet	Description
	qu'etherHistoryFragments s'incrémente. En effet, il compte à la fois les runts (qui sont des occurrences normales dues aux collisions) et les bruits.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.2.1.1.1 **Définition :** historique dont cette entrée fait partie. L'historique identifié par une valeur particulière de cet index est le même historique que celui identifié par la même valeur de historyControlIndex.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryIntervalStart	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** 1.3.6.1.2.1.16.2.2.1.3.1 **Définition :** valeur de sysUpTime au début de l'intervalle sur lequel cet échantillon a été mesuré. Si la sonde conserve une trace de l'heure de la journée, elle doit démarrer le premier échantillon de l'historique à un moment tel que lorsque l'heure suivante de la journée commence. Un échantillon est démarré à cet instant. Notez que le respect de cette règle peut obliger la sonde à retarder la collecte du premier échantillon de l'historique, car chaque échantillon doit appartenir au même intervalle. Notez également que l'échantillon actuellement collecté n'est accessible dans ce tableau qu'à la fin de son intervalle.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryJabbers	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.13.1 **Définition :** nombre de paquets reçus au cours de cet intervalle d'échantillonnage dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était supérieure à 1518 octets et qui avaient soit une séquence de contrôle de trame erronée (Frame Check Sequence, FCS) avec un nombre entier d'octets (erreur FCS) soit une FCS erronée avec un nombre d'octets non entier (erreur d'alignement). Notez que cette définition d'une transmission anormalement longue est différente de la définition fournie dans IEEE-802.3 section 8.2.1.5 (10BASE5) et section 10.3.1.4 (10BASE2). Ces documents définissent une transmission anormalement longue comme la condition dans laquelle tout paquet dépasse 20 ms. La plage autorisée pour détecter une transmission anormalement longue est comprise entre 20 ms et 150 ms.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryMulticastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.8.1 **Définition :** nombre de bons paquets reçus pendant cet intervalle d'échantillonnage qui ont été dirigés vers une adresse de multidiffusion. Notez que ce nombre n'inclut pas les paquets adressés à l'adresse de diffusion.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryOctets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.5.1 **Définition :** nombre total d'octets de données (y compris ceux des mauvais paquets) reçus sur le réseau (à l'exclusion des bits de trame mais y compris les octets FCS).
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryOversizePkts	**Accès :** lecture seule **Syntaxe :** Counter32

Groupe/objet	Description
	OID : 1.3.6.1.2.1.16.2.2.1.11.1 **Définition :** nombre de paquets reçus au cours de cet intervalle d'échantillonnage dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était supérieure à 1 518 octets mais qui étaient par ailleurs bien formés.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.6.1 **Définition :** nombre de paquets (y compris les mauvais paquets) reçus pendant cet intervalle d'échantillonnage.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistorySampleIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.2.1.2.1 **Définition :** index identifiant de manière unique l'échantillon spécifique que cette entrée représente parmi tous les échantillons associés au même historyControlEntry. Cet index commence à 1 et est incrémenté de un à chaque nouveau prélèvement d'échantillon.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryUndersizePkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.2.2.1.10.1 **Définition :** nombre de paquets reçus au cours de cet intervalle d'échantillonnage dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était inférieure à 64 octets et qui étaient par ailleurs bien formés.
Groupe : rmonEthernetHistoryGroup **Trap :** etherHistoryUtilization	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.2.1.15.1 **Définition :** meilleure estimation de l'utilisation moyenne du réseau de la couche physique sur cette interface pendant cet intervalle d'échantillonnage en centièmes de pour cent.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsBroadcastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.6.1 **Définition :** nombre total de bons paquets reçus qui ont été dirigés vers l'adresse de diffusion. Notez que cela n'inclut pas les paquets de multidiffusion.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsCollisions	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.13.1 **Définition :** meilleure estimation du nombre total de collisions sur ce segment Ethernet. La valeur renvoyée dépend de l'emplacement de la sonde RMON. La section 8.2.1.3 (10BASE-5) et la section 10.3.1.3 (10BASE-2) de la norme IEEE 802.3 stipulent qu'une station doit détecter une collision en mode réception si trois stations ou plus émettent simultanément. Un port répéteur doit détecter une collision lorsque deux stations ou plus émettent simultanément. Ainsi, une sonde placée sur un port répéteur peut enregistrer plus de collisions qu'une sonde connectée à une station sur le même segment. L'emplacement de la sonde joue un rôle beaucoup moins

Groupe/objet	Description
	important si l'on se base sur 10BASE-T. 14.2.1.4 (10BASE-T) de la norme IEEE 802.3 définit une collision comme la présence simultanée de signaux sur les circuits DO et RD (d'émission et de réception simultanément). Une station 10BASE-T ne peut détecter les collisions que lorsqu'elle émet. Ainsi les sondes placées sur une station et un répéteur devraient signaler le même nombre de collisions. Notez également qu'une sonde RMON à l'intérieur d'un répéteur devrait idéalement signaler les collisions entre le répéteur et un ou plusieurs autres hôtes (collisions de transmission telles que définies par IEEE 802.3k) ainsi que les collisions de récepteur observées sur tous les segments coaxiaux auxquels le répéteur est connecté.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsCRCAlignErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.8.1 **Définition :** nombre total de paquets reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 64 et 1518 octets inclus, mais qui avaient soit une séquence de contrôle de trame erronée (Frame Check Sequence, FCS) avec un nombre entier d'octets (erreur FCS), soit une FCS erronée avec un nombre d'octets non entier (erreur d'alignement).
Groupe : rmonEtherStatsGroup **Trap :** etherStatsDataSource	**Accès :** Lecture et création **OID :** 1.3.6.1.2.1.16.1.1.1.2.1 **Définition :** cet objet identifie la source des données que cette entrée etherStats est configurée pour analyser. Cette source peut être n'importe quelle interface Ethernet sur cet appareil. Afin d'identifier une interface spécifique, cet objet doit identifier l'instance de l'objet ifIndex définie dans RFC 2233 [17] pour l'interface souhaitée. Par exemple, si une entrée doit recevoir des données de l'interface n°1, cet objet est défini sur ifIndex.1. Les statistiques de ce groupe reflètent tous les paquets sur le segment de réseau local attaché à l'interface identifiée. Un agent peut ou non être en mesure de dire si des modifications fondamentales du support de l'interface se sont produites qui nécessitent une invalidation de cette entrée. Par exemple, une carte Ethernet enfichable à chaud peut être retirée et remplacée par une carte Token Ring. Dans ce cas, si l'agent a connaissance de cette modification, il est recommandé qu'il invalide cette entrée. Cet objet ne peut pas être modifié si l'objet etherStatsStatus associé est égal à valid(1).
Groupe : rmonEtherStatsGroup **Trap :** etherStatsDropEvents	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.3.1 **Définition :** nombre total d'événements au cours desquels des paquets ont été abandonnés par la sonde en raison d'un manque de ressources. Notez que ce nombre ne correspond pas nécessairement au nombre de paquets abandonnés. Il s'agit juste le nombre de fois que cette condition a été détectée.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsFragments	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.11.1 **Définition :** nombre total de paquets reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était inférieure à 64 octets, et qui avaient soit une séquence de contrôle de trame erronée (Frame Check Sequence, FCS) avec un nombre entier d'octets (erreur FCS) soit une FCS erronée avec un nombre d'octets non entier (erreur d'alignement). Notez qu'il est tout à fait normal qu'etherStatsFragments s'incrémente. En effet,

Groupe/objet	Description
	il compte à la fois les runts (qui sont des occurrences normales dues aux collisions) et les bruits.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsIndex	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.1.1.1.1.1 **Définition :** la valeur de cet objet identifie de manière unique cette entrée etherStats. **Remarque** Deux entrées par port sont créées dans etherStatsTable.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsJabbers	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.12.1 **Définition :** nombre total de paquets reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était supérieure à 1518 octets et qui avaient soit une séquence de contrôle de trame erronée (Frame Check Sequence, FCS) avec un nombre entier d'octets (erreur FCS) soit une FCS erronée avec un nombre d'octets non entier (erreur d'alignement). Notez que cette définition d'une transmission anormalement longue est différente de la définition fournie dans IEEE-802.3 section 8.2.1.5 (10BASE5) et section 10.3.1.4 (10BASE2). Ces documents définissent une transmission anormalement longue comme la condition dans laquelle tout paquet dépasse 20 ms. La plage autorisée pour détecter une transmission anormalement longue est comprise entre 20 ms et 150 ms.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsMulticastPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.7.1 **Définition :** nombre total de bons paquets reçus qui ont été dirigés vers une adresse de multidiffusion. Notez que ce nombre n'inclut pas les paquets dirigés vers l'adresse de diffusion.

Groupe : rmonEtherStatsGroup
Trap : etherStatsOctets
	Accès : lecture seule
	Syntaxe : Counter32
	OID : 1.3.6.1.2.1.16.1.1.1.4.1
	Définition : nombre total d'octets de données (y compris ceux des mauvais paquets) reçus sur le réseau (à l'exclusion des bits de trame mais y compris les octets FCS). Cet objet peut être utilisé comme une estimation raisonnable de l'utilisation d'Ethernet 10 mégabits. Si une plus grande précision est souhaitée, les objets etherStatsPkts et etherStatsOctets doivent être échantillonnés avant et après un intervalle commun. Les différences dans les valeurs échantillonnées sont Pkts et Octets, respectivement, et le nombre de secondes dans l'intervalle est Interval. Ces valeurs sont utilisées pour calculer l'utilisation comme suit :
	`Pkts * (9.6 + 6.4) + (Octets * .8)`
	`Utilization = ----------------------------------`
	`Interval * 10,000`
	Le résultat de cette équation est la valeur Utilization qui est le pourcentage d'utilisation du segment Ethernet sur une échelle de 0 à 100 %.

Groupe/objet	Description
Groupe : rmonEtherStatsGroup **Trap :** etherStatsOversizePkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.10.1 **Définition :** nombre total de paquets reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était supérieure à 1 518 octets et qui étaient par ailleurs bien formés.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsOwner	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.1.1.1.20.1 **Définition :** entité qui a configuré cette entrée et utilise donc les ressources qui lui sont affectées. La valeur de cette entrée est toujours définie sur `Monitor` et ne peut pas être modifiée.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.5.1 **Définition :** nombre total de paquets (y compris les mauvais paquets, les paquets de diffusion et les paquets de multidiffusion) reçus.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts1024to1518Octets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.19.1 **Définition :** nombre total de paquets (y compris les mauvais paquets) reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 1024 et 1518 octets inclus.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts128to255Octets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.16.1 **Définition :** nombre total de paquets (y compris les mauvais paquets) reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 128 et 255 octets inclus.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts256to511Octets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.17.1 **Définition :** nombre total de paquets (y compris les mauvais paquets) reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 256 et 511 octets inclus.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts512to1023Octets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.18.1 **Définition :** nombre total de paquets (y compris les mauvais paquets) reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 512 et 1023 octets inclus.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts64Octets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.14.1

Groupe/objet	Description
	Définition : nombre total de paquets (y compris les mauvais paquets) reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était de 64 octets.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsPkts65to127Octets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.15.1 **Définition :** nombre total de paquets (y compris les mauvais paquets) reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était comprise entre 65 et 127 octets inclus.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsStatus	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.1.1.1.21.1 **Définition :** état de cette entrée etherStats. **Remarque** Une entrée par port est créée dans etherStatsTable lors de l'initialisation. Ces entrées ne peuvent être ni modifiées ni supprimées. Aucune nouvelle entrée ne peut être créée. Par conséquent, historyControlStatus est toujours défini sur `valid(1)`.
Groupe : rmonEtherStatsGroup **Trap :** etherStatsUndersizePkts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.16.1.1.1.9.1 **Définition :** nombre total de paquets reçus dont la longueur (à l'exclusion des bits de trame mais y compris les octets FCS) était inférieure à 64 octets et qui étaient par ailleurs bien formés.
Groupe : rmonEventGroup **Trap :** eventCommunity	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.9.1.1.4.1 **Définition :** si un trap SNMP doit être envoyé, il est envoyé à la communauté SNMP spécifiée par cette chaîne d'octets. Une chaîne de 30 caractères maximum est prise en charge pour cet objet.
Groupe : rmonEventGroup **Trap :** eventDescription	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.9.1.1.2.1 **Définition :** commentaire décrivant cette entrée d'événement.
Groupe : rmonEventGroup **Trap :** eventIndex	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.9.1.1.1.1 **Définition :** index qui identifie de manière unique une entrée dans le tableau Event. Chacune de ces entrées définit un événement qui doit être généré lorsque les conditions appropriées se produisent. En moyenne, une entrée par alarmEntry peut être créée dans eventTable.

Groupe/objet	Description
Groupe : rmonEventGroup **Trap :** eventLastTimeSent	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** lecture seule **Syntaxe :** Timeticks **OID :** 1.3.6.1.2.1.16.9.1.1.5.1 **Définition :** valeur de sysUpTime 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 nulle.
Groupe : rmonEventGroup **Trap :** eventOwner	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.9.1.1.6.1 **Définition :** entité qui a configuré cette entrée et utilise donc les ressources qui lui sont affectées. Si cet objet contient une chaîne commençant par `monitor` et a des entrées associées dans le tableau Log, toutes les stations de gestion connectées doivent récupérer ces entrées de journal, car elles peuvent avoir une signification pour toutes les stations de gestion connectées à cet appareil. La valeur par défaut d'eventOwner est une chaîne `Monitor`.
Groupe : rmonEventGroup **Trap :** eventStatus	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.9.1.1.7.1 **Définition :** état de cette entrée d'événement. Si cet objet n'est pas égal à valid(1), toutes les entrées de journal associées doivent être supprimées par l'agent.
Groupe : rmonEventGroup **Trap :** eventType	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.9.1.1.3.1 **Définition :** type de notification générée par la sonde à propos de cet événement. Dans le cas de 'log', une entrée est ajoutée dans le tableau Log pour chaque événement. Dans le cas de snmp-trap, un trap SNMP est envoyé à une ou plusieurs stations de gestion. La valeur par défaut d'eventType est `logandtrap(4)`.
Groupe : rmonHistoryControlGroup **Trap :** historyControlBucketsGranted	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.1.1.4.1 **Définition :** nombre d'intervalles d'échantillonnage discrets pendant lesquels les données doivent être sauvegardées dans la partie du tableau spécifique au support associée à cet objet historyControlEntry. Lors de la création ou de la modification de l'objet historyControlBucketsRequested associé, la sonde doit définir cet objet aussi près de la valeur demandée que possible pour la mise en œuvre spécifique de la sonde et les ressources disponibles. La sonde ne doit pas diminuer cette valeur sauf à la suite d'une modification de l'objet historyControlBucketsRequested associé. Il y aura des moments où le nombre réel de compartiments associés à cette entrée sera inférieur à la valeur de cet objet. Dans ce cas, un nouveau compartiment sera ajouté au tableau spécifique au support à la fin de chaque intervalle d'échantillonnage. Lorsque le nombre de compartiments atteint la valeur de cet objet et qu'un nouveau compartiment doit être ajouté au tableau spécifique au support,

Groupe/objet	Description
	le compartiment le plus ancien associé à cet objet historyControlEntry doit être supprimé par l'agent afin que le nouveau compartiment puisse être ajouté. Lorsque la valeur de cet objet passe à une valeur inférieure à la valeur actuelle, les entrées sont supprimées du tableau spécifique au support associé à cet objet historyControlEntry. Un nombre suffisant des plus anciennes de ces entrées doit être supprimé par l'agent pour que leur nombre reste inférieur ou égal à la nouvelle valeur de cet objet. Lorsque la valeur de cet objet passe à une valeur supérieure à la valeur actuelle, le nombre d'entrées spécifiques au support associées peut être autorisé à augmenter.
Groupe : rmonHistoryControlGroup **Trap :** historyControlBucketsRequested	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.1.1.3.1 **Définition :** nombre demandé d'intervalles de temps discrets pendant lesquels les données doivent être sauvegardées dans la partie du tableau spécifique au support associée à cet objet historyControlEntry. Lors de la création ou de la modification de cet objet, la sonde doit définir historyControlBucketsGranted aussi près de cet objet que possible pour la mise en œuvre spécifique de la sonde et les ressources disponibles. **Définition :** La valeur de historyControBucketRequested est limitée à 4 000.
Groupe : rmonHistoryControlGroup **Trap :** historyControlDataSource	**Accès :** Lecture et création **Syntaxe :** OID **OID :** 1.3.6.1.2.1.16.2.1.1.2.1 **Définition :** cet objet identifie la source des données pour lesquelles les données d'historique ont été collectées et placées dans un tableau spécifique au support au nom de cet objet historyControlEntry. Cette source peut être n'importe quelle interface sur cet appareil. Afin d'identifier une interface spécifique, cet objet doit identifier l'instance de l'objet ifIndex définie dans RFC 2233 [17] pour l'interface souhaitée. Par exemple, si une entrée doit recevoir des données de l'interface n°1, cet objet est défini sur ifIndex.1. Les statistiques de ce groupe reflètent tous les paquets sur le segment de réseau local attaché à l'interface identifiée. Un agent peut ou non être en mesure de dire si des modifications fondamentales du support de l'interface se sont produites qui nécessitent une invalidation de cette entrée. Par exemple, une carte Ethernet enfichable à chaud peut être retirée et remplacée par une carte Token Ring. Dans ce cas, si l'agent a connaissance de cette modification, il est recommandé qu'il invalide cette entrée. Cet objet ne peut pas être modifié si l'objet historyControlStatus associé est égal à valid(1).
Groupe : rmonHistoryControlGroup **Trap :** historyControlIndex	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.1.1.1.1 **Définition :** index qui identifie de manière unique une entrée dans le tableau historyControl. Chacune de ces entrées définit un ensemble d'échantillons à un intervalle spécifique pour une interface sur l'appareil. Quatre entrées par port Ethernet en moyenne peuvent être créées dans historyControlTable.
Groupe : rmonHistoryControlGroup **Trap :** historyControlInterval	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.1.1.5.1

Groupe/objet	Description
	Définition : intervalle en secondes pendant lequel les données sont échantillonnées pour chaque compartiment dans la partie du tableau spécifique au support associée à cet objet historyControlEntry. Cet intervalle peut être défini sur n'importe quel nombre de secondes entre 1 et 3600 (1 heure). Étant donné que les compteurs d'un compartiment peuvent déborder à leur valeur maximale sans aucune indication, un gestionnaire prudent prendra en compte la possibilité de débordement de l'un des compteurs associés. Il est important de prendre en compte le temps minimum pendant lequel un compteur peut déborder sur un type de support particulier et de définir l'objet historyControlInterval sur une valeur inférieure à cet intervalle. C'est généralement ce qui est le plus important pour le compteur `octets` dans n'importe quel tableau spécifique au support. Par exemple, sur un réseau Ethernet, le compteur etherHistoryOctets peut déborder en une heure environ à utilisation maximale d'Ethernet. Cet objet ne peut pas être modifié si l'objet historyControlStatus associé est égal à valid(1).
Groupe : rmonHistoryControlGroup **Trap :** historyControlOwner	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.2.1.1.6.1 **Définition :** entité qui a configuré cette entrée et utilise donc les ressources qui lui sont affectées. La valeur par défaut d'historyControlOwner est une chaîne `Monitor`.
Groupe : rmonHistoryControlGroup **Trap :** historyControlStatus	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.2.1.1.7.1 **Définition :** état de cet objet historyControlEntry. Chaque instance du tableau spécifique au support associée à cet objet historyControlEntry est supprimée par l'agent si historyControlEntry n'est pas égale à valid(1).
Groupe : rmonEventGroup **Trap :** logDescription	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** 1.3.6.1.2.1.16.9.2.1.4.1 **Définition :** une description dépendante de la mise en œuvre de l'événement ayant activé cette entrée de journal.
Groupe : rmonEventGroup **Trap :** logEventIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.9.2.1.1.1 **Définition :** entrée d'événement ayant généré cette entrée de journal. Le journal identifié par une valeur particulière de cet index est associé à la même eventEntry que celui identifié par la même valeur d'eventIndex.
Groupe : rmonEventGroup **Trap :** logIndex	**Capacité de l'agent :** RC-RMON-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.16.9.2.1.2.1 **Définition :** index identifiant de manière unique une entrée dans le tableau Log parmi celles générées par les mêmes eventEntries. Ces index sont affectés en commençant par 1 et sont incrémentés de un à chaque nouvelle entrée de journal. L'association entre les valeurs de logIndex et logEntries est fixe pendant la durée de vie de chaque logEntry. L'agent peut choisir de supprimer les instances les plus anciennes de logEntry selon les besoins en

Groupe/objet	Description
	raison d'un manque de mémoire. Le moment où cette suppression peut se produire est une question spécifique à la mise en œuvre. **Remarque** Pour chaque eventEntry, une centaine d'entrées dans logTable peuvent être créées. La valeur de cet objet augmente pour chaque nouveau journal généré pour l'événement correspondant. Lorsque la valeur de cet objet dépasse 100, les entrées les plus anciennes sont supprimées.
Groupe : rmonEventGroup **Trap :** logTime	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** 1.3.6.1.2.1.16.9.2.1.3.1 **Définition :** valeur de sysUpTime lors de la création de cette entrée de journal.

