

## **Administration d'Oracle® Solaris : Interfaces réseau et virtualisation réseau**

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

#### U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

# Table des matières

---

<b>Préface</b> .....	15
<b>1 Présentation de la pile réseau</b> .....	21
Configuration réseau dans cette version d'Oracle Solaris .....	21
Pile réseau dans Oracle Solaris .....	22
Noms des périphériques réseau et des liaisons de données .....	26
Noms de lien génériques par défaut .....	26
Affectation de noms génériques aux liaisons de données .....	27
Personnalisation de l'affectation des noms de lien génériques .....	28
Noms de lien dans les systèmes mis à niveau .....	29
Administration d'autres types de liens .....	31
<b>Partie I Configuration automatique de réseau</b> .....	35
<b>2 Présentation de NWAM</b> .....	37
Définition d'une configuration NWAM .....	38
Composants fonctionnels NWAM .....	39
Cas d'utilisation de NWAM .....	40
Fonctionnement de la configuration NWAM .....	41
Comportement par défaut de NWAM .....	42
Fonctionnement de NWAM avec d'autres technologies de mise en réseau Oracle Solaris .....	43
Sources contenant les tâches de configuration réseau .....	44
<b>3 Configuration et administration NWAM (présentation)</b> .....	47
Présentation de la configuration NWAM .....	47
Définition des profils réseau .....	47
Description d'un NCP .....	48

Description d'une NCU .....	49
Description des NCP automatiques et définis par l'utilisateur .....	50
Description d'un profil d'emplacement .....	51
Description d'un ENM .....	52
A propos des WLAN connus .....	52
Données de configuration NWAM .....	53
Valeurs de propriété de NCU .....	55
Valeurs de propriété des emplacements définis par le système .....	56
Activation des profils NWAM .....	58
Stratégie d'activation NCP .....	59
Critères de sélection de l'activation d'emplacement .....	61
Configuration de profils à l'aide de la commande <code>netcfg</code> .....	63
Mode interactif <code>netcfg</code> .....	65
Mode de ligne de commande <code>netcfg</code> .....	65
Mode fichier de commande <code>netcfg</code> .....	66
Sous-commandes <code>netcfg</code> prises en charge .....	66
Administration des profils à l'aide de la commande <code>netadm</code> .....	69
Présentation des démons NWAM .....	71
Description du démon de moteur de stratégie NWAM ( <code>nwamd</code> ) .....	71
Description du démon de référentiel NWAM( <code>netcfgd</code> ) .....	72
Services réseau SMF et configuration NWAM .....	72
Activation et désactivation de la gestion de configuration NWAM .....	73
Présentation de la sécurité NWAM .....	74
Autorisations et profils liés à NWAM .....	74
Autorisations nécessaires pour utiliser les interfaces utilisateur NWAM .....	75
<b>4 Configuration de profil NWAM (tâches) .....</b>	<b>77</b>
Création de profils .....	78
Création de profils en mode de ligne de commande .....	78
Création interactive de profils .....	79
Création d'un NCP .....	80
Création de NCU pour un NCP .....	80
▼ Création d'un NCP en mode interactif .....	83
Création d'un profil d'emplacement .....	88
Création d'un profil ENM .....	93

Création de WLAN .....	96
Suppression de profils .....	98
Définition et modification des valeurs de propriétés pour un profil .....	100
Interrogation du système pour l'obtention d'informations du profil .....	102
Création de la liste de tous les profils d'un système .....	103
Création d'une liste de toutes les valeurs de propriétés pour un profil spécifique .....	104
Obtention de valeurs d'une propriété spécifique .....	105
Affichage interactif et modification des valeurs de propriété à l'aide de la sous-commande walkprop .....	107
Exportation et restauration d'une configuration de profil .....	108
Restauration d'un profil défini par l'utilisateur .....	111
Gestion de la configuration réseau par l'intermédiaire de SMF .....	112
▼ Procédure permettant de passer du mode de configuration réseau NWAM au mode de configuration réseau classique .....	112
▼ Procédure permettant de passer du mode de configuration réseau classique au mode de configuration réseau NWAM .....	113
<b>5 Administration des profils NWAM (tâches) .....</b>	<b>115</b>
Obtention d'informations sur les états de profils .....	116
Affichage de l'état actuel d'un profil .....	116
Valeurs d'état auxiliaire .....	118
Activation et désactivation des profils .....	118
Exécution d'une analyse sans fil et connexion aux réseaux sans fil disponibles .....	121
Dépannage de la configuration réseau NWAM .....	122
Surveillance de l'état en cours de toutes les connexions réseau .....	122
Correction des problèmes liés à la configuration de l'interface réseau .....	122
<b>6 A propos de l'interface graphique NWAM .....</b>	<b>125</b>
Présentation de l'interface graphique NWAM .....	125
Accès à l'interface graphique NWAM à partir du bureau .....	126
Différences entre l'interface de ligne de commande NWAM et l'interface graphique NWAM .....	127
Composants fonctionnels de l'interface graphique NWAM .....	128
Interaction avec NWAM à partir du bureau .....	130
Vérification de l'état de votre connexion réseau .....	130
Contrôle des connexions réseau à partir du bureau .....	132

Connexion et gestion des réseaux sans fil favoris .....	134
▼ Connexion à un réseau sans fil .....	135
Gestion des réseaux favoris .....	136
Gestion des profils réseau .....	136
A propos de la boîte de dialogue Préférences réseau .....	137
Visualisation des informations relatives aux profils réseau .....	139
Passage d'un profil réseau à un autre .....	139
Ajout ou suppression d'un profil réseau .....	140
Modification de profils réseau .....	140
Utilisation des groupes de priorité .....	141
Création et gestion des emplacements .....	143
Modification des emplacements .....	146
A propos des modificateurs réseau externes .....	146
A propos de la boîte de dialogue Modificateurs réseau .....	147
▼ Ajout d'un ENM de ligne de commande .....	148
 <b>Partie II Configuration de liaisons de données et d'interfaces .....</b>	<b>151</b>
 <b>7 Utilisation des commandes de configuration de l'interface et de liaison de données sur les profils .....</b>	<b>153</b>
Points principaux de la configuration réseau basée sur les profils .....	153
Profils et des outils de configuration .....	154
▼ Procédure de détermination du mode de gestion réseau .....	155
Etapas suivantes .....	156
 <b>8 Configuration et administration des liaisons de données .....</b>	<b>157</b>
Configuration des liaisons de données (tâches) .....	157
Commande dladm .....	158
▼ Renommage d'une liaison de données .....	160
▼ Affichage des informations relatives aux attributs physiques des liaisons de données .....	161
▼ Affichage des informations concernant les liaisons de données .....	162
▼ Suppression d'une liaison de données .....	163
Définition des propriétés de liaison de données .....	164
Présentation des propriétés des liaisons de données .....	164
Configuration des propriétés de liaisons de données à l'aide de la commande dladm .....	165

Tâches de configuration supplémentaires sur les liaisons de données .....	173
▼ Procédure de remplacement d'une NIC avec la reconfiguration dynamique .....	173
Configuration de modules STREAMS sur les liaisons de données .....	175
<b>9 Configuration d'une interface IP .....</b>	<b>179</b>
A propos de la configuration d'interface IP .....	179
Commande <code>ipadm</code> .....	179
Configuration d'interfaces IP (tâches) .....	181
▼ SPARC : Garantie de l'unicité de l'adresse MAC d'une interface .....	181
Configuration d'interfaces IP .....	183
▼ Configuration d'une interface IP .....	183
Définition des propriétés des adresses IP .....	187
Définition des propriétés d'interfaces IP .....	189
Administration de propriétés de protocole .....	193
Définition de propriétés TCP/IP .....	193
Contrôle d'interfaces et d'adresses IP .....	198
▼ Procédure d'obtention d'informations sur les interfaces réseau .....	198
Dépannage de la configuration de l'interface .....	202
La commande <code>ipadm</code> ne fonctionne pas. ....	202
L'adresse IP ne peut pas être affectée à la commande <code>ipadm create-addr</code> . ....	202
Le message <code>cannot create address object: Invalid argument provided</code> s'affiche pendant la configuration de l'adresse IP. ....	203
Message <code>cannot create address: Persistent operation on temporary object</code> lors de la configuration d'interface IP .....	203
Tableaux de comparaison : commande <code>ipadm</code> et autres commandes réseau .....	204
Options des commandes <code>ifconfig</code> et <code>ipadm</code> .....	204
Options des commandes <code>ndd</code> et <code>ipadm</code> .....	206
<b>10 Configuration des communications via une interface sans fil sur Oracle Solaris .....</b>	<b>209</b>
Liste des tâches des communications Wi-Fi .....	209
Communication par le biais d'interfaces Wi-Fi .....	210
Recherche de réseau Wi-Fi .....	210
Planification des communications Wi-Fi .....	211
Connexion et utilisation du Wi-Fi sur des systèmes Oracle Solaris .....	212
▼ Connexion à un réseau Wi-Fi .....	212

▼ Contrôle du lien Wi-Fi .....	216
Communications Wi-Fi sécurisées .....	218
▼ Configuration d'une connexion chiffrée à un réseau Wi-Fi .....	218
<b>11 Administration des ponts .....</b>	<b>221</b>
Présentation du pontage .....	221
Propriétés de liaison .....	225
Démon STP .....	226
Démon TRILL .....	227
Débogage des ponts .....	228
Autres comportements des ponts .....	228
Exemples de configuration de pont .....	231
Administration de ponts (liste des tâches) .....	231
▼ Affichage d'informations sur les ponts configurés .....	233
▼ Affichage des informations de configuration sur les liaisons de pont .....	235
▼ Création d'un pont .....	235
▼ Modification du type de protection pour un pont .....	236
▼ Ajout d'une ou de plusieurs liaisons à un pont existant .....	236
▼ Suppression des liaisons d'un pont .....	237
▼ Suppression d'un pont du système .....	238
<b>12 Administration de groupements de liens .....</b>	<b>239</b>
Présentation des groupements de liens .....	239
Notions de base sur les groupements de liens .....	240
Groupements de liens dos à dos .....	241
Stratégies et équilibrage de charge .....	242
Mode de groupement et commutateurs .....	243
Conditions requises pour la création de groupements de liens .....	243
Noms flexibles pour les groupements de liens .....	244
Administration des groupements de liens (liste des tâches) .....	244
▼ Procédure de création d'un groupement de liens .....	245
▼ Procédure de modification d'un groupement .....	247
▼ Procédure d'ajout d'un lien à un groupement .....	248
▼ Procédure de suppression d'un lien dans un groupement .....	249
▼ Procédure de suppression d'un groupement .....	249



<b>13</b>	<b>Administration des réseaux locaux virtuels</b>	251
	Administration de réseaux locaux virtuels	251
	Présentation de la topologie du VLAN	252
	Administration de VLAN (liste des tâches)	254
	Planification de plusieurs VLAN sur un réseau	255
	Configuration des VLAN	256
	VLAN sur les périphériques hérités	260
	Autres tâches d'administration sur les VLAN	261
	Association de tâches de configuration réseau et utilisation de noms personnalisés	263
<b>14</b>	<b>Présentation d'IPMP</b>	267
	Nouveautés d'IPMP	267
	Déploiement d'IPMP	268
	Avantages d'IPMP	268
	Quand utiliser IPMP	269
	Comparaison d'IPMP et du groupement de liens	270
	Utilisation de noms de liaison flexibles sur une configuration d'IPMP	271
	Fonctionnement d'IPMP	272
	Composants IPMP dans Oracle Solaris	278
	Types de configurations d'interface IPMP	279
	Adressage IPMP	280
	Adresses test IPv4	281
	Adresses test IPv6	281
	Détection de défaillance et de réparation dans IPMP	281
	Types de détection de défaillance dans IPMP	281
	Détection de réparation d'interface physique	284
	IPMP et reconfiguration dynamique	286
	Connexion de nouvelles cartes réseau	287
	Déconnexion de cartes d'interface réseau	287
	Remplacement de cartes réseau	287
	Terminologie et concepts IPMP	288
<b>15</b>	<b>Administration d'IPMP</b>	299
	Liste des tâches d'administration d'IPMP	299
	Création et configuration de groupe IPMP (liste des tâches)	300

Maintenance des groupes IPMP (liste des tâches) .....	300
Configuration de la détection de défaillance basée sur sonde (liste des tâches) .....	301
Contrôle des groupes IPMP (liste des tâches) .....	301
Configuration de groupes IPMP .....	302
▼ Procédure de planification pour un groupe IPMP .....	302
▼ Procédure de configuration d'un groupe IPMP à l'aide du protocole DHCP .....	304
▼ Procédure de configuration manuelle d'un groupe IPMP actif-actif .....	306
▼ Procédure de configuration manuelle d'un groupe IPMP actif-de réserve .....	308
Maintenance de groupes IPMP .....	310
▼ Procédure d'ajout d'une interface à un groupe IPMP .....	310
▼ Procédure de suppression d'une interface d'un groupe IPMP .....	310
▼ Procédure d'ajout ou de suppression d'adresses IP .....	311
▼ Procédure de déplacement d'une interface d'un groupe IPMP vers un autre .....	312
▼ Procédure de suppression d'un groupe IPMP .....	313
Configuration pour la détection de défaillance basée sur sonde .....	314
▼ Procédure de spécification manuelle de systèmes cible pour la détection de défaillance basée sur sonde .....	315
▼ Procédure de sélection de méthode de détection de défaillance à utiliser .....	315
▼ Procédure de configuration du comportement du démon IPMP .....	316
Restauration d'une configuration d'IPMP avec la reconfiguration dynamique .....	317
▼ Procédure de remplacement d'une carte physique qui a échoué .....	318
Contrôle des informations d'IPMP .....	319
▼ Procédures d'obtention d'informations sur le groupe IPMP .....	320
▼ Procédures d'obtention d'informations sur les adresses de données IPMP .....	321
▼ Procédure d'obtention d'informations sur les interfaces IP sous-jacentes d'un groupe ....	322
▼ Procédures d'obtention d'informations sur les cibles de sonde IPMP .....	323
▼ Procédure d'observation des sondes IPMP .....	325
▼ Procédure de personnalisation de la sortie de la commande <code>ipmpstat</code> dans un script .....	326
▼ Procédure de génération d'une sortie analysable par machine pour la commande <code>ipmpstat</code> .....	327
<b>16 Echange d'informations sur la connectivité réseau à l'aide du protocole LLDP .....</b>	<b>329</b>
Présentation du protocole LLDP dans Oracle Solaris .....	329
Composants d'une implémentation LLDP .....	329
Fonctionnalités de l'agent LLDP .....	331
Configuration du fonctionnement de l'agent LLDP .....	331

Configuration des informations à diffuser .....	332
Gestion des unités TLV .....	335
▼ Définition des valeurs TLV globales .....	336
Data Center Bridging .....	337
Contrôle des agents LLDP .....	339
▼ Affichage des diffusions .....	339
▼ Affichage des statistiques LLDP .....	340
<b>Partie III Virtualisation du réseau et gestion des ressources .....</b>	<b>343</b>
<b>17 Introduction à la virtualisation du réseau et au contrôle des ressources (présentation) .....</b>	<b>345</b>
Virtualisation du réseau et réseaux virtuels .....	345
Parties du réseau virtuel interne .....	346
Responsables de l'implémentation des réseaux virtuels .....	348
Définition du contrôle des ressources .....	349
Fonctionnement de la gestion de la bande passante et du contrôle de flux .....	349
Allocation du contrôle des ressources et de la gestion de la bande passante sur un réseau .....	350
Responsable de l'implémentation des fonctions de contrôle des ressources .....	352
Fonctions d'observabilité pour la virtualisation du réseau et le contrôle des ressources .....	352
<b>18 Planification de la virtualisation du réseau et du contrôle des ressources .....</b>	<b>355</b>
Liste des tâches de virtualisation du réseau et de contrôle des ressources .....	355
Planification et conception d'un réseau virtuel .....	356
Réseau virtuel basique sur un système unique .....	356
Réseau privé virtuel sur un système unique .....	358
Pour plus d'informations .....	360
Implémentation des contrôles sur les ressources réseau .....	360
Contrôle des ressources basé sur l'interface pour un réseau classique .....	362
Contrôle de flux pour le réseau virtuel .....	362
▼ Création d'une politique d'utilisation des applications sur un réseau virtuel .....	364
▼ Création d'un accord de niveau de service pour le réseau virtuel .....	364

<b>19</b>	<b>Configuration des réseaux virtuels (tâches)</b>	367
	Réseaux virtuels (liste des tâches)	367
	Configuration de composants de virtualisation réseau dans Oracle Solaris	368
	▼ Procédure de création d'interface réseau virtuelle	369
	▼ Création d'etherstubs	371
	Utilisation de VNIC et de zones	373
	Création de nouvelles zones pour l'utiliser avec des VNIC	373
	Modification de la configuration de zones existantes pour utiliser des VNIC	379
	Création d'un réseau virtuel privé	383
	▼ Procédure de suppression du réseau virtuel sans suppression des zones	385
<b>20</b>	<b>Utilisation de la protection des liens dans les environnements virtualisés</b>	387
	Présentation de la protection de liens	387
	Types de protection des liens	388
	Configuration de la protection des liens (liste des tâches)	389
	▼ Activation du mécanisme de protection des liens	390
	▼ Désactivation de la protection des liens	390
	▼ Spécification des adresses IP pour la protection contre l'usurpation d'adresse IP	390
	▼ Affichage de la configuration de la protection des liens	391
<b>21</b>	<b>Gestion des ressources réseau</b>	393
	Présentation de la gestion des ressources réseau	393
	Propriétés de liaisons de données pour le contrôle des ressources	393
	Gestion des ressources réseau à l'aide de flux	394
	Commandes pour la gestion des ressources réseau	395
	Gestion des ressources réseau (liste des tâches)	396
	Gestion des ressources sur liaisons de données	397
	Transmission et réception d'anneaux	397
	Pools et CPU	411
	Gestion des ressources sur les flux	416
	Configuration de flux sur le réseau	416
<b>22</b>	<b>Contrôle du trafic réseau et de l'utilisation des ressources</b>	423
	Présentation du flux de trafic réseau	423

---

Contrôle du trafic et de l'utilisation des ressources (liste des tâches) .....	426
Collecte de statistiques relatives au trafic réseau sur les liaisons .....	427
▼ Procédure d'obtention de statistiques de base sur le trafic réseau .....	428
▼ Procédure d'obtention de statistiques sur l'utilisation d'anneaux .....	430
▼ Procédure d'obtention de statistiques sur le trafic réseau sur des couloirs .....	431
Collecte de statistiques relatives au trafic réseau sur les flux .....	433
▼ Procédure d'obtention de statistiques sur les flux .....	434
Configuration de la comptabilisation du réseau .....	436
▼ Procédure de configuration de la comptabilisation réseau étendue .....	436
▼ Procédure d'obtention de statistiques historiques sur le trafic réseau .....	437
 <b>Glossaire</b> .....	 441
 <b>Index</b> .....	 451



# Préface

---

Bienvenue dans Administration d'Oracle Solaris : Interfaces réseau et virtualisation réseau. Ce manuel fait partie d'un jeu de 14 volumes couvrant une partie importante des informations d'administration système Oracle Solaris. Ce manuel suppose que vous avez déjà installé Oracle Solaris. Vous devez être prêt à configurer votre réseau ou tout logiciel de gestion de réseau requis.

---

**Remarque** – Cette version d'Oracle Solaris prend en charge les systèmes utilisant les architectures de processeur SPARC et x86. Les systèmes pris en charge sont répertoriés dans les listes de la page [Oracle Solaris OS: Hardware Compatibility Lists](#). Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

---

## Utilisateurs de ce manuel

Ce document s'adresse aux administrateurs de systèmes réseau exécutant Oracle Solaris. Pour utiliser ce manuel, vous devez avoir au moins deux ans d'expérience en administration de systèmes UNIX. Une formation en administration de systèmes UNIX peut se révéler utile.

## Organisation des guides d'administration système

La liste des différents sujets traités par les guides d'administration système est la suivante.

Titre du manuel	Sujets
<i>Initialisation et arrêt d'Oracle Solaris sur les plates-formes SPARC</i>	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement de l'initialisation, initialisation à partir de ZFS, gestion de l'archive d'initialisation et dépannage de l'initialisation sur les plates-formes SPARC
<i>Initialisation et arrêt d'Oracle Solaris sur les plates-formes x86</i>	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement de l'initialisation, initialisation à partir de ZFS, gestion de l'archive d'initialisation et dépannage de l'initialisation sur les plates-formes x86

Titre du manuel	Sujets
<i>Administration d'Oracle Solaris : Tâches courantes</i>	Utilisation des commandes Oracle Solaris, initialisation et arrêt d'un système, gestion des comptes d'utilisateurs et des groupes, gestion des services, des pannes matérielles, des informations système, des ressources système et des performances du système, gestion du logiciel, de l'impression, de la console et des terminaux, et résolution des problèmes logiciels et système
<i>Administration d'Oracle Solaris : Périphériques et systèmes de fichiers</i>	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
<i>Administration d'Oracle Solaris : Services IP</i>	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP et IPQoS
<i>Oracle Solaris Administration: Naming and Directory Services</i>	Services d'annuaire et de nommage DNS, NIS et LDAP, y compris transition de NIS à LDAP
<i>Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau</i>	Configuration d'interface IP manuelle et automatique, y compris la configuration sans fil Wi-Fi ; administration des ponts, réseaux locaux virtuels (VLAN), agrégations, LLDP et IPMP ; gestion des ressources et cartes d'interface réseau virtuelles
<i>Administration d'Oracle Solaris : Services réseau</i>	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), mail, SLP et PPP
<i>Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources</i>	Fonctions de gestion des ressources, permettant de contrôler la façon dont les applications utilisent les ressources système disponibles ; technologie de partitionnement logiciel Oracle Solaris Zones, qui virtualise les services de système d'exploitation pour créer un environnement isolé pour les applications en cours d'exécution ; et Oracle Solaris 10 Zones, qui héberge les environnements Oracle Solaris 10 en cours d'exécution sur le noyau Oracle Solaris 11
<i>Administration d'Oracle Solaris : services de sécurité</i>	Audit, gestion de périphériques, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique, gestion des clés, privilèges, RBAC, SASL Secure Shell et analyse des virus
<i>Oracle Solaris Administration: SMB and Windows Interoperability</i>	Service SMB, qui permet de configurer un système Oracle Solaris afin de rendre disponibles les partages SMB aux clients SMB ; client SMB, qui permet d'accéder aux partages SMB ; et services de mappage d'identités natifs, qui permettent de mapper des identités de groupe et d'utilisateur entre les systèmes Oracle Solaris et les systèmes Windows
<i>Administration d'Oracle Solaris : Systèmes de fichiers ZFS</i>	Création et gestion de pools de stockage et de systèmes de fichiers ZFS, instantanés, clones, sauvegardes à l'aide de listes de contrôle d'accès (ACL) pour protéger les fichiers ZFS, utilisation de Solaris ZFS sur un système Solaris avec des zones installées, volumes émulés et dépannage et récupération de données



Titre du manuel	Sujets
<i>Configuration et administration d'Oracle Solaris Trusted Extensions</i>	Installation, configuration et administration système, spécifique à Trusted Extensions
<i>Directives de sécurité d'Oracle Solaris 11</i>	Sécurisation d'un système Oracle Solaris, et scénarios d'utilisation de ses fonctions de sécurité (zones, ZFS et Trusted Extensions)
<i>Transition d'Oracle Solaris 10 vers Oracle Solaris 11</i>	Fournit les informations d'administration système et d'autres exemples de transition à partir d'Oracle Solaris 10 vers Oracle Solaris 11 dans les domaines suivants : gestion de l'installation, des périphériques, des disques et des systèmes de fichiers, gestion des logiciels, mise en réseau, gestion des systèmes, sécurité, virtualisation, fonctions du bureau, gestion des comptes utilisateur et des volumes émulés des environnements utilisateur et dépannage et récupération de données

## Références à des sites Web tiers connexes

Des URL tierces offrant l'accès à des informations complémentaires sont citées dans ce document.

---

**Remarque** – Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

---

## Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> adapté aux utilisateurs malentendants.

# Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P-1 Conventions typographiques

Type de caractères	Signification	Exemple
AaBbCc123	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier <code>.login</code> .  Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers.  <code>nom_machine%</code> Vous avez reçu du courrier.
<b>AaBbCc123</b>	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	<code>nom_machine% su</code>  Mot de passe :
<i>aabbcc123</i>	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est <code>rm nom_fichier</code> .
<i>AaBbCc123</i>	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du <i>Guide de l'utilisateur</i> .  Un <i>cache</i> est une copie des éléments stockés localement.  <i>N'enregistrez pas</i> le fichier.  <b>Remarque</b> : en ligne, certains éléments mis en valeur s'affichent en gras.

# Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite superutilisateur pour les shells faisant partie du SE Oracle Solaris. L'invite système par défaut qui s'affiche dans les exemples de commandes dépend de la version Oracle Solaris.

TABLEAU P-2 Invites de shell

Shell	Invite
Bash shell, korn shell et bourne shell	\$
Bash shell, korn shell et bourne shell pour superutilisateur	#
C shell	<code>nom_machine%</code>

TABLEAU P-2 Invites de shell (Suite)

Shell	Invite
C shell pour superutilisateur	nom_machine#



# Présentation de la pile réseau

---

Ce chapitre présente l'administration réseau dans Oracle Solaris. Il décrit les rapports entre les interfaces, les liaisons de données sur lesquelles les interfaces sont configurées et les périphériques réseau. La prise en charge de noms flexibles pour les liaisons de données est également abordée en détail.

## Configuration réseau dans cette version d'Oracle Solaris

Notez les différences entre cette version et les versions antérieures d'Oracle Solaris en ce qui concerne la configuration du réseau.

- La configuration du réseau est gérée par un profil. Le type de configuration en vigueur dans un système dépend du profil de configuration réseau actif. Reportez-vous à la [Partie I](#).
- Les liaisons de données sur la couche 2 de la pile réseau sont administrées à l'aide de la commande `ladm`. Cette commande remplace les options de commande `ifconfig` précédentes pour configurer les propriétés des liaisons de données. Par conséquent, la configuration des groupements de liens, des VLAN et des tunnels IP a également changé. Reportez-vous aux [Chapitre 8](#), “[Configuration et administration des liaisons de données](#)”, [Chapitre 12](#), “[Administration de groupements de liens](#)”, et [Chapitre 13](#), “[Administration des réseaux locaux virtuels](#)”. Reportez-vous également au [Chapitre 6](#), “[Configuration de tunnels IP](#)” du manuel *Administration d'Oracle Solaris : Services IP*.
- Les noms des liaisons de données ne sont plus liés à leurs pilotes matériels. Par conséquent, les liaisons de données se voient attribuer par défaut des noms de lien génériques tels que `net0`, `net1` et ainsi de suite. Reportez-vous à la section “[Noms des périphériques réseau et des liaisons de données](#)” à la page 26.
- Les interfaces IP sur la couche 3 de la pile de réseau sont administrées à l'aide de la commande `ipadm`. Cette commande remplace les options de commande `ifconfig` précédentes pour configurer les interfaces IP. Reportez-vous au [Chapitre 9](#), “[Configuration d'une interface IP](#)”.

- Les groupes IPMP sont mis en oeuvre en tant qu'interfaces IP et sont donc configurés de la même manière à l'aide de la commande `ipadm`. En outre, la nouvelle commande `impstat` permet d'obtenir des informations et des statistiques sur IPMP. Reportez-vous au [Chapitre 14, “Présentation d'IPMP”](#) et au [Chapitre 15, “Administration d'IPMP”](#).
- La virtualisation est mise en oeuvre au niveau du périphérique réseau. Ainsi, vous pouvez configurer les VNIC et gérer l'utilisation des ressources réseau pour une plus grande efficacité. Reportez-vous à la [Partie III](#).

## Pile réseau dans Oracle Solaris

Les interfaces réseau assurent la connexion entre le système et le réseau. Ces interfaces sont configurées sur les liaisons de données, qui à leur tour correspondent à des instances de périphériques matériels dans le système. Les périphériques matériels sont également appelés *cartes d'interface réseau (NIC)* ou *adaptateurs réseau*. Les NIC peuvent être intégrées dans le système et donc être déjà présentes à l'achat de ce dernier. Cependant, vous êtes libre d'acheter des NIC distinctes pour les ajouter au système. Certaines NIC n'ont qu'une interface unique résidant sur la carte. D'autres marques peuvent avoir plusieurs interfaces que vous pouvez configurer pour effectuer des opérations sur le réseau.

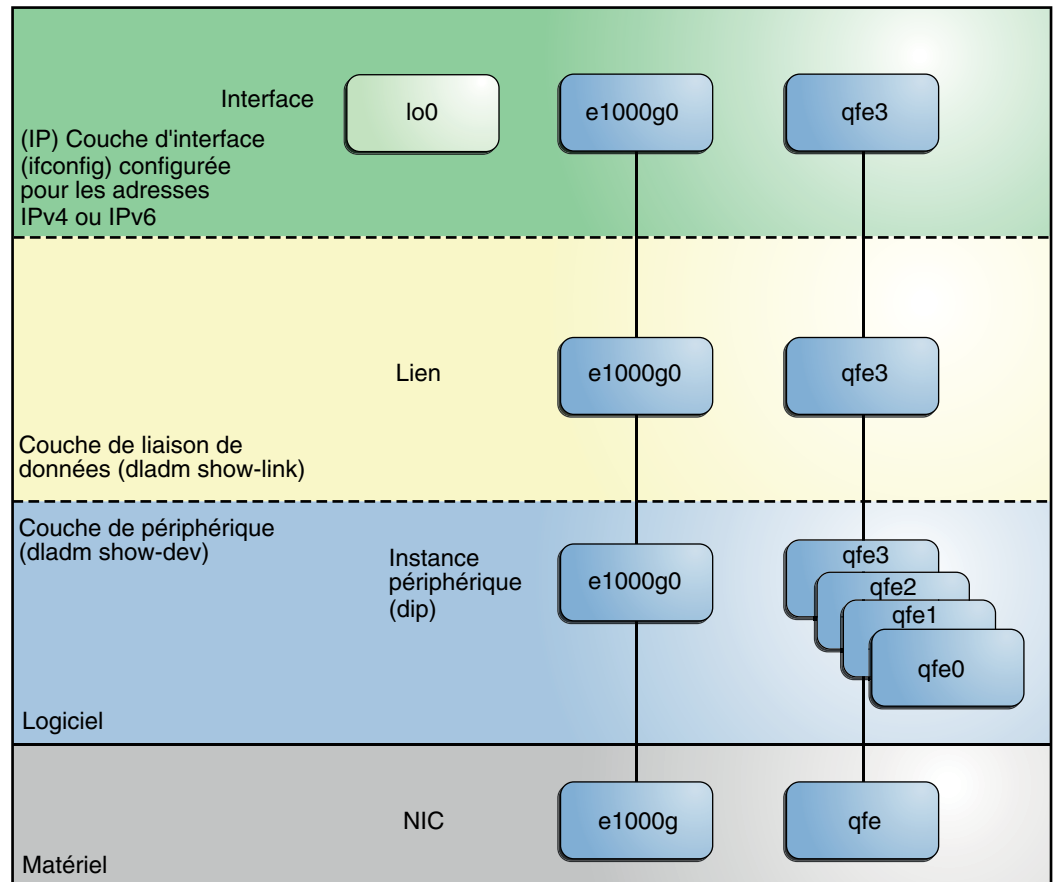
Dans le modèle actuel de la pile de réseau, les interfaces et les liens sur la couche logicielle se construisent sur les périphériques situés dans la couche matérielle. Plus précisément, une instance de périphérique matériel dans la couche matérielle possède un lien correspondant sur la couche de liaison de données et une interface configurée sur la couche d'interface. Cette relation bi-univoque entre le périphérique réseau, sa liaison de données et l'interface IP est illustrée dans la figure qui suit.

---

**Remarque** – Pour obtenir une explication complète de la pile TCP/IP, reportez-vous au [Chapitre 1, “Oracle Solaris TCP/IP Protocol Suite \(Overview\)”](#) du manuel *System Administration Guide: IP Services*.

---

FIGURE 1-1 Pile réseau illustrant les périphériques réseau, liens et interfaces — modèle Oracle Solaris 10



La figure présente deux NIC sur la couche matérielle : `e1000` avec une seule instance de périphérique `e1000g0` et `qfe` avec plusieurs instances de périphérique, de `qfe0` à `qfe3`. Les périphériques `qfe0` à `qfe2` ne sont pas utilisés. Les périphériques `e1000g` et `qfe3` sont utilisés et leurs liens correspondants `e1000g` et `qfe3` figurent sur la couche de liaison de données. Dans la figure, les interfaces IP sont également nommées d'après leur matériel sous-jacent respectif, `e1000g0` et `qfe3`. Ces interfaces peuvent être configurées avec des adresses IPv4 ou IPv6 pour héberger les deux types de trafic réseau. Il faut également noter la présence de l'interface de loopback `lo0` sur la couche d'interface. Elle permet de vérifier, par exemple, le bon fonctionnement de la pile IP.

Différentes commandes d'administration sont utilisées à chaque couche de la pile. Par exemple, les périphériques matériels installés sur le système sont répertoriés par la commande `dladm`

`show-dev`. Les informations à propos des liens sur la couche de liaison de données sont affichées par la commande `dladm show-link`. La commande `ifconfig` indique la configuration de l'interface IP sur la couche d'interface.

Dans ce modèle, une relation bi-univoque lie le périphérique, la liaison de données et l'interface. Cette relation implique que la configuration réseau est dépendante de la configuration matérielle et de la topologie réseau. Les interfaces doivent être reconfigurées si des modifications sont appliquées dans la couche matérielle (remplacement de la NIC ou modification de la topologie réseau, par exemple).

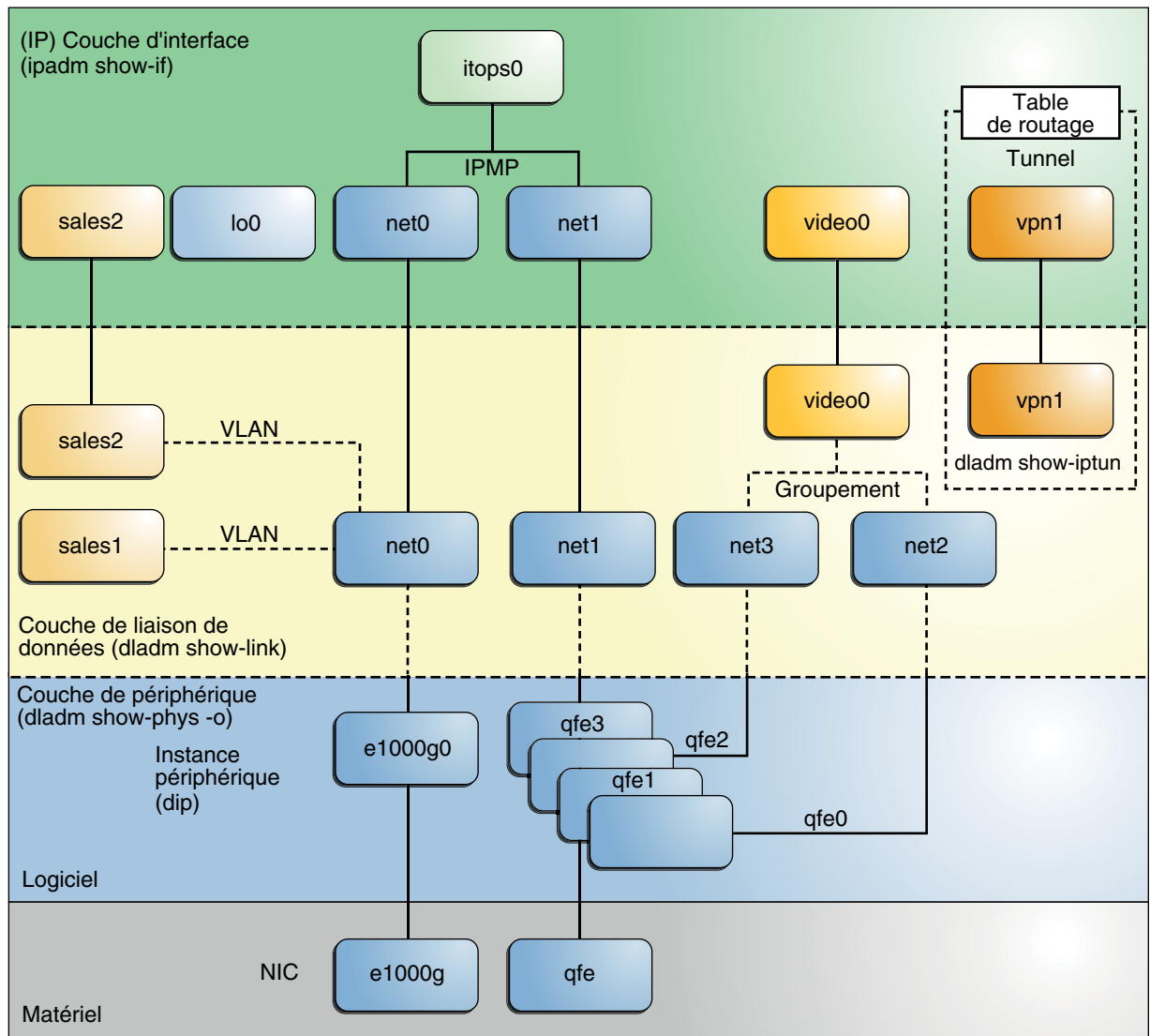
Oracle Solaris 11 présente une mise en oeuvre de la pile réseau, qui conserve la relation de base entre le matériel, la liaison de données et les couches d'interface. Toutefois, la couche logicielle est séparée de la couche matérielle. Par conséquent, la configuration réseau sur le niveau logiciel n'est plus liée au chipset ou à la topologie réseau dans la couche matérielle. Cette mise en oeuvre assouplit l'administration réseau des façons suivantes :

- La configuration du réseau est isolée de toutes les modifications susceptibles de se produire dans la couche matérielle. Les configurations de lien et d'interface sont conservées même si le matériel sous-jacent est supprimé. Ces mêmes configurations peuvent alors être réappliquées à une NIC de remplacement, à condition que les deux NIC soient du même type.
- La séparation de la configuration réseau de la configuration du matériel réseau permet également d'utiliser des noms de lien personnalisés dans la couche de liaison de données.
- Avec l'abstraction de la couche de liaison de données, plusieurs abstractions ou configurations réseau, telles que les VLAN, les VNIC, les périphériques physiques, les groupements de liens et les tunnels IP sont réunis en une même entité administrative : la liaison de données.

La figure ci-dessous illustre la création de ces configurations réseau sur la pile réseau :



FIGURE 1-2 Pile réseau illustrant des périphériques réseau, liens et interfaces — modèle Oracle Solaris 11



Les configurations dans cette illustration sont expliquées plus en détail dans la section “Administration d'autres types de liens” à la page 31.

# Noms des périphériques réseau et des liaisons de données

D'un point de vue administratif, les administrateurs créent des interfaces IP sur les *liaisons de données*. La liaison de données représente un objet de lien dans la deuxième couche du modèle OSI (Open Systems Interconnection). Le *lien physique* est directement associé à un périphérique et possède un nom de périphérique. Le nom de périphérique est essentiellement le nom de l'instance de périphérique ; il est composé du nom du pilote et du numéro de l'instance de périphérique. Le numéro de l'instance peut avoir une valeur comprise entre zéro et  $n$ , en fonction du nombre de NIC utilisant ce pilote sur le système.

Prenons l'exemple d'une carte Gigabit Ethernet, fréquemment utilisée en tant que NIC principale sur les systèmes hôte et serveur. `bge` et `e1000g` sont des noms typiques de pilote pour cette NIC. Si l'interface Gigabit Ethernet est utilisée en tant que NIC principale, son nom de périphérique est du type `bge0` ou `e1000g0`. D'autres noms de pilotes sont `nge`, `nxge` et ainsi de suite.

Dans cette version d'Oracle Solaris, le nom de l'instance de périphérique continue de dépendre du matériel sous-jacent. Cependant, les liaisons de données situées au-dessus de ces périphériques ne sont pas liées de la même façon et peuvent recevoir des noms significatifs. Par exemple, l'administrateur peut attribuer à la liaison de données sur l'instance de périphérique `e1000g0` le nom `itops0`. Dans cette version d'Oracle Solaris, les liaisons de données par défaut sont fournies avec des noms génériques. Pour afficher la mise en correspondance entre les liaisons de données avec leurs noms génériques et les instances de périphérique correspondantes, utilisez la sous-commande `dladm sho-phys`.

## Noms de lien génériques par défaut

Lorsque vous installez cette version d'Oracle Solaris sur un système pour la première fois, Oracle Solaris fournit automatiquement des noms de lien génériques pour tous les périphériques réseau physiques du système. Cette affectation de nom utilise la convention de nommage `net #` où `#` est le numéro d'instance. Ce numéro d'instance est incrémenté pour chaque périphérique, par exemple, `net0`, `net1`, `net2` et ainsi de suite.

Les noms de lien génériques ou flexibles offrent des avantages en matière de configuration réseau, comme indiqué dans les exemples suivants :

- Dans un système unique, la reconfiguration dynamique est simplifiée. La configuration réseau définie pour une NIC donnée peut être héritée par un autre remplacement NIC.
- La migration de zone est simplifiée en ce qui concerne la configuration réseau. La zone dans le système migré conserve sa configuration réseau si le lien du système de destination partage le même nom avec le lien assigné à la zone avant la migration. Par conséquent, aucune autre configuration réseau dans la zone n'est nécessaire après la migration.

- Le schéma de nommage générique facilite la configuration réseau spécifiée dans le manifeste SC (System Configuration) La liaison de donnée réseau principale est généralement appelée `net0` pour tous les systèmes. Par conséquent, un manifeste SC générique peut être utilisé pour plusieurs systèmes qui spécifient une configuration pour `net0`.
- L'administration des liaisons de données est également assouplie. Vous pouvez personnaliser davantage le nom des liaisons de données, par exemple pour refléter leur fonction spécifique, comme illustré à la [Figure 1–2](#).

Le tableau ci-après illustre la nouvelle correspondance entre le matériel (NIC), l'instance de périphérique, le nom de lien et l'interface sur le lien. Les noms des liaisons de données sont automatiquement fournis par le SE.

Matériel (NIC)	Instance de périphérique	Nom attribué du lien	Interface IP
e1000g	e1000g0	net0	net0
qfe	qfe1	net1	net1

Comme l'indique le tableau, alors que le nom de l'instance du périphérique reste basé sur le matériel, les liaisons de données ont été renommées par le SE après son installation.

## Affectation de noms génériques aux liaisons de données

Dans Oracle Solaris, les noms génériques sont automatiquement attribués à l'ensemble des liaisons de données en fonction de critères spécifiques. Tous les périphériques partagent le même préfixe `net`. Cependant, les numéros d'instance sont affectés en fonction des éléments suivants :

- Les périphériques réseau physiques sont classés selon leur type de média, où certains types ont priorité sur les autres. Les types de médias sont classés par ordre décroissant de priorité comme suit :
  1. Ethernet
  2. IP sur IB (périphériques Infiniband)
  3. Ethernet sur IB
  4. Wi-Fi
- Une fois regroupés et triés en fonction des types de média, les périphériques sont classés selon leur emplacement physique, où les périphériques intégrés sont préférés aux unités périphériques.
- Les périphériques présentant une priorité supérieure en fonction de leur type de média et emplacement reçoivent des numéros d'instance inférieurs.

En fonction de ces critères, les périphériques Ethernet sur les cartes mères ou cartes d'E/S, ponts hôtes, complexes de racine PCIe, bus, périphériques et fonctions inférieurs sont classés avant les autres périphériques.

Pour afficher les correspondances entre les noms de lien, périphériques et emplacements, utilisez la commande `dladm show-phys` comme suit :

```
# dladm show-phys -L
LINK      DEVICE      LOCATION
net0      e1000g0      MB
net1      e1000g1      MB
net2      e1000g2      MB
net3      e1000g3      MB
net4      ibp0       MB/RISER0/PCIE0/PORT1
net5      ibp1       MB/RISER0/PCIE0/PORT2
net6      eoib2      MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
net7      eoib4      MB/RISER0/PCIE0/PORT2/cloud-nm2gw-2/1A-ETH-2
```

## Personnalisation de l'affectation des noms de lien génériques

Oracle Solaris utilise le préfixe `net` dans le cadre de l'attribution des noms aux liens. Cependant, n'importe quel préfixe personnalisé peut être utilisé à la place, comme `eth`, par exemple. Si vous préférez, vous pouvez également désactiver l'affectation automatique de noms de lien neutres.



**Attention** – Vous devez personnaliser l'affectation automatique des noms de lien génériques *avant* d'installer Oracle Solaris. Une fois l'installation terminée, il vous est impossible de personnaliser les noms de lien par défaut sans détruire les configurations existantes.

---

Pour désactiver le nommage automatique de lien ou pour personnaliser le préfixe des noms de lien, définissez la propriété suivante dans les manifestes SC utilisés par le programme d'installation automatisée (IA).

```
<service name="network/datalink-management"
  version="1" type="service">
  <instance name="default enabled="true">
    <property_group name='linkname-policy'
      type='application'>
      <propval name='phys-prefix' type='astring'
        value='net' />
    </property_group>
  </instance>
</service>
```

Par défaut, la valeur de `phys-prefix` est définie sur `net`, comme indiqué en gras.

- Pour désactiver le nommage automatique, supprimez toutes les valeurs définies pour `phys-prefix`. Si vous désactivez le nommage automatique, les noms de liaison de données sont basés sur les pilotes matériels associés, tels que `bge0`, `e1000g0`, et ainsi de suite.
- Pour utiliser un préfixe autre que `net`, spécifiez un nouveau préfixe comme valeur de `phys-prefix`, tel que `eth`.

Si la valeur fournie pour `phys-prefix` n'est pas valide, elle est ignorée. Les liaisons de données sont nommées conformément aux pilotes matériels associés, tels que `bge0`, `e1000g0` et ainsi de suite. Pour plus d'informations sur les noms de lien valides, reportez-vous à la section [“Règles applicables aux noms de lien valides”](#) à la page 30.

## Noms de lien dans les systèmes mis à niveau

Dans des systèmes où cette version d'Oracle Solaris vient d'être installée, les liaisons de données sont automatiquement nommées de `net0` à `net N-1`, où `N` représente le nombre total de périphériques réseau.

Tel n'est pas le cas si la mise à niveau concerne Oracle Solaris 11 Express. Sur ces systèmes mis à niveau, les liaisons de données conservent le nom qu'elles portaient avant la mise à niveau. Il s'agit soit des noms par défaut basés sur le matériel, soit des noms personnalisés que l'administrateur a attribué aux liaisons de données avant la mise à niveau. De plus, sur ces systèmes mis à niveau, les nouveaux périphériques réseau qui sont ajoutés par la suite conservent également les noms par défaut basés sur le matériel au lieu de recevoir des noms neutres. Ce comportement des systèmes mis à niveau garantit qu'aucun nom neutre affecté par le SE ne soit confondu avec d'autres noms basés sur le matériel ou personnalisés que l'administrateur a attribués avant la mise à niveau.

Dans tous les systèmes dotés de cette version d'Oracle Solaris, les noms basés sur le matériel et les noms fournis par le SE peuvent être remplacés par d'autres noms à votre convenance. En règle générale, les noms de lien par défaut affectés par le SE s'avèrent suffisants pour créer la configuration réseau du système. Cependant, si vous choisissez de modifier des noms de lien, prenez en compte les points abordés dans les sections suivantes.

## Remplacement des noms de lien basés sur le matériel

Si les liens de votre système ont des noms basés sur le matériel, renommez-les avec au moins des noms génériques. Conserver les noms de lien basés sur le matériel risque de porter à confusion lors de la suppression ou du remplacement de ces périphériques physiques.

Par exemple, vous conservez le nom de lien `bge0`, associé au périphérique `bge0`. Toutes les configurations de lien font référence au nom de lien. Par la suite, vous pouvez remplacer la NIC `bge` par la NIC `e1000g`. Pour réappliquer la configuration de lien de l'ancien périphérique à la nouvelle NIC `e1000g0`, vous devez réaffecter le nom de lien `bge0` à `e1000g0`. L'association d'un

nom de lien basé sur le matériel bge0 à une autre NIC associée e1000g0 risque de porter à confusion. L'utilisation de noms qui ne sont pas basés sur le matériel permet de mieux distinguer les liens des périphériques associés.

## Avertissement à propos de la modification de noms de liens

Bien qu'il soit conseillé de remplacer les noms de liens basés sur le matériel, vous devez toujours planifier soigneusement le renommage des liens. Modifier le nom de lien du périphérique ne propage pas automatiquement le nouveau nom à toutes les configurations associées existantes. Les exemples suivants illustrent les risques associés à la modification des noms de lien :

- Certaines règles dans une configuration de filtre IP s'appliquent à des liens spécifiques. Lorsque vous modifiez le nom d'un lien, les règles de filtre continuent de faire référence au nom original du lien. Par conséquent, ces règles ne se comportent plus comme prévu une fois que vous renommez le lien. Vous devez ajuster les règles de filtre à appliquer à la liaison à l'aide du nouveau nom de lien.
- Prenez en compte la possibilité d'exporter les informations de configuration réseau. Comme expliqué précédemment, à l'aide des noms net # par défaut fournis par le SE, vous pouvez faire migrer des zones et exporter la configuration réseau vers un autre système en toute simplicité. Si les périphériques réseau du système cible portent des noms génériques, tels que net0, net1 et autres, la zone hérite tout simplement de la configuration réseau de la liaison de données dont le nom correspond à la liaison de données assignée à la zone.

Par conséquent, en règle générale, ne renommez pas les liaisons de données au hasard. Lors de l'attribution d'un nouveau nom aux liaisons de données, assurez-vous que toutes les configurations associées du lien continuent à s'appliquer après la modification du nom du lien. Certaines configurations sur lesquelles le renommage peut avoir des incidences sont les suivantes :

- Règles de filtre IP
- Configurations IP spécifiées dans les fichiers de configuration, comme /etc/dhclient.conf.
- Zones Oracle Solaris 11
- Configuration autopush

---

**Remarque** – Aucune modification n'est nécessaire dans la configuration autopush lorsque vous renommez des liens. Toutefois, vous devez connaître le fonctionnement de la configuration avec la propriété autopush par lien une fois le lien renommé. Pour plus d'informations, reportez-vous à la rubrique "[Procédure de définition de modules STREAMS sur les liaisons de données](#)" à la page 176.

---

## Règles applicables aux noms de lien valides

Lorsque vous affectez des noms de lien, observez les règles suivantes :

- Les noms de lien sont composés d'une chaîne et d'un numéro *PPA* (*point d'attache physique*) .
- Ce nom doit respecter les restrictions suivantes :
  - Les noms sont composés de 3 à 8 caractères. Toutefois, ils peuvent contenir un maximum de 16 caractères.
  - Les caractères valides pour les noms sont les caractères alphanumériques (a-z, 0-9) et le caractère de soulignement ('\_').




---

**Attention** – N'utilisez pas les majuscules dans les noms de lien.

---

- Chaque liaison de données doit avoir un seul nom de lien à un moment donné.
- Chaque liaison de données doit avoir un nom de lien unique au sein du système.

---

**Remarque** – Autre restriction : vous ne pouvez pas utiliser `lo0` comme nom de lien flexible. Ce nom est réservé à l'identification de l'interface de loopback IP.

---

La fonction du lien dans votre configuration réseau peut être une référence utile lorsque vous affectez des noms de lien. Par exemple, `netmgt0` peut être un lien dédié à la gestion du réseau. `Upstream2` peut être le lien connecté à l'ISP. En règle générale, pour éviter toute confusion, n'affectez *pas* des noms de périphériques connus à vos liens.

## Administration d'autres types de liens

La séparation entre la configuration réseau et la configuration matérielle réseau introduit la même flexibilité à d'autres types de configurations de lien. Par exemple, les VLAN, les groupements de liens et les tunnels IP peuvent recevoir un nom choisi administrativement, puis être configurés par référence à ces noms. Les autres tâches connexes, comme l'exécution de la reconfiguration dynamique (DR) pour remplacer les périphériques matériels, sont également plus faciles à effectuer dans la mesure où aucune reconfiguration du réseau n'est nécessaire, à condition que la configuration du réseau n'ait pas été supprimée.

La figure suivante indique les relations entre les périphériques, les types de lien et les interfaces correspondantes.

---

**Remarque** – Dans la figure, les liaisons de données sont nommées conformément aux fonctions spécifiques qu'elles effectuent dans le système (`video0` ou `sales2`, par exemple). La figure souligne la flexibilité avec laquelle vous pouvez nommer les liaisons de données. Cependant, l'utilisation de noms neutres par défaut, tels que `net0`, fournis par le SE est suffisante et préférable.

---

La figure offre également un exemple de l'utilisation de noms choisis administrativement dans la configuration du réseau :

- Les VLAN sont configurés sur le lien `net0`. Ces VLAN, à leur tour, reçoivent également des noms personnalisés, tels que `sales1` et `sales2`. L'interface IP du VLAN `sales2` est montée et opérationnelle.
- Les instances de périphériques `qfe0` et `qfe2` sont utilisées dans le cadre de la prise en charge du trafic vidéo. Par conséquent, les liens correspondants dans la couche de liaison de données reçoivent les noms `subvideo0` et `subvideo1`. Ces deux liens sont regroupés dans la source vidéo hôte. Le groupement de liens possède son propre nom personnalisé, `video0`.
- Deux interfaces (`net0` et `net1`) dotées du matériel sous-jacent différent (`e1000g` et `qfe`) sont regroupées en tant que groupe IPMP (`itops0`) pour héberger le trafic d'e-mails.

---

**Remarque** – Bien que les interfaces IPMP ne soient pas des liens sur la couche de liaison de données, ces interfaces, comme les liens, peuvent également recevoir des noms personnalisés. Pour plus d'informations sur les groupes IPMP, reportez-vous au [Chapitre 14, “Présentation d'IPMP”](#).

---

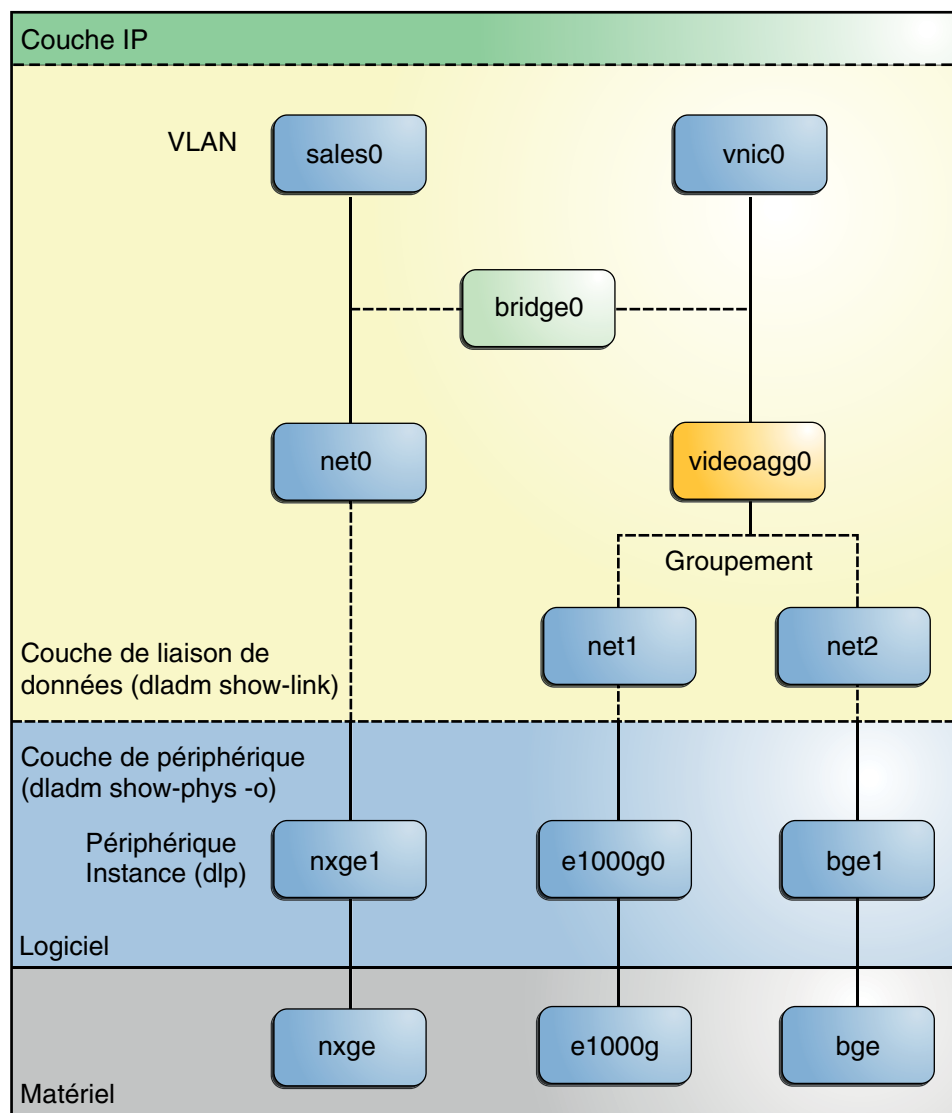
- Deux interfaces n'ont aucun périphérique sous-jacent : le tunnel `vpn1`, qui est configuré pour les connexions VPN et `lo0` pour les opérations de loopback IP.

Toutes les configurations de lien et d'interface dans cette figure sont indépendantes des configurations dans le matériel sous-jacent. Par exemple, si la carte `qfe` est remplacée, la configuration de l'interface `video0` pour le trafic vidéo est conservée et peut ensuite être appliquée à une NIC de remplacement.

La figure ci-dessous illustre une configuration de pont. Deux interfaces, `net0` et `videoagg0`, sont configurées en tant que pont, `bridge0`. Les paquets reçus sur une interface sont transmis à l'autre. Après la configuration du pont, les deux interfaces peuvent toujours être utilisées pour configurer des VLAN et interfaces IP.



FIGURE 1-3 Ponts dans la pile réseau





## PARTIE I

# Configuration automatique de réseau

NWAM (Network Auto-Magic) est une fonction d'Oracle Solaris qui automatise la configuration réseau de base de votre système. Les sujets traités dans ces chapitres décrivent les composants de l'architecture NWAM et la manière dont ils fonctionnent ensemble dans le cadre de la configuration réseau automatisée sur votre système Oracle Solaris.

Cette documentation se concentre principalement sur la gestion de la configuration de votre réseau à l'aide des utilitaires de ligne de commande NWAM. Les informations de base relatives à l'utilisation de l'interface graphique NWAM pour afficher et contrôler l'état de votre réseau, mais aussi interagir avec NWAM à partir du bureau sont également incluses. Vous trouverez des instructions détaillées sur le contrôle et la gestion de votre configuration réseau à l'aide de l'interface graphique NWAM dans l'aide en ligne.



## Présentation de NWAM

---

La fonction NWAM (Network Auto-Magic) simplifie la configuration réseau de base en traitant les configurations Ethernet et Wi-Fi élémentaires, par exemple la connexion à un réseau câblé ou sans fil au démarrage et l'affichage de notifications sur l'état de la connexion réseau active sur le bureau. Elle est également conçue pour simplifier certaines des tâches réseau les plus complexes, telles que la création et la gestion de profils de réseau à l'échelle du système, par exemple, la configuration des services de nommage, IP Filter et IPsec (sécurité IP), qui sont des fonctions d'Oracle Solaris.

Ce chapitre comprend les sections suivantes :

- “Définition d'une configuration NWAM” à la page 38
- “Cas d'utilisation de NWAM” à la page 40
- “Fonctionnement de la configuration NWAM” à la page 41
- “Fonctionnement de NWAM avec d'autres technologies de mise en réseau Oracle Solaris ” à la page 43
- “Sources contenant les tâches de configuration réseau ” à la page 44

Ce chapitre est destiné aux utilisateurs et administrateurs système possédant des connaissances rudimentaires en concepts réseau, ainsi qu'une expérience en gestion de configuration de réseau à l'aide d'outils et de commandes de mise en réseau classiques. Si vous êtes prêt à utiliser NWAM pour gérer votre configuration réseau, passez au [Chapitre 4, “Configuration de profil NWAM \(tâches\)”](#).

Pour obtenir des informations de base sur l'administration d'interfaces réseau dans Oracle Solaris, reportez-vous à la [Partie II](#).