RS-232-MIB

Groupe/objet	Description
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortAutobaud	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.3.1.3.101 **Définition :** contrôle pour la capacité du port à détecter automatiquement la vitesse d'entrée. Lorsque rs232PortAutoBaud est `enabled`, un port peut transmettre automatiquement à des valeurs différentes des valeurs définies pour la vitesse, la parité et la taille des caractères. Par conséquent, un système de gestion de réseau peut observer temporairement des valeurs différentes de ce qui a été défini précédemment.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortBits	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.5.1.4 **Définition :** nombre de bits du port dans un caractère.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortFramingErrs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.10.33.2.1.5.1.2 **Définition :** nombre total de caractères comportant une erreur de verrouillage de trame entrés à partir du port depuis la réinitialisation du système et pendant que l'état du port était `up` ou `test`.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.5.1.1 **Définition :** valeur unique pour chaque port. Sa valeur est la même que rs232PortIndex pour le port.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortOverrunErrs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.10.33.2.1.5.1.3

Groupe/objet	Description
	Définition : nombre total de caractères comportant une erreur de dépassement, entrés à partir du port depuis la réinitialisation du système et pendant que l'état du port était `up` ou `test`.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortParity	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.1.0 **Définition :** détection par le port d'un bit de parité de caractère.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortParityErrs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.10.33.2.1.6.1.4 **Définition :** nombre total de caractères comportant une erreur de parité, entrés à partir du port depuis la réinitialisation du système et pendant que l'état du port était `up` ou `test`.
Groupe : rs232AsyncGroup **Trap :** rs232AsyncPortStopBits	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.6.1.2 **Définition :** nombre de bits d'arrêt du port.
Groupe : rs232Group **Trap :** rs232InSigChanges	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.10.33.2.1.6.1.1 **Définition :** nombre de fois où le signal est passé de `on` à `off` ou de `off` à `on`.
Groupe : rs232Group **Trap :** rs232InSigName	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.6.1.3 **Définition :** identification d'un signal matériel comme suit : • rts : demande pour émettre • cts : prêt à émettre • dsr : Data Set Ready (prêt à fonctionner) • dtr : Data Terminal Ready (terminal de données prêt) • ri : indicateur d'appel • dcd : détecteur de signal de ligne reçu • sq : détecteur de qualité du signal • srs : sélecteur de débit de signalisation de données • srts : semande d'émission secondaire • scts : autorisation d'émission secondaire • sdcd : détecteur de signal de ligne reçu secondaire
Groupe : rs232Group **Trap :** rs232InSigPortIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.1.101 **Définition :** valeur de rs232PortIndex pour le port auquel appartient cette entrée.
Groupe : rs232Group **Trap :** rs232InSigState	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.7.101

Groupe/objet	Description
	Définition : état actuel du signal.
Groupe : rs232Group **Trap :** rs232Number	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.3.101 **Définition :** nombre de ports (indépendamment de leur état actuel) dans le tableau général des ports de type RS-232.
Groupe : rs232Group **Trap :** rs232OutSigChanges	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.5.101 **Définition :** nombre de fois où le signal est passé de `on` à `off` ou de `off` à `on`.
Groupe : rs232Group **Trap :** rs232OutSigName	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.7.101 **Définition :** identification d'un signal matériel comme suit : • rts : demande pour émettre • cts : prêt à émettre • dsr : Data Set Ready (prêt à fonctionner) • dtr : Data Terminal Ready (terminal de données prêt) • ri : indicateur d'appel • dcd : détecteur de signal de ligne reçu • sq : détecteur de qualité du signal • srs : sélecteur de débit de signalisation de données • srts : semande d'émission secondaire • scts : autorisation d'émission secondaire • sdcd : détecteur de signal de ligne reçu secondaire
Groupe : rs232Group **Trap :** rs232OutSigPortIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.4.101 **Définition :** valeur de rs232PortIndex pour le port auquel appartient cette entrée.
Groupe : rs232Group **Trap :** rs232OutSigState	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.5.101 **Définition :** état actuel du signal.
Groupe : rs232Group **Trap :** rs232PortIndex	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.10.33.2.1.2.101 **Définition :** valeur d'ifIndex pour ce port. Par convention et si possible, les numéros de port matériel correspondent directement aux connecteurs externes. La valeur de chaque port doit rester constante au moins d'une réinitialisation de l'agent de gestion de réseau à la suivante.
Groupe : rs232Group **Trap :** rs232PortInFlowType	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.10.2.1.2.0

Groupe/objet	Description
	Définition : type de contrôle de flux d'entrée du port. `none` indique l'absence de contrôle de flux à ce niveau. `ctsRts` et `dsrDtr` indiquent l'utilisation des signaux matériels spécifiés.
Groupe : rs232Group **Trap :** rs232PortInSigNumber	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.10.2.1.1.0 **Définition :** nombre de signaux d'entrée pour le port dans le tableau des signaux d'entrée (rs232PortInSigTable). Le tableau contient des entrées uniquement pour les signaux que le logiciel peut détecter et qu'il est utile d'observer.
Groupe : rs232Group **Trap :** rs232PortInSpeed	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.10.2.1.4.0 **Définition :** vitesse d'entrée du port en bits par seconde. Notez que les valeurs non standard, telles que 9612, ne sont probablement pas autorisées sur la plupart des mises en œuvre.
Groupe : rs232Group **Trap :** rs232PortOutFlowType	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.10.2.1.3.0 **Définition :** type de contrôle de flux de sortie du port. `none` indique l'absence de contrôle de flux à ce niveau. `ctsRts` et `dsrDtr` indiquent l'utilisation des signaux matériels spécifiés.
Groupe : rs232Group **Trap :** rs232PortOutSigNumber	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.11.6.0 **Définition :** nombre de signaux de sortie pour le port dans le tableau des signaux de sortie (rs232PortOutSigTable). Le tableau contient des entrées uniquement pour les signaux que le logiciel peut affirmer et qu'il est utile d'observer.
Groupe : rs232Group **Trap :** rs232PortOutSpeed	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.11.4.0 **Définition :** vitesse de sortie du port en bits par seconde. Notez que les valeurs non standard, telles que 9612, ne sont probablement pas autorisées sur la plupart des mises en œuvre.
Groupe : rs232Group **Trap :** rs232PortType	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.11.5.0 **Définition :** type de matériel du port.

RSTP-MIB

Groupe/objet	Description
Groupe : rstpPortGroup **Trap :** dot1dStpPortAdminEdgePort	**Accès :** lecture et écriture **TruthValue** **OID :** .1.3.6.1.2.1.17.2.19.1.2

Groupe/objet	Description
	Définition : valeur administrative du paramètre Edge Port. La valeur true(1) indique que ce port doit être considéré comme un port de périphérie, et la valeur false(2) indique que ce port doit être considéré comme un port non périphérique. La définition de cet objet entraîne également le passage de l'instance correspondante de dot1dStpPortOperEdgePort à la même valeur. Notez que même lorsque la valeur de cet objet est true, la valeur de l'instance correspondante de dot1dStpPortOperEdgePort peut être false si une BPDU a été reçue. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : rstpPortGroup **Trap :** dot1dStpPortAdminPathCost	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.19.1.6 **Définition :** valeur affectée administrativement pour la contribution de ce port au coût des chemins vers la racine du Spanning Tree. L'écriture de la valeur `0` affecte au port la valeur de coût de chemin par défaut calculée automatiquement. Si le coût de chemin par défaut est utilisé, cet objet renvoie `0` lors de la lecture. Ceci complète l'objet dot1dStpPortPathCost ou dot1dStpPortPathCost32, qui renvoie la valeur opérationnelle du coût du chemin. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : rstpPortGroup **Trap :** dot1dStpPortAdminPointToPoint	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.19.1.4 **Définition :** statut administratif point à point du segment LAN attaché à ce port, utilisant les valeurs d'énumération de la clause IEEE 802.1w. La valeur forceTrue(0) indique que ce port doit toujours être traité comme s'il était connecté à une liaison point à point. La valeur forceFalse(1) indique que ce port doit être traité comme ayant une connexion multimédia partagée. La valeur auto(2) indique que ce port est considéré comme ayant une liaison point à point s'il s'agit d'un agrégateur et que tous ses membres peuvent être agrégés, ou si l'entité MAC est configurée pour un fonctionnement en duplex intégral, soit par auto-négociation ou soit par des moyens de gestion. La manipulation de cet objet modifie l'adminPortToPortMAC sous-jacent. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.
Groupe : rstpPortGroup **Trap :** dot1dStpPortOperEdgePort	**Accès :** lecture seule **TruthValue** **OID :** .1.3.6.1.2.1.17.2.19.1.3 **Définition :** valeur opérationnelle du paramètre Edge Port. L'objet est initialisé à la valeur de l'instance correspondante de dot1dStpPortAdminEdgePort. Lorsque l'instance correspondante de dot1dStpPortAdminEdgePort est définie, cet objet est également modifié. Cet objet est également défini sur False à la réception d'une BPDU.
Groupe : rstpPortGroup **Trap :** dot1dStpPortOperPointToPoint	**Accès :** lecture seule **TruthValue** **OID :** .1.3.6.1.2.1.17.2.19.1.5 **Définition :** état opérationnel point à point du segment LAN attaché à ce port. Il indique si un port est considéré comme ayant une connexion point à point. Si adminPointToPointMAC est réglé sur auto(2), la valeur de operPointToPointMAC est déterminée conformément aux procédures spécifiques définies pour l'entité MAC concernée, comme défini dans IEEE 802.1w, clause 6.5. La valeur est déterminée dynamiquement. C'est-à-

Groupe/objet	Description
	dire qu'elle est réévaluée chaque fois que la valeur d'adminPointToPointMAC change, et chaque fois que les procédures spécifiques définies pour l'entité MAC évaluent un changement dans son état point à point.
Groupe : rstpBridgeGroup **Trap :** dot1dStpTxHoldCount	**Capacité de l'agent :** RC-RSTP-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.17.0 **Définition :** valeur utilisée par la machine d'état Port Transmit pour limiter la vitesse de transmission maximum. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion. **Remarque** La plage spécifiée par RFC est 1..10. La mise en œuvre utilise 0...100. La valeur 0 est utilisée pour Unlimited et la plage ROS est en fait 3..100.
Groupe : rstpBridgeGroup **Trap :** dot1dStpVersion	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.17.2.16.0 **Définition :** version du protocole Spanning Tree que le pont exécute actuellement. La valeur `stpCompatible(0)` indique le protocole Spanning Tree spécifié dans IEEE 802.1D-1998 et `rstp(2)` indique le Rapid Spanning Tree Protocol spécifié dans IEEE 802.1w et la clause 17 de 802.1D-2004. Les valeurs proviennent directement de la norme IEEE. De nouvelles valeurs peuvent être définies au fur et à mesure que de futures versions du protocole deviennent disponibles. La valeur de cet objet DOIT être conservée lors des réinitialisations du système de gestion.

SNMP-FRAMEWORK-MIB

Groupe/objet	Description
Groupe : snmpEngineGroup **Trap :** snmpEngineBoots	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.11.31.0 **Définition :** nombre d'initialisations (ou de réinitialisations) du moteur SNMP depuis la dernière configuration de snmpEngineID.
Groupe : snmpEngineGroup **Trap :** snmpEngineID	**Accès :** lecture seule **Syntaxe :** chaîne hexadécimale **OID :** 1.3.6.1.2.1.1.4.0 **Définition :** identificateur administrativement unique d'un moteur SNMP. Ces informations DOIVENT être stockées dans un stockage non volatil afin qu'elles restent constantes lors des réinitialisations du moteur SNMP.
Groupe : snmpEngineGroup **Trap :** snmpEngineMaxMessageSize	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.1.1.0 **Définition :** longueur maximale en octets d'un message SNMP que ce moteur SNMP peut envoyer ou recevoir et traiter, déterminée comme le minimum des valeurs de taille de message maximales prises en charge parmi tous les transports à disposition du moteur et pris en charge par celui-ci.

Groupe/objet	Description
Groupe : snmpEngineGroup **Trap :** snmpEngineTime	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.1.6.0 **Définition :** nombre de secondes depuis la dernière modification de la valeur de l'objet snmpEngineBoots. Lorsque l'incrémentation de la valeur de cet objet le ferait dépasser son maximum, snmpEngineBoots est incrémenté comme si une réinitialisation s'était produite, et la valeur de cet objet revient par conséquent à zéro.

SNMP-USER-BASED-SM-MIB

Groupe/objet	Description
Groupe : usmMIBBasicGroup **Trap :** usmStatsDecryptionErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.9 **Définition :** nombre total de paquets reçus par le moteur SNMP qui ont été abandonnés parce qu'ils n'ont pas pu être déchiffrés.
Groupe : usmMIBBasicGroup **Trap :** usmStatsNotInTimeWindows	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.8.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Définition :** nombre total de paquets reçus par le moteur SNMP qui ont été abandonnés parce qu'ils sont apparus en dehors de la fenêtre du moteur SNMP faisant autorité.
Groupe : usmMIBBasicGroup **Trap :** usmStatsUnknownEngineIDs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.11 **Définition :** nombre total de paquets reçus par le moteur SNMP qui ont été abandonnés parce qu'ils faisaient référence à un snmpEngineID qui n'était pas connu du moteur SNMP.
Groupe : usmMIBBasicGroup **Trap :** usmStatsUnknownUserNames	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.3 **Définition :** nombre total de paquets reçus par le moteur SNMP qui ont été abandonnés parce qu'ils faisaient référence à un utilisateur qui n'était pas connu du moteur SNMP.
Groupe : usmMIBBasicGroup **Trap :** usmStatsUnsupportedSecLevels	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.1.0 **Définition :** nombre total de paquets reçus par le moteur SNMP qui ont été abandonnés parce qu'ils ont demandé un niveau de sécurité (securityLevel) inconnu du moteur SNMP ou autrement indisponible.
Groupe : usmMIBBasicGroup **Trap :** usmStatsWrongDigests	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.13

Groupe/objet	Description
	Définition : nombre total de paquets reçus par le moteur SNMP qui ont été abandonnés parce qu'ils ne contenaient pas la valeur de digest (synthèse) attendue.
Groupe : usmMIBBasicGroup **Trap :** usmUserAuthKeyChange	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.15.1.2.2.1.12 **Définition :** objet qui, lorsqu'il est modifié, provoque la modification de la clé secrète d'authentification utilisée pour les messages envoyés au nom de cet utilisateur vers/depuis le moteur SNMP identifié par usmUserEngineID via une fonction à sens unique. Le protocole associé est usmUserAuthProtocol. La clé secrète associée est la clé secrète d'authentification de l'utilisateur (authKey). L'algorithme de hachage associé est l'algorithme utilisé par l'usmUserAuthProtocol de l'utilisateur. Lors de la création d'un nouvel utilisateur, la référence d'une opération de réglage à cet objet est une erreur `inconsistentName` à moins que cet objet n'ait été précédemment ou simultanément initialisé via une opération de réglage sur l'instance correspondante d'usmUserCloneFrom. Lorsque la valeur de l'usmUserAuthProtocol correspondant est usmNoAuthProtocol, le réglage est réussi, mais il est en fait un no-op. Lors de la lecture de cet objet, une chaîne de longueur nulle (vide) est renvoyée. La marche à suivre recommandée pour effectuer un changement de clé est la suivante : • 1) GET(usmUserSpinLock.0) et save (enregistrer) dans sValue. • 2) Générer la valeur keyChange sur la base de l'ancienne clé secrète (existante) et de la nouvelle clé secrète, que l'on apellera kcValue. Si vous effectuez le changement de clé au nom d'un autre utilisateur : • 3) SET(usmUserSpinLock.0=sValue, usmUserAuthKeyChange=kcValue usmUserPublic=randomValue) Si vous effectuez le changement de clé pour vous-même : • 4) SET(usmUserSpinLock.0=sValue, usmUserOwnAuthKeyChange=kcValue usmUserPublic=randomValue) Si vous obtenez une réponse avec un l'état d'erreur noError, le réglage (SET) a réussi et la nouvelle clé est active. Si vous n'obtenez pas de réponse, vous pouvez émettre un GET(usmUserPublic) et vérifier si la valeur est égale à la randomValue que vous avez envoyée dans le réglage (SET). Si tel est le cas, le changement de clé a réussi et la nouvelle clé est active (la réponse a probablement été perdue). Si ce n'est pas le cas, la requête SET n'a probablement jamais atteint la cible et vous pouvez donc recommencer avec la procédure ci-dessus.
Groupe : usmMIBBasicGroup **Trap :** usmUserAuthProtocol	**Accès :** Lecture et création **Syntaxe :** OID **OID :** 1.3.6.1.6.3.16.1.4.1.4.8.71.112.114.105.118.97.116.101.0.2.1 **Définition :** indication si des messages envoyés au nom de cet utilisateur vers/depuis le moteur SNMP identifié par usmUserEngineID peuvent être authentifiés et, le cas échéant, le type de protocole d'authentification utilisé. Une instance de cet objet est créée en même temps que la création de toute autre instance d'objet pour le même utilisateur (c'est-à-dire dans le cadre du traitement de l'opération de réglage qui crée la première instance d'objet dans la même ligne conceptuelle). Si une opération de réglage initiale (c'est-à-dire au moment de la création de la ligne) essaie de définir une valeur pour un protocole inconnu ou non pris en charge, une erreur `wrongValue` sera renvoyée. La valeur sera écrasée/définie lorsqu'une opération de réglage est effectuée sur l'instance correspondante d'usmUserCloneFrom. Une fois instanciée, la valeur d'une telle instance

Groupe/objet	Description
	de cet objet ne peut être portée à la valeur d'usmNoAuthProtocol que via une opération de réglage. Si une opération de réglage tente de modifier la valeur d'une instance existante de cet objet à une valeur autre qu'usmNoAuthProtocol, une erreur `inconsistentValue` sera renvoyée. Si une opération de réglage tente de définir la valeur sur usmNoAuthProtocol alors que la valeur d'usmUserPrivProtocol dans la même ligne n'est pas égale à usmNoPrivProtocol, une erreur `inconsistentValue` sera renvoyée. Cela signifie qu'une application de générateur de commandes SNMP doit d'abord s'assurer qu'usmUserPrivProtocol est défini sur la valeur usmNoPrivProtocol avant de pouvoir définir la valeur d'usmUserAuthProtocol sur usmNoAuthProtocol.
Groupe : usmMIBBasicGroup **Trap :** usmUserCloneFrom	**Accès :** Lecture et création **Syntaxe :** OID **OID :** 1.3.6.1.6.3.16.1.4.1.7.8.71.112.114.105.118.97.116.101.0.2.1 **Définition :** pointeur vers une autre ligne conceptuelle dans cette usmUserTable. L'utilisateur de cette autre ligne conceptuelle est appelé l'utilisateur cloné. Lorsqu'un nouvel utilisateur est créé (c'est-à-dire qu'une nouvelle ligne conceptuelle est instanciée dans ce tableau), les paramètres de confidentialité et d'authentification du nouvel utilisateur doivent être clonés à partir de son utilisateur cloné. Ces paramètres sont : • - protocole d'authentification (usmUserAuthProtocol) • - protocole de confidentialité (usmUserPrivProtocol) Ils sont copiés quelle que soit la valeur actuelle. Le clonage entraîne également la définition des valeurs initiales de la clé d'authentification secrète (authKey) et de la clé de chiffrement secrète (privKey) du nouvel utilisateur sur les mêmes valeurs que les secrets correspondants de l'utilisateur cloné pour permettre au processus KeyChange de se produire comme requis lors de la création de l'utilisateur. La première fois qu'une instance de cet objet est définie par une opération de gestion (au moment de son instanciation ou après), le processus de clonage est appelé. Les écritures suivantes réussissent mais n'appellent aucune action à entreprendre par le récepteur. Le processus de clonage échoue en émettant une erreur `inconsistentName` si la ligne conceptuelle représentant l'utilisateur cloné n'existe pas ou n'est pas dans un état actif lorsque le processus de clonage est appelé. Lors de la lecture de cet objet, l'OID ZeroDotZero est renvoyé.
Groupe : usmMIBBasicGroup **Trap :** usmUserOwnAuthKeyChange	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.16.1.4.1.5.8.71.112.114.105.118.97.116.101.0.2.1 **Définition :** se comporte exactement comme usmUserAuthKeyChange, avec une différence notable : pour que l'opération de réglage réussisse, l'usmUserName du demandeur de l'opération doit correspondre à l'usmUserName qui indexe la ligne ciblée par cette opération. De plus, le modèle de sécurité USM doit être utilisé pour cette opération. L'idée ici est que l'accès à cette colonne peut être public, puisqu'il permet uniquement à un utilisateur de changer sa propre clé secrète d'authentification (authKey). Notez que cela ne peut être fait que lorsque la ligne est active. Lorsqu'un réglage est reçu et que l'usmUserName du demandeur n'est pas le même que l'umsUserName qui indexe la ligne ciblée par cette opération, une erreur `noAccess` sera renvoyée. Lorsqu'un ensemble est reçu et que le modèle de sécurité utilisé n'est pas USM, une erreur `noAccess` sera renvoyée.
Groupe : usmMIBBasicGroup **Trap :** usmUserOwnPrivKeyChange	**Accès :** Lecture et création **Syntaxe :** Chaîne

Groupe/objet	Description
	OID : 1.3.6.1.6.3.16.1.4.1.9.8.71.112.114.105.118.97.116.101.0.2.1 **Définition :** se comporte exactement comme usmUserPrivKeyChange, avec une différence notable : pour que l'opération de réglage réussisse, l'usmUserName du demandeur de l'opération doit correspondre à l'usmUserName qui indexe la ligne ciblée par cette opération. De plus, le modèle de sécurité USM doit être utilisé pour cette opération. L'idée ici est que l'accès à cette colonne peut être public, puisqu'il permet uniquement à un utilisateur de changer sa propre clé secrète de confidentialité (privKey). Notez que cela ne peut être fait que lorsque la ligne est active. Lorsqu'un réglage est reçu et que l'usmUserName du demandeur n'est pas le même que l'umsUserName qui indexe la ligne ciblée par cette opération, une erreur `noAccess` sera renvoyée. Lorsqu'un ensemble est reçu et que le modèle de sécurité utilisé n'est pas USM, une erreur `noAccess` sera renvoyée.
Groupe : usmMIBBasicGroup **Trap :** usmUserPrivKeyChange	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.16.1.4.1.8.8.71.112.114.105.118.97.116.101.0.2.1 **Définition :** objet qui, lorsqu'il est modifié, provoque la modification de la clé secrète de chiffrage utilisée pour les messages envoyés au nom de cet utilisateur vers/depuis le moteur SNMP identifié par usmUserEngineID via une fonction à sens unique. Le protocole associé est usmUserPrivProtocol. La clé secrète associée est la clé secrète de confidentialité de l'utilisateur (privKey). L'algorithme de hachage associé est l'algorithme utilisé par l'usmUserAuthProtocol de l'utilisateur. Lors de la création d'un nouvel utilisateur, la référence d'une opération de réglage à cet objet est une erreur `inconsistentName` à moins que cet objet n'ait été précédemment ou simultanément initialisé via une opération de réglage sur l'instance correspondante d'usmUserCloneFrom. Lorsque la valeur de l'usmUserPrivProtocol correspondant est usmNoPrivProtocol, le réglage est réussi, mais il est en fait un no-op. Lors de la lecture de cet objet, une chaîne de longueur nulle (vide) est renvoyée. Voir la clause de description d'usmUserAuthKeyChange pour obtenir la procédure recommandée pour effectuer un changement de clé.
Groupe : usmMIBBasicGroup **Trap :** usmUserPrivProtocol	**Accès :** Lecture et création **Syntaxe :** OID **OID :** 1.3.6.1.6.3.16.1.4.1.6.8.71.112.114.105.118.97.116.101.0.2.1 **Définition :** indication si des messages envoyés au nom de cet utilisateur vers/depuis le moteur SNMP identifié par usmUserEngineID peuvent être protégés contre la divulgation et, le cas échéant, le type de protocole de confidentialité utilisé. Une instance de cet objet est créée en même temps que la création de toute autre instance d'objet pour le même utilisateur (c'est-à-dire dans le cadre du traitement de l'opération de réglage qui crée la première instance d'objet dans la même ligne conceptuelle). Si une opération de réglage initiale (c'est-à-dire au moment de la création de la ligne) essaie de définir une valeur pour un protocole inconnu ou non pris en charge, une erreur `wrongValue` sera renvoyée. La valeur sera écrasée/définie lorsqu'une opération de réglage est effectuée sur l'instance correspondante d'usmUserCloneFrom. Une fois instanciée, la valeur d'une telle instance de cet objet ne peut être portée à la valeur d'usmNoPrivProtocol que via une opération de réglage. Si une opération de réglage tente de modifier la valeur d'une instance existante de cet objet à une valeur autre qu'usmNoPrivProtocol, une erreur `inconsistentValue` sera renvoyée. Notez que si un protocole de confidentialité est utilisé, vous devez également utiliser un protocole d'authentification. En d'autres termes, si usmUserPrivProtocol est défini sur autre chose qu'usmNoPrivProtocol, l'instance correspondante d'usmUserAuthProtocol ne peut pas avoir la valeur

Groupe/objet	Description
	usmNoAuthProtocol. Si c'est le cas, une erreur `inconsistentValue` sera renvoyée.
Groupe : usmMIBBasicGroup **Trap :** usmUserPublic	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.16.1.1.1.1 **Définition :** valeur lisible publique qui peut être écrite dans le cadre de la procédure de modification de la clé secrète d'authentification et/ou de confidentialité d'un utilisateur, et lue ultérieurement pour déterminer si la modification du secret a été effectuée.
Groupe : usmMIBBasicGroup **Trap :** usmUserSecurityName	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.16.1.2.1.3.2.7.112.114.105.118.97.116.101 **Définition :** chaîne lisible par l'homme représentant l'utilisateur dans un format indépendant du modèle de sécurité. La transformation par défaut de l'ID de sécurité dépendant du modèle de sécurité basé sur l'utilisateur en securityName et vice versa est la fonction d'identité afin que securityName soit identique à userName.
Groupe : usmMIBBasicGroup **Trap :** usmUserSpinLock	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.16.1.2.1.5.2.7.112.114.105.118.97.116.101 **Définition :** verrou consultatif utilisé pour permettre à plusieurs applications de générateur de commandes coopérantes de coordonner leur utilisation des installations pour modifier les secrets dans usmUserTable.
Groupe : usmMIBBasicGroup **Trap :** usmUserStatus	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.16.1.2.1.4.2.7.112.114.105.118.97.116.101 **Définition :** état de cette ligne conceptuelle. Jusqu'à ce que les instances de toutes les colonnes correspondantes soient correctement configurées, la valeur de l'instance correspondante de la colonne usmUserStatus est `notReady`. En particulier, une ligne venant d'être créée pour un utilisateur qui utilise l'authentification ne peut pas être activée tant que les usmUserCloneFrom et usmUserAuthKeyChange correspondants n'ont pas été définis. De plus, une ligne venant d'être créée pour un utilisateur qui utilise également la confidentialité ne peut pas être activée tant que usmUserPrivKeyChange n'a pas été défini. RowStatus TC [RFC2579<rfc2579.html>] exige que cette clause DESCRIPTION indique dans quelles circonstances d'autres objets de cette ligne peuvent être modifiés : la valeur de cet objet n'a aucun effet sur la possibilité de modifier d'autres objets de cette ligne conceptuelle, à l'exception d'usmUserOwnAuthKeyChange et usmUserOwnPrivKeyChange. Pour ces 2 objets, la valeur d'usmUserStatus DOIT être active.
Groupe : usmMIBBasicGroup **Trap :** usmUserStorageType	**Accès :** Lecture et création **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.16.1.5.1.0 **Définition :** type de stockage pour cette ligne conceptuelle. Les lignes conceptuelles ayant la valeur `permanent` doivent permettre l'accès en écriture au minimum à : • - usmUserAuthKeyChange, usmUserOwnAuthKeyChange et usmUserPublic pour un utilisateur qui utilise l'authentification, et

Groupe/objet	Description
	• - usmUserPrivKeyChange, usmUserOwnPrivKeyChange et usmUserPublic pour un utilisateur qui utilise la confidentialité. Notez que tout utilisateur qui utilise l'authentification ou la confidentialité doit autoriser la mise à jour de son ou ses secrets et ne peut donc pas être `readOnly`. Si une opération de réglage initiale tente de définir la valeur sur `readOnly` pour un utilisateur qui utilise l'authentification ou la confidentialité, une erreur `inconsistentValue` sera renvoyée. Notez que les règles définies dans la convention textuelle StorageType s'appliquent si la valeur a été précédemment définie (implicitement ou explicitement) sur une valeur quelconque. Décider si un réglage (SET) pour une ligne readOnly ou permanente est accepté est une question de mise en œuvre. Cela peut s'avérer judicieux dans certains contextes, dans d'autres non. Si un réglage (SET) pour une ligne readOnly ou permanente n'est pas du tout accepté, une erreur `wrongValue` sera renvoyée.

SNMPv2-MIB

Groupe/objet	Description
Groupe : snmpBasicNotificationsGroup **Trap :** AuthenticationFailure	**Accès :** 0 **Syntaxe :** — **OID :** 1.3.6.1.6.3.1.1.5.5 **Définition :** un trap authenticationFailure signifie que l'entité SNMPv2, qui joue le rôle d'agent, a reçu un message de protocole qui n'est pas correctement authentifié. Alors que toutes les mises en œuvre de SNMPv2 doivent être capables de générer ce trap, l'objet snmpEnableAuthenTraps indique si ce trap sera généré.
Groupe : snmpGroup **Trap :** snmpInASNParseErrs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.5.0 **Définition :** nombre total d'erreurs ASN.1 ou BER détectées par l'entité SNMP lors du décodage des messages SNMP reçus.
Groupe : snmpCommunityGroup **Trap :** snmpInBadCommunityNames	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.2.0 **Définition :** nombre total de messages SNMP envoyés à l'entité SNMP, qui ont utilisé un nom de communauté SNMP inconnu de ladite entité.
Groupe : snmpCommunityGroup **Trap :** snmpInBadCommunityUses	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.9.1.3.0 **Définition :** nombre total de messages SNMP envoyés à l'entité SNMP qui représentait une opération SNMP non autorisée par la communauté SNMP nommée dans le message.
Groupe : snmpGroup **Trap :** snmpInBadVersions	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.9.1.2.0 **Définition :** nombre total de messages SNMP envoyés à l'entité SNMP qui concernaient une version SNMP non prise en charge.
Groupe : snmpGroup	**Accès :** lecture seule

Groupe/objet	Description
Trap : snmpInPkts	**Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.8.0 **Définition :** nombre total de messages envoyés à l'entité SNMP depuis le service de transport.
Groupe : snmpGroup **Trap :** snmpProxyDrops	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.9.1.4.0 **Définition :** nombre total de PDU GetRequest, PDU GetNextRequest, PDU GetBulkRequest, PDU SetRequest et PDU InformRequest envoyées à l'entité SNMP qui ont été silencieusement abandonnées parce que la transmission du message (éventuellement traduit) à une cible proxy a échoué d'une manière (autre qu'une expiration) telle qu'aucune PDU de réponse ne puisse être renvoyée.
Groupe : snmpSetGroup **Trap :** snmpSetSerialNo	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.2.1.1.7.0 **Définition :** verrou consultatif utilisé pour permettre à plusieurs entités SNMPv2 coopérantes qui jouent toutes le rôle de gestionnaire de coordonner leur utilisation de l'opération de réglage SNMPv2. Cet objet est utilisé pour la coordination grossière. Pour obtenir une coordination fine, un ou plusieurs objets similaires peuvent être définis au sein de chaque groupe MIB, selon le cas.
Groupe : snmpGroup **Trap :** snmpSilentDrops	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.2.1.1.3.0 **Définition :** nombre total de PDU GetRequest, PDU GetNextRequest, PDU GetBulkRequest, PDU SetRequest et PDU InformRequest envoyées à l'entité SNMP qui ont été silencieusement abandonnées car la taille d'une réponse contenant une autre PDU de réponse avec un champ de liaison de variables vide était supérieure à une contrainte locale ou à la taille de message maximale associée à l'expéditeur de la demande.
Groupe : systemGroup **Trap :** sysContact	**Capacité de l'agent :** RC-SNMPv2-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.6.5.0 **Définition :** identification textuelle de la personne à contacter pour ce nœud géré, accompagnée d'informations sur la façon de contacter cette personne. Si aucune information de contact n'est connue, la valeur est une chaîne de longueur nulle. Une chaîne de 49 caractères maximum est prise en charge pour cet objet.
Groupe : systemGroup **Trap :** sysDescr	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.6.7.0 **Définition :** description textuelle de l'entité. Cette valeur doit inclure le nom complet et l'identification de la version du type de matériel du système, du système d'exploitation logiciel et du logiciel réseau.
Groupe : systemGroup **Trap :** sysLocation	**Capacité de l'agent :** RC-SNMPv2-MIB-AC **Accès :** lecture et écriture

Groupe/objet	Description
	Syntaxe : Chaîne **OID :** .1.3.6.1.2.1.6.13.1.2.0.0.0.0.22.0.0.0.0.0 **Définition :** emplacement physique de ce nœud (par exemple `telephone closet, 3rd floor`). Si l'emplacement est inconnu, la valeur est une chaîne de longueur nulle. Une chaîne de 49 caractères maximum est prise en charge pour cet objet.
Groupe : systemGroup **Trap :** sysName	**Capacité de l'agent :** RC-SNMPv2-MIB-AC **Accès :** lecture et écriture **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.6.13.1.3.0.0.0.0.22.0.0.0.0.0 **Définition :** nom affecté administrativement à ce nœud géré. Par convention, il s'agit du nom de domaine complet du nœud. Si le nom est inconnu, la valeur est une chaîne de longueur nulle. Une chaîne de 24 caractères maximum est prise en charge pour cet objet.
Groupe : systemGroup **Trap :** sysObjectID	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.6.13.1.4.0.0.0.0.22.0.0.0.0.0 **Définition :** identification officielle du fournisseur du sous-système de gestion de réseau contenu dans l'entité. Cette valeur est attribuée dans la sous-arborescence des entreprises SMI (1.3.6.1.4.1) et fournit un moyen simple et non ambigu de déterminer que `what kind of box` est géré. Par exemple, si la sous-arborescence 1.3.6.1.4.1.4242 a été affectée au fournisseur `Flintstones, Inc.`, il peut affecter l'identificateur 1.3.6.1.4.1.4242.1.1 à son `Fred Router`.
Groupe : systemGroup **Trap :** sysORDescr	**Accès :** lecture seule **Syntaxe :** Chaîne **OID :** .1.3.6.1.2.1.6.13.1.5.0.0.0.0.22.0.0.0.0.0 **Définition :** description textuelle des capacités identifiées par l'instance correspondante de sysORID.
Groupe : systemGroup **Trap :** sysORID	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.6.13.1.1.0.0.0.0.22.0.0.0.0.0 **Définition :** identification faisant autorité d'une déclaration de capacités par rapport à divers modules MIB pris en charge par l'entité SNMPv2 locale jouant le rôle d'agent.
Groupe : systemGroup **Trap :** sysORLastChange	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.6.9.0 **Définition :** valeur de sysUpTime au moment du dernier changement d'état ou de valeur de toute instance de sysORID.
Groupe : systemGroup **Trap :** sysORUpTime	**Accès :** lecture seule **Syntaxe :** TimeStamp **OID :** .1.3.6.1.2.1.6.8.0 **Définition :** valeur de sysUpTime au moment de la dernière instanciation de cette ligne conceptuelle.
Groupe : systemGroup **Trap :** sysServices	**Accès :** lecture seule **Syntaxe :** Integer

Groupe/objet	Description
	OID : .1.3.6.1.2.1.6.14.0 **Définition :** valeur indiquant l'ensemble des services que cette entité peut potentiellement offrir. La valeur est une somme. Cette somme prend initialement la valeur zéro, puis, pour chaque couche L, est comprise dans la plage allant de 1 à 7, pour laquelle ce nœud effectue des transactions, 2 élevé à (L - 1) est ajouté à la somme. Par exemple, un nœud qui n'exécute que des fonctions de routage aurait une valeur de 4 (2^(3-1)). En revanche, un nœud qui est un hôte offrant des services d'application aurait une valeur de 72 (2^(4-1) + 2^(7-1)). Notez que, dans le contexte de la suite de protocoles Internet, les valeurs doivent être calculées en conséquence : • Layer 1 (couche 1) : physique (p. ex. répéteurs) • Layer 2 (couche 2) : liaison de données/sous-réseau (p. ex. ponts) • Layer 3 (couche 3) : Internet (p. ex. prend en charge IP) • Layer 4 (couche 4) : de bout en bout (p. ex. prend en charge TCP) • Layer 7 (couche 7) : applications (p. ex. prend en charge SMTP) Pour les systèmes comprenant des protocoles OSI, les couches 5 et 6 peuvent également être comptées.
Groupe : systemGroup **Trap :** sysUpTime	**Accès :** lecture seule **Syntaxe :** Timeticks **OID :** .1.3.6.1.2.1.6.17.0 **Définition :** temps (en centièmes de seconde) depuis la dernière réinitialisation de la partie de gestion de réseau du système.