# Définition d'une configuration NWAM

Une configuration NWAM comporte plusieurs composants qui collaborent afin de mettre en oeuvre la configuration réseau d'un système la plus automatisée possible. Fonction axée principalement sur la mobilité, NWAM peut modifier de façon dynamique la configuration d'un système, suite à différents événements réseau ou à une demande de l'utilisateur. NWAM inclut des options dynamiques chargées de traiter toute modification des conditions du réseau, comme la déconnexion d'une interface réseau ou la disponibilité d'un nouveau réseau sans fil.

La configuration du réseau par le biais de NWAM est constituée de propriétés et de leurs valeurs, associées à différents types de profils, parfois appelés des *objets de configuration*.

Ces profils et objets de configuration sont les suivants :

- **Profils de configuration réseau (NCP, Network Configuration Profiles)**

Un NCP spécifie la configuration de liens et interfaces de réseau. Ce profil est l'un des principaux types de profils qui constituent une configuration NWAM. Le deuxième type de profil principal est le profil d'emplacement.

Le système définit toujours un NCP appelé NCP Automatique. Ce NCP est activé en l'absence d'entrée de l'utilisateur. Le NCP Automatique est créé et mis à jour par le système, à savoir qu'il ne peut pas être modifié ni supprimé.

Vous pouvez également créer d'autres NCP définis par l'utilisateur, en fonction des besoins. Pour obtenir une description complète du NCP Automatique et des NCP définis par l'utilisateur, reportez-vous à la section [“Description des NCP automatiques et définis par l'utilisateur”](#) à la page 50.

- **Unités de configuration réseau (NCU, Network Configuration Units)**

Les NCU sont les différents objets de configuration contenant toutes les propriétés dont un NCP est constitué. Le NCP est essentiellement un conteneur dans lequel sont stockées les NCU qui le définissent. Chaque NCU correspond à un lien ou une interface du système. Pour obtenir une description complète d'une NCU, reportez-vous à la section [“Description d'une NCU”](#) à la page 49.

- **Emplacements**

Le profil d'emplacement est l'un des deux principaux types de profils qui constituent une configuration NWAM. L'emplacement indique la configuration réseau à l'échelle du système, notamment les services de nommage, le domaine, le filtre IP et la configuration IPsec. Ces informations se composent d'un ensemble de propriétés qui s'appliquent à la configuration réseau à l'échelle du système. Certains emplacements sont définis par le système, tandis que d'autres par l'utilisateur. Pour obtenir une description complète du profil d'emplacement, reportez-vous à la section [“Description d'un profil d'emplacement”](#) à la page 51.

- **Modificateurs réseau externes (ENM, External Network Modifiers)**

Les ENM sont des profils de gestion des applications externes à NWAM, par exemple, une application de réseau privé virtuel (VPN, Virtual Private Network). Ces applications peuvent créer et modifier la configuration réseau. Le démon `nwamd` active ou désactive un ENM, en fonction des conditions spécifiées dans le cadre de l'ENM. Pour obtenir une description complète d'un ENM, reportez-vous à la section [“Description d'un ENM”](#) à la page 52.

- **Réseaux locaux sans fil connus (WLAN, Wireless Local Area Networks)**

Les WLAN connus sont des objets de configuration que NWAM utilise pour contrôler et stocker des informations sur les réseaux sans fil connus de votre système. NWAM gère une liste de tous ces réseaux sans fil à laquelle il se réfère pour déterminer l'ordre dans lequel les connexions aux réseaux sans fil disponibles sont tentées. Pour obtenir une description complète des WLAN connus, reportez-vous à la section [“A propos des WLAN connus”](#) à la page 52.

## Composants fonctionnels NWAM

NWAM comprend les composants fonctionnels suivants :

- **Référentiel de profils NWAM** : le référentiel de profils est l'emplacement de stockage des données de configuration NWAM. L'accès au référentiel de profils est géré par le démon de référentiel, `netcfgd`.

Le référentiel de profils NWAM comprend un instantané de votre configuration réseau lorsque la fonction NWAM est activée. Ces données sont préservées dans le cas où vous auriez besoin de revenir à la configuration manuelle de votre réseau. Pour plus d'informations, reportez-vous à la section [“Données de configuration NWAM”](#) à la page 53.

- **Programmes de configuration de profil (interfaces utilisateur)** : l'architecture NWAM comprend à la fois une interface de ligne de commande (CLI) et une interface graphique. Ces interfaces peuvent être utilisées pour exécuter des tâches similaires, notamment la création et la modification de profils, l'activation de profils et l'interrogation du système pour obtenir des informations sur les profils.

La CLI NWAM se compose de deux commandes d'administration, `netcfg` et `netadm`. La commande `netcfg` permet de créer et de modifier les profils. Cette commande fonctionne dans les modes interactif, ligne de commande et fichier de commande. La commande `netadm` permet d'effectuer certaines opérations, par exemple, l'activation ou la désactivation d'un profil et l'énumération d'informations sur les états de profils. Pour plus d'informations, reportez-vous aux pages de manuel [netcfg\(1M\)](#) et [netadm\(1M\)](#).

Pour obtenir des instructions détaillées sur la création et la gestion de profils à l'aide de la CLI NWAM, reportez-vous au [Chapitre 4, “Configuration de profil NWAM \(tâches\)”](#) et au [Chapitre 5, “Administration des profils NWAM \(tâches\)”](#).

L'interface graphique NWAM permet également de créer et de gérer des profils réseau. L'interface utilisateur possède des fonctionnalités supplémentaires qui vous permettent d'afficher rapidement mais aussi de contrôler l'état des connexions réseau à partir du bureau. Elle présente également une fonction de notification qui vous informe de l'évolution de l'état de votre réseau. La fonctionnalité de notification n'est disponible que dans l'interface graphique. Pour en savoir plus sur l'utilisation de l'interface graphique NWAM, reportez-vous au [Chapitre 6, “A propos de l'interface graphique NWAM”](#) ou à l'aide en ligne. Reportez-vous également aux pages de manuel `nwamgr(1M)` et `nwamgr-properties(1M)`.

- **Démon de moteur de stratégie** : le démon `nwamd` est le composant de stratégie NWAM. Ce démon remplit plusieurs rôles et gère votre configuration réseau en fonction des profils stockés dans le référentiel de profils. Il détermine le profil à activer selon les conditions du réseau, puis active ce profil. Pour accomplir cette tâche, le démon intègre les informations en provenance de plusieurs sources. Les différents rôles que le démon `nwamd` remplit sont décrits en détail dans la section [“Présentation des démons NWAM” à la page 71](#).
- **Démon de référentiel** : le démon `netcfgd` contrôle le référentiel de profil commun où toutes les données de configuration pour les profils et autres objets de configuration sont stockées. La commande `netcfg`, l'interface graphique NWAM et le démon `nwamd` interagissent avec le démon `netcfgd` par l'envoi de demandes d'accès au référentiel de profils. Le démon de référentiel est chargé de vérifier si les divers processus qui tentent d'accéder aux données de référentiel possèdent les autorisations correctes. Le démon interdit (fait échouer) toute tentative d'accès par les processus non autorisés. Pour plus d'informations, reportez-vous à la section [“Description du démon de référentiel NWAM\(`netcfgd`\)” à la page 72](#).
- **Interface de bibliothèque NWAM** : la bibliothèque `libnwam` offre une interface fonctionnelle pour interagir avec le référentiel de profils, et permettre ainsi à NWAM de lire et de modifier les informations sur les profils.
- **SMF (Service Management Facility, utilitaire de gestion des services)** : plusieurs services réseau que NWAM utilise font déjà partie d'Oracle Solaris. Cependant, certains de ces services existants ont été modifiés, tandis que de nouveaux services spécifiques à NWAM ont vu le jour. Pour plus d'informations, reportez-vous à la section [“Services réseau SMF et configuration NWAM” à la page 72](#).

## Cas d'utilisation de NWAM

D'une façon générale, si vous modifiez fréquemment vos environnements de travail et méthodes de connexion (câblées ou sans fil), il est conseillé de tirer parti de la fonctionnalité de configuration réseau automatisée de NWAM. Vous pouvez utiliser NWAM pour configurer des profils définis par l'utilisateur, qui vous permettent de vous connecter à des réseaux dans diverses configurations (au bureau, à la maison ou en déplacement, par exemple). NWAM est un outil précieux pour les utilisateurs de systèmes et modèles d'ordinateurs portables, qui nécessitent des changements fréquents d'environnements réseau. En outre, l'interface



graphique NWAM simplifie la configuration IP statique et les connexions aux réseaux Wi-Fi, par rapport aux commandes et outils de mise en réseau traditionnels.

La fonction NWAM peut être configurée de façon à s'adapter aux changements de votre environnement réseau, comme la perte de connexion Ethernet, ou l'ajout ou la suppression d'une carte réseau (NIC).

---

**Remarque** – Vous pouvez choisir de configurer votre réseau manuellement, par exemple, si vous utilisez les fonctions réseau avancées, qui ne sont pas actuellement prises en charge par NWAM. Pour plus d'informations, reportez-vous à la section [“Gestion de la configuration réseau par l'intermédiaire de SMF”](#) à la page 112.

---

## Fonctionnement de la configuration NWAM

Le comportement par défaut de NWAM consiste à effectuer une configuration de base de votre réseau câblé ou sans fil "automatiquement", c'est-à-dire sans aucune intervention de l'utilisateur. La seule interaction nécessaire avec NWAM consiste à fournir des informations supplémentaires, comme une clé de sécurité ou un mot de passe d'un réseau sans fil, lorsque vous y êtes invité.

La configuration automatique NWAM est déclenchée par les événements et activités suivants :

- Connexion ou déconnexion d'un câble Ethernet
- Connexion ou déconnexion d'une carte WLAN
- Initialisation d'un système lorsqu'une interface câblée, une interface sans fil ou les deux sont disponibles
- Reprise après une interruption lorsqu'une interface câblée, une interface sans fil ou les deux sont disponibles (en cas de prise en charge)
- Acquisition ou perte d'une location DHCP

Les composants NWAM interagissent de la façon suivante :

- A tout moment, un profil NCP et un profil d'emplacement doivent être actifs sur le système.
- Lors d'une initialisation du système, le démon moteur de stratégie, `nwamd`, effectue les actions suivantes :
  1. Il consulte la propriété du service pour le NCP actif.
  2. Il fonctionne jusqu'à ce qu'une ou plusieurs adresses IP aient été configurées.
  3. Il vérifie les conditions des profils d'emplacement.
  4. Il active le profil d'emplacement qui est spécifié par le moteur de stratégie.
  5. Il configure le ou les réseaux, en conséquence.
- Lorsque des événements pouvant déclencher une modification de la configuration réseau se produisent, le démon NWAM `nwamd` remplit divers rôles et exécute les opérations suivantes :

1. En tant que gestionnaire d'événements, `nwamd` détecte chaque événement tel qu'il se produit.
2. En tant que démon de profil, `nwamd` consulte le profil actif.
3. En fonction de la modification, `nwamd` peut reconfigurer le ou les réseaux, en conséquence.

## Comportement par défaut de NWAM

En l'absence de profils réseau définis par l'utilisateur, `nwamd` gère la configuration réseau basée sur les trois profils définis par le système suivants :

- NCP Automatique
- Emplacement automatique
- Emplacement NoNet

Le NCP Automatique met en oeuvre la stratégie de base suivante :

- Configurez toutes les interfaces Ethernet (connectées) disponibles à l'aide de DHCP.
- Si aucune interface Ethernet n'est connectée, ou si aucune ne peut obtenir une adresse IP, activez une interface sans fil, qui se connecte automatiquement au meilleur WLAN disponible dans la *liste des WLAN connus*. Vous pouvez également attendre que l'utilisateur sélectionne un réseau sans fil auquel se connecter.
- Jusqu'à ce qu'une adresse IPv4 au moins soit obtenue, l'emplacement NoNet reste actif. Ce profil d'emplacement offre un ensemble strict de règles de filtre IP qui transmettent uniquement des données pertinentes à l'acquisition d'adresse IP (messages autoconf DHCP et IPv6). Toutes les propriétés de l'emplacement NoNet, à l'exception des conditions d'activation, peuvent être modifiées.
- Lorsqu'une adresse IPv4 au moins a été affectée à l'une des interfaces du système, l'emplacement Automatique est activé. Ce profil d'emplacement n'a pas de règle de sécurité IP ni de filtre IP. Le profil d'emplacement s'applique aux données de configuration DNS, obtenues à partir du serveur DHCP. A l'instar des emplacements NoNet, toutes les propriétés de l'emplacement automatique, à l'exception de ses conditions d'activation, peuvent être modifiées.
- L'emplacement NoNet est toujours appliqué lorsqu'aucune adresse IPv4 n'est affectée au système. Lorsqu'au moins une adresse IPv4 est affectée, le système sélectionne le profil d'emplacement avec les règles d'activation qui correspondent le mieux aux conditions du réseau. En l'absence d'une meilleure correspondance, le système se replie sur l'emplacement automatique. Pour plus d'informations, reportez-vous à la section "[Activation des profils NWAM](#)" à la page 58.

# Fonctionnement de NWAM avec d'autres technologies de mise en réseau Oracle Solaris

NWAM fonctionne avec les autres technologies de mise en réseau Oracle Solaris suivantes :

- **Virtualisation réseau**

NWAM fonctionne avec les diverses technologies de virtualisation réseau Oracle Solaris comme suit :

- **Machines virtuelles : Oracle VM Server pour SPARC (anciennement Logical Domains) et Oracle VM VirtualBox**

La fonctionnalité NWAM est prise en charge aussi bien dans les hôtes que dans les invités Oracle Solaris. NWAM gère uniquement les interfaces qui appartiennent aux machines virtuelles spécifiées et n'interfère pas avec d'autres machines virtuelles.

- **Instances de pile et zones Oracle Solaris**

NWAM fonctionne dans les zones globales ou dans une zone non globale de pile exclusive.

---

**Remarque** – NWAM ne fonctionne pas dans une zone de pile partagée.

---

- **VNIC**

Bien que la mise en oeuvre NWAM actuelle ne gère pas les VNIC, les VNIC créées manuellement sont conservées après la réinitialisation et peuvent être créées, par exemple, pour être affectées à une zone de pile exclusive.

- **Technologie de création de pont**

Grâce à la technologie de création de pont, il est possible de connecter des segments de réseau distincts pour permettre la communication entre les noeuds reliés, comme si un seul segment était utilisé. Bien que la mise en oeuvre NWAM ne prenne pas activement en charge les configurations réseau qui utilisent la technologie de création de pont, il n'est pas nécessaire de désactiver la gestion de la configuration NWAM avant d'utiliser cette technologie sur votre système.

- **Reconfiguration dynamique et profils de configuration réseau**

Les systèmes prenant en charge la reconfiguration dynamique (Dynamic Reconfiguration, DR) et les fonctionnalités enfichables à chaud ont recours à ces fonctions uniquement si le NCP actif sur ces systèmes est `DefaultFixed`.

Si le NCP activé sur ces systèmes est `Automatic` ou tout autre NCP créé par l'utilisateur, vous devez effectuer l'une des étapes suivantes avant d'effectuer des opérations de reconfiguration dynamique :

- Arrêtez le service réseau. Cette action entraîne l'interruption de toutes les interfaces réseau sur le système. Par conséquent, vous devez utiliser la console système pour arrêter le service. Après avoir supprimé ou remplacé le périphérique, redémarrez le service.
- Supprimez l'interface IP de la configuration du NCP actif à l'aide de la commande `netcfg`. Ensuite, vous pouvez procéder à la suppression ou au remplacement physique du périphérique matériel sous-jacent de cette interface IP. Le cas échéant, reconfigurez l'interface IP à l'issue de la reconfiguration dynamique.

■ **Utilitaires et commandes réseau traditionnels**

A tout moment, le système utilise *soit* la configuration réseau traditionnelle, soit la configuration réseau NWAM. Si le NCP `DefaultFixed` est activé, le système utilise la configuration réseau traditionnelle. Le système applique la configuration persistante, qui est stockée dans les fichiers `/etc/ipadm/ipadm.conf` et `/etc/dladm/datalink.conf` lorsque ce NCP est activé. En outre, vous pouvez utiliser les commandes `ipadm` et `dladm` pour visualiser et modifier la configuration réseau. Si un NCP NWAM est activé, le système ignore la configuration `/etc/ipadm/ipadm.conf` et NWAM gère la configuration du réseau en fonction de la stratégie spécifiée dans le NCP actif.

Lorsque NWAM gère la configuration réseau, vous pouvez toujours utiliser les utilitaires de ligne de commande, `dladm` et `ipadm`, pour afficher les composants de votre configuration réseau actuelle.

**Remarque** – Apporter des modifications à la configuration réseau à l'aide d'outils de ligne de commande n'est pas pris en charge, dans la mesure où ces modifications risquent d'entrer en conflit avec la stratégie appliquée par NWAM.

■ **Fonctionnalité de chemins d'accès multiples (fonctionnalité multipathing)**

NWAM ne prend pas actuellement en charge l'utilisation d'IPMP. Avant de configurer votre réseau en vue d'utiliser IPMP, assurez-vous que le NCP `DefaultFixed` est activé.

# Sources contenant les tâches de configuration réseau

Le tableau ci-dessous répertorie les rubriques concernant la configuration réseau et les sources d'informations supplémentaires.

Tâches de mise en réseau	Pour plus d'informations
Rechercher plus d'informations générales sur NWAM	<a href="#">Chapitre 3, “Configuration et administration NWAM (présentation)”</a>
Créer, modifier et supprimer des profils et objets de configuration à l'aide de la CLI NWAM	<a href="#">Chapitre 4, “Configuration de profil NWAM (tâches)”</a>

Tâches de mise en réseau	Pour plus d'informations
Visualiser des informations, et administrer des profils et objets de configuration à l'aide de la CLI NWAM	<a href="#">Chapitre 5, “Administration des profils NWAM (tâches)”</a>
Afficher les informations sur l'état de votre réseau, passer d'une connexion réseau à l'autre, et créer et modifier des profils et objets de configuration à l'aide de l'interface graphique NWAM à partir du bureau	<a href="#">Chapitre 6, “A propos de l'interface graphique NWAM”</a> et aide en ligne
Passer du mode de configuration réseau NWAM au mode de configuration réseau traditionnel	<a href="#">“Gestion de la configuration réseau par l'intermédiaire de SMF”</a> à la page 112
Gérer la configuration réseau à l'aide d'outils et commandes réseau traditionnels	<a href="#">Chapitre 8, “Configuration et administration des liaisons de données”</a> et <a href="#">Chapitre 9, “Configuration d'une interface IP”</a>
Configurer et gérer des réseaux virtuels	<a href="#">Chapitre 17, “Introduction à la virtualisation du réseau et au contrôle des ressources (présentation)”</a>



## Configuration et administration NWAM (présentation)

---

Ce chapitre contient des informations contextuelles et générales sur la configuration et l'administration NWAM. La mise en oeuvre des profils que NWAM utilise pour simplifier et automatiser la configuration du réseau est également décrite en détail.

Ce chapitre comprend les sections suivantes :

- “Présentation de la configuration NWAM ” à la page 47
- “Données de configuration NWAM ” à la page 53
- “Activation des profils NWAM” à la page 58
- “Configuration de profils à l'aide de la commande `netcfg`” à la page 63
- “Administration des profils à l'aide de la commande `netadm`” à la page 69
- “Présentation des démons NWAM” à la page 71
- “Services réseau SMF et configuration NWAM ” à la page 72
- “Présentation de la sécurité NWAM ” à la page 74

### Présentation de la configuration NWAM

NWAM gère la configuration réseau en stockant les valeurs de propriété préférées sous forme de profils sur le système. NWAM détermine alors le profil à activer, en fonction des conditions réseau, puis active ce profil. La mise en oeuvre des profils NWAM est un composant principal de NWAM.

### Définition des profils réseau

Les profils réseau sont des collections de propriétés qui déterminent la configuration et le fonctionnement du réseau, en fonction des conditions réseau.

Les types de profil et objets de configuration suivants composent la configuration NWAM :

- Profils de configuration réseau (NCP, Network Configuration Profiles)
- Profils d'emplacement
- Modificateurs réseau externes (ENM, External Network Modifiers)
- WLAN connus

Le profil NCP et le profil d'emplacement constituent les deux principaux types de profils réseau. Pour parvenir à configurer automatiquement le réseau par le biais de NWAM, un profil NCP et un profil d'emplacement doivent être actifs sur le système à tout moment.

Le profil NCP spécifie la configuration du réseau local, y compris la configuration de chaque composant (liens physiques et interfaces IP, notamment). Chaque profil NCP se compose de différents objets de configuration, appelés *NCU* (*Network Configuration Units, unités de configuration réseau*). Chaque NCU représente un lien physique ou une interface dont elle définit la configuration par le biais des propriétés qui la composent. Le processus de configuration d'un profil NCP défini par l'utilisateur implique la création de NCU spécifiques. Pour plus d'informations, reportez-vous à la section [“Description d'une NCU” à la page 49](#).

Un profil d'emplacement contient des informations de configuration réseau à l'échelle du système, y compris les suivantes :

- Conditions dans lesquelles le profil d'emplacement est activé
- Service de nommage à utiliser
- Nom de domaine
- Ensemble de règles de filtre IP
- Stratégie IPsec

Pour plus d'informations, reportez-vous à la section [“Description d'un profil d'emplacement” à la page 51](#).

Les ENM sont des profils NWAM pour les applications externes capables de créer et de modifier la configuration réseau. NWAM peut être configuré de façon à activer et désactiver ces applications externes dans les conditions que vous indiquez lorsque vous créez l'ENM.

Les WLAN connus sont des profils NWAM utilisés pour gérer la liste des réseaux sans fil connus auxquels vous vous êtes connecté précédemment. Pour plus d'informations, reportez-vous aux sections [“Description d'un ENM” à la page 52](#) et [“A propos des WLAN connus” à la page 52](#).

## Description d'un NCP

Un NCP définit la configuration réseau d'un système. Les NCU qui constituent un NCP précisent la manière de configurer les divers liens et interfaces réseau (par exemple, la ou les interfaces à activer), et les conditions dans lesquelles activer l'interface, ainsi que la méthode d'obtention de l'adresse IP de l'interface. Il existe deux types de NCP : automatique et défini par



l'utilisateur. Le profil NCP automatique est défini par le système et créé automatiquement par NWAM. Il ne peut pas être créé, modifié ni supprimé. Les NCP définis par l'utilisateur sont des profils que vous créez pour répondre aux besoins de votre configuration réseau. Un NCP défini par l'utilisateur peut être modifié ou supprimé par l'utilisateur.

Le NCP automatique est une représentation de tous les liens et interfaces présents dans le système. Le contenu du NCP automatique est modifié lorsque des périphériques réseau sont ajoutés ou supprimés. Cependant, il est impossible de modifier les préférences de configuration associées au NCP automatique. Le NCP automatique est créé pour procurer l'accès à un profil qui utilise DHCP et la configuration automatique d'adresse permettant d'obtenir des adresses IP pour le système. Ce profil met également en oeuvre une stratégie de sélection de lien, favorisant les liens câblés par rapport aux liens sans fil. Si la spécification d'une autre stratégie de configuration IP ou d'une autre stratégie de sélection de lien est nécessaire, vous devez créer des NCP définis par l'utilisateur supplémentaires sur votre système.

## Description d'une NCU

Les NCU sont les différents objets de configuration composant un NCP. Les NCU représentent les différents liens physiques et interfaces présents sur un système. Le processus de configuration d'un NCP défini par l'utilisateur comprend la création de NCU qui indiquent comment et dans quelles conditions chaque lien et interface doit être configuré(e).

Il existe deux types de NCU :

- **NCU de lien**

Les NCU de lien (par exemple, les périphériques physiques) sont des entités de couche 2 dans le modèle OSI (Open Systems Interconnection).

- **NCU d'interface**

Les NCU d'interface (plus précisément, les interfaces IP) sont des entités de couche 3 dans le modèle OSI.

Les NCU de lien représentent des liaisons de données. Il existe plusieurs classes de liaisons de données :

- Liens physiques (Ethernet ou Wi-Fi)
- Tunnels
- Groupement
- Réseaux locaux virtuels (VLAN)
- Cartes réseau virtuelles (VNIC)

---

**Remarque** – La mise en oeuvre NWAM actuelle inclut la prise en charge de la configuration réseau de base des liens physiques (Ethernet et Wi-Fi) *uniquement*. Bien qu'elles ne soient pas activement prises en charge par NWAM, plusieurs technologies de mise en réseau avancées (VNIC et pontage, par exemple) peuvent être configurées sur votre réseau sans qu'il soit nécessaire de désactiver la gestion de la configuration NWAM.

Cependant, si vous configurez votre système pour utiliser l'IPMP (IP Network Multipathing, multipathing sur réseau IP), il vous est impossible d'utiliser la gestion de configuration NWAM. Vous devez utiliser la configuration réseau classique. Pour plus d'instructions, reportez-vous à la section [“Procédure permettant de passer du mode de configuration réseau NWAM au mode de configuration réseau classique”](#) à la page 112.

---

## Description des NCP automatiques et définis par l'utilisateur

Le NCP automatique est un profil défini par le système, constitué d'une NCU de lien et d'une NCU d'interface pour chaque lien physique présent dans le système. La stratégie d'activation NCU dans ce NCP consiste à préférer des liens câblés et connectés par rapport aux liens sans fil, et de monter IPv4 et IPv6 sur chaque lien activé. DHCP est utilisé pour obtenir les adresses IPv4. La configuration automatique sans état et DHCP sont utilisés pour obtenir les adresses IPv6. Le NCP automatique change de façon dynamique lorsque de nouveaux liens sont insérés ou supprimés dans le système. Toutes les NCU correspondant au lien inséré ou supprimé sont également ajoutées ou supprimées en même temps. Le profil est automatiquement mis à jour par le démon `nwamd`.

Les NCP définis par l'utilisateur sont créés et gérés par celui-ci. Vous devez ajouter et supprimer explicitement les NCU dans le profil spécifié. Vous pouvez créer des NCU qui ne sont pas en corrélation avec des liens présents dans le système. Vous pouvez également supprimer des NCU qui ne sont pas en corrélation avec des liens présents dans le système. En outre, vous pouvez déterminer la stratégie pour le NCP défini par l'utilisateur. Par exemple, vous pouvez autoriser l'activation de plusieurs liens et interfaces sur le système à un moment donné, et définir des relations de dépendance différentes entre les NCU et les adresses IP statiques.

Pour obtenir des instructions détaillées sur la création d'un NCP défini par l'utilisateur et sur l'ajout ou la suppression de NCU pour ce NCP, reportez-vous à la section [“Création d'un NCP”](#) à la page 80.

## Description d'un profil d'emplacement

Un profil d'emplacement fournit des détails supplémentaires de mise en réseau après l'établissement de la connectivité IP de base. Les emplacements contiennent des informations de configuration réseau se composant d'un ensemble de propriétés associées à la configuration réseau sur l'ensemble du système.

Un profil d'emplacement se compose de certaines informations de configuration réseau (paramètres du pare-feu et du service de nommage, par exemple) appliqués conjointement, le cas échéant. En outre, étant donné qu'un emplacement ne correspond pas nécessairement à un emplacement physique, vous pouvez configurer plusieurs profils d'emplacement pour répondre à différents besoins de mise en réseau. Par exemple, un emplacement peut être utilisé lorsque vous êtes connecté à l'intranet de l'entreprise. Un autre emplacement peut être utilisé lorsque vous êtes connecté à Internet à l'aide d'un point d'accès sans fil situé dans votre bureau.

Par défaut, deux profils d'emplacement sont prédéfinis par le système :

- **NoNet**

L'emplacement NoNet présente des conditions d'activation très spécifiques. Ce profil est appliqué par NWAM à un système autonome lorsqu'aucune adresse IP n'a été affectée à une interface locale. Vous pouvez modifier l'emplacement NoNet après son activation initiale sur votre système. Une copie en lecture seule de l'emplacement NoNet d'origine est stockée sur le système, au cas où vous souhaiteriez restaurer les paramètres par défaut de cet emplacement.

- **Automatique**

L'emplacement Automatique est activé si des réseaux sont disponibles, mais qu'aucun autre profil d'emplacement ne le remplace. Vous pouvez modifier l'emplacement Automatique après son activation initiale sur votre système. Une copie en lecture seule de l'emplacement Automatique d'origine est stockée sur le système, au cas où vous souhaiteriez restaurer les paramètres par défaut de cet emplacement.

---

**Remarque** – Il ne faut pas confondre l'emplacement Automatique avec le NCP automatique. L'emplacement Automatique est un type de profil d'emplacement qui définit les propriétés réseau à l'échelle du système, une fois la configuration réseau initiale d'un système en place. Le NCP automatique spécifie la configuration réseau de lien et d'interface d'un système.

---

Les emplacements définis par l'utilisateur sont des profils que vous créez avec des valeurs que vous spécifiez pour la configuration réseau à l'échelle du système. Les emplacements définis par l'utilisateur sont identiques à ceux définis par le système, à ceci près que les emplacements définis par l'utilisateur sont configurés avec des valeurs que vous définissez, tandis que les emplacements définis par le système ont des valeurs prédéfinies.

Pour plus d'informations sur la création des emplacements définis par l'utilisateur, reportez-vous à la section [“Création d'un profil d'emplacement”](#) à la page 88.

## Description d'un ENM

Les ENM sont des profils appartenant à des applications externes à NWAM. Ces applications peuvent créer et modifier la configuration réseau. Des ENM sont inclus dans la conception NWAM pour créer et supprimer une configuration réseau personnalisée, qui n'est pas un profil d'emplacement ni un profil NCP. Un ENM peut également être défini comme service ou application qui modifie directement la configuration réseau après son activation ou sa désactivation. Vous pouvez configurer NWAM pour activer et désactiver des ENM dans les conditions que vous précisez. Contrairement à un profil d'emplacement ou NCP où un seul des types de profil peut être actif sur le système à un moment donné, plusieurs ENM sont susceptibles d'être actifs simultanément sur le système. Les ENM qui sont actifs sur un système à un moment donné ne sont pas nécessairement dépendants du profil d'emplacement ou NCP qui est également activé sur le système en même temps.

Bien qu'il existe plusieurs services et applications externes pour lesquels vous pouvez créer un ENM, l'exemple type est l'application VPN (Virtual Private Network, réseau privé virtuel). Après l'installation et la configuration de VPN sur votre système, vous pouvez créer un ENM qui active et désactive automatiquement l'application dans les conditions que vous précisez.

---

**Remarque** – Il est important de bien comprendre que NWAM ne possède pas la capacité d'en savoir plus automatiquement sur les applications externes capables de modifier directement la configuration réseau d'un système. Pour gérer l'activation ou la désactivation d'une application VPN ou d'une application ou d'un service externe, vous devez tout d'abord installer l'application, puis créer un ENM à l'aide de la CLI ou de l'interface graphique NWAM.

---

Les informations persistantes sur la configuration réseau réalisée par un ENM ne sont pas stockées ni suivies par NWAM de la même manière que le sont les informations sur un profil d'emplacement ou NCP. Cependant, NWAM est capable de détecter une configuration réseau lancée en externe, puis en fonction des modifications de configuration apportées au système par un ENM, de réévaluer le profil d'emplacement qui doit être actif, puis de l'activer. Il peut s'agir, par exemple, de basculer vers un emplacement activé de manière conditionnelle lorsqu'une certaine adresse IP est en cours d'utilisation. Si le service `svc:/network/physical:default` est redémarré à tout moment, la configuration réseau spécifiée par le NCP actif est rétablie. Les ENM sont également redémarrés, démolissant et recréant éventuellement la configuration réseau au cours du processus.

Pour plus d'informations sur la création et la modification des propriétés d'un ENM, reportez-vous à la section [“Création d'un profil ENM” à la page 93](#).

## A propos des WLAN connus

Les WLAN connus sont des objets de configuration que NWAM utilise dans le cadre de la gestion des réseaux sans fil connus du système. NWAM gère une liste générale de ces réseaux

sans fil connus. Ces informations servent ensuite à déterminer l'ordre dans lequel NWAM tente de se connecter aux réseaux sans fil disponibles. Si un réseau sans fil présent dans la *liste des WLAN connus* est disponible, NWAM s'y connecte automatiquement. Si deux réseaux sans fil connus ou plus sont disponibles, NWAM tente de se connecter au réseau sans fil doté de la priorité la plus élevée (numéro le plus bas). Tout nouveau réseau sans fil auquel NWAM se connecte est automatiquement ajouté en tête de la liste des WLAN connus et devient le réseau sans fil à la priorité la plus élevée.

Les WLAN connus sont sélectionnés dans l'ordre de priorité, affectée par un entier non signé. Dans la liste des WLAN connus, la priorité est d'autant plus élevée que le nombre est inférieur. La première fois que vous vous connectez à un réseau sans fil, NWAM ajoute automatiquement ce WLAN à la liste. Lorsqu'un nouveau WLAN est ajouté, il endosse la priorité la plus élevée dans cette liste. Le comportement par défaut NWAM consiste à préférer des WLAN plus récemment connectés par rapport aux WLAN auxquels vous vous êtes connecté précédemment. Les WLAN connus ne peuvent partager la même priorité à aucun moment. Si un nouveau WLAN est ajouté dans la liste avec la même valeur de priorité qu'un WLAN existant, une valeur de priorité inférieure est attribuée à ce dernier. Par la suite, la valeur de priorité de tous les autres WLAN de la liste est remplacée dynamiquement par une valeur de priorité inférieure.

Un ou plusieurs noms de touche peuvent également être associés à un WLAN connu. Les *noms de touche* vous permettent de créer vos propres touches à l'aide de la commande `dladm create-secobj`. Vous pouvez ensuite associer ces touches à des WLAN en ajoutant les noms d'objet sécurisés à la propriété `keyname` de WLAN connu. Pour plus d'informations, reportez-vous à la page de manuel [dladm\(1M\)](#).

Pour plus d'informations sur l'utilisation des utilitaires de ligne de commande NWAM dans le cadre de la gestion des WLAN, reportez-vous à la section [“Exécution d'une analyse sans fil et connexion aux réseaux sans fil disponibles”](#) à la page 121.

## Données de configuration NWAM

En réalité, il existe deux référentiels de configuration sur le système : le référentiel de profil NWAM, stocké dans le répertoire `/etc/nwam` et le référentiel de configuration traditionnel, qui comprend les fichiers `/etc/ipadm/ipadm.conf` et `/etc/dladm/data-link.conf`, ainsi que d'autres fichiers de configuration associés aux services réseau.

Lorsque NWAM gère la configuration réseau, il fonctionne principalement à partir de son propre référentiel. La configuration d'interface qui est stockée dans le fichier `/etc/ipadm/ipadm.conf` est ignorée. NWAM configure des interfaces et liens physiques directement sur la base de données NCP.

Les données de profil d'emplacement sont lues à partir du référentiel de profils NWAM. Lorsqu'un emplacement est activé, cette configuration est appliquée au système en cours

d'exécution dans la plupart des cas en définissant les propriétés de service SMF appropriées et en redémarrant les services correspondants pour appliquer les changements de configuration. Cette action remplace les valeurs existantes de ces propriétés de service.

Dans la mesure où NWAM écrase les données de configuration héritées lors de l'application de profils d'emplacement, les configurations qui pourraient être écrasées sont enregistrées au démarrage. NWAM restaure ensuite cette configuration lors de l'arrêt. Bien qu'il ne s'agisse pas d'un emplacement applicable dans le cadre de l'opération NWAM, ces données sont appelées des données d'*emplacement hérité*.

Les valeurs des propriétés des profils réseau définis par le système et des profils réseau définis par l'utilisateur ci-dessous sont stockées dans le référentiel NWAM :

- NCP : contient des valeurs pour le NCP automatique et tous les NCP définis par l'utilisateur.
- NCU : contient des valeurs pour les NCU autant de lien que d'interface.
- Emplacements : contient des valeurs pour les trois types d'emplacement définis par le système, ainsi que des valeurs pour tous les emplacements définis par l'utilisateur.
- ENM : contient des informations sur les applications.
- WLAN connus : contient des informations à propos des réseaux sans fil auxquels vous pouvez être connecté automatiquement.

Des données de configuration pour chaque NCP sont stockées de façon permanente sous forme de fichier dans le répertoire `/etc/nwam` au format `ncp- name`. On compte un fichier par NCP, dont les entrées représentent chaque NCU. Par exemple, le fichier pour le NCP automatique est nommé `ncp-Automatic.conf`. Tous les fichiers NCP sont stockés dans le répertoire `/etc/nwam`.

Les propriétés d'emplacement sont stockées dans le fichier `/etc/nwam/loc.conf`.

Les propriétés ENM sont stockées dans le fichier `/etc/nwam/enm.conf`. Les WLAN connus sont stockés dans le fichier `/etc/nwam/known-wlan.conf`. Ce format de fichier est similaire à celui de `/etc/dladm/datalink.conf`.

---

**Remarque** – Bien qu'il soit possible de modifier des profils réseau en éditant directement les fichiers dans le référentiel de profils NWAM, la méthode appropriée pour modifier un profil consiste à utiliser la commande `net cfg` ou les panneaux de configuration de l'interface graphique NWAM. Le format et l'utilisation des fichiers sont susceptibles de changer dans les futures versions. Reportez-vous à la section [“Définition et modification des valeurs de propriétés pour un profil”](#) à la page 100.

---

# Valeurs de propriété de NCU

Les NCU, objets de configuration individuels d'un NCP, représentent les liens et interfaces d'un système. Les propriétés générales des deux types de NCU (lien et interface), ainsi que les propriétés spécifiques à chaque type de NCU, sont stockées dans le référentiel de profils NWAM. Les propriétés `type`, `class` et `parent` sont définies à la création de la NCU et ne peuvent pas être modifiées par la suite. En outre, vous ne pouvez pas modifier directement une propriété activée. La propriété est modifiée indirectement en activant ou désactivant une NCU à l'aide de la commande `netadm`.

Le NCP automatique est constitué d'une NCU de lien pour chaque lien physique détecté dans le système et d'une NCU d'interface montée sur chaque lien. Le NCP automatique change de façon dynamique lors de l'insertion de liens physiques supplémentaires. A mesure que des nouveaux liens sont insérés, une NCU de lien et la NCU d'interface correspondante sont créées pour chacun d'eux. Les tableaux suivants définissent les valeurs affectées à chaque NCU constituant le NCP automatique.

**Remarque** – Les propriétés de cette table sont répertoriées dans l'ordre de leur apparition lorsque vous affichez les propriétés NCU du NCP automatique. Certaines valeurs s'appliquent à chaque type de NCU.

TABLEAU 3-1 Propriétés de la NCU de lien du NCP automatique

Propriétés	Valeur de la NCU de lien
<code>type</code>	<code>link</code>
<code>class</code>	<code>phys</code>
<code>parent</code>	<code>Automatic</code>
<code>enabled</code>	<code>true</code>
<code>activation-mode</code>	<code>prioritized</code>
<code>priority-group</code>	<code>0</code> (pour liens 802.3) ou <code>1</code> (pour liens 802.11)
<code>priority-group-mode</code>	<code>shared</code> (pour liens 802.3) ou <code>exclusive</code> (pour liens 802.11)
<code>mac-address</code>	Affecté par le matériel
<code>autopush</code>	N/D
<code>MTU</code>	N/D

TABLEAU 3-2 Propriétés de la NCU d'interface du NCP automatique

Propriétés	Valeur de la NCU d'interface
type	interface
class	IP
parent	Automatic
enabled	true
ip-version	ipv4, ipv6
ipv4-addrsrc	dhcp
ipv4-static-addr	N/D
ipv6-addrsrc	dhcp, autoconf
ipv6-static-addr	N/D

## Valeurs de propriété des emplacements définis par le système

Le tableau suivant présente les valeurs de propriété par défaut pour l'emplacement Automatique, qui est un profil défini par le système. Vous pouvez modifier ces valeurs, à l'exception des propriétés `activation-mode` et `enabled`. Le système active toujours l'emplacement Automatique lorsqu'une interface au moins est active et qu'aucun autre profil d'emplacement ne le remplace.

TABLEAU 3-3 Propriétés des emplacements définis par le système

Propriétés	Valeur
name	Automatic
activation-mode	system
enabled	system modifiée, le cas échéant
conditions	N/D
default-domain	N/D
nameservices	dns
nameservices-config-file	/etc/nsswitch.dns
dns-nameservice-configsrc	dhcp
dns-nameservice-domain	N/D



TABLEAU 3-3 Propriétés des emplacements définis par le système (Suite)

Propriétés	Valeur
dns-nameservice-servers	N/D
dns-nameservice-search	N/D
nis-nameservice-configsrc	N/D
nis-nameservice-servers	N/D
ldap-nameservice-configsrc	N/D
ldap-nameservice-servers	N/D
nfsv4-domain	N/D
ipfilter-config-file	N/D
ipfilter-v6-config-file	N/D
ipnat-config-file	N/D
ippool-config-file	N/D
ike-config-file	N/D
ipsecpolicy-config-file	N/D

Le tableau suivant contient les propriétés prédéfinies de l'emplacement NoNet. Notez que vous pouvez modifier ces valeurs, à l'exception des propriétés activation-mode et enabled. Le système active toujours l'emplacement NoNet lorsque aucune interface n'est active.

TABLEAU 3-4 Propriétés de l'emplacement NoNet

Propriétés	Valeur
name	NoNet
activation-mode	system
enabled	system modifiée, le cas échéant
conditions	N/D
default-domain	N/D
nameservices	files
nameservices-config-file	/etc/nsswitch.files
dns-nameservice-configsrc	N/D
dns-nameservice-domain	N/D

TABLEAU 3-4 Propriétés de l'emplacement NoNet (Suite)	
Propriétés	Valeur
dns-nameservice-servers	N/D
dns-nameservice-search	N/D
nis-nameservice-configsrc	N/D
nis-nameservice-servers	N/D
ldap-nameservice-configsrc	N/D
ldap-nameservice-servers	N/D
nfsv4-domain	N/D
ipfilter-config-file	/etc/nwam/loc/NoNet/ipf.conf, qui se compose des règles de filtre IP bloquant tout le trafic non-loopback, hormis une quantité minimale de trafic réseau nécessaire à NWAM pour effectuer une configuration réseau, notamment l'affectation d'adresse DHCP.
ipfilter-v6-config-file	/etc/nwam/loc/NoNet/ipf6.conf, qui se compose des règles de filtre IP, comme décrit pour ipfilter-config-file.
ipnat-config-file	N/D
ippool-config-file	N/D
ike-config-file	N/D
ipsecpolicy-config-file	N/D

Pour plus d'informations sur les propriétés d'emplacement, y compris les propriétés constituant des emplacements définis par l'utilisateur, reportez-vous à la page de manuel [netcfg\(1M\)](#).

## Activation des profils NWAM

Les NCP, profils d'emplacement et ENM ont des propriétés `activation-mode`. Les valeurs autorisées pour chaque type de profil diffèrent. En outre, la validation de la propriété `activation-mode` est différente pour chaque type de profil, à l'instar des conditions dans lesquelles chaque profil est activé.

Pour les emplacements définis par le système (Automatique et NoNet), la valeur de la propriété `activation-mode` est définie sur `system`, ce qui signifie que l'emplacement peut uniquement être activé par le système, lorsque les conditions prédéterminées par le système sont vérifiées pour l'emplacement indiqué.

Pour les emplacements définis par l'utilisateur, vous pouvez définir les propriétés activation-mode et conditions sur manual, conditional-any ou conditional-all. Pour plus d'informations, reportez-vous à la section "[Critères de sélection de l'activation d'emplacement](#)" à la page 61.

Un profil d'emplacement peut être activé manuellement à l'aide de la commande `netadm` ou de l'interface graphique NWAM. Si vous n'activez pas explicitement un emplacement, le démon NWAM `nwamd` vérifie les règles d'activation pour tous les profils d'emplacement activés conditionnellement et activés par le système, puis choisit l'emplacement qui correspond le mieux à l'environnement réseau actuel.

NWAM utilise un algorithme pour déterminer la "meilleure correspondance" lors du choix de l'emplacement. S'il n'existe pas de correspondance adéquate pour un emplacement, l'emplacement Automatique est activé. Lorsque vous modifiez l'environnement réseau, le démon `nwamd` réévalue constamment la sélection de l'emplacement pour déterminer la meilleure correspondance. Cependant, si vous activez explicitement un profil d'emplacement à l'aide de la commande `netadm` (un emplacement activé manuellement ou un emplacement activé conditionnellement), il reste actif jusqu'à ce que vous le désactiviez explicitement ou que vous activiez un autre emplacement. Dans ce cas, les changements dans l'environnement réseau n'entraînent pas une modification des profils d'emplacement, qu'une meilleure correspondance soit disponible ou pas. En réalité, la spécification explicite de l'emplacement actuel en fait la meilleure correspondance possible. Pour plus d'instructions sur l'activation et la désactivation des profils, reportez-vous à la section "[Activation et désactivation des profils](#)" à la page 118.

## Stratégie d'activation NCP

NWAM permet de spécifier une stratégie NCP, qui détermine les conditions d'activation des NCU. La stratégie NCP est appliquée par le biais de l'utilisation des propriétés et conditions, qui peuvent être spécifiées pour chaque NCU. Voici deux exemples de stratégies que vous pouvez spécifier : "Préférer les connexions câblées aux connexions sans fil" ou "Activer une interface à la fois". Le moment et le mode d'activation des NCP sont définis dans les propriétés de chaque type de NCU.

---

**Remarque** – Une NCU d'interface doit toujours être associée à une NCU de lien sous-jacente. Chaque NCU d'interface devient active lorsque son NCU de lien associée est activée. Vous pouvez remplacer le comportement par défaut d'une NCU à l'aide de la commande `netadm`. Toutefois, la dépendance par rapport à la NCU de lien sous-jacente ne peut jamais être supprimée. Par exemple, si vous activez une NCU d'interface sans activer son NCU de lien associée, l'interface n'est mise en ligne qu'à l'activation de son NCU sous-jacente.

---

## Exemple de stratégie NCP

Dans l'exemple ci-dessous, les propriétés NCU sont définies pour le moment où la stratégie NCP doit indiquer que tous les liens câblés sont activés, et qu'une connexion sans fil doit être utilisée uniquement si aucune connexion câblée n'est disponible.

Pour tous les liens physiques :

- Type de NCU : link
- Classe de NCU : phys
- activation-mode: prioritized
- priority-group: 0 pour connexion câblée ; 1 pour connexion sans fil
- priority-mode: shared pour connexion câblée ; exclusive pour connexion sans fil

Dans l'exemple suivant, les propriétés NCU sont définies en fonction d'une stratégie NCP qui spécifie qu'il n'y a qu'un seul lien actif sur le système à un moment donné, et qu'une connexion câblée est préférée à une connexion sans fil.

Pour tous les liens physiques :

- Type de NCU : link
- Classe de NCU : phys
- activation-mode: prioritized
- priority-group: 0 pour connexion câblée ; 1 pour connexion sans fil
- priority-mode: exclusive

## Propriétés d'activation de NCU

L'activation des connexions réseau est définie dans les propriétés NCU de lien. Les propriétés suivantes permettent de définir la stratégie d'activation des NCU :

- Propriété activation-mode

Cette propriété peut être définie sur manual ou prioritized.

- manual : l'activation NCU est gérée par l'administrateur. Vous pouvez utiliser l'interface graphique ou la CLI NWAM pour activer ou désactiver la NCU. Si la propriété activation-mode est définie sur manual, les valeurs qui sont définies à la fois pour les propriétés NCU priority-group et priority-mode sont ignorées.
- prioritized : la NCU est activée en fonction des valeurs définies dans les propriétés priority-group et priority-mode pour la NCU spécifiée. La propriété enabled est toujours true (vraie) pour les NCU prioritized.

L'activation par ordre de priorité permet d'activer des groupes de liens simultanément. Ce mode d'activation permet également de préférer un ou plusieurs liens par rapport à d'autres. La propriété priority-group affecte un niveau de priorité numérique à un lien

donné. Tous les liens d'un même niveau de priorité sont examinés en tant que groupe. La propriété `priority-mode` définit le nombre de membres qui peuvent ou doivent être disponibles pour que le groupe soit activé.

- Propriété `enabled` (activation-mode définie sur `manual` )

La valeur de cette propriété peut être `true` ou `false`. Vous ne pouvez pas définir la valeur de cette propriété. La valeur reflète plutôt l'état actuel d'une NCU activée manuellement, qui peut être modifiée à l'aide de la commande `netadm` ou de l'interface graphique NWAM.

- La propriété `priority-group` (activation-mode est définie sur `prioritized`)

La valeur est numérique. Zéro (0) indique le niveau de priorité le plus élevé. Les valeurs négatives ne sont pas valides.

Parmi tous les `priority-groups` disponibles, seules les NCU dans la `priority-group` la plus élevée sont activées. Lorsque plusieurs NCU avec la même priorité sont disponibles, le comportement d'activation est défini par la propriété `priority-mode`. Le numéro de priorité n'est pas une valeur absolue. Il peut changer lors de la mise à jour du référentiel NCP.

---

**Remarque** – L'ordre de priorité est strictement appliqué.

---

- La propriété `priority-mode` (activation-mode est définie sur `prioritized`)

La propriété est définie lorsqu'une valeur pour la propriété `priority-group` a été spécifiée.

Les valeurs de cette propriété sont les suivantes :

- `exclusive` : spécifie que seule une NCU dans `priority-group` peut être active à un moment donné. NWAM active la première NCU disponible dans le groupe de priorités et ignore les autres.
- `shared` : spécifie que plusieurs NCU dans le groupe de priorité peuvent être actives en même temps. Toutes les NCU disponibles dans le groupe de priorité sont activées.
- `all` : spécifie que toutes les NCU dans le groupe de priorité doivent être disponibles au groupe de priorité pour être considérées comme disponibles et par conséquent devenir actives.

## Critères de sélection de l'activation d'emplacement

Chaque profil d'emplacement contient des propriétés qui définissent des critères d'activation. Ces propriétés spécifient des informations sur les conditions dans lesquelles un emplacement est activé. NWAM réévalue en permanence les critères de sélection pour tous les emplacements configurés, déterminant chaque fois l'emplacement doté des critères qui correspondent le mieux à l'environnement réseau actuel. Si des modifications surviennent dans l'environnement

réseau actuel aboutissent à une meilleure correspondance, NWAM désactive le profil d'emplacement actuel et active le profil d'emplacement constituant la meilleure correspondance pour le nouvel environnement.

Les critères de sélection déterminant le moment et la méthode d'activation de l'emplacement sont spécifiés par les propriétés suivantes :

- `activation-mode`
- `conditions`

La propriété `activation-mode` est définie sur l'une des valeurs possibles suivantes :

- `manual`
- `conditional-any`
- `conditional-all`
- `system`

**Remarque** – La valeur `system` de la propriété `activation-mode` peut uniquement être affectée à des emplacements fournis par le système : les emplacements Automatique et NoNet. La valeur `system` indique que le système détermine le moment où ces emplacements sont activés.

Si la propriété `activation-mode` est définie sur `conditional-any` ou `conditional-all`, la propriété `conditions` contient une ou des expressions conditionnelles définies par l'utilisateur. Chaque expression contient une condition qui peut être attribuée à une valeur booléenne, par exemple, "`ncu ip:net0 is-not active`".

Si la propriété `activation-mode` est définie sur `conditional-any`, la condition est vérifiée si l'une des conditions est vraie.

Si la propriété `activation-mode` est définie sur `conditional-all`, la condition est vérifiée uniquement si *toutes* les conditions sont vraies. Les critères et les opérations permettant de construire les chaînes de condition sont définis dans le tableau suivant.

TABLEAU 3–5 Critères et opérations pour la construction des chaînes de condition

Type d'objet/Attribut	Condition	Objet
<code>ncu</code> , <code>enm</code> , <code>loc</code>	Est/N'est pas actif	Nom
<code>ssid</code>	Est/N'est pas Contient/Ne contient pas	Chaîne de nom
<code>bssid</code>	Est/N'est pas	Chaîne bssid
<code>ip-address</code>	Est/N'est pas	Adresses IPv4 ou IPv6
<code>ip-address</code>	Est dans la plage/N'est pas dans la plage	Adresse IPv4 ou IPv6 plus masque réseau/prefixlen

TABLEAU 3-5 Critères et opérations pour la construction des chaînes de condition (Suite)

Type d'objet/Attribut	Condition	Objet
advertised-domain	Est/N'est pas	Chaîne de nom
	Contient/Ne contient pas	
system-domain	Est/N'est pas	Chaîne de nom
	Contient/Ne contient pas	

**Remarque** – La propriété `ssid` représente un ESSID (Extended Server Set Identifier), qui est le nom de réseau d'un LAN sans fil (WLAN). La propriété `bssid` représente un BSSID (Basic Service Set Identifier), qui est l'adresse MAC d'un point d'accès sans fil (WAP) donné ou un point d'accès quelconque.

Notez la différence entre les attributs `advertised-domain` et `system-domain`. Le domaine annoncé est découvert par le biais de communications externes, par exemple, les noms de domaine `DNSdomain` ou `NISdomain`, qui sont annoncés par un serveur DHCP. Cet attribut est utile pour l'activation conditionnelle des emplacements, par exemple, si le domaine annoncé est `mycompany.com`, l'emplacement `work` est activé. L'attribut `system-domain` est le domaine affecté au système. Il s'agit de la valeur qui est renvoyée par la commande `domainname`. Cet attribut est utile pour l'activation conditionnelle des ENM, car il ne deviendra vrai qu'après l'activation de l'emplacement et la configuration du système pour un domaine particulier. Pour plus d'informations, reportez-vous à la page de manuel [domainname\(1M\)](#).

Pour plus d'informations sur les propriétés d'emplacement, reportez-vous à la section “Description d'un profil d'emplacement” à la page 51.

## Configuration de profils à l'aide de la commande netcfg

La commande `netcfg`, décrite dans la page de manuel [netcfg\(1M\)](#), permet de configurer les propriétés et valeurs des profils réseau.

Vous pouvez utiliser la commande `netcfg` pour effectuer les tâches suivantes :

- Création ou modification d'un profil défini par l'utilisateur

**Remarque** – Vous ne pouvez pas créer ni détruire un profil défini par le système.

- Création de la liste de tous les profils qui existent sur un système et de leurs valeurs de propriété
- Création de la liste de toutes les valeurs de propriété et des ressources d'un profil spécifié

- Affichage de chaque propriété associée à un profil
- Définition ou modification d'une ou de toutes les propriétés d'un profil spécifié
- Exportation de la configuration actuelle d'un profil défini par l'utilisateur vers la sortie standard ou un fichier

---

**Remarque** – Vous ne pouvez pas exporter un profil défini par le système.

---

- Suppression de toutes les modifications qui ont été apportées à un profil et rétablissement de la configuration précédente de ce profil
- Vérification de la configuration correcte d'un profil

Vous pouvez utiliser l'interface utilisateur netcfg en mode interactif, mode ligne de commande ou mode fichier de commande. Dans la mesure où la commande netcfg est hiérarchique, elle est mieux comprise lorsqu'elle est utilisée en mode interactif.

Le concept de *portée* est utilisé pour la commande netcfg. Lorsque vous utilisez la commande en mode interactif, la portée dans laquelle vous vous trouvez à un moment donné dépend du type de profil et de la tâche que vous effectuez. Lorsque vous saisissez la commande netcfg dans une fenêtre de terminal, une invite s'affiche au niveau de la *portée générale*.

A partir de là, vous pouvez utiliser les sous-commandes select ou create pour afficher, modifier ou créer les profils de haut niveau suivants :

- NCP
- Emplacements
- ENM
- WLAN connus

Avant de créer ou de sélectionner un profil, l'invite interactive netcfg s'affiche au format suivant :

```
netcfg>
```

Une fois un profil créé ou sélectionné, l'invite interactive netcfg s'affiche comme suit :

```
netcfg:profile-type:profile-name>
```

---

**Remarque** – En mode ligne de commande, vous devez taper la commande complète sur une seule ligne. Les modifications que vous apportez à un profil sélectionné à l'aide de la commande netcfg en mode ligne de commande sont validées pour le référentiel permanent dès que vous avez fini de saisir la commande.

---



Pour obtenir des instructions détaillées sur l'utilisation de la commande `netcfg`, reportez-vous au [Chapitre 4, “Configuration de profil NWAM \(tâches\)”](#). Pour plus d'informations sur la commande `netcfg`, reportez-vous à la page de manuel [netcfg\(1M\)](#).

## Mode interactif netcfg

La sélection ou la création d'un profil de haut niveau en mode interactif `netcfg` génère une invite de commande qui s'affiche dans la *portée* des profils d'emplacement et ENM. Par exemple :

```
netcfg> select loc foo
netcfg:loc:foo>
```

Si un NCP est sélectionné, l'invite de commande s'affiche dans la *portée* NCP. Dans la portée NCP, il est possible de sélectionner ou de créer une NCU. La sélection ou la création d'une NCU génère une invite de portée de profil pour la NCU sélectionnée. Dans cette portée, toutes les propriétés associées au profil sélectionné peuvent être affichées et définies, comme indiqué dans l'exemple suivant où le NCP User a été sélectionné en premier, puis une NCU a été créée dans la portée NCP. Cette action a généré la portée de profil pour la nouvelle NCU. Dans cette portée, les propriétés de la NCU peuvent être affichées ou définies :

```
netcfg> select ncp User
netcfg:ncp:User> create ncu phys net2
Created ncu 'net2'. Walking properties ...
activation-mode (manual) [manual|prioritized]>
```

Dans une portée donnée, l'invite de commande indique le profil sélectionné. Toutes les modifications que vous apportez au profil dans cette portée peuvent être *validées*, ce qui signifie qu'elles sont enregistrées dans le référentiel permanent. Les modifications sont validées implicitement lorsque vous sortez de la portée. Si vous ne souhaitez pas valider les modifications que vous avez apportées au profil sélectionné, vous pouvez rétablir le dernier état validé pour ce profil. Cette action restaure toutes les modifications que vous avez apportées au profil à ce niveau. Les sous-commandes `reset` et `cancel` fonctionnent de la même manière.

## Mode de ligne de commande netcfg

En mode ligne de commande, les sous-commandes qui ont une incidence sur une propriété ou un profil sélectionné doivent être exécutées dans la portée particulière où la propriété ou le profil sélectionné existe. Par exemple, pour obtenir la valeur d'une propriété d'une NCU, vous devez exécuter la sous-commande `get` dans la portée de cette NCU particulière. En mode interactif `netcfg`, il est relativement facile de comprendre la syntaxe à utiliser pour cette commande. Toutefois, en mode ligne de commande, la syntaxe risque d'être moins évidente.

Par exemple, pour obtenir la valeur d'une propriété "foo", attribut d'une NCU appelée `myncu` dans le NCP User, vous devez utiliser la syntaxe suivante :

```
$ netcfg "select ncp User; select ncu ip myncu; get foo"
```

Dans cet exemple, notez les informations suivantes :

- Les portées sont séparées par un point-virgule.
- La sous-commande `select` est émise à chaque portée, une fois à la portée générale et une fois à la portée de profil.
- La sous-commande `get` est utilisée dans la portée dans laquelle la propriété "foo" existe.
- Des guillemets droits sont requis pour éviter que le shell n'interprète les points-virgules.

## Mode fichier de commande netcfg

En mode fichier de commande, les informations de configuration sont extraites d'un fichier. La sous-commande `export` permet de générer ce fichier. La configuration peut alors être imprimée sur la sortie standard ou l'option `-f` peut être utilisée pour spécifier un fichier de sortie. La sous-commande `export` peut également être utilisée de façon interactive. Pour plus d'informations, reportez-vous à la section [“Sous-commandes netcfg prises en charge” à la page 66](#).

## Sous-commandes netcfg prises en charge

Les sous-commandes `netcfg` suivantes sont prises en charge en mode interactif et en mode ligne de commande. Notez que certaines sous-commandes n'ont pas la même sémantique dans chaque portée. Si une sous-commande ne peut pas être utilisée dans un certain mode, elle a été notée dans la description de la sous-commande.

- `cancel`  
Met fin à la spécification de profil actuelle sans valider les modifications du stockage persistant, puis passe à la portée suivante, située un niveau plus haut.
- `clear prop-name`  
Efface la valeur de la propriété spécifiée.
- `commit`  
Valide le profil dans le stockage persistant. La configuration doit être correcte pour être validée. Par conséquent, cette opération exécute également automatiquement une commande `verify` sur le profil ou l'objet. L'opération `commit` s'effectue automatiquement dès que vous quittez la portée actuelle à l'aide de la sous-commande `end` ou `exit`.
- `create [ -t template ] object-type [ class ] object-name`  
Crée un profil en mémoire avec le type et le nom spécifié. L'option `-t template` spécifie que le nouveau profil est identique à *template*, où *template* est le nom d'un profil existant du même type. Si l'option `-t` n'est pas utilisée, le nouveau profil est créé avec les valeurs par défaut.