SNMP-VIEW-BASED-ACM-MIB

Groupe/objet	Description
Groupe : vacmBasicGroup **Trap :** vacmAccessContextMatch	**Capacité de l'agent :** RC-SNMP-VIEW-BASED-ACM-MIB-AC **Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.16.1.5.2.1.3.5.86.49.77.105.98.1.1 **Définition :** si la valeur de cet objet est exact(1), toutes les lignes où le contextName correspond exactement à vacmAccessContextPrefix sont sélectionnées. Si la valeur de cet objet est prefix(2), toutes les lignes où le contextName dont les octets de départ correspondent exactement à vacmAccessContextPrefix sont sélectionnées. Cela permet une forme simple d'attribution de caractères génériques.
Groupe : vacmBasicGroup **Trap :** vacmAccessNotifyViewName	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.16.1.5.2.1.6.5.86.49.77.105.98.1.1 **Définition :** la valeur d'une instance de cet objet identifie la vue MIB du contexte SNMP à laquelle cette ligne conceptuelle autorise l'accès pour les notifications. La vue MIB identifiée est celle pour laquelle vacmViewTreeFamilyViewName a la même valeur que l'instance de cet objet. Aucun accès n'est accordé si la valeur est une chaîne vide ou s'il n'y a pas de vue MIB active ayant cette valeur de vacmViewTreeFamilyViewName.
Groupe : vacmBasicGroup **Trap :** vacmAccessReadViewName	**Accès :** Lecture et création **Syntaxe :** Chaîne **OID :** 1.3.6.1.6.3.16.1.5.2.1.5.5.86.49.77.105.98.1.1

Groupe/objet	Description
	Définition : la valeur d'une instance de cet objet identifie la vue MIB du contexte SNMP à laquelle cette ligne conceptuelle autorise l'accès en lecture. La vue MIB identifiée est celle pour laquelle vacmViewTreeFamilyViewName a la même valeur que l'instance de cet objet. Aucun accès n'est accordé si la valeur est une chaîne vide ou s'il n'y a pas de vue MIB active ayant cette valeur de vacmViewTreeFamilyViewName.
Groupe : vacmBasicGroup **Trap :** vacmAccessStatus	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.16.1.5.2.1.4.5.86.49.77.105.98.1.1 **Définition :** état de cette ligne conceptuelle. RowStatus TC [RFC2579<rfc2579.html>] exige que cette clause DESCRIPTION indique dans quelles circonstances d'autres objets de cette ligne peuvent être modifiés : La valeur de cet objet n'a aucun effet sur la possibilité de modifier d'autres objets de cette ligne conceptuelle.
Groupe : vacmBasicGroup **Trap :** vacmAccessStorageType	**Accès :** lecture seule **Syntaxe :** Integer **Définition :** type de stockage pour cette ligne conceptuelle. Les lignes conceptuelles ayant la valeur `permanent` n'ont pas besoin d'autoriser l'accès en écriture aux objets en colonne de la ligne.
Groupe : vacmBasicGroup **Trap :** vacmAccessWriteViewName	**Accès :** Lecture et création **Syntaxe :** Chaîne **Définition :** la valeur d'une instance de cet objet identifie la vue MIB du contexte SNMP à laquelle cette ligne conceptuelle autorise l'accès en écriture. La vue MIB identifiée est celle pour laquelle vacmViewTreeFamilyViewName a la même valeur que l'instance de cet objet. Aucun accès n'est accordé si la valeur est une chaîne vide ou s'il n'y a pas de vue MIB active ayant cette valeur de vacmViewTreeFamilyViewName.
Groupe : vacmBasicGroup **Trap :** vacmContextName	**Accès :** lecture seule **Syntaxe :** Chaîne **Définition :** nom lisible par l'homme identifiant un contexte spécifique au niveau d'une entité SNMP spécifique. Le contextName vide (de longueur nulle) représente le contexte par défaut.
Groupe : vacmBasicGroup **Trap :** vacmGroupName	**Accès :** Lecture et création **Syntaxe :** Chaîne **Définition :** nom du groupe auquel cette entrée (par exemple, la combinaison de securityModel et securityName) appartient. Ce groupName est utilisé comme index dans vacmAccessTable pour sélectionner une stratégie de contrôle d'accès. Cependant, une valeur dans ce tableau n'implique pas qu'une instance ayant cette valeur existe dans le tableau vacmAccesTable.
Groupe : vacmBasicGroup **Trap :** vacmSecurityToGroupStatus	**Accès :** Lecture et création **Syntaxe :** Integer **Définition :** état de cette ligne conceptuelle. Jusqu'à ce que les instances de toutes les colonnes correspondantes soient correctement configurées, la valeur de l'instance correspondante de la colonne vacmSecurityToGroupStatus est `notReady`. En particulier, une ligne qui vient d'être créée ne peut pas être activée tant qu'une valeur n'a pas été définie pour vacmGroupName. RowStatus TC [RFC2579<rfc2579.html>] exige que cette clause DESCRIPTION indique dans quelles circonstances d'autres objets de cette ligne peuvent être modifiés : La valeur de cet objet

Groupe/objet	Description
	n'a aucun effet sur la possibilité de modifier d'autres objets de cette ligne conceptuelle.
Groupe : vacmBasicGroup **Trap :** vacmSecurityToGroupStorageType	**Accès :** Lecture et création **Syntaxe :** Integer **Définition :** type de stockage pour cette ligne conceptuelle. Les lignes conceptuelles ayant la valeur `permanent` n'ont pas besoin d'autoriser l'accès en écriture aux objets en colonne de la ligne.
Groupe : vacmBasicGroup **Trap :** vacmViewSpinLock	**Accès :** lecture et écriture **Syntaxe :** Integer **Définition :** verrou consultatif utilisé pour permettre aux applications de générateur de commandes SNMP coopérantes de coordonner leur utilisation de l'opération de réglage lors de la création ou de la modification de vues. Lors de la création d'une nouvelle vue ou de la modification d'une vue existante, il est important de comprendre les interactions potentielles avec d'autres utilisations de la vue. vacmViewSpinLock doit être récupéré. Le nom de la vue à créer doit être déterminé comme étant unique par l'application de générateur de commandes SNMP en consultant vacmViewTreeFamilyTable. Enfin, la vue nommée peut être créée (Set), y compris le verrou consultatif. Si une autre application du générateur de commandes SNMP a modifié les vues entre-temps, la valeur du verrou tournant aura changé et cette création échouera car elle spécifiera la mauvaise valeur pour le verrou tournant. Comme il s'agit d'un verrou consultatif, l'utilisation de ce verrou n'est pas obligatoire.
Groupe : vacmBasicGroup **Trap :** vacmViewTreeFamilyMask	**Accès :** lecture seule **Syntaxe :** Chaîne **Définition :** masque binaire qui, en combinaison avec l'instance correspondante de vacmViewTreeFamilySubtree, définit une famille de sous-arborescences de vue. Chaque bit de ce masque de bits correspond à un sous-identifiant de vacmViewTreeFamilySubtree, le bit le plus significatif du i-ième octet de cette valeur de chaîne d'octets (étendu si nécessaire, voir ci-dessous) correspondant au (8*i - 7)-ième sous-identifiant, et le bit le moins significatif du i-ième octet de cette chaîne d'octets correspondant au (8*i)-ième sous-identifiant, où i est compris entre 1 et 16. Chaque bit de ce masque de bits spécifie si les sous-identifiants correspondants doivent ou non correspondre pour déterminer si un OBJECT IDENTIFIER se trouve dans cette famille de sous-arborescences de vue : `1` indique qu'il doit y avoir une correspondance exacte : `0` indique `wild card`, c'est-à-dire que toute valeur de sous-identifiant correspond. Ainsi, l'OBJECT IDENTIFIER X d'une instance d'objet est contenu dans une famille de sous-arborescences de vue si, pour chaque sous-identifiant de la valeur de vacmViewTreeFamilySubtree, soit : • - le i-ième bit de vacmViewTreeFamilyMask est 0, soit • - le ième sous-identifiant de X est égal au ième sous-identifiant de la valeur de vacmViewTreeFamilySubtree. Si la valeur de ce masque de bits est de M bits de long et qu'il y a plus de M sous-identifiants dans l'instance correspondante de vacmViewTreeFamilySubtree, le masque de bits est étendu avec des 1 pour avoir la longueur requise. Notez que, lorsque la valeur de cet objet est une chaîne de longueur nulle, cette règle d'extension entraîne l'utilisation d'un masque contenant uniquement des 1 (c'est-à-dire, aucun `wild card`), et la famille de sous-arborescences de vue est la seule sous-arborescence de vue identifiée de manière unique par l'instance correspondante de vacmViewTreeFamilySubtree. Notez que les masques de longueur supérieure à zéro n'ont pas besoin d'être pris en charge. Dans ce cas, cet objet est mis en lecture seule.

Groupe/objet	Description
Groupe : vacmBasicGroup **Trap :** vacmViewTreeFamilyStatus	**Accès :** lecture seule **Syntaxe :** Integer **Définition :** état de cette ligne conceptuelle. RowStatus TC [RFC2579<rfc2579.html>] exige que cette clause DESCRIPTION indique dans quelles circonstances d'autres objets de cette ligne peuvent être modifiés : La valeur de cet objet n'a aucun effet sur la possibilité de modifier d'autres objets de cette ligne conceptuelle.
Groupe : vacmBasicGroup **Trap :** vacmViewTreeFamilyStorageType	**Accès :** lecture seule **Syntaxe :** Integer **Définition :** type de stockage pour cette ligne conceptuelle. Les lignes conceptuelles ayant la valeur `permanent` n'ont pas besoin d'autoriser l'accès en écriture aux objets en colonne de la ligne.
Groupe : vacmBasicGroup **Trap :** vacmViewTreeFamilyType	**Accès :** lecture seule **Syntaxe :** Integer **Définition :** indique si les instances correspondantes de vacmViewTreeFamilySubtree et vacmViewTreeFamilyMask définissent une famille de sous-arborescences de vue qui est incluse dans la vue MIB ou exclue de celle-ci.

TCP-MIB

Groupe/objet	Description
Groupe : tcpGroup **Trap :** tcpActiveOpens	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.6.4.0 **Définition :** nombre de transitions directes effectuées par les connexions TCP vers l'état SYN-SENT à partir de l'état CLOSED.
Groupe : tcpGroup **Trap :** tcpAttemptFails	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.6.15.0 **Définition :** nombre de transitions directs effectuées par les connexions TCP vers l'état CLOSED à partir de l'état SYN-SENT ou de l'état SYN-RCVD, plus le nombre de transitions directes effectués par les connexions TCP vers l'état LISTEN depuis l'état SYN-RCVD.
Groupe : tcpGroup **Trap :** tcpConnLocalAddress	**Accès :** lecture seule **Syntaxe :** IpAddress **OID :** .1.3.6.1.2.1.6.11.0 **Définition :** adresse IP locale de cette connexion TCP. La valeur 0.0.0.0 est utilisée dans le cas d'une connexion à l'état d'écoute qui est disposée à accepter des connexions pour toute interface IP associée au nœud.
Groupe : tcpGroup **Trap :** tcpConnLocalPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.6.6.0 **Définition :** numéro de port local de cette connexion TCP.
Groupe : tcpGroup **Trap :** tcpConnRemAddress	**Accès :** lecture seule **Syntaxe :** IpAddress

Groupe/objet	Description
	OID : .1.3.6.1.2.1.6.12.0 **Définition :** adresse IP distante de cette connexion TCP.
Groupe : tcpGroup **Trap :** tcpConnRemPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.6.1.0 **Définition :** numéro de port distant de cette connexion TCP.
Groupe : tcpGroup **Trap :** tcpConnState	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.6.3.0 **Définition :** état de cette connexion TCP. La seule valeur pouvant être définie par une station de gestion est deleteTCB(12). En conséquence, il convient qu'un agent renvoie une réponse `badValue` si une station de gestion tente de définir cet objet sur une toute autre valeur. Si une station de gestion définit cet objet sur la valeur deleteTCB(12), cela a pour effet de supprimer le TCB (tel que défini dans la RFC 793) de la connexion correspondante sur le nœud géré, ce qui entraîne l'arrêt immédiat de la connexion. En tant qu'option spécifique à la mise en œuvre, un segment RST peut être envoyé du nœud géré à l'autre point de terminaison TCP (notez cependant que les segments RST ne sont pas envoyés de manière fiable).
Groupe : tcpGroup **Trap :** tcpCurrEstab	**Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.3.6.1.2.1.6.2.0 **Définition :** nombre de connexions TCP pour lesquelles l'état actuel est ESTABLISHED ou CLOSE-WAIT.
Groupe : tcpGroup **Trap :** tcpEstabResets	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.7.1.0 **Définition :** nombre de transitions directes effectuées par les connexions TCP vers l'état CLOSED à partir de l'état ESTABLISHED ou de l'état CLOSE-WAIT.
Groupe : tcpGroup **Trap :** tcpInErrs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.7.3.0 **Définition :** nombre total de segments reçus par erreur (par exemple, sommes de contrôle TCP erronées).
Groupe : tcpGroup **Trap :** tcpInSegs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.7.5.1.1.0.0.0.0.69 **Définition :** nombre total de segments reçus, y compris ceux reçus par erreur. Ce nombre inclut les segments reçus sur les connexions actuellement établies.
Groupe : tcpGroup **Trap :** tcpMaxConn	**Accès :** lecture seule **Syntaxe :** Integer **OID :** .1.3.6.1.2.1.7.5.1.2.0.0.0.0.69

Groupe/objet	Description
	Définition : limite du nombre total de connexions TCP que l'entité peut prendre en charge. Dans les entités où le nombre maximal de connexions est dynamique, cet objet doit contenir la valeur -1.
Groupe : tcpGroup **Trap :** tcpOutRsts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.7.2.0 **Définition :** nombre de segments TCP envoyés contenant l'indicateur RST.
Groupe : tcpGroup **Trap :** tcpOutSegs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.2.1.7.4.0 **Définition :** nombre total de segments envoyés, y compris ceux sur les connexions actuelles mais à l'exclusion de ceux contenant uniquement des octets retransmis.
Groupe : tcpGroup **Trap :** tcpPassiveOpens	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.1.6.0 **Définition :** nombre de transitions directes effectuées par les connexions TCP vers l'état SYN-RCVD depuis l'état LISTEN.
Groupe : tcpGroup **Trap :** tcpRetransSegs	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.1.2.0 **Définition :** nombre de transitions directes effectuées par les connexions TCP vers l'état SYN-RCVD depuis l'état LISTEN.
Groupe : tcpGroup **Trap :** tcpRtoAlgorithm	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.15.1.1.4.0 **Définition :** algorithme utilisé pour déterminer la valeur d'expiration utilisée pour retransmettre les octets non acquittés.
Groupe : tcpGroup **Trap :** tcpRtoMax	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.15.1.1.3.0 **Définition :** valeur maximale autorisée par une mise en œuvre TCP pour le délai de retransmission, mesurée en millisecondes. Une sémantique plus fine pour les objets de ce type dépend de l'algorithme utilisé pour déterminer le délai de retransmission. Un objet de ce type a la sémantique de la quantité UBOUND décrite dans RFC 793, en particulier lorsque l'algorithme d'expiration est rsre(3).
Groupe : tcpGroup **Trap :** tcpRtoMin	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.15.1.1.1.0 **Définition :** valeur minimale autorisée par une mise en œuvre TCP pour le délai de retransmission, mesurée en millisecondes. Une sémantique plus fine pour les objets de ce type dépend de l'algorithme utilisé pour déterminer le délai de retransmission. Un objet de ce type a la sémantique de la quantité LBOUND décrite dans RFC 793, en particulier lorsque l'algorithme d'expiration est rsre(3).

UDP-MIB

Groupe/objet	Description
Groupe : udpGroup **Trap :** udpInDatagrams	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.1.5.0 **Définition :** nombre total de datagrammes UDP envoyés aux utilisateurs UDP.
Groupe : udpGroup **Trap :** udpInErrors	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.6 **Définition :** nombre de datagrammes UDP reçus qui n'ont pas pu être envoyés pour des raisons autres que l'absence d'une application au port de destination.
Groupe : udpGroup **Trap :** udpLocalAddress	**Accès :** lecture seule **Syntaxe :** IpAddress **OID :** 1.3.6.1.6.3.15.1.2.2.1.5.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Définition :** adresse IP locale de cet auditeur UDP. Dans le cas d'un auditeur UDP qui est disposé à accepter des datagrammes pour toute interface IP associée au nœud, la valeur 0.0.0.0 est utilisée.
Groupe : udpGroup **Trap :** udpLocalPort	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.6.3.15.1.2.2.1.4.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Définition :** numéro de port local de cet auditeur UDP.
Groupe : udpGroup **Trap :** udpNoPorts	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.7 **Définition :** nombre total de datagrammes UDP reçus pour lesquels il n'y avait pas d'application au port de destination.
Groupe : udpGroup **Trap :** udpOutDatagrams	**Accès :** lecture seule **Syntaxe :** Counter32 **OID :** 1.3.6.1.6.3.15.1.2.2.1.10 **Définition :** nombre total de datagrammes UDP envoyés depuis cette entité.

15.2 MIB RUGGEDCOM propriétaires prises en charge

RUGGEDCOM ROS prend en charge les MIB RUGGEDCOM propriétaires suivantes :

⚠ NOTA

Cette section répertorie toutes les MIB prises en charge par RUGGEDCOM ROS, et est destinée uniquement à des fins de référence. La prise en charge de chaque appareil peut varier.

- **RUGGEDCOM-AAA-SERVER-MIB**

  Pour plus d'informations, voir "RUGGEDCOM-AAA-SERVER-MIB".

- **RUGGEDCOM-DIGITAL-INPUTS-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-DIGITAL-INPUTS-MIB".
- **RUGGEDCOM-GPS-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-GPS-MIB".
- **RUGGEDCOM-IP-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-IP-MIB".
- **RUGGEDCOM-IRIGB-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-IRIGB-MIB".
- **RUGGEDCOM-MC30-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-MC30-MIB".
- **RUGGEDCOM-NTP-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-NTP-MIB".
- **RUGGEDCOM-POE-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-POE-MIB".
- **RUGGEDCOM-SERIAL-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-SERIAL-MIB".
- **RUGGEDCOM-SFP-DDM-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-SFP-DDM-MIB".
- **RUGGEDCOM-STP-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-STP-MIB".
- **RUGGEDCOM-SYS-INFO-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-SYS-INFO-MIB".
- **RUGGEDCOM-TIMECONFIG-MIB**
  Pour plus d'informations, voir "RUGGEDCOM-TIMECONFIG-MIB".

RUGGEDCOM-AAA-SERVER-MIB

Groupe(s)	Objet	Description
rcRadiusNotifyGroup	radiusServiceAvailableChange	**OID :** 1.3.6.1.4.1.15004.4.14.1.2.1.3 **Définition :** notification générée lorsque l'état du service RADIUS change.
rcRadiusBaseGroup	rcRadiusServerAutUdpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.1.1.1.1.3 **Définition :** port UDP du serveur RADIUS.
rcRadiusBaseGroup	rcRadiusServerId	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.1.1.1.1.1

Groupe(s)	Objet	Description
		Définition : valeur d'index utilisée pour identifier le serveur RADIUS. 1. Serveur principal 2. Serveur de sauvegarde
rcRadiusBaseGroup	rcRadiusServerIP	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.14.1.1.1.1.2 **Définition :** adresse IP du serveur RADIUS.
rcRadiusBaseGroup	rcRadiusServerMaxRetry	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.1.1.1.1.4 **Définition :** nombre maximum de tentatives par l'authentificateur de contact avec le serveur RADIUS pour authentifier l'utilisateur en cas de défaillance quelconque.
rcRadiusBaseGroup rcRadiusServiceStatusGroup	rcRadiusServerReachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.14.1.1.1.1.6 **Définition :** état du serveur RADIUS principal.
rcRadiusBaseGroup	rcRadiusServerTimeOut	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.1.1.1.1.5 **Définition :** délai d'attente en millisecondes pendant lequel l'authentificateur attend une réponse du serveur RADIUS.
rcRadiusBaseGroup	rcTacacsServerAutTcpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.2.1.1.1.3 **Définition :** port TCP du serveur TACACS.
rcRadiusBaseGroup	rcTacacsServerId	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.2.1.1.1.1 **Définition :** valeur d'index utilisée pour identifier le serveur TACACS. 1. Serveur principal 2. Serveur de sauvegarde
rcRadiusBaseGroup	rcTacacsServerIP	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.14.2.1.1.1.2 **Définition :** adresse IP du serveur TACACS.
rcRadiusBaseGroup	rcTacacsServerMaxRetry	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.2.1.1.1.4 **Définition :** nombre maximum de tentatives par l'authentificateur de contact avec le serveur TACACS pour authentifier l'utilisateur en cas de défaillance quelconque.