- `destroy -a`  
Supprime tous les profils définis par l'utilisateur de la mémoire et du stockage persistant.
- `destroy object-type [ class ] object-name`  
Supprime le profil défini par l'utilisateur spécifié dans la mémoire et le stockage persistant.




---

**Attention** – Cette opération est immédiate et n'a pas besoin d'être validée. La destruction d'un profil ne peut pas être annulée.

---

- `end`  
Met fin à la spécification de profil actuelle et procède à la portée suivante, située un niveau plus haut. Le profil actuel est vérifié et validé avant que ne prenne fin l'opération de modification. Si l'une des opérations, `verify` ou `commit`, échoue, un message d'erreur s'affiche. Vous avez alors la possibilité de mettre fin à l'opération sans valider les modifications en cours. Vous pouvez également rester dans la portée actuelle et poursuivre la modification du profil.
- `exit`  
Quitte la session interactive `netcfg`. Le profil actuel est vérifié et validé avant que la session en cours ne se termine. Si l'une des opérations, `verify` ou `commit`, échoue, un message d'erreur s'affiche. Vous avez alors la possibilité de mettre fin à la session sans valider les modifications en cours. Vous pouvez également rester dans la portée actuelle et poursuivre la modification du profil.
- `export [ -d ] [ -f output-file ] [ object-type [ class ] object-name ]`  
Imprime la configuration actuelle à la portée actuelle ou spécifiée sur la sortie standard ou dans un fichier spécifié avec l'option `-f`. L'option `-d` génère la sous-commande `destroy -a` en tant que la première ligne de la sortie. Cette sous-commande génère une sortie dans un format adapté pour une utilisation dans un fichier de commandes.

---

**Remarque** – Les profils définis par le système (NCP automatique et emplacements Automatique, NoNet et Hérité) ne peuvent pas être exportés.

---

- `get [ -V ] prop-name`  
Obtient la valeur actuelle en mémoire de la propriété spécifiée. Par défaut, la valeur et le nom de la propriété sont imprimés. Si l'option `-V` est spécifiée, seule la valeur de la propriété est imprimée.
- `help [ subcommand ]`  
Affiche l'aide générale ou l'aide sur un sujet spécifique.
- `list [-a] [object-type [ class ] object-name ]`

Répertorie tous les profils, paires propriété-valeur et ressources qui seront utilisés dans la portée actuelle ou spécifiée. Si l'option `-a` est spécifiée, toutes les propriétés sont répertoriées, y compris celles qui seront ignorées, en fonction des paramètres en cours.

- `revert`

Supprime les modifications en cours qui ont été apportées à un profil, puis rétablit les valeurs à partir du stockage persistant.

- `select object-type [ class ] object-name`

Sélectionne l'objet spécifié.

- `set prop-name= value`

Définit la valeur actuelle en mémoire de la propriété spécifiée.

Si elle est effectuée en mode ligne de commande, la modification est également validée immédiatement dans le stockage persistant.

Le séparateur des propriétés à valeurs multiples est une virgule ( , ). Si une valeur spécifique d'une propriété donnée contient une virgule, elle doit être précédée d'une barre oblique inverse ( \ ). Les virgules dans les propriétés à valeur unique ne sont pas interprétées comme des séparateurs et n'ont pas besoin d'être précédées d'une barre oblique inverse.

- `verify`

Vérifie que la configuration de l'objet ou du profil en mémoire actuel est correcte.

- `walkprop [ -a ]`

"Parcourt" chaque propriété associée au profil en cours. Pour chaque propriété, le nom et la valeur en cours sont affichés. Une invite est fournie pour vous permettre de modifier la valeur en cours. Si une propriété n'est pas utilisée, en fonction des valeurs définies précédemment, elle n'est pas affichée. Par exemple, si la propriété `ipv4-addrsrc` est définie sur `static`, la propriété `ipv4-addr` n'est pas utilisée, et n'est pas parcourue ni répertoriée, sauf si vous spécifiez l'option `-a`.

Lorsqu'elle est utilisée, l'option `-a` itère toutes les propriétés disponibles pour l'objet ou le profil spécifié.

Le séparateur des propriétés à valeurs multiples est une virgule ( , ). Si une valeur individuelle d'une propriété donnée contient une virgule, elle doit être précédée d'une barre oblique inverse ( \ ). Les virgules dans les propriétés à valeur unique ne sont pas interprétées comme des séparateurs et n'ont pas besoin d'être précédées d'une barre oblique inverse.

---

**Remarque** – Cette sous-commande est utile lorsqu'elle est utilisée en mode interactif uniquement.

---

Pour obtenir des informations relatives aux tâches, reportez-vous au [Chapitre 4](#), "Configuration de profil NWAM (tâches)".

# Administration des profils à l'aide de la commande netadm

La commande `netadm` est utilisée pour administrer et obtenir l'état des profils (NCP, emplacements, ENM et WLAN) et des NCU, les différents objets de configuration qui composent un NCP. En outre, vous pouvez utiliser la commande `netadm` pour interagir avec le démon NWAM (`nwamd`) en l'absence d'une interface graphique. Pour plus d'informations sur `netadm`, reportez-vous à la page de manuel [netadm\(1M\)](#).

Les sous-commandes `netadm` suivantes sont prises en charge :

- `enable [ -p profile-type ] [ -c ncu-class ] profile-name`  
Active le profil spécifié. Si le nom de profil n'est pas unique, le type de profil doit être spécifié. Si le type de profil est `ncu` et que le nom n'est pas unique (par exemple, s'il existe à la fois une `ncu` de lien et d'interface portant le même nom), les deux NCU sont activées, sauf si l'option `-c` est utilisée pour indiquer la classe NCU.

Le type du profil doit être l'un des types suivants :

- `ncp`
- `ncu`
- `loc`
- `enm`
- `wlan`

La classe NCU doit être spécifiée comme `phys` ou `ip`.

- `disable [ -p profile-type ] [ -c ncu-class ] profile-name`  
Désactive le profil spécifié. Si le nom de profil n'est pas unique, le type de profil doit être spécifié pour identifier le profil à désactiver. Si le type de profil est `ncu` et que le nom n'est pas unique (par exemple, s'il existe à la fois une `ncu` de lien et d'interface portant le même nom), les deux NCU sont activées, sauf si l'option `-c` est utilisée pour indiquer la classe NCU.

Le type du profil doit être l'un des types suivants :

- `ncp`
- `ncu`
- `loc`
- `enm`
- `wlan`

La classe NCU doit être spécifiée comme `phys` ou `ip`.

- `list [ -x ] [ -p profile-type ] [ -c ncu-class ] [ profile-name ]`  
Répertorie tous les profils disponibles et leur état actuel. Les différentes valeurs d'état sont répertoriées dans la section ci-dessous. Si un profil est spécifié par son nom, seul l'état actuel de ce profil est répertorié. Si le nom de profil n'est pas unique, tous les profils portant ce nom

sont répertoriés. Le type de profil ou la classe NCU ou les deux peuvent être inclus pour identifier un profil spécifique. Si seul le type de profil est spécifié, tous les profils de ce type sont répertoriés.

Lorsque le NCP activé est inclus dans la liste, toutes les NCU qui le constituent le sont aussi.

Si l'option -x est spécifiée, une description détaillée de l'état de chaque profil répertorié est également incluse dans la sortie.

Les valeurs d'état de profil possibles sont les suivantes :

- **disabled**  
Indique un profil activé manuellement, qui n'est pas actif.
- **offline**  
Indique un profil activé conditionnellement ou par le système, qui n'est pas actif. Le profil peut ne pas être actif parce que ses conditions n'ont pas été vérifiées. Il peut également ne pas être actif parce qu'un autre profil dont les conditions spécifiques sont vérifiées a été activé. Cette condition s'applique aux types de profils qui doivent être activés séparément, tels que le profil d'emplacements.
- **online**  
Indique un profil activé conditionnellement ou par le système, dont les conditions sont vérifiées et qui est actif. Peut également indiquer un profil activé manuellement, devenu actif à la demande de l'utilisateur.
- **maintenance**  
Indique que la tentative d'activation du profil a échoué.
- **initialized**  
Indique que le profil représente un objet de configuration correct pour lequel aucune action n'a encore été entreprise.
- **uninitialized**  
Indique que le profil représente un objet de configuration absent du système. Par exemple, cet état peut indiquer une NCU correspondant à un lien physique supprimé du système.
- **show-events**  
Ecoute un flux d'événements à partir du démon NWAM et les affiche.
- **scan-wifi *link-name***  
Lance une analyse sans fil sur le lien spécifié en tant que *link\_name*.
- **select-wifi *link-name***  
Sélectionne un réseau sans fil auquel se connecter à partir des résultats de l'analyse sur le lien spécifié en tant que *link-name*.
- **help**

Affiche un message d'utilisation avec une brève description de chaque sous-commande.

Pour obtenir des informations relatives aux tâches, reportez-vous au [Chapitre 5](#), “Administration des profils NWAM (tâches)”.

## Présentation des démons NWAM

NWAM utilise deux démons : `nwamd` et `netcfgd`. Le démon de moteur de stratégie, `nwamd`, détermine la configuration automatique du réseau en endossant plusieurs rôles. Le démon de référentiel, `netcfgd`, contrôle l'accès au référentiel de configuration du réseau.

### Description du démon de moteur de stratégie NWAM (`nwamd`)

Le démon `nwamd`, détermine la configuration automatique du réseau en endossant les rôles suivants :

- **Collecteur d'événements**

Ce rôle implique la collecte des événements liés aux liens à détecter par le biais du socket de routage et de l'enregistrement `sysevent`. Voici un exemple qui illustre comment `nwamd` effectue cette tâche : le démon obtient un `EC_DEV_ADD` `sysevent`, ce qui signifie qu'une carte réseau a été connectée à chaud dans le système. Tous ces événements sont intégrés dans la structure d'événements `nwamd`, puis transmis au thread de gestion d'événement chargé de cette tâche.

- **Gestionnaire d'événements**

Ce rôle implique l'exécution d'un thread de boucle d'événement pour répondre à des événements d'intérêt. Le gestionnaire d'événements s'exécute sur les machines d'état associées aux différents objets gérés par le service NWAM. Au cours de la gestion des événements, le démon `nwamd` détecte les changements de l'environnement réseau, qui peuvent déclencher des modifications d'un ou de plusieurs profils.

- **Dispatcheur d'événements**

Ce rôle implique l'envoi d'événements à des consommateurs externes, qui ont enregistré un intérêt pour ce type d'événements. Parmi les exemples de répartition d'événement, les événements d'analyse sans fil contenant des informations sur les WLAN disponibles sont utiles à l'interface graphique NWAM. L'interface graphique peut, à son tour, afficher les options disponibles à l'utilisateur.

- **Gestionnaire de profil**

La gestion de ces profils par le démon `nwamd` implique l'application de la configuration réseau, en fonction des informations suivantes :

- Liens et interfaces activés
- Caractéristiques des réseaux connectés
- Imprévus et dépendances intégrés dans les profils activés
- Événements externes reçus

## Description du démon de référentiel NWAM(`netcfgd`)

Le démon de profil, `netcfgd`, contrôle et gère l'accès au référentiel de configuration réseau. Le démon est lancé automatiquement par le service SMF `svc:/network/netcfg:default`. Le démon s'assure que toute application qui tente de lire ou d'écrire des informations dans le référentiel dispose des autorisations suivantes :

- `solaris.network.autoconf.read`
- `solaris.network.autoconf.write`

Pour plus d'informations sur les autorisations, reportez-vous à la page de manuel [auth\\_attr\(4\)](#). Pour plus d'informations sur les profils de sécurité, reportez-vous à la page de manuel [prof\\_attr\(4\)](#).

Pour plus d'informations sur les démons `netcfgd`, reportez-vous à la page de manuel [netcfgd\(1M\)](#)

## Services réseau SMF et configuration NWAM

Dans Oracle Solaris, la configuration réseau est mise en oeuvre par plusieurs services SMF :

- `svc:/network/loopback:default` : crée les interfaces de loopback IPv4 et IPv6.
- `svc:/network/netcfg:default` : ce service est une condition préalable au service `svc:/network/physical:default`. Le service gère le référentiel de configuration réseau, sa fonction principale étant de démarrer le démon `netcfgd`.
- `svc:/network/physical:default` : connecte des liens et monte des interfaces IP. Ce service détermine si NWAM ou une configuration réseau classique est en cours d'utilisation, en fonction du NCP actif. Si NWAM est en cours d'utilisation, le service démarre le démon de stratégie, `nwamd`. Si le NCP `DefaultFixed` est actif, le service arrête `nwamd` et applique la configuration `ipadm` persistante.
- `svc:/network/location:default` : ce service dépend du service `svc:/network/physical:default` et est responsable de l'activation du profil d'emplacement qui est sélectionné par le démon `nwamd`.



---

**Remarque** – Le service `svc:/network/location:default` dispose d'une propriété qui stocke le profil d'emplacement actuel. Ne manipulez pas directement cette propriété. Utilisez plutôt l'interface graphique NWAM ou la CLI pour effectuer ces types de modifications.

---

## Activation et désactivation de la gestion de configuration NWAM

Quand un NCP NWAM est activé, le démon `nwamd` gère activement la configuration réseau du système. Par conséquent, des liens et interfaces sont connectés et déconnectés en fonction de la stratégie spécifiée dans le NCP actif. Le profil d'emplacement dont la stratégie correspond le mieux aux conditions réseau actuelles est appliqué en modifiant le service de noms et les valeurs de sécurité, comme spécifié dans le profil d'emplacement.

Le NCP NWAM par défaut est le NCP automatique. Pour plus d'informations à propos du NCP automatique, reportez-vous aux sections [“Description des NCP automatiques et définis par l'utilisateur”](#) à la page 50 et [“Comportement par défaut de NWAM”](#) à la page 42.

Lorsque NWAM gère la configuration réseau, vous ne devez pas tenter d'apporter des modifications à la configuration active en modifiant directement les liens, les interfaces, les règles de filtrage IP, la stratégie IPsec, la configuration de service de nom ou le domaine NFS. Modifiez plutôt le profil NWAM approprié en utilisant la commande `netcfg` ou l'interface graphique NWAM. Les modifications sont appliquées au système en cours d'exécution lorsque le profil est activé par `nwamd`. Si le profil est actif au moment où les modifications sont apportées, celles-ci sont appliquées immédiatement.

Passer au NCP `DefaultFixed` désactive cette gestion de la configuration automatique. La configuration en vigueur avant l'activation d'un NCP NWAM est appliquée au système. Si le NCP NWAM est actif au moment où le système est installé, ce dernier ne présente aucune configuration réseau. Lorsque le NCP `DefaultFixed` est actif, les modifications de configuration sont apportées aux liens et interfaces directement à l'aide des commandes `ladm` et `ipadm`. Les modifications sont apportées aux valeurs Services de noms, Filtre IP, IPsec et Domaine NFS en modifiant les fichiers et les propriétés de service appropriés ou en exécutant les commandes que vous pouvez utiliser avec ces sous-systèmes.

Utilisez la commande `netadm` pour modifier le NCP actif.

Par exemple, pour changer le NCP actif et activer la configuration classique, vous devez saisir la commande suivante :

```
$ netadm enable -p ncp DefaultFixed
```

De même, pour activer la configuration NWAM avec le NCP automatique, vous devez saisir la commande suivante :

```
$ netadm enable -p ncp Automatic
```

Pour plus d'informations sur netadm, reportez-vous à la page de manuel [netadm\(1M\)](#).

## Présentation de la sécurité NWAM

La sécurité pour NWAM est conçue pour englober les composants suivants :

- CLI (commandes `netcfg` et `netadm`)
- Interface graphique NWAM
- Démon du référentiel de profils NWAM (`netcfgd`)
- Démon de moteur de stratégie (`nwamd`)
- Bibliothèque NWAM (`libnwam`)

Le démon `netcfgd` contrôle le référentiel où toutes les informations de configuration du réseau sont stockées. La commande `netcfg`, l'interface graphique NWAM et le démon `nwamd` envoient des demandes au démon `netcfgd` pour accéder au référentiel. Ces composants fonctionnels adressent des demandes par le biais de la bibliothèque NWAM `libnwam`.

Le démon `nwamd` est le moteur de stratégie qui reçoit les événements système, configure le réseau et lit les informations de configuration du réseau. L'interface graphique NWAM et la commande `netcfg` sont des outils de configuration qui peuvent être utilisés pour afficher et modifier la configuration du réseau. Ces composants sont également utilisés pour actualiser le service NWAM lorsqu'une nouvelle configuration doit être appliquée au système.

## Autorisations et profils liés à NWAM

La mise en oeuvre NWAM actuelle utilise les autorisations suivantes afin d'effectuer des tâches spécifiques :

- `solaris.network.autoconf.read` : permet la lecture des données de configuration NWAM, vérifiées par le démon `netcfgd`
- `solaris.network.autoconf.write` : permet l'écriture des données de configuration NWAM, vérifiées par le démon `netcfgd`
- `solaris.network.autoconf.select` : permet l'application de nouvelles données de configuration, vérifiées par le démon `nwamd`
- `solaris.network.autconf.wlan` : permet l'écriture des données de configuration de WLAN connus

Ces autorisations sont enregistrées dans la base de données `auth_attr`. Pour plus d'informations, reportez-vous à la page de manuel [auth\\_attr\(4\)](#).

Deux profils de sécurité sont fournis : Network Autoconf User et Network Autoconf Admin. Le profil User dispose des autorisations `read`, `select` et `wlan`. Le profil Admin ajoute l'autorisation `write`. Le profil Network Autoconf User est affecté au profil Console User. Par

conséquent, par défaut, toute personne qui s'est connectée à la console peut afficher, activer et désactiver les profils. Dans la mesure où `Console User` ne dispose pas de l'autorisation `solaris.network.autoconf.write`, l'utilisateur ne peut pas créer ni modifier les NCP, les NCU, les emplacements ni les ENM. Toutefois, le profil `Console User` permet d'afficher, de créer et de modifier les WLAN.

## Autorisations nécessaires pour utiliser les interfaces utilisateur NWAM

Les commandes NWAM, `netcfg` et `netadm`, peuvent être utilisées pour afficher et activer les profils NWAM par tous ceux qui possèdent les privilèges `Console User`. Ces privilèges sont automatiquement affectés à un utilisateur qui est connecté au système à partir de `/dev/console`.

Pour modifier les profils NWAM à l'aide de la commande `netcfg`, vous avez besoin de l'autorisation `solaris.network.autoconf.write` ou du profil `Network Autoconf Admin`.

Vous pouvez déterminer les privilèges associés à un profil de droits en utilisant la commande `profiles` avec le nom du profil. Pour plus d'informations, reportez-vous à la page de manuel [profiles\(1\)](#).

Par exemple, pour déterminer les privilèges associés au profil de droits `Console User`, utilisez la commande suivante.

```
$ profiles -p "Console User" info
Found profile in files repository.
  name=Console User
  desc=Manage System as the Console User
  auths=solaris.system.shutdown,solaris.device.cdrw,solaris.smf.manage.vbiosd,
  solaris.smf.value.vbiosd
  profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
  Network Autoconf User,Desktop Removable Media User
  help=RtConsUser.html
```

L'interface graphique NWAM comprend trois composants, qui ne sont pas privilégiés. Ces composants se voient octroyer des autorisations, en fonction de la manière dont ils ont été lancés et des tâches qu'ils doivent exécuter :

- **Présence du panneau spécifique à NWAM**

Ce composant est l'applet de panneau sur le bureau qui permet à un utilisateur d'interagir avec NWAM. Le panneau peut être exécuté par n'importe quel utilisateur pour surveiller la configuration automatique du système et gérer les notifications d'événement. Le panneau peut également être utilisé pour effectuer certaines tâches de configuration réseau de base, par exemple, la sélection d'un réseau Wi-Fi ou la commutation manuelle des emplacements. Pour effectuer ces types de tâches, le profil de droits `Network Autoconf User` est requis. Ce

profil de droits est disponible dans la configuration par défaut, car le panneau s'exécute avec les autorisations de l'utilisateur qui est connecté à partir de `/dev/console` et qui dispose par conséquent du profil `Console User`.

- **Interface graphique NWAM**

L'interface graphique NWAM est le principal moyen d'interaction avec NWAM à partir de l'ordinateur de bureau. L'interface utilisateur est utilisée pour afficher l'état du réseau, pour créer et modifier des NCP et des profils d'emplacement, et pour démarrer et arrêter des ENM configurés. L'interaction avec l'interface graphique requiert quatre des autorisations `solaris.network.autoconf` ou le profil `Network Autoconf Admin`. Par défaut, le profil `Console User` possède les autorisations suffisantes pour afficher l'état et les profils du réseau à l'aide de l'interface graphique. En outre, il vous faut l'autorisation `solaris.network.autoconf.write` ou le profil `Network Autoconf Admin` pour modifier les profils à l'aide de l'interface graphique.

Vous pouvez obtenir d'autres autorisations de l'une des façons suivantes :

- Affectez le profil `Network Autoconf Admin` à un utilisateur spécifique.

Vous pouvez affecter des autorisations appropriées, ou des profils de droits, directement à un utilisateur donné en modifiant le fichier `/etc/user_attr` de cet utilisateur.

- Affectez le profil `Network Autoconf Admin` à `Console User`.

Vous pouvez affecter ce profil à `Console User` au lieu du profil `Network Autoconf User`, qui est affecté par défaut. Pour affecter ce profil, modifiez l'entrée dans le fichier `/etc/security/prop_attr`.

## Configuration de profil NWAM (tâches)

---

Ce chapitre décrit les tâches de configuration de profil NWAM que vous pouvez effectuer à l'aide de la commande `netcfg`. Ces tâches de configuration sont les suivantes : création, modification et destruction de profils, ainsi que gestion des différents services SMF qui contrôlent la configuration NWAM. Ce chapitre décrit l'utilisation de la commande `netcfg` en mode interactif et de ligne de commande.

Il comprend les sections suivantes :

- “Création de profils” à la page 78
- “Suppression de profils” à la page 98
- “Définition et modification des valeurs de propriétés pour un profil” à la page 100
- “Interrogation du système pour l'obtention d'informations du profil” à la page 102
- “Exportation et restauration d'une configuration de profil” à la page 108
- “Gestion de la configuration réseau par l'intermédiaire de SMF” à la page 112

Pour plus d'informations sur l'affichage des états de profil, l'activation et la désactivation des profils, et la gestion des réseaux sans fil connus à l'aide de la commande `netadm`, reportez-vous au [Chapitre 5, “Administration des profils NWAM \(tâches\)”](#).

Pour plus d'informations sur l'interaction avec NWAM et la gestion de la configuration réseau à partir du bureau, reportez-vous au [Chapitre 6, “A propos de l'interface graphique NWAM”](#).

Pour obtenir une présentation de NWAM, reportez-vous au [Chapitre 2, “Présentation de NWAM”](#).

Pour de plus amples informations sur NWAM, y compris une description des modes d'interfaces utilisateur `netcfg`, reportez-vous au [Chapitre 3, “Configuration et administration NWAM \(présentation\)”](#).

## Création de profils

La commande `netcfg`, qui est décrite dans la page de manuel [netcfg\(1M\)](#), est l'une des deux commandes d'administration de l'interface de ligne de commande NWAM.

La commande `netcfg` peut être utilisée pour afficher les données de configuration de profil, et pour afficher, créer et modifier les objets WLAN connus, par toute personne disposant de privilèges `Console User`. Ces privilèges sont automatiquement attribués à tout utilisateur qui est connecté au système à partir de `/dev/console`. Les utilisateurs qui possèdent le profil `Network Autoconf Admin` peuvent également créer et modifier tous les types de profils NWAM et d'objets de configuration. Pour plus d'informations, reportez-vous à la section “[Présentation de la sécurité NWAM](#)” à la page 74.

Vous pouvez utiliser la commande `netcfg` pour sélectionner, créer, modifier et détruire les profils définis par l'utilisateur. La commande peut être utilisée en mode interactif ou de ligne de commande. La commande `netcfg` prend également en charge l'exportation des informations de configuration de profil dans les fichiers de commandes.

Vous pouvez créer, modifier et supprimer les profils et les objets de configuration suivants :

- Profils de configuration réseau (NCP, Network Configuration Profiles)
- Profils d'emplacement
- Modificateurs réseau externes (ENM, External Network Modifiers)
- Réseaux locaux sans fil connu (WLAN, Wireless Local Area Networks)
- Unités de configuration réseau (NCU, Network Configuration Units)

## Création de profils en mode de ligne de commande

La syntaxe de commande de base à utiliser pour créer un profil à partir de la ligne de commande est la suivante :

**netcfg create** [ **-t** *template* ] *object-type* [ *class* ] *object-name*

**create**            Crée un profil en mémoire (ou un objet de configuration) avec le type et le nom spécifiés.

**-t** *template*      Spécifie que le nouveau profil doit être identique au *template* (modèle), où *template* est le nom d'un profil existant du même type. Si l'option **-t** n'est pas utilisée, le nouveau profil est créé avec les valeurs par défaut.

*object-type*       Spécifie le type de profil à créer.

Vous pouvez spécifier l'une des valeurs suivantes pour l'option *object-type* :

- `ncp`
- `umn`
- `loc`

- enm
- wlan

Tous les profils qui sont spécifiés par l'option *object-type*, à l'exception d'un ncu, doivent être créés au niveau global avant de pouvoir utiliser la commande `netcfg select` pour sélectionner l'objet concerné.

<i>class</i>	Spécifie la classe de profil qui est spécifiée par <i>object-type</i> . Ce paramètre est utilisé uniquement pour le type d'objet ncu, et a deux valeurs possibles, phys ou ip.
<i>object-name</i>	Spécifie le nom du profil défini par l'utilisateur. Pour une unité monétaire nationale, <i>object-name</i> est le nom du lien ou de l'interface correspondante. Pour tous les autres types de profil, <i>object-name</i> est un nom défini par l'utilisateur.

Par exemple, pour créer un NCP nommé User, vous devez saisir la commande suivante :

```
$ netcfg create ncp User
```

où ncp est le type d'objet (*type-objet*) et User est le nom de l'objet (*object-name*).

---

**Remarque** – Pour la création de NCP, l'option `class` n'est pas requise.

---

Si vous le souhaitez, vous pouvez utiliser une copie du NCP automatique en tant que modèle, puis apporter des modifications à ce profil, comme indiqué ci-après :

```
$ netcfg create -t Automatic ncp
```

Pour créer un profil d'emplacement nommé office, vous devez saisir la commande suivante :

```
$ netcfg create loc office
```

## Création interactive de profils

Vous pouvez utiliser la commande `netcfg` en mode interactif pour effectuer les tâches suivantes :

- créer un profil ;
- sélectionner et modifier un profil ;
- vérifier que toutes les informations requises sur un profil sont définies et valides ;
- valider les modifications pour un nouveau profil ;
- annuler la configuration de profil en cours sans valider les modifications dans le stockage persistant ;

- annuler les modifications que vous avez apportées à un profil.

## Création d'un NCP

La création d'un profil en mode interactif entraîne l'affichage d'une invite de commande qui correspond à l'une des portées suivantes :

- Dans la portée du NCP, si un NCP est créé
- Dans la portée du profil, si un profil d'emplacement, un ENM, ou un objet WLAN est créé

La création d'un NCP ou d'une NCU déplace le focus dans la portée de cet objet, ce qui vous permet de parcourir les propriétés par défaut du profil indiqué.

Pour créer un NCP de façon interactive, vous devez commencer en lançant une session interactive `netcfg`. Ensuite, vous utilisez la sous-commande `create` pour créer le nouveau NCP `User`, comme suit :

```
$ netcfg
netcfg> create ncp User
netcfg:ncp:User>
```

## Création de NCU pour un NCP

Le NCP est essentiellement un conteneur qui se compose d'un ensemble de NCU. Tous les NCP contiennent des NCU de lien et d'interface. Les NCU de lien spécifient à la fois la configuration de lien et la stratégie de sélection de lien. Les NCU d'interface spécifient la stratégie de configuration d'interface. Si la connectivité IP est nécessaire, deux NCU, de lien et d'interface, sont requises. Des NCU doivent être ajoutées ou supprimées explicitement en utilisant la commande `netcfg` ou à l'aide du GUID.

---

**Remarque** – Il est possible d'ajouter des NCU qui ne sont pas en corrélation avec des liens qui sont actuellement installés sur le système. En outre, vous pouvez supprimer les NCU qui correspondent à un lien qui est actuellement installé sur le système.

---

Vous pouvez créer des NCU à l'aide de la commande `netcfg` en mode interactif ou en mode de ligne de commande. Etant donné que la création d'une NCU implique plusieurs opérations, il est plus facile et plus efficace de créer les NCU en mode interactif, plutôt que d'essayer de construire une commande d'une seule ligne qui crée la NCU et toutes ses propriétés. Vous pouvez créer les NCU lors de la création initiale d'un NCP, ou ultérieurement. Le processus de création ou de modification d'une NCU implique la définition des propriétés générales de NCU, ainsi que la définition des propriétés s'appliquant spécifiquement à chaque type de NCU.



Les propriétés qui vous sont présentées au cours de la procédure de création de NCU pour un NCP sont les plus logiques par rapport aux choix que vous avez effectués au cours de la création du NCP en question.

Lorsque vous créez une NCU en mode interactif, `netcfg` passe en revue chaque propriété pertinente, en affichant à la fois la valeur par défaut, s'il en existe une, et les valeurs possibles. Si vous appuyez sur la touche Entrée sans spécifier de valeur, la valeur par défaut est appliquée (ou la propriété est laissée vide s'il n'y a aucune valeur par défaut). Vous pouvez également spécifier une autre valeur. Les propriétés qui s'affichent lors du processus de création des NCU pour un NCP sont pertinentes par rapport aux choix que vous avez déjà effectués. Par exemple, si vous choisissez l'option `dhcp` pour la propriété `ipv4-addrsrc` d'une NCU d'interface, vous n'êtes pas invité à spécifier une valeur pour la propriété `ipv4-addr`.

Le tableau suivant décrit toutes les propriétés de NCU que vous pouvez spécifier lors de la création ou la modification d'une NCU. Certaines propriétés s'appliquent aux deux types de NCU. D'autres propriétés s'appliquent à une NCU de lien ou une NCU d'interface. Pour obtenir une description complète de l'ensemble des propriétés de NCU, y compris des règles et conditions qui peuvent s'appliquer lorsque vous spécifiez ces propriétés, reportez-vous à la page de manuel [netcfg\(1M\)](#).

**TABEAU 4-1** Propriétés de création ou modification d'une NCU

Propriétés	Description	Valeurs possibles	Type de NCU
<code>type</code>	Spécifie le type de NCU (lien ou interface).	<code>link</code> ou <code>interface</code>	Lien et interface
<code>classe</code>	Spécifie la classe de NCU.	<code>phys</code> (pour les NCU de lien) ou <code>ip</code> (pour les NCU d'interface)	Lien et interface
<code>parent</code>	Spécifie le NCP auquel cette NCU appartient.	<code>parent-NCP</code>	Lien et interface
<code>enabled</code>	Indique si la NCU est activée ou désactivée. Cette propriété est en lecture seule. Elle est modifiée indirectement uniquement lorsque vous utilisez la commande <code>netadm</code> ou l'interface graphique NWAM pour activer ou désactiver la NCU.	<code>true</code> ou <code>false</code>	Lien et interface

TABLEAU 4-1 Propriétés de création ou modification d'une NCU (Suite)

Propriétés	Description	Valeurs possibles	Type de NCU
activation-mode	Spécifie le type de déclencheur pour l'activation automatique de la NCU.	manual ou prioritized  La valeur par défaut est manual.	Lien
priority-group	Spécifie le numéro de priorité de groupe.	0 (pour les liens câblés) ou 1 (pour les liens sans fil)  Pour les NCP définis par l'utilisateur, des stratégies différentes peuvent être spécifiées, par exemple, le lien sans fil 1 est de priorité 1, le lien câblé 1 est de priorité 2, et le lien câblé 2 est de priorité 3.  <b>Remarque</b> – Un nombre inférieur indique une priorité plus élevée.	Lien
priority-mode	Spécifie le mode utilisé pour déterminer le comportement d'activation d'un groupe de priorités, si la propriété activation-mode est définie sur prioritized.	exclusive, shared ou all  Reportez-vous à la page de manuel <a href="#">netcfg(1M)</a> pour connaître les règles qui s'appliquent lorsque vous indiquez ces valeurs.	Lien
link-mac-addr	Indique l'adresse MAC qui est affectée à ce lien. Par défaut, NWAM utilise la configuration d'usine ou une autre adresse MAC par défaut. Une valeur différente peut être définie ici pour remplacer cette sélection.	Une chaîne contenant une adresse MAC 48 bits	
link-autopush	Identifie les modules qui sont automatiquement répercutés sur le lien lorsqu'il est ouvert.	Une liste de chaînes (modules à répercuter sur le lien)  Reportez-vous à la page de manuel <a href="#">autopush(1M)</a> .	Lien

TABLEAU 4-1 Propriétés de création ou modification d'une NCU (Suite)

Propriétés	Description	Valeurs possibles	Type de NCU
link-mtu	Est automatiquement définie pour la MTU par défaut du lien physique. La valeur par défaut peut être remplacée en définissant la propriété sur une valeur différente.	Taille de la MTU pour le lien	Lien
ip-version	Spécifie la version d'IP à utiliser. Plusieurs valeurs peuvent être affectées.	ipv4 et ipv6  La valeur par défaut est ipv4, ipv6.	Interface
ipv4-addrsrc	Permet d'identifier l'origine des adresses IPv4 qui sont affectés à cette NCU. Plusieurs valeurs peuvent être affectées.	dhcp et static  La valeur par défaut est dhcp.	Interface
ipv6-addrsrc	Permet d'identifier l'origine des adresses IPv6 affectées à cette NCU. Plusieurs valeurs peuvent être affectées.	dhcp, autoconf ou static  La valeur par défaut est dhcp,autoconf.	Interface
ipv4-addr	Spécifie une ou plusieurs adresses IPv4 à affecter à cette NCU.	Une ou plusieurs adresses IPv4 à affecter	Interface
ipv6-addr	Spécifie une ou plusieurs adresses IPv6 à affecter à cette NCU.	Une ou plusieurs adresses IPv6 à affecter	Interface
ipv4-default-router	Spécifie la route par défaut d'une adresse IPv4.	Une adresse IPv4	Interface
ipv6-default-router	Spécifie la route par défaut pour une adresse IPv6.	Une adresse IPv6	Interface

## ▼ Création d'un NCP en mode interactif

La procédure suivante décrit la création d'un NCP en mode interactif.

**Astuce** – L'examen effectué par NWAM au cours de la création du profil initial garantit que vous êtes invité à indiquer uniquement les propriétés pertinentes, en fonction des choix que vous avez effectués précédemment. En outre, la sous-commande `verify` qui est décrite dans cette procédure vérifie votre configuration. Si les valeurs requises sont manquantes, vous en êtes informé. Vous pouvez utiliser la sous-commande `verify` explicitement lors de la création ou de la modification d'un profil ou implicitement en utilisant la sous-commande `commit` pour enregistrer vos modifications.

---

**1 Lancez une session `netcfg` en mode interactif.**

```
$ netcfg
netcfg>
```

**2 Créez le NCP.**

```
netcfg> create ncp User
netcfg:ncp:User>
```

où `ncp` est le type de profil et `User` est le nom du profil.

La création automatique du NCP vous conduit à la portée du NCP. Si vous créez un emplacement, un ENM, ou un objet WLAN, l'invite de commande vous conduirait à la portée du profil.

**3 Créez les NCU de lien et d'interface pour le NCP.**

**a. Pour créer la NCU de lien, tapez la commande suivante :**

```
netcfg:ncp:User> create ncu phys net0
Created ncu 'net0', Walking properties ...
```

où `ncu` est le type d'objet, `phys` est la classe et `net0` (à titre d'exemple *uniquement*) est le nom de l'objet.

La création d'une NCU vous place dans la portée de l'objet et vous permet de parcourir les propriétés par défaut de l'objet.

**b. Pour créer une NCU d'interface, tapez la commande suivante :**

```
netcfg:ncp:User> create ncu ip net0
Created ncu 'net0'. walking properties ...
```

où `ncu` est le type d'objet, `ip` est la classe et `net0` (à titre d'exemple *uniquement*) est le nom de l'objet.

La création d'une NCU vous place dans la portée de l'objet et vous permet de parcourir les propriétés par défaut de l'objet.

Au cours de la création d'une NCU, l'option `class` est utilisée pour faire la différence entre deux types de NCU. Cette option est particulièrement utile dans les situations où différents types de NCU partagent le même nom. Si l'option `class` n'est pas précisée, il est beaucoup plus difficile de distinguer les NCU qui partagent le même nom.

#### 4 Ajoutez les propriétés appropriées pour la NCU que vous avez créée.

---

**Remarque** – Répétez les étapes 3 et 4 jusqu'à ce que toutes les NCU requises pour le NCP aient été créées.

---

#### 5 Au cours de la création de la NCU, ou lorsque vous définissez les valeurs de propriétés d'une NCU spécifique, utilisez la sous-commande `verify` pour vous assurer que les modifications que vous avez apportées sont correctes.

```
netcfg:ncp:User:ncu:net0> verify
All properties verified
```

#### 6 Validez les propriétés que vous avez définies pour la NCU.

```
netcfg:ncp:User:ncu:net0> commit
committed changes.
```

Vous pouvez également utiliser la sous-commande `fin` pour effectuer une validation implicite, ce qui a pour effet de déplacer la session interactive d'un niveau jusqu'à la portée supérieure. Dans cet exemple, si vous avez terminé la création du NCP et l'ajout des NCU à celui-ci, vous pouvez quitter la session interactive directement à partir de la portée du NCP.

---

#### Remarque –

- En mode interactif, les modifications ne sont pas enregistrées dans le stockage persistant tant que vous ne les avez pas validées. Lorsque vous utilisez la sous-commande `commit`, l'ensemble du profil est validé. Pour assurer la cohérence du stockage persistant, l'opération de validation comprend également une étape de vérification. Si la vérification échoue, la validation échoue également. Si une validation implicite échoue, vous avez la possibilité de mettre fin à la session interactive, ou de la fermer, sans valider les modifications effectuées. Vous pouvez également rester dans la portée actuelle et continuer à apporter des modifications au profil.
- Pour annuler les modifications que vous avez apportées, utilisez la sous-commande `cancel` ou `revert`.

La sous-commande `cancel` termine la configuration de profil actuelle sans valider les modifications actuelles dans le stockage persistant, puis déplace la session interactive d'un niveau jusqu'à la portée suivante. La sous-commande `revert` annule les modifications que vous avez apportées et lit à nouveau la configuration précédente. Lorsque vous utilisez la sous-commande `revert`, la session interactive reste dans la même portée.

---

#### 7 Utilisez la sous-commande `list` pour afficher la configuration NCP.

#### 8 Lorsque vous avez fini de configurer le NCP, quittez la session interactive.

```
netcfg:ncp:User> exit
```

Chaque fois que vous utilisez la sous-commande `exit` pour mettre fin à une session `netcfg` interactive, le profil actuel est vérifié et validé. Si l'opération de vérification ou de validation

échoue, un message d'erreur approprié est affiché, et vous avez la possibilité de quitter sans valider les modifications actuelles. Vous pouvez également rester dans la portée actuelle et continuer à apporter des modifications au profil.

---

**Remarque** – Pour quitter la portée sans quitter la session `netcfg` interactive, saisissez la commande `fin` :

```
netcfg:ncp:User> end
netcfg>
```

---

#### Exemple 4–1 Création d'un NCP en mode interactif

Dans l'exemple suivant, un NCP et deux NCU (de lien et d'interface) sont créés.

```
$ netcfg
netcfg> create ncp User
netcfg:ncp:User> create ncu phys net0
Created ncu 'net0', Walking properties ...
activation-mode (manual) [manual|prioritized]>
link-mac-addr>
link-autopush>
link-mtu>
netcfg:ncp:User:ncu:net0> end
Committed changes
netcfg:ncp:User> create ncu ip net0
Created ncu 'net0'. Walking properties ...
ip-version (ipv4,ipv6) [ipv4|ipv6]> ipv4
ipv4-addrsrc (dhcp) [dhcp|static]>
ipv4-default-route>
netcfg:ncp:User:ncu:net0> verify
All properties verified
netcfg:ncp:User:ncu:net0> end
Committed changes
netcfg:ncp:User> list
NCUs:
      phys      net0
      ip        net0
netcfg:ncp:User> list ncu phys net0
ncu:net0
      type                link
      class               phys
      parent              "User"
      activation-mode     manual
      enabled              true
netcfg:ncp:User> list ncu ip net0
ncu:net0
      type                interface
      class               ip
      parent              "User"
      enabled              true
      ip-version          ipv4
      ipv4-addrsrc        dhcp
      ipv6-addrsrc        dhcp,autoconf
netcfg:ncp:User> exit
$
```

Dans cet exemple, la valeur `ipv4` n'étant pas choisie, aucune invite n'est affichée pour la propriété `ipv6-addrsrc`, car cette propriété n'est pas utilisée. De la même façon, pour la NCU `phys`, la valeur par défaut (activation manuelle) de la propriété `priority-group` est acceptée, de sorte qu'aucune autre propriété associée de manière conditionnelle n'est appliquée.

## Exemple 4–2 Création d'une NCU pour un NCP existant

Pour créer une NCU pour un NCP existant ou pour modifier les propriétés de n'importe quel profil, utilisez la commande `netcfg` avec la sous-commande `select`.

Dans l'exemple suivant, une NCU IP est créée pour un NCP existant. Le processus de modification d'un profil existant en mode interactif est semblable à la création d'un profil. La différence entre l'exemple suivant et [Exemple 4–1](#) est que, dans cet exemple, la sous-commande `select` est utilisée à la place de la sous-commande `create` car le NCP existe déjà.

```
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> list
NCUs:
    phys    net0
netcfg:ncp:User> create ncu ip net0
Created ncu 'net0'. Walking properties ...
ip-version (ipv4,ipv6) [ipv4|ipv6]> ipv4
ipv4-addrsrc (dhcp) [dhcp|static]>
ipv4-default-route>
netcfg:ncp:User:ncu:net0> end
Committed changes
netcfg:ncp:User> list
NCUs:
    phys    net0
    ip      net0
netcfg:ncp:User> list ncu phys net0
ncu:net0
    type                link
    class               phys
    parent              "User"
    activation-mode      manual
    enabled              true
netcfg:ncp:User> list ncu ip net0
NCU:net0
    type                interface
    class               ip
    parent              "User"
    enabled              true
    ip-version           ipv4
    ipv4-addrsrc         dhcp
    ipv6-addrsrc         dhcp,autoconf
netcfg:ncp:User> exit
$
```

## Création d'un profil d'emplacement

Un profil d'emplacement contient les propriétés qui définissent les paramètres de configuration réseau qui ne sont pas directement liés à la connectivité de lien et IP de base. Les paramètres de service de nommage et de filtre IP qui sont appliqués conjointement, lorsque nécessaire, en sont des exemples. A un moment donné, un profil d'emplacement et un NCP doivent être actifs sur le système. Il existe des emplacements définis par le système et d'autres définis par l'utilisateur. Les emplacements système sont la valeur par défaut que NWAM choisit sous certaines conditions, par exemple, si vous n'avez pas indiqué d'emplacement, ou si aucun emplacement n'a été activé manuellement, et qu'aucune des conditions des emplacements activés de manière conditionnelle n'a été satisfaite. Les emplacements définis par le système possèdent un mode activation `system`. Les emplacements définis par l'utilisateur sont ceux qui sont configurés pour être activés manuellement ou de manière conditionnelle, en fonction des conditions de réseau, par exemple, une adresse IP qui est obtenue par une connexion réseau.

Pour plus d'informations sur l'activation manuelle d'un profil d'emplacement, reportez-vous à la section [“Activation et désactivation des profils”](#) à la page 118.

Vous pouvez créer des emplacements à l'aide de la commande `netcfg` en mode interactif ou en mode de ligne de commande. Lorsque vous créez un profil d'emplacement, vous devez définir ses propriétés en indiquant des valeurs qui définissent les paramètres de configuration spécifiques de cet emplacement. Les propriétés d'emplacement sont classées par groupe, où le groupe correspond à une classe spécifique de préférences de configuration.

Les propriétés d'emplacement sont également stockées par NWAM dans un référentiel. Lorsqu'un profil d'emplacement spécifique est activé, NWAM configure automatiquement le réseau, en fonction des propriétés qui sont définies pour l'emplacement. La création ou la modification des emplacements consiste à définir les différentes propriétés qui définissent la façon dont le profil est configuré, ce qui détermine ensuite la façon dont NWAM configure automatiquement votre réseau. Les propriétés qui vous sont présentées pendant le processus de configuration sont celles qui sont les plus pertinentes, en fonction des choix que vous avez effectués précédemment.

Le tableau ci-dessous présente l'ensemble des propriétés d'emplacement qui peuvent être spécifiées. Notez que les propriétés d'emplacement sont classées par groupe. Pour obtenir une description complète de toutes les propriétés d'emplacement, y compris les règles, les conditions et les dépendances qui peuvent s'appliquer lorsque vous spécifiez l'une de ces propriétés, reportez-vous à la page de manuel [netcfg\(1M\)](#).



TABLEAU 4-2 Propriétés d'emplacement et leurs descriptions

Groupe de propriétés et description	Valeur de propriété et description
<b>Critères de sélection</b> Spécifie les critères définissant comment et quand un emplacement est activé ou désactivé.	<ul style="list-style-type: none"> <li>■ <code>activation-mode</code> Les valeurs possibles pour la propriété <code>activation-mode</code> sont <code>manual</code>, <code>conditional-any</code> et <code>conditional-all</code>.</li> <li>■ <code>conditions</code></li> </ul>
<b>System domain</b> Détermine le nom de domaine d'un hôte qui sera utilisé directement par le service de nommage NIS.	La propriété <code>system-domain</code> se compose de la propriété <code>default-domain</code> . Cette propriété spécifie le domaine à l'échelle du système qui est utilisé pour les échanges d'appel de procédure à distance (RPC).
<b>Informations sur les services de noms</b> Spécifie le service de nommage à utiliser, et la configuration de commutation de service de nommage.	La liste suivante répertorie les propriétés du service de nommage spécifié : <ul style="list-style-type: none"> <li>■ <code>domain-name</code></li> <li>■ <code>nameservices</code></li> <li>■ <code>nameservices-config-file</code></li> <li>■ <code>dns-nameservice-configsrc</code></li> <li>■ <code>dns-nameservice-domain</code></li> <li>■ <code>dns-nameservice-servers</code></li> <li>■ <code>dns-nameservice-search</code></li> <li>■ <code>dns-nameservice-sortlist</code></li> <li>■ <code>dns-nameservice-options</code></li> <li>■ <code>nis-nameservice-configsrc</code></li> <li>■ <code>nis-nameservice-servers</code></li> <li>■ <code>ldap-nameservice-configsrc</code></li> <li>■ <code>ldap-nameservice-servers</code></li> </ul> Pour plus d'informations sur ces propriétés, reportez-vous à la section Propriétés d'emplacement de la page de manuel <a href="#">netcfg(1M)</a> .
<b>Domaine NFSv4</b> Spécifie le domaine NFSv4.	Valeur qui est utilisée pour la propriété <code>nfsmapid_domain</code> du système. Cette valeur est utilisée pour définir la propriété SMF <code>nfsmapid_domain</code> , comme décrit dans la page de manuel <code>nfsmapid</code> , pendant que l'emplacement est actif. Si cette propriété n'est pas définie, la propriété <code>nfsmapid_property</code> du système est effacée lorsque l'emplacement est actif. Reportez-vous à la page de manuel <a href="#">nfsmapid(1M)</a> pour de plus amples informations.

TABLEAU 4-2 Propriétés d'emplacement et leurs descriptions (Suite)

Groupe de propriétés et description	Valeur de propriété et description
<b>Configuration d'IP Filter</b> Spécifie les paramètres qui sont utilisés pour la configuration d'IP Filter. Pour ces propriétés, les chemins d'accès aux fichiers <code>ipf</code> et <code>ipnat</code> appropriés contenant les règles IP Filter et NAT sont spécifiés.	<ul style="list-style-type: none"><li>■ <code>ipfilter-config-file</code></li><li>■ <code>ipfilter-v6-config-file</code></li><li>■ <code>ipnat-config-file</code></li><li>■ <code>ippool-config-file</code></li></ul> Si un fichier de configuration est spécifié, les règles qui sont contenues dans les fichiers identifiés sont appliquées au sous-système <code>ipfilter</code> .
<b>Fichiers de configuration pour IPsec</b> Spécifie les fichiers à utiliser pour la configuration IPsec.	<ul style="list-style-type: none"><li>■ <code>ike-config-file</code></li><li>■ <code>ipsecpolicy-config-file</code></li></ul>

▼ **Création d'un profil d'emplacement en mode interactif**

La procédure suivante décrit la création d'un profil d'emplacement.

**Astuce** – L'examen effectué par NWAM au cours de la création initiale d'un profil vous invite uniquement à définir les propriétés pertinentes, en fonction des valeurs que vous avez saisies précédemment. En outre, la sous-commande `verify` effectue une vérification pour s'assurer que votre configuration est correcte. Si les valeurs requises sont manquantes, vous en êtes informé. Notez que vous pouvez utiliser la sous-commande `verify` de manière explicite lors de la création ou de la modification d'une configuration de profil ou implicitement en utilisant la sous-commande `commit` pour enregistrer vos modifications.

**1 Lancez une session `netcfg` en mode interactif.**

```
$ netcfg
netcfg>
```

**2 Créez ou sélectionnez l'emplacement.**

```
netcfg> create loc office
netcfg:loc:office>
```

Dans cet exemple, l'emplacement `office` est créé.

La création de l'emplacement vous déplace automatiquement dans la portée du profil pour cet emplacement.

**3 Définissez les propriétés appropriées pour l'emplacement.**

#### 4 Affichez la configuration de profil.

Par exemple, la sortie suivante affiche les propriétés de l'emplacement office :

```
netcfg:loc:office> list
LOC:office
  activation-mode      conditional-any
  conditions           "ncu ip:wpi0 is active"
  enabled              false
  nameservices         dns
  nameservices-config-file "/etc/nsswitch.dns"
  dns-nameservice-configsrc dhcp
  ipfilter-config-file  "/export/home/test/wifi.ipf.conf"
```

#### 5 Vérifiez que la configuration du profil est correcte.

Dans l'exemple suivant, la configuration de l'emplacement office est vérifiée :

```
netcfg:loc:office> verify
All properties verified
```

#### 6 Lorsque vous avez terminé la vérification, validez le profil d'emplacement dans le stockage permanent.

```
netcfg:loc:office> commit
Committed changes
```

Vous pouvez également utiliser la sous-commande `end` pour mettre fin à la session, qui permet également d'enregistrer la configuration du profil.

```
netcfg:loc:office> end
Committed changes
```

---

#### Remarque –

- En mode interactif, les modifications ne sont pas enregistrées dans le stockage persistant tant que vous ne les avez pas validées. Lorsque vous utilisez la sous-commande `commit`, l'ensemble du profil est validé. Pour assurer la cohérence du stockage persistant, l'opération de validation comprend également une étape de vérification. Si la vérification échoue, la validation échoue également. Si une validation implicite échoue, vous avez la possibilité de mettre fin à la session interactive, ou de la fermer, sans valider les modifications effectuées. Vous pouvez également rester dans la portée actuelle et continuer à apporter des modifications au profil.
  - Pour annuler les modifications que vous avez apportées, utilisez la sous-commande `cancel`. La sous-commande `cancel` termine la configuration de profil actuelle sans valider les modifications actuelles dans le stockage persistant, puis déplace la session interactive d'un niveau jusqu'à la portée suivante.
- 

#### 7 Quittez la session interactive.

```
netcfg> exit
Nothing to commit
$
```

### Exemple 4–3 Création interactive d'un profil d'emplacement

Dans l'exemple suivant, un emplacement nommé office est créé.

```
$ netcfg
netcfg> create loc office
Created loc 'office'. Walking properties ...
activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-any
conditions> ncu ip:wpi0 is active
nameservices (dns) [dns|files|nis|ldap]>
nameservices-config-file ("/etc/nsswitch.dns")>
dns-nameservice-configsrc (dhcp) [manual|dhcp]>
nfsv4-domain>
ipfilter-config-file> /export/home/test/wifi.ipf.conf
ipfilter-v6-config-file>
ipnat-config-file>
ippool-config-file>
ike-config-file>
ipsecpolicy-config-file>
netcfg:loc:office> list
LOC:office
    activation-mode          conditional-any
    conditions                "ncu ip:wpi0 is active"
    enabled                  false
    nameservices              dns
    nameservices-config-file  "/etc/nsswitch.dns"
    dns-nameservice-configsrc dhcp
    ipfilter-config-file      "/export/home/test/wifi.ipf.conf"
netcfg:loc:office> verify
All properties verified
netcfg:loc:office> commit
Committed changes
netcfg> list
NCPs:
    User
    Automatic
Locations:
    Automatic
    NoNet
    test-loc
WLANS:
    sunwifi
    ibahn
    gogoinflight
    admiralsclub
    hhonors
    sjcfreewifi
netcfg> exit
Nothing to commit
$
```

Dans cet exemple, les propriétés suivantes ont été spécifiées pour l'emplacement office :

- La propriété activation-mode a été définie sur conditional-any, entraînant une invite de commande qui permet aux conditions d'activation d'être spécifiées.
- La condition d'activation a été spécifiée comme : ncu ip:wpi0 is active.

---

**Remarque** – La propriété `conditions` est requise car la propriété `conditional-any` a été spécifiée à l'étape précédente. Si, par exemple, la propriété `manual` avait été spécifiée, la propriété `conditions` ne serait pas requise.

---

- Les valeurs par défaut suivantes ont été acceptées en appuyant sur Entrée :
  - `nameservices`
  - `nameservices-config-file`
  - `dns-nameservice-configsrc`
  - `nfsv4-domain`
- Pour la propriété `ipfilter-config-file`, le fichier `/export/home/test/wifi.ipf.conf` a été spécifié.
- Les valeurs par défaut suivantes ont été acceptées en appuyant sur Entrée :
  - `ipfilter-v6-config-file`
  - `ipnat-config-file`
  - `ippool-config-file`
  - `ike-config-file`
  - `ipsecpolicy-config-file`
- La sous-commande `list` a été utilisée pour afficher les propriétés du profil d'emplacement.
- La sous-commande `verify` a été utilisée pour effectuer une vérification de la configuration.
- La sous-commande `commit` a été utilisée pour valider les modifications apportées à l'espace de stockage persistant.
- La sous-commande `list` a été utilisée à nouveau pour s'assurer que le nouvel emplacement a été créé correctement et qu'il contient les informations correctes.
- La sous-commande `exit` a été utilisée pour quitter la session interactive `netcfg`.

Pour obtenir des instructions sur les valeurs qui peuvent être spécifiées pour ces propriétés, reportez-vous à la page de manuel [netcfg\(1M\)](#).

## Création d'un profil ENM

Les ENM se rapportent à la configuration d'applications qui sont externes à NWAM, par exemple, une application de réseau privé virtuel (VPN). Ces applications peuvent créer et modifier la configuration réseau. Les ENM peuvent également être définis en tant que services ou applications qui modifient directement la configuration réseau lorsqu'ils sont activés ou désactivés. Vous pouvez configurer NWAM pour activer et désactiver des ENM dans les conditions que vous précisez. Contrairement à un profil d'emplacement ou à un NCP où un seul des types de profil peut être actif sur un système à un moment donné, plusieurs ENM sont susceptibles d'être actifs simultanément sur un système. Les ENM qui sont actifs sur un système

à un moment donné ne sont pas nécessairement dépendants du profil d'emplacement ou du NCP qui est également activé sur le système en même temps.

**Remarque** – NWAM ne reconnaît pas automatiquement une application pour laquelle vous pouvez créer un ENM. Ces applications doivent d'abord être installées et configurées sur votre système avant de pouvoir utiliser la commande `netcfg` afin de créer un ENM pour elles.

Pour créer un ENM, tapez la commande suivante :

```
$ netcfg
netcfg> create enm my_enm
Created enm 'my_enm'. Walking properties ...
```

où `enm` est le profil ENM et `my_enm` est le nom de l'objet.

Le processus de création des ENM vous permet d'accéder à la portée du profil pour l'ENM récemment créé, et lance automatiquement une visite des propriétés dans celui-ci. A partir de là, vous pouvez définir les propriétés de l'ENM stipulant quand et comment l'ENM est activé, ainsi que d'autres conditions, y compris la méthode de démarrage et d'arrêt de l'ENM.

Pour de plus amples instructions sur la spécification des propriétés d'ENM, reportez-vous à la page de manuel [netcfg\(1M\)](#).

Le tableau suivant décrit toutes les propriétés que vous pouvez spécifier lors de la création ou la modification d'un ENM.

Nom de propriété	Description	Valeurs possibles
activation-mode	Mode utilisé pour déterminer l'activation d'un ENM	conditional-any, conditional-all, manual
conditions	Si le mode d'activation est conditional-any ou conditional-all , spécifie le test permettant de déterminer si l'ENM doit être activé.	Une ou plusieurs chaînes de caractères formatées tel que spécifié dans la section relative aux expressions de condition de la page de manuel <a href="#">netcfg(1M)</a> , si la propriété est utilisée.
start	(Facultatif) Chemin absolu vers le script à exécuter lors de l'activation	Chemin d'accès au script, si cette propriété est utilisée
stop	(Facultatif) Chemin absolu vers le script à exécuter lors de la désactivation	Chemin d'accès au script, si cette propriété est utilisée

Nom de propriété	Description	Valeurs possibles
fmri	<p>(Facultatif) FMRI (Fault Managed Resource Identifier) à activer lors de l'activation de l'ENM</p> <p><b>Remarque</b> – Un FMRI ou un script de démarrage doit être spécifié. Si un FMRI est spécifié, les propriétés start et stop sont ignorées.</p>	Chemin d'accès au script

**EXEMPLE 4-4** Création interactive d'un profil ENM

Dans l'exemple suivant, un ENM nommé test-enm est créé en mode interactif.

```
$ netcfg
netcfg> create enm test-enm
Created enm 'testenm'. Walking properties ...
activation-mode (manual) [manual|conditional-any|conditional-all]>
fmri> svc:/application/test-app:default
start>
stop>
netcfg:enm:test-enm> list
ENM:test-enm
    activation-mode    manual
    enabled            false
    fmri               "svc:/application/test-enm:default"
netcfg:enm:test-enm> verify
All properties verified
netcfg:enm:test-enm> end
Committed changes
netcfg> list
NCPs:
    User
    Automatic
Locations:
    Automatic
    NoNet
    test-loc
ENMs:
    test-enm
WLANS:
    sunwifi
    ibahn
    gogoinflight
    admiralsclub
    hhonors
    sjcfreewifi
netcfg> end
$
```

Dans cet exemple, un ENM nommé test-enm a été créé avec les valeurs de propriété suivantes :

- La valeur par défaut (manual) pour la propriété activation-mode a été acceptée en appuyant sur la touche Entrée.

EXEMPLE 4-4    Création interactive d'un profil ENM      (Suite)

- La propriété `SMF FMRI svc:/application/test-enm:default` a été spécifiée en tant que méthode à utiliser pour l'activation et désactivation de l'application.  
Notez que dans la mesure où un FMRI a été spécifié, les propriétés de méthode `start` et `stop` ont été ignorées.
- La sous-commande `list` a été utilisée pour afficher les propriétés de l'ENM.
- La sous-commande `verify` a été utilisée pour s'assurer que la configuration du profil est correcte.
- La sous-commande `end` a été utilisée pour enregistrer implicitement la configuration.
- La sous-commande `end` a été utilisée à nouveau pour mettre fin à la session interactive.

## Création de WLAN

NWAM gère une liste à l'échelle du système répertoriant les WLAN connus. Les WLAN sont des objets de configuration qui contiennent l'historique et les informations de configuration pour les réseaux sans fil auxquels vous-vous connectez à partir de votre système. Cette liste sert ensuite à déterminer l'ordre dans lequel NWAM tente de se connecter aux réseaux sans fil disponibles. Si un réseau sans fil qui existe dans la liste des WLAN connus est disponible, NWAM se connecte automatiquement à ce réseau. Si deux ou plusieurs réseaux connus sont disponibles, NWAM se connecte au réseau sans fil qui a la priorité la plus élevée (numéro le plus bas). Tout nouveau réseau sans fil auquel NWAN se connecte est ajouté en tête de la liste des WLAN connus et devient le nouveau réseau sans fil à la priorité la plus élevée.

Pour créer un objet WLAN, tapez la commande suivante :

```
$ netcfg
netcfg> create wlan mywifi
Created wlan 'mywifi'. Walking properties ...
```

où `wlan` est l'objet WLAN et `mywifi` est le nom de l'objet.

Le processus de création d'un objet WLAN vous permet d'accéder à la portée du profil pour le WLAN récemment créé, et lance automatiquement une visite des propriétés dans celui-ci. Vous pouvez alors définir les propriétés pour le WLAN qui définit sa configuration.

Le tableau suivant décrit toutes les propriétés que vous pouvez spécifier lors de la création ou la modification de WLAN.

Propriété de WLAN connue	Type de données de la propriété
<code>name</code>	ESSID (nom de réseau sans fil)



Propriété de WLAN connue	Type de données de la propriété
bssids	ID de station de base des WLAN auxquels s'est connecté votre système tout en étant connecté au WLAN spécifié
priority	Préférences de connexion des WLAN (les valeurs inférieures sont préférées)
keyslot	Numéro de l'emplacement (1–4) dans lequel la clé WEP est contenue
keyname	Nom de la clé de WLAN qui est créée à l'aide de la commande <code>dladm create-secobj</code> .
security-mode	Le type de clé de chiffrement en cours d'utilisation. Le type doit être <code>none</code> , <code>wep</code> ou <code>wpa</code> .

#### EXEMPLE 4-5 Création d'un WLAN

Dans l'exemple suivant, un objet WLAN nommé `mywifi` est créé.

Cet exemple suppose qu'un objet sécurisé nommé `mywifi-key`, qui contient la clé spécifiée par la propriété `keyname` pour le WLAN `mywifi`, est créé *avant* l'ajout du WLAN.

Le numéro de priorité peut changer à mesure que d'autres WLAN sont ajoutés ou supprimés. Notez que deux WLAN ne peuvent pas avoir le même numéro de priorité assigné. Les nombres inférieurs indiquent une priorité plus élevée, en termes de préférence des WLAN. Dans cet exemple, le numéro de priorité 100 est affecté au WLAN pour s'assurer qu'il a un niveau de priorité inférieur à celui de toute autre WLAN connu.

Lorsque la sous-commande `list` est utilisée à la fin de la procédure, le nouveau WLAN est ajouté à la fin de la liste, indiquant qu'il a le niveau de priorité le plus bas de tous les WLAN connus. Si le WLAN avait le numéro de priorité de zéro (0), qui est la valeur par défaut, il serait affiché en haut de la liste, indiquant la priorité la plus élevée. Par conséquent, l'ordre de priorité de tous les autres réseaux WLAN aurait été déplacés vers le bas et aurait été affiché dans la liste après le WLAN venant d'être ajouté.

```
$ netcfg
netcfg> create wlan mywifi
Created wlan 'mywifi'. Walking properties ...
priority (0)> 100
bssids>
keyname> mywifi-key
keyslot>
security-mode [none|wep|wpa]> wpa
netcfg:wlan:mywifi> list
WLAN:mywifi
    priority          100
    keyname           "mywifi-key"
    security-mode     wpa
netcfg:wlan:mywifi> verify
```

**EXEMPLE 4-5** Création d'un WLAN (Suite)

```
All properties verified
netcfg:wlan:mywifi> end
Committed changes
netcfg> list
NCPs:
    User
    Automatic
Locations:
    Automatic
    NoNet
    test-loc
ENMs:
    test-enm
WLANS:
    sunwifi
    ibahn
    gogoinflight
    admiralsclub
    hhonors
    sjcfreewifi
    mywifi
netcfg> exit
Nothing to commit
$
```

## Suppression de profils

Vous pouvez supprimer tous les profils définis par l'utilisateur ou un profil défini par l'utilisateur spécifié de la mémoire et du stockage persistant en utilisant la commande `netcfg destroy -a`.

---

**Remarque** – Les profils définis par le système, qui incluent le NCP automatique et les profils NoNet et d'emplacement automatique, ne peuvent pas être supprimés.

---

La syntaxe de la commande `destroy` est la suivante :

```
netcfg destroy object-type [ class ] object-name
```

Vous pouvez également utiliser la commande suivante pour supprimer tous les profils définis par l'utilisateur dans un système :

```
netcfg destroy -a
```

**EXEMPLE 4-6** Suppression de tous les profils définis par l'utilisateur à l'aide du mode ligne de commande `netcfg`

Pour supprimer tous les profils définis par l'utilisateur sur un système, tapez la commande suivante :

**EXEMPLE 4-6** Suppression de tous les profils définis par l'utilisateur à l'aide du mode ligne de commande `netcfg` (Suite)

```
$ netcfg destroy -a
```

Dans la mesure où au moins un profil doit être actif sur le système à tout moment, et pour éviter toute erreur en cours d'utilisation lors de la suppression de profils définis par l'utilisateur, assurez-vous que vous avez activé le NCP automatique avant d'utiliser la commande `destroy -a`.

**EXEMPLE 4-7** Suppression d'un profil défini par l'utilisateur spécifique à l'aide du mode ligne de commande `netcfg`

Pour supprimer un profil spécifique défini par l'utilisateur sur le système, par exemple le NCP nommé `User`, tapez la commande suivante :

```
$ netcfg destroy ncp User
```

La commande `destroy` peut également être utilisée pour supprimer les NCU d'un NCP existant. Dans l'exemple suivant, une interface NCU avec le nom `net1` est supprimée du NCP défini par l'utilisateur :

```
$ netcfg "select ncp User; destroy ncu ip net1"
```

Pour confirmer qu'un profil a été supprimé, utilisez la sous-commande `list`, comme indiqué ici :

```
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> list
NCUs:
    phys    net1
netcfg> exit
Nothing to commit
$
```

**EXEMPLE 4-8** Suppression interactive d'un profil

Dans l'exemple ci-après, une NCU IP nommé `net2` est supprimé.

```
$ netcfg list
NCPs:
    Automatic
    User
Locations:
    Automatic
    NoNet
    test
    foo
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> list
```

**EXEMPLE 4-8** Suppression interactive d'un profil (Suite)

```

NCUs:
    phys    net2
    ip      net2
netcfg:ncp:User> destroy ncu ip net2
Destroyed ncu 'net2'
netcfg:ncp:User> list
NCUs:
    phys    net2
netcfg:ncp:User> end
netcfg> exit
Nothing to commit
$

```

## Définition et modification des valeurs de propriétés pour un profil

Les valeurs de propriété pour les profils nouveaux et existants définis par l'utilisateur sont définis à l'aide de la commande `netcfg` avec la sous-commande `set`. Cette sous-commande peut être utilisée en mode interactif ou en mode ligne de commande. Si une valeur de propriété est définie ou modifiée en mode ligne de commande, le changement est immédiatement validé dans le stockage permanent.

La syntaxe de la sous-commande `set` est comme suit :

```
netcfg set prop-name=value1[,value2...]
```

Si vous avez besoin de récupérer une valeur de propriété spécifique, utilisez la commande `netcfg get`. Pour plus d'informations, reportez-vous à la section [“Obtention de valeurs d'une propriété spécifique” à la page 105](#).

**EXEMPLE 4-9** Définition des valeurs de propriété en mode ligne de commande `netcfg`

Si vous utilisez la commande `netcfg` pour définir une valeur de propriété en mode ligne de commande, plusieurs sous-commands doivent être saisies sur la ligne de commande.

Par exemple, pour définir la propriété `mtu` d'une NCU de lien `net1`, vous devez taper la commande suivante :

```
$ netcfg "select ncp User; select ncu phys net1; set mtu=1492"
```

Dans cet exemple, la sous-commande `select` est utilisée pour sélectionner le profil de niveau supérieur, puis de nouveau pour sélectionner le NCU qui contient la valeur de propriété `mtu` qui est modifiée.

Vous pouvez définir plusieurs valeurs en même temps pour une propriété donnée à partir de la ligne de commande. Lorsque vous définissez plusieurs valeurs, chaque valeur doit être séparée par une virgule (,). Si les valeurs d'une propriété spécifiée contiennent une virgule, la virgule

**EXEMPLE 4-9** Définition des valeurs de propriété en mode ligne de commande netcfg (Suite)

qui fait partie de la valeur de propriété doit être précédée d'une barre oblique inverse (\,). Les virgules dans les propriétés à valeur unique ne sont pas interprétées comme des séparateurs et n'ont donc pas besoin d'être précédées d'une barre oblique inverse.

Dans l'exemple suivant, la valeur de propriété ip-version du NCU, myncu, dans le NCP User est définie :

```
$ netcfg "select ncp User; select ncu ip myncu; set ip-version=ipv4,ipv6"
```

**EXEMPLE 4-10** Définition interactive des valeurs de propriétés pour un profil

Lors du paramétrage interactif des valeurs de propriété, vous devez d'abord sélectionner un profil à la portée actuelle, ce qui a pour effet de déplacer la session interactive dans la portée de ce profil. Depuis cette portée, vous pouvez sélectionner l'objet dont vous souhaitez modifier la propriété. Le profil sélectionné est alors chargé dans la mémoire à partir du stockage permanent. Dans cette portée, vous pouvez modifier le profil ou ses propriétés, comme indiqué dans l'exemple suivant :

```
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> select ncu ip iwk0
netcfg:ncp:User:ncu:iwk0> set ipv4-default-route = 129.174.7.366
```

Dans l'exemple suivant, la propriété ipfilter-config-file de l'emplacement foo est définie :

```
$ netcfg
netcfg> list
NCPs:
    Automatic
    User
Locations:
    Automatic
    NoNet
    foo

netcfg> select loc foo
netcfg:loc:foo> list
LOC:foo
    activation-mode          manual
    enabled                  false
    nameservices             dns
    dns-nameservice-configsrc dhcp
    nameservices-config-file  "/etc/nsswitch.dns"
netcfg:loc:foo> set ipfilter-config-file=/path/to/ipf-file
netcfg:loc:foo> list
LOC:foo
    activation-mode          manual
    enabled                  false
    nameservices             dns
    dns-nameservice-configsrc dhcp
    nameservices-config-file  "/etc/nsswitch.dns"
```

**EXEMPLE 4-10** Définition interactive des valeurs de propriétés pour un profil (Suite)

```

    ipfilter-config-file      "/path/to/ipf-file"
netcfg:loc:foo> end
Committed changes
netcfg> exit
Nothing to commit
$

```

Dans l'exemple suivant, la propriété `link-mtu` du NCU `net0` dans le NCP User est modifiée en mode interactif :

```

$ netcfg
netcfg> select ncp User
netcfg:ncp:User> select ncu phys net0
netcfg:ncp:User:ncu:net0> list
NCU:net0
  type          link
  class         phys
  parent        "User"
  enabled       true
  activation-mode prioritized
  priority-mode  exclusive
  priority-group 1
netcfg:ncp:User:ncu:net0> set link-mtu=5000
netcfg:ncp:User:ncu:net0> list
NCU:net0
  type          link
  class         phys
  parent        "User"
  enabled       true
  activation-mode prioritized
  priority-mode  exclusive
  priority-group 1
  link-mtu      5000
netcfg:ncp:User:ncu:net0> commit
Committed changes
netcfg:ncp:User:ncu:net0> exit
Nothing to commit
$

```

## Interrogation du système pour l'obtention d'informations du profil

La commande `netcfg` peut être utilisée avec la sous-commande `list` pour obtenir la liste de tous les profils, les paires propriété-valeur et les ressources qui existent au niveau de la portée actuelle ou spécifiée. Utilisez la sous-commande `list` pour interroger le système pour obtenir des informations générales sur tous les profils ou pour récupérer des informations spécifiques sur un profil particulier. La sous-commande `list` peut être utilisée en mode interactif ou en mode ligne de commande.

Si vous avez besoin d'obtenir des informations sur les profils et leur état actuel, utilisez la commande `netadm` avec la sous-commande `list`. Pour plus d'informations, reportez-vous à la section [“Affichage de l'état actuel d'un profil”](#) à la page 116.

## Création de la liste de tous les profils d'un système

La commande `netcfg list` répertorie tous les profils définis par le système et par l'utilisateur d'un système. Notez que l'utilisation de la sous-commande `list` sans aucune option affiche tous les profils de niveau supérieur qui sont dans un système. La commande ne répertorie pas l'état de chaque profil. Pour afficher la liste des profils et leur état (en ligne ou hors ligne), utilisez la commande `netadm list`.

Pour obtenir la liste de tous les profils de niveau supérieur sur un système, tapez la commande suivante :

```
$ netcfg list
NCPs:
    Automatic
    User
Locations:
    Automatic
    NoNet
    home
    office
ENMs:
    myvpn
    testenm
WLANs:
    workwifi
    coffeeshop
    homewifi
```

Dans cet exemple, les profils suivants sont répertoriés :

- **NCP**  
Deux NCP sont répertoriés : le NCP automatique, qui est un profil défini par le système, et un NCP défini par l'utilisateur nommé `User`.
- **Emplacements**  
Il existe quatre profils d'emplacements indiqués : deux emplacements qui sont définis par le système (`Automatic` et `NoNet`) et deux emplacements qui sont définis par l'utilisateur (`home` et `office`).
- **ENM**  
Il y a deux ENM répertoriés : un ENM pour une application VPN installée et configurée, et un ENM test.
- **WLAN**  
Il existe trois réseaux WLAN répertoriés : un WLAN pour le travail, un WLAN pour le café local et un WLAN pour le réseau personnel sans fil de l'utilisateur.

---

**Remarque** – Seuls les profils définis par l'utilisateur peuvent être créés, modifiés ou supprimés.

---

## Création d'une liste de toutes les valeurs de propriétés pour un profil spécifique

Utilisez la commande `netcfg` avec la sous-commande `list` pour obtenir la liste de toutes les valeurs des propriétés d'un profil spécifié.

La syntaxe de la sous-commande `list` est comme suit :

```
$ netcfg list [ object-type [ class ] object-name ]
```

**EXEMPLE 4-11** Création d'une liste de toutes les valeurs de propriété d'une NCU

Par exemple, pour créer une liste de toutes les valeurs de propriétés d'une NCU IP dans le NCP User, vous devez taper la commande suivante :

```
$ netcfg "select ncp User; list ncu ip net0"
NCU:net0
      type                interface
      class               ip
      parent              "User"
      enabled             true
      ip-version          ipv4
      ipv4-addrsrc        dhcp
      ipv6-addrsrc        dhcp,autoconf
```

**EXEMPLE 4-12** Création d'une liste de toutes les valeurs de propriété d'un ENM

Dans l'exemple suivant, toutes les propriétés pour un ENM nommé `myenm` sont répertoriées.

```
$ list enm myenm
ENM:myenm
activation-mode manual
enabled      true
start        "/usr/local/bin/myenm start"
stop         "/bin/alt_stop"
```

Dans cet exemple, la sortie de la sous-commande `list` affiche les informations suivantes :

- La propriété `activation-mode` de cet ENM est définie sur `manual`.
- L'ENM est activé.
- Les propriétés de méthode `start` et `stop` ont été spécifiées plutôt que d'utiliser un FMRI.



## Obtention de valeurs d'une propriété spécifique

Vous pouvez utiliser la commande `netcfg` avec la sous-commande `get` pour obtenir la valeur spécifique d'une propriété spécifiée. Cette sous-commande peut être utilisée dans le mode interactif ou le mode ligne de commande.

La syntaxe de la sous-commande `get` est comme suit :

```
netcfg get [ -V ] prop-name
```

Pour obtenir la valeur de la propriété `ip-version` d'une unité monétaire nationale nommée `myncu`, qui est une partie du NCP User, vous devez taper la commande suivante. Par exemple :

```
$ netcfg "select ncp User; select ncu ip myncu; get -V ip-version"  
ipv4
```

Si l'option `-V` est utilisée avec la sous-commande `get`, seule la valeur de la propriété est affichée, comme illustré ici :

```
netcfg:ncp:User:ncu:net0> get -V activation-mode  
manual
```

Dans le cas contraire, la propriété et sa valeur s'affichent. Par exemple :

```
netcfg:ncp:User:ncu:net0> get activation-mode  
activation-mode      manual
```

### ▼ Obtention interactive d'une seule valeur de propriété

Cette procédure décrit la méthode d'obtention d'une seule valeur de propriété à l'aide de la commande `netcfg get` en mode interactif `netcfg`. Dans cette procédure, certains de ces exemples montrent comment obtenir une seule valeur de propriété pour une NCU dans le NCP user. Ces exemples sont utilisés à des fins de démonstration *uniquement*. Les informations que vous fournissez lorsque vous utilisez cette commande peuvent varier, selon le profil et la valeur de la propriété que vous tentez d'obtenir.

Si vous voulez afficher toutes les valeurs des propriétés d'un profil, vous pouvez aussi utiliser la sous-commande `walkprop`. Cette sous-commande vous guide à travers toutes les propriétés d'un profil donné, une par une, ce qui vous permet de modifier une ou l'ensemble des propriétés du profil. Pour plus d'informations, reportez-vous à la section [“Affichage interactif et modification des valeurs de propriété à l'aide de la sous-commande `walkprop`”](#) à la page 107.

#### 1 Lancez une session `netcfg` en mode interactif.

```
$ netcfg  
netcfg>
```

## 2 Sélectionnez le profil ou l'objet de configuration qui contient la valeur de la propriété que vous souhaitez obtenir.

```
netcfg> select object-type [ class ] object-name
```

---

**Remarque** – Le paramètre *class* est applicable *uniquement* si vous sélectionnez une NCU. En outre, le paramètre *class* doit être spécifié si les NCU de classe *phys* et *ip* partagent le même nom. Cependant, si le nom de NCU est unique, le paramètre *class* n'est pas obligatoire.

---

Par exemple, pour sélectionner le NCP User, vous devez taper :

```
netcfg> select User NCP
```

Dans cet exemple, la sélection du NCP User déplace la session interactive dans la portée de l'objet sélectionné.

## 3 (Facultatif) Affichez les composants du profil.

```
netcfg:ncp:User> list
NCUs:
      phys      net0
      ip        net0
```

## 4 Sélectionnez l'objet qui contient la valeur de la propriété que vous souhaitez obtenir.

Dans l'exemple suivant, le lien (phys) NCU *net0* dans le NCP User est sélectionné :

```
netcfg:ncp:User> select ncu phys net0
```

La sélection de la NCU *net0* déplace la session interactive à la portée de l'objet et charge les propriétés en cours de la NCU de la mémoire de l'ordinateur.

## 5 Obtenez la valeur de propriété spécifiée.

```
netcfg:ncp:User:ncu:net0> get property-value
```

Par exemple, pour obtenir la valeur de la propriété *activation-mode*, tapez :

```
netcfg:ncp:User:ncu:net0> get activation-mode
activation-mode      manual
```

### Étapes suivantes

A ce stade, vous pouvez définir une nouvelle valeur pour la propriété en utilisant la sous-commande *set*, ou vous pouvez quitter la session interactive sans effectuer de modifications. Notez que si vous modifiez une valeur de propriété tout en étant en mode interactif, vous devez utiliser la sous-commande *commit* ou *exit* pour enregistrer vos modifications. Pour plus d'informations sur la définition d'une valeur de propriété en mode interactif *netcfg*, reportez-vous à la section “[Définition et modification des valeurs de propriétés pour un profil](#)” à la page 100.

## Affichage interactif et modification des valeurs de propriété à l'aide de la sous-commande `walkprop`

La sous-commande `walkprop` peut être utilisée de façon interactive pour afficher les propriétés d'un profil. Cette sous-commande vous guide à travers un profil, une propriété à la fois, en affichant le nom et la valeur actuelle de chaque propriété. Une invite de commande interactive est également affichée que vous pouvez utiliser pour modifier la valeur en cours de la propriété spécifiée. Le séparateur des propriétés à valeurs multiples est une virgule ( , ). Si une valeur spécifique d'une propriété donnée contient une virgule, elle doit être précédée d'une barre oblique inverse ( \ ). Les virgules dans les propriétés à valeur unique ne sont pas interprétées comme des séparateurs et n'ont pas besoin d'être précédées d'une barre oblique inverse.

---

**Remarque** – La sous-commande `walkprop` est utile lorsqu'elle est utilisée en mode interactif uniquement.

---

**EXEMPLE 4-13** Affichage et modification des valeurs de propriétés pour un profil spécifique

Dans l'exemple suivant, la propriété `activation-mode` pour l'emplacement `foo` est affichée, puis modifiée en utilisant la sous-commande `walkprop`. Notez que lorsque vous utilisez la sous-commande `walkprop`, il n'est pas nécessaire d'utiliser la sous-commande `set` pour définir la valeur de la propriété.

```
$ netcfg
netcfg> select loc foo
netcfg:loc:foo> list
loc:foo
    activation-mode          manual
    enabled                  false
    nameservices             dns
    nameservices-config-file "/etc/nsswitch.dns"
    dns-nameservice-configsrc dhcp
    nfsv4-domain             "Central.oracle.com"

netcfg:loc:foo> walkprop
activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-all
conditions> advertised-domain is oracle.com
nameservices (dns) [dns|files|nis|ldap]>
nameservices-config-file ("/etc/nsswitch.dns")>
dns-nameservice-configsrc (dhcp) [manual|dhcp]>
nfsv4-domain ("Central.oracle.com")>
ipfilter-config-file>
ipfilter-v6-config-file>
ipnat-config-file>
ippool-config-file>
ike-config-file>
ipsecpolicy-config-file>
netcfg:loc:foo> list
loc:foo
    activation-mode          conditional-all
    conditions               "advertised-domain is oracle.com"
    enabled                  false
```

**EXEMPLE 4-13** Affichage et modification des valeurs de propriétés pour un profil spécifique (Suite)

```
nameservices          dns
nameservices-config-file  "/etc/nsswitch.dns"
dns-nameservice-configsrc dhcp
nfsv4-domain          "Central.oracle.com"
netcfg:loc:foo> commit
Committed changes
netcfg:loc:foo> end
netcfg> exit
$
```

---

**Remarque** – Seules les propriétés pertinentes sont parcourues. Par exemple, si la propriété `ipv4-addrsrc` est définie sur `static`, la propriété `ipv4-addr` est incluse dans le parcours. Cependant, si `ipv4-addrsrc` est définie sur `dhcp`, la propriété `ipv4-addr` n'est pas parcouru.

---

## Exportation et restauration d'une configuration de profil

Vous pouvez utiliser la sous-commande `export` pour enregistrer et restaurer les configurations de profil. L'exportation d'un profil peut être utile aux administrateurs système chargés de la maintenance de plusieurs serveurs nécessitant des configurations réseau identiques. La sous-commande `export` peut être utilisée en mode interactif ou en mode ligne de commande. Vous pouvez également utiliser la commande en mode fichier de commande pour spécifier un fichier en tant que la sortie de la commande.

La syntaxe de commande de la sous-commande `export` est comme suit :

```
$ netcfg export [ -d ] [ -f output-file ] [ object-type [ class ] object-name ]
```

---

**Remarque** – Les options `-d` et `-f` de la sous-commande `export` peuvent être utilisées indépendamment les unes des autres.

---

**EXEMPLE 4-14** Exportation d'une configuration de profil

Dans l'exemple suivant, la sous-commande `export` est utilisée pour afficher la configuration de profil d'un système à l'écran.

```
$ netcfg
netcfg> export
create ncp "User"
create ncu ip "net2"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
```

**EXEMPLE 4-14** Exportation d'une configuration de profil (Suite)

```

create ncu phys "net2"
set activation-mode=manual
set link-mtu=5000
end
create ncu phys "wpi2"
set activation-mode=prioritized
set priority-group=1
set priority-mode=exclusive
set link-mac-addr="13:10:73:4e:2"
set link-mtu=1500
end
end
create loc "test"
set activation-mode=manual
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domainl.oracle.com"
end
create loc "foo"
set activation-mode=conditional-all
set conditions="system-domain is oracle.com"
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create enm "myenm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 1.2.3.4"
set start="/my/start/script"
set stop="/my/stop/script"
end
create wlan "mywlan"
set priority=0
set bssids="0:13:10:73:4e:2"
end
netcfg> end
$

```

**EXEMPLE 4-15** Exportation d'une configuration de profil netcfg en mode interactif

Dans l'exemple suivant, l'option `-d` est utilisée avec la sous-commande `exporter`. L'option `-d` ajoute la commande `destroy -a` en tant que première ligne de la sortie `netcfg export`.

```

$ netcfg
netcfg> export -d
destroy -a
create ncp "User"
create ncu ip "net2"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
create ncu phys "net2"

```

**EXEMPLE 4-15** Exportation d'une configuration de profil netcfg en mode interactif (Suite)

```

set activation-mode=manual
set link-mtu=5000
end
create ncu phys "wpi2"
set activation-mode=prioritized
set priority-group=1
set priority-mode=exclusive
set link-mac-addr="13:10:73:4e:2"
set link-mtu=1500
end
end
create loc "test"
set activation-mode=manual
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create loc "foo"
set activation-mode=conditional-all
set conditions="system-domain is oracle.com"
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create enm "myenm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 1.2.3.4"
set start="/my/start/script"
set stop="/my/stop/script"
end
create wlan "mywlan"
set priority=0
set bssids="0:13:10:73:4e:2"
end
netcfg> end
$

```

**EXEMPLE 4-16** Exportation d'un profil de configuration netcfg en mode fichier de commande

Dans l'exemple suivant, les informations de configuration pour le NCP User sont écrites dans un fichier à l'aide de la commande `netcfg export` avec l'option `-f`. L'option `-f` option écrit la sortie dans un nouveau fichier nommé `user2`. L'option `-d` ajoute la commande `destroy -a` en tant que première ligne de la sortie `netcfg export`.

```
$ netcfg export -d -f user2 ncp User
```

```

$ ls -al
drwx-----  3 root    root          4 Oct 14 10:53 .
drwxr-xr-x  37 root    root        40 Oct 14 10:06 ..
-rw-r--r--   1 root    root       352 Oct 14 10:53 user2
$

```

**EXEMPLE 4-16** Exportation d'un profil de configuration netcfg en mode fichier de commande (Suite)

```

$ cat user2
destroy -a
create ncp "User"
create ncu ip "net2"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
create ncu phys "net2"
set activation-mode>manual
set link-mtu=5000
end
create ncu phys "wpi2"
set activation-mode=prioritized
set priority-group=1
set priority-mode=exclusive
set link-mac-addr="13:10:73:4e:2"
set link-mtu=1500
end
end
create loc "test"
set activation-mode>manual
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create loc "foo"
set activation-mode=conditional-all
set conditions="system-domain is oracle.com"
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create enm "myenm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 1.2.3.4"
set start="/my/start/script"
set stop="/my/stop/script"
end
create wlan "mywlan"
set priority=0
set bssids="0:13:10:73:4e:2"
end
$

```

## Restauration d'un profil défini par l'utilisateur

Vous pouvez restaurer un profil défini par l'utilisateur à l'aide de la commande `netcfg` avec l'option `-f`, comme suit :

```
$ netcfg [ -f ] profile-name
```

Par exemple :

```
$ netcfg -f user2
```

Cette commande exécute le fichier de commandes qui contient la configuration exportée.

## Gestion de la configuration réseau par l'intermédiaire de SMF

La gestion de la configuration réseau est actuellement répartie sur plusieurs services SMF. La configuration de liens et d'interfaces, et le style de gestion sont gérés par le service `network/physical:default`.

### ▼ Procédure permettant de passer du mode de configuration réseau NWAM au mode de configuration réseau classique

Si vous utilisez des fonctions réseau avancées qui ne sont pas actuellement prises en charge par la gestion de configuration NWAM, ou si vous préférez la gestion de configuration réseau traditionnelle, vous pouvez activer le NCP `DefaultFixed`, comme indiqué dans la procédure suivante.

**1 Connectez-vous en tant qu'utilisateur root.**

**2 Activez le NCP `DefaultFixed`.**

```
# netadm enable -p ncp DefaultFixed
```

**3 Vérifiez que le service `network/physical:default` a redémarré et qu'il est en ligne.**

```
# svcs -xv network/physical:default
svc:/network/physical:default (physical network interface configuration)
State: online since Fri Aug 26 16:19:18 2011
  See: man -M /usr/share/man -s 1M ipadm
  See: man -M /usr/share/man -s 5 nwam
  See: /var/svc/log/network-physical:default.log
Impact: None.
#
```

**4 Vérifiez que le NCP `DefaultFixed` est actif.**

```
# netadm list
netadm: DefaultFixed NCP is enabled;
automatic network management is not available.
'netadm list' is only supported when automatic network management is active.
```



## ▼ Procédure permettant de passer du mode de configuration réseau classique au mode de configuration réseau NWAM

Pour revenir au mode de configuration réseau NWAM à partir du mode de mode de configuration réseau traditionnel, activez le NCP NWAM que vous souhaitez utiliser.

**1 Connectez-vous en tant qu'utilisateur root.**

**2 Activez un NCP NWAM.**

```
# netadm enable -p ncp Automatic
```

**3 Vérifiez que le service network/physical:default a redémarré et qu'il est en ligne.**

```
# svcs -xv network/physical:default
svc:/network/physical:default (physical network interface configuration)
  State: online since Fri Aug 26 16:19:18 2011
    See: man -M /usr/share/man -s 1M ipadm
    See: man -M /usr/share/man -s 5 nwam
    See: /var/svc/log/network-physical:default.log
  Impact: None.
#
```

**4 Vérifiez l'état du NCP et des autres profils NWAM.**

```
# netadm list -x
```

TYPE	PROFILE	STATE	AUXILIARY STATE
ncp	Automatic	online	active
ncu:phys	net0	online	interface/link is up
ncu:ip	net0	online	interface/link is up
ncu:phys	net1	offline	interface/link is down
ncu:ip	net1	offline	conditions for activation are unmet
ncp	User	disabled	disabled by administrator
loc	Automatic	online	active
loc	NoNet	offline	conditions for activation are unmet

```
#
```



## Administration des profils NWAM (tâches)

---

Ce chapitre décrit l'utilisation de la commande `netadm` pour administrer les profils NCP, emplacements, ENM et WLAN. La commande `netadm` permet également d'administrer les NCU, à savoir les objets de configuration qui composent un NCP, et d'interagir avec le démon NWAM (`nwamd`) en l'absence de l'interface graphique NWAM. Pour plus d'informations sur la commande `netadm`, reportez-vous à la page de manuel [netadm\(1M\)](#).

Ce chapitre comprend les sections suivantes :

- “Obtention d'informations sur les états de profils” à la page 116
- “Activation et désactivation des profils ” à la page 118
- “Exécution d'une analyse sans fil et connexion aux réseaux sans fil disponibles ” à la page 121
- “Dépannage de la configuration réseau NWAM” à la page 122

Pour plus d'informations sur la création de profils et la configuration de leurs propriétés à l'aide de la commande `net cfg`, reportez-vous au [Chapitre 4, “Configuration de profil NWAM \(tâches\)”](#).

Pour plus d'informations sur l'interaction avec la configuration NWAM et la gestion de la configuration réseau à partir du bureau à l'aide de l'interface graphique NWAM, reportez-vous au [Chapitre 6, “A propos de l'interface graphique NWAM”](#).

Pour obtenir une présentation de NWAM, reportez-vous au [Chapitre 2, “Présentation de NWAM”](#).

Pour plus d'informations sur tous les composants, NWAM et plus de détails sur la configuration NWAM, reportez-vous au [Chapitre 3, “Configuration et administration NWAM \(présentation\)”](#).

## Obtention d'informations sur les états de profils

La commande `netadm` exécutée avec la sous-commande `list` permet d'afficher tous les profils disponibles sur un système et leur état ou un profil spécifique et son état.

La syntaxe de la sous-commande `list` est la suivante :

```
netadm list [ -p profile-type ] [ -c ncu-class ] [ profile-name ]
```

Par exemple, pour afficher tous les profils d'un système et leur état, vous devez saisir la commande suivante :

```
$ netadm list
TYPE          PROFILE      STATE
ncp            User         disabled
ncp            Automatic    online
ncu:ip         net1         offline
ncu:phys       net1         offline
ncu:ip         net0         online
ncu:phys       net0         online
loc            foo          disabled
loc            test         disabled
loc            NoNet        offline
loc            Automatic    online
$
```

Dans cet exemple, tous les profils définis par le système et définis par l'utilisateur présents sur le système sont affichés avec leur état actuel. Notez que la sous-commande `list` affiche le NCP activé et toutes les NCU qui le constituent.

## Affichage de l'état actuel d'un profil

Le type de profil et la classe de NCU peuvent être inclus dans la syntaxe de commande pour identifier un profil spécifique. Si seul un type de profil est fourni, tous les profils de ce type s'affichent. Si un profil est spécifié nominativement, l'état actuel de ce profil s'affiche. Si le nom du profil n'est pas unique, tous les profils portant ce nom sont répertoriés.

Les valeurs d'état possibles pour chaque profil sont les suivantes :

**disabled** Indique un profil activé manuellement, qui n'est pas actif.

**offline** Indique un profil activé conditionnellement ou par le système, qui n'est pas actif. Le profil n'est peut-être pas actif parce que ses conditions n'ont pas été satisfaites ou parce qu'un autre profil dont les conditions plus spécifiques ont été satisfaites est actif.

---

**Remarque** – L'état `offline` survient plus souvent dans le cas des types de profil devant être activés séparément, comme le profil d'emplacement.

---

<code>online</code>	Indique un profil activé conditionnellement ou par le système, dont les conditions sont vérifiées et dont l'activation a réussi. Peut également indiquer un profil activé manuellement, devenu actif à la demande de l'utilisateur.
<code>maintenance</code>	Indique que la tentative d'activation du profil a échoué.
<code>initialized</code>	Indique que le profil est valide, mais qu'aucune action n'a été entreprise sur le profil.
<code>uninitialized</code>	Indique que le profil n'est pas présent dans le système. Par exemple, cet état peut se produire lorsqu'une NCU correspondant à un lien physique est retirée du système.

#### EXEMPLE 5-1 Affichage de l'état en cours d'un profil spécifié

L'exemple suivant indique l'état actuel du NCP Automatique, spécifié par un nom :

```
$ netadm list Automatic
TYPE      PROFILE      STATE
ncp        Automatic    online
ncu:ip     net1         offline
ncu:phys   net1         offline
ncu:ip     net0         online
ncu:phys   net0         online
loc        Automatic    online
```

Dans l'exemple suivant, la sous-commande `list` est utilisée avec l'option `-p` pour afficher tous les emplacements sur le système :

```
$ netadm list -p loc
TYPE      PROFILE      STATE
loc        foo          disabled
loc        test        disabled
loc        NoNet       offline
loc        Automatic   online
$
```

Dans l'exemple suivant, la sous-commande `list` est utilisée avec l'option `-c` pour afficher toutes les NCU d'interface dans le NCP actif :

```
$ netadm list -c ip
TYPE      PROFILE      STATE
ncu:ip     net0         online
ncu:ip     net1         disabled
$
```

## Valeurs d'état auxiliaire

L'état auxiliaire d'un profil fournit la raison pour laquelle un profil donné est online ou offline (activé ou désactivé). Pour répertorier les valeurs d'état auxiliaire, utilisez l'option `-x` avec la sous-commande `list`, comme indiqué dans l'exemple suivant :

```
$ netadm list -x
TYPE      PROFILE      STATE      AUXILIARY STATE
ncp       Automatic    disabled   disabled by administrator
ncp       User         online     active
ncu:phys  nge0         online     interface/link is up
ncu:ip    nge0         online     interface/link is up
ncu:phys  nge1         offline    interface/link is down
ncu:ip    nge1         offline    conditions for activation are unmet
loc       Automatic    offline    conditions for activation are unmet
loc       NoNet        offline    conditions for activation are unmet
loc       office       online     active
```

Les valeurs d'état auxiliaire varient selon le type de profil. Pour obtenir des informations détaillées sur les états auxiliaires, reportez-vous à la page de manuel [nwamd\(1M\)](#).

## Activation et désactivation des profils

Les NCP définis par l'utilisateur, les profils d'emplacement et les ENM possèdent tous des propriétés `activation-mode`. Les valeurs autorisées pour chaque profil sont déterminées par son type.

Pour activer ou désactiver manuellement un profil ou objet de configuration, utilisez la commande `netadm enable` ou `netadm disable`, respectivement. Les profils définis par le système aussi bien que ceux définis par l'utilisateur peuvent être activés et désactivés, si la propriété `activation-mode` du profil spécifié est définie sur `manual`. La propriété `activation-mode` est définie lorsque vous créez ou modifiez un profil à l'aide de la commande `netcfg`. Pour plus d'informations, reportez-vous à la section [“Activation des profils NWAM” à la page 58](#).

A tout moment, un profil d'emplacement et un NCP doivent être actifs sur le système. L'activation d'un autre NCP ou emplacement dont la propriété `activation-mode` est définie sur `manual` désactive implicitement le NCP ou le profil d'emplacement actif. L'emplacement actuel peut également être désactivé, si sa propriété `activation-mode` est définie sur `manual`. Si aucun autre emplacement n'est disponible, NWAM a recours à un des emplacements définis par le système, à savoir soit l'emplacement Automatique (si la configuration IP a réussi), soit l'emplacement NoNet. Les emplacements conditionnels et système peuvent être activés manuellement, ce qui signifie qu'ils restent actifs jusqu'à leur désactivation explicite. De par ce comportement, il est facile qu'un profil d'emplacement conditionnel devienne "toujours activé". La désactivation de l'emplacement conditionnel redonne au système son comportement

conditionnel normal. Lorsqu'un emplacement est activé manuellement, le système ne le modifie pas, même si les conditions de l'emplacement activé conditionnellement sont remplies.

---

**Remarque** – Vous ne pouvez pas désactiver explicitement le NCP qui est actif sur un système, car vous arrêteriez alors la connectivité réseau de base du système. Un NCP est désactivé implicitement lorsqu'un autre NCP est activé manuellement. Toutefois, il n'existe aucune contrainte sur l'activation ENM. Aucun ou plusieurs ENM peuvent être actifs sur un système à un moment donné. Par conséquent, l'activation ou la désactivation d'un ENM n'a aucun effet sur les autres ENM actifs.

---

Vous pouvez également activer et désactiver manuellement chaque NCU. Notez que la NCU spécifiée doit faire partie du NCP actif et que sa propriété `activation-mode` doit être définie sur `manual`. Si la classe NCU n'est pas spécifiée, toutes les NCU (une NCU de lien et une NCU d'interface avec ce nom) sont activées ou désactivées.

L'activation et la désactivation d'objets s'effectuent de manière asynchrone. Par conséquent, la demande d'activation ou de désactivation peut réussir, alors que l'action (activer ou désactiver) échoue. Une défaillance de ce genre se reflète dans l'état du profil, qui devient `maintenance`, indiquant l'échec de la dernière action effectuée sur le profil. Pour plus d'informations sur l'affichage de l'état des profils, reportez-vous à la section [“Obtention d'informations sur les états de profils” à la page 116](#).

#### EXEMPLE 5-2 Activation d'un profil

La syntaxe pour activer manuellement un profil est la suivante :

```
netadm enable [ -p profile-type ] [ -c ncu-class ] profile-name
```

Si le nom de profil n'est pas unique (par exemple, s'il existe sur le système plusieurs profils portant le même nom, mais de types différents), vous devez également spécifier le type de profil.

L'option `-p` permet de spécifier un des types de profil suivants :

- `ncp`
- `ncu`
- `loc`
- `enm`

Si le type de l'objet de configuration est `ncu`, l'option `-c` permet de distinguer la classe NCU. L'option `-c` s'avère utile lorsque deux NCU dont les noms sont identiques existent sur le système.

Si l'option `-c` est utilisée, elle doit spécifier le type de classe `phys` ou `ip`.

Dans l'exemple suivant, un emplacement nommé `office` est activé :

**EXEMPLE 5-2** Activation d'un profil (Suite)

```
$ netadm enable -p loc office
```

Où *profile-type* est *loc* et *profile-name* est *office*. Notez que l'option *-c ncu-class* n'est pas utilisée dans cet exemple, car le type de profil est un emplacement et non un NCP.

```
$ netadm enable -p ncp user
Enabling ncp 'User'
.
.
.
```

Notez que lorsque vous spécifiez les noms de profil, la commande *netadm* est sensible à la casse.

**EXEMPLE 5-3** Désactivation d'un profil

La syntaxe pour désactiver manuellement un profil est la suivante :

```
netadm disable [ -p profile-type ][ -c ncu-class ] profile-name
```

Si le nom de profil n'est pas unique, vous devez également spécifier le type de profil.

L'option *-p* peut être utilisée pour spécifier un des types d'objet ou de profil suivants :

- *ncp*
- *ncu*
- *loc*
- *enm*

Si le type de l'objet de configuration est *ncu*, l'option *-c* doit également être utilisée pour distinguer la classe NCU.

La classe NCU doit être spécifiée en tant que *phys* ou *ip*.

Par exemple, pour désactiver manuellement une NCU de lien nommée *net1*, vous devez taper la commande suivante :

```
$ netadm disable -p ncu -c phys net1
```

Où *profile-type* est *ncu*, *ncu-class* est *phys* et *profile-name* est *net1*. Notez que l'option *-c ncu-class* est utilisée dans cet exemple, car l'objet de configuration est une NCU.



## Exécution d'une analyse sans fil et connexion aux réseaux sans fil disponibles

Vous pouvez rechercher les réseaux sans fil disponibles et vous y connecter à l'aide de la commande `netadm`.

Utilisez la commande `netadm scan-wifi link-name` pour analyser une liaison sans fil et obtenir une liste des réseaux sans fil disponibles.

Utilisez la commande `netadm select-wifi link-name` pour sélectionner un réseau sans fil et vous y connecter dans les résultats de l'analyse du lien spécifié comme *link-name*. La sous-commande `select-wifi link-name` vous invite à fournir une sélection Wi-Fi, une clé et un emplacement de clé, si nécessaire.

---

**Remarque** – Vous devez créer une clé avant d'utiliser la commande `netadm select-wifi`.

---

Vous pouvez également déclencher une analyse ultérieure du réseau pour rechercher des réseaux sans fil disponibles à l'aide de la commande `netadm scan-wifi link-name`. Notez qu'une analyse ultérieure risque de ne pas déclencher un événement d'analyse, si les nouveaux résultats sont identiques à ceux qui existent déjà. Le démon `nwamd` effectue l'analyse, indépendamment des modifications apportées aux données depuis la dernière analyse.

Dans l'exemple suivant, la commande `netadm scan-wifi` est utilisée pour effectuer une analyse de la liaison sans fil `net1`. La commande `netadm select-wifi` est ensuite utilisée pour afficher une liste des réseaux sans fil dans laquelle effectuer votre choix. La liste qui s'affiche est fonction des résultats de l'analyse précédemment exécutée sur `net1`.

```
$ netadm select-wifi net1
1: ESSID home BSSID 0:b:e:85:26:c0
2: ESSID neighbor1 BSSID 0:b:e:49:2f:80
3: ESSID testing BSSID 0:40:96:29:e9:d8
4: Other
Choose WLAN to connect to [1-4]: 1
$
```

Dans cet exemple, le réseau sans fil représenté par le chiffre 1 sélectionne le réseau `home`.

Lorsque le WLAN nécessite une clé, vous êtes invité à saisir la clé et son emplacement, si WEP est spécifié. Par exemple :

```
Enter WLAN key for ESSID home: mywlankey
Enter key slot [1-4]: 1
```

## Dépannage de la configuration réseau NWAM

Les informations contenues dans cette section portent sur la résolution des problèmes de configuration réseau NWAM.

### Surveillance de l'état en cours de toutes les connexions réseau

La commande `netadm` peut être utilisée avec la sous-commande `show-events` pour écouter et afficher les événements surveillés par le démon NWAM, `nwamd`. Cette sous-commande fournit des informations utiles sur les événements liés au processus de configuration des profils et objets de configuration, tels que configurés par NWAM.

La syntaxe de la commande `netadm show-events` est la suivante :

**netadm show-events [-v]**

Dans l'exemple suivant, la commande `nwam show-events` est utilisée avec l'option `-v` pour afficher les événements en mode détaillé :

```
$ netadm show-events -v
EVENT DESCRIPTION
LINK_STATE net0 -> state down
OBJECT_STATE ncu link:net0 -> state online*, interface/link is down
OBJECT_STATE ncu link:net0 -> state offline, interface/link is down
OBJECT_STATE ncu interface:net0 -> state online*, conditions for act
OBJECT_STATE ncu interface:net0 -> state offline, conditions for act
IF_STATE net0 -> state (0) flags 2004801
IF_STATE net0 -> state (0) flags 2004800
IF_STATE net0 -> state (0) flags 1004803
IF_STATE net0 -> state index 4 flags 0x0 address fe80::214:4fff:
IF_STATE net0 -> state (0) flags 1004802
IF_STATE net0 -> state index 4 flags 0x0 address 129.156.235.229
IF_STATE net0 -> state (0) flags 1004803
IF_STATE net0 -> state (0) flags 1004802
IF_STATE net0 -> state (0) flags 1004803
IF_STATE net0 -> state (0) flags 1004802
```

### Correction des problèmes liés à la configuration de l'interface réseau

La commande `netadm list -x` est utile pour déterminer pourquoi une interface réseau n'est peut-être pas configurée correctement. Cette commande affiche les diverses entités configurées par NWAM, leur état actuel et la raison pour laquelle ces entités sont dans cet état.

Par exemple, si un câble est débranché, vous pouvez utiliser la commande `netadm list -x` pour déterminer si l'état de la liaison est `offline` et pour quelle raison ("liaison arrêtée", par exemple). De même, pour la détection d'adresses dupliquées, la sortie de la commande `netadm list -x` révèle que le lien physique est en ligne, mais que l'interface IP est dans un état de maintenance. Dans cette instance, la raison donnée est qu'une adresse en double a été détectée.

Voici un exemple de résultat de la commande `netadm list -x` :

```
$ netadm list -x
TYPE      PROFILE      STATE      AUXILIARY STATE
ncp        Automatic    online     active
ncu:phys   net0         offline    interface/link is down
ncu:ip     net0         offline    conditions for activation are unmet
ncu:phys   net1         offline*   need WiFi network selection
ncu:ip     net1         offline    conditions for activation are unmet
ncp        User         disabled   disabled by administrator
loc        Automatic    offline    conditions for activation are unmet
loc        NoNet        online     active
loc        office       offline    conditions for activation are unmet
$
```

Après avoir déterminé la raison pour laquelle un lien ou une interface se trouve hors ligne, procédez à la résolution du problème. Dans le cas d'une adresse IP en double, vous devez modifier l'adresse IP statique affectée à l'interface spécifiée à l'aide de la commande `netcfg`. Pour obtenir des d'instructions, reportez-vous à la section [“Définition et modification des valeurs de propriétés pour un profil” à la page 100](#). Une fois les modifications validées, exécutez la commande `netadm list -x` à nouveau pour vérifier que l'interface est maintenant configurée correctement et que son état affiché est `online`.

Une autre raison pour laquelle une interface peut ne pas être configurée correctement est l'indisponibilité de WLAN connus. Dans ce cas, l'état du lien Wi-Fi affiché est `offline`, car une sélection wifi est attendue. Ou, si une sélection Wi-Fi a été effectuée, mais qu'une clé est requise, la configuration incorrecte de l'interface est due à l'absence de clé wifi.



## A propos de l'interface graphique NWAM

---

Ce chapitre propose une introduction à l'interface graphique NWAM, y compris une description de ses composants. Il contient également des instructions générales relatives à l'interaction avec NWAM à partir du bureau, au contrôle des connexions réseau, à l'ajout de réseaux sans fil, et la création et la gestion des profils réseau.

Ce chapitre ne fournit pas d'instructions détaillées sur la gestion de votre réseau exclusivement à l'aide de l'interface graphique. Pour obtenir des instructions étape par étape, reportez-vous à l'aide en ligne, accessible en cliquant avec le bouton droit de la souris sur l'icône Etat du réseau, qui s'affiche en permanence dans la zone de notification du bureau. Des liens dans l'interface graphique vous permettent d'accéder à des pages de l'aide en ligne fournissant des informations plus détaillées sur chaque rubrique. Vous pouvez également naviguer dans l'aide en ligne en cliquant sur les liens intégrés dans le texte ou sur les différentes rubriques dans le panneau latéral.

Ce chapitre comprend les sections suivantes :

- [“Présentation de l'interface graphique NWAM” à la page 125](#)
- [“Composants fonctionnels de l'interface graphique NWAM” à la page 128](#)
- [“Interaction avec NWAM à partir du bureau” à la page 130](#)
- [“Connexion et gestion des réseaux sans fil favoris” à la page 134](#)
- [“Gestion des profils réseau” à la page 136](#)
- [“Création et gestion des emplacements” à la page 143](#)
- [“A propos des modificateurs réseau externes” à la page 146](#)

## Présentation de l'interface graphique NWAM

L'interface graphique NWAM est l'équivalent graphique de l'interface utilisateur de ligne de commande NWAM. L'interface graphique NWAM vous permet de visualiser et de contrôler l'état de votre réseau sur le bureau, mais aussi d'interagir avec NWAM pour gérer la configuration Ethernet et sans fil. En outre, vous pouvez réaliser diverses tâches liées à la mise en réseau à partir du bureau, telles que la connexion à un réseau câblé ou sans fil au démarrage

et la configuration de nouveaux réseaux câblés ou sans fil. L'interface graphique NWAM peut également être utilisée pour créer et gérer des emplacements, profils qui simplifient la tâche complexe consistant à configurer le réseau à l'échelle du système. Le composant d'interface graphique comporte une fonction qui affiche les notifications concernant l'état actuel de votre connexion réseau, ainsi que des informations sur l'état général de votre environnement réseau.

Fonctions de base de l'interface graphique NWAM :

- Notification de l'état du réseau
- Détection des événements d'enfichage à chaud
- Création et gestion des profils réseau
- Gestion des réseaux sans fil

L'interface graphique NWAM gère la configuration réseau de la même façon que l'interface de ligne de commande (CLI) NWAM, par stockage des valeurs de propriété souhaitées sous forme de profils sur le système. Le service NWAM détermine quel profil doit être actif à un moment donné en fonction des conditions du réseau, puis active le profil qui convient le mieux.

## Accès à l'interface graphique NWAM à partir du bureau

L'interface graphique NWAM est constituée de deux composants : l'icône de notification Etat du réseau, qui s'affiche en permanence sur le panneau du bureau, et les boîtes de dialogue de configuration du réseau, qui sont accessibles à partir du menu Système → Administration ou en cliquant avec le bouton droit sur l'icône de notification. L'interface graphique NWAM fonctionne de façon très similaire à n'importe quelle autre application dotée d'une icône de notification d'état en continu, par exemple, l'icône de gestion de l'alimentation ou l'icône d'imprimante. Ces applications permettent de réaliser certaines tâches en accédant à leur menu contextuel (clic droit) ou en utilisant les boîtes de dialogue de configuration, accessibles à partir de l'icône ou de divers menus de préférences.

L'icône du panneau est votre point de contact le plus fréquent avec NWAM. Elle indique si vous êtes connecté à un réseau câblé ou sans fil. Placez le curseur de la souris sur l'icône pour qu'une info-bulle affiche des informations supplémentaires, telles que le NCP et le profil d'emplacement actifs. En cliquant avec le bouton droit de la souris sur l'icône, vous pouvez modifier la configuration réseau de base de votre système, par exemple la connexion à un autre réseau sans fil.

Cliquez (avec le bouton gauche) sur l'icône du panneau et la boîte de dialogue Préférences réseau s'ouvre. Cette boîte de dialogue peut également s'ouvrir à partir du menu Système → Administration. Elle permet d'effectuer des tâches de configuration réseau plus détaillées, comme la définition des adresses IPv4 et IPv6 statiques, la définition des priorités de connexion, la gestion des ENM (External Network Modifier, modificateur réseau externe) et la création de groupes de paramètres réseau à utiliser dans des emplacements différents.

## Différences entre l'interface de ligne de commande NWAM et l'interface graphique NWAM

Vous pouvez gérer la configuration réseau via NWAM à l'aide de l'interface de ligne de commande ou de l'interface graphique. Les deux interfaces utilisateur peuvent être utilisées pour gérer la configuration du réseau et interagir avec la configuration NWAM. Le choix de l'interface de ligne de commande ou de l'interface graphique pour effectuer une tâche particulière dépend de la tâche elle-même et de la situation donnée. Pour certaines tâches, il est plus logique d'utiliser l'interface graphique NWAM. Il peut s'agir, par exemple, de vérifier l'état de votre connexion réseau active ou de sélectionner un réseau sans fil auquel vous connecter au démarrage. Ces tâches peuvent être plus facilement et rapidement exécutées par interaction directe avec NWAM à partir du bureau via l'interface graphique. Pour effectuer des tâches plus complexes, telles que la spécification d'un script en tant que méthode de démarrage et d'arrêt pour un nouvel ENM, il est conseillé d'utiliser le mode ligne de commande.

Bien que la CLI et l'interface graphique soient pratiquement identiques, il convient de noter les différences suivantes :

- **Différences de fonctionnalités**

L'interface utilisateur comprend des fonctionnalités qui vous permettent d'interagir avec NWAM et de vérifier les connexions réseau à partir du bureau. La méthode d'obtention des informations concernant l'état de votre réseau varie légèrement entre les utilitaires d'interface graphique et d'interface de ligne de commande. Si vous utilisez le composant d'interface graphique, les notifications s'affichent sur le bureau au moment où elles se produisent. Si vous utilisez l'utilitaire de ligne de commande, vous pouvez surveiller les événements NWAM lorsqu'ils se produisent à l'aide de la commande `netadm show-events`. Pour plus d'informations, reportez-vous à la section [“Surveillance de l'état en cours de toutes les connexions réseau” à la page 122](#).

En outre, pour obtenir des informations sur l'état de votre réseau à l'aide de l'interface graphique, vous devez vérifier, déplacer le curseur de la souris sur ou cliquer sur l'icône de notification Etat du réseau affichée sur le bureau. Pour obtenir plus d'informations sur l'état de votre réseau à partir de la ligne de commande, utilisez la commande `netadm` avec la sous-commande `list`. Le résultat de cette commande fournit des informations sur l'état de base de chaque objet réseau configuré sur votre système. Toutefois, l'interface graphique fournit des d'informations plus détaillées sur l'état du réseau, notamment le réseau sans fil auquel vous êtes connecté et l'adresse IP de votre connexion réseau.

Certaines commandes exécutables par le biais de la CLI ne peuvent pas l'être par le biais de l'interface graphique. Par exemple, vous ne pouvez pas exporter une configuration de profil à l'aide du composant d'interface graphique. Pour exporter une configuration de profil, utilisez la commande `netcfg export`. Pour plus d'informations, reportez-vous à la section [“Exportation et restauration d'une configuration de profil” à la page 108](#).

- **Différences dans l'utilisation des termes et noms de composants**

Dans l'interface graphique, un profil de configuration réseau (NCP, Network Configuration Profile) est l'équivalent d'un *profil réseau*. Les unités de configuration réseau (NCU, Network Configuration Units) dans l'interface de ligne de commande sont appelées des *connexions réseau* dans l'interface graphique.

Activer et désactiver des NCP par le biais de l'interface de ligne de commande revient à *commuter des profils réseau ou des connexions* dans l'interface graphique.

## Composants fonctionnels de l'interface graphique NWAM

L'interface graphique NWAM comprend plusieurs composants fonctionnels permettant d'effectuer pratiquement les mêmes tâches qu'à l'aide de la CLI. Le [Tableau 6–1](#) décrit chacun de ces composants. Notez que certaines boîtes de dialogue peuvent être consultées ou ouvertes de plusieurs façons. En outre, certaines affichent des informations différentes, en fonction de la méthode utilisée pour y accéder. Des informations spécifiques sur ces différences sont indiquées dans les sections connexes tout au long de ce chapitre et expliquées en détail dans l'aide en ligne.

TABLEAU 6–1 Composants principaux de l'interface graphique NWAM

Composant	Fonction	Méthode d'accès
Icône de notification Etat du réseau	Méthode permettant d'afficher l'état de votre réseau et d'interagir avec NWAM à partir du bureau. L'icône contient également un menu contextuel, qui permet de créer et gérer la configuration réseau à l'aide de l'interface graphique.	<ul style="list-style-type: none"><li>■ En consultant l'icône, laquelle est affichée en permanence dans la zone de notification du panneau du bureau.</li><li>■ En déplaçant le curseur de la souris sur l'icône pour afficher une info-bulle contenant des informations sur l'état actuel du réseau.</li><li>■ En cliquant sur l'icône, ce qui ouvre la boîte de dialogue Préférences réseau.</li><li>■ En cliquant avec le bouton droit de la souris sur l'icône, ce qui ouvre le menu contextuel.</li></ul>



TABLEAU 6–1 Composants principaux de l'interface graphique NWAM (Suite)

Composant	Fonction	Méthode d'accès
Boîte de dialogue Préférences réseau	<p>Méthode d'activation et de gestion des deux principaux types de profil réseau : le profil Automatique défini par le système et plusieurs profils réseau définis par l'utilisateur. Le profil Automatique et les profils réseau définis par l'utilisateur gèrent la configuration réseau pour chaque interface réseau.</p> <p>Cette boîte de dialogue permet également de configurer les adresses IPv4 et IPv6 de chaque interface réseau, et de gérer les réseaux sans fil favoris.</p>	<ul style="list-style-type: none"> <li>■ En cliquant sur l'icône de notification Etat du réseau sur le bureau.</li> <li>■ En choisissant Système → Administration → Réseau à partir de la barre de menu principale figurant sur le panneau du bureau.</li> <li>■ En sélectionnant l'option Préférences réseau dans le menu de l'icône de notification Etat du réseau.</li> </ul>
Boîte de dialogue Emplacements réseau	Méthode de création, d'activation et de gestion des propriétés des profils d'emplacement définis par le système et par l'utilisateur. Les emplacements spécifient certains éléments d'une configuration réseau (par exemple, un service de nommage et les paramètres du pare-feu), appliqués conjointement, le cas échéant.	<ul style="list-style-type: none"> <li>■ En choisissant Emplacements réseau dans le menu contextuel de l'icône de notification Etat du réseau.</li> <li>■ Ou en cliquant sur le bouton Emplacements dans la vue Etat de connexion de la boîte de dialogue Préférences réseau.</li> </ul>
Boîte de dialogue Joindre un réseau sans fil	<p>Méthode permettant de joindre les réseaux sans fil et de gérer une liste des réseaux favoris.</p> <p><b>Remarque</b> – Cette boîte de dialogue s'ouvre automatiquement si vous tentez d'ajouter un réseau sans fil et que des informations supplémentaires sur ce réseau sont nécessaires.</p>	<ul style="list-style-type: none"> <li>■ En sélectionnant l'option Joindre un réseau sans fil non répertorié dans le menu contextuel de l'icône de notification.</li> <li>■ En cliquant sur le bouton équivalent dans la boîte de dialogue Sélecteur sans fil.</li> <li>■ En cliquant sur le message de notification qui indique qu'aucun réseau sans fil n'a été trouvé et que vous devez cliquer pour joindre un réseau sans fil non répertorié.</li> </ul>

TABLEAU 6-1 Composants principaux de l'interface graphique NWAM (Suite)

Composant	Fonction	Méthode d'accès
Boîte de dialogue Sélecteur sans fil	Méthode permettant de choisir et de se connecter à un réseau sans fil.	En cliquant sur le message de notification qui indique que <i>l'interface</i> est déconnectée de <i>ESSID</i> et que vous devez cliquer pour afficher d'autres réseaux disponibles.  <b>Remarque</b> – Cette boîte de dialogue s'ouvre automatiquement chaque fois que vous devez choisir parmi plusieurs réseaux sans fil disponibles à connecter.
Boîte de dialogue Modificateurs réseau	Méthode permettant d'ajouter des applications ENM, capables de créer ou de modifier la configuration réseau.	<ul style="list-style-type: none"><li>■ En cliquant sur le bouton Modificateurs de la vue Etat de connexion de la boîte de dialogue Préférences réseau.</li><li>■ En cliquant avec le bouton droit de la souris sur l'icône de notification Etat du réseau, puis en sélectionnant l'élément du menu des préférences de modificateur réseau.</li></ul>

## Interaction avec NWAM à partir du bureau

L'icône de notification Etat du réseau affichée en permanence dans la zone de notification du panneau du bureau constitue le principal moyen d'afficher l'état de votre réseau et d'interagir avec le processus de configuration réseau automatique. L'icône de notification Etat du réseau est également l'emplacement d'affichage des messages d'information sur votre réseau. Le menu contextuel (clic droit) de l'icône permet d'accéder rapidement aux principales fonctionnalités du réseau. L'apparence de l'icône indique l'état général du réseau.