Groupe(s)	Objet	Description
rcTacacsBaseGroup rcTacacsServiceStatusGroup	rcTacacsServerReachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.14.2.1.1.1.6 **Définition :** état du serveur TACACS.
rcTacacsBaseGroup	rcTacacsServerTimeOut	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.14.2.1.1.1.5 **Définition :** délai d'attente en millisecondes pendant lequel l'authentificateur attend une réponse du serveur TACACS.
rcTacacsNotifyGroup	tacacsServiceAvailableChange	**OID :** 1.3.6.1.4.1.15004.5.23 **Définition :** notification générée lorsque l'état du service TACACS change.

RUGGEDCOM-DIGITAL-INPUTS-MIB

Groupe(s)	Objet	Description
rcDigitalInputsTableGroup	rcDiActiveState	**Accès :** lecture et écriture **Syntaxe :** RcLowOrHigh **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.3.1 **Définition :** état qui activerait une alarme pour cette entrée TOR.
rcDigitalInputsTableGroup	rcDiAlarm	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.2.1 **Définition :** état d'alarme actuel pour cette entrée TOR. Un changement de la valeur de cet objet entraîne l'envoi d'une notification (trap) digitalInputTrap.
rcDigitalInputsTableGroup	rcDiAlarmStatus	**Accès :** lecture seule **Syntaxe :** RcActiveOrInactive **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.8.1 **Définition :** état d'alarme actuel pour cette entrée TOR. Un changement de la valeur de cet objet entraîne l'envoi d'une notification (trap) digitalInputTrap.
rcDigitalInputsTableGroup	rcDiDelayOff	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.5.1 **Définition :** délai pendant lequel l'entrée doit être inactive avant que l'alarme ne soit désactivée.
rcDigitalInputsTableGroup	rcDiDelayOn	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.4.1 **Définition :** délai pendant lequel l'entrée doit être active avant que l'alarme ne soit activée.
rcDigitalInputsTableGroup	rcDiDescription	**Accès :** lecture et écriture

Groupe(s)	Objet	Description
		Syntaxe : DisplayString **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.6.1 **Définition :** état d'entrée TOR actuel lu depuis le matériel.
rcDigitalInputsTableGroup	rcDiID	**Accès :** non accessible **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.1 **Définition :** ID d'entrée TOR physique de l'appareil pour lequel cette entrée contient des réglages de configuration.
rcDigitalInputsTableGroup	rcDiInputState	**Accès :** lecture seule **Syntaxe :** RcLowOrHigh **OID :** 1.3.6.1.4.1.15004.4.8.1.1.1.7.1 **Définition :** état d'entrée TOR actuel lu depuis le matériel.

RUGGEDCOM-GPS-MIB

Groupe(s)	Objet	Description
rcGpsBaseGroup01	rcFreqAdj	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.9.1.9.0 **Définition :** quantité actuelle de discipline appliquée à la référence de fréquence locale (TCXO).
rcGpsBaseGroup01	rcGpsAntPower	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.9.1.4.0 **Définition :** le récepteur GPS requiert une antenne active. Une antenne active comprend un préamplificateur qui filtre et amplifie les signaux GPS avant de l'envoyer au récepteur. Cette option permet à l'utilisateur d'activer ou de désactiver l'alimentation de l'antenne GPS. Si l'antenne GPS est partagée entre plusieurs appareils, tous les appareils sauf un doivent l'alimenter.
rcGpsBaseGroup01	rcGpsCableCompensate	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.9.1.3.0 **Définition :** la compensation de câble en nanosecondes peut servir à compenser une longueur de câble importante afin de minimiser l'inexactitude horaire.
rcGpsBaseGroup01	rcGpsLatitude	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.9.1.6.0 **Définition :** latitude GPS.
rcGpsBaseGroup01	rcGpsLocInt	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.9.1.2.0

Groupe(s)	Objet	Description
		Définition : intervalle de temps en minutes pendant lequel le récepteur GPS doit acquérir un verrouillage de la source de temps. Normalement, le récepteur GPS a besoin de quelques minutes pour verrouiller le signal. L'utilisateur doit définir un intervalle de temps raisonnable. Si l'intervalle de temps expire sans acquisition du verrouillage, le système distribue l'heure à l'aide de l'horloge locale.
rcGpsBaseGroup01	rcGpsLongtitude	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.9.1.7.0 **Définition :** longitude GPS.
rcGpsNotifyGroup rcGpsBaseGroup rcGpsBaseGroup01	rcGpsStatus	**Accès :** lecture seule **Syntaxe :** RcTimeSyncStatus **OID :** 1.3.6.1.4.1.15004.4.9.1.1.0 **Définition :** état de synchronisation du système lorsque le GPS est une source de temps principale. Si la valeur de cet objet est modifiée, une notification rcGpsStatusChange est générée.
rcGpsNotifyGroup	rcGpsStatusChange	**OID :** 1.3.6.1.4.1.15004.5.19 **Définition :** notification générée si l'état du module GPS est modifié.
rcGpsBaseGroup01	rcOFM	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.9.1.8.0 **Définition :** décalage horaire actuel entre les horloges système et de référence.
rcGpsBaseGroup01	rcSatelliteInView	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.9.1.5.0 **Définition :** nombre de satellites actuellement suivis par le module GPS.

RUGGEDCOM-IP-MIB

Groupe(s)	Objet	Description
rcIpObjectsGroup	rcIpConfigDefaultGateway	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.3.1.3.0 **Définition :** passerelle IP par défaut pour l'appareil.
rcIpObjectsGroupDflt	rcIpConfigDfltMgmtIpAddress	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.3.1.4.0 **Définition :** adresse IP de gestion de l'appareil.
rcIpObjectsGroupDflt	rcIpConfigDfltMgmtIpSubnet	**Accès :** lecture et écriture **Syntaxe :** IpAddress

Groupe(s)	Objet	Description
		OID : 1.3.6.1.4.1.15004.4.3.1.5.0 **Définition :** masque de sous-réseau associé à l'entrée d'adresse IP de gestion. La valeur du masque est une adresse IP avec tous les bits de réseau mis à 1 et tous les bits d'hôtes mis à 0.
rcIpObjectsGroup	rcIpConfigMgmtIpAddress	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.3.1.1.0 **Définition :** adresse IP de gestion de l'appareil.
rcIpObjectsGroup	rcIpConfigMgmtIpSubnet	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.3.1.2.0 **Définition :** masque de sous-réseau associé à l'entrée d'adresse IP de gestion. La valeur du masque est une adresse IP avec tous les bits de réseau mis à 1 et tous les bits d'hôtes mis à 0.

RUGGEDCOM-IRIGB-MIB

Groupe(s)	Objet	Description
rcIrigbAMOutGroup	rcIrigbAMOutput	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.10.1.2.0 **Définition :** sélectionne le mode AM (modulation d'amplitude) d'un port IRIGB.
rcIrigbCommonGroup	rcIrigbCableComp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.7.0 **Définition :** la compensation de câble en nanosecondes peut servir à compenser une longueur de câble importante afin de minimiser l'inexactitude horaire.
rcIrigbCommonGroup	rcIrigbExt	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.10.1.4.0 **Définition :** les extensions IRIGB utilisent des bits supplémentaires de la partie fonctions de contrôle (Control Functions (CF)) du code horaire IRIGB. Dans cette partie du code horaire, des bits sont désignés pour des fonctionnalités supplémentaires, notamment : année civile, secondes intercalaires, secondes intercalaires en attente, Daylight Saving Time (DST), DST en attente, décalage horaire local et qualité du temps. Notez que seuls les codes horaires Bxx0, Bxx1, Bxx4 et Bxx5 prennent en charge les extensions IRIGB.
rcIrigbCommonGroup	rcIrigbFreqAdj	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.9.0

Groupe(s)	Objet	Description
		Définition : quantité actuelle de discipline appliquée à la référence de fréquence locale (TCXO).
rcIrigbInputGroup	rcIrigbInput	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.10.1.5.0 **Définition :** ce paramètre couvre les entrées AM et PWM.
rcIrigbCommonGroup	rcIrigbLockInt	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.6.0 **Définition :** Intervalle de temps en minutes pendant lequel le récepteur IRIGB doit acquérir un verrouillage de la source de temps. Normalement, le récepteur IRIGB a besoin de quelques minutes pour verrouiller le signal. L'utilisateur doit définir un intervalle de temps raisonnable. Si l'intervalle de temps expire sans acquisition du verrouillage, le système distribue l'heure à l'aide de l'horloge locale.
rcIrigbCommonGroup	rcIrigbOFM	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.8.0 **Définition :** décalage horaire actuel entre les horloges système et de référence.
rcIrigbTTLOutput01Group	rcIrigbOutputPWM1	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.10.1.10.0 **Définition :** sélectionne le mode de fonctionnement pour le port de sortie TTL. Le mode PWM est conforme à la norme IRIG 200-04. PPx fournit une impulsion générique par interface de X secondes pour synchroniser des appareils externes.
rcIrigbTTLOutput02Group	rcIrigbOutputPWM2	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.10.1.14.0 **Définition :** sélectionne le mode de fonctionnement pour le port2 de sortie TTL. Le mode PWM est conforme à la norme IRIG 200-04. PPx fournit une impulsion générique par interface de X secondes pour synchroniser des appareils externes.
rcIrigbTTLOutput01Group	rcIrigbPulseInterval1	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.11.0 **Définition :** sélectionne l'intervalle d'impulsion en secondes pour le port de sortie TTL. Ce paramètre est utilisé en combinaison avec PPx afin de fournir une impulsion générique par interface de X secondes pour synchroniser des appareils externes.
rcIrigbTTLOutput02Group	rcIrigbPulseInterval2	**Accès :** lecture et écriture **Syntaxe :** Integer32

Groupe(s)	Objet	Description
		OID : 1.3.6.1.4.1.15004.4.10.1.15.0 **Définition :** sélectionne l'intervalle d'impulsion en secondes pour le port2 de sortie TTL. Ce paramètre est utilisé en combinaison avec PPx afin de fournir une impulsion générique par interface de X secondes pour synchroniser des appareils externes.
rcIrigbTTLOutput01Group	rcIrigbPulseWidth1	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.12.0 **Définition :** sélectionne la largeur d'impulsion en ms pour le port de sortie TTL. Ce paramètre est utilisé en combinaison avec PPx afin de contrôler la largeur de l'impulsion.
rcIrigbTTLOutput02Group	rcIrigbPulseWidth2	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.10.1.16.0 **Définition :** sélectionne la largeur d'impulsion en ms pour le port2 de sortie TTL. Ce paramètre est utilisé en combinaison avec PPx afin de contrôler la largeur de l'impulsion.
rcIrigbTTLOutput01Group	rcIrigbStartTime1	**Accès :** lecture et écriture **Syntaxe :** RcTimeStamp **OID :** 1.3.6.1.4.1.15004.4.10.1.13.0 **Définition :** ce paramètre est utilisé en combinaison avec PPx pour définir l'heure de lancement du premier événement PPx. Ce paramètre doit être défini sur au moins 15 secondes avant le démarrage du PPx souhaité. Le premier événement PPx pourrait sinon être perdu.
rcIrigbTTLOutput02Group	rcIrigbStartTime2	**Accès :** lecture et écriture **Syntaxe :** RcTimeStamp **OID :** 1.3.6.1.4.1.15004.4.10.1.17.0 **Définition :** ce paramètre est utilisé en combinaison avec PPx pour définir l'heure de lancement du premier événement PPx. Ce paramètre doit être défini sur au moins 15 secondes avant le démarrage du PPx souhaité. Le premier événement PPx pourrait sinon être perdu.
rcIrigbCommonGroup rcIrigbBaseGroup	rcIrigbStatus	**Accès :** lecture seule **Syntaxe :** RcTimeSyncStatus **OID :** 1.3.6.1.4.1.15004.4.10.1.1.0 **Définition :** état de synchronisation du système lorsqu'IRIGB est une source de temps principale. Si la valeur de cet objet est modifiée, une notification rcIrigbStatusChange est envoyée.
rcIrigbNotifyGroup	rcIrigbStatusChange	**OID :** 1.3.6.1.4.1.15004.5.20 **Définition :** notification générée si l'état du module IRIGB est modifié.
rcIrigbCommonGroup	rcIrigbTimeCode	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.10.1.3.0

Groupe(s)	Objet	Description
		Définition : cet appareil utilise la convention suivante pour décoder le code horaire IRIGB : la lettre [B] représente le format IRIG-B, [xx] représente [00] pour le mode de fonctionnement PWM/TTL et [12] pour le mode de fonctionnement AM. Par exemple, Bxx7 représente B007 pour le mode de fonctionnement PWM/TTL et B127 pour le mode de fonctionnement AM. Seuls les codes horaires Bxx0, Bxx1, Bxx4 et Bxx5 prennent en charge les extensions IRIGB.

RUGGEDCOM-MC30-MIB

Groupe(s)	Objet	Description
rcPoeNotifyGroup	rcPoeOverheat	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.5.12.1 **Définition :** la valeur de cet objet sera définie sur 'true(1)' si PoE est en surchauffe. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification rcPoeOverheat.

RUGGEDCOM-NTP-MIB

Groupe(s)	Objet	Description
rcNTPNotifyGroup	ntpServiceAvailableChange	**OID :** 1.3.6.1.4.1.15004.5.21 **Définition :** notification générée lorsque l'état du service NTP change.
rcNTPBaseGroup	rcNTPBackUpServerIP	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.13.1.4.0 **Définition :** adresse IP du serveur de sauvegarde.
rcNTPServiceStatusGroup	rcNTPBackUpServerReachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.13.1.9.0 **Définition :** état du serveur de sauvegarde NTP.
rcNTPBaseGroup	rcNTPBackUpServerUpdatePeriod	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.13.1.5.0 **Définition :** fréquence en minutes à laquelle le serveur (S)NTP est interrogé pour une mise à jour de l'heure.
rcNTPBaseGroup	rcNTPFRQADJ	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.13.1.7.0 **Définition :** quantité de discipline appliquée à la référence de fréquence locale (TCXO) ; c'est-

Groupe(s)	Objet	Description
		à-dire la quantité de corrections requises sur ce système pour synchroniser la référence actuelle.
rcNTPBaseGroup	rcNTPOFM	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.13.1.6.0 **Définition :** décalage horaire actuel entre le serveur (S)NTP et les horloges client, calculé avec <heure sur l'horloge client> - <heure sur l'horloge du serveur>.
rcNTPBaseGroup	rcNTPPriServerIP	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.13.1.2.0 **Définition :** adresse IP du serveur principal.
rcNTPServiceStatusGroup	rcNTPPriServerReachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.13.1.8.0 **Définition :** état du serveur NTP principal.
rcNTPBaseGroup	rcNTPPriServerUpdatePeriod	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.13.1.3.0 **Définition :** fréquence en minutes à laquelle le serveur (S)NTP est interrogé pour une mise à jour de l'heure.
rcNTPBaseGroup	rcSNTPEnabled	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.13.1.1.0 **Définition :** activer/désactiver la fonctionnalité de serveur SNTP.

RUGGEDCOM-POE-MIB

Groupe(s)	Objet	Description
rcBasePoeGroup	rcPoeCapacity	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.1.1.0 **Définition :** puissance de sortie totale maximum pouvant être fournie par des ports PoE. Si la valeur de cet objet est définie sur '0', la capacité est illimitée. Lorsque la consommation électrique totale atteint cette limite, les ports PoE à basse priorité sont fermés.
rcBasePoeGroup	rcPoeConsumption	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.1.4.0 **Définition :** consommation électrique totale actuelle de tous les appareils PoE.

Groupe(s)	Objet	Description
rcBasePoeGroup	rcPoeMinimumVoltage	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.1.2.0 **Définition :** tension minimum requise à fournir par des ports PoE. Tension minimum requise pour les ports PoE. Lorsque la tension PoE tombe en dessous de ce seuil, les ports PoE à basse priorité sont fermés.
rcBasePoeStatusGroup	rcPoeOverheatStatus	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.7.1.5.0 **Définition :** la valeur de cet objet sera définie sur true(1) si PoE est en surchauffe. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification *rcPoeOverheat*.
rcPoeNotifyGroup	rcPoeOverload	**Accès :** lecture seule **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.5.12.2 **Définition :** la valeur de cet objet sera définie sur true(1) si PoE est en surcharge. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification *rcPoeOverload*.
rcBasePoeStatusGroup	rcPoeOverloadStatus	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.7.1.6.0 **Définition :** la valeur de cet objet sera définie sur true(1) si PoE est en surcharge. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification *rcPoeOverload*.
rcPoeTableGroup	rcPoePort	**Accès :** non accessible **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.1 **Définition :** port PoE pour lequel cette entrée contient des informations. La valeur est limitée par le nombre de ports de l'appareil.
rcPoeTableGroup	rcPoePortAdmin	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.2.13 **Définition :** port PoE pour lequel cette entrée contient des informations. La valeur est limitée par le nombre de ports de l'appareil.
rcPoeTableGroup	rcPoePortClass	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.5.13 **Définition :** valeur de classe PoE définissant le niveau de puissance.
rcPoeTableGroup	rcPoePortCurrent	**Accès :** lecture seule

Groupe(s)	Objet	Description
		Syntaxe : Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.7.13 **Définition :** valeur de classe PoE définissant le niveau de puissance.
rcPoeTableGroup	rcPoePortPowered	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.4.13 **Définition :** définit si l'alimentation est actuellement fournie par le port.
rcPoeTablePriorityGroup	rcPoePortPriority	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.3.13 **Définition :** priorité du port. Les ports à basse priorité sont fermés en premier si l'alimentation est surchargée.
rcPoeTableGroup	rcPoePortVoltage	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.7.2.1.1.6.13 **Définition :** valeur de classe PoE définissant le niveau de puissance.
rcBasePoeGroup	rcPoeReenableTime	**Accès :** lecture et écriture **Syntaxe :** Unsigned32 **OID :** 1.3.6.1.4.1.15004.4.7.1.3.0 **Définition :** temps d'attente pour la réactivation de ports PoE à basse priorité après leur fermeture en raison de la condition de surcharge.
rcPoeNotifyGroup	rcPoeUndervoltage	**OID :** 1.3.6.1.4.1.15004.5.12.3 **Définition :** tension PoE faible.
rcBasePoeStatusGroup	rcPoeUndervoltageStatus	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.7.1.7.0 **Définition :** caractère pouvant être utilisé pour forcer la transmission de données accumulées au réseau pour la connexion au maître dynamique. Si aucun caractère de mise en paquet n'est configuré, les données accumulées sont transmises sur la base du paramètre de délai de mise en paquet *rcPreemptRSDynPackTimer*.