### Vérification de l'état de votre connexion réseau

Le moyen le plus rapide d'obtenir les informations essentielles relatives à votre réseau consiste à consulter l'icône de notification Etat du réseau affichée dans la zone de notification du panneau du bureau. L'icône de notification Etat du réseau constitue le principal moyen d'afficher l'état de votre connexion réseau activée et d'interagir avec NWAM. L'apparence de l'icône change en fonction de l'état de la connexion réseau actuellement activée. Vous pouvez également afficher des informations sur votre connexion réseau active en plaçant le curseur de la souris sur l'icône



de notification Etat du réseau. Pour accéder au menu contextuel de l'icône de notification, cliquez avec le bouton droit de la souris sur l'icône. Vous pouvez alors modifier l'interface réseau activée et visualiser des informations plus détaillées sur le réseau sans fil, le cas échéant, auquel vous êtes connecté.



---

**Remarque** – L'icône de notification Etat du réseau ne s'affiche dans le bureau que si vous utilisez NWAM pour configurer automatiquement votre réseau.

---

Le tableau ci-après illustre l'apparence de l'icône Etat du réseau, qui évolue de manière à refléter l'état des connexions réseau activées sur votre système.

Icône	Etat	Description
	Toutes en ligne (câblées)	Indique que l'ensemble des connexions activées manuellement figurant dans le profil réseau actif sont en ligne et que le nombre requis de connexions dans le groupe de profils activé (si un tel groupe existe) est en ligne. Le « nombre requis » est le suivant : <ul style="list-style-type: none"> <li>■ Une connexion si le type de priorité du groupe est Exclusive.</li> <li>■ Une ou plusieurs connexions si le type de priorité du groupe est Partagée.</li> <li>■ Toutes les connexions du groupe si le type de priorité du groupe est Toutes.</li> </ul>
	Toutes en ligne (sans fil)	Indique que l'ensemble des connexions activées manuellement figurant dans le profil réseau actif sont en ligne et que le nombre requis de connexions dans le groupe de profils activé (si un tel groupe existe) est en ligne. Le nombre requis est le même que celui décrit pour l'état <i>Toutes en ligne (câblées)</i> .  Notez qu'au moins une connexion en ligne est sans fil.

Icône	Etat	Description
	Partiellement en ligne (câblée)	Indique qu'une ou plusieurs connexions activées manuellement ou de groupe de priorité sont hors ligne, de sorte que l'état n'est plus <i>Toutes en ligne</i> . Dans cet exemple, au moins une connexion câblée est en ligne.  L'icône de notification Etat du réseau indique également l'état <i>Partiellement en ligne</i> si une connexion sans fil requiert la saisie d'informations d'un utilisateur, par exemple la sélection d'un réseau sans fil disponible ou le mot de passe d'accès au réseau sans fil.
	Hors ligne (câblées)	Indique que le service NWAM est désactivé ou en mode de maintenance.

## ▼ Affichage des détails sur une connexion réseau activée

- 1 Ouvrez la boîte de dialogue Préférences réseau et sélectionnez Etat de connexion dans la liste déroulante, si nécessaire.

Vous pouvez ouvrir la boîte de dialogue Préférences réseau de l'une des manières suivantes :

- Cliquez sur l'icône de notification Etat du réseau dans le panneau du bureau.
- Choisissez Système → Administration → Réseau à partir de la barre de menu principale figurant sur le panneau du bureau.
- Cliquez avec le bouton droit de la souris sur l'icône de notification Etat du réseau pour ouvrir son menu, puis sélectionnez Préférences réseau.  
Pour les connexions réseau sans fil, l'adresse IP, l'intensité du signal, l'état de la vitesse de connexion et le type de sécurité s'affichent.

- 2 Pour afficher ou modifier plus de propriétés d'une connexion réseau spécifique, double-cliquez sur la connexion dans la liste ou sélectionnez-la dans le menu déroulant Afficher situé en haut de la boîte de dialogue.

## Contrôle des connexions réseau à partir du bureau

Par défaut, NWAM tente de maintenir une connexion réseau à tout moment. Si une connexion réseau câblée échoue, une connexion à l'un de vos réseaux sans fil favoris est tentée. Si cette tentative échoue, d'autres connexions à des réseaux sans fil disponibles sont tentées, avec votre permission.

Vous pouvez également, le cas échéant, basculer manuellement d'un réseau câblé à un réseau sans fil, et vice-versa.

---

**Remarque** – Pour tous les types de connexion, le comportement de connexion est défini pour la session en cours *uniquement*. Lorsque vous réinitialisez le système ou que vous vous déconnectez, une tentative est effectuée pour établir des connexions réseau, selon les priorités définies par le profil réseau activé.

---

Vous pouvez contrôler les connexions réseau à partir du bureau via NWAM de l'une des façons suivantes :

- **Modifier la priorité de connexion par défaut**

Par défaut, toutes les connexions réseau câblées ont la priorité sur toutes les connexions réseau sans fil. En d'autres termes, une connexion réseau sans fil est tentée si une connexion câblée ne peut pas être établie et à cette seule condition. Si plusieurs réseaux sans fil sont disponibles à l'emplacement actuel, vous êtes invité à sélectionner le réseau auquel vous connecter. Ce comportement est défini par le profil réseau Automatique, activé par défaut. Pour appliquer un comportement différent, vous devez créer et activer un autre profil réseau.

- **Passer d'un réseau câblé à un réseau sans fil**

Si le profil réseau Automatique est activé, débranchez les câbles réseau de toutes les interfaces câblées activées.

Par défaut, si certains de vos réseaux sans fil favoris sont disponibles, une tentative de connexion est effectuée selon leur ordre d'apparition dans la liste des favoris. Dans le cas contraire, la boîte de dialogue Sélecteur sans fil s'affiche. Dans cette boîte de dialogue, vous pouvez sélectionner le réseau auquel vous connecter.

---

**Remarque** – Vous pouvez modifier la façon dont la connexion aux réseaux sans fil est établie dans l'onglet Sans fil de la vue Propriétés de connexion.

---

Si un profil réseau autre que le profil réseau Automatique est activé, la méthode utilisée pour passer à un réseau sans fil dépend de la définition de ce profil réseau.

Utilisez l'une des méthodes suivantes :

- Utilisez le sous-menu Connexions de l'icône de notification Etat du réseau pour désactiver la connexion câblée, puis activer une connexion sans fil. Notez que cette méthode n'est possible que si les deux connexions sont du type Activation manuelle.
- Modifiez le profil réseau activé pour activer la connexion câblée et désactiver d'autres connexions selon vos besoins.

Une fois la connexion sans fil établie, un message de notification s'affiche.

- **Passer d'un réseau sans fil à un réseau câblé**

Si le profil réseau Automatique est activé, branchez un câble réseau dans une interface câblée disponible.

Si un profil réseau autre que le profil réseau Automatique est activé, la méthode utilisée pour passer à un réseau câblé dépend de la définition de ce profil réseau.

Utilisez l'une des méthodes suivantes :

- Utilisez le sous-menu Connexions de l'icône de notification Etat du réseau pour désactiver la connexion sans fil, puis activer une connexion câblée. Notez que cette méthode n'est possible que si les deux connexions sont du type Activation manuelle.
- Modifiez le profil réseau activé pour activer la connexion câblée et désactiver la connexion sans fil.

Une fois la connexion câblée établie, un message de notification s'affiche.

Pour consulter les autres tâches que vous pouvez effectuer à l'aide de l'interface graphique NWAM, reportez-vous à l'aide en ligne.

## Connexion et gestion des réseaux sans fil favoris

Par défaut, lorsque des connexions réseau sans fil sont activées, NWAM tente de se connecter à l'un des réseaux disponibles de la liste des favoris sans vous poser de question, selon l'ordre dans lequel les connexions sont répertoriées. Si aucun des réseaux favoris n'est disponible, la boîte de dialogue Sélecteur sans fil s'affiche. Dans cette boîte de dialogue, vous pouvez choisir le réseau sans fil auquel vous connecter.

Vous pouvez également modifier la manière dont les connexions aux réseaux sans fil sont tentées dans l'onglet Sans fil de la vue Propriétés de connexion de la boîte de dialogue Préférences réseau. Si nécessaire, vous pouvez vous connecter manuellement à un autre réseau sans fil en accédant au menu contextuel de l'icône de notification Etat du réseau.

---

**Astuce** – Vous pouvez accéder à la vue Propriétés de connexion d'un réseau sélectionné par le biais de la boîte de dialogue Préférences réseau. Cette boîte de dialogue contient une liste déroulante intitulée Afficher. Cette liste vous permet de basculer entre les vues d'un réseau donné. Chaque vue contient différentes tâches que vous pouvez effectuer et des informations sur le réseau sélectionné, spécifiques à cette vue.

Les vues suivantes existent pour chaque connexion réseau dans chaque profil réseau présent sur le système :

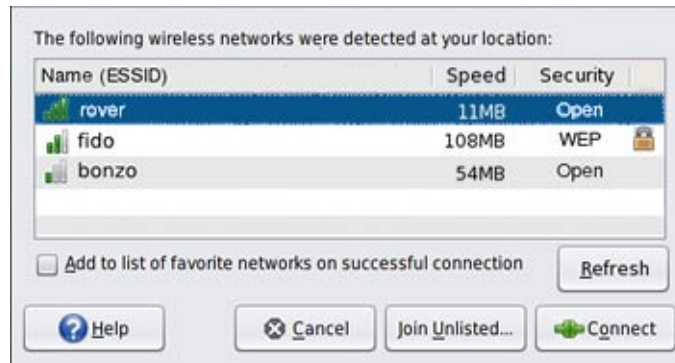
- Etat de la connexion
- Profil réseau
- Propriétés de la connexion

Pour obtenir plus d'informations sur l'utilisation des profils réseau, y compris la description de la boîte de dialogue Préférences réseau, reportez-vous à la section "[Gestion des profils réseau](#)" à la page 136.

## ▼ Connexion à un réseau sans fil

Les réseaux sans fil sont connectés à l'aide de l'option Joindre un réseau sans fil, disponible en cliquant avec le bouton droit de la souris sur l'icône de notification Etat du réseau. La boîte de dialogue Sélecteur sans fil vous permet de sélectionner un réseau sans fil auquel vous connecter, à partir de la liste des réseaux disponibles qui s'affiche.

- 1 Pour vous connecter manuellement à un autre réseau sans fil, vous pouvez effectuer l'une des opérations suivantes :
  - Sélectionner un réseau sans fil disponible dans le menu contextuel de l'icône de notification Etat du réseau.
  - Sélectionner l'option Joindre un réseau sans fil non répertorié dans le menu de l'icône de notification Etat du réseau.  
Un réseau sans fil non répertorié est un réseau configuré de manière à ne pas diffuser son nom de réseau tout en restant disponible pour s'y connecter.
  - Sélectionner un réseau sans fil disponible dans la boîte de dialogue Sélecteur sans fil. Cette boîte de dialogue s'affiche automatiquement, lorsque plusieurs réseaux sans fil auxquels se connecter sont disponibles.



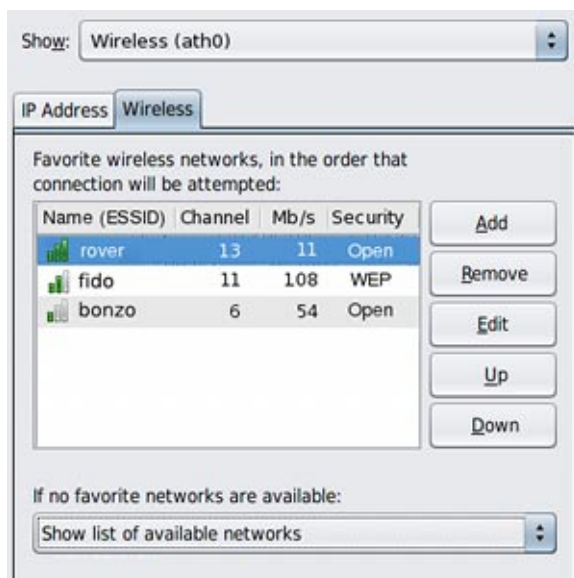
- 2 Si la boîte de dialogue Joindre un réseau sans fil s'ouvre, indiquez toutes les informations nécessaires pour le réseau sans fil de votre choix.

Pour de plus amples informations sur les données que vous devez éventuellement fournir, reportez-vous à l'aide en ligne de l'interface graphique NWAM.

## Gestion des réseaux favoris

Par défaut, lorsque vous vous connectez à un réseau sans fil pour la première fois, une case à cocher intitulée Ajouter à la liste des réseaux favoris en cas de connexion réussie s'affiche dans la boîte de dialogue Joindre un réseau sans fil.

- Pour ajouter le réseau sans fil à votre liste de favoris, si la connexion est établie, sélectionnez cette case. Si vous ne souhaitez pas que le réseau soit ajouté à votre liste de favoris, désélectionnez la case. La case est sélectionnée par défaut.
- Pour ajouter un réseau sans fil qui n'est pas disponible ou qui ne diffuse pas son nom dans votre liste de favoris, accédez à l'onglet Sans fil de la vue Propriétés de connexion, puis cliquez sur le bouton Ajouter. Pour ajouter le réseau, vous devez connaître son nom, le type de sécurité et la clé de sécurité.



## Gestion des profils réseau

Dans l'interface graphique NWAM, les profils réseau sont l'équivalent des NCP, décrits dans la section ["Description d'un NCP" à la page 48](#).

Un profil réseau spécifie les interfaces réseau qui peuvent être activées ou désactivées à un moment donné. Il peut être utile d'utiliser des profils réseau dans les cas où plusieurs interfaces réseau sont disponibles. Par exemple, la plupart des portables modernes possèdent à la fois une interface câblée et une interface sans fil. En fonction de votre emplacement physique et de votre



environnement de travail, il peut être judicieux de n'utiliser qu'une interface et de désactiver l'autre pour des raisons de sécurité, entre autres.

Deux types de profil réseau sont disponibles dans l'interface graphique NWAM, le profil réseau Automatique par défaut et le profil réseau défini par l'utilisateur. Vous pouvez activer et désactiver les deux types de profils. Vous pouvez modifier les profils définis par l'utilisateur, mais pas le profil Automatique. Vous ne pouvez pas créer ni détruire le profil Automatique à l'aide de l'interface de ligne de commande ou de l'interface graphique NWAM. Cependant, vous pouvez créer, modifier et détruire les profils réseau définis par l'utilisateur à l'aide de l'interface graphique ou de l'interface de ligne de commande.

Par défaut, le profil réseau Automatique tente d'abord d'activer une connexion câblée. En cas d'échec, il tente d'activer une connexion sans fil.

## A propos de la boîte de dialogue Préférences réseau

La boîte de dialogue Préférences réseau permet de configurer les connexions réseau et d'afficher l'état actuel de chaque connexion réseau. Cette boîte de dialogue permet d'accéder aux différentes vues et de passer de l'une à l'autre à l'aide de la liste déroulante située dans la partie supérieure.

Vous pouvez ouvrir la boîte de dialogue de plusieurs manières :

- En cliquant sur l'icône de notification Etat du réseau sur le bureau.
- En choisissant Système → Administration → Réseau à partir de la barre de menu principale figurant sur le panneau du bureau.
- En sélectionnant l'option Préférences réseau dans le menu de l'icône de notification Etat du réseau.

En haut de la boîte de dialogue Préférences réseau figure une liste déroulante intitulée Afficher. Cette liste vous permet de changer de vue pour chaque connexion réseau figurant dans un profil réseau : vue Etat de connexion, vue Profil réseau et vue Propriétés de connexion.

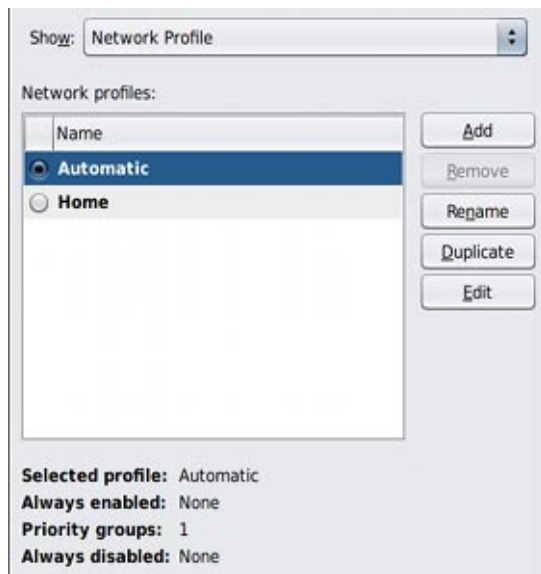
### Vue Etat de connexion

- La vue Etat de connexion affiche des informations sur chaque connexion réseau activée dans le profil réseau activé dont le type d'activation est manuel et chaque connexion (activées ou désactivées) dans le groupe de priorité actif. La section Connexions activées répertorie l'ensemble des connexions activées, selon l'ordre dans lequel elles sont répertoriées dans la vue Profil réseau. Reportez-vous à la section [“Affichage des détails sur une connexion réseau activée”](#) à la page 132.

## Vue Profil réseau

- Les informations sur un profil réseau peuvent être consultées dans la vue Profil réseau de la boîte de dialogue Préférences réseau.

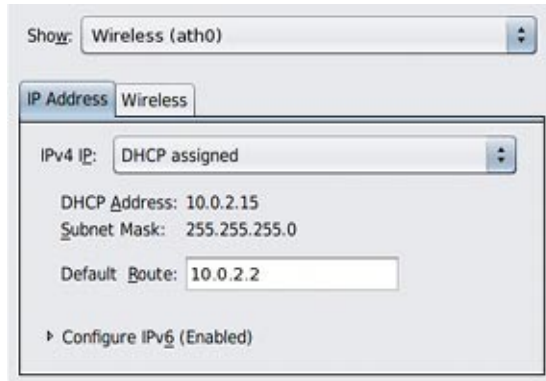
Pour afficher cette vue, sélectionnez Profil réseau dans la liste déroulante située en haut de la boîte de dialogue Préférences réseau.



## Vue Propriétés de connexion

- La vue Propriétés de connexion permet de visualiser et de modifier les propriétés d'une connexion réseau spécifiée. Pour passer à cette vue, sélectionnez le nom de connexion dans la liste déroulante Afficher ou double-cliquez sur le nom de connexion dans la vue Etat de connexion ou Profil réseau. Une fenêtre comportant des onglets s'affiche, dans laquelle vous pouvez visualiser ou modifier les propriétés de connexion.

La vue Propriétés de connexion contient deux onglets : Adresse IP et Sans fil. L'onglet Sans fil ne s'affiche que si le type de connexion est sans fil. Dans l'onglet Adresse IP, vous pouvez configurer les adresses IPv4 et IPv6. Dans l'onglet Sans fil, vous pouvez configurer la liste de vos réseaux favoris et choisir la façon dont l'interface sans fil se connecte aux réseaux disponibles.



## Visualisation des informations relatives aux profils réseau

Les informations sur un profil réseau peuvent être consultées dans la vue Profil réseau de la boîte de dialogue Préférences réseau.

Pour afficher cette vue, sélectionnez Profil réseau dans la liste déroulante située en haut de la boîte de dialogue Préférences réseau.

La liste Profils réseau affiche le nom de chaque profil réseau disponible. Le profil activé est affiché avec un indicateur de bouton radio. Par défaut, il existe un profil, le profil Automatique, que vous pouvez activer, mais pas modifier ni supprimer. Cependant, vous pouvez créer plusieurs autres profils réseau. Les profils réseau qui sont créés manuellement peuvent être activés, modifiés ou supprimés, selon les besoins.

Vous trouverez sous la liste des profils réseau un résumé du profil sélectionné. Pour visualiser le profil sélectionné dans son intégralité ou modifier le profil, cliquez sur le bouton Modifier.

---

**Remarque** – Le profil *sélectionné* peut être différent du profil *activé*.

---

## Passage d'un profil réseau à un autre

1. Ouvrez la vue Profil réseau de la boîte de dialogue Préférences réseau.
2. Sélectionnez le bouton radio en regard du profil réseau à activer.
3. Pour passer d'un profil réseau à un autre, cliquez sur OK ou pour fermer la boîte de dialogue sans changer de profil, cliquez sur Annuler.

## Ajout ou suppression d'un profil réseau

Pour créer ou modifier un profil réseau, sélectionnez Profil réseau dans la liste déroulante située en haut de la boîte de dialogue Préférences réseau.

- Pour créer un profil réseau, cliquez sur le bouton Ajouter, puis saisissez le nom du nouveau profil.
- Pour dupliquer un profil réseau existant, sélectionnez-le dans la liste, cliquez sur le bouton Dupliquer, puis saisissez le nom du nouveau profil.
- Pour supprimer un profil réseau, sélectionnez-le dans la liste, puis cliquez sur le bouton Supprimer.

---

**Remarque** – Vous ne pouvez pas supprimer le profil réseau Automatique.

---

Pour plus d'informations sur la modification d'un profil que vous avez ajouté ou dupliqué, reportez-vous à la section “[Modification de profils réseau](#)” à la page 140.

## Modification de profils réseau

Lorsque vous ajoutez manuellement un profil réseau ou dupliquez un profil réseau existant, vous devez modifier le nouveau profil afin d'indiquer les connexions réseau qui sont activées ou désactivées par le nouveau profil.

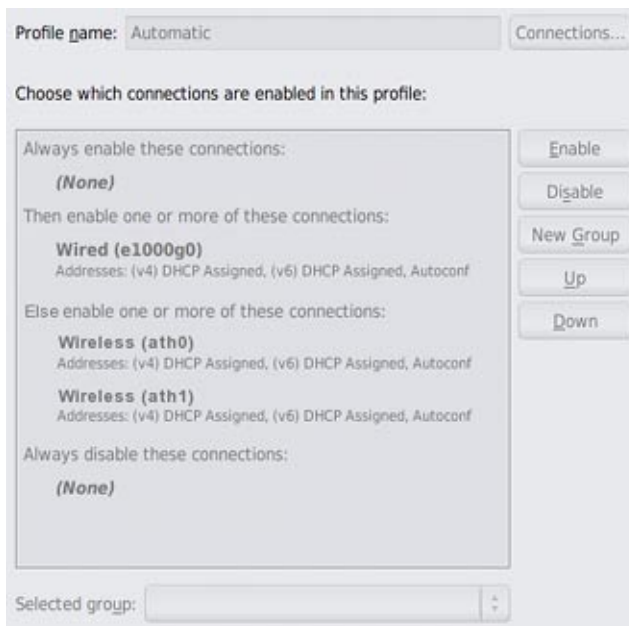
---

**Remarque** – Vous pouvez modifier et supprimer un profil réseau créé manuellement. Toutefois, vous ne pouvez pas modifier ni supprimer le profil réseau Automatique.

---

## ▼ Ouverture de la boîte de dialogue Profil réseau

- Pour modifier un profil réseau, sélectionnez-le dans la vue Profil réseau de la boîte de dialogue Préférences réseau, puis cliquez sur Modifier.



La liste des profils réseau se compose au minimum de deux descriptions de groupe de niveau supérieur. Par exemple, le profil Automatique indiqué dans la figure précédente contient quatre descriptions de groupe détaillées dans les sections suivantes.

---

**Remarque** – Le profil réseau Automatique ne peut pas être modifié ni supprimé. Lorsque le profil réseau Automatique est sélectionné dans la boîte de dialogue Modifier un profil réseau, l'ensemble des boutons et listes déroulantes de modification du profil sont désactivés.

---

Pour plus d'informations, reportez-vous à l'aide en ligne.

## Utilisation des groupes de priorité

Une connexion réseau figurant dans le groupe "Toujours activé(e)" est toujours activée lorsque le profil réseau sélectionné est actif.

Pour déplacer une connexion réseau dans le groupe "Toujours activé(e)", sélectionnez d'abord la connexion, puis effectuez l'une des opérations suivantes :

- Cliquez sur le bouton Activer.
- Cliquez sur le bouton Haut jusqu'à ce que la connexion soit déplacée dans le groupe "Toujours activé(e)".

Une connexion réseau figurant dans le groupe "Toujours désactivé(e)" est toujours désactivée lorsque le profil réseau sélectionné est actif.

Pour déplacer une connexion réseau dans le groupe "Toujours désactivé(e)", sélectionnez d'abord la connexion, puis effectuez l'une des opérations suivantes :

- Cliquez sur Disable (Désactiver).
- Cliquez sur le bouton Bas jusqu'à ce que la connexion soit déplacée dans le groupe "Toujours désactivé(e)".

Vous pouvez créer un profil réseau qui traite une ou plusieurs interfaces réseau comme un groupe. Si une ou plusieurs des interfaces figurant dans le groupe à la priorité la plus élevée ne peuvent pas être activées en raison du type de priorité du groupe, l'utilisation du groupe disposant du niveau de priorité suivant est considérée.

Le tableau suivant décrit les trois différents groupes de priorité disponibles.

Type de priorité	Description
Exclusive	Une connexion dans le groupe est activée alors que toutes les autres sont désactivées. Tant qu'une connexion du groupe est activée (pas nécessairement la même à chaque fois), aucune tentative d'activation des connexions figurant dans l'un des groupes à priorité moins élevée n'est effectuée.
Shared	Toutes les connexions dans le groupe qui peuvent être activées le sont. Tant qu'une connexion du groupe demeure activée, aucune tentative d'activation des connexions figurant dans l'un des groupes à priorité moins élevée n'est effectuée.
All	Toutes les connexions du groupe sont activées. Si l'une des connexions est perdue, toutes les connexions dans le groupe sont désactivées. Tant que toutes les connexions restent activées, aucune tentative n'est effectuée pour activer les connexions dans les groupes à priorité moins élevée.

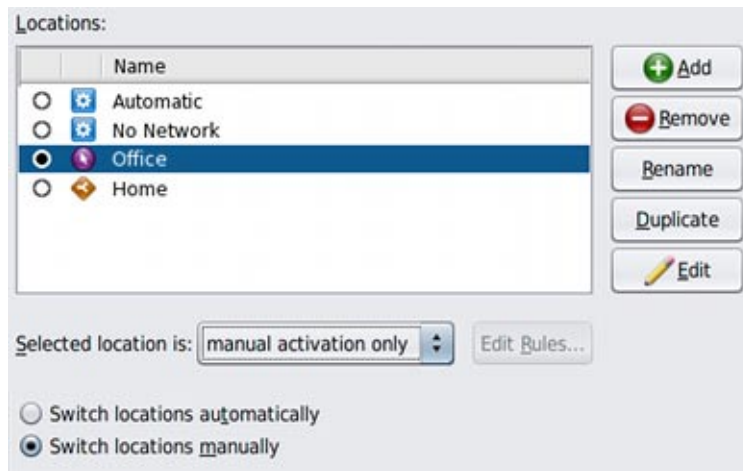
Par exemple, le profil réseau Automatique par défaut contient deux groupes de priorité Exclusive. Le groupe à priorité plus élevée contient toutes les connexions réseau *câblées*. Le groupe à priorité plus basse contient toutes les connexions réseau *sans fil*.

Pour obtenir des instructions détaillées sur l'exécution de ces tâches, reportez-vous à l'aide en ligne.

## Création et gestion des emplacements

Un emplacement comprend certains éléments d'une configuration réseau (par exemple, un service de nommage et les paramètres du pare-feu), appliqués conjointement, le cas échéant. Vous pouvez créer plusieurs emplacements pour différents usages. Par exemple, un emplacement peut être utilisé lorsque vous êtes connecté au bureau à l'intranet de l'entreprise. Un autre emplacement peut être utilisé lorsque vous êtes connecté chez vous à Internet à l'aide d'un point d'accès sans fil. Les emplacements peuvent être activés manuellement ou automatiquement, selon les conditions d'environnement, telles que l'adresse IP qui est obtenue par une connexion réseau.

La boîte de dialogue Emplacements réseau vous permet de changer d'emplacement, de modifier les propriétés d'un emplacement, ainsi que de créer et de supprimer des emplacements. Notez que seuls les emplacements définis par l'utilisateur peuvent être créés et supprimés. La boîte de dialogue Emplacement peut être ouverte à partir de la vue Etat de connexion de la boîte de dialogue Préférences réseau.



La liste Emplacements est similaire à celle du menu de l'icône de notification Etat du réseau. Chaque emplacement disponible, accompagné d'une icône représentant le type d'activation, est répertorié.

Les types d'emplacement sont les suivants :

- **Système** : les emplacements de ce type sont définis par le système (Automatique et Aucun réseau), ce qui signifie que le système détermine le moment où l'emplacement est activé, en fonction des conditions du réseau.
- **Manuel** : les emplacements de ce type peuvent être activés ou désactivés manuellement à l'aide de la boîte de dialogue Emplacements réseau ou de l'icône de notification Etat du réseau.
- **Conditionnel** : les emplacements de ce type sont activés ou désactivés automatiquement, selon les règles que vous spécifiez lors de leur création.

Le type d'activation de l'emplacement sélectionné est également affiché dans la liste déroulante Emplacement sélectionné. L'emplacement activé est représenté par un bouton radio sélectionné qui s'affiche dans la première colonne de la liste.

## ▼ **Modification du mode d'activation d'un emplacement**

La tâche suivante décrit comment modifier le mode activation pour un emplacement à l'aide de l'interface graphique NWAM. Si vous utilisez la commande `netcfg`, vous devez modifier le mode activation en modifiant les propriétés de l'emplacement spécifié. Pour plus d'informations, reportez-vous à la section [“Définition et modification des valeurs de propriétés pour un profil” à la page 100](#).

- 1 **Dans le sous-menu Emplacement de l'icône de notification Etat du réseau, sélectionnez Emplacements réseau. Ou, dans la vue Etat de connexion de la boîte de dialogue Préférences réseau, cliquez sur le bouton Emplacements.**
- 2 **Pour changer le mode d'activation d'un emplacement, sélectionnez l'emplacement dans la liste, puis sélectionnez le nouveau mode d'activation dans la liste déroulante Emplacement sélectionné.**

---

**Remarque** – Notez que lorsqu'un emplacement du système est sélectionné, la liste déroulante affiche Activation par le système et la liste déroulante ainsi que le bouton Modifier les règles sont désactivés.

---

Quand un emplacement Manuel ou Conditionnel est sélectionné, les options de la liste déroulante sont les suivantes :

- **Activation manuelle uniquement** : cet emplacement est activé uniquement lorsqu'il est sélectionné manuellement. Lorsque cette option est sélectionnée, le bouton Modifier les règles est *désactivé*.
- **Activation en fonction de règles** : cet emplacement est automatiquement sélectionné dans certaines conditions du réseau. Lorsque cette option est sélectionnée, le bouton Modifier les règles est *activé*.



### 3 (Facultatif) Pour définir des règles relatives au mode et au moment d'activation d'un emplacement, cliquez sur le bouton **Modifier les règles**.

Pour plus d'instructions, reportez-vous à la rubrique relative à l'utilisation de la boîte de dialogue Règles de l'aide en ligne.

## ▼ **Passage d'un emplacement à l'autre**

La tâche suivante décrit comment passer d'un emplacement à un autre à l'aide de l'interface graphique NWAM. Pour passer d'un emplacement à l'autre à l'aide de la CLI, utilisez la commande `netadm` pour activer un nouvel emplacement. Dans la mesure où un seul emplacement doit être activé sur le système à tout moment, l'activation d'un nouvel emplacement désactive implicitement le l'emplacement activé. La même règle s'applique lors de l'activation d'un profil réseau. Pour plus d'informations sur l'activation et la désactivation des emplacements, reportez-vous à la section [“Activation et désactivation des profils” à la page 118](#).

### ● **Dans le sous-menu Emplacement de l'icône de notification Etat du réseau, sélectionnez l'emplacement à activer.**

Si l'option **Modifier les emplacements automatiquement** est sélectionnée dans le sous-menu Emplacements, il est impossible de sélectionner un emplacement manuellement pour l'activer. L'emplacement **Système** ou **Conditionnel** le plus approprié est activé automatiquement à tout moment donné, en fonction de l'évolution de l'environnement du réseau.

Si l'option **Changer les emplacements manuellement** est sélectionnée dans le sous-menu Emplacements, vous pouvez activer l'emplacement disponible de votre choix, quel que soit son type d'activation. Cet emplacement reste actif indéfiniment.

### ■ **Sinon, vous pouvez passer d'un emplacement à l'autre dans la boîte de dialogue Emplacements réseau. Pour ce faire, suivez les étapes ci-après :**

a. Dans le sous-menu **Emplacement de l'icône de notification Etat du réseau**, sélectionnez **Emplacements réseau**. Ou, dans la vue **Etat de connexion** de la boîte de dialogue **Préférences réseau**, cliquez sur le bouton **Emplacements**.

b. Sélectionnez le bouton radio de l'emplacement auquel vous souhaitez passer, puis cliquez sur **OK**.

- Si le bouton radio **Modifier les emplacements automatiquement** est sélectionné dans la boîte de dialogue **Emplacements réseau**, il est impossible de sélectionner un emplacement manuellement pour l'activer. L'emplacement **Système** ou **Conditionnel** le plus approprié est activé automatiquement à tout moment donné, en fonction de l'évolution de l'environnement du réseau.

- Si le bouton radio **Changer les emplacements manuellement** est sélectionné dans la boîte de dialogue **Emplacements réseau**, vous pouvez activer l'emplacement disponible de votre choix, quel que soit son type d'activation. Notez que cet emplacement reste activé indéfiniment.

## Modification des emplacements

Modifier un emplacement à l'aide de l'interface graphique NWAM revient à modifier les propriétés d'un emplacement à l'aide de la CLI NWAM.

Pour modifier un emplacement, choisissez **Emplacements réseau** dans le sous-menu **Emplacement** de l'icône de notification **Etat du réseau**. Ou, dans la vue **Etat de connexion** de la boîte de dialogue **Préférences réseau**, cliquez sur le bouton **Emplacements**.

Pour modifier les propriétés d'un emplacement spécifié, sélectionnez l'emplacement dans la liste, puis cliquez sur **Modifier**.

Vous pouvez également double-cliquer sur l'emplacement dans la liste.

La boîte de dialogue **Modifier l'emplacement** contenant les deux onglets suivants s'ouvre :

Services de noms	Vous permet de configurer les services de nommage à l'emplacement spécifié.
Sécurité	Vous permet de sélectionner les fichiers de configuration à utiliser par les fonctions IPfilter et IPsec lorsque l'emplacement spécifié est activé.

Pour afficher les informations à modifier, sélectionnez l'onglet approprié.

## A propos des modificateurs réseau externes

Les modificateurs réseau externes (ENM) sont des profils créés pour les applications externes à NWAM. Cependant, ces applications peuvent créer et modifier la configuration réseau. Par exemple, les applications VPN activent les connexions réseau dans le cadre de communications avec un réseau privé virtuel. Les ENM sont configurés et contrôlés dans l'interface graphique NWAM à l'aide de la boîte de dialogue *Modificateurs réseau*.

---

**Remarque** – Avant de pouvoir gérer une application ou un service de modificateur réseau à l'aide de l'interface graphique NWAM, vous devez l'installer manuellement, puis effectuer la configuration initiale (installation d'un certificat ou d'un secret partagé, par exemple).

---

Un ENM peut être démarré et arrêté manuellement, comme nécessaire. Un ENM peut également être démarré automatiquement, en fonction de règles définies par l'utilisateur. Pour être géré à l'aide de cette boîte de dialogue, une application de modificateur réseau externe doit être mise en oeuvre comme un outil de ligne de commande, ou comme un service SMF.

Pour en savoir plus sur la création et la gestion des ENM à l'aide de la CLI NWAM, reportez-vous à la section [“Création d'un profil ENM”](#) à la page 93.

## A propos de la boîte de dialogue Modificateurs réseau

Cette boîte de dialogue permet d'ajouter ou de supprimer, de démarrer et d'arrêter, et de modifier des modificateurs réseau externes (ENM), applications capables de créer et de modifier la configuration réseau.

Available network modifiers:

Application Name	Status
OpenVPN	Stopped

Buttons: Add, Remove, Rename, Start, Stop

☐ Start/stop 'OpenVPN' according to rules Edit Rules...

☒ Manage modifier using command line applications:

Start Command:  Browse...

Stop Command:  Browse...

☐ Manage modifier using an SMF service:

Service FMRI:

Examples:  
 svc:/localhost/system/system-log:default  
 svc:/system/system-log:default  
 system/system-log:default

Ouvrez la boîte de dialogue par l'une des méthodes suivantes :

- Cliquez sur le bouton Modificateurs de la vue Etat de connexion de la boîte de dialogue Préférences réseau.
- Cliquez avec le bouton droit de la souris sur l'icône de notification Etat du réseau, puis choisissez l'option de menu Préférences de modificateurs réseau.

La section principale de la boîte de dialogue se compose d'une liste à trois colonnes, qui affiche les informations suivantes pour chaque ENM :

- Etat d'activation (Manuel ou Conditionnel)
- Nom défini par l'utilisateur, par exemple : « Cisco VPN »
- Etat actuel, « Exécution en cours » ou « Arrêté »

La case Démarrer/arrêter en fonction de règles est cochée si le type d'activation de l'application de modificateur réseau sélectionnée est Conditionnel, et non cochée si le type d'activation est Manuel. Pour changer le type d'activation, sélectionnez ou désélectionnez la case à cocher.

## ▼ Ajout d'un ENM de ligne de commande

La procédure suivante décrit comment ajouter un ENM de ligne de commande. Pour plus d'informations sur l'ajout d'un service d'application de modificateur réseau, reportez-vous à l'aide en ligne.

### 1 Ouvrez la boîte de dialogue **Modificateurs réseau** d'une des manières suivantes :

- Dans la vue Etat de connexion de la boîte de dialogue **Préférences réseau**, cliquez sur le bouton **Modificateurs**.
- Cliquez avec le bouton droit de la souris sur l'icône de notification Etat du réseau, puis choisissez l'option de menu **Préférences de modificateurs réseau**.

### 2 Cliquez sur le bouton **Ajouter**.

### 3 Saisissez le nom de la nouvelle application de modificateur réseau.

### 4 Effectuez l'une des opérations suivantes :

- **Pour ajouter une nouvelle entrée dont le type d'activation est Manuel, appuyez sur la touche Entrée ou de tabulation.**

Les deux boutons radio **Gérer les modificateurs** sont activés. Le premier d'entre eux, **Applications de ligne de commande**, est sélectionné par défaut. Les champs de commande **Démarrer** et **Arrêter** ainsi que les deux boutons **Parcourir** sont également activés.

- **Pour annuler vos modifications, appuyez sur Echap.**

### 5 Saisissez la commande de démarrage de l'application de modificateur réseau dans le champ **Commande de démarrage**.

Vous pouvez également utiliser le bouton **Parcourir** pour ouvrir la boîte de dialogue d'un sélecteur de fichiers dans laquelle vous pouvez sélectionner la commande à utiliser.

Le bouton Démarrer reste désactivé pour l'application de modificateur réseau tant qu'une commande valide n'est pas saisie dans ce champ.

**6 Saisissez la commande d'arrêt de l'application de modificateur réseau dans le champ Commande d'arrêt.**

Vous pouvez également utiliser le bouton Parcourir pour ouvrir la boîte de dialogue d'un sélecteur de fichiers dans laquelle vous pouvez sélectionner la commande à utiliser.

Le bouton Arrêter reste désactivé pour l'application de modificateur réseau tant qu'une commande valide n'est pas saisie dans ce champ.

**7 Pour ajouter cette application, cliquez sur OK.**

Le modificateur réseau externe est ajouté.



## PARTIE II

# Configuration de liaisons de données et d'interfaces

Cette partie décrit les procédures de configuration de liaisons de données et d'interfaces dans le contexte des profils de configuration réseau tel que présenté dans la section [Partie I](#). Les procédures s'appliquent à tout profil fixe activé.





# Utilisation des commandes de configuration de l'interface et de liaison de données sur les profils

---

Ce chapitre décrit l'utilisation des commandes de configuration classiques telles que `dladm` et `ipadm`, étant donné qu'elles sont liées à la configuration réseau basée sur les profils.

## Points principaux de la configuration réseau basée sur les profils

Dans cette version Oracle Solaris, la configuration réseau est basée sur les profils. La configuration réseau d'un système est gérée par un profil de configuration réseau spécifique (NCP, network configuration profile) et un profil d'emplacement correspondant. Pour plus d'informations sur les NCP, les profils d'emplacement et autres types de profil, leurs propriétés et les commandes permettant de manipuler et de surveiller les profils, reportez-vous à la section [Partie I](#).

---

**Remarque** – Pour la configuration réseau, les types de profils principaux sont les NCP, les profils d'emplacement, les modificateurs de réseau externe (external network modifiers, ENM), et les réseaux locaux sans fil (WLAN). Parmi ces types, le profil principal est le NCP. Dans Tout au long de cette documentation, sauf indication contraire, le terme *profil* fait référence au NCP.

---

Vous trouverez ci-après les points principaux de la configuration réseau basée sur les profils :

- Une seule paire de NCP et profils d'emplacement peut être active à un moment donné pour gérer la configuration réseau d'un système. Les autres NCP existants dans le système ne sont pas opérationnels.
- Le NCP actif peut être *réactif* ou *fixe*. Avec un profil réactif, la configuration réseau est surveillée pour s'adapter aux changements dans l'environnement réseau du système. Avec un profil fixe, la configuration du réseau est instanciée mais n'est pas surveillée.
- Les valeurs des différentes propriétés d'un NCP constituent une stratégie qui régit la manière dont le profil gère la configuration réseau.

- Les modifications apportées aux propriétés du NCP sont immédiatement implémentées en tant que nouvelles valeurs de propriété, qui deviennent partie intégrante de la stratégie du profil qui gère la configuration réseau.

---

**Remarque** – Sur un système qui a été mis à niveau à partir de la version Oracle Solaris 11.1.1 Express, la configuration réseau opérationnelle avant la mise à niveau devient le profil actif après celle-ci. Si la configuration précédente a été créée par les commandes `dladm` et `ipadm`, cette configuration constitue le profil `DefaultFixed` qui devient actif dans le système. Dans le cas contraire, la configuration devient le profil `Automatic` qui gère la configuration réseau du système.

---

## Profils et des outils de configuration

Les outils à utiliser pour personnaliser les profils dépendent du profil actif. Si le profil actif est réactif, comme `Automatic`, utilisez les commandes `netcfg` et `netadm` pour configurer et surveiller le profil. Si le profil actif est fixe, comme `DefaultFixed`, utilisez les commandes `dladm` et `ipadm`.

Les commandes `dladm` et `ipadm` sont applicables uniquement sur les profils actifs. Par conséquent, avant d'utiliser ces commandes, vous devez :

- Connaître le profil actif pour vous assurer que vous apportez les modifications au profil cible correct à l'aide des commandes appropriées.
- Savoir si le profil cible est réactif ou fixe pour éviter de causer des comportements de configuration inattendus après avoir utilisé les commandes. Un profil réactif gère la configuration du réseau différemment d'un profil fixe. Ainsi, le comportement des deux profils diffère également lorsque des modifications sont implémentées.

---

**Remarque** – L'utilisation de l'option `-t` des commandes `dladm` et `ipadm` pour créer des paramètres temporaires peut fonctionner uniquement sur un profil fixe. L'option n'est pas prise en charge sur les profils réactifs.

---

Suivez ces deux procédures afin d'utiliser correctement les commandes `dladm` et `ipadm` sur les profils.

## ▼ Procédure de détermination du mode de gestion réseau

Le mode de gestion du réseau d'un système est automatique si le NCP actif dans le système est un NCP réactif tel que `Automatic`. Utilisez cette procédure pour identifier le mode de gestion réseau avant toute configuration réseau. La procédure garantit que vous utilisez les commandes correctes pour configurer le profil approprié.

### 1 Affichez la liste des profils dans le système.

```
# netadm list -x
```

TYPE	PROFILE	STATE	AUXILIARY STATE
ncp	Automatic	online	active
ncu:phys	net0	online	interface/link is up
ncu:ip	net0	online	interface/link is up
ncu:phys	net1	online	interface/link is up
ncu:ip	net1	offline*	waiting for IP address to be set
ncp	testcfg	disabled	disabled by administrator
loc	Automatic	offline	conditions for activation are unmet
loc	NoNet	offline	conditions for activation are unmet
loc	Lab	online	active
loc	User	disabled	disabled by administrator

La sortie fournit deux informations :

- La commande `netadm list` est uniquement prise en charge si le mode de gestion réseau est automatique. Par conséquent, la génération d'une liste des profils indique que la gestion de réseau est en mode automatique. Dans le cas contraire, la commande `netadm list` aurait généré le message suivant pour indiquer que le profil `DefaultFixed` est actif dans le système.  
  

```
netadm: DefaultFixed NCP is enabled; automatic network management is not available.
'netadm list' is only supported when automatic network management is active.
```
- Si elle est générée, la liste des profils indique également le NCP réactif actif par le biais de son état, `online`. Dans l'exemple de sortie, le NCP `Automatic` est répertorié comme l'unique NCP réactif. Si d'autres NCP créés par l'utilisateur avaient été présents dans le système, ils auraient été inclus dans la liste,.

### 2 Assurez-vous que le profil approprié est actif pour les outils de configuration que vous souhaitez utiliser.

Par exemple, les commandes `dladm` et `ipadm` peuvent uniquement être utilisées sur le profil `DefaultFixed`. Cependant, la commande `netcfg` ne peut être utilisée que sur des profils réactifs tels que `Automatic`, où la gestion de réseau est en mode automatique.

Si le profil dont vous souhaitez modifier les propriétés avec les outils de configuration sélectionnés n'est pas actif, passez à l'étape suivante pour activer le profil approprié. Sinon, vous pouvez commencer à utiliser les outils pour configurer le réseau.

Par exemple, vous ne souhaitez pas que la gestion du réseau soit en mode automatique car vous préférez utiliser des lignes de commande telles que `dladm` et `ipadm` pour configurer

manuellement les liaisons de données et les interfaces. La sortie de l'étape 1 indique que le profil `Automatic` est activé. Pour utiliser des lignes de commande pour la configuration réseau, vous devez donc activer le profil `DefaultFixed`.

### 3 Pour configurer un profil différent, activez ce profil en tapant ce qui suit :

```
# netadm enable -p ncp profile-name
```

Par exemple :

```
# netadm enable -p ncp defaultfixed
```

Vous utilisez la même syntaxe de commande lorsque la gestion de réseau est en mode automatique, et que vous voulez utiliser un autre NCP réactif. Dans l'exemple de sortie de l'étape 1, supposons que vous souhaitiez activer le NCP `testcfg` créé par l'utilisateur en lieu et place de `Automatic`. Vous allez donc taper :

```
# netadm enable -p ncp testcfg
```



**Attention** – La commande intervertit les profils actifs. Lorsque vous intervertissez les profils actifs, la configuration réseau existante est supprimée et une nouvelle configuration est créée. Les modifications permanentes qui ont été mises en oeuvre sur un NCP précédemment actif sont exclues du nouveau NCP actif.

## Étapes suivantes

Les chapitres suivants décrivent les procédures que vous pouvez utiliser pour effectuer différentes configurations de types de liaison de données et d'interface.

- Pour configurer les liaisons de données, reportez-vous au [Chapitre 8, “Configuration et administration des liaisons de données”](#).
- Pour configurer les interfaces IP, reportez-vous au [Chapitre 9, “Configuration d'une interface IP”](#).
- Pour configurer les interfaces sans fil, reportez-vous au [Chapitre 10, “Configuration des communications via une interface sans fil sur Oracle Solaris”](#).
- Pour configurer les ponts, reportez-vous au [Chapitre 11, “Administration des ponts”](#).
- Pour configurer groupements de liens, reportez-vous au [Chapitre 12, “Administration de groupements de liens”](#).
- Pour configurer les VLAN, reportez-vous au [Chapitre 13, “Administration des réseaux locaux virtuels”](#).
- Pour configurer les groupes IPMP, reportez-vous au [Chapitre 14, “Présentation d'IPMP”](#) et au [Chapitre 15, “Administration d'IPMP”](#).
- Pour configurer le protocole LLDP, reportez-vous au [Chapitre 16, “Echange d'informations sur la connectivité réseau à l'aide du protocole LLDP”](#).

# Configuration et administration des liaisons de données

Ce chapitre aborde la commande d'adm et la façon dont elle est utilisée pour configurer les liaisons de données.

## Configuration des liaisons de données (tâches)

Les tableaux ci-dessous répertorient les différentes tâches de configuration de liaisons de données que vous pouvez effectuer à l'aide de la commande d'adm. Les tables fournissent également des liens vers les procédures étape par étape permettant de réaliser les tâches.

**TABEAU 8-1** Configuration de base de liaison de données (liste des tâches)

Tâche	Description	Voir
Renommage d'une liaison de données	Personnalise un nom de liaison de données au lieu d'utiliser le nom basé sur le matériel.	<a href="#">“Renommage d'une liaison de données” à la page 160</a>
Affichage des attributs physiques d'une liaison de données	Etablit une liste des informations physiques qui sous-tendent une liaison de données, y compris le type de média, l'instance de périphérique associée et autres informations.	<a href="#">“Affichage des informations relatives aux attributs physiques des liaisons de données” à la page 161</a>
Affichage de l'état des liaisons de données	Etablit une liste des informations sur l'état des liaisons de données.	<a href="#">“Affichage des informations concernant les liaisons de données” à la page 162</a>
Suppression d'une liaison de données	Supprime une configuration de lien associée à une NIC qui n'est plus utilisée.	<a href="#">“Suppression d'une liaison de données” à la page 163</a>

TABLEAU 8-2 Configuration des propriétés de liaison de données (liste des tâches)

Tâche	Description	Voir
Modification de la taille de l'unité de transmission maximale (MTU)	Augmente la taille de la MTU de transmission de paquets pour gérer les jumbo frames.	<a href="#">“Procédure d'activation de la prise en charge des jumbo frames” à la page 165</a>
Modification de la vitesse de la liaison	Désactive la vitesse de liaison plus élevée et publie uniquement la vitesse de liaison inférieure afin de permettre les communications avec un système plus ancien.	<a href="#">“Procédure de modification des paramètres de vitesse de liaison” à la page 167</a>
Affichage des informations sur les propriétés de liaison	Etablit une liste des propriétés de liaison et leur configuration actuelle ; établit une liste des paramètres Ethernet.	<a href="#">“Procédure d'obtention des informations d'état concernant les propriétés de liaisons de données” à la page 168</a>
Configuration du pilote pour qu'il utilise la liaison DMA	Définit le seuil qui fait que le pilote passe de la liaison DMA à la fonction bcopy lors de la transmission.	<a href="#">“Procédure de configuration du pilote e1000g afin d'utiliser une liaison DMA” à la page 170</a>
Définition des taux d'interruption	Définit manuellement les taux auxquels les interruptions sont fournies par le pilote plutôt que d'avoir le taux défini automatiquement.	<a href="#">“Procédure de définition manuelle du taux d'interruption” à la page 171</a>
Remplacement d'une NIC (Network Interface Card, carte d'interface réseau)	Modifie une NIC dans un système lors de la reconfiguration dynamique.	<a href="#">“Procédure de remplacement d'une NIC avec la reconfiguration dynamique” à la page 173</a>
Définition des propriétés autopush par liaison	Configure le module STREAMS de sorte qu'il soit empilé sur une liaison de données.	<a href="#">“Procédure de définition de modules STREAMS sur les liaisons de données” à la page 176</a>

## Commande dladm

Suite à l'implémentation complète de la structure de configuration de pilote GLDv3, la commande `dladm` a acquis des fonctionnalités étendues au fil du temps. La structure améliore la configuration des pilotes NIC comme suit :

- Une seule interface de commande unique, la commande `dladm`, est nécessaire pour configurer les propriétés du pilote réseau.
- Une syntaxe uniforme est utilisée indépendamment des propriétés : `dladm subcommand properties datalink` .
- L'utilisation de la commande `dladm` s'applique aux propriétés publiques et privées du pilote.

- L'utilisation de la commande dladm sur un pilote spécifique ne perturbe pas les connexions réseau d'autres NIC de types similaires. Ainsi, vous pouvez configurer les propriétés de liaisons de données de façon dynamique.
- Les paramètres de configuration de données sont stockés dans un référentiel dladm et persistent même après la réinitialisation du système.

Pour profiter des avantages répertoriés précédemment lorsque vous configurez des liaisons de données, il est conseillé d'utiliser dladm en tant qu'outil de configuration à la place des outils habituels des versions précédentes, par exemple la commande ndd.

Pour l'administration des liaisons de données, utilisez les sous-commandes dladm suivantes :

- dladm rename-link modifie le nom d'une liaison de données.
- dladm show-link affiche les liaisons de données existantes dans le système.
- dladm show-phys affiche les caractéristiques physiques des liaisons de données.
- dladm delete-phys supprime une liaison de données.
- dladm show-linkprop affiche les propriétés associées à la liaison de données.
- dladm set-linkprop définit les propriétés de liaison de données spécifiées.
- dladm reset-linkprop rétablit les paramètres par défaut des propriétés.
- dladm show-ether affiche les paramètres Ethernet d'une liaison de données.

La commande dladm est également utilisée pour exécuter d'autres types d'administration de liaison, notamment ce qui suit :

- Configuration de ponts. Reportez-vous au [Chapitre 11, “Administration des ponts”](#)
- Configuration de groupements de liens. Reportez-vous au [Chapitre 12, “Administration de groupements de liens”](#)
- Configuration des VLAN. Reportez-vous au [Chapitre 13, “Administration des réseaux locaux virtuels”](#)
- Configuration de tunnels. Reportez-vous au [Chapitre 6, “Configuration de tunnels IP”](#) du manuel *Administration d'Oracle Solaris : Services IP*.

Pour plus d'informations sur les commandes, reportez-vous à la page de manuel [dladm\(1M\)](#).

Les procédures ci-dessous indiquent comment utiliser la commande dladm pour configurer les liaisons de données. Dans la plupart des cas, la configuration de liaisons de données fait une partie de la configuration d'une interface IP sur cette liaison. Par conséquent, le cas échéant, les procédures incluent les étapes de configuration d'interface IP avec la commande ipadm. Toutefois, la configuration d'interface IP et la commande ipadm sont abordées plus en détail dans le [Chapitre 9, “Configuration d'une interface IP”](#).

## ▼ Renommage d'une liaison de données

Utilisez cette procédure si vous souhaitez personnaliser le nom d'une liaison de données. Par exemple, certaines liaisons de données dans le système mis à niveau ont pu conserver des noms hérités basés sur le matériel et vous souhaitez remplacer ces noms par des noms génériques.

### Avant de commencer

Assurez-vous d'avoir étudié et d'être prêt à effectuer les autres étapes nécessaires sur les configurations associées qui peuvent être affectées par la modification des noms de liaisons. Pour plus d'informations, reportez-vous à la section [“Noms de lien dans les systèmes mis à niveau” à la page 29](#).

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

#### 2 Si une interface IP est configurée sur la liaison de données, supprimez-la.

```
# ipadm delete-ip interface
```

#### 3 Modifiez le nom actuel de la liaison.

```
# dladm rename-link old-linkname new-linkname
```

*old-linkname*      Fait référence au nom actuel de la liaison de données. Par défaut, le nom de la liaison est basé sur le matériel, par exemple bge0.

*new-linkname*      Fait référence à tout nom que vous souhaitez attribuer à la liaison de données. Pour obtenir des informations sur les règles d'affectation de noms de liaisons, reportez-vous à la section [“Règles applicables aux noms de lien valides” à la page 30](#). Reportez-vous également à la section [“Noms de lien dans les systèmes mis à niveau” à la page 29](#) pour obtenir des informations supplémentaires sur le renommage de liaisons de données.

Si vous ne souhaitez pas que le nouveau nom de liaison persiste après une réinitialisation du système, utilisez l'option `-t` immédiatement après la sous-commande. L'option renomme la liaison temporairement. Le nom d'origine de la liaison est rétabli lorsque le système est redémarré.

---

**Remarque** – Vous pouvez utiliser `dladm rename-link` pour transférer les configurations d'une liaison de données à une autre. Pour obtenir un exemple, reportez-vous à la section [“Procédure de remplacement d'une NIC avec la reconfiguration dynamique” à la page 173](#). Lorsque vous renommez un lien dans ce but, assurez-vous que le lien qui hérite de la configuration n'est pas doté de configurations existantes. Dans le cas contraire, le transfert échoue.

---



**Exemple 8-1** Modification de l'interface réseau principale du système

L'exemple suivant illustre comment basculer l'interface réseau principale de votre système sur une deuxième NIC en renommant les liaisons de données. L'interface réseau principale du système est `net0`, le nom générique de la liaison de données sur `e1000g0`. Cette interface réseau principale passe de l'utilisation de `e1000g0` en tant qu'interface sous-jacente à celle de `nge0`. Vous pouvez utiliser cet exemple comme faisant partie de la procédure de création d'un nouvel environnement d'initialisation.

```
# dladm show-phys
LINK    MEDIA    STATE    SPEED    DUPLEX    DEVICE
net0    Ethernet  up       1000     full      e1000g0
net1    Ethernet  up       1000     full      nge0

# dladm rename-link net0 oldnet0
# dladm rename-link net1 net0

# dladm show-phys
LINK    MEDIA    STATE    SPEED    DUPLEX    DEVICE
oldnet0 Ethernet  up       1000     full      e1000g0
net0     Ethernet  up       1000     full      nge0
```

## ▼ Affichage des informations relatives aux attributs physiques des liaisons de données

Cette procédure répertorie les étapes d'affichage des informations relatives aux attributs physique des liaisons de données d'un système.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Affichez les informations sur les caractéristiques physiques des liaisons de données actuellement sur le système.

```
# dladm show-phys
```

Vous pouvez utiliser l'option `-P` avec cette commande pour afficher l'état de l'indicateur de chaque liaison. Une liaison de données devient indisponible si son matériel associé a été supprimé. Sans l'option `-P`, la commande affiche uniquement les liaisons de données disponibles.

Pour visualiser le chemin d'accès /devices des liaisons de données, utilisez l'option `-v`.

### Exemple 8-2 Affichage des liaisons de données disponibles

Dans l'exemple suivant, l'option -P inclut la colonne FLAGS où les liaisons indisponibles sont indiquées. L'indicateur r pour la liaison de données net0 indique que le matériel qui lui est associé (nge) a été supprimé.

```
# dladm show-phys
LINK      MEDIA      STATE    SPEED    DUPLEX    DEVICE
net0      Ethernet    up      100Mb    full     e1000g0
net1      Infiniband  down    0Mb      --       ibd0
net3      Ethernet    up      100Mb    full     bge0
net4      Ethernet    --      0Mb      --       nge0
```

L'exemple suivant illustre les liaisons et leurs emplacements physiques qui s'affichent lorsque vous utilisez l'option -L.

```
# dladm show-phys -L
LINK      DEVICE      LOCATION
net0      bge0        MB
net2      ibp0        MB/RISER0/PCIE0/PORT1
net3      ibp1        MB/RISER0/PCIE0/PORT2
net4      eoib2       MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
```

## ▼ Affichage des informations concernant les liaisons de données

Cette procédure affiche l'état des liaisons disponibles.

- 1 **Connectez-vous en tant qu'administrateur.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 2 **Affichez les informations concernant la liaison.**

```
# dladm show-link
```

### Exemple 8-3 Affichage des liaisons disponibles

L'exemple suivant montre les liaisons persistantes et disponibles sur le système.

```
# dladm show-link -P
LINK      CLASS    BRIDGE    OVER
net0      phys     --        --
net1      phys     --        --
net2      phys     --        --
```

L'option -P affiche également toute liaison persistante mais non disponible existante. Une liaison persistante n'est pas disponible lorsque la liaison est temporairement supprimée. Une liaison devient également indisponible si le matériel associé a été supprimé.

## ▼ Suppression d'une liaison de données

Cette procédure supprime les configurations de liaison associées aux NIC. Si vous détachez une NIC sans envisager de la remplacer, vous pouvez supprimer la configuration de liaison associée à cette NIC. Une fois la procédure terminée, le nom de la liaison peut être réutilisé.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Affichez les liaisons de données sur le système, y compris les liaisons dont le matériel a été supprimé.