RUGGEDCOM-SERIAL-MIB

Groupe(s)	Objet	Description
rcSerialConnStatsGroup	rcConnStatsRxPkts	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.15.1.1.4 **Définition :** nombre de paquets reçus.
rcSerialConnStatsGroup	rcConnStatsTxPkts	**Accès :** lecture seule

Groupe(s)	Objet	Description
		Syntaxe : Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.15.1.1.5 **Définition :** nombre de paquets transmis
rcSerialDnpGroup	rcDnpAgingTimer	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.8.4.0 **Définition :** le temps d'inactivité de communication après lequel une adresse DNP apprise est supprimée du tableau d'adresses d'appareil. Les entrées dans le tableau Link Statistics (statistiques de liaison) avec l'adresse vieillie sont conservées jusqu'à ce que les statistiques soient effacées.
rcSerialDnpGroup	rcDnpDscp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.8.6.0 **Définition :** valeur de l'octet DS à définir dans l'en-tête IP. La définition de l'octet DS est prise en charge dans la direction de sortie uniquement.
rcSerialDnpGroup	rcDnpIpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.8.2.0 **Définition :** numéro de port local sur lequel le protocole DNP écoute des connexions ou des datagrammes UDP.
rcSerialDnpGroup	rcDnpLearning	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.6.8.3.0 **Définition :** active ou désactive l'apprentissage d'adresses. L'apprentissage peut être désactivé ou activé sur l'interface IP de gestion, ou activé sur une interface avec une adresse IP spécifique. Si l'apprentissage est activé et une adresse distante est inconnue, un message de transmission UDP est envoyé et les adresses sources sont apprises sur les appareils qui exécutent le protocole DNP. Si une adresse locale est inconnue, un message est envoyé à tous les ports série exécutant le protocole DNP. Les adresses locales sont apprises des réponses locales. Si le transport TCP est configuré, une connexion est établie avec les appareils avec l'adresse IP correspondante.
rcSerialDnpGroup	rcDnpLinkStats	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.8.5.0 **Définition :** active la collecte de statistiques de liaisons.
rcSerialDnpRsGroup	rcDnpRsCalllDir	**Accès :** lecture et écriture **Syntaxe :** RcCallDir **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.2.1 **Définition :** définit les éléments suivants : • in(0) : accepte une connexion entrante. • out(1) : place une connexion sortante

Groupe(s)	Objet	Description
		• both(2) : place une connexion sortante et attend une connexion entrante **Remarque** Ce paramètre est applicable uniquement au transport TCP.
rcSerialDnpRsGroup	rcDnpRsIpAdd	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.7.1 **Définition :** définit l'adresse IP comme suit : • Pour la connexion TCP sortante (client), 'rcRawSockCallDir' est défini sur 'out(2)'. Il s'agit de l'adresse IP distante avec laquelle communiquer. • Pour la connexion TCP entrante (serveur), 'rcRawSockCallDir' est défini sur 'out(2)' ou 'both(3)'. Il s'agit de l'adresse IP de l'interface locale à écouter pour le port local pour une demande de connexion. • Si les connexions sortantes et entrantes sont activées (client ou serveur), 'rcRawSockCallDir' est défini sur 'both(3)'. Il s'agit de l'adresse IP distante où placer une demande de connexion TCP sortante ou de laquelle accepter des appels. • Pour le transport UDP, adresse de l'interface à écouter pour les datagrammes UDP.
rcSerialDnpRsGroup	rcDnpRsLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.8.1 **Définition :** active la collecte de statistiques de liaisons.
rcSerialDnpRsGroup	rcDnpRsLocPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.5.1 **Définition :** port IP local à écouter pour une connexion TCP entrante ou des datagrammes UDP.
rcSerialDnpRsGroup	rcDnpRsMaxConns	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.4.1 **Définition :** nombre maximum de connexions TCP entrantes autorisées.
rcSerialDnpRsGroup	rcDnpRsRemPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.6.1 **Définition :** port TCP distant à utiliser lors du placement d'une connexion sortante.
rcSerialDnpRsGroup	rcDnpRsTransport	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.9.1.1.3.1

Groupe(s)	Objet	Description
		Définition : protocole de transport utilisé pour le trafic IP pour DNPRS sur ce port.
rcSerialDnpGroup	rcDnpTransport	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.8.1.0 **Définition :** protocole de transport utilisé pour le trafic IP pour le protocole DNP.
	rcMbClient	**OID :** 1.3.6.1.4.1.15004.4.6.3 **Définition :** sous-arborescence principale pour la gestion des réglages du client de protocole Modbus sur des appareils série RUGGEDCOM.
	rcMbClientDscp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.3.4.0 **Définition :** valeur de l'octet DS à définir dans l'en-tête IP. La définition de l'octet DS est prise en charge dans la direction de sortie uniquement.
	rcMbClientFwdExcp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.3.2.0 **Définition :** active la transmission de messages d'exception au maître sous forme des codes d'exception 10 (aucun chemin) ou 11 (aucune réponse). Lorsque le maître interroge une RTU non configurée ou si le serveur Modbus distant reçoit une interrogation pour une RTU qui n'est pas configurée ou expire, il renvoie un message d'exception. Cet objet doit être défini sur 'disabled(2)' si le maître ne prend pas en charge les exceptions mais reconnaît une défaillance d'expiration pendant l'attente d'une réponse.
	rcMbClientIPPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.3.1.0 **Définition :** numéro de port distant auquel le gestionnaire de connexions de protocole envoie des demandes de connexion TCP.
	rcMbClientLinkStats	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.3.3.0 **Définition :** active la collecte de statistiques de liaison.
rcSerialMbServerGroup	rcMbServerAuxTcpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.2.1.1.3.1 **Définition :** numéro de port TCP alternatif où un 'rcMbServerPort' peut écouter les connexions TCP entrantes. Comme le serveur TCP Modbus écoute toujours sur le port TCP 502, ce paramètre permet à l'appareil série RUGGEDCOM d'accepter les demandes de connexion de protocole TCP Modbus sur les deux ports TCP.

Groupe(s)	Objet	Description
rcSerialMbServerGroup	rcMbServerLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.2.1.1.5.1 **Définition :** active la collecte de statistiques de liaisons.
	rcMbServerPort	**Accès :** non accessible **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.6.2.1.1.1 **Définition :** numéro de port série physique pour lequel cette entrée contient les réglages de configuration du protocole Modbus Server.
rcSerialMbServerGroup	rcMbServerRespTimer	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.2.1.1.2.1 **Définition :** délai d'attente autorisé pour le démarrage de la réponse de la RTU.
rcSerialMbServerGroup	rcMbServerSendExcep	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.2.1.1.4.1 **Définition :** permet aux appareils série RUGGEDCOM d'activer ou de désactiver le renvoi d'une exception TCP Modbus au maître si aucune réponse n'a été reçue de la RTU pendant le délai imparti.
rcSerialMicrolokGroup	rcMicrolokDscp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.7.4.0 **Définition :** valeur de l'octet DS à définir dans l'en-tête IP. La définition de l'octet DS est prise en charge dans la direction de sortie uniquement.
rcSerialMicrolokGroup	rcMicrolokIpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.7.2.0 **Définition :** numéro de port local sur lequel le protocole Microlok écoute des connexions ou des datagrammes UDP.
rcSerialMicrolokGroup	rcMicrolokLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.7.3.0 **Définition :** active la collecte de statistiques de liaisons.
rcSerialMicrolokGroup	rcMicrolokTransport	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.7.1.0 **Définition :** protocole de transport utilisé pour le trafic IP pour le protocole Microlok.
rcSerialMirrBitsGroup	rcMirrBitsIpAdd	**Accès :** lecture et écriture **Syntaxe :** IpAddress

Groupe(s)	Objet	Description
		OID : 1.3.6.1.4.1.15004.4.6.10.1.1.5.1 **Définition :** adresse IP de l'interface à écouter pour les datagrammes UDP.
rcSerialMirrBitsGroup	rcMirrBitsLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.10.1.1.6.1 **Définition :** active la collecte de statistiques de liaisons.
rcSerialMirrBitsGroup	rcMirrBitsLocPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.10.1.1.3.1 **Définition :** port IP local à écouter pour des datagrammes UDP.
rcSerialMirrBitsGroup	rcMirrBitsRemPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.10.1.1.4.1 **Définition :** port distant vers lequel les protocoles de ce port peuvent échanger des datagrammes UDP.
rcSerialMirrBitsGroup	rcMirrBitsTransport	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.10.1.1.2.1 **Définition :** protocole de transport utilisé pour le trafic IP pour les bits mis en miroir sur ce port. Cet objet est toujours défini sur la valeur 'udp(2)'.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynPackChar	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.10.1 **Définition :** caractère pouvant être utilisé pour forcer la transmission de données accumulées au réseau pour la connexion au maître dynamique. Si aucun caractère de mise en paquet n'est configuré, les données accumulées sont transmises sur la base du paramètre de délai de mise en paquet *rcPreemptRSDynPackTimer*.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynPackTimer	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.11.1 **Définition :** délai en millisecondes entre le dernier caractère reçu et la transmission des données au maître dynamique.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynTimeout	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.12.1 **Définition :** délai (en secondes) pendant lequel un maître dynamique est autorisé à rester inactif avant que sa connexion ne soit fermée. Le protocole écoute le socket ouvert sur le maître dynamique, et si la connexion est fermée si aucune donnée n'est reçue pendant cet intervalle.
rcSerialPreEmpRawSockGroup	rcPreemptRSFlowControl	**Accès :** lecture et écriture

Groupe(s)	Objet	Description
		Syntaxe : RcFlowControl **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.5.1 **Définition :** type de FlowControl à utiliser sur ce port.
rcSerialPreEmpRawSockGroup	rcPreemptRSIpAdd	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.8.1 **Définition :** définit l'adresse IP comme suit : • Pour les connexions TCP sortantes (client), 'rcRawSockCallDir' défini sur 'out(2)' est l'adresse IP distante avec laquelle communiquer. • Pour les connexions TCP entrantes (serveur), 'rcRawSockCallDir' est défini sur 'out(2)' ou 'both(3)', il s'agit de l'adresse IP de l'interface locale à écouter pour le port local pour une demande de connexion. • Si les connexions sortantes et entrantes sont activées (client ou serveur), 'rcRawSockCallDir' est défini sur 'both(3)', il s'agit de l'adresse IP distante à utiliser pour placer une demande de connexion TCP sortante ou de laquelle accepter des appels.
rcSerialPreEmpRawSockGroup	rcPreemptRSLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.9.1 **Définition :** active la collecte de statistiques de liaisons.
rcSerialPreEmpRawSockGroup	rcPreemptRSLocPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.6.1 **Définition :** port IP local à écouter pour une connexion TCP entrante ou un datagramme UDP.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackChar	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.2.1 **Définition :** caractère pouvant être utilisé pour forcer la transmission de données accumulées au réseau. Si aucun caractère de mise en paquet n'est configuré, l'objet est défini sur la valeur '256' et les données accumulées sont transmises sur la base du paramètre de délai de mise en paquet qui est la valeur définie pour l'objet *rcPreemptRSDynPackTimer*.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackSize	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.4.1 **Définition :** nombre maximum d'octets reçus du port série à mettre dans un paquet IP.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackTimer	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.3.1 **Définition :** délai en millisecondes entre le dernier caractère reçu et la transmission des données.

Groupe(s)	Objet	Description
rcSerialPreEmpRawSockGroup	rcPreemptRSRemPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.5.1.1.7.1 **Définition :** port TCP distant à utiliser lors du placement d'une connexion sortante.
rcSerialRawSocketGroup	rcRawSockCallDir	**Accès :** lecture et écriture **Syntaxe :** RcCallDir **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.7.1 **Définition :** définit les éléments suivants : **Remarque** Ce paramètre est applicable uniquement au transport TCP. • in(0) : accepte une connexion entrante. • out(1) : place une connexion sortante • both(2) : place une connexion sortante et attend une connexion entrante
rcSerialRawSocketGroup	rcRawSockFlowControl	**Accès :** lecture et écriture **Syntaxe :** RcFlowControl **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.5.1 **Définition :** type de FlowControl à utiliser sur ce port.
rcSerialRawSocketGroup	rcRawSockIpAdd	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.11.1 **Définition :** définit l'adresse IP comme suit : • Pour les connexions TCP sortantes (client), 'rcRawSockCallDir' défini sur 'out(2)' est l'adresse IP distante avec laquelle communiquer. • Pour les connexions TCP entrantes (serveur), 'rcRawSockCallDir' est défini sur 'out(2)' ou 'both(3)', il s'agit de l'adresse IP de l'interface locale à écouter pour le port local pour une demande de connexion. • Si les connexions sortantes et entrantes sont activées (client ou serveur), 'rcRawSockCallDir' est défini sur 'both(3)', il s'agit de l'adresse IP distante à utiliser pour placer une demande de connexion TCP sortante ou de laquelle accepter des appels. • Pour le transport UDP, adresse de l'interface à écouter pour les datagrammes UDP.
rcSerialRawSocketGroup	rcRawSockLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.12.1 **Définition :** active la collecte de statistiques de liaisons pour RawSocket sur ce port.
rcSerialRawSocketGroup	rcRawSockLocPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.9.1

Groupe(s)	Objet	Description
		Définition : port IP local à écouter pour une connexion TCP entrante ou des datagrammes UDP.
rcSerialRawSocketGroup	rcRawSockMaxConn	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.8.1 **Définition :** nombre maximum de connexions TCP entrantes autorisées.
rcSerialMbClientGroup	rcRawSockPackChar	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.2.1 **Définition :** caractère pouvant être utilisé pour forcer la transmission de données accumulées au réseau. Si aucun caractère de mise en paquet n'est configuré, l'objet est défini sur la valeur '256' et les données accumulées sont transmises sur la base du paramètre de délai de mise en paquet qui est la valeur définie pour l'objet *rcRawSockPackTimer*.
rcSerialRawSocketGroup	rcRawSockPackSize	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.4.1 **Définition :** nombre maximum d'octets reçus du port série à transmettre.
rcSerialRawSocketGroup	rcRawSockPackTimer	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.3.1 **Définition :** délai en ms entre le dernier caractère reçu et la transmission des données.
rcSerialRawSocketGroup	rcRawSockRemPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.10.1 **Définition :** port IP distant à utiliser lors du placement d'une connexion sortante.
rcSerialRawSocketGroup	rcRawSockTransport	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.4.1.1.6.1 **Définition :** protocole de transport utilisé pour le trafic IP pour les protocoles sur ce port.
rcSerialCommandsGroup	rcSerDeviceCmndClearStats	**Accès :** lecture et écriture **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.6.16.2.0 **Définition :** liste des ports pour lesquels la commande Clearing Statistics doit être exécutée sur des appareils série RUGGEDCOM. Une tentative de lecture pour cet objet renvoie toujours une liste de ports vide.
rcSerialCommandsGroup	rcSerDeviceCmndResetPort	**Accès :** lecture et écriture **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.6.16.1.0

Groupe(s)	Objet	Description
		Définition : liste des ports pour lesquels la réinitialisation doit être exécutée sur des appareils série RUGGEDCOM. Une tentative de lecture pour cet objet renvoie toujours une liste de ports vide.
rcSerialPortParamsGroup	rcSerialDscp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.9.1 **Définition :** valeur de l'octet DS à définir dans l'en-tête IP. La définition de l'octet DS est prise en charge dans la direction de sortie uniquement.
rcSerialPortParamsGroup	rcSerialForceHD	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.5.1 **Définition :** permet de forcer le mode de fonctionnement semi-duplex sur le port série. Pendant l'envoi de données depuis le port série, toutes les données reçues sont ignorées. Ce mode de fonctionnement est uniquement disponible sur des ports fonctionnant en mode duplex intégral.
rcSerialPortParamsGroup	rcSerialHoldTime	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.8.1 **Définition :** temps maximum (en millisecondes) pendant lequel un paquet série peut être mis en attente dans la file d'attente avant d'être envoyé à la ligne série. Le temps est mesuré à partir du moment où le paquet est reçu de la couche IP.
rcSerialPortParamsGroup	rcSerialPortIfIndex	**Accès :** lecture et écriture **Syntaxe :** InerfaceIndex **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.2.1 **Définition :** valeur d'ifIndex pour ce port. Cette valeur est identique à 'rs232PortIndex' qui est l'index utilisé pour 'rs232PortTable' dans RS-232-MIB.
rcSerialPortParamsGroup	rcSerialPortType	**Accès :** lecture et écriture **Syntaxe :** RcSerPortType **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.4.1 **Définition :** type de port série pris en charge sur le port série représenté par cette entrée.
rcSerialPortParamsGroup	rcSerialPostTxDelay	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.7.1 **Définition :** nombre de bits nécessaires pour générer le délai requis avec la vitesse de transmission configurée ('rs232PortOutSpeed') après l'envoi du dernier bit du paquet avant que l'UART série commence à écouter la ligne RX. La valeur n'est pertinente que pour l'interface RS485 avec 'rs232PortType' égal à other(1).
rcSerialPortParamsGroup	rcSerialProtocol	**Accès :** lecture et écriture **Syntaxe :** RcSerProtocol

Groupe(s)	Objet	Description
		OID : 1.3.6.1.4.1.15004.4.6.1.1.1.3.1 **Définition :** protocole série pris en charge sur le port série représenté par cette entrée.
rcSerialPortParamsGroup	rcSerialRxtoTxDelay	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.10.1 **Définition :** temps minimum (en millisecondes) pour le délai de transmission d'un nouveau message après la réception du dernier message via le port AI. Ce paramètre est utile, particulièrement pour le mode de transmission semi-duplex, notamment le protocole série RS485 2 fils. Il garantit que l'appareil connecté a suffisamment de temps pour désactiver son émetteur et activer son récepteur, afin qu'il puisse recevoir le message suivant sans perdre un seul bit.
rcSerialPortParamsGroup	rcSerialTurnAround	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.1.1.1.6.1 **Définition :** délai entre la transmission de messages individuels depuis le port série. Pour la valeur modbusServer(3) de l'objet 'rcSerialProtocol', la valeur doit être différente de zéro. Elle représente le délai entre l'envoi d'un message de diffusion et l'interrogation suivante du port série. Les RTU ne répondant pas à une transmission, un délai suffisant doit être assuré pour leur traitement.
rcSerialTelnetComportGroup	rcTelnetComportCallDir	**Accès :** lecture et écriture **Syntaxe :** RcCallDir **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.6.1 **Définition :** définit les éléments suivants : **Remarque** Ce paramètre est applicable uniquement au transport TCP. • in(0) : accepte une connexion entrante. • out(1) : place une connexion sortante • both(2) : place une connexion sortante et attend une connexion entrante
rcSerialTelnetComportGroup	rcTelnetComportFlowControl	**Accès :** lecture et écriture **Syntaxe :** RcFlowControl **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.5.1 **Définition :** type de FlowControl à utiliser sur ce port.
rcSerialTelnetComportGroup	rcTelnetComportIpAdd	**Accès :** lecture et écriture **Syntaxe :** IpAddress **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.9.1 **Définition :** définit l'adresse IP comme suit : • Pour les connexions TCP sortantes (client), 'rcRawSockCallDir' défini sur 'out(2)' est l'adresse IP distante avec laquelle communiquer. • Pour les connexions TCP entrantes (serveur), 'rcRawSockCallDir' est défini sur 'out(2)' ou 'both(3)', il

Groupe(s)	Objet	Description
		s'agit de l'adresse IP de l'interface locale à écouter pour le port local pour une demande de connexion. • Si les connexions sortantes et entrantes sont activées (client ou serveur), 'rcRawSockCallDir' est défini sur 'both(3)', il s'agit de l'adresse IP distante à utiliser pour placer une demande de connexion TCP sortante ou de laquelle accepter des appels.
rcSerialTelnetComportGroup	rcTelnetComportLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.10.1 **Définition :** définit l'adresse IP comme suit : • Pour les connexions TCP sortantes (client), 'rcRawSockCallDir' défini sur 'out(2)' est l'adresse IP distante avec laquelle communiquer. • Pour les connexions TCP entrantes (serveur), 'rcRawSockCallDir' est défini sur 'out(2)' ou 'both(3)', il s'agit de l'adresse IP de l'interface locale à écouter pour le port local pour une demande de connexion. • Si les connexions sortantes et entrantes sont activées (client ou serveur), 'rcRawSockCallDir' est défini sur 'both(3)', il s'agit de l'adresse IP distante à utiliser pour placer une demande de connexion TCP sortante ou de laquelle accepter des appels.
rcSerialTelnetComportGroup	rcTelnetComportLocPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.7.1 **Définition :** port IP local à écouter pour une connexion TCP entrante.
rcSerialTelnetComportGroup	rcTelnetComportPackChar	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.2.1 **Définition :** caractère pouvant être utilisé pour forcer la transmission de données accumulées au réseau. Si aucun caractère de mise en paquet n'est configuré, l'objet est défini sur la valeur '256' et les données accumulées sont transmises sur la base du paramètre de délai de mise en paquet qui est la valeur définie pour l'objet *rcTelnetComportPackTimer*.
rcSerialTelnetComportGroup	rcTelnetComportPackSize	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.4.1 **Définition :** nombre maximum d'octets reçus du port série à mettre dans un paquet IP.
rcSerialTelnetComportGroup	rcTelnetComportPackTimer	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.3.1 **Définition :** délai entre le dernier caractère reçu et la transmission des données.
rcSerialTelnetComportGroup	rcTelnetComportRemPort	**Accès :** lecture et écriture

Groupe(s)	Objet	Description
		Syntaxe : Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.11.1.1.8.1 **Définition :** port TCP distant à utiliser lors du placement d'une connexion sortante.
rcTimeConfigBaseGroup	rcTimeAndDate	**Accès :** lecture et écriture **Syntaxe :** DateandTime **OID :** 1.3.6.1.4.1.15004.4.11.1.2.0 **Définition :** ce paramètre permet l'affichage et le réglage de la date et de l'heure locales au format *DateAndTime*. DateAndTime est une convention textuelle standard définie dans SNMPv2-TC.

RUGGEDCOM-SFP-DDM-MIB

Groupe(s)	Objet	Description
rcSfpDdmCfgGroup	rcSfpDdmPollingInterval	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.1.1 **Définition :** intervalle de temps d'attente en minutes entre deux lectures consécutives d'émetteurs-récepteurs SFP/SFP+ installés. Lorsque cet intervalle est défini sur 0, la fonctionnalité SFP DDM est désactivée sur le système.
rcSfpDdmTableGroup	rcSfpDdmPortTable	**Accès :** non accessible **Syntaxe :** SÉQUENCE DE RcSfpDdmPortEntry **OID :** 1.3.6.1.4.1.15004.4.17.2.1 **Définition :** liste d'entrées de port SFP DDM.
rcSfpDdmTableGroup	rcSfpDdmPortEntry	**Accès :** non accessible **Syntaxe :** RcSfpDdmPortEntry **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1 **Définition :** paramètres SFP DDM pour un port SFP.
rcSfpDdmTableGroup	rcSfpPortId	**Accès :** non accessible **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.1 **Définition :** identificateur de port SFP pour lequel cette entrée contient des informations. La valeur est limitée par le nombre de ports SFP sur l'appareil.
rcSfpDdmTableGroup	rcSfpPlugged	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.2 **Définition :** l'émetteur-récepteur SFP est branché ou non. Il est branché avec true(1) et il est débranché avec false(2).

Groupe(s)	Objet	Description
rcSfpDdmTableGroup	rcSfpDdmVendorName	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.3 **Définition :** nom du fournisseur de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmVendorPartNumber	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.4 **Définition :** n° d'article du fournisseur de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmVendorRevision	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.5 **Définition :** révision du fournisseur de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmVendorSerialNumber	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.6 **Définition :** numéro de série du fournisseur de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmEncoding	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.7 **Définition :** mécanisme de codage de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmNominalBitrate	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.8 **Définition :** débit binaire nominal de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmConnectorType	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.9 **Définition :** type de connecteur de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmWavelength	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.10 **Définition :** longueur d'onde laser de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmLinkLength	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.11

Groupe(s)	Objet	Description
		Définition : longueur de liaison de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmImplemented	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.12 **Définition :** SFP DDM est mis en œuvre ou non sur l'émetteur-récepteur SFP. Il est mis en œuvre avec true(1), il n'est pas mis en œuvre avec false(2).
rcSfpDdmTableGroup	rcSfpDdmCurrentStatus	**Accès :** lecture seule **Syntaxe :** RcSfpDdmAlarmWarnStatus **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.12 **Définition :** alarme actuelle et état d'avertissement de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmCurrentTemperature	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.14 **Définition :** température actuelle (en unités de 0,001 degrés Celsius) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTempAlarmLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.15 **Définition :** seuil d'alarme de température basse (en unités de 0,001 degrés Celsius) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTempWarnLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.16 **Définition :** seuil d'avertissement de température basse (en unités de 0,001 degrés Celsius) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTempWarnHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.17 **Définition :** seuil d'avertissement de température élevée (en unités de 0,001 degrés Celsius) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTempAlarmHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.18 **Définition :** seuil d'alarme de température élevée (en unités de 0,001 degrés Celsius) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmCurrentVoltage	**Accès :** lecture seule **Syntaxe :** Integer32

Groupe(s)	Objet	Description
		OID : 1.3.6.1.4.1.15004.4.17.2.1.1.19 **Définition :** tension actuelle (en millivolts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageAlarmLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.20 **Définition :** seuil d'alarme de tension basse (en millivolts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageWarnLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.21 **Définition :** seuil d'avertissement de tension basse (en millivolts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageWarnHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.22 **Définition :** seuil d'avertissement de tension élevée (en millivolts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageAlarmHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.23 **Définition :** seuil d'alarme de tension élevée (en millivolts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmCurrentTxBiasCurrent	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.24 **Définition :** courant de polarisation Tx actuel (en microampères) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasAlarmLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.25 **Définition :** seuil d'alarme de courant de polarisation Tx faible (en microampères) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasWarnLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.26 **Définition :** seuil d'avertissement de courant de polarisation Tx faible (en microampères) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasWarnHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.27

Groupe(s)	Objet	Description
		Définition : seuil d'avertissement de courant de polarisation Tx élevé (en microampères) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasAlarmHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.28 **Définition :** seuil d'alarme de courant de polarisation Tx élevé (en microampères) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmCurrentRxPower	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.29 **Définition :** puissance Rx actuelle (en nanowatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerAlarmLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.30 **Définition :** seuil d'alarme de puissance Rx faible (en nanowatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerWarnLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.31 **Définition :** seuil d'avertissement de puissance Rx faible (en nanowatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerWarnHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.32 **Définition :** seuil d'avertissement de puissance Rx élevée (en nanowatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerAlarmHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.33 **Définition :** seuil d'alarme de puissance Rx élevée (en nanowatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmCurrentTxPower	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.34 **Définition :** puissance Tx actuelle (en microwatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerAlarmLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.35

Groupe(s)	Objet	Description
		Définition : seuil d'alarme de puissance Tx faible (en microwatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerWarnLow	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.36 **Définition :** seuil d'avertissement de puissance Tx faible (en microwatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerWarnHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.37 **Définition :** seuil d'avertissement de puissance Tx élevée (en microwatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerAlarmHigh	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.38 **Définition :** seuil d'alarme de puissance Tx élevée (en microwatts) de l'émetteur-récepteur SFP.
rcSfpDdmTableGroup	rcSfpDdmWarningFlags	**Accès :** lecture seule **Syntaxe :** Bits • tempHighWarning(0) • tempLowWarning(1) • vccHighWarning(2) • vccLowWarning(3) • txbiasHighWarning(4) • txbiasLowWarning(5) • rxpowerHighWarning(6) • rxpowerLowWarning(7) • txpowerHighWarning(8) • txpowerLowWarning(9) **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.39 **Définition :** les indicateurs d'avertissement spécifient si l'un des paramètres surveillés dépasse ou non son seuil d'avertissement. La modification de la valeur de l'un de ces bits génère un trap d'avertissement.
rcSfpDdmTableGroup	rcSfpDdmAlarmFlags	**Accès :** lecture seule **Syntaxe :** Bits • tempHighAlarm(0) • tempLowAlarm(1) • vccHighAlarm(2) • vccLowAlarm(3) • txbiasHighAlarm(4) • txbiasLowAlarm(5) • rxpowerHighAlarm(6)

Groupe(s)	Objet	Description
		• rxpowerLowAlarm(7) • txpowerHighAlarm(8) • txpowerLowAlarm(9) **OID :** 1.3.6.1.4.1.15004.4.17.2.1.1.40 **Définition :** les indicateurs d'alarme indiquent si l'un des paramètres surveillés dépasse ou non son seuil d'alarme. La modification de la valeur de l'un de ces bits génère un trap d'alarme.

RUGGEDCOM-STP-MIB

Groupe(s)	Objet	Description
rcRstpBaseGroup	rcRstpDot1dRstpAlternatePorts	**Accès :** lecture seule **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.5.1.5.0 **Définition :** sous-ensemble de ports avec un rôle Alternate (alternatif).
rcRstpBaseGroup	rcRstpDot1dRstpBackupPorts	**Accès :** lecture seule **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.5.1.6.0 **Définition :** sous-ensemble de ports avec un rôle Backup (sauvegarde).
rcRstpBaseGroup	rcRstpDot1dStpBlockedPorts	**Accès :** lecture seule **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.5.1.3.0 **Définition :** sous-ensemble de ports avec un rôle Blocked (bloqué).
rcRstpBaseGroup	rcRstpDot1dStpBrokenPorts	**Accès :** lecture seule **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.5.1.4.0 **Définition :** sous-ensemble de ports dans *dot1dStpPortTable* qui sont dans un état 'broken' (la valeur de l'objet *dot1dStpPortState* est 'broken').
rcRstpBaseGroup	rcRstpDot1dStpForwardingPorts	**Accès :** lecture seule **Syntaxe :** PortList **OID :** 1.3.6.1.4.1.15004.4.5.1.2.0 **Définition :** sous-ensemble de ports dans *dot1dStpPortTable* qui sont dans un état 'forwarding' (la valeur de l'objet *dot1dStpPortState* est 'forwarding').
rcRstpBaseStpTxHoldCountGroup	rcRstpDot1dStpTxHoldCount	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.5.1.1.0 **Définition :** valeur utilisée par la machine d'état Port Transmit pour limiter la vitesse

Groupe(s)	Objet	Description
		de transmission maximum. Une valeur plus élevée permet au réseau de récupérer plus rapidement en cas de liaisons défaillantes/ ponts défaillants. La valeur '0' signifie une vitesse de transmission illimitée. Si la valeur de l'objet *dot1dStpTxHoldCount* est 3..10, cet objet doit correspondre à la valeur de l'objet *dot1dStpTxHoldCount* (RSTP-MIB). Si la valeur de l'objet *dot1dStpTxHoldCount* est 10, la valeur de cet objet représente la limite réelle de vitesse de transmission configurée.

RUGGEDCOM-SYS-INFO-MIB

Groupe(s)	Objet	Description
rcSysDeviceCommGroup	rcDeviceCommClearAlarms	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.4.3.0 **Définition :** la définition de la valeur de cet objet sur 'true(1)' entraîne l'effacement de toutes les alarmes par l'appareil. Suite à une demande de lecture, l'agent renvoie la valeur 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommClearLogs	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.4.5.0 **Définition :** la définition de la valeur de cet objet sur 'true(1)' entraîne l'effacement des fichiers syslog.txt et crashlog.txt par l'appareil. Suite à une demande de lecture, l'agent renvoie la valeur 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommClearSyslog	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.4.4.0 **Définition :** la définition de la valeur de cet objet sur 'true(1)' entraîne l'effacement du fichier syslog.txt par l'appareil. Suite à une demande de lecture, l'agent renvoie la valeur 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommLoadDefaultCfg	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.4.2.0 **Définition :** la définition de la valeur de cet objet sur 'true(1)' force l'appareil à charger la configuration par défaut dans tous les tableaux. Suite à une demande de lecture, l'agent renvoie la valeur 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommReset	**Accès :** lecture et écriture **Syntaxe :** TruthValue

Groupe(s)	Objet	Description
		OID : 1.3.6.1.4.1.15004.4.2.4.1.0 **Définition :** la définition de la valeur de cet objet sur 'true(1)' entraîne le redémarrage de l'appareil. Suite à une demande de lecture, l'agent renvoie la valeur 'false(2)'.
rcSysErrObjectsGroup	rcDeviceErrBootPTftpTrFailed	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.9.0 **Définition :** indique si le fichier a été transféré correctement après avoir obtenu une adresse IP du serveur BootP. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification genericTrap.
rcSysErrObjectsGroup	rcDeviceErrBootupError	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.2.1.1.0 **Définition :** erreur découverte lors du processus de démarrage. S'il n'y a pas eu d'erreur lors du démarrage de l'appareil, DisplayString de longueur nulle sera récupéré.
rcSysErrObjectsGroup	rcDeviceErrConfigurationFailure	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.3.0 **Définition :** indique si des erreurs ont été détectées lors de l'application des réglages de configuration à partir du fichier de configuration. La configuration est mise à jour à partir du fichier de configuration au moment du démarrage lorsqu'un fichier est chargé à partir de la mémoire non volatile ou lorsqu'un nouveau fichier est téléchargé sur l'appareil. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification genericTrap.
rcSysErrObjectsGroup	rcDeviceErrCrashLogCreated	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.4.0 **Définition :** indique si l'erreur d'appareil qui a provoqué la création d'une entrée dans le fichier crashlog.txt a été détectée. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification genericTrap.
rcSysErrObjectsGroup	rcDeviceErrDateAndTimeSetFailed	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.7.0 **Définition :** indique si le réglage de la date et de l'heure dans l'appareil a échoué. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification genericTrap.

Groupe(s)	Objet	Description
rcSysErrObjectsGroup	rcDeviceErrHeapError	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.6.0 **Définition :** indique si la corruption de la mémoire système a été détectée. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification genericTrap.
rcSysErrObjectsGroup	rcDeviceErrNtpServerUnreachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.8.0 **Définition :** indique si l'un des serveurs NTP (si nécessaire) est accessible. La valeur de cet objet est 'false' si les deux serveurs deviennent inaccessibles. Chaque fois que la valeur de cet objet change, l'appareil génère la notification *ntpServiceAvailableChange*.
rcSysErrObjectsGroup	rcDeviceErrRadiusServerUnreachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.10.0 **Définition :** indique si le serveur RADIUS (si nécessaire) est accessible. Chaque fois que la valeur de cet objet change, l'appareil génère la notification *radiusServiceAvailableChange*.
rcSysErrObjectsGroup	rcDeviceErrStackOverflow	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.5.0 **Définition :** indique si la pile de l'une des tâches système est utilisée au-delà du seuil système. Chaque fois que la valeur de cet objet passe de false(2) à true(1), l'appareil génère une notification *genericTrap*.
rcSysErrObjectsGroup	rcDeviceErrTacacsServerUnreachable	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.11.0 **Définition :** indique si le serveur TACACS+ (si nécessaire) est accessible. Chaque fois que la valeur de cet objet change, l'appareil génère la notification *tacacsServiceAvailableChange*.
rcSysErrObjectsGroup	rcDeviceErrWatchdogReset	**Accès :** lecture seule **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.2.1.2.0 **Définition :** indique si le dernier redémarrage de l'appareil a été causé par le chien de garde (watchdog).
rcSysInfoDeviceInfoGroup	rcDeviceInfoBootSwVersion	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.2.3.2.0

Groupe(s)	Objet	Description
		Définition : version et date de version du logiciel chargeur de démarrage.
rcSysInfoDeviceInfoGroup	rcDeviceInfoCfgRevision	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.2.3.8.0 **Définition :** révision du fichier de configuration. Le numéro de révision est mis à jour chaque fois qu'un fichier est enregistré dans la mémoire flash. Ce numéro est enregistré dans config.csv au moment où le fichier est chargé depuis l'appareil. Chaque fois que la valeur de cet objet change, l'appareil génère une notification *cfgChangeTrap*.
rcSysInfoDeviceInfoGroup	rcDeviceInfoMainBoardType	**Accès :** lecture seule **Syntaxe :** RcMainBoard **OID :** 1.3.6.1.4.1.15004.4.2.3.4.0 **Définition :** code d'identification de la carte mère de l'appareil.
rcSysInfoDeviceInfoGroup	rcDeviceInfoMainSwVersion	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.2.3.3.0 **Définition :** version et date de version du logiciel du système d'exploitation principal.
rcSysInfoDeviceInfoGroup	rcDeviceInfoPendingBootSwVersion	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.2.3.6.0 **Définition :** version et date de version du logiciel chargeur de démarrage qui a été chargé sur l'appareil et qui est en attente de redémarrage. Chaque fois que la valeur de cet objet passe de DisplayString de longueur nulle à un DisplayString de longueur non nulle quelconque, l'appareil génère une notification *swUpgradeTrap*.
rcSysInfoDeviceInfoGroup	rcDeviceInfoPendingMainSwVersion	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.2.3.7.0 **Définition :** version et date de version du logiciel du système d'exploitation principal qui a été chargé sur l'appareil et qui est en attente de redémarrage. Chaque fois que la valeur de cet objet passe de DisplayString de longueur nulle à un DisplayString de longueur non nulle quelconque, l'appareil génère une notification *swUpgradeTrap*.
rcSysInfoDeviceInfoGroup	rcDeviceInfoSerialNumber	**Accès :** lecture seule **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.2.3.1.0

Groupe(s)	Objet	Description
		Définition : numéro de série de fabrication de l'appareil.
rcSysInfoDeviceInfoGroup	rcDeviceInfoTotalRam	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.2.3.5.0 **Définition :** nombre d'octets total de la mémoire RAM dans la CPU de contrôle du système.
rcSysStsPowerSupplyGroup	rcDeviceStsPowerSupply1	**Accès :** lecture seule **Syntaxe :** RcHardwareStatus **OID :** 1.3.6.1.4.1.15004.4.2.2.4.0 **Définition :** indique l'état du module d'alimentation 1. Chaque fois que la valeur de cet objet passe de functional(2) à notFunctional(3), ou de notFunctional(3) à functional(2), l'appareil génère une notification *powerSupplyTrap*.
rcSysStsPowerSupplyGroup	rcDeviceStsPowerSupply2	**Accès :** lecture seule **Syntaxe :** RcHardwareStatus **OID :** 1.3.6.1.4.1.15004.4.2.2.5.0 **Définition :** indique l'état du module d'alimentation 2. Chaque fois que la valeur de cet objet passe de functional(2) à notFunctional(3), ou de notFunctional(3) à functional(2), l'appareil génère une notification *powerSupplyTrap*.
rcSysStsObjectsTemperatureGroup	rcDeviceStsTemperature	**Accès :** lecture seule **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.2.2.3.0 **Définition :** température mesurée dans l'appareil.