Pour inclure des informations sur le matériel supprimé, utilisez l'option -P.

```
# dladm show-phys
```

### 3 Supprimez la configuration de la liaison du matériel supprimé que vous n'avez pas l'intention de remplacer.

```
# dladm delete-phys link
```

## Exemple 8–4 Suppression d'une liaison de données

Dans l'exemple suivant, l'indicateur r pour net2 indique que le matériel associé à la liaison (e1000g0) a été supprimé. Par conséquent, vous pouvez également supprimer le lien net2 et réaffecter le nom à une nouvelle liaison de données.

```
# dladm show-phys -P
LINK          DEVICE      MEDIA      FLAGS
net0          nge0        Ethernet   -----
net1          bge0        Ethernet   -----
net2          e1000g0     Ethernet   r-----

# dladm delete-phys net2
```

## Définition des propriétés de liaison de données

Outre la configuration de base de liaisons de données, vous pouvez également utiliser la commande `dladm` pour définir les propriétés de liaison de données et les personnaliser en fonction des besoins de votre réseau.

---

**Remarque** – Vous pouvez personnaliser les propriétés de liaisons de données à l'aide de la commande `dladm` à condition que le pilote de réseau de la liaison ait été converti pour la structure GLDV3, par exemple `e1000g`. Pour vérifier si votre pilote prend en charge cette fonction, reportez-vous à la page de manuel du pilote.

---

## Présentation des propriétés des liaisons de données

Les propriétés de liaisons de données qui peuvent être personnalisées varient selon les propriétés prises en charge par un pilote de NIC spécifique. Les propriétés de liaisons de données configurables à l'aide de la commande `dladm` peuvent être classées dans l'une des deux catégories suivantes :

- Les *propriétés publiques* qui peuvent être appliquées à n'importe quel pilote du type de média indiqué, telles que la vitesse de liaison, la négociation automatique pour Ethernet ou la taille de la MTU qui peut être appliquée à tous les pilotes de liaisons de données.
- Les *propriétés privées* qui sont propres à un certain sous-ensemble de pilotes de NIC pour un certain type de média. Ces propriétés peuvent être spécifiques à ce sous-ensemble car elles sont étroitement liées soit au matériel associé au pilote, soit aux détails de l'implémentation du pilote lui-même, par exemple les paramètres réglables de débogage.

Les propriétés de liaison ont en règle générale les paramètres par défaut. Cependant, certains scénarios de mise en réseau peuvent nécessiter la modification de certains paramètres de propriétés d'une liaison de données. Ces paramètres de propriétés peuvent être des propriétés publiques ou privées. Par exemple, une NIC peut communiquer avec un ancien commutateur qui n'effectue pas correctement la négociation automatique. Un commutateur peut également avoir été configuré pour prendre en charge les jumbo frames. Enfin, les propriétés spécifiques à un pilote qui régulent la transmission ou la réception de paquets peuvent avoir besoin d'être modifiées pour le pilote indiqué. Dans Oracle Solaris, tous ces paramètres peuvent maintenant être réinitialisés à l'aide d'un seul outil d'administration, `dladm`.

## Configuration des propriétés de liaisons de données à l'aide de la commande `dladm`

La section suivante indique les procédures permettant de définir certaines propriétés de liaisons de données et fournit des exemples. Les propriétés sélectionnées sont publiques et communes à tous les pilotes de NIC. Une section distincte décrit les propriétés de liaisons de données spécifiques aux pilotes. Cette section est suivie des procédures de configuration d'une sélection de propriétés privées du pilote `e1000g`.

### ▼ Procédure d'activation de la prise en charge des jumbo frames

L'activation de la prise en charge des jumbo frames dans une configuration réseau est une tâche courante pour la plupart des scénarios de réseau. La prise en charge des jumbo frames requiert l'augmentation de la taille de la MTU d'une liaison de données. La procédure suivante inclut l'utilisation de noms personnalisés pour l'identification de liaisons de données. Pour obtenir une présentation des noms personnalisés et de leur utilisation dans une configuration réseau, reportez-vous à la section [“Pile réseau dans Oracle Solaris” à la page 22](#).

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

#### 2 Afin d'identifier le périphérique Ethernet spécifique dont provient la taille de MTU nécessaire pour réinitialiser, affichez les liaisons dans le système.

```
# dladm show-phys
```

Effectuez cette étape en particulier si votre configuration réseau utilise des noms personnalisés pour les liaisons de données. Avec les noms personnalisés, les liaisons de données ne sont plus nécessairement identifiées par leur nom basé sur le matériel. Par exemple, le périphérique Ethernet est `bge0`. Toutefois, la liaison de données sur le périphérique est renommée `net0`. Par conséquent, vous devez configurer la taille de MTU de `net0`. Reportez-vous à la section [“Configuration d'interfaces IP \(tâches\)” à la page 181](#) pour obtenir des exemples de tâches de configuration sur des liaisons de données qui utilisent des noms personnalisés.

#### 3 (Facultatif) Affichez la taille actuelle de MTU de la liaison de données et autres propriétés.

- Pour afficher une propriété spécifique d'une liaison de données, utilisez la syntaxe suivante :

```
dladm show-linkprop -p property datalink
```

Cette commande affiche les paramètres de la propriété que vous indiquez.

- Pour afficher plusieurs propriétés sélectionnées de la liaison de données, utilisez la syntaxe suivante :

```
# dladm show-link datalink
```

Cette commande affiche les informations relatives à la liaison de données, y compris la taille de MTU.

- 4 Si une interface IP est configurée sur la liaison de données, supprimez-la.  
`# ipadm delete-ip interface`
- 5 Modifiez la taille de MTU de la liaison à 9000, soit le paramètre pour les jumbo frames.  
`# dladm set-linkprop -p mtu=9000 datalink`
- 6 Créez l'interface IP.  
`# ipadm create-ip interface`
- 7 Configurez l'interface IP.  
`# ipadm create-addr -T addr-type [-a address] addrobj`  
Pour plus d'informations sur la commande ipadm, reportez-vous à la section [ipadm\(1M\)](#).
- 8 (Facultatif) Vérifiez que l'interface utilise la nouvelle taille de MTU à l'aide de l'une des syntaxes de commande de l'étape 3.  
`# dladm show-linkprop -p mtu datalink`
- 9 (Facultatif) Affichez les paramètres Ethernet actuels de la liaison.  
`# dladm show-ether datalink`

**Exemple 8-5** Activation de la prise en charge des jumbo frames

L'exemple ci-après qui permet la prise en charge des jumbo frames s'appuie sur le scénario suivant :

- Le système dispose de deux NIC bge : bge0 et bge1.
- Le périphérique bge0 est utilisé en tant qu'interface principale, tandis que le périphérique bge1 est utilisé à des fins de test.
- Vous souhaitez activer la prise en charge des jumbo frames sur bge1, tout en conservant la taille de MTU par défaut de l'interface principale.
- La configuration réseau utilise des noms personnalisés pour les liaisons de données. Le nom de la liaison de bge0 est net0. Le nom de la liaison de bge1 est net1.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net0      ether      up         100Mb      full        bge0
net1      ether      up         100Mb      full        bge1
net2      ether      up         100Mb      full        nge3

# dladm show-linkprop -p mtu net1
LINK      PROPERTY  VALUE      DEFAULT      POSSIBLE
```

```

net1      mtu      1500      1500      - -

# ipadm delete-ip net1
# dladm set-linkprop -p mtu=9000 net1
# ipadm create-ip net1
# ipadm create-addr -T static -a 10.10.1.2/35 net1/v4

# dladm show-link web1
LINK      CLASS      MTU      STATE      BRIDGE      OVER
web1      phys      9000      up          --          --

```

Notez que le paramètre de MTU est maintenant 9000. Dans cet exemple, la commande `dladm` vous permet de modifier la taille de MTU de `net1` directement. La méthode précédente qui utilise la commande `ndd` aurait nécessité que vous supprimiez également `net0`, ce qui aurait perturbé inutilement les opérations de l'interface principale.

## ▼ Procédure de modification des paramètres de vitesse de liaison

La plupart des configurations réseau sont constituées d'une combinaison de systèmes avec diverses fonctions de vitesse. Par exemple, la vitesse annoncée entre un système plus ancien et un nouveau système peut avoir besoin d'être modifiée sur un paramètre plus bas afin de permettre la communication. Par défaut, toutes les capacités de vitesse et de duplex d'une carte réseau sont publiées. Cette procédure indique comment désactiver les capacités Gbit et publier uniquement les Mbit.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 (Facultatif) Affichez l'état actuel de la propriété que vous souhaitez modifier.

```
# dladm show-linkprop -p property datalink
```

### 3 Pour publier les capacités de vitesse inférieures, désactivez les capacités de vitesse supérieure pour les empêcher d'être publiées.

```
# dladm set-linkprop -p property=value1 datalink
```

## Exemple 8–6 Désactivation de la publication des capacités Gbit d'une NIC

Cet exemple illustre comment empêcher la liaison `net1` de publier les capacités Gbit.

```

# dladm show-linkprop -p adv_1000fdx_cap net1
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net1      adv_1000fdx_cap  1          --          1,0

# dladm show-linkprop -p adv_1000hdx_cap web1
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net1      adv_1000hdx_cap  1          --          1,0

```

Les propriétés qui publient les capacités Gbit de la liaison sont `adv_1000fdx_cap` et `adv_1000hdx_cap`. Pour désactiver la publication de ces propriétés, tapez la commande suivante :

```
# dladm set-linkprop -p adv_1000fdx_cap=0 net1
# dladm set-linkprop -p adv_1000hdx_cap=0 net1
```

La liste des paramètres Ethernet s'afficherait la sortie suivante :

```
# dladm show-ether net1
LINK      PTYPE      STATE      AUTO  SPEED-DUPLEX      PAUSE
net1      current    up         yes   1G-f              both
```

## ▼ Procédure d'obtention des informations d'état concernant les propriétés de liaisons de données

Vous pouvez obtenir des informations sur les propriétés de la liaison de données en affichant les paramètres Ethernet ou les propriétés de la liaison.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 Pour obtenir plus d'informations sur les paramètres Ethernet, utilisez la commande suivante :

```
# dladm show-ether [-x] datalink
```

où l'option `-x` inclut des informations de paramètres supplémentaires concernant la liaison. Sans l'option `-x`, seuls les paramètres actuels sont affichés.

### 3 Pour obtenir des informations sur l'ensemble des propriétés de la liaison, utilisez la commande suivante :

```
# dladm show-linkprop datalink
```

## Exemple 8-7 Affichage des paramètres Ethernet

Cet exemple affiche une liste étendue d'informations de paramètres d'une liaison spécifique.

```
# dladm show-ether -x net1
LINK      PTYPE      STATE      AUTO  SPEED-DUPLEX      PAUSE
net1      current    up         yes   1G-f              both
--      capable    --         yes   1G-fh,100M-fh,10M-fh  both
--      adv        --         yes   100M-fh,10M-fh      both
--      peeradv    --         yes   100M-f,10M-f        both
```

Avec l'option `-x`, la commande affiche également les fonctions intégrées du lien spécifié, ainsi que les fonctions qui sont actuellement publiées entre l'hôte et le partenaire de liaison. Les informations suivantes sont affichées :



- Pour l'état actuel du périphérique Ethernet, la liaison est active et opérationnelle à 1 Gbit par seconde en duplex intégral. Sa capacité de négociation automatique est activée et dispose du contrôle de flux bidirectionnel, dans lequel l'hôte et le partenaire de liaison peuvent envoyer et recevoir des trames de pause.
- Quel que soit le paramètre actuel, les capacités du périphérique Ethernet sont répertoriées. Le type de négociation peut être défini sur automatique, le périphérique peut prendre en charge des vitesses de 1 Gbit par seconde, 100 Mbits par seconde, et 10 Mbits par seconde, en duplex intégral et semi-duplex. De même, les trames de pause peuvent être reçues ou envoyées dans les deux sens entre l'hôte et le partenaire de liaison.
- Les capacités de net1 sont publiées comme suit : négociation automatique, duplex de vitesse et contrôle de flux des trames de pause.
- De même, la liaison ou le partenaire pair de net1 publie les capacités suivantes : négociation automatique, duplex de vitesse et contrôle de flux des trames de pause.

### Exemple 8-8 Affichage des propriétés de la liaison

Cet exemple illustre comment obtenir la liste toutes les propriétés d'une liaison. Si vous souhaitez afficher uniquement des propriétés spécifiques, utilisez l'option -p avec les propriétés spécifiques que vous souhaitez surveiller.

```
# dladm show-linkprop net1
```

LINK	PROPERTY	VALUE	DEFAULT	POSSIBLE
net1	speed	1000	--	--
net1	autopush	--	--	--
net1	zone	--	--	--
net1	duplex	half	--	half, full
net1	state	unknown	up	up, down
net1	adv_autoneg_cap	1	1	1, 0
net1	mtu	1500	1500	--
net1	flowctrl	no	bi	no, tx, rx, bi
net1	adv_1000fdx_cap	1	1	1, 0
net1	en_1000fdx_cap	1	1	1, 0
net1	adv_1000hdx_cap	1	1	1, 0
net1	en_1000hdx_cap	1	1	1, 0
net1	adv_100fdx_cap	0	0	1, 0
net1	en_100fdx_cap	0	0	1, 0
net1	adv_100hdx_cap	0	0	1, 0
net1	en_100hdx_cap	0	0	1, 0
net1	adv_10fdx_cap	0	0	1, 0
net1	en_10fdx_cap	0	0	1, 0
net1	adv_10hdx_cap	0	0	1, 0
net1	en_10hdx_cap	0	0	1, 0

Les paramètres pour les capacités de vitesse et de duplex de la liaison lien sont configurés manuellement sur les propriétés de vitesse activées qui sont étiquetées en\_\*\_cap. Par exemple, en\_1000fdx\_cap est la propriété pour la capacité de duplex intégral Gbits et en\_100hdx\_cap est la propriété de la capacité en semi-duplex 100 Mbits. Les paramètres de ces propriétés de vitesse

activée sont publiées entre l'hôte et son partenaire de liaison par les propriétés de vitesse correspondantes publiées, qui sont étiquetées `adv_*_cap` comme `adv_1000fdx_cap` et `adv_100hdx_cap`.

Normalement, les paramètres d'une propriété de vitesse activée spécifique et la propriété correspondante annoncée sont identiques. Cependant, si une NIC prend en charge certaines fonctionnalités avancées telles que la gestion de l'alimentation, celles-ci peuvent définir des limites sur les bits sont réellement publiés entre l'hôte et son partenaire de liaison. Par exemple, avec la gestion de l'alimentation, les paramètres des propriétés `adv_*_cap` pourraient uniquement être un sous-ensemble des paramètres des propriétés en `*_cap`. Pour plus d'informations sur les propriétés de vitesse activées et publiées, reportez-vous à la page de manuel [dladm\(1M\)](#).

## ▼ Procédure de configuration du pilote e1000g afin d'utiliser une liaison DMA

Cette procédure et la procédure suivante indiquent comment configurer des propriétés privées. Les deux procédures s'appliquent aux propriétés spécifiques du pilote e1000g. Cependant, les étapes générales peuvent également être utilisées pour configurer les propriétés privées d'autres pilotes NIC.

Le trafic de masse, telles que les transferts de fichiers, implique habituellement la négociation de paquets de grande taille au sein du réseau. Dans de tels cas, vous pouvez obtenir de meilleures performances du pilote e1000g en le configurant de sorte qu'il utilise automatiquement la liaison DMA, où un seuil est défini pour les tailles de fragment de paquet. Si la taille de fragment dépasse le seuil, la liaison DMA est utilisée pour la transmission. Si la taille de fragment ne dépasse pas le seuil, le mode bcopy est utilisé, où les données de fragment sont copiées sur le tampon de transmission préalloué.

Pour définir le seuil, procédez comme suit :

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “Procédure d'obtention des droits d'administration” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Définissez le paramètre approprié de la propriété `_tx_bcopy_threshold`.

```
# dladm set-linkprop -p _tx_bcopy_threshold=value e1000g-datalink
```

Pour cette propriété, les paramètres valides pour le seuil sont compris entre 60 et 2048.

---

**Remarque** – A l'instar de la configuration des propriétés publiques, l'interface doit également être démontée avant que les paramètres de propriété privés puissent être modifiés.

---

**3 (Facultatif) Vérifiez le nouveau paramètre de seuil.**

```
# dladm show-linkprop -p _tx_bcopy_threshold e1000g-datalink
```

**▼ Procédure de définition manuelle du taux d'interruption**

Les paramètres qui régissent le taux auquel les interruptions sont fournies par le pilote `e1000g` affectent également les performances réseau et système. En règle générale, les paquets du réseau sont fournis à la couche supérieure de la pile en générant une interruption pour chaque paquet. En retour, le taux d'interruption, par défaut, est automatiquement ajusté par la couche GLD dans le noyau. Cependant, il se peut que ce mode ne soit pas souhaitable dans toutes les conditions de trafic réseau. Pour une discussion sur ce problème, consultez ce document (<http://www.stanford.edu/class/cs240/readings/mogul.pdf>) qui a été présenté lors de la conférence technique USENIX en 1996. Par conséquent, dans certaines circonstances, la définition manuelle du taux d'interruption est nécessaire pour obtenir de meilleures performances.

Pour définir le taux d'interruption, vous devez définir les paramètres suivants :

- `_intr_throttling_rate` détermine le délai d'attente entre les assertions interruption indépendamment des conditions du trafic réseau.
- `_intr_adaptive` détermine si le réglage automatique du taux de régulation d'interruption est activé. Par défaut, ce paramètre est activé.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Si nécessaire, identifiez le périphérique dont vous souhaitez modifier la propriété de pilote.**

```
# dladm show-phys
```

**3 Désactivez le réglage automatique du taux de régulation d'interruption.**

```
# dladm set-linkprop -p _intr_adaptive=0 e1000g-datalink
```

---

**Remarque** – Lorsque le réglage automatique du taux de régulation d'interruption est activé, tout paramètre existant pour le paramètre `_intr_throttling_rate` est ignoré.

---

**4 Supprimez toute interface IP qui est configurée sur la liaison de données.****5 Définissez le paramètre pour le niveau minimum inter-interruption.**

```
# dladm set-linkprop -p _intr_throttling_rate=value e1000g-datalink
```

---

**Remarque** – La définition par défaut du paramètre `_intr_throttling_rate` est de 550 sur les systèmes SPARC et de 260 sur les systèmes basés sur x86. La définition de la valeur minimale du niveau inter-interruption sur 0 désactive la logique de régulation d'interruption.

---

## 6 Configurez l'interface IP.

## 7 (Facultatif) Affichez les nouveaux paramètres du seuil.

### Exemple 8–9 Configuration de la liaison DMA et définition du taux de régulation d'interruption

Cet exemple utilise un système x86 avec une NIC `e1000g`. Le pilote est configuré avec un paramètre de seuil permettant de basculer entre l'utilisation de la liaison DMA ou du mode `bcopy` pour transmettre les paquets. Le paramètre du taux de régulation d'interruption est également modifié. De plus, la liaison de données `e1000g` utilise le nom générique par défaut qui est affecté par le système d'exploitation. Par conséquent, la configuration est effectuée sur la liaison de données en faisant référence au nom personnalisé, `net0`.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net0      ether      up         100Mb      full        e1000g0

# dladm show-linkprop -p _tx_bcopy_threshold net0
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _tx_bcopy_threshold  512        512          --

# dladm show-linkprop -p _intr_throttling_rate
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _intr-throttling_rate  260        260          --

# ipadm delete-ip net0
# dladm set-linkprop -p _tx_bcopy_threshold=1024 net0
# dladm set-linkprop -p _intr_adaptive=0 net0
# dladm set-linkprop -p _intr_throttling_rate=1024 net0

# ipadm create-ip net0
# ipadm create-addr -T static -a 10.10.1.2/24 net0/v4addr
# dladm show-linkprop -p _tx_bcopy_threshold=1024 net0
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _tx_bcopy_threshold  1024        512          --

# dladm show-linkprop -p _intr_adaptive net0
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _intr-adaptive    0          1            --

# dladm show-linkprop -p _intr_throttling_rate
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _intr-throttling_rate  1024        260          --
```

# Tâches de configuration supplémentaires sur les liaisons de données

Cette section décrit d'autres procédures de configuration courantes qui ont été simplifiées par l'utilisation de la commande `dladm`, par exemple la reconfiguration dynamique (DR) et l'utilisation de modules STREAMS.

## ▼ Procédure de remplacement d'une NIC avec la reconfiguration dynamique

Cette procédure s'applique uniquement aux systèmes qui prennent en charge la reconfiguration dynamique (DR). Elle illustre comment la DR est désormais facilitée par la séparation de la configuration de liaison réseau de la configuration matérielle du réseau. Il est désormais inutile de reconfigurer vos liaisons réseau après avoir terminé la DR. Maintenant, il suffit de transférer les configurations de liaison de la NIC retirée afin qu'elles soient héritées par la NIC de remplacement.

### Avant de commencer

Les procédures de DR varient en fonction du type de système. Assurez-vous de terminer ce qui suit au préalable :

- Assurez-vous que votre système prend en charge la reconfiguration dynamique.
- Assurez-vous que votre profil de configuration réseau actif est `DefaultFixed`. Reportez-vous à la section *Dynamic Reconfiguration and Network Configuration Profiles* in “Fonctionnement de NWAM avec d'autres technologies de mise en réseau Oracle Solaris” à la page 43 for information about using DR if your system's active NCP is not `DefaultFixed`.
- Consultez le manuel approprié décrivant la DR sur votre système.

Pour localiser la documentation actuelle sur la reconfiguration dynamique sur les serveurs Sun d'Oracle, recherchez `dynamic reconfiguration` à l'adresse <http://www.oracle.com/technetwork/indexes/documentation/index.html>

---

**Remarque** – La procédure suivante fait uniquement référence aux aspects de la DR qui sont spécifiquement liés à l'utilisation de noms flexibles pour les liaisons de données. La procédure ne comporte pas l'ensemble des étapes nécessaires pour effectuer la DR. Vous devez consulter la documentation relative à la DR appropriée pour votre système.

---

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “Procédure d'obtention des droits d'administration” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 (Facultatif) Affichez les informations sur les caractéristiques physiques des liaisons de données et leurs emplacements respectifs sur le système.**

```
# dladm show-phys -L
```

Pour plus d'informations sur le type d'informations affichées par `dladm show-phys -L`, reportez-vous à la page de manuel [dladm\(1M\)](#).

**3 Effectuez les procédures DR comme détaillé dans la documentation de votre système pour supprimer une NIC, puis insérez une NIC de remplacement.**

Reportez-vous à la documentation relative à la DR de votre système pour effectuer cette étape.

Une fois la NIC de remplacement installée, passez à l'étape suivante.

**4 Si vous avez inséré la NIC de remplacement dans le même emplacement que l'ancienne, passez à l'étape 6. Dans le cas contraire, passez à l'étape suivante.**

Lorsque la nouvelle NIC utilise le même emplacement que l'ancienne, la nouvelle NIC hérite du nom et de la configuration de liaison de l'ancienne NIC.

**5 Effectuez l'une des étapes ci-dessous en fonction des circonstances qui s'appliquent.**

- Si l'ancienne NIC à remplacer reste dans son emplacement dans le système comme une NIC inutilisée, procédez comme suit :

- a. Attribuez un nom différent à la NIC à remplacer.

```
# dladm rename-link oldNIC new-name
```

*oldNIC*            Fait référence à la NIC remplacée mais que vous conservez dans le système.

*new-name*        Fait référence au nouveau nom que vous attribuez à *removedNIC*. Aucune autre liaison dans le système ne peut partager ce nom.

- b. Attribuez le nom de l'ancienne NIC à celle de remplacement.

```
# dladm rename-link replacementNIC oldNIC
```

*replacementNIC*    Fait référence à la nouvelle NIC que vous venez d'installer. Cette carte d'interface réseau reçoit automatiquement le nom de liaison par défaut en fonction de l'emplacement qu'elle occupe dans le système.

*oldNIC*            Fait référence à la NIC remplacée mais que vous conservez dans le système.

- Si vous avez supprimé l'ancienne NIC et que vous installez la NIC de remplacement dans un emplacement différent, mais souhaitez que la NIC hérite des configurations de l'ancienne NIC, attribuez le nom de l'ancienne NIC à la nouvelle.

```
# dladm rename-link replacementNIC oldNIC
```

- 6 Terminez le processus de reconfiguration dynamique en activant les nouvelles ressources de la NIC pour qu'elles soient disponibles pour une utilisation par Oracle Solaris.**

Par exemple, la commande `cfgadm` vous permet de configurer la NIC. Pour plus d'informations, reportez-vous à la page de manuel [cfgadm\(1M\)](#).

- 7 (Facultatif) Affichez les informations concernant la liaison.**

Par exemple, vous pouvez utiliser `dladm show-phys` ou `dladm show-link` pour afficher des informations sur les liaisons de données.

### Exemple 8–10 Reconfiguration dynamique à l'aide de l'installation d'une nouvelle carte réseau

Cet exemple illustre comment remplacer une carte bge avec le nom de liaison `net0` par une carte `e1000g`. Les configurations de liaison de `net0` sont transférées de bge à `e1000g` une fois que `e1000g` est connecté au système.

```
# dladm show-phys -L
LINK      DEVICE      LOCATION
net0      bge0           MB
net1      ibp0           MB/RISER0/PCIE0/PORT1
net2      ibp1           MB/RISER0/PCIE0/PORT2
net3      eoib2          MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
```

Vous effectuez les étapes spécifiques à la DR, notamment l'utilisation de `cfgadm` pour supprimer bge et installer `e1000g` à sa place. Une fois la carte installée, la liaison de données de `e1000g0` prend automatiquement le nom `net0` et hérite des configurations de liaison.

```
# dladm show-phys -L
LINK      DEVICE      LOCATION
net0      e1000g0      MB
net1      ibp0           MB/RISER0/PCIE0/PORT1
net2      ibp1           MB/RISER0/PCIE0/PORT2
net3      eoib2          MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
```

```
# dladm show-link
LINK      CLASS      MTU      STATE      OVER
net0      phys       9600     up         ---
net1      phys       1500     down       ---
net2      phys       1500     down       --
net3      phys       1500     down       ---
```

## Configuration de modules STREAMS sur les liaisons de données

Si nécessaire, vous pouvez définir jusqu'à huit modules STREAMS pour qu'ils soient empilés sur une liaison de données. Ces modules sont généralement utilisés par un logiciel de gestion de

réseau tiers, notamment les réseaux privés virtuels (VPN) et les pare-feux. La documentation concernant de tels logiciels de gestion de réseau est fournie par l'éditeur du logiciel.

La liste des modules STREAMS à empiler sur une liaison de données est contrôlée par la propriété de liaison autopush. Par conséquent, la valeur de la propriété de liaison autopush est définie à l'aide de la sous-commande `dladm set-linkprop`.

Une commande autopush distincte peut également être utilisée pour définir les modules STREAMS autopush pilote par pilote. Cependant, le pilote est toujours lié à la NIC. Si la NIC sous-jacente de la liaison de données est supprimée, les informations relatives à la propriété autopush de la liaison sont également perdues.

Pour configurer les modules STREAMS à empiler sur une liaison de données, l'utilisation de la commande `dladm set-linkprop` est préférable à celle de la commande autopush. Si des types de configuration autopush par pilote et par liaison existent tous deux pour une liaison de données spécifique, les informations par liaison définies avec `dladm set-linkprop` sont utilisées et les informations par pilote sont ignorées.

## ▼ Procédure de définition de modules STREAMS sur les liaisons de données

La procédure suivante décrit comment configurer les modules STREAMS à l'aide de la commande `dladm set-linkprop`.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Déplacez les modules dans le flux de données lors de l'ouverture de la liaison.

```
# dladm set-linkprop -p autopush=modulelist link
```

*modulelist*      Spécifie la liste de modules que vous voulez déplacer automatiquement dans le flux de données. Un maximum de huit modules peut être déplacé sur une liaison. Ces modules sont déplacés suivant l'ordre dans lequel ils sont répertoriés dans *modulelist*. Séparez les différents modules dans la liste en utilisant des points comme séparateurs.

*link*            Spécifie la liaison sur laquelle les modules sont déplacés.

## Exemple 8–11 Définition de la propriété de liaison autopush

Dans cet exemple, vous empilez les modules `vpnmod` et `bufmod` sur la liaison `net0`. Le périphérique sous-jacent de la liaison est `bge0`.

```
# dladm set-linkprop -p autopush=vpnmod.bufmod net0
```



Si vous remplacez ultérieurement la carte bge par e1000g, vous pouvez passer à la nouvelle liaison de données sans avoir à reconfigurer les paramètres autopush. La carte e1000g hérite automatiquement du nom de liaison et de la configuration de bge.

## ▼ Obtention des paramètres de propriétés de liaison autopush

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Affichez les paramètres de la propriété de liaison autopush.

```
# dladm show-linkprop -p autopush [link]
```

Si vous ne spécifiez pas *link*, les informations de toutes les liaisons configurées s'affichent.

## ▼ Procédure de suppression des paramètres de propriété de liaison autopush

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Supprimez les paramètres de propriété de liaison autopush d'une liaison de données spécifique.

```
# dladm reset-linkprop [-t] -p autopush link
```

Utilisez l'option `-t` pour supprimer les paramètres de propriété temporairement. Les paramètres sont restaurés lorsque vous réinitialisez le système.



# Configuration d'une interface IP

---

Ce chapitre fournit les procédures qui sont utilisées pour configurer une interface IP sur une liaison de données.

## A propos de la configuration d'interface IP

Une fois que vous avez installé Oracle Solaris, vous pouvez effectuer les tâches suivantes :

- Configurer une interface IP sur une liaison de données pour une configuration d'interface de base. Ce chapitre décrit les procédures.
- Configurer des interfaces sans fil. Les procédures sont décrites dans le [Chapitre 10, “Configuration des communications via une interface sans fil sur Oracle Solaris”](#)
- Configurer des interfaces IP en tant que membres d'un groupe IPMP. Les procédures sont décrites dans le [Chapitre 15, “Administration d'IPMP”](#).

## Commande ipadm

Les progrès dans Oracle Solaris ont surpassé les capacités des outils traditionnels pour gérer efficacement différents aspects de la configuration réseau. La commande `ifconfig`, par exemple, était l'outil habituel pour configurer les interfaces réseau. Cependant, cette commande n'implémente pas de paramètres de configuration persistants. Au fil du temps, `ifconfig` a fait l'objet d'améliorations par l'ajout de fonctions dans l'administration réseau. Cependant, la commande est devenue complexe et difficile à utiliser.

Un autre problème avec la configuration et l'administration d'interface est l'absence d'outils simples pour administrer les propriétés ou les paramètres réglables du protocole Internet TCP/IP. La commande `ndd` était l'outil de personnalisation conçu pour cet objectif. Cependant, à l'instar de la commande `ifconfig`, la commande `ndd` n'implémente pas de paramètres de configuration persistants. Auparavant, les paramètres persistants pouvaient être simulés pour

un scénario de réseau en modifiant les scripts d'initialisation. Avec l'introduction de la fonction de SMF d'Oracle Solaris, l'utilisation de ce type de solutions de rechange peut devenir risquée à cause de la complexité de la gestion des dépendances SMF, notamment à la lumière des mises à niveau vers l'installation Oracle Solaris.

La commande `ipadm` est introduite pour remplacer à terme la commande `ifconfig` pour la configuration d'interface. La commande remplace également la commande `ndd` pour configurer les propriétés de protocole.

Comme outil de configuration d'interfaces, la commande `ipadm` offre les avantages suivants :

- Elle gère les interfaces IP et les adresses IP plus efficacement en étant l'outil unique pour l'administration d'interfaces IP, contrairement à la commande `ifconfig` qui est utilisée à des fins autres que la configuration d'interfaces.
- Elle fournit une option pour implémenter des paramètres persistants de configuration d'interfaces et d'adresses.

Pour obtenir une liste d'options d'`ifconfig` et leurs sous-commandes `ipadm` équivalentes, reportez-vous à la section [“Options des commandes `ifconfig` et `ipadm`”](#) à la page 204.

Comme outil de définition de propriétés de protocole, la commande `ipadm` offre les avantages suivants :

- Elle peut définir des propriétés de protocole temporaires ou persistantes pour les IP, l'ARP (Address Resolution Protocol, protocole de résolution d'adresse), l'SCTP (Stream Control Transmission Protocol, protocole de transmission de contrôle de flux) et l'ICMP (Internet Control Message Protocol, protocole de messages de contrôle Internet) ainsi que les protocoles de couche supérieure comme TCP et UDP (User Datagram Protocol, protocole de datagramme utilisateur).
- Elle fournit des informations concernant chaque paramètre TCP/IP, comme le paramètre actuel et par défaut d'une propriété, ainsi que la gamme de paramètres possibles. Par conséquent, les informations de débogage sont plus faciles à obtenir.
- La commande `ipadm` suit aussi une syntaxe de commande cohérente et par conséquent est plus facile à utiliser.

Pour obtenir une liste d'options de `ndd` et leurs sous-commandes `ipadm` équivalentes, reportez-vous à la section [“Options des commandes `ndd` et `ipadm`”](#) à la page 206.

Pour plus d'informations sur la commande `ipadm`, reportez-vous à la page de manuel [ipadm\(1M\)](#).

## Configuration d'interfaces IP (tâches)

Cette section décrit les procédures de configuration de base d'interfaces IP. Le tableau suivant décrit les tâches de configuration et fait correspondre ces tâches aux procédures correspondantes.

TABLEAU 9-1 Configuration d'interfaces IP (liste des tâches)

Tâche	Description	Voir
Définition d'un système pour prendre en charge les adresses MAC uniques	Configure un système SPARC pour permettre les adresses MAC uniques pour les interfaces.	<a href="#">“SPARC : Garantie de l'unicité de l'adresse MAC d'une interface” à la page 181</a>
Configuration de base d'interfaces IP à l'aide de la commande <code>ipadm</code>	Crée une interface IP et affecte des adresses IP valides, statiques ou DHCP.	<a href="#">“Configuration d'une interface IP” à la page 183</a>
Personnalisation d'une adresse IP à l'aide de la commande <code>ipadm</code>	Définit l'ID de réseau d'une adresse IP donnée.	<a href="#">“Procédure de définition des propriétés d'une adresse IP” à la page 188</a>
Obtention d'informations sur les interfaces à l'aide de la commande <code>ipadm</code>	Répertorie différentes propriétés d'interfaces, d'adresses et de protocoles ainsi que leurs paramètres.	<a href="#">“Procédure d'obtention d'informations sur les interfaces réseau” à la page 198</a>

### ▼ SPARC : Garantie de l'unicité de l'adresse MAC d'une interface

Certaines applications exigent que les adresses MAC de toutes les interfaces d'un hôte soient uniques. Toutefois, les systèmes SPARC possèdent une adresse MAC à l'échelle du système appliquée à toutes les interfaces par défaut. Vous devez configurer les adresses MAC d'origine des interfaces d'un système SPARC dans les deux contextes suivants :

- Dans le cadre d'un regroupement de liens, vous devez utiliser les adresses MAC d'origine des interfaces de la configuration de regroupement.
- Dans le cadre des groupes IPMP, chaque interface doit posséder une adresse MAC unique. Ces interfaces doivent utiliser les adresses MAC d'origine.

Le paramètre `EEPROM local-mac-address?` détermine si les interfaces du système SPARC utilisent l'adresse MAC du système ou leur adresse MAC unique. La procédure suivante indique comment vérifier la valeur actuelle du paramètre `local-mac-address?` à l'aide de la commande `eeprom` et la modifier, au besoin.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Déterminez si toutes les interfaces du système utilisent l'adresse MAC système.**

```
# eeprom local-mac-address?
local-mac-address?=false
```

Dans cet exemple, la réponse à la commande `eeprom local-mac-address?=false`, indique que toutes les interfaces utilisent l'adresse MAC du système. Pour que les interfaces puissent devenir membres d'un groupe IPMP, vous devez remplacer `local-mac-address?=false` par `local-mac-address?=true`. Vous devez également remplacer `local-mac-address?=false` par `local-mac-address?=true` pour les regroupements.

**3 Si nécessaire, modifiez la valeur de `local-mac-address?` comme suit :**

```
# eeprom local-mac-address?=true
```

A la réinitialisation du système, les interfaces avec adresses MAC d'origine utilisent celles-ci plutôt que l'adresse MAC du système. Les interfaces sans adresses MAC d'origine continuent d'utiliser les adresses MAC d'origine.

**4 Vérifiez l'adresse MAC de toutes les interfaces du système.**

Recherchez des cas dans lesquels plusieurs interfaces possèdent la même adresse MAC. Dans cet exemple, toutes les interfaces utilisent l'adresse MAC système `8:0:20:0:0:1`.

```
# dladm show-linkprop -p mac-address
```

LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
net0	mac-address	rw	8:0:20:0:0:1	8:0:20:0:0:1	--
net1	mac-address	rw	8:0:20:0:0:1	8:0:20:0:0:1	--
net3	mac-address	rw	0:14:4f:45:c:2d	0:14:4f:45:c:2d	--

---

**Remarque** – Passez à l'étape suivante uniquement si plusieurs interfaces réseau possèdent une même adresse MAC. Sinon, passez à la dernière étape.

---

**5 Au besoin, configurez manuellement les interfaces restantes de sorte que chaque interface possède une adresse MAC unique.**

```
# dladm set-linkprop -p mac-address=mac-address interface
```

Dans l'exemple de l'étape précédente, vous devez configurer les interfaces `net0` et `net1` avec des adresses MAC gérées localement. Par exemple, pour reconfigurer l'interface `net0` avec l'adresse MAC gérée localement `06:05:04:03:02`, vous devez taper la commande suivante :

```
# dladm set-linkprop -p mac-address=06:05:04:03:02 net0
```

Pour plus d'informations sur cette commande, reportez-vous à la page de manuel [dladm\(1M\)](#).

## 6 Réinitialisez le système.

# Configuration d'interfaces IP

Les procédures suivantes vous indiquent comment utiliser la commande `ipadm` pour différents besoins de configuration IP. Bien que la commande `ifconfig` fonctionne toujours pour configurer des interfaces, il est préférable d'utiliser la commande `ipadm`. Pour une présentation de la commande `ipadm` et de ses avantages, reportez-vous à la section “[Commande ipadm](#)” à la page 179.

---

**Remarque** – En règle générale, la configuration d'interfaces IP et la configuration de liaisons de données s'effectuent ensemble. Par conséquent, les procédures qui suivent incluent parfois des étapes de configuration de liaisons de données avec l'utilisation de la commande `dladm`. Pour plus d'informations sur l'utilisation de la commande `dladm` pour configurer et administrer des liaisons de données, reportez-vous au [Chapitre 8, “Configuration et administration des liaisons de données”](#).

---

## ▼ Configuration d'une interface IP

La procédure ci-après donne un exemple de configuration de base d'une interface IP.

### Avant de commencer

Déterminez si vous souhaitez renommer les liaisons de données sur le système. En règle générale, vous utilisez les noms génériques affectés par défaut aux liaisons de données. Pour modifier les noms des liens, reportez-vous à la section “[Renommage d'une liaison de données](#)” à la page 160.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 (Facultatif) Affichez des informations sur les attributs physiques des liaisons de données actuellement présentes sur le système.

```
# dladm show-phys
```

Cette commande affiche les cartes réseau physiques installées sur votre système et certaines de leurs propriétés. Pour plus d'informations sur cette commande, reportez-vous à la section [Affichage des informations relatives aux attributs physiques des liaisons de données](#).

### 3 Affichez les informations relatives aux liaisons de données actuellement présentes sur le système.

```
# dladm show-link
```

Cette commande permet d'afficher les liaisons de données et certaines propriétés qui ont été définies pour elles, y compris les cartes physiques sur lesquelles les liens ont été créés.

#### 4 Créez l'interface IP.

# **ipadm create-interface-class** *interface*

*interface-class*      Fait référence à l'une des trois classes d'interfaces que vous pouvez créer :

- Interface IP. Cette classe d'interface est la plus couramment créée lors de la configuration du réseau. Pour créer cette classe d'interface, utilisez la sous-commande `create-ip`.
- Pilote d'interface réseau virtuelle STREAMS (interface VNI). Pour créer cette classe d'interface, utilisez la sous-commande `create-vni`. Pour plus d'informations sur les périphériques ou interfaces VNI, reportez-vous à la page de manuel [vni\(7d\)](#).
- Interface IPMP. Cette interface est utilisée lorsque vous configurez les groupes IPMP. Pour créer cette classe d'interface, utilisez la sous-commande `create-ipmp`. Pour plus d'informations sur les groupes IPMP, reportez-vous au [Chapitre 14, "Présentation d'IPMP"](#) et au [Chapitre 15, "Administration d'IPMP"](#).

*interface*              Fait référence au nom de l'interface. Le nom est identique au nom du lien sur lequel l'interface est créée.

---

**Remarque** – Vous devez créer l'interface IP avant de pouvoir lui affecter l'adresse IP.

---

#### 5 Configurez l'interface IP à l'aide d'une adresse IP valide.

La syntaxe suivante attribue une adresse statique à une interface. Reportez-vous à la page de manuel [ipadm\(1M\)](#) pour découvrir d'autres options d'attribution d'adresses IP.

# **ipadm create-addr -T** *address-type* **-a** *address/prefixlen addrobj*

**-T** *address-type*      Spécifie le type de l'adresse IP affectée à l'interface, qui est l'un des suivants : `static`, `dhcp` ou `addrconf`. `Addrconf` fait référence aux adresses IPv6 générées automatiquement.

**-a**                      Indique l'adresse IP à configurer dans l'interface. Vous pouvez spécifier uniquement une adresse locale, ou une adresse locale et une adresse distante dans le cas de la configuration d'un tunnel. En règle générale, vous affectez uniquement une adresse locale. Dans ce cas, vous indiquez l'adresse directement avec l'option `-a`, par exemple : `-a address`. L'adresse est automatiquement considérée comme une adresse locale.

Si vous configurez des tunnels, vous pouvez être invité à fournir l'adresse locale du système et l'adresse distante du système de destination. Dans ce cas, vous devez spécifier `local` et `remote` afin de distinguer les deux



adresses, comme suit : -a local=*local-addr*, remote=*remote-addr*. Pour plus d'informations sur les tunnels, reportez-vous au [Chapitre 6](#), “Configuration de tunnels IP” du manuel *Administration d'Oracle Solaris : Services IP*.

Si vous utilisez une adresse IP numérique, utilisez le format *address/prefixlen* pour les adresses en notation CIDR, par exemple, 1.2.3.4/24. Reportez-vous à l'explication relative à l'option *prefixlen*.

Si vous le souhaitez, vous pouvez spécifier un nom d'hôte pour *address* au lieu d'une adresse IP numérique. Un nom d'hôte peut être utilisé si une adresse IP numérique correspondante est définie pour ce nom d'hôte dans le fichier */etc/hosts*. Si aucune adresse IP numérique n'est définie dans le fichier, la valeur numérique est uniquement obtenue à l'aide de la commande de l'interpréteur indiquée pour *host* dans le service *name-service/switch*. Si plusieurs entrées existent pour un nom d'hôte donné, une erreur est générée.

---

**Remarque** – Au cours du processus d'initialisation, la création d'adresses IP précède l'attribution de noms aux services mis en ligne. Vous devez donc vous assurer que tout nom d'hôte utilisé dans la configuration réseau est défini dans le fichier */etc/hosts*.

---

*/prefixlen*

Spécifie la longueur de l'identité réseau faisant partie de l'adresse IPv4 lorsque vous utilisez la notation CIDR. Dans l'adresse 12.34.56.78/24, 24 est le *prefixlen*. Si vous n'incluez pas *prefixlen*, le masque de réseau est calculé en fonction de la séquence répertoriée pour *netmask* dans le service *name-service/switch* ou à l'aide de la sémantique d'adressage classful.

*addrobj*

Spécifie un identificateur pour l'adresse IP unique ou l'ensemble d'adresses utilisé(e) dans le système. Les adresses peuvent être de type IPv4 ou IPv6. L'identificateur utilise le format *interface/ user\_specified\_string*.

La variable *interface* fait référence à l'interface IP à laquelle l'adresse est affectée. La variable *interface* doit refléter le nom de la liaison de données sur laquelle l'interface IP est configurée.

*user-specified-string* fait référence à une chaîne de caractères alphanumériques qui commence par une lettre alphabétique et d'une longueur maximale de 32 caractères. Par la suite, vous pouvez faire référence à *addrobj* plutôt qu'à l'adresse IP numérique lorsque vous utilisez une sous-commande *ipadm* qui gère les adresses dans le système, telle que *ipadm show-addr* ou *ipadm delete-addr*.

**6 (Facultatif) Affichez des informations sur l'interface IP nouvellement configurée.**

Vous pouvez utiliser les commandes suivantes, en fonction des informations que vous souhaitez vérifier :

- Affichez l'état général de l'interface.

```
# ipadm show-if [interface]
```

Si vous ne spécifiez pas l'interface, les informations s'affichent pour toutes les interfaces du système.

- Affichez les informations relatives à l'adresse de l'interface.

```
# ipadm show-addr [addrobj]
```

Si vous ne spécifiez pas *addrobj*, les informations s'affichent pour tous les objets d'adresse dans le système.

Pour plus d'informations sur la sortie de la sous-commande `ipadm show-*`, reportez-vous à la section [“Contrôle d'interfaces et d'adresses IP” à la page 198](#).

**7 (Facultatif) Ajoutez des entrées pour les adresses IP dans le fichier `/etc/hosts` .**

Les entrées de ce fichier sont constituées d'adresses IP et des noms d'hôtes correspondants.

---

**Remarque** – Cette étape s'applique uniquement si vous configurez des adresses IP statiques qui utilisent les noms d'hôtes. Si vous configurez les adresses DHCP, vous n'avez pas besoin de mettre à jour le fichier `/etc/hosts`.

---

**Exemple 9–1 Configuration d'une interface réseau à l'aide d'une adresse statique**

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net3      Ethernet   up         100Mb      full        bge3

# dladm show-link
LINK      CLASS      MTU      STATE      BRIDGE      OVER
net3      phys       1500     up         --          --

# ipadm create-ip net3
# ipadm create-addr -T static -a 192.168.84.3/24 net3/v4static

# ipadm show-if
IFNAME    CLAS        STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3      ip         ok         yes         --

# ipadm show-addr
ADDROBJ    TYPE      STATE      ADDR
lo0/?      static    ok         127.0.0.1/8
net3/v4     static    ok         192.168.84.3/24
```

```
# vi /etc/hosts
# Internet host table
# 127.0.0.1      localhost
10.0.0.14       myhost
192.168.84.3    campus01
```

Notez que si campus01 est déjà défini dans le fichier /etc/hosts, vous pouvez utiliser ce nom d'hôte lors de l'attribution de l'adresse suivante :

```
# ipadm create-addr -T static -a campus01 net3/v4static
```

### Exemple 9-2 Configuration automatique d'une interface réseau à l'aide d'une adresse IP

Cet exemple utilise le même périphérique réseau que l'exemple précédent mais configure l'interface IP afin qu'elle reçoive son adresse à partir d'un serveur DHCP.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net3      Ethernet   up         100Mb      full        bge3

# dladm show-link
LINK      CLASS      MTU        STATE      BRIDGE      OVER
net3      phys       1500       up         --          --

# ipadm create-ip net3

# ipadm create-addr -T dhcp net3/dhcp

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3      ip         ok         yes         --

# ipadm show-addr net3/dhcp
ADDROBJ   TYPE      STATE      ADDR
net3/dhcp dhcp       ok         10.8.48.242/24

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/?     static    ok         127.0.0.1/8
net3/dhcp dhcp       ok         10.8.48.242/24
```

## Définition des propriétés des adresses IP

La commande `ipadm` permet de définir les propriétés spécifiques des adresses une fois ces dernières affectées aux interfaces. En définissant ces propriétés, vous pouvez déterminer les éléments suivants :

- La propriété `prefixlen` d'une adresse.
- Si une adresse IP peut être utilisée comme adresse source pour les paquets sortants.

- Si l'adresse appartient à une zone globale ou non globale.
- Si l'adresse est une adresse privée.

Pour dresser la liste des propriétés d'une adresse IP, utilisez la syntaxe suivante :

```
# ipadm show-addrprop [-p property] [addrobj]
```

Les informations affichées varient selon les options que vous utilisez.

- Si vous ne spécifiez pas de propriété ni d'objet d'adresse, toutes les propriétés de toutes les adresses existantes s'affichent alors.
- Si vous n'indiquez que la propriété, alors cette propriété s'affiche pour toutes les adresses.
- Si vous n'indiquez que l'objet d'adresse, toutes les propriétés de cet objet d'adresse sont alors affichées.

---

**Remarque** – Les propriétés d'adresse peuvent uniquement être définies séparément.

---

## ▼ Procédure de définition des propriétés d'une adresse IP

Cette procédure indique les principales étapes de configuration des propriétés d'une adresse IP.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 Affichez la liste des adresses IP en cours d'utilisation sur le système.

```
# ipadm show-addr
```

### 3 (Facultatif) Déterminez le paramètre actuel d'une propriété particulière d'une adresse IP que vous souhaitez modifier.

```
# ipadm show-addrprop -p property addrobj
```

Si vous ne connaissez pas la propriété, vous pouvez lancer une commande `ipadm show-addrprop` générale. Lorsque vous affichez les adresses IP à l'aide de cette commande, les adresses sont affichées avec les paramètres actuels de toutes leurs propriétés.

### 4 Définissez la propriété sélectionnée à la valeur souhaitée.

```
# ipadm set-addrprop -p property=value addrobj
```

### 5 Affichez le nouveau paramètre de la propriété.

```
# ipadm show-addrprop -p property addrobj
```

### Exemple 9-3 Définition de la propriété `prefixlen` d'une adresse

La propriété `prefixlen` fait référence au masque de réseau d'une adresse IP. L'exemple suivant modifie la longueur de la propriété `prefixlen` de l'adresse IP de `net3`. Dans cet exemple, l'option `-t` est utilisée pour créer une modification temporaire dans la propriété. Si le système est redémarré, la valeur de la propriété revient à sa valeur par défaut.

```
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/?        static    ok          127.0.0.1/8
net3/v4       static    ok          192.168.84.3/24

# ipadm show-addrprop -p prefixlen net3/v4
ADDROBJ  PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
net3/v4  prefixlen rw     24       24          24        1-30,32

# ipadm set-addrprop -t -p prefixlen=8 net3/v4
# ipadm show-addrprop -p prefixlen net3/v4
ADDROBJ  PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
net3/v4  prefixlen rw     8        24          24        1-30,32
```

## Définition des propriétés d'interfaces IP

Les interfaces IP, comme les liaisons de données, possèdent des propriétés que vous pouvez personnaliser pour vos paramètres réseau. Pour chaque interface, il existe deux ensembles de propriétés qui s'appliquent aux protocoles IPv4 et IPv6, respectivement. Certaines propriétés, comme MTU, sont communes aux liaisons de données et aux interfaces IP. Par conséquent, il est possible d'avoir un paramètre MTU pour une liaison de données et un autre paramètre MTU pour l'interface configurée sur cette liaison. De plus, vous pouvez avoir différents paramètres MTU qui s'appliquent aux paquets IPv4 et IPv6, respectivement, qui passent par l'interface IP.

La transmission IP est une propriété d'interface IP qui est généralement configurée dans les scénarios de mise en réseau. La procédure suivante indique les étapes.

### Activation de la transmission de paquets

Dans un réseau, un hôte peut recevoir des paquets de données destinés à un autre système hôte. En activant la transmission de paquets dans le système local de destination, ce système peut transmettre les paquets de données à l'hôte de destination. Par défaut, la transmission IP est désactivée. Les deux procédures suivantes décrivent l'activation de cette fonctionnalité. Dans les versions précédentes d'Oracle Solaris, la commande `routeadm` était utilisée pour activer la transmission de paquets. La syntaxe `ipadm` dans cette procédure remplace la commande `routeadm`.

Les points suivants vous aideront à déterminer s'il vaut mieux utiliser la procédure basée sur l'interface ou sur le protocole.

- Si vous souhaitez être sélectif dans la façon dont les paquets sont envoyés, activez la transmission de paquets dans l'interface. Par exemple, vous pouvez disposer d'un système doté de plusieurs cartes réseau. Certaines cartes d'interface réseau sont connectées au réseau externe, tandis que d'autres sont connectées au réseau privé. Par conséquent, il vaut mieux activer la transmission de paquets uniquement sur certaines interfaces, plutôt que sur toutes. Reportez-vous à la section [“Procédure d'activation de la transmission de paquets IP via la définition d'une propriété d'interface”](#) à la page 190.
- Pour implémenter la transmission de paquets dans l'ensemble du système, activez la propriété forwarding du protocole. Pour en savoir plus sur cette seconde méthode, reportez-vous à la section [“Procédure d'activation de la transmission de paquets via la définition de la propriété du protocole”](#) à la page 192.

---

**Remarque** – Les deux méthodes de transmission de paquets sont compatibles. Par exemple, vous pouvez activer la transmission de paquets à l'échelle globale, puis personnaliser la propriété forwarding pour chaque interface. Ainsi, la transmission de paquets peut toujours être sélective pour ce système particulier.

---

## ▼ **Procédure d'activation de la transmission de paquets IP via la définition d'une propriété d'interface**

Cette procédure montre comment activer la transmission de paquets IP de manière sélective en configurant la propriété de transmission IP sur des interfaces spécifiques.

---

**Remarque** – La transmission de paquets implique le protocole IP. Par conséquent, l'établissement d'une distinction entre les *versions du protocole* IP fait également partie de la procédure.

---

### **1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### **2 Affichez le paramètre actuel de la propriété de transmission IP d'une interface.**

```
# ipadm show-ifprop -p forwarding [-m protocol-version] interface
```

où *protocol-version* peut être `ipv4` ou `ipv6`. Si vous n'indiquez pas la version, les paramètres des protocoles IPv4 et IPv6 s'affichent.

**Remarque** – Pour afficher l'ensemble des propriétés de protocole valides d'une interface donnée, n'indiquez pas de propriété, comme suit :

```
# ipadm show-ifprop interface
```

Cette syntaxe est également présentée dans l'[Exemple 9–4](#).

- 3 Pour chaque interface sur laquelle vous souhaitez activer la transmission de paquets, saisissez la commande suivante :

```
# ipadm set-ifprop forwarding=on -m protocol-version interface
```

- 4 (Facultatif) Affichez les paramètres de la propriété **forwarding** d'une interface.

```
# ipadm show-ifprop -p forwarding interface
```

- 5 Pour restaurer la propriété **forwarding** d'une interface à ses paramètres par défaut, saisissez la commande suivante :

```
# ipadm reset-ifprop -p forwarding -m protocol-version interface
```

#### Exemple 9–4 Activation d'une interface afin qu'elle transmette uniquement les paquets IPv4

L'exemple suivant montre comment implémenter la transmission sélective des paquets, c'est-à-dire que la transmission de paquets IPv4 est uniquement activée dans l'interface `net0`. Dans les autres interfaces du système, la transmission de paquets est désactivée, ce qui correspond au paramètre par défaut.

```
# ipadm show-ifprop -p forwarding net0
```

IFNAME	PROPERTY	PROTO	PERM	CURRENT	PERSISTENT	DEFAULT	POSSIBLE
net0	forwarding	ipv4	rw	off	off	off	on,off
net0	forwarding	ipv6	rw	off	--	off	on,off

La syntaxe de commande `ipadm show-ifprop` qui utilise l'option `-p property` fournit uniquement des informations sur une propriété spécifique.

```
# ipadm set-ifprop -p forwarding=on -m ipv4 net0
# ipadm show-ifprop net0
```

IFNAME	PROPERTY	PROTO	PERM	CURRENT	PERSISTENT	DEFAULT	POSSIBLE
...							
net0	forwarding	ipv4	rw	on	on	off	on,off
...							

La syntaxe de commande `ipadm show-ifprop` sans l'option `-p property` affiche toutes les propriétés d'une interface et leurs paramètres.

```
# ipadm reset-ifprop -p forwarding -m ipv4 net0
# ipadm show-ifprop -p forwarding -m ipv4 net0
```

IFNAME	PROPERTY	PROTO	PERM	CURRENT	PERSISTENT	DEFAULT	POSSIBLE

```
net0      forwarding  ipv4    rw      off      off      off      on,off
```

La syntaxe de commande `ipadm reset -i fprop` réinitialise la propriété spécifiée aux paramètres par défaut.

## ▼ Procédure d'activation de la transmission de paquets via la définition de la propriété du protocole

Cette procédure montre comment activer la transmission de paquets dans l'ensemble du système.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Affichez le paramètre actuel de la propriété de transmission IP.

```
# ipadm show-prop -p forwarding protocol-version
```

où *protocol-version* peut être `ipv4` ou `ipv6`.

---

**Remarque** – Pour afficher toutes les propriétés réglables valides pour un protocole donné et leurs paramètres actuels, saisissez la commande suivante :

```
# ipadm show-prop protocol
```

où *protocol* peut être `ip`, `ipv4`, `ipv6`, `udp`, `tcp`, `icmp` et `sctp`.

Cette syntaxe est illustrée dans l'[Exemple 9–5](#).

---

### 3 Pour chaque version du protocole pour laquelle vous voulez activer la transmission, saisissez la commande suivante :

```
# ipadm set-prop forwarding=on protocol-version
```

### 4 (Facultatif) Affichez les paramètres de la propriété de transmission IP en effectuant l'une des opérations suivantes :

- Pour afficher toutes les propriétés et paramètres actuels d'un protocole, saisissez la commande suivante :  

```
# ipadm show-prop protocol
```
- Pour afficher une propriété spécifique d'un protocole, saisissez la commande suivante :  

```
# ipadm show-prop -p property protocol
```
- Pour afficher une propriété spécifique d'une version de protocole spécifique, saisissez la commande suivante :



```
# ipadm show-prop -p property protocol-version
```

- 5 Pour réinitialiser une propriété spécifique d'une version de protocole à sa valeur par défaut, saisissez la commande suivante :

```
# ipadm reset-prop -p property protocol-version
```

### Exemple 9–5 Activation de la transmission de paquets IPv4 et IPv6

L'exemple suivant est calqué sur l'exemple précédent illustrant la transmission des paquets sur des interfaces. Les deux utilisations de `ipadm show-prop` affichent les paramètres d'une propriété spécifiée ou toutes les propriétés d'un protocole et paramètres.

```
# ipadm show-prop -p forwarding ip
PROTO  PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4    forwarding rw    off      --          off      on,off
ipv6    forwarding rw    off      --          off      on,off
#
# ipadm set-prop -p forwarding=on ipv4
# ipadm set-prop -p forwarding=on ipv6
#
# ipadm show-prop ip
PROTO  PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4    forwarding rw    on        on          off      on,off
ipv4    ttl        rw    255      --          255      1-255
ipv6    forwarding rw    on        on          off      on,off
ipv6    hoplimit  rw    255      --          255      1-255#
```

## Administration de propriétés de protocole

Mises à part les interfaces, la commande `ipadm` peut être utilisée pour configurer des propriétés de protocole, également appelées paramètres réglables. La commande `ipadm` remplace la commande `ndd` qui était couramment utilisée dans les versions précédentes pour définir les paramètres réglables. Cette section présente des procédures et des exemples pour personnaliser les propriétés de protocole TCP/IP sélectionnées.

### Définition de propriétés TCP/IP

Les propriétés TCP/IP peuvent être basées sur une interface ou globales. Les propriétés peuvent être appliquées à une interface spécifique, ou au niveau global à toutes les interfaces de la zone. Les propriétés globales peuvent avoir des paramètres dans plusieurs zones non globales. Pour obtenir la liste des propriétés de protocole prises en charge, reportez-vous à la page de manuel [ipadm\(1M\)](#).

En règle générale, les paramètres par défaut du protocole Internet TCP/IP s'avèrent suffisants pour que le réseau fonctionne. Cependant, si les paramètres par défaut ne sont pas suffisants pour votre topologie de réseau, les procédures décrites dans le tableau suivant indiquent comment personnaliser ces propriétés TCP/IP.

Le tableau décrit les tâches de configuration de certaines propriétés du protocole et fournit des liens vers les procédures correspondantes.

TABLEAU 9-2 Définition des propriétés TCP/IP sélectionnées

Tâche	Description	Voir
Marquage d'un port privilégié.	Réserve un port de l'interface pour limiter son accès, sauf pour l'utilisateur root.	<a href="#">"Restriction de l'accès à un port à l'utilisateur root uniquement" à la page 194</a>
Personnalisation du comportement des paquets IP en cours de réception ou de transmission sur des hôtes multiréseau.	Personnalise le routage symétrique dans les hôtes multiréseau.	<a href="#">"Implémentation du routage symétrique sur des hôtes multiréseau" à la page 196</a>
Affichage d'informations relatives à une propriété d'un protocole.	Affiche une propriété du protocole et son paramètre actuel.	<a href="#">"Contrôle d'interfaces et d'adresses IP" à la page 198</a>

**Remarque** – Pour plus d'informations sur les procédures qui utilisent l'outil `ipadm` pour configurer les interfaces réseau et les adresses IP, reportez-vous à la section ["Configuration d'interfaces IP" à la page 183](#).