RUGGEDCOM-TIMECONFIG-MIB

Groupe(s)	Objet	Description
rcTimeConfigBaseGroup	rcCurrentUTCOfst	**Accès :** lecture et écriture **Syntaxe :** Unsigned32 **OID :** 1.3.6.1.4.1.15004.4.11.1.4.0 **Définition :** permet à l'utilisateur d'ajuster la différence entre UTC et TAI.
rcTimeConfigBaseGroup	rcDSTOfst	**Accès :** lecture et écriture **Syntaxe :** Unsigned32 **OID :** 1.3.6.1.4.1.15004.4.11.1.3.0 **Définition :** ce paramètre spécifie la durée à avancer/reculer lorsque l'heure DTS (heure d'été/hiver) démarre ou s'arrête. Par exemple, sur la plupart du territoire des USA et du Canada, le décalage de l'heure DST (heure d'été/hiver) est d'1

Groupe(s)	Objet	Description
		heure (01:00:00) vers l'avant lorsque l'heure DST commence et d'1 heure vers l'arrière lorsque l'heure DST se termine.
rcTimeConfigBaseGroup	rcDSTRule	**Accès :** lecture et écriture **Syntaxe :** DisplayString **OID :** 1.3.6.1.4.1.15004.4.11.1.6.0 **Définition :** 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). Format : mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS • 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 L'heure DST commence le 2ème dimanche de mars à 2h00 du matin. L'heure DST se termine le 1er dimanche de novembre à 2h00 du matin.
rcTimeConfigBaseGroup	rcLeapSecPending	**Accès :** lecture et écriture **Syntaxe :** TruthValue **OID :** 1.3.6.1.4.1.15004.4.11.1.5.0 **Définition :** ce paramètre permet à l'utilisateur de gérer l'événement Seconde intercalaire. Une seconde intercalaire est une seconde ajoutée au Coordinated Universal Time (UTC).
rcTimeConfigBaseGroup	rcTimeSource	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.11.1.1.0 **Définition :** source de temps pilotant l'horloge locale.
rcSerialTinAndWinGroup	rcTinAndWinAddrAgingTime	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.6.7.0 **Définition :** le temps d'inactivité de communication en millisecondes après lequel une adresse TIN apprise est supprimée du tableau d'adresses d'appareil dynamique. Les entrées dans le tableau Link Statistics (statistiques de liaison) avec l'adresse vieillie sont conservées jusqu'à ce que les statistiques soient effacées.
rcSerialTinAndWinGroup	rcTinAndWinBroadCastAddr	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.6.6.8.0

Groupe(s)	Objet	Description
		Définition : tableau d'adresses d'appareil dans lequel les adresses sont trouvées pour les messages de diffusion.
rcSerialTinAndWinGroup	rcTinAndWinLinkStats	**Accès :** lecture et écriture **Syntaxe :** EnabledStatus **OID :** 1.3.6.1.4.1.15004.4.6.6.10.0 **Définition :** active la collecte de statistiques de liaisons pour les protocoles TIN et WIN.
rcSerialTinAndWinGroup	rcTinAndWinMsgAgingTime	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.6.6.0 **Définition :** temps de vieillissement pour les messages TIN mode2. La fonctionnalité est désactivée si la valeur de cet objet est '0'. Lorsque la fonctionnalité est activée, tout message TIN mode2 reçu est stocké dans un tableau interne. Si le même message est reçu pendant l'intervalle de temps spécifié par ce paramètre, le nouveau message est considéré comme un doublon et donc rejeté.
rcSerialTinAndWinGroup	rcTinAndWinTinDscp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.6.12.0 **Définition :** valeur de l'octet DS à définir dans l'en-tête IP. La définition de l'octet DS est prise en charge dans la direction de sortie uniquement.
rcSerialTinAndWinGroup	rcTinAndWinTinIpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.6.4.0 **Définition :** numéro de port local sur lequel le protocole TIN écoute des connexions ou des datagrammes UDP.
rcSerialTinAndWinGroup	rcTinAndWinTinMode	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.6.6.1.0 **Définition :** mode de fonctionnement Protocole TIN.
rcSerialTinAndWinGroup	rcTinAndWinTinTrans	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.6.2.0 **Définition :** protocole de transport utilisé pour le trafic IP pour le protocole TIN.
rcSerialTinAndWinGroup	rcTinAndWinUniAddr	**Accès :** lecture et écriture **Syntaxe :** Integer **OID :** 1.3.6.1.4.1.15004.4.6.6.9.0 **Définition :** tableau d'adresses d'appareil dans lequel les adresses sont trouvées pour les messages de monodiffusion.
rcSerialTinAndWinGroup	rcTinAndWinWinDscp	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.6.11.0

Groupe(s)	Objet	Description
		Définition : valeur de l'octet DS à définir dans l'en-tête IP. La définition de l'octet DS est prise en charge dans la direction de sortie uniquement.
rcSerialTinAndWinGroup	rcTinAndWinWinIpPort	**Accès :** lecture et écriture **Syntaxe :** Integer32 **OID :** 1.3.6.1.4.1.15004.4.6.6.5.0 **Définition :** numéro de port local sur lequel le protocole WIN écoute des connexions ou des datagrammes UDP.
rcSerialTinAndWinGroup	rcTinAndWinWinTrans	**Accès :** lecture et écriture **Syntaxe :** RcTransport **OID :** 1.3.6.1.4.1.15004.4.6.6.3.0 **Définition :** protocole de transport utilisé pour le trafic IP pour le protocole WIN.

15.3 Fonctionnalités d'agent prises en charge

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

⚠ NOTA

Cette section répertorie toutes les MIB prises en charge par RUGGEDCOM ROS, et est destinée uniquement à des fins de référence. La prise en charge de chaque appareil peut varier.

Remarque

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

Nom de fichier	Fonctionnalité de l'agent	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

Nom de fichier	Fonctionnalité de l'agent	MIB prise en charge
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-GPS-MIB-AC.mib	RC-GPS-MIB-AC	GPS-MIB
RC-IRIGB-MIB-AC.mib	RC-IRIGB-MIB-AC	IRIGB-MIB
RC-NTP-MIB-AC.mib	RC-NTP-MIB-AC	NTP-MIB
RC-PTP1588-MIB-AC.mib	RC-PTP1588-MIB-AC	PTP1588-MIB
RC-TIMECONFIG-MIB-AC.mib	RC-TIMECONFIG-MIB-AC	TIMECONFIG-MIB
RC-SNMP-FRAMEWORK-MIB-AC.MIB	RC-SNMP-FRAMEWORK-MIB-AC	SNMP-FRAMEWORK-MIB.MIB
RC-RUGGEDCOM-AAA-SERVER-MIB-AC.MIB	RC-RUGGEDCOM-AAA-SERVER-MIB-AC	RUGGEDCOM-AAA-SERVER-MIB.MIB
RC-RUGGEDCOM-SFP-DDM-MIB-AC.mib	RC-RUGGEDCOM-SFP-DDM-MIB-AC	RUGGEDCOM-SFP-DDM-MIB

15.4 Traps SNMP

L'appareil génère les traps suivants :

Traps standard

Variable	Description
coldStart	**Groupe d'objets :** snmpBasicNotificationsGroup **MIB :** SNMPv2-MIB **Accès :** lecture seule **OID :** 1.3.6.1.6.3.1.1.5.1.0 **Standard :** RFC-1907 **Définition :** un trap coldStart signifie que l'entité SNMPv2 jouant le rôle d'agent se réinitialise et que sa configuration a peut-être été modifiée.
linkDown	**Groupe d'objets :** linkUpDownNotificationsGroup **MIB :** IF-MIB **Accès :** lecture seule **Syntaxe :** Counter32 **OID :** .1.3.6.1.6.3.1.1.5.3 **Standard :** RFC-2863 **Définition :** un trap linkDown signifie que l'entité SNMP jouant le rôle d'agent a détecté que l'objet ifOperStatus pour l'une de ses liaisons de communication est sur le point de passer à l'état down à partir d'un autre état (mais pas à partir de l'état notPresent). Cet autre état est indiqué par la valeur incluse d'ifOperStatus.

Variable	Description
linkUp	**Groupe d'objets :** linkUpDownNotificationsGroup **MIB :** IF-MIB **Capacité de l'agent :** RC-IF-MIB-AC **Accès :** lecture seule **OID :** .1.3.6.1.6.3.1.1.5.4 **Définition :** un trap linkUp signifie que l'entité SNMP jouant le rôle d'agent a détecté que l'objet ifOperStatus pour l'une de ses liaisons de communication a quitté l'état down et est passé à un autre état (mais pas à l'état notPresent). Cet autre état est indiqué par la valeur incluse d'ifOperStatus.
lldpRemTablesChange	**Groupe d'objets :** lldpNotificationsGroup **MIB :** LLDP-MIB **Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture seule **Syntaxe :** STRING **OID :** 1.0.8802.1.1.2.0.0.1.0 **Standard :** ISO8802-LLDP-MIB **Définition :** une notification lldpRemTablesChange est envoyée lorsque la valeur de lldpStatsRemTableLastChangeTime change. Elle peut être utilisée par un NMS pour déclencher des interrogations de maintenance de tableaux de systèmes distants LLDP. Notez que la transmission des notifications lldpRemTablesChange est limitée par l'agent, comme spécifié par l'objet 'lldpNotificationInterval'.
lldpStatsRemTablesAgeouts	**Groupe d'objets :** lldpStatsRxGroup **MIB :** LLDP-MIB **Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.0.8802.1.1.2.1.2.5.0 **Standard :** ISO8802-LLDP-MIB **Définition :** nombre de fois que l'ensemble complet d'informations annoncées par un MSAP spécifique a été supprimé des tableaux contenus dans les objets lldpRemoteSystemsData et lldpExtensions parce que l'intervalle d'actualité des informations a expiré. Ce compteur ne doit être incrémenté qu'une seule fois lorsque l'ensemble complet d'informations est entièrement invalidé (a expiré) dans tous les tableaux associés. Le vieillissement partiel, à l'instar d'un cas de suppression, n'est pas autorisé et ne doit donc pas modifier la valeur de ce compteur.
lldpStatsRemTablesDeletes	**Groupe d'objets :** lldpStatsRxGroup **MIB :** LLDP-MIB **Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.0.8802.1.1.2.1.2.3.0

Variable	Description
	Standard : ISO8802-LLDP-MIB **Définition :** notez que la transmission des notifications lldpRemTablesChange est limitée par l'agent, comme spécifié par l'objet 'lldpNotificationInterval'.
lldpStatsRemTablesDrops	**Groupe d'objets :** lldpStatsRxGroup **MIB :** LLDP-MIB **Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.0.8802.1.1.2.1.2.4.0 **Standard :** nombre de fois que l'ensemble complet d'informations annoncées par un MSAP spécifique n'a pas pu être entré dans les tableaux contenus dans les objets lldpRemoteSystemsData et lldpExtensions en raison de ressources insuffisantes. **Définition :** ISO8802-LLDP-MIB
lldpStatsRemTablesInserts	**Groupe d'objets :** lldpStatsRxGroup **MIB :** LLDP-MIB **Capacité de l'agent :** RC-LLDP-MIB-AC **Accès :** lecture seule **Syntaxe :** Gauge32 **OID :** .1.0.8802.1.1.2.1.2.2.0 **Standard :** ISO8802-LLDP-MIB **Définition :** nombre de fois que l'ensemble complet d'informations annoncées par un MSAP spécifique a été inséré dans des tableaux contenus dans les objets lldpRemoteSystemsData et lldpExtensions. L'ensemble complet d'informations reçues d'un MSAP particulier doit être inséré dans des tableaux associés. Si des informations partielles ne peuvent pas être insérées pour une raison telle que le manque de ressources, l'ensemble complet d'informations doit être supprimé. Ce compteur ne doit être incrémenté qu'une seule fois après l'enregistrement de l'ensemble complet d'informations avec succès dans tous les tableaux associés. Toute défaillance lors de l'insertion d'un ensemble d'informations entraînant la suppression d'informations précédemment insérées ne doit déclencher aucune modification dans lldpStatsRemTablesInserts puisque l'insertion n'est pas encore terminée ou dans lldpStatsRemTablesDeletes, car la suppression ne serait qu'une suppression partielle. Si la défaillance était le résultat d'un manque de ressources, le compteur lldpStatsRemTablesDrops doit être incrémenté une fois.
RMON_alarmIndex	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.3.1.1.1.0 **OID :** 1.3.6.1.2.1.16.3.1.1.1.0 **Standard :** RFC-2819
RMON_alarmSampleType	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.3.1.1.4.0

Variable	Description
	OID : 1.3.6.1.2.1.16.3.1.1.4.0 **Standard :** RFC-2819
RMON_alarmThreshold	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.3.1.1.0.0 **OID :** 1.3.6.1.2.1.16.3.1.1.0.0 **Standard :** RFC-2819
RMON_alarmValue	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.3.1.1.5.0 **OID :** 1.3.6.1.2.1.16.3.1.1.5.0 **Standard :** RFC-2819
RMON_alarmVariable	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.3.1.1.3.0 **OID :** 1.3.6.1.2.1.16.3.1.1.3.0 **Standard :** RFC-2819
RMON_fallingAlarm	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.0.2.0 **OID :** 1.3.6.1.2.1.16.0.2.0 **Standard :** RFC-2819
RMON_risingAlarm	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.16.0.1.0 **OID :** 1.3.6.1.2.1.16.0.1.0 **Standard :** RFC-2819
RstpNewRoot	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.17.0.1.0 **OID :** 1.3.6.1.2.1.17.0.1.0 **Standard :** RFC-4188
RstpTopolgyChange	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.2.1.17.0.2.0 **OID :** 1.3.6.1.2.1.17.0.2.0 **Standard :** RFC-4188
SnmpAuthenticationFailure	**Accès :** lecture seule **Syntaxe :** 1.3.6.1.6.3.1.1.5.5.0 **OID :** 1.3.6.1.6.3.1.1.5.5.0 **Standard :** RFC-1907
snmpEnableAuthenTraps	**Groupe d'objets :** snmpGroup **MIB :** SNMPv2-MIB **Accès :** lecture et écriture **Syntaxe :** INTEGER **OID :** 1.3.6.1.2.1.11.30.0 **Définition :** indique si l'entité SNMP est autorisée à générer des traps authenticationFailure. La valeur de cet objet remplace toute information de configuration. En tant que tel, il fournit

Variable	Description
	un moyen par lequel tous les traps authenticationFailure peuvent être désactivés. Notez qu'il est fortement recommandé de stocker cet objet dans une mémoire non volatile afin qu'il reste constant à travers les réinitialisations du système de gestion de réseau.
warmStart	**Groupe d'objets :** ROS-Standard-Trap **MIB :** SNMPv2-MIB **Accès :** lecture seule **Syntaxe :** 1.3.6.1.6.3.1.1.5.2.0 **OID :** 1.3.6.1.6.3.1.1.5.2.0 **Définition :** un trap warmStart signifie que l'entité SNMPv2, jouant un rôle d'agent, se réinitialise de telle sorte que sa configuration n'est pas modifiée.

Traps propriétaires spécifiques

Variable	Description
bootVersionMismatchTrap	**Groupe d'objets :** ruggedcomSecurityGroup01 **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.5.14 **Définition :** trap d'indication de la version du logiciel de démarrage généré par des appareils RUGGEDCOM.
cfgChangeTrap	**Groupe d'objets :** ruggedcomNotificationsGroup **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.5.4 **Définition :** trap générique généré lors d'un changement de configuration. La fréquence à laquelle cette notification peut être fournie est de 60 secondes.
defaultKeysTrap	**Groupe d'objets :** ruggedcomSecurityGroup01 **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.5.13 **Définition :** trap d'indication d'utilisation des clés par défaut pour les services sécurisés (SSH et SSL) généré par des appareils RUGGEDCOM.
genericTrap	**Groupe d'objets :** ruggedcomNotificationsGroup **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.5.1 **Définition :** trap d'indication d'utilisation des clés par défaut pour les services sécurisés (SSH et SSL) généré par des appareils RUGGEDCOM.
genericTrapDescription	**Groupe d'objets :** ruggedcomGenericTrapGroup **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.4.1.1.1.2 **Définition :** description d'un trap générique.
genericTrapSeverity	**Groupe d'objets :** ruggedcomGenericTrapGroup **MIB :** RUGGEDCOM-TRAPS-MIB

Variable	Description
	OID : 1.3.6.1.4.1.15004.4.1.1.1.1 **Définition :** degré de gravité du trap générique.
powerSupplyDescription	**Groupe d'objets :** ruggedcomPowerSupplyGroup **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.4.1.1.2.1 **Définition :** description de l'alimentation qui tombe en panne.
powerSupplyTrap	**Groupe d'objets :** ruggedcomNotificationsGroup **MIB :** RUGGEDCOM-TRAPS-MIB **OID :** 1.3.6.1.4.1.15004.5.2 **Définition :** trap généré lorsqu'une alimentation tombe en panne ou est établie. Le premier trap serait généré lors de la première panne d'alimentation. L'état de l'alimentation (en panne ou rétablie) est récupéré via l'objet powerSupplyDescription au moment de la génération du trap. L'état des blocs d'alimentation dans l'appareil peut être récupéré via les objets rcDeviceStsPowerSupply1 et rcDeviceStsPowerSupply2. Il est recommandé d'ajouter l'objet powerSupplyIdentifier en tant que paramètre facultatif à la liste des objets.
rcSfpDdmAlarmTrap	**Groupe d'objets :** rcSfpDdmNotifyGroup **MIB :** RUGGEDCOM-SFP-DDM-MIB **OID :** 1.3.6.1.4.1.15004.5.52.2 **Définition :** un trap d'alarme SFP DDM indique qu'au moins l'un des indicateurs d'alarme est défini ou effacé sur l'émetteur-récepteur SFP.
rcSfpDdmWarningTrap	**Groupe d'objets :** rcSfpDdmNotifyGroup **MIB :** RUGGEDCOM-SFP-DDM-MIB **OID :** 1.3.6.1.4.1.15004.5.52.1 **Définition :** un trap d'avertissement SFP DDM indique qu'au moins l'un des indicateurs d'avertissement est défini ou effacé sur l'émetteur-récepteur SFP.
rcRstpNewTopology	**Groupes d'objets :** rcRstpNotifyGroup, rcDigitalInputsNotifyGroup **MIB :** RUGGEDCOM-STP-MIB **OID :** 1.3.6.1.4.1.15004.5.11.1 **Définition :** un trap rcRstpNewTopology est envoyé par un pont après l'apparition d'un trap de changement de topologie sur un ou plusieurs ports (des traps topologyChange sont envoyés) et la topologie devient stable. La topologie est stable lorsque le temporisateur tcWhile de tous les ports de ce pont est égal à zéro. Ce trap est désactivé si le trap topologyChange est désactivé par la configuration de l'appareil.
swUpgradeTrap	**Groupe d'objets :** ruggedcomNotificationsGroup **MIB :** RUGGEDCOM-SYS-INFO-MIB **OID :** 1.3.6.1.4.1.15004.5.3 **Définition :** trap générique généré lors de la mise à niveau logicielle. La fréquence à laquelle cette notification peut être fournie est de 60 secondes.

Variable	Description
weakPasswordTrap	**Groupe d'objets :** ruggedcomSecurityGroup01 **MIB :** RUGGEDCOM-SYS-INFO-MIB **OID :** 1.3.6.1.4.1.15004.5.8 **Définition :** trap d'indication de mot de passe faible généré par des appareils RUGGEDCOM.

Informations complémentaires

Siemens RUGGEDCOM
https://www.siemens.com/ruggedcom

Industry Online Support (service et assistance)
https://support.industry.siemens.com

Industry Mall
https://mall.industry.siemens.com

Siemens Canada Ltd.
Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

© 2022 Siemens Canada Ltd.
Modifications possibles