▼ **Restriction de l'accès à un port à l'utilisateur root uniquement**

Pour les protocoles de transport tels que TCP, UDP et SCTP, les ports 1–1023 sont par défaut les ports privilégiés auxquels seuls les processus qui s'exécutent avec des autorisations root peuvent être liés. En utilisant la commande `ipadm`, vous pouvez réserver un port au-delà de cette plage par défaut afin qu'il devienne un port privilégié. Ainsi, seuls les processus root peuvent être liés à ce port. Pour cette procédure, vous utilisez les propriétés de protocole de transport suivantes :

- `smallest_nonpriv_port`
- `extra_priv_ports`

**1 Déterminez si le port désigné se trouve dans la plage de ports standard et peut donc être utilisé.**

```
# ipadm show-prop -p smallest_nonpriv_port protocol
```

où *protocol* correspond au type de protocole pour lequel vous souhaitez configurer un port privilégié, tel que IP, UDP, ICMP, etc.

Dans la sortie de la commande, le champ POSSIBLE indique la plage de numéros de port auxquels les utilisateurs standard peuvent être liés. Si le port désigné se trouve dans cette plage, vous pouvez le définir en tant que port privilégié.

**2 Vérifiez si le port que vous souhaitez réserver est disponible et n'est pas déjà marqué comme un port privilégié.**

```
# ipadm show-prop -p extra_priv_ports protocol
```

Dans la sortie de la commande, le champ CURRENT indique les ports qui sont actuellement marqués comme privilégiés. Si le port désigné n'apparaît pas dans ce champ, vous pouvez le définir comme port privilégié.

**3 Ajoutez le port désigné en tant que port privilégié.**

```
# ipadm set-prop -p extra_priv_ports=port-number protocol
```

**4 Pour chaque port supplémentaire que vous voulez ajouter ou supprimer en tant que port privilégié, effectuez l'une des actions suivantes :**

- Pour ajouter un port en tant que port privilégié, saisissez la syntaxe suivante.

```
# ipadm set-prop -p extra_priv_ports+=portnumber protocol
```

---

**Remarque** – Avec le qualificatif plus (+), vous pouvez sélectionner plusieurs ports pour qu'ils deviennent des ports privilégiés. Le qualificatif plus (+) vous permet d'établir une liste de ces ports. Utilisez cette syntaxe avec le qualificatif pour ajouter des ports à la liste séparément. Si vous n'utilisez pas le qualificatif, le port que vous affectez remplace tous les autres ports qui ont été précédemment répertoriés comme privilégiés.

---

- Pour supprimer un port de la liste des ports privilégiés, saisissez la syntaxe suivante.

```
# ipadm set-prop -p extra_priv_ports-=portnumber protocol
```

---

**Remarque** – En utilisant le qualificatif moins (-), vous pouvez supprimer le port de la liste des ports existants actuellement répertoriés comme privilégiés. Utilisez la même syntaxe pour supprimer tous les ports privilégiés supplémentaires, y compris les ports par défaut.

---

**5 Vérifiez le nouveau statut du port désigné.**

```
# ipadm show-prop -p extra_priv_ports protocol
```

Dans la sortie de la commande, assurez-vous que les ports désignés sont désormais inclus dans le champ CURRENT.

## Exemple 9–6 Définition d'un port privilégié

Dans cet exemple, vous définissez les ports 3001 et 3050 comme ports privilégiés. Vous pouvez également supprimer le port 4045, actuellement répertorié comme port privilégié.

Dans la sortie pour la propriété `smallest_nonpriv_port`, le champ `POSSIBLE` indique que le port 1024 est le port non privilégié le plus bas et que les ports 3001 et 3050 désignés se trouvent dans la plage des ports privilégiés à utiliser. Dans la sortie pour la propriété `extra_priv_ports`, les ports 2049 et 4045 sous le champ `CURRENT` sont marqués comme privilégiés. Vous pouvez ainsi procéder à la configuration du port 3001 en tant que port privilégié.

```
# ipadm show-prop -p smallest_nonpriv_port tcp
PROTO PROPERTY      PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp    smallest_nonpriv_port  rw    1024    --          1024     1024-32768

# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY      PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp    extra_priv_ports  rw    2049,4045  --          2049,4045  1-65535

# ipadm set-prop -p extra_priv_ports+=3001 tcp
# ipadm set-prop -p extra_priv_ports+=3050 tcp
# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY      PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp    extra_priv_ports  rw    2049,4045  3001,3050  2049,4045  1-65535
                                     3001,3050

# ipadm set-prop -p extra_priv_ports-=4045 tcp
# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY      PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp    extra_priv_ports  rw    2049,3001  3001,3050  2049,4045  1-65535
                                     3050
```

## ▼ Implémentation du routage symétrique sur des hôtes multiréseau

Par défaut, un système disposant de plusieurs interfaces, également appelé *hôte multiréseau*, achemine son trafic réseau en fonction de la route la plus longue vers la destination du trafic dans la table de routage. Si plusieurs routes de longueur égale vers la destination existent, Oracle Solaris applique les algorithmes de multipathing à coût égal pour répartir le trafic sur ces routes.

Répartir le trafic de cette manière n'est pas toujours idéal. Un paquet IP peut être envoyé par le biais d'une interface sur l'hôte multiréseau qui ne se trouve pas sur le même sous-réseau que l'adresse IP source dans le paquet. De plus, si le paquet sortant est une réponse à une certaine demande entrante, par exemple une requête d'écho ICMP, la requête et la réponse peuvent ne pas traverser la même interface. Une telle configuration du routage du trafic est appelée routage asymétrique. Si votre fournisseur d'accès Internet implémente un filtrage d'entrée tel que décrit dans la norme RFC 3704 (<http://rfc-editor.org/rfc/bcp/bcp84.txt>), une configuration de routage asymétrique peut entraîner la suppression d'un paquet sortant par le fournisseur.

Cette norme vise à limiter les attaques par déni de service sur Internet. Pour s'y conformer, le réseau doit être configuré pour un routage symétrique. Dans Oracle Solaris, la propriété

hostmodel IP permet de répondre à cette exigence. Cette propriété contrôle le comportement des paquets IP reçus ou transmis via un hôte multiréseau.

La procédure suivante montre comment utiliser la commande `ipadm` pour définir la propriété `hostmodel` pour une configuration de routage spécifique :

- 1 Sur l'hôte multiréseau, devenez administrateur.
- 2 Configurez le routage des paquets réseau dans le système.

```
# ipadm set-prop -p hostmodel=value protocol
```

La propriété peut être définie sur l'un des trois paramètres suivants :

strong	Correspond au modèle de système final fort, tel que défini dans la norme RFC 1122. Ce paramètre implémente le routage symétrique.
weak	Correspond au modèle de système final faible tel que défini dans la norme RFC 1122. Avec ce paramètre, un hôte multiréseau utilise le routage asymétrique.
src-priority	Configure le routage de paquets en utilisant des routes préférées. Si plusieurs routes vers la destination existent dans la table de routage, les routes préférées sont celles qui utilisent les interfaces sur lesquelles l'adresse IP source d'un paquet sortant est configurée. Si de telles routes n'existent pas, les paquets sortants utiliseront la route correspondante la plus longue vers la destination IP du paquet.

- 3 (Facultatif) Vérifiez les paramètres de la propriété `hostmodel`.

```
# ipadm show-prop protocol
```

**Exemple 9–7** Définition du routage symétrique sur un hôte multiréseau

Dans cet exemple, vous souhaitez appliquer le routage symétrique de l'ensemble du trafic IP sur tous les hôtes multiréseau.

```
# ipadm set-prop -p hostmodel=strong ip
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv6    hostmodel  rw    strong   --          weak     strong,
src-priority,
weak
ipv4    hostmodel  rw    strong   --          weak     strong,
src-priority,
weak
```

## Contrôle d'interfaces et d'adresses IP

La commande `ipadm` est également l'outil préféré pour contrôler et obtenir des informations sur les interfaces IP et leurs propriétés ou paramètres. Les sous-commandes `ipadm`, pour obtenir des informations relatives aux interfaces, utilisent la syntaxe de base suivante :

**`ipadm show-*`** [*other-arguments*] [*interface*]

- Pour obtenir des informations sur les interfaces, utilisez `ipadm show-if`.
- Pour obtenir des informations sur les adresses, utilisez `ipadm show-addr`.
- Pour obtenir des informations sur une propriété d'interface spécifique, utilisez `ipadm show-ifprop`.
- Pour obtenir des informations sur une propriété d'adresse spécifique, utilisez `ipadm show-addrprop`.

Cette section propose plusieurs exemples d'utilisation de la commande `ipadm` pour obtenir des informations sur les interfaces réseau. Pour d'autres types de contrôle des tâches que vous effectuez sur le réseau, reportez-vous au [Chapitre 5, “Administration d’un réseau TCP/IP” du manuel \*Administration d’Oracle Solaris : Services IP\*](#).

---

**Remarque** – Pour obtenir une explication sur tous les champs dans les commandes `ipadm show-*`, reportez-vous à la page de manuel [ipadm\(1M\)](#).

---

### ▼ Procédure d'obtention d'informations sur les interfaces réseau

Cette procédure décrit la manière d'afficher plus d'informations sur l'état général, les informations d'adresse ou les propriétés IP d'une interface.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d’Oracle Solaris : services de sécurité*.

#### 2 Pour obtenir des informations sur l'état d'une interface, tapez la commande suivante :

**# `ipadm show-if`** [*interface*]

Si vous ne spécifiez pas une interface, l'information couvre toutes les interfaces du système.

Les champs de la sortie de la commande font référence à ce qui suit :

**IFNAME**      Désigne l'interface dont les informations sont affichées.

**CLASS**      Désigne la classe d'interface, qui peut être une des quatre suivantes :

	<ul style="list-style-type: none"> <li>▪ <code>ip</code> fait référence à une interface IP</li> <li>▪ <code>ipmp</code> fait référence à une interface IPMP</li> <li>▪ <code>vni</code> fait référence à une interface virtuelle</li> <li>▪ <code>loopback</code> fait référence à une interface de loopback, qui est automatiquement créée. À l'exception de l'interface de loopback, vous pouvez créer manuellement les 3 autres classes d'interface.</li> </ul>
STATE	<p>Fait référence à l'état de l'interface, qui peut être <code>ok</code>, <code>offline</code>, <code>failed</code>, <code>down</code> ou <code>disabled</code>.</p> <p>L'état <code>failed</code> s'applique aux groupes IPMP et peut faire référence à une liaison de données ou une interface IP qui est arrêtée et ne peut pas héberger le trafic. Si l'interface IP appartient à un groupe IPMP, alors l'interface IPMP peut continuer à recevoir et envoyer le trafic à l'aide d'autres interfaces IP actives dans le groupe.</p> <p>L'état <code>down</code> fait référence à une interface IP qui est mise hors ligne par l'administrateur.</p> <p>L'état <code>disabled</code> fait référence à l'interface IP qui est démontée à l'aide de la commande <code>ipadm disable-if</code>.</p>
ACTIVE	Indique si l'interface est utilisée pour héberger le trafic et est défini sur <code>yes</code> ou <code>no</code> .
OVER	S'applique uniquement à la classe IPMP d'interfaces et fait référence aux interfaces sous-jacentes qui constituent l'interface ou le groupe IPMP.

### 3 Pour obtenir des informations sur l'adresse d'une interface, tapez la commande suivante :

```
# ipadm show-addr [addrobj]
```

Si vous ne spécifiez pas d'identificateur d'adresse, les informations d'adresse sont fournies pour tous les identificateurs d'adresse sur le système.

Les champs de la sortie de la commande font référence à ce qui suit :

ADDROBJ	Spécifie l'objet d'adresse dont l'adresse est répertoriée.
TYPE	Indique si l'adresse IP est <code>static</code> , <code>dhcp</code> ou <code>addrconf</code> . Le paramètre <code>addrconf</code> indique que l'adresse a été obtenue en utilisant la configuration d'adresse sans état ou avec état.
STATE	Décrit l'objet d'adresse dans la configuration active actuelle. Pour obtenir la liste complète de ces valeurs, reportez-vous à la page de manuel <a href="#">ipadm(1M)</a> .
ADDR	Spécifie l'adresse IP qui est configurée sur l'interface. L'adresse peut être IPv4 ou IPv6. Une interface de tunnel affiche les deux adresses locales et distantes.

Pour plus d'informations sur les tunnels, reportez-vous au [Chapitre 6](#), “Configuration de tunnels IP” du manuel *Administration d'Oracle Solaris* :

*Services IP.***4 Pour obtenir des informations sur les propriétés d'interfaces, tapez la commande suivante :**

```
# ipadm show-ifprop [-p property] interface
```

Si vous ne spécifiez pas une propriété, toutes les propriétés et leurs paramètres sont affichés.

Les champs de la sortie de la commande font référence à ce qui suit :

IFNAME	Désigne l'interface dont les informations sont affichées.
PROPERTY	Fait référence à la propriété de l'interface. Une interface peut avoir plusieurs propriétés.
PROTO	Fait référence au protocole auquel la propriété s'applique et qui peut être IPv4 ou IPv6.
PERM	Fait référence aux permissions autorisées d'une propriété donnée, qui peuvent être en lecture seule, en écriture seule ou les deux.
CURRENT	Indique le paramètre actuel de la propriété de la configuration active.
PERSISTENT	Fait référence au paramètre de la propriété qui est réappliqué lorsque le système est réinitialisé.
DEFAULT	Indique le paramètre par défaut de la propriété spécifiée.
POSSIBLE	Fait référence à une liste de valeurs qui peuvent être affectées à la propriété spécifiée. Pour les paramètres numériques, une plage de valeurs acceptables s'affiche.

---

**Remarque** – Si une valeur de champ est inconnue, comme lorsqu'une interface ne prend pas en charge la propriété dont les informations sont demandées, le paramètre s'affiche sous la forme d'un point d'interrogation (?).

---

**5 Pour obtenir des informations sur une propriété d'adresse, saisissez la commande suivante :**

```
# ipadm show-addrprop [-p property, ...] [addrobj]
```

Les informations affichées varient selon les options que vous utilisez.

- Si vous ne spécifiez pas une propriété, toutes les propriétés sont répertoriées.
- Si vous n'indiquez que la propriété, alors cette propriété s'affiche pour toutes les adresses.
- Si vous n'indiquez que l'objet d'adresse, les propriétés de toutes les adresses existantes sur le système s'affichent.

Les champs de la sortie de la commande font référence à ce qui suit :

ADDROBJ            Fait référence à l'objet d'adresse dont les propriétés sont répertoriées.



PROPERTY	Fait référence à la propriété de l'objet d'adresse. Un objet d'adresse peut avoir plusieurs propriétés.
PERM	Fait référence aux permissions autorisées d'une propriété donnée, qui peuvent être en lecture seule, en écriture seule ou les deux.
CURRENT	Fait référence au paramètre actuel de la propriété dans la configuration actuelle.
PERSISTENT	Fait référence au paramètre de la propriété qui est réappliqué lorsque le système est réinitialisé.
DEFAULT	Indique le paramètre par défaut de la propriété spécifiée.
POSSIBLE	Fait référence à une liste de paramètres qui peuvent être affectés à la propriété spécifiée. Pour les paramètres numériques, une plage de valeurs acceptables s'affiche.

**Exemple 9–8** Utilisation de la commande ipadm pour contrôler des interfaces

Cet ensemble d'exemples montre les types d'informations qui peuvent être obtenues à l'aide des sous-commandes `ipadm show-*`. Tout d'abord, les informations générales d'interface s'affichent. Ensuite, les informations d'adresse sont fournies. Enfin, les informations sur une propriété spécifique, le MTU de l'interface `net1`, sont fournies. Les exemples incluent des interfaces de tunnel ainsi que des interfaces qui utilisent un nom personnalisé.

```
# ipadm show-if
IFNAME      CLASS      STATE      ACTIVE      OVER
lo0          loopback   ok         yes         --
net0         ip         ok         yes         --
net1         ip         ok         yes         --
tun0         ip         ok         yes         --

# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/?        static    ok         127.0.0.1/8
net0/v4       static    ok         192.168.84.3/24
tun0/v4tunaddr static    ok         173.129.134.1-->173.129.134.2
```

Notez qu'un objet d'adresse est répertorié comme *interface/?* indique que l'adresse a été configurée sur l'interface par une application qui n'utilisait pas l'API `libipadm`. De telles applications ne sont pas sous le contrôle de la commande `ipadm` qui nécessite que le nom de l'objet d'adresse utilise le format *interface/ user-defined-string*. Pour des exemples de attribution d'adresses IP, reportez-vous à la section “[Configuration d'une interface IP](#)” à la page 183.

```
# ipadm show-ifprop -p mtu net1
IFNAME  PROPERTY  PROTO  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
net1    mtu       ipv4   rw    1500     --          1500     68-1500
net1    mtu       ipv6   rw    1500     --          1500     1280-1500
```

```
# ipadm show-addrprop net1/v4
ADDROBJ      PROPERTY  PERM  CURRENT      PERSISTENT  DEFAULT      POSSIBLE
net1/v4      broadcast r-    192.168.84.255 --          192.168.84.255 --
net1/v4      deprecated rw    off         --          off          on,off
net1/v4      prefixlen rw    24         24          24          1-30,32
net1/v4      private  rw    off         --          off          on,off
net1/v4      transmit rw    on         --          on           on,off
net1/v4      zone     rw    global      --          global       --
```

## Dépannage de la configuration de l'interface

Cette section traite des problèmes courants que vous pouvez rencontrer lors de l'utilisation de la commande `ipadm` pour configurer les interfaces IP.

### La commande `ipadm` ne fonctionne pas.

La configuration manuelle de l'interface IP avec les commandes `dladm` et `ipadm` fonctionne uniquement sur les profils de configuration réseau (NCP) de type fixe, tels que `DefaultFixed`. Si le NCP actif dans le système est un profil de type automatique, vous devez passer à un profil de type fixe avant d'utiliser les commandes `dladm` et `ipadm`.

```
# netadm list
TYPE  PROFILE      STATE
ncp   DefaultFixed disabled
ncp   Automatic    online
loc   Automatic    offline
loc   NoNet        offline
...

# netadm enable -p ncp defaultfixed
```

### L'adresse IP ne peut pas être affectée à la commande `ipadm create-addr`.

Avec la commande `ifconfig` classique, vous pouvez monter et affecter une adresse IP à l'aide d'une seule syntaxe commande. Lorsque vous utilisez la commande `ipadm create-addr` pour configurer une adresse IP, vous devez d'abord créer l'interface IP à l'aide d'une commande distincte.

```
# ipadm create-ip interface
# ipadm create-addr -T addr-type -a address addrobj
```

## Le message cannot create address object: Invalid argument provided s'affiche pendant la configuration de l'adresse IP.

L'objet d'adresse identifie une adresse IP spécifique liée à une interface IP. L'objet d'adresse est un identifiant unique pour chaque adresse IP sur l'interface IP. Vous devez spécifier un autre objet d'adresse pour identifier une deuxième adresse IP que vous souhaitez assigner à la même interface IP. Si vous souhaitez utiliser le même nom d'objet d'adresse, vous devez supprimer la première instance de l'objet d'adresse avant de l'assigner pour identifier une adresse IP différente.

```
# ipadm show-addr
ADDROBJ   TYPE      STATE    ADR
lo0        static    ok       127.0.0.1/10
net0/v4    static    ok       192.168.10.1

# ipadm create-addr -T static -a 192.168.10.5 net0/v4b

ou
```

```
# ipadm show-addr
ADDROBJ   TYPE      STATE    ADR
lo0        static    ok       127.0.0.1/10
net0/v4    static    ok       192.168.10.1

# ipadm delete-addr net0/v4
# ipadm create-addr -T static -a 192.168.10.5 net0/v4
```

## Message cannot create address: Persistent operation on temporary object lors de la configuration d'interface IP

La commande `ipadm` crée une configuration persistante. Si l'interface IP que vous configurez a été créée en tant qu'interface temporaire, vous ne pouvez pas utiliser la commande `ipadm` pour configurer des paramètres persistants sur l'interface. Après avoir vérifié qu'une interface que vous êtes en train de configurer est temporaire, supprimez cette interface, créez-la à nouveau en tant qu'objet persistant, puis reprenez la configuration.

```
# ipadm show-if -o all
IFNAME    CLASS    STATE    ACTIVE    CURRENT          PERSISTENT    OVER
lo0        loopback ok        yes       -m46-v-----    46--          --
net0       ip        ok        yes       bm4-----      ----          --
```

L'absence de l'indicateur 4 pour la configuration IPv4 ou de l'indicateur 6 pour la configuration IPv6 sur le champ `PERSISTENT` indique que `net0` a été créée en tant qu'interface temporaire.

```
# ipadm delete-ip net0
# ipadm create-ip net0
# # ipadm create-addr -T static -a 192.168.1.10 net0/v4
```

# Tableaux de comparaison : commande ipadm et autres commandes réseau

La commande ipadm est l'outil préféré à utiliser pour toutes les tâches de configuration sur les interfaces IP. Cette commande remplace les commandes des versions précédentes qui étaient utilisées pour la configuration réseau, telles que les commandes ifconfig et ndd. Les tableaux ci-dessous répertorient les options de commandes sélectionnées de ces outils précédents et leurs équivalents dans la commande ipadm.

**Remarque** – Ces tableaux ne fournissent pas une liste complète des options ipadm. Pour obtenir une liste complète, reportez-vous à la page de manuel [ipadm\(1M\)](#).

## Options des commandes ifconfig et ipadm

Le tableau suivant présente les options de la commande ifconfig et les sous-commandes ipadm équivalentes correspondantes.

TABLEAU 9-3 Mappage de syntaxe entre les commandes ifconfig et ipadm

Commande ifconfig	Commande ipadm
plumb/unplumb	ipadm create-ip ipadm create-vni ipadm create-ipp ipadm enable-addr ipadm delete-ip ipadm delete-vni ipadm delete-ipp ipadm disable-addr

TABLEAU 9-3 Mappage de syntaxe entre les commandes ifconfig et ipadm (Suite)

Commande ifconfig	Commande ipadm
[address[/prefix-length] [dest-address]] [addif address[ prefix-length]] [removeif address[ prefix-length]][netmask mask][destination dest-address]{auto-dhcp dhcp}[primary][wait seconds]extend   release   start	ipadm create-addr -T static ipadm create-addr -T dhcp ipadm create-addr -T addrconf  ipadm show-addr  ipadm delete-addr  ipadm refresh-addr
[deprecated   -deprecated] [preferred   -preferred] [private   -private] [zone zonename   -zones   -all-zones][xmit   -xmit]	ipadm set-addprop ipadm reset-addprop  ipadm show-addprop
up	ipadm up-addr
down	ipadm down-addr
[metric n] [mtu n] [nud   -nud] [arp   -arp] [usesrc [name   none] [router   -router]	ipadm set-ifprop  ipadm show-ifprop  ipadm reset-ifprop
[ipmp] [group [name   ""]] standby   -standby] [failover   -failover]	ipadm create-ipmp  ipadm delete-ipmp  ipadm add-ipmp  ipadm remove-ipmp  ipadm set-ifprop -p [standby] [group]
[tdest tunnel-dest-addr] [tsrc tunnel-srcs-addr] [encaplimit n  -encaplimit] [thoplimit n]	Ensemble de commandes dladm *-iptun. Pour plus de détails, reportez-vous à la page de manuel <a href="#">dladm(1M)</a> et à la section “ <a href="#">Configuration et administration du tunnel avec la commande dladm</a> ” du manuel <i>Administration d’Oracle Solaris : Services IP</i> .
[auth_algs authentication algorithm] [encr_algs encryption algorithm] [encr_auth_algs encryption authentication algorithm]	ipseccnf  Pour plus détails, reportez-vous à la page de manuel <a href="#">ipseccnf(1M)</a> et au Chapitre 15, “ <a href="#">Configuration d’IPsec (tâches)</a> ” du manuel <i>Administration d’Oracle Solaris : Services IP</i> .

TABLEAU 9-3 Mappage de syntaxe entre les commandes ifconfig et ipadm (Suite)

Commande ifconfig	Commande ipadm
[auth_revarp] [ether <i>address</i> ] [index <i>if-index</i> ] [subnet <i>subnet-address</i> ] [broadcast <i>broadcast-address</i> ] [token <i>address /prefix-length</i> ]  options dhcp – inform, ping, release, status, drop	Sous-commandes équivalentes actuellement indisponibles.
modlist] [modinsert <i>mod_name@ pos</i> ] [modremove <i>mod_name@pos</i> ]	Sous-commandes équivalentes actuellement indisponibles.

## Options des commandes ndd et ipadm

Le tableau suivant présente les options de la commande ndd et les sous-commandes ipadm équivalentes correspondantes.

TABLEAU 9-4 Mappage de syntaxe entre les commandes ndd et ipadm

Commande ndd	Commande ipadm
Récupération des propriétés	

TABLEAU 9-4 Mappage de syntaxe entre les commandes ndd et ipadm (Suite)

Commande ndd	Commande ipadm
<pre>bash-3.2# ndd -get /dev/ip ? ip_def_ttl      (read and write) ip6_def_hops    (read and write) ip_forward_directed_broadcasts                 (read and write) ip_forwarding   (read and write) ... ...</pre>	<pre>bash-3.2# ipadm show-prop ip PROTO PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE ipv4  forwarding  rw    off      --          off      on,off ipv4  ttl          rw    255     --          255     1-255 ipv6  forwarding  rw    off      --          off      on,off ipv6  hoplimit    rw    255     --          255     1-255 ...</pre>
<pre>bash-3.2# ndd -get /dev/ip \ ip_def_ttl 100 bash-3.2# ndd -get /dev/ip \ ip6_def_hops 255</pre>	<pre>bash-3.2# ipadm show-prop -p ttl,hoplimit ip PROTO PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE ipv4  ttl          rw    255     --          255     1-255 ipv6  hoplimit    rw    255     --          255     1-255</pre>
<pre>bash-3.2# ndd -get /dev/tcp ? tcp_cwnd_max    (read and write) tcp_strong_iss  (read and write) tcp_time_wait_interval                 (read and write) tcp_tstamp_always (read and write) tcp_tstamp_if_wscale                 (read and write) ... ...</pre>	<pre>bash-3.2# ipadm show-prop tcp PROTO PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE tcp  ecn          rw    passive --          passive  never,passive,                 active tcp  extra_      rw    2049    2049,4045  2049,4045  1-65535       priv_ports tcp  largest_    rw    65535   --          65535     1024-65535       anon_port tcp  recv_       rw    128000  --          128000    2048-1073741824       maxbuf tcp  sack        rw    active  --          active     never,passive,                 active tcp  send_       rw    49152   --          49152     4096-1073741824       maxbuf tcp  smallest_   rw    32768   --          32768     1024-65535       anon_port tcp  smallest_   rw    1024    --          1024      1024-32768       nonpriv_port ... ... ...</pre>
<pre>bash-3.2# ndd -get /dev/tcp ecn 1 bash-3.2# ndd -get /dev/tcp sack 2</pre>	<pre>bash-3.2# ipadm show-prop -p ecn,sack tcp PROTO PROPERTY  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE tcp  ecn          rw    passive --          passive  never,passive,active tcp  sack        rw    active  --          active     never,passive,active</pre>
Définition des propriétés	

TABLEAU 9-4 Mappage de syntaxe entre les commandes nnd et ipadm (Suite)

Commande nnd	Commande ipadm
bash-3.2# nnd -set /dev/ip \ ip_def_ttl 64	bash-3.2# ipadm set-prop -p ttl=64 ipv4
bash-3.2# nnd -get /dev/ip \ ip_def_ttl 64	bash-3.2# ipadm show-prop -p ttl ip PROTO PROPERTY FAMILY PERM VALUE DEFAULT POSSIBLE ip ttl inet rw 64 255 1-255 PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE ipv4 ttl rw 64 64 255 1-255
	bash-3.2# ipadm reset-prop -p ttl ip
	bash-3.2# ipadm show-prop -p ttl ip PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE ipv4 ttl rw 255 255 255 1-255



## Configuration des communications via une interface sans fil sur Oracle Solaris

---

Ce chapitre explique comment configurer et utiliser les communications via l'interface sans fil sur un ordinateur portable exécutant Oracle Solaris. Il comprend les rubriques suivantes :

- Communication par le biais d'interfaces Wi-Fi
- Recherche de réseau Wi-Fi
- Connexion et utilisation du Wi-Fi sur des systèmes Oracle Solaris
- Communications Wi-Fi sécurisées

### Liste des tâches des communications Wi-Fi

Tâche	Description	Voir
Planification des communications Wi-Fi sur votre système	Paramètre votre ordinateur portable ou votre configuration réseau sans fil, en incluant éventuellement un routeur, à un emplacement qui prend en charge le Wi-Fi.	<a href="#">“Procédure de préparation d'un système pour les communications Wi-Fi” à la page 211</a>
Connexion à un réseau Wi-Fi	Configure et établit la communication avec un réseau Wi-Fi.	<a href="#">“Connexion à un réseau Wi-Fi” à la page 212</a>
Contrôle des communications sur le lien Wi-Fi	Utilise les outils de mise en réseau Oracle Solaris standard pour vérifier l'état du lien Wi-Fi.	<a href="#">“Contrôle du lien Wi-Fi” à la page 216</a>
Etablissement d'une communication Wi-Fi sécurisée	Crée une clé WEP et l'utilise pour établir une connexion à un réseau Wi-Fi sécurisé.	<a href="#">“Configuration d'une connexion chiffrée à un réseau Wi-Fi” à la page 218</a>

## Communication par le biais d'interfaces Wi-Fi

Les normes IEEE 802.11 définissent les communications sans fil pour les réseaux locaux. Ces normes et les réseaux qu'elles décrivent sont appelés collectivement *Wi-Fi*, un terme déposé par le consortium Wi-Fi Alliance. Les réseaux Wi-Fi sont relativement faciles à configurer par les fournisseurs et les clients potentiels. Par conséquent, ils sont de plus en plus populaires et couramment utilisés dans le monde entier. Les réseaux Wi-Fi utilisent la même technologie d'ondes radio que les téléphones portables, les téléviseurs et les radios.

Oracle Solaris contient des fonctionnalités qui vous permettent de configurer un système en tant que client Wi-Fi. Cette section explique comment utiliser les options de connectivité Wi-Fi de la commande `dladm` pour connecter un ordinateur portable ou un ordinateur personnel à un réseau Wi-Fi local.

---

**Remarque** – Oracle Solaris ne contient pas de fonctions pour la configuration de serveurs Wi-Fi ou de points d'accès.

---

## Recherche de réseau Wi-Fi

Les réseaux Wi-Fi appartiennent en règle générale aux variétés suivantes :

- réseaux Wi-Fi disponibles dans le commerce ;
- réseaux Wi-Fi municipaux ;
- réseaux Wi-Fi privés.

Un emplacement doté d'une connexion Wi-Fi est appelé *point actif*. Chaque point actif inclut un point d'accès. Le *point d'accès* est un routeur avec une connexion "filaire" à Internet, par exemple, Ethernet ou ADSL. La connexion à Internet s'effectue généralement par le biais d'un fournisseur de services Internet sans fil ou d'un FAI classique.

## Réseaux Wi-Fi commerciaux

De nombreux hôtels et cafés offrent des connexions Internet sans fil en tant que service à leur clients possédant un ordinateur portable. Ces points actifs commerciaux sont situés au sein de leurs installations. Il s'agit de routeurs avec connexions câblées à un fournisseur d'accès Internet sans fil qui sert les emplacements commerciaux. Les fournisseurs d'accès Internet sans fil courants incluent des fournisseurs indépendants et les fournisseurs de services de téléphonie mobile aux entreprises.

Vous pouvez utiliser un ordinateur portable qui exécute Oracle Solaris pour vous connecter à un réseau Wi-Fi proposé par un hôtel ou autre point actif commercial. Demandez des instructions au point actif afin de vous connecter au réseau Wi-Fi. En règle générale, le processus de connexion implique la fourniture d'une clé à un navigateur que vous lancez lors de la connexion. Il se peut que l'accès au réseau de l'hôtel ou du fournisseur d'accès Internet sans fil soit payant.

Les lieux commerciaux dotés de points actifs en font généralement la publicité auprès de leurs clients. Vous pouvez également localiser la liste des points actifs à partir de différents sites Web, notamment [Wi-FiHotSpotList.com](http://www.wi-fihotspotlist.com) (<http://www.wi-fihotspotlist.com>).

## Réseaux Wi-Fi municipaux

Des villes du monde entier ont mis en place des réseaux Wi-Fi municipaux gratuits auxquels leurs citoyens peuvent accéder à partir de systèmes installés à leurs domiciles. Le Wi-Fi municipal utilise des émetteurs radio sur des pylônes téléphoniques ou autres lieux en extérieur pour former une "trame" au-dessus de la zone desservie par le réseau. Ces émetteurs sont les points d'accès au réseau Wi-Fi municipal. Si votre domaine est desservi par un réseau Wi-Fi municipal, votre domicile peut être inclus dans la trame du réseau.

L'accès au Wi-Fi municipal est généralement gratuit. Vous pouvez accéder au réseau municipal à partir d'un ordinateur portable équipé correctement ou d'un ordinateur personnel qui exécute Oracle Solaris. Un routeur personnel n'est pas nécessaire pour accéder au réseau municipal à partir de votre système. Toutefois, la configuration d'un routeur personnel est recommandée pour les zones où le signal du réseau municipal est faible. Les routeurs personnels sont également recommandés si vous avez besoin de sécuriser les connexions sur le réseau Wi-Fi. Pour plus d'informations, reportez-vous à la section "[Communications Wi-Fi sécurisées](#)" à la page 218.

## Réseaux Wi-Fi privés

Les réseaux Wi-Fi étant relativement faciles à configurer, les entreprises et les universités privées utilisent de réseaux Wi-Fi avec un accès limité aux employés ou aux étudiants. Les réseaux Wi-Fi privés requièrent généralement l'entrée d'une clé lors de la connexion ou l'exécution d'un VPN sécurisé une fois la connexion établie. Vous devez disposer d'un ordinateur portable ou PC équipé correctement qui exécute Oracle Solaris et de l'autorisation d'utiliser les fonctions de sécurité afin de vous connecter au réseau privé.

# Planification des communications Wi-Fi

Avant de pouvoir connecter votre système à un réseau Wi-Fi, procédez comme suit.

## ▼ Procédure de préparation d'un système pour les communications Wi-Fi

### 1 Equipez votre système avec une interface Wi-Fi prise en charge.

Votre système doit disposer d'une carte Wi-Fi prise en charge par Oracle Solaris, par exemple, de cartes qui prennent en charge les jeux de puces Atheros. Pour obtenir la liste actuelle des pilotes et jeux de puces pris en charge, reportez-vous à la page [Wireless Networking for OpenSolaris](http://hub.opensolaris.org/bin/view/Community+Group+laptop/wireless) (<http://hub.opensolaris.org/bin/view/Community+Group+laptop/wireless>).

Si l'interface n'est pas déjà présente sur le système, suivez les instructions du fabricant pour l'installation de la carte d'interface. Vous pouvez configurer le logiciel de l'interface au cours de la procédure [“Connexion à un réseau Wi-Fi”](#) à la page 212.

**2 Localisez l'emplacement de votre système dans un endroit qui est desservi par un réseau Wi-Fi commercial, municipal ou privé.**

Votre système doit être près d'un point d'accès au réseau, ce qui n'est normalement pas un élément à prendre en compte s'il s'agit d'un point actif commercial ou privé. Cependant, si vous prévoyez d'utiliser un réseau municipal gratuit, votre emplacement doit être proche de l'émetteur du point d'accès.

**3 (Facultatif) Configurez un routeur sans fil qui fera office de point d'accès supplémentaire.**

Configurez votre propre routeur si aucun réseau Wi-Fi n'est disponible à votre emplacement. Par exemple, si vous avez une ligne ADSL, connectez le routeur sans fil au routeur ADSL. Ensuite, le routeur sans fil devient le point d'accès pour vos périphériques sans fil.

# Connexion et utilisation du Wi-Fi sur des systèmes Oracle Solaris

Cette section présente des tâches permettant d'établir et de contrôler les connexions Wi-Fi d'un ordinateur portable ou un d'ordinateur de bureau exécutant Oracle Solaris.

## ▼ Connexion à un réseau Wi-Fi

**Avant de commencer**

La procédure suivante suppose que vous avez suivi les instructions de la section [“Procédure de préparation d'un système pour les communications Wi-Fi”](#) à la page 211.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Vérifiez la présence de liens disponibles.**

```
# dladm show-link
LINK      CLASS  MTU   STATE  BRIDGE  OVER
ath0      phys   1500  up     --      --
e1000g0    phys   1500  up     --      --
```

Dans cet exemple, la sortie indique que deux liens sont disponibles. Le lien `ath0` prend en charge les communications Wi-Fi. Le lien `e1000g0` sert à connecter le système à un réseau câblé.

**3 Configurez l'interface Wi-Fi.**

Exécutez les étapes suivantes pour configurer l'interface :

- Créez l'interface prenant en charge le Wi-Fi :

```
# ipadm create-ip ath0
```

- Vérifiez que le lien a été monté :

```
# ipadm show-if
IFNAME      CLASS      STATE      ACTIVE      OVER
lo0         loopback   ok         yes         --
e1000g0     ip         ok         yes         --
ath0        ip         ok         yes         --
```

#### 4 Vérifiez les réseaux disponibles.

```
# dladm scan-wifi
LINK      ESSID      BSSID/IBSSID  SEC      STRENGTH  MODE  SPEED
ath0      net1       00:0e:38:49:01:d0 none     good      g      54Mb
ath0      net2       00:0e:38:49:02:f0 none     very weak g      54Mb
ath0      net3       00:0d:ed:a5:47:e0 none     very good g      54Mb
```

L'exemple de sortie de la commande `scan-wifi` affiche des informations sur les réseaux Wi-Fi disponibles à l'emplacement actuel. Les informations contenues dans la sortie incluent :

LINK	Nom du lien à utiliser pour la connexion Wi-Fi.
ESSID	Extended Service Set ID. ESSID est le nom du réseau Wi-Fi, tel que <code>net1</code> , <code>net2</code> et <code>net3</code> dans l'exemple de sortie.
BSSID/IBSSID	Basic Service Set ID, l'identificateur unique pour un ESSID particulier. Le BSSID correspond à l'adresse MAC 48 bits du point d'accès le plus proche qui dessert le réseau à l'aide d'un ESSID particulier.
SEC	Type de sécurité nécessaire pour accéder au réseau. Les valeurs sont <code>none</code> ou <code>WEP</code> . Pour plus d'informations sur le chiffrement WEP, reportez-vous à la section <a href="#">“Communications Wi-Fi sécurisées” à la page 218</a> .
STRENGTH	Intensité des signaux radio des réseaux Wi-Fi disponibles sur votre site.
MODE	Version du protocole 802.11 exécutée par le réseau. Les modes sont <code>a</code> , <code>b</code> ou <code>g</code> , ou une combinaison de ces modes.
SPEED	Vitesse en mégabits par seconde du réseau particulier.

#### 5 Connectez-vous à un réseau Wi-Fi.

Effectuez l'une des actions suivantes :

- Connectez-vous au réseau Wi-Fi non sécurisé avec le signal le plus fort.

```
# dladm connect-wifi
```

- Connectez-vous à un réseau non sécurisé en spécifiant son ESSID.

```
# dladm connect-wifi -e ESSID
```

La sous-commande `connect-wifi` de la commande `dladm` dispose de plusieurs options pour la connexion à un réseau Wi-Fi. Pour plus d'informations, reportez-vous à la page de manuel [dladm\(1M\)](#).

## 6 Configurez une adresse IP pour l'interface.

Effectuez l'une des opérations suivantes :

- Obtenez une adresse IP à partir d'un serveur DHCP.

```
# ipadm create-addr -T dhcp addrobj
```

où *addrobj* utilise la convention de nommage *interface/user-defined-string*.

Si le réseau Wi-Fi ne prend pas en charge le protocole DHCP, vous recevez le message suivant :

```
ipadm: interface: interface does not exist or cannot be managed using DHCP
```

- Configurez une adresse IP statique :

Utilisez cette option si vous disposez d'une adresse IP dédiée pour le système.

```
# ipadm create-addr -T static -a address addrobj
```

## 7 Vérifiez l'état du réseau Wi-Fi auquel le système est connecté.

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      connected   net3       none     very good g      36Mb
```

Dans cet exemple, la sortie indique que le système est maintenant connecté au réseau `net3`. La sortie `scan-wifi` précédente indiquait que `net3` avait le signal le plus fort de tous les réseaux disponibles. La commande `dladm show-wifi` sélectionne automatiquement le réseau Wi-Fi avec le signal le plus fort, sauf si vous indiquez directement un autre réseau.

## 8 Accédez à Internet via le réseau Wi-Fi.

Effectuez l'une des opérations suivantes, en fonction du réseau auquel le système est connecté :

- Si le point d'accès offre des services gratuits, vous pouvez maintenant lancer un navigateur ou une application de votre choix.
- Si le point d'accès se trouve dans un point actif commercial qui nécessite un paiement, suivez les instructions fournies à l'emplacement actuel. En règle générale, vous exécutez un navigateur, fournissez une clé et donnez des informations de carte de crédit au fournisseur réseau.

## 9 Terminez la session.

Effectuez l'une des actions suivantes :

- Mettez fin à la session Wi-Fi mais laissez le système en cours d'exécution.

```
# dladm disconnect-wifi
```

- Mettez fin à une session Wi-Fi particulière lorsque plusieurs sessions sont actuellement en cours d'exécution.

```
# dladm disconnect-wifi link
```

où *link* représente l'interface utilisée pour la session.

- Arrêtez le système proprement alors que la session Wi-Fi est en cours d'exécution.

```
# shutdown -g0 -i5
```

Il n'est pas nécessaire de déconnecter la session Wi-Fi explicitement avant de désactiver le système par le biais de la commande `shutdown`.

### Exemple 10–1 Connexion à un réseau Wi-Fi spécifique

L'exemple suivant présente un cas typique que vous pouvez rencontrer lors de l'utilisation d'un ordinateur portable exécutant Oracle Solaris dans un café Internet.

Découvrez si un lien Wi-Fi est disponible.

```
# dladm show-wifi
ath0                type: non-vlan      mtu: 1500          device: ath0
```

Le lien `ath0` est installé sur l'ordinateur portable. Configurez l'interface `ath0` et vérifiez qu'elle est opérationnelle.

```
# ipadm create-ip ath0
IFNAME    STATE    CURRENT    PERSISTENT
lo0       ok       -m-v-----46 ---
ath0      ok       bm-----46 -46
```

Affichez les liens Wi-Fi disponibles à l'endroit où vous vous trouvez.

```
# dladm scan-wifi
LINK      ESSID          BSSID/IBSSID    SEC    STRENGTH  MODE  SPEED
ath0      net1           00:0e:38:49:01:d0 none    weak      g     54Mb
ath0      net2           00:0e:38:49:02:f0 none    very weak g     54Mb
ath0      net3           00:0d:ed:a5:47:e0 wep     very good g     54Mb
ath0      citinet        00:40:96:2a:56:b5 none    good      b     11Mb
```

La sortie indique que `net3` a le meilleur signal. `net3` requiert une clé, pour laquelle le fournisseur du café fait payer des frais. `citinet` est un réseau libre fourni par la ville.

Connectez-vous au réseau `citinet`.

```
# dladm connect-wifi -e citinet
```

L'option `-e` de la commande `connect-wifi` prend l'ESSID du réseau Wi-Fi préféré comme argument. L'argument dans cette commande est `citinet`, l'ESSID du réseau local gratuit. La

commande `dladm connect-wifi` offre plusieurs options de connexion au réseau Wi-Fi. Pour plus d'informations, reportez-vous à la page de manuel [dladm\(1M\)](#).

Configurez une adresse IP pour l'interface Wi-Fi.

```
# ipadm create-addr -T static -a 10.192.16.3/8 ath0/v4
# ipadm show-addr
ADDROBJ          TYPE      STATE      ADDR
lo0/v4           static    ok         127.0.0.1/8
e1000g0/v4       static    ok         129.146.69.34/24
ath0/v4static    static    ok         10.192.16.3/8
lo0/v6           static    ok         ::1/128
```

Cet exemple suppose que l'adresse IP statique 10.192.16.3/24 est configurée sur votre ordinateur portable.

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      connected   citinet    none     good      g     11Mb
```

La sortie indique que l'ordinateur portable est maintenant connecté au réseau citinet .

```
# firefox
```

La page d'accueil du navigateur Firefox s'affiche.

Lancez un navigateur ou une autre application pour commencer à travailler sur le réseau Wi-Fi.

```
# dladm disconnect-wifi
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      disconnected --         --         --         --         --
```

La sortie de la commande `show-wifi` vérifie que vous vous êtes déconnecté du lien `ath0` à partir du réseau Wi-Fi.

## ▼ Contrôle du lien Wi-Fi

Cette procédure indique comment contrôler l'état d'un lien Wi-Fi via des outils réseau standard, et comment modifier les propriétés du lien à l'aide de la sous-commande `linkprop`.

- 1 **Connectez-vous en tant qu'administrateur.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 2 **Connectez-vous à un réseau Wi-Fi, comme décrit à la section “[Connexion à un réseau Wi-Fi](#)” à la page 212.**



### 3 Affichez les propriétés du lien.

Utilisez la syntaxe suivante :

```
# dladm show-linkprop interface
```

Par exemple, utilisez la syntaxe suivante pour afficher l'état de la connexion établie sur le lien `ath0` :

```
# dladm show-linkprop ath0
```

PROPERTY	VALUE	DEFAULT	POSSIBLE
channel	5	--	--
powermode	off	off	off,fast,max
radio	?	on	on,off
speed	36	--	1,2,5,6,9,11,12,18,24,36,48,54

### 4 Définissez une vitesse fixe pour le lien.



**Attention** – Oracle Solaris choisit automatiquement la vitesse optimale pour la connexion Wi-Fi. Si vous modifiez la vitesse initiale du lien, cela peut entraîner une diminution des performances ou empêcher l'établissement de certaines connexions Wi-Fi.

Vous pouvez modifier la vitesse du lien avec l'une des valeurs de vitesse possibles répertoriées dans la sortie `show-linkprop`.

```
# dladm set-linkprop -p speed=value link
```

### 5 Vérifiez le flux de paquets sur le lien.

```
# netstat -I ath0 -i 5
```

input		ath0		output		input (Total)		output		
packets	errs	packets	errs	colls	packets	errs	packets	errs	colls	
317	0	106	0	0	2905	0	571	0	0	
14	0	0	0	0	20	0	0	0	0	
7	0	0	0	0	16	0	1	0	0	
5	0	0	0	0	9	0	0	0	0	
304	0	10	0	0	631	0	316	0	0	
338	0	9	0	0	722	0	381	0	0	
294	0	7	0	0	670	0	371	0	0	
306	0	5	0	0	649	0	338	0	0	
289	0	5	0	0	597	0	301	0	0	

#### Exemple 10–2 Configuration de la vitesse d'un lien

Cet exemple indique comment définir la vitesse d'un lien une fois que vous êtes connecté à un réseau Wi-Fi

```
# dladm show-linkprop -p speed ath0
```

PROPERTY	VALUE	DEFAULT	POSSIBLE
speed	24	--	1,2,5,6,9,11,12,18,24,36,48,54

```
# dladm set-linkprop -p speed=36 ath0
```

```
# dladm show-linkprop -p speed ath0
PROPERTY      VALUE      DEFAULT    POSSIBLE
speed          36         - -        1,2,5,6,9,11,12,18,24,36,48,54
```

## Communications Wi-Fi sécurisées

Grâce aux technologies d'onde radio, les réseaux Wi-Fi sont facilement disponibles et souvent en accès libre pour les utilisateurs dans de nombreux endroits. Par conséquent, se connecter à un réseau Wi-Fi peut être incertain. Cependant, certains types de connexions Wi-Fi sont plus sûrs :

- Connexion à un réseau Wi-Fi privé, à accès limité

Les réseaux privés, tels que les réseaux internes établis par des entreprises ou des universités, restreignent l'accès à leurs réseaux aux utilisateurs qui peuvent fournir la réponse correcte au défi de sécurité. Les utilisateurs potentiels doivent fournir une clé au cours de la connexion ou se connecter au réseau via VPN sécurisé.

- Chiffrement de votre connexion au réseau Wi-Fi

Vous pouvez chiffrer les communications entre votre système et un réseau Wi-Fi à l'aide d'une clé de sécurité. Le point d'accès au réseau Wi-Fi doit être un routeur à votre domicile ou votre bureau doté d'une fonction de génération de clé sécurisée. Votre système et le routeur établissent puis partagent la clé avant de créer la connexion sécurisée.

La commande `dladm` peut utiliser une clé WEP (Wired Equivalent Privacy) pour le chiffrement des connexions via le point d'accès. Le protocole WEP est défini dans les normes IEEE 802.11 pour les connexions sans fil. Pour obtenir des informations complètes sur les options associées au protocole WEP de la commande `dladm`, reportez-vous à la page de manuel [dladm\(1M\)](#).

## ▼ Configuration d'une connexion chiffrée à un réseau Wi-Fi

La procédure ci-après présente la configuration de communications sécurisées entre un système et un routeur à votre domicile. De nombreux routeurs filaires ou sans fil pour les particuliers possèdent une fonctionnalité de chiffrement qui peut générer une clé sécurisée. Cette procédure suppose que vous utilisez un tel routeur et que vous possédez sa documentation. Elle suppose également que votre système est déjà branché sur le routeur.

### 1 Démarrez le logiciel pour configurer votre routeur particulier.

Reportez-vous aux instructions fournies par le fabricant pour de plus amples informations. Les fabricants de routeur proposent généralement un site Web interne ou une interface graphique pour la configuration du routeur.

**2 Générez la valeur pour la clé WEP.**

Suivez les instructions du fabricant pour créer une clé sécurisée pour le routeur. L'interface graphique de configuration du routeur peut vous demander de fournir une phrase de passe de votre choix pour la clé. Ensuite, le logiciel l'utilise pour générer une chaîne hexadécimale, généralement d'une longueur de 5 ou 13 octets. Cette chaîne devient la valeur à utiliser pour la clé WEP.

**3 Appliquez et enregistrez la configuration de la clé.**

Reportez-vous aux instructions fournies par le fabricant pour de plus amples informations.

**4 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

**5 Créez un objet sécurisé contenant la clé WEP.**

Ouvrez une fenêtre de terminal sur le système et saisissez la commande suivante :

```
# dladm create-secobj -c wep keyname
```

où *keyname* représente le nom que vous souhaitez donner à la clé.

**6 Indiquez la valeur de la clé WEP à l'objet sécurisé.**

La sous-commande `create-secobj` exécute ensuite un script qui demande la valeur de la clé.

```
provide value for keyname: 5 or 13 byte key
confirm value for keyname: retype key
```

Cette valeur est la clé générée par le routeur. Le script accepte une chaîne de 5 ou 13 octets, au format ASCII ou en hexadécimal comme valeur de la clé.

**7 Affichez le contenu de la clé que vous venez de créer.**

```
# dladm show-secobj
OBJECT          CLASS
keyname         wep
```

où *keyname* est le nom de l'objet sécurisé.

**8 Etablissez une connexion chiffrée au réseau Wi-Fi.**

```
# dladm connect-wifi -e network -k keyname interface
```

**9 Vérifiez que la connexion est sécurisée.**

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      connected    net1      wep      good      g     11Mb
```

La valeur `wep` sous l'en-tête `SEC` indique que le chiffrement WEP est en place pour la connexion.

**Exemple 10-3** Configuration de communications Wi-Fi chiffrées

Cet exemple suppose que vous avez déjà effectué les opérations suivantes :

- Connexion de votre système à un routeur personnel pouvant créer une clé WEP
- Suivi de la documentation du fabricant du routeur et création de la clé WEP
- Enregistrement de la clé afin de pouvoir l'utiliser pour créer l'objet sécurisé sur votre système

```
# dladm create-secobj -c wep mykey
provide value for mykey: *****
confirm value for mkey: *****
```

Lorsque vous tapez la clé WEP générée par le routeur, des astérisques masquent la valeur que vous saisissez.

```
# dladm show-secobj
OBJECT          CLASS
mykey           wep
# dladm connect-wifi -e citinet -k mykey ath0
```

Cette commande établit une connexion chiffrée pour le réseau Wi-Fi `citinet`, à l'aide de l'objet sécurisé `mykey`.

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      connected   citinet    wep      good      g     36Mb
```

Cette sortie vérifie que vous êtes connecté à `citinet` via le chiffrement WEP.

# Administration des ponts

---

Ce chapitre décrit les ponts et la façon de les administrer.

Ce chapitre comprend les sections suivantes :

- “Présentation du pontage” à la page 221
- “Administration de ponts (liste des tâches)” à la page 231

## Présentation du pontage

Les ponts permettent de connecter des segments du réseau. Dans le cas d'une connexion par pont, les segments réseau reliés communiquent comme s'ils formaient un seul et même segment réseau. Le pontage est mis en oeuvre au niveau de la couche de liaison de données (L2) de la pile réseau. Les ponts utilisent un mécanisme de transmission de paquets pour connecter des sous-réseaux.

Bien que le pontage et le routage puissent être utilisés pour diffuser des informations sur l'emplacement des ressources réseau, ils diffèrent de plusieurs façons. Le routage est mis en oeuvre au niveau de la couche IP (L3) et utilise les protocoles de routage. Aucun protocole de routage n'est utilisé sur la couche de liaison de données. En revanche, les destinations des paquets transmis sont déterminées par l'examen du trafic sur le réseau, reçu sur les liaisons reliées au pont.

Lorsqu'un paquet est reçu, son adresse source est examinée. L'adresse source du paquet associe le noeud à partir duquel le paquet a été envoyé à la liaison sur laquelle il est reçu. Par la suite, lorsqu'un paquet reçu utilise cette même adresse comme adresse de destination, le pont transmet le paquet sur la liaison vers cette adresse.

La liaison associée à une adresse source peut être une liaison intermédiaire, connectée à un autre pont au sein du sous-réseau constitué de ponts. Au fil du temps, tous les ponts au sein du sous-réseau "apprennent" quelle est la liaison qui envoie un paquet vers un noeud donné. Par conséquent, l'adresse de destination du paquet est utilisée pour le diriger vers sa destination finale par le biais d'un pontage de connexions directes.

Une notification locale d'interruption de liaison indique que tous les noeuds d'une liaison donnée ne sont plus accessibles. Dans cette situation, le transfert de paquet vers la liaison est interrompu et toutes les entrées de transfert sur la liaison sont supprimées. Au fil du temps, les entrées de transfert sont également supprimées. Lorsqu'une liaison est restaurée, les paquets reçus via cette liaison sont traités comme des nouveaux paquets. Le "processus d'apprentissage" basé sur l'adresse source d'un paquet recommence. Ce processus permet au pont de transférer correctement des paquets sur cette liaison lorsque l'adresse est utilisée comme adresse de destination.

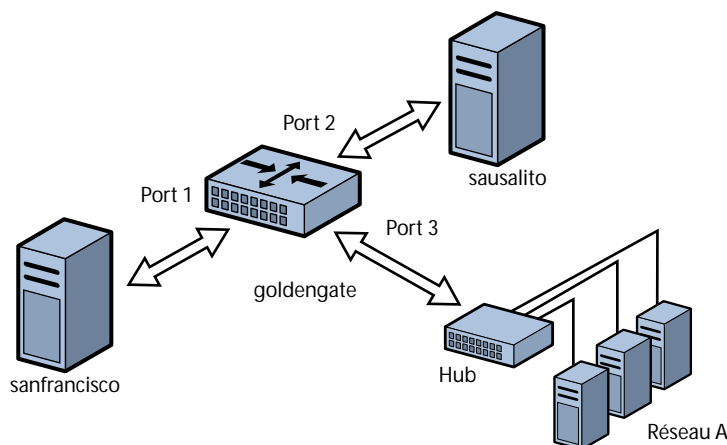
Pour transférer les paquets à leur destination, les ponts doivent écouter en mode de promiscuité toutes les liaisons reliées au pont. L'écoute en mode de promiscuité rend les ponts vulnérables aux occurrences de boucles de transfert dans lesquelles les paquets tournent indéfiniment à taux plein. Par conséquent, le pontage utilise le mécanisme STP (Spanning Tree Protocol) pour éviter les boucles réseau qui rendraient les sous-réseaux inutilisables.

Outre l'utilisation de STP et de RSTP (Rapid Spanning Tree Protocol) pour les ponts, Oracle Solaris prend en charge l'amélioration de la protection TRILL. STP est utilisé par défaut, mais vous pouvez utiliser TRILL en spécifiant l'option `-P trill` pour les commandes de pontage.

L'utilisation d'une configuration de pont simplifie l'administration des divers noeuds réseau en les connectant au sein d'un seul et même réseau. En reliant ces segments par un pont, tous les noeuds partagent un réseau unique de diffusion. Par conséquent, chaque noeud peut atteindre les autres en utilisant des protocoles réseau tels qu'IP plutôt que des routeurs pour transférer le trafic d'un segment du réseau à l'autre. Si vous n'utilisez pas un pont, vous devez configurer le routage IP de sorte à autoriser le transfert du trafic IP entre les noeuds.

La figure ci-dessous illustre une configuration réseau de ponts simple. Le pont `goldengate` est un système Oracle Solaris dont le pontage est configuré. Les systèmes `sanfrancisco` et `sausalito` sont connectés physiquement au pont. Le réseau A utilise un hub physiquement connecté au pont d'un côté et à des systèmes informatiques de l'autre côté. Les ports de pont sont des liaisons, tels que `bge0`, `bge1` et `bge2`.

FIGURE 11-1 Réseau simple relié par des ponts



Les réseaux de pont peuvent être formés en anneaux connectant physiquement plusieurs ponts. Ces configurations sont courantes dans les réseaux. Ce type de configuration risque de générer des problèmes dus aux paquets anciens qui saturent les liaisons réseau en tournant en boucle indéfiniment autour de l'anneau. Afin d'éviter de telles conditions de mise en boucle, les ponts Oracle Solaris mettent en oeuvre les protocoles STP et TRILL. Notez que la plupart des ponts matériels mettent également en oeuvre la protection contre les boucles STP.

La figure suivante illustre un réseau relié par des ponts, configuré dans un anneau. La configuration présente trois ponts. Deux systèmes sont connectés physiquement à *westminster*. Un système est connecté physiquement à *waterloo*. Un système est connecté physiquement à *tower*. Chaque pont est connecté physiquement aux autres par le biais des ports de pont.

Lorsque le protocole STP ou RSTP est utilisé dans le cadre de la protection contre les boucles, la boucle physique est atténuée en empêchant une des connexions dans la boucle de transmettre des paquets. Dans la figure, la liaison physique entre les ponts *westminster* et *tower* ne sert pas à transmettre des paquets.

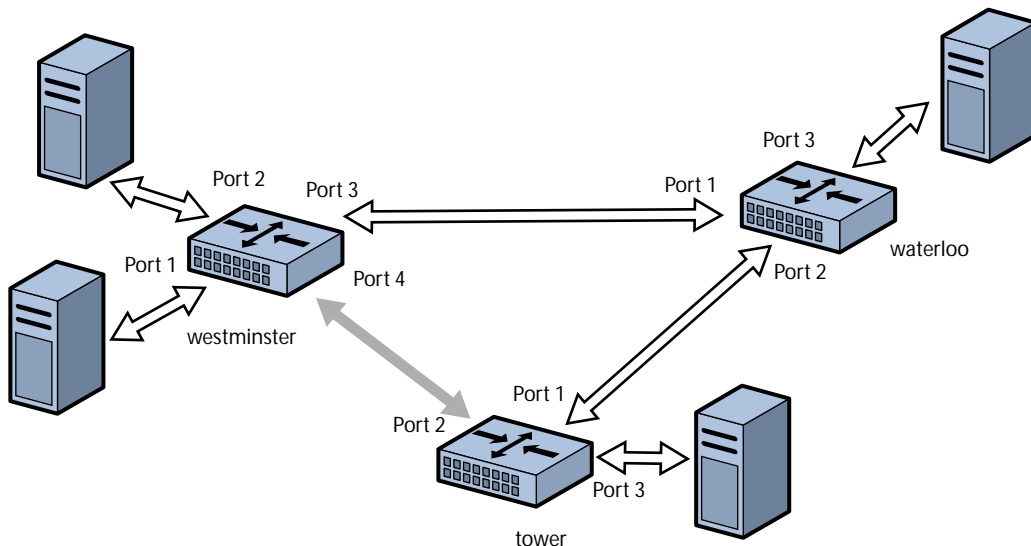
Notez que si des liaisons physiques utilisables sont fermées dans le cadre de la protection contre les boucles, les protocoles STP et RSTP vous font perdre de la bande passante.

Contrairement à STP et RSTP, le protocole TRILL ne ferme pas les liaisons physiques afin d'éviter les boucles. TRILL calcule plutôt les informations du chemin le plus court pour chaque nœud TRILL au sein du réseau et les utilise pour transférer les paquets vers différentes destinations.

Par conséquent, TRILL permet au système de ne jamais interrompre *aucune* liaison utilisée. Les boucles ne posent pas problème dans la mesure où elles sont gérées de la même manière qu'IP

gère les boucles. En d'autres termes, TRILL crée des routes en fonction des besoins et utilise des limites de connexion directe de transfert pour éviter les problèmes causés par les états de boucle temporaires.

FIGURE 11-2 Anneau de réseau relié par un pont



**Attention** – Ne définissez *pas* `local-mac-address?=false` sur les plates-formes SPARC, sinon les systèmes utiliseront la même adresse MAC sur plusieurs ports et sur le même réseau.

**Remarque** – Ne configurez *pas* une liaison dans un pont lorsque les plus hauts niveaux de performances sont requis. Le pontage *requiert* que les interfaces sous-jacentes soient en mode de promiscuité, ce qui désactive un nombre d'optimisations importantes dans les couches de matériel, pilote et autres du système. La désactivation de ces améliorations de performances est une conséquence inévitable du mécanisme de pontage.

Vous pouvez utiliser un pont sur un système où *certaines* liaisons ne sont pas reliées par un pont et ne sont donc pas soumises à ces contraintes. Ces problèmes de performances n'ont d'incidence que sur les liaisons configurées pour faire partie d'un pont.

Pour plus d'informations sur le protocole STP, reportez-vous au document IEEE 802.1D-1998. Pour plus d'informations sur le protocole RSTP, reportez-vous au document IEEE 820.1Q-2004.



Pour plus d'informations sur le protocole TRILL, reportez-vous aux documents [Internet Engineering Task Force \(IETF\) TRILL draft documents \(http://tools.ietf.org/wg/trill\)](http://tools.ietf.org/wg/trill).

## Propriétés de liaison

Ces propriétés de liaison peuvent être affichées et modifiées par les commandes `dladm show-linkprop`, `dladm set-linkprop` et `reset-linkprop` :

**default\_tag** Définit l'ID VLAN (virtual local area network, réseau local virtuel) par défaut pour les paquets sans étiquette envoyés depuis et vers la liaison. Les valeurs valides sont comprises entre 0 et 4094. La valeur par défaut est 1. Seules les liaisons non-VLAN et non-VNIC (virtual network interface card, carte réseau virtuelle) possèdent cette propriété. La définition de cette valeur sur 0 désactive la transmission de paquets sans étiquette depuis et vers le port. (Il s'agit d'une propriété MAC.)

---

**Remarque** – Cette propriété est également utilisée en dehors de la portée du pontage pour spécifier le PVID (Port VLAN Identifier) IEEE de cette liaison. Lorsque la propriété `default_tag` n'est pas définie sur zéro, vous ne pouvez pas créer un VLAN qui a ce même ID sur la liaison, car la liaison de base elle-même représente automatiquement le PVID.

Si, par exemple, le PVID est défini sur 5 sur `net0`, vous ne pouvez pas créer un VLAN avec l'ID 5 sur `net0`. Pour définir le VLAN 5 dans cette situation, utilisez `net0`.

Vous ne pouvez pas définir la propriété `default_tag` pour qu'elle soit égale à l'ID d'un VLAN existant créé sur ce lien. Par exemple, la commande suivante crée VLAN 22 sur `net0` :

```
# dladm create-vlan -l net0 -v 22 myvlan0
```

Dans cette situation, vous ne pouvez pas définir `default_tag` sur 22, car `net0` et `myvlan0` représenteraient le même VLAN.

En définissant `default_tag` sur 0, vous permettez que les paquets sans étiquette sur `net0` soient dissociés de tous les VLAN. Cette situation permet d'empêcher la transmission de ces paquets par un pont configuré.

---

**forward** Active et désactive la transmission de trafic via le pont. Cette propriété existe sur toutes les liaisons, à l'exception des liaisons VNIC. Les valeurs valides sont 1 (vrai) et 0 (faux). La valeur par défaut est 1. Lorsqu'il est désactivé, un VLAN associé à une instance de liaison ne transfère pas de trafic via le pont.

Désactiver le transfert revient à supprimer le VLAN de "l'ensemble autorisé" pour un pont traditionnel. Cela signifie que les E/S VLAN vers la liaison sous-jacente des clients locaux se poursuit, mais que le transfert sur les ponts n'a pas lieu.

<code>stp</code>	Active et désactive les protocoles STP et RSTP. Les valeurs valides sont 1 (vrai) et 0 (faux). La valeur par défaut 1 permet d'activer les protocoles STP et RSTP. Lorsqu'elle est définie sur 0, la liaison n'utilise pas n'importe quel type de protocole STP et elle est placée en mode de transfert à tout moment. Le mode de transfert utilise la protection BPDU (bridge protocol data unit). Désactivez les protocoles STP et RSTP lorsque vous souhaitez configurer des liaisons point à point connectées aux noeuds de fin. Seules les liaisons de type non-VLAN et non-VNIC possèdent cette propriété.
<code>stp_cost</code>	Représente les valeurs de coût STP et RSTP pour utiliser la liaison. Les valeurs valides sont comprises entre 1 et 65535. La valeur par défaut 0 signale que le coût est automatiquement calculé par le type de liaison. Les valeurs suivantes représentent le coût pour plusieurs types de liaisons : 100 pour 10 Mbit/s, 19 pour 100 Mbit/s, 4 pour 1 Gbit/s et 2 pour 10 Gbit/s.
<code>stp_edge</code>	Indique si le port est connecté à d'autres ponts. Les valeurs valides sont 1 (vrai) et 0 (faux). La valeur par défaut est 1. Si l'option est définie sur 0, le démon suppose que le port est connecté à d'autres ponts même si aucun BPDU d'aucun type n'est visible.
<code>stp_p2p</code>	Spécifie le type du mode de connexion. Les valeurs valides sont <code>true</code> , <code>false</code> et <code>auto</code> . La valeur par défaut <code>auto</code> détecte automatiquement les connexions point à point. Spécifiez <code>true</code> afin d'appliquer le mode point à point, et spécifiez <code>false</code> pour appliquer le mode multipoint normal.
<code>stp_priority</code>	Définit la valeur de la priorité de port STP et RSTP. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 128. La valeur de priorité du port STP et RSTP permet de déterminer le port racine préféré d'un pont en ajoutant la valeur au début de l'identificateur du port. La priorité est d'autant plus élevée que la valeur numérique est petite.

## Démon STP

Chaque pont que vous créez à l'aide de la commande `dladm create-bridge` est représenté comme une instance SMF nommée de manière identique de `svc:/network/bridge`. Chaque instance exécute une copie du démon `/usr/lib/bridged`, qui met en oeuvre le protocole STP.

L'exemple de commande suivant crée un pont appelé `pontevecchio` :

```
# dladm create-bridge pontevecchio
```

Le système crée un service SMF appelé `svc:/network/bridge:pontavecchio` et un noeud d'observabilité appelé `/dev/net/pontavecchio0`.

Pour des raisons de sécurité, tous les ports exécutent le protocole STP standard par défaut. Un pont qui n'exécute pas un type de protocole de pontage, tel que STP, peut former des boucles de transfert durables sur le réseau. Dans la mesure où Ethernet n'a pas de compte de connexion directe ou TTL sur les paquets, toutes les boucles de ce type sont fatales pour le réseau.

Si vous savez qu'un port particulier n'est pas connecté à un autre pont (par exemple, une connexion point à point directe à un système hôte), vous pouvez désactiver administrativement STP pour ce port. Même si STP est désactivé sur tous les ports d'un pont, le démon STP continue de s'exécuter. Et ce pour les raisons suivantes :

- pour traiter les nouveaux ports qui sont ajoutés ;
- pour mettre en oeuvre la protection BPDU ;
- pour activer ou désactiver le transfert sur les ports, si nécessaire.

Lorsque STP est désactivé sur un port, le démon `bridged` continue d'être à l'écoute des BPDU (protection BPDU). Le démon utilise `syslog` pour marquer toutes les erreurs et désactive le transfert sur le port pour indiquer une grave erreur de configuration réseau. La liaison est réactivée lorsque l'état de liaison fluctue ou que vous supprimez manuellement la liaison avant de la rajouter.

Si vous désactivez l'instance de service SMF d'un pont, le transfert par pont s'interrompt sur ces ports à l'arrêt du démon STP. Si l'instance est redémarrée, STP commence à partir de son état initial.

## Démon TRILL

Chaque pont que vous créez à l'aide de la commande `dladm create-bridge -P trill` est représenté comme une instance SMF portant le même nom de `svc:/network/bridge` et `svc:/network/routing/trill`. Chaque instance de `svc:/network/routing/trill` exécute une copie du démon `/usr/lib/trilld`, qui met en oeuvre le protocole TRILL.

L'exemple de commande suivant crée un pont appelé `bridgeofsighs` :

```
# dladm create-bridge -P trill bridgeofsighs
```

Le système crée deux services SMF appelés `svc:/network/bridge:bridgeofsighs` et `svc:/network/routing/trill:bridgeofsighs`. En outre, le système crée un noeud d'observabilité appelé `/dev/net/bridgeofsighs0`.

## Débogage des ponts

Chaque instance de pont reçoit un "noeud d'observabilité" qui apparaît dans le répertoire `/dev/net/` et porte le nom du pont suivi d'un 0 de fin.

Le noeud d'observabilité est destiné à être utilisé avec les utilitaires `snoop` et `wireshark`. Ce noeud se comporte comme une interface Ethernet classique, à l'exception de la transmission des paquets, qui sont silencieusement supprimés. Vous ne pouvez pas monter IP sur un noeud d'observabilité, ni effectuer des demandes de liaison (`DL_BIND_REQ`), sauf si vous utilisez l'option `passive`.

Lorsqu'il est utilisé, le noeud d'observabilité effectue une seule copie non modifiée de chaque paquet géré par le pont à la disposition de l'utilisateur. Ce comportement est similaire à celui d'un port de "surveillance" sur un pont traditionnel, et est soumis aux règles habituelles de "mode de promiscuité" DLPI. Vous pouvez utiliser `pmod` ou les fonctions des utilitaires `snoop` et `wireshark` pour filtrer en fonction de l'ID VLAN.

Les paquets transmis représentent les données reçues par le pont.



---

**Attention** – Dans le cas où le pontage ajoute, supprime ou modifie une étiquette VLAN, les données affichées décrivent l'état qui précède ce processus. Ce cas rare peut être problématique si des valeurs `default_tag` distinctes sont utilisées sur différentes liaisons.

---

Pour afficher les paquets transmis et reçus sur une liaison particulière (une fois le pontage terminé), exécutez `snoop` sur chaque liaison plutôt que sur le noeud d'observabilité.

Pour plus d'informations à propos des noeuds d'observabilité, reportez-vous à la section [“Fonctions d'observabilité pour la virtualisation du réseau et le contrôle des ressources”](#) à la page 352.

## Autres comportements des ponts

Les sections suivantes décrivent comment le comportement des liaisons est modifié lorsque des ponts sont utilisés dans la configuration.

Pour plus d'informations sur le comportement des liaisons standard, reportez-vous à la section [“Administration de réseaux locaux virtuels”](#) à la page 251.

## Comportement DLPI

La section suivante décrit les différences dans le comportement des liaisons lorsqu'un pont est activé :

- Les notifications d'activation de liaison (DL\_NOTE\_LINK\_UP) et de désactivation de liaison (DL\_NOTE\_LINK\_DOWN) sont fournies dans l'agrégat. En d'autres termes, lorsque toutes les liaisons externes affichent l'état de désactivation de liaison, les clients de niveau supérieur qui utilisent les couches MAC voient également les événements de désactivation de liaison. Lorsqu'une liaison externe sur le pont affiche l'état d'activation de liaison, tous les clients de niveau supérieur voient l'activation de liaison.

Ce rapport global sur l'activation et la désactivation des liaisons est élaboré pour les raisons suivantes :

- Lorsque la désactivation de liaison s'affiche, les noeuds sur la liaison ne sont plus accessibles. Ce n'est pas vrai lorsque le code de pontage peut toujours envoyer et recevoir des paquets par le biais d'une autre liaison. Les applications d'administration qui nécessitent l'état réel des liaisons peuvent utiliser les statistiques du noyau sur la couche MAC pour révéler l'état. Ces applications sont différentes des clients ordinaires, comme IP, dans le sens où elles signalent des informations d'état matériel et qu'elles ne sont pas impliquées dans le processus de transfert.
- Lorsque toutes les liaisons externes sont interrompues, l'état indique que le pont lui-même est fermé. Dans ce cas particulier, le système reconnaît qu'il est impossible d'accéder à quoi que ce soit. En contrepartie, les ponts ne peuvent pas être utilisés pour permettre des communications uniquement locales dans le cas où toutes les interfaces sont "réelles" (non virtuelles) et déconnectées.
- Toutes les fonctions spécifiques aux liaisons sont généralisées. Les liaisons qui prennent en charge les fonctions spéciales d'accélération matérielle ne sont pas en mesure de les utiliser, car la détermination de la liaison de sortie réelle n'est pas entièrement effectuée par le client. La fonction de transfert de pont doit choisir une liaison de sortie en fonction de l'adresse MAC de destination, et cette liaison de sortie peut être n'importe quelle liaison sur le pont.

## Administration VLAN

Par défaut, les réseaux locaux virtuels (VLAN, virtual local area networks) configurés sur le système sont transférés entre tous les ports sur une instance de pont. Lorsque vous appelez la commande `dladm create-vlan` ou `dladm create-vnic -v` et que la liaison sous-jacente fait partie d'un pont, cette commande permet également d'activer le transfert du VLAN spécifié sur cette liaison de pont.

Pour configurer un VLAN sur une liaison et désactiver le transfert vers ou à partir d'autres liaisons sur le pont, vous devez désactiver le transfert en définissant la propriété `forward` avec la commande `dladm set-linkprop`.

Utilisez la commande `dladm create-vlan` pour activer automatiquement le VLAN pour le pontage lorsque la liaison sous-jacente est configurée dans le cadre d'un pont.

Les VLAN sont ignorés dans le STP conforme aux normes. Le protocole de pontage calcule une seule topologie sans boucle à l'aide de messages BPDU sans étiquette et utilise cette arborescence pour activer et désactiver les liaisons. Vous devez configurer les liaisons, qui sont fournies dans vos réseaux, en double de telle sorte que, lorsqu'elles sont automatiquement désactivées par STP, les VLAN configurés ne sont pas déconnectés. Cela signifie que vous devez exécuter tous les VLAN en tout point de votre infrastructure de ponts ou examiner soigneusement toutes les liaisons redondantes.

Il n'est pas nécessaire que TRILL suive les règles STP complexes. Au contraire, TRILL encapsule automatiquement les paquets dont l'étiquette VLAN est intacte et les transmet à travers le réseau. En d'autres termes, TRILL relie les VLAN isolés lorsque le même ID de VLAN a été réutilisé dans un réseau de ponts unique.

Il s'agit d'une différence importante par rapport à STP où vous pouvez réutiliser les étiquettes VLAN dans des sections isolées du réseau pour gérer des ensembles de VLAN dépassant la limite de 4094. Bien que vous ne puissiez pas utiliser TRILL pour gérer les réseaux de cette manière, vous pouvez mettre en oeuvre d'autres solutions, comme des VLAN basés sur le fournisseur.

Dans un réseau STP présentant des VLAN, il peut s'avérer difficile de configurer les caractéristiques de basculement pour empêcher le partitionnement VLAN lorsque STP désactive la "mauvaise" liaison. La perte relativement minime de fonctionnalités dans les VLAN isolés est plus que compensée par la robustesse du modèle TRILL.

## Comportement VLAN

Le pont effectue le transfert en examinant l'ensemble autorisé de VLAN et la propriété `default_tag` pour chaque liaison. Le processus général s'effectue comme suit :

- **Détermination du VLAN d'entrée.** Cette tâche commence lorsqu'un paquet est reçu sur une liaison. Lorsqu'un paquet est reçu, une étiquette VLAN est recherchée. Si cette étiquette est absente ou s'il s'agit d'une étiquette uniquement de priorité (zéro), l'étiquette `default_tag` configurée sur cette liaison (si elle n'est pas définie sur zéro) sert d'étiquette VLAN interne. Si l'étiquette est absente ou définie sur zéro et que `default_tag` est définie sur zéro, le paquet est ignoré. Aucun transfert sans étiquette n'est réalisé. Si l'étiquette est présente et égale à `default_tag`, le paquet est également ignoré. Dans le cas contraire, l'étiquette d'entrée est considérée comme le VLAN d'entrée.
- **Vérification de l'appartenance de la liaison.** Si le VLAN d'entrée n'est pas configuré comme un VLAN autorisé sur cette liaison, le paquet est ignoré. Le transfert est alors calculé, et la même vérification est effectuée pour la liaison de sortie.

- **Mise à jour d'étiquette.** Si le VLAN (différent de zéro à ce stade) est égal à `default_tag` sur la liaison de sortie, l'étiquette sur le paquet (le cas échéant) est supprimée, indépendamment de la priorité. Si le VLAN n'est pas égal à `default_tag` sur la liaison de sortie, une balise est ajoutée, si elle n'est pas présente, et définie pour le paquet de sortie, la priorité actuelle étant copiée dans le paquet.

---

**Remarque** – Dans le cas où le transfert a lieu vers plusieurs interfaces (destinations de diffusion, multidiffusion et inconnues), la vérification de liaison de sortie et la mise à jour d'étiquette doivent être effectuées indépendamment pour chaque liaison de sortie. Certaines transmissions peuvent être balisées, d'autres non.

---

## Exemples de configuration de pont

Les exemples suivants montrent comment afficher des informations sur les configurations de pont et les services de pontage.

- Vous pouvez obtenir des informations sur les ponts à l'aide de la commande suivante :

```
# dladm show-bridge
BRIDGE      PROTECT ADDRESS                PRIORITY DESROOT
tonowhere    trill  32768/66:ca:b0:39:31:5d 32768 32768/66:ca:b0:39:31:5d
sanluisrey   stp    32768/ee:2:63:ed:41:94 32768 32768/ee:2:63:ed:41:94
pontoon      trill  32768/56:db:46:be:b9:62 32768 32768/56:db:46:be:b9:62
```

- Vous pouvez obtenir des informations sur le surnom TRILL d'un pont à l'aide de la commande suivante :

```
# dladm show-bridge -t tonowhere
NICK FLAGS LINK          NEXTHOP
38628 --  simblue2        56:db:46:be:b9:62
58753 L   --              --
```

## Administration de ponts (liste des tâches)

Oracle Solaris utilise la commande `dladm` et la fonctionnalité SMF pour administrer les ponts. Utilisez les commandes SMF pour activer, désactiver et surveiller les instances de pont à l'aide du FMRI (fault-managed resource identifier) de l'instance, `svc:/network/bridge`. Utilisez la commande `dladm` pour créer ou détruire des ponts, ainsi que pour affecter des liaisons aux ponts ou supprimer des liaisons de ceux-ci.

Le tableau suivant indique les tâches que vous pouvez effectuer dans le cadre de l'administration des ponts.

Tâche	Description	Voir
Affichage des informations sur les ponts configurés	Utilisez la commande <code>dladm show-bridge</code> pour afficher des informations sur les ponts configurés sur le système. Vous pouvez afficher des informations sur les ponts configurés, les liaisons, les statistiques et les entrées de transfert au niveau du noyau.	<a href="#">“Affichage d’informations sur les ponts configurés” à la page 233</a>
Affichage des informations de configuration sur les liaisons connectées à un pont	Utilisez la commande <code>dladm show-link</code> pour afficher des informations sur les liaisons configurées sur le système. Si la liaison est associée à un pont, reportez-vous à la sortie dans le champ <code>BRIDGE</code> .	<a href="#">“Affichage des informations de configuration sur les liaisons de pont” à la page 235</a>
Création d’un pont	Utilisez la commande <code>dladm create-bridge</code> pour créer un pont et ajouter des liaisons facultatives.  Par défaut, les ponts sont créés à l’aide de STP. Pour utiliser TRILL à la place, ajoutez <code>-P trill</code> à la ligne de commande <code>dladm create-bridge</code> ou utilisez la commande <code>dladm modify-bridge</code> pour activer TRILL.	<a href="#">“Création d’un pont” à la page 235</a>
Modification du type de protection d’un pont	Utilisez la commande <code>dladm modify-bridge</code> pour modifier le type de protection d’un pont.  Par défaut, les ponts sont créés à l’aide de STP. Pour utiliser TRILL à la place, utilisez <code>-P trill</code> avec la commande <code>dladm modify-bridge</code> pour activer TRILL.	<a href="#">“Modification du type de protection pour un pont ” à la page 236</a>
Ajout d’une liaison vers un pont	Utilisez la commande <code>dladm add-bridge</code> pour ajouter une ou plusieurs liaisons vers un pont existant.	<a href="#">“Ajout d’une ou de plusieurs liaisons à un pont existant ” à la page 236</a>



Tâche	Description	Voir
Suppression des liaisons d'un pont	Utilisez la commande <code>dladm remove-bridge</code> pour supprimer les liaisons d'un pont. Vous ne pouvez pas supprimer un pont tant que toutes ses liaisons ne sont pas supprimées.	<a href="#">“Suppression des liaisons d'un pont” à la page 237</a>
Suppression d'un pont du système	Utilisez la commande <code>dladm delete-bridge</code> pour supprimer un pont du système.	<a href="#">“Suppression d'un pont du système” à la page 238</a>

## ▼ Affichage d'informations sur les ponts configurés

Cette procédure illustre l'utilisation de la commande `dladm show-bridge` et de ses diverses options pour afficher différents types d'informations sur les ponts configurés.

Pour plus d'informations sur les options de la commande `dladm show-bridge`, reportez-vous à la page de manuel [dladm\(1M\)](#).

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 Affichez des informations concernant un pont ou tous les ponts configurés.

- Afficher la liste des ponts  
# `dladm show-bridge`
- Afficher l'état de la liaison pour le pont  
# `dladm show-bridge -l bridge-name`
- Afficher les statistiques du pont  
# `dladm show-bridge -s bridge-name`

---

**Remarque** – Les noms et définitions des statistiques dans les rapports sont sujets à modification.

---

- Afficher les statistiques sur les liaisons du pont  
# `dladm show-bridge -ls bridge-name`
- Afficher les entrées de transfert du noyau pour le pont  
# `dladm show-bridge -f bridge-name`
- Afficher les informations TRILL sur le pont

```
# dladm show-bridge -t bridge-name
```

### Exemple 11–1 Affichage d'informations relatives au pont

Les éléments suivants sont des exemples d'utilisation de la commande `dladm show-bridge` avec différentes options.

- Ce qui suit illustre les informations sur tous les ponts configurés sur le système :

```
# dladm show-bridge
BRIDGE      PROTECT ADDRESS          PRIORITY DESROOT
goldengate  stp      32768/8:0:20:bf:f 32768     8192/0:d0:0:76:14:38
baybridge   stp      32768/8:0:20:e5:8 32768     8192/0:d0:0:76:14:38
```

- La commande `dladm show-bridge -l` suivante affiche les informations d'état relatives aux liaisons d'une seule instance de pont, `tower`. Pour afficher les paramètres configurés, utilisez plutôt la commande `dladm show-linkprop`.

```
# dladm show-bridge -l tower
LINK      STATE      UPTIME    DESROOT
hme0      forwarding 117       8192/0:d0:0:76:14:38
qfe1      forwarding 117       8192/0:d0:0:76:14:38
```

- La commande `dladm show-bridge -s` suivante affiche les statistiques pour le pont spécifié, `terabithia` :

```
# dladm show-bridge -s terabithia
BRIDGE      DROPS      FORWARDS
terabithia  0          302
```

- La commande `dladm show-bridge -ls` suivante affiche les statistiques pour toutes les liaisons sur le pont spécifié, `london` :

```
# dladm show-bridge -ls london
LINK      DROPS      RECV      XMIT
hme0      0          360832    31797
qfe1      0          322311    356852
```

- La commande `dladm show-bridge -f` suivante affiche les entrées de transfert du noyau pour le pont spécifié, `avignon` :

```
# dladm show-bridge -f avignon
DEST      AGE      FLAGS    OUTPUT
8:0:20:bc:a7:dc 10.860  --      hme0
8:0:20:bf:f9:69  --      L        hme0
8:0:20:c0:20:26 17.420  --      hme0
8:0:20:e5:86:11  --      L        qfe1
```

- La commande `dladm show-bridge -t` suivante affiche les informations TRILL sur le pont spécifié, `key` :

```
# dladm show-bridge -t key
NICK FLAGS LINK      NEXTHOP
38628 -- london 56:db:46:be:b9:62
58753 L  --      --
```

## ▼ Affichage des informations de configuration sur les liaisons de pont

La sortie d'`dladm show-link` inclut un champ `BRIDGE`. Si une liaison est membre d'un pont, ce champ identifie le nom du pont dont il est membre. Ce champ est affiché par défaut. Pour les liaisons ne faisant pas partie d'un pont, le champ est vide si l'option `-p` est utilisée. Dans le cas contraire, le champ affiche `--`.

Le noeud d'observabilité du pont apparaît également dans la sortie d'`dladm show-link` sous forme de liaison distincte. Pour ce noeud, le champ `OVER` répertorie les liaisons membres du pont.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Affichez les informations de configuration sur les liaisons membres d'un pont.

```
# dladm show-link [-p]
```

L'option `-p` génère une sortie dans un format analysable.

## ▼ Création d'un pont

Cette procédure illustre l'utilisation de STP pour créer un pont (par défaut). Pour plus d'informations sur les options de création de pont, reportez-vous à la description de `dladm create-bridge` dans la page de manuel `dladm(1M)`.

---

**Remarque** – Pour utiliser plutôt TRILL pour créer un pont, ajoutez `-P trill` à la ligne de commande `dladm create-bridge` ou utilisez la commande `dladm modify-bridge` pour activer TRILL.

---

La commande `dladm create-bridge` crée une instance de pont et éventuellement affecte une ou plusieurs liaisons réseau au nouveau pont. Dans la mesure où aucune instance de pont n'est présente sur le système par défaut, Oracle Solaris ne relie pas les liaisons réseau par défaut.

Pour relier les liaisons entre elles, vous devez créer au moins une instance de pont. Chaque instance de pont est distincte. Les ponts n'incluent pas de connexion de transfert entre eux et une liaison est membre au plus d'un pont.

*bridge-name* est une chaîne arbitraire qui doit être un nom légal d'instance de service SMF. Ce nom est un composant FMRI qui n'a aucune séquence d'échappement, ce qui signifie qu'il ne peut pas contenir des blancs, des caractères de contrôle ASCII et les caractères suivants :

; / ? : @ & = + \$ , % < > # "

Le nom default est réservé, tout comme les noms commençant par la chaîne SUNW. Les noms contenant des chiffres de fin sont réservés à la création de "périphériques d'observabilité". En raison de l'utilisation des périphériques d'observabilité, les noms d'instances de pont légaux doivent également être des noms **dLpi(7P)** légaux. Le nom doit commencer et finir par un caractère alphabétique ou un caractère de soulignement. Le reste peut être des caractères alphanumériques et des caractères de soulignement.

## 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section "[Procédure d'obtention des droits d'administration](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

## 2 Créez le pont.

```
# dladm create-bridge [-l link]... bridge-name
```

L'option `-l link` permet d'ajouter une liaison au pont. Notez que si l'une des liaisons indiquées ne peut pas être ajoutée, la commande échoue et le pont n'est pas créé.

L'exemple suivant illustre comment créer le pont `brooklyn` en connectant les liaisons `hme0` et `qfe1` :

```
# dladm create-bridge -l hme0 -l qfe1 brooklyn
```

## ▼ Modification du type de protection pour un pont

Cette procédure illustre l'utilisation de la commande `dladm modify-bridge` pour remplacer le type de protection STP par TRILL ou inversement.

### ● Modifiez le type de protection d'un pont.

```
# dladm modify-bridge -P protection-type bridge-name
```

L'option `-P protection-type` spécifie le type de protection à utiliser. Par défaut, le type de protection est STP (`-P stp`). Pour utiliser le type de protection TRILL à sa place, exécutez l'option `-P trill`.

L'exemple suivant indique comment modifier le type de protection pour le pont `brooklyn` en remplaçant la valeur par défaut STP par TRILL :

```
# dladm modify-bridge -P trill brooklyn
```

## ▼ Ajout d'une ou de plusieurs liaisons à un pont existant

Cette procédure illustre comment ajouter une ou plusieurs liaisons à une instance de pont.

Une liaison peut être membre de tout au plus un pont. Par conséquent, si vous souhaitez déplacer une liaison d'une instance de pont à l'autre, vous devez d'abord supprimer la liaison du pont actuel avant de l'ajouter à un autre.

Les liaisons qui sont affectées à un pont ne peuvent pas être des VLAN, des VNIC ni des tunnels. Seules les liaisons acceptables dans le cadre d'une agrégation ou les liaisons qui sont des agrégations elles-mêmes peuvent être affectées à un pont.

Les liaisons affectées à un pont doivent toutes posséder la même valeur MTU. Notez que Oracle Solaris permet de modifier la valeur MTU sur une liaison existante. Dans ce cas, l'instance de pont passe à l'état de maintenance jusqu'à ce que vous supprimiez ou modifiez les liaisons affectées, de telle sorte que les valeurs MTU correspondent avant le redémarrage du pont.

Les liaisons affectées au pont doivent être de type Ethernet (médias 802.3 et 802.11 compris).

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Ajoutez un nouveau lien au pont existant.

```
# dladm add-bridge -l new-link bridge-name
```

L'exemple suivant illustre comment ajouter la liaison qfe2 au pont rialto :

```
# dladm add-bridge -l qfe2 rialto
```

## ▼ Suppression des liaisons d'un pont

Cette procédure illustre comment supprimer une ou plusieurs liaisons d'une instance de pont. Utilisez cette procédure si vous envisagez de supprimer un pont. Avant de supprimer un pont, vous devez supprimer toutes ses liaisons.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Supprimez les liaisons du pont.

```
# dladm remove-bridge [-l link]... bridge-name
```

L'exemple suivant illustre comment supprimer les liaisons hme0, qfe1 et qfe2 du pont charles :

```
# dladm remove-bridge -l hme0 -l qfe1 -l qfe2 charles
```

## ▼ Suppression d'un pont du système

Cette procédure illustre comment supprimer une instance de pont. Avant de supprimer un pont, vous devez désactiver toutes les liaisons connectées à l'aide de la commande `dladm remove-bridge`. Reportez-vous à la section [“Suppression des liaisons d'un pont”](#) à la page 237.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Supprimez le pont du système.

```
# dladm delete-bridge bridge-name
```

L'exemple ci-dessous indique comment supprimer d'abord les liaisons `hme0`, `qfe1` et `qfe2` du pont `coronado`, puis supprimer le pont lui-même du système :

```
# dladm remove-bridge -l hme0 -l qfe1 -l qfe2 coronado
# dladm delete-bridge coronado
```

# Administration de groupements de liens

---

Ce chapitre décrit les procédures de configuration et de maintenance des groupements de liens. Les procédures incluent des étapes qui utilisent les nouvelles fonctionnalités telles que la prise en charge des noms de liaisons flexibles.

## Présentation des groupements de liens

Oracle Solaris permet d'organiser les interfaces réseaux sous la forme de groupements de liens. Un *groupement de liens* est un ensemble de plusieurs interfaces d'un système configurées en une seule unité logique. Le groupement de liens, aussi appelé *jonction*, est défini par la norme [IEEE 802.3ad Link Aggregation Standard \(http://www.ieee802.org/3/index.html\)](http://www.ieee802.org/3/index.html).

La norme IEEE 802.3ad décrit la manière d'associer les capacités de plusieurs liens Ethernet duplex intégral à un seul lien logique. Un tel groupement de liens est ensuite traité en tant que lien unique.

Le groupement de liens fournit les fonctions suivantes :

- **Plus grande bande passante** : les capacités de plusieurs liens sont réunies en un seul lien logique.
- **Basculerment/rétablissement automatique** : le trafic sur un lien rompu est basculé vers un lien actif du groupement.
- **Équilibrage de charge** : le trafic entrant et sortant est distribué en fonction des stratégies d'équilibrage de charge sélectionnées par l'utilisateur (par exemple, adresses sources et cibles MAC ou IP).
- **Prise en charge de la redondance** : deux systèmes peuvent être configurés avec des groupements parallèles.
- **Administration améliorée** : toutes les interfaces sont administrées de façon unitaire.
- **Réduction du nombre de drains dans le pool d'adresses réseau** : le groupement entier peut être assigné à une seule adresse IP.

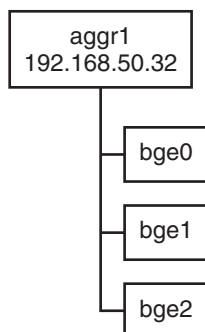
## Notions de base sur les groupements de liens

La topologie élémentaire d'un groupement de liens se définit par un ensemble unique contenant plusieurs interfaces physiques. La création de groupements de liens élémentaires est utile dans les cas suivants :

- Systèmes exécutant une application avec un trafic distribué intense. Dédiez dans ce cas un groupement de liens au trafic de cette application.
- Sites avec un nombre d'adresses IP limité, mais sur lesquels une large bande passante est nécessaire. Grâce au groupement de liens, vous pouvez réunir un grand nombre d'interfaces sous une seule adresse IP.
- Sites sur lesquels les interfaces internes doivent être masquées. Avec l'adresse IP d'un groupement de liens, les applications externes n'ont pas accès aux interfaces.

La [Figure 12-1](#) illustre un groupement de liens créé sur un serveur hébergeant un site Web connu. La bande passante doit être élargie afin d'assurer le bon fonctionnement du trafic de requêtes entre les clients en ligne et le serveur de la base de données du site. Pour des raisons de sécurité, les interfaces individuelles de ce serveur doivent être masquées aux applications externes. La solution consiste à créer un groupement `aggr1` avec l'adresse IP `192.168.50.32`. Ce groupement se compose de trois interfaces, de `bge0` à `bge2`. Chaque interface est dédiée à la transmission du trafic sortant en réponse aux requêtes des clients. Toutes ces interfaces possèdent la même adresse sortante sur le trafic de paquets, `aggr1 : 192.168.50.32`.

FIGURE 12-1 Topologie élémentaire d'un groupement de liens

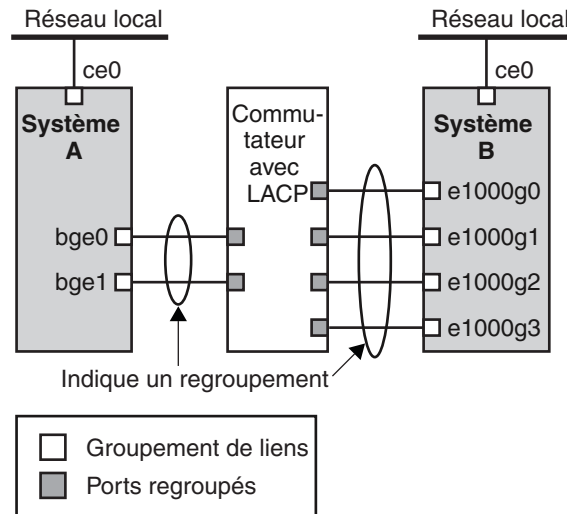


La [Figure 12-2](#) décrit un réseau local constitué de deux systèmes possédant chacun un groupement. Les deux systèmes sont connectés par un commutateur. Pour exécuter un groupement par le biais d'un commutateur, celui-ci doit prendre en charge la technologie de groupement. Ce type de configuration s'applique particulièrement bien aux systèmes à haute disponibilité ainsi qu'aux systèmes redondants.



Sur cette figure, le système A possède un groupement composé de deux interfaces, bge0 et bge1. Ces interfaces sont connectées au commutateur par le biais de ports groupés. Le système B possède un groupement de quatre interfaces, allant de e1000g0 à e1000g3. Ces interfaces sont également connectées au commutateur par le biais de ports groupés.

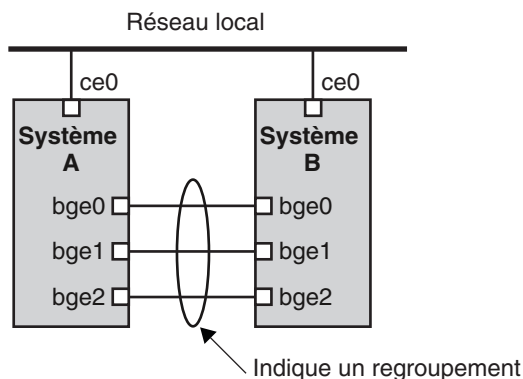
FIGURE 12-2 Topologie d'un groupement avec un commutateur



## Groupements de liens dos à dos

La topologie d'un groupement de liens dos à dos consiste en deux systèmes distincts directement connectés l'un à l'autre (voir figure suivante). Ces systèmes exécutent deux groupements parallèles.

FIGURE 12-3 Topologie élémentaire d'un groupement dos à dos



Sur cette figure, le périphérique bge0 du système A est directement connecté au périphérique bge0 du système B, etc. Cela permet aux systèmes A et B de prendre en charge la redondance ainsi que les services de haute disponibilité et d'assurer des communications haut débit entre les deux systèmes. Chaque système possède une interface ce0 dédiée au flux du trafic au sein du réseau local.

Les groupements de liens dos à dos sont le plus fréquemment utilisés avec les serveurs de base de données mis en miroir. Chaque serveur doit être mis à jour en même temps que l'autre et nécessite pour cela une large bande passante ainsi qu'un flux haut débit et une grande fiabilité. Les groupements de liens dos à dos sont le plus fréquemment utilisés dans les centres de données.

## Stratégies et équilibrage de charge

Avant de mettre en oeuvre un groupement de liens, définissez une stratégie pour le trafic sortant. Cette stratégie peut spécifier la manière dont les paquets doivent être distribués entre les différents liens disponibles dans le groupement, établissant ainsi un équilibrage de charge. Vous pouvez élaborer la stratégie pour le groupement avec l'un des spécificateurs de couche décrits ci-dessous :

- **L2** – Détermine le lien sortant en hachant l'en-tête MAC (L2) de chaque paquet.
- **L3** – Détermine le lien sortant en hachant l'en-tête IP (L3) de chaque paquet.
- **L4** – Détermine le lien sortant en hachant l'en-tête TCP, UDP ou autre en-tête ULP (L4) de chaque paquet.

Vous pouvez également combiner plusieurs de ces stratégies. L4 constitue la stratégie par défaut. Pour plus d'informations, reportez-vous à la page de manuel d'adm(1M).

## Mode de groupement et commutateurs

Si la topologie du groupement nécessite une connexion à un commutateur, vérifiez si le commutateur prend en charge le *protocole de contrôle des groupements de liens* (*Link Aggregation Control Protocol, LACP*). Si c'est le cas, vous devez configurer le LACP de manière à ce qu'il fonctionne avec le commutateur et le groupement. Cependant, vous pouvez définir l'un des *modes* de fonctionnement suivants pour le LACP :

- **Off (inactif)** : mode des groupements par défaut. Ce mode ne génère pas les paquets LACP, ou *PDULACP*.
- **Active (actif)** : ce mode génère des PDULACP à une fréquence d'intervalle personnalisable.
- **Passive (passif)** : ce mode ne génère un PDULACP que lorsqu'il en reçoit un du commutateur. Si le commutateur et le groupement sont définis sur le mode passif, ils ne peuvent échanger aucun PDULACP.

Pour plus d'informations sur la syntaxe à utiliser, reportez-vous à la page de manuel d'`ladm(1M)` ainsi qu'à la documentation fournie par le fabricant du commutateur.

## Conditions requises pour la création de groupements de liens

Vous devez respecter les conditions suivantes pour configurer un groupement de liens :

- Le groupement doit être créé à l'aide de la commande `dladm`.
- Une interface qui a été créée ne peut pas être membre d'un groupement.
- Toutes les interfaces du groupement doivent s'exécuter à la même vitesse et en mode duplex intégral.
- Vous devez définir les adresses MAC sur `True` dans le paramètre EEPROM `local-mac-address?` (voir les instructions de la section [Garantie de l'unicité de l'adresse MAC d'une interface](#)).

Certains périphériques ne remplissent pas les conditions de la norme IEEE 802.3ad d'agrégation de liaisons pour la prise en charge des notifications d'état de liaison. Cette prise en charge doit exister pour qu'un port se joigne à un groupement ou s'en détache. Les périphériques qui ne prennent pas en charge la notification d'état de liaison peuvent être groupés uniquement en utilisant l'option `-f` de la commande `dladm create-aggr`. Pour de tels périphériques, l'état de la liaison est toujours signalé comme UP. Pour plus d'informations sur l'utilisation de l'option `-f`, reportez-vous à la section [“Procédure de création d'un groupement de liens” à la page 245](#).

# Noms flexibles pour les groupements de liens

Il est possible d'affecter des noms flexibles aux groupements de liens. Tout nom significatif peut être affecté à un groupement de liens. Pour plus d'informations sur les noms flexibles ou personnalisés, reportez-vous à la section “[Noms des périphériques réseau et des liaisons de données](#)” à la page 26. Les versions précédentes d'Oracle Solaris identifient un groupement de liens à l'aide de la valeur d'une *clé* que vous attribuez au groupement. Pour obtenir une explication sur cette méthode, reportez-vous à la section [Présentation des groupements de liens](#). Bien que cette méthode reste valide, il est préférable d'utiliser des noms personnalisés pour identifier les groupements de liens.

Comme pour tous les autres configurations de liaisons de données, les groupements de liens sont gérés à l'aide de la dladm.

## Administration des groupements de liens (liste des tâches)

Le tableau ci-dessous contient des liens vers les procédures d'administration des groupements de liens.

Tâches	Description	Voir
Création d'un groupement	Configure un groupement composé de plusieurs liaisons de données.	<a href="#">“Procédure de création d'un groupement de liens” à la page 245</a>
Modification d'un groupement	Modifie la stratégie et le mode de groupements.	<a href="#">“Procédure de modification d'un groupement” à la page 247</a>
Modification des liaisons qui constituent un groupement	Augmente ou diminue le nombre de données qui sous-tendent un groupement.	<a href="#">“Procédure d'ajout d'un lien à un groupement” à la page 248</a> ou <a href="#">“Procédure de suppression d'un lien dans un groupement” à la page 249</a>
Suppression d'un groupement	Supprime complètement un groupement de liens depuis la configuration réseau.	<a href="#">“Procédure de suppression d'un groupement” à la page 249</a>

## ▼ Procédure de création d'un groupement de liens

### Avant de commencer

**Remarque** – Les groupements de liens ne fonctionnent qu'avec des liens de même vitesse, en mode duplex intégral et point à point. Assurez-vous que les interfaces de votre groupement répondent à ces critères.

Configurez les éléments suivants avant d'insérer un commutateur dans la topologie du groupement :

- Les ports du commutateur doivent pouvoir être utilisés dans un groupement.
- Si le commutateur prend en charge le LACP, celui-ci doit être configuré en mode actif ou passif.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Affichez les informations de liaison de données du réseau.

```
# dladm show-link
```

#### 3 Assurez-vous que la liaison sur laquelle vous créez le groupement n'est pas ouverte dans une application.

Par exemple, si l'interface IP sur la liaison est créée, supprimez l'interface.

##### a. Pour déterminer si une liaison n'est en cours d'utilisation par une application, examinez la sortie de la syntaxe `dladm show-link` ou `ipadm show-if`.

- Si la liaison de données est en cours d'utilisation, le champ STATE de la sortie de `dladm show-link` indique que la liaison est up. Par conséquent :

```
# dladm show-link
LINK      CLASS      MTU      STATE      BRIDGE      OVER
qfe3      phys       1500     up         --          --
```

- Si la liaison de données est en cours d'utilisation, l'interface IP sur cette liaison sera incluse dans la sortie de la syntaxe `ipadm show-if`. Par conséquent :

```
# ipadm show-if
IFNAME      CLASS      STATE      ACTIVE      OVER
lo0         loopback   ok         yes         --
qfe3        ip         ok         no          --
```

**Remarque** – Même si la sortie affiche un statut `off line`, la liaison de données est toujours en cours d'utilisation car une interface IP existe sur la liaison.

**b. Pour supprimer l'interface IP, tapez la commande suivante :**

```
# ipadm delete-ip interface
```

où

*interface* Spécifie l'interface IP qui est créée sur la liaison.

**4 Créez un groupement de liens.**

```
# dladm create-aggr [-f] -l link1 -l link2 [...] aggr
```

*-f* Force la création du groupement. Utilisez cette option lorsque vous tentez de grouper les périphériques qui ne prennent pas en charge la notification d'état de liaison.

*linkn* Spécifie les liaisons de données que vous souhaitez regrouper.

*aggr* Spécifie le nom que vous souhaitez assigner au groupement.

**5 Créez une interface IP sur le groupement.**

```
# ipadm create-ip interface
```

**6 Configurez l'interface IP avec une adresse IP valide.**

```
# ipadm create-addr interface -T static -a IP-address addrobj
```

où *interface* doit prendre le nom du groupement et *addrobj* utilise la convention d'attribution de nom *interface/user-defined-string*.

**7 Vérifiez le statut du groupement que vous venez de créer.**

L'état du groupement doit être UP.

```
# dladm show-aggr
```

**Exemple 12–1 Création d'un groupement de liens**

Cet exemple présente les commandes utilisées pour créer un groupement de liens avec deux liaisons de données, subvideo0 et subvideo1. La configuration est persistante après réinitialisation du système.

```
# dladm show-link
LINK      CLASS      MTU      STATE   BRIDGE   OVER
subvideo0  phys        1500     up      --       ----
subvideo1  phys        1500     up46    --       ----

# ipadm delete-ip subvideo0
# ipadm delete-ip subvideo1
# dladm create-aggr -l subvideo0 -l subvideo1 video0
# ipadm create-ip video0
# ipadm create-addr -T static -a 10.8.57.50/24 video/v4
# dladm show-aggr
LINK      POLICY  ADDRPOLICY  LACPACTIVITY  LACPTIMER  FLAGS
video0    L4      auto        off           short      -----
```

Lorsque vous affichez les informations de lien, le groupement de liens est inclus dans la liste.

```
# dladm show-link
LINK      CLASS  MTU   STATE  BRIDGE  OVER
subvideo0 phys   1500  up     --      ----
subvideo1 phys   1500  up     --      ----
video0    aggr   1500  up     --      subvideo0, subvideo1
```

## ▼ Procédure de modification d'un groupement

Cette procédure permet d'apporter les modifications suivantes à la définition d'un groupement :

- modification de la stratégie pour le groupement ;
- modification du mode pour le groupement.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Modifiez la stratégie du groupement.

```
# dladm modify-aggr -P policy-key aggr
```

*policy-key*      Nom de la stratégie ou des stratégies telles que L2, L3 et L4 (voir l'explication de la section [“Stratégies et équilibrage de charge”](#) à la page 242).

*aggr*              Spécifie le groupement dont vous souhaitez modifier la stratégie.

### 3 Modifiez le mode LACP du groupement.

```
# dladm modify-aggr -L LACP-mode -T timer-value aggr
```

-L *LACP-mode*      Mode LACP dans lequel le groupement s'exécute. Les valeurs de cette variable sont les suivantes : *active*, *passive* et *off*. Si le commutateur exécute le LACP en mode passif, veillez à définir le groupement sur le mode actif.

-T *timer-value*      Valeur de l'horloge du LACP (short ou long).

## Exemple 12-2 Modification d'un groupement de liens

L'exemple suivant décrit la procédure à suivre pour modifier la stratégie de groupement *video0* en L2 et activer le mode LACP actif.

```
# dladm modify-aggr -P L2 video0
# dladm modify-aggr -L active -T short video0
# dladm show-aggr
LINK      POLICY  ADDRPOLICY  LACPACTIVITY  LACPTIMER  FLAGS
video0    L2      auto        active        short      ----
```

## ▼ Procédure d'ajout d'un lien à un groupement

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Assurez-vous que le lien que vous souhaitez ajouter n'a pas d'interface IP montée sur le lien.

```
# ipadm delete-ip interface
```

### 3 Ajoutez le lien au groupement.

```
# dladm add-aggr -l link [-l link] [...] aggr
```

où *link* représente une liaison de données que vous êtes en train d'ajouter au groupement.

### 4 Effectuez d'autres tâches pour modifier la totalité de la configuration de groupement de liens après avoir ajouté des liaisons de données supplémentaires.

Par exemple, dans le cas d'une configuration illustrée dans la [Figure 12-3](#), il se peut que vous deviez ajouter ou modifier des connexions de câble et reconfigurer les commutateurs pour accueillir les liaisons de données supplémentaires. Reportez-vous à la documentation du commutateur pour effectuer les tâches de reconfiguration du commutateur.

## Exemple 12-3 Ajout d'un lien à un groupement

Cet exemple montre comment ajouter un lien au groupement video0.

```
# dladm show-link
LINK      CLASS    MTU     STATE    BRODGE    OVER
subvideo0  phys     1500    up       --        ----
subvideo1  phys     1500    up       --        ----
video0     aggr     1500    up       --        subvideo0, subvideo1
net3       phys     1500    unknown  --        ----

# ipadm delete-ip video0
# dladm add-aggr -l net3 video0
# dladm show-link
LINK      CLASS    MTU     STATE    BRIDGE    OVER
subvideo0  phys     1500    up       --        ----
subvideo1  phys     1500    up       --        ----
video0     aggr     1500    up       --        subvideo0, subvideo1, net3
net3       phys     1500    up       --        ----
```



## ▼ Procédure de suppression d'un lien dans un groupement

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Supprimez un lien du groupement.

```
# dladm remove-aggr -l link aggr-link
```

#### Exemple 12–4 Suppression d'un lien d'un groupement

Cet exemple montre comment supprimer un lien du groupement video0.

```
dladm show-link
LINK          CLASS      MTU      STATE    OVER
subvideo0     phys      1500    up       --       ----
subvideo1     phys      1500    up       --       ----
video0        aggr      1500    up       --       subvideo0, subvideo1, net3
net3          phys      1500    up       --       ----

# dladm remove-aggr -l net3 video0
# dladm show-link
LINK          CLASS      MTU      STATE    BRIDGE    OVER
subvideo0     phys      1500    up       --       ----
subvideo1     phys      1500    up       --       ----
video0        aggr      1500    up       --       subvideo0, subvideo1
net3          phys      1500    unknown --       ----
```

## ▼ Procédure de suppression d'un groupement

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Supprimez l'interface IP qui est configurée sur le groupement.

```
# ipadm delete-ip IP-aggr
```

où *IP-aggr* est l'interface IP sur le groupement de liens.

### 3 Supprimez le groupement de liens.

```
# dladm delete-aggr aggr
```

### **Exemple 12-5**    Suppression d'un groupement

Cet exemple supprime le groupement `video0`. La suppression est persistante.

```
# ipadm delete-ip video0  
# dladm delete-aggr video0
```

# Administration des réseaux locaux virtuels

---

Ce chapitre décrit les procédures de configuration et de maintenance des réseaux locaux virtuels (VLAN). Les procédures incluent des étapes qui utilisent les fonctionnalités telles que la prise en charge des noms de liaisons flexibles.

## Administration de réseaux locaux virtuels

Un *réseau local virtuel* (*Virtual Local Network, VLAN*) est une sous-division d'un réseau local située sur la couche de liaison de données de la pile du protocole TCP/IP. Vous pouvez créer des VLAN pour tout réseau local utilisant la technologie de commutation. L'assignation de groupes d'utilisateurs à des VLAN permet d'améliorer l'administration et la sécurité du réseau local entier. Vous pouvez également assigner les interfaces d'un même système à des VLAN différents.

La création de VLAN est utile dans les cas suivants :

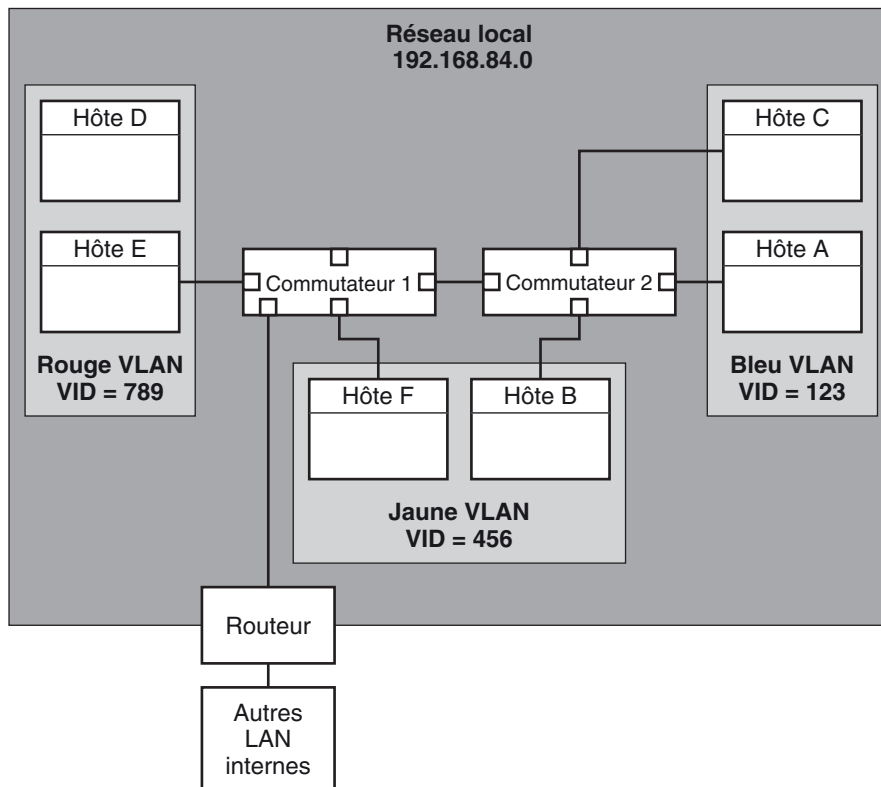
- Création de divisions logiques de groupes de travail  
Supposons par exemple que tous les hôtes d'un étage d'un immeuble sont connectés à un réseau local commuté. Vous pouvez dans ce cas créer un VLAN distinct pour chaque groupe de travail de cet étage.
- Application de stratégies de sécurité différentes selon les groupes de travail  
Par exemple, les besoins en matière de sécurité varient considérablement entre un service financier et un service informatique. Si les systèmes de ces deux services partagent le même réseau local, vous pouvez alors créer un VLAN distinct pour chaque service et appliquer la stratégie de sécurité qui convient à chaque VLAN.
- Division de groupes de travail en domaines de diffusion gérables  
Les VLAN réduisent la taille des domaines de diffusion et améliorent ainsi l'efficacité du réseau.

## Présentation de la topologie du VLAN

La technologie de commutation du réseau local permet d'organiser les systèmes d'un réseau local en plusieurs VLAN. Pour diviser un réseau local en VLAN, vous devez obtenir des commutateurs qui prennent en charge la technologie de réseau local virtuel. Vous pouvez configurer tous les ports d'un commutateur de manière à ce qu'ils servent un VLAN unique ou plusieurs VLAN (selon la topologie du réseau). La configuration des ports d'un commutateur varie en fonction du fabricant de ce dernier.

La figure suivante illustre un réseau local dont l'adresse de sous-réseau est 192.168.84.0. Ce réseau local est divisé en trois VLAN (rouge, jaune et bleu).

FIGURE 13-1 Réseau local avec trois VLAN

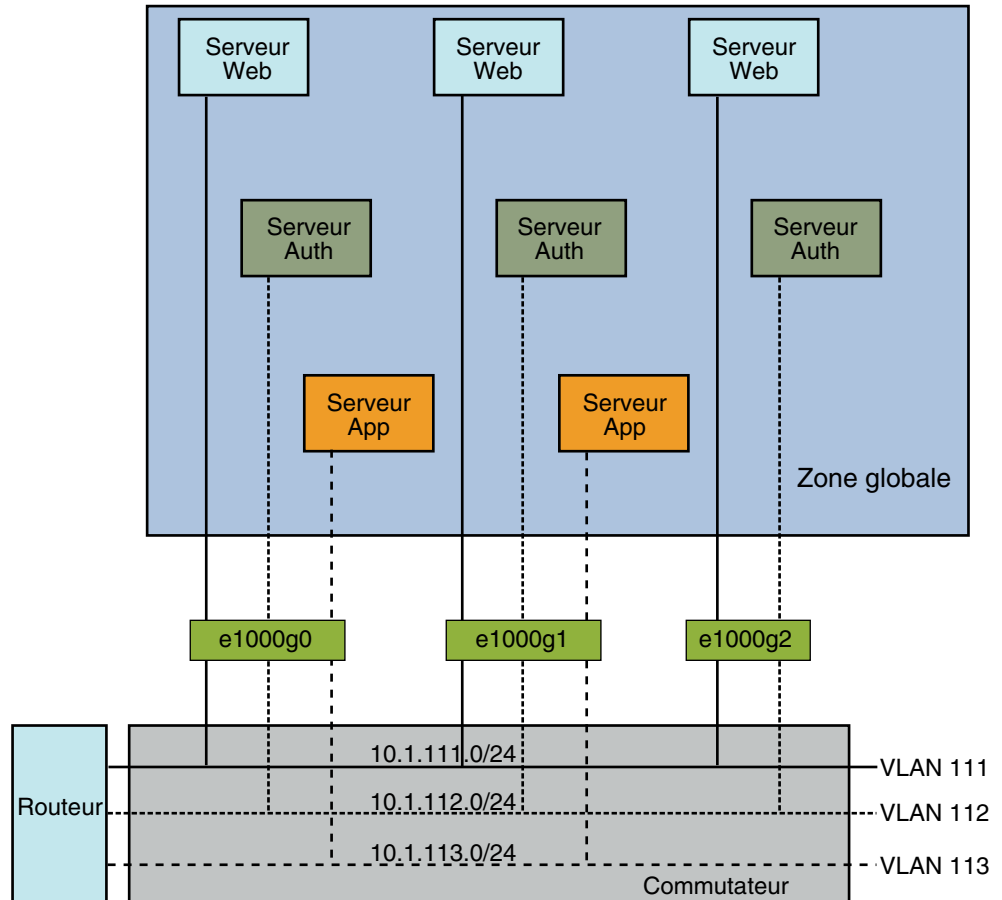


La connectivité sur le LAN 192.168.84.0 est gérée par les commutateurs 1 et 2. Le VLAN rouge contient des systèmes dans le groupe de travail de la comptabilité, ceux des ressources humaines au VLAN jaune. Les systèmes du groupe de travail des technologies de l'information sont assignés au VLAN bleu.

## Consolidation du réseau à l'aide de VLAN

Les VLAN sur les zones permettent également de configurer plusieurs réseaux virtuels au sein d'une seule unité de réseau comme un commutateur. Prenons l'illustration suivante d'un système avec trois NIC physiques :

FIGURE 13-2 Système comportant plusieurs VLAN



Sans VLAN, vous devez configurer différents systèmes pour qu'ils exécutent des fonctions spécifiques et connectez ces systèmes à des réseaux distincts. Par exemple, les serveurs web seraient connectés à un réseau local, les serveurs d'authentification à un autre et les serveurs d'application à un troisième réseau. Avec les VLAN et les zones, vous pouvez réduire les huit systèmes et les configurer en tant que zones dans un système unique. Ensuite, utilisez des balises

VLAN ou des ID de VLAN (VID) pour affecter un VLAN à chaque ensemble de zones qui effectue les mêmes fonctions. Les informations fournies dans la figure peuvent être classées comme suit :

Fonction	Nom de zone	Nom de VLAN	VID	Adresse IP	NIC
Serveur Web	webzone1	web1	111	10.1.111.0	e1000g0
Serveur d'authentification	authzone1	auth1	112	10.1.112.0	e1000g0
Serveur d'applications	appzone1	app1	113	10.1.113.0	e1000g0
Serveur Web	webzone2	web2	111	10.1.111.0	e1000g1
Serveur d'authentification	authzone2	auth2	112	10.1.112.0	e1000g1
Serveur d'applications	appzone2	app2	113	10.1.113.0	e1000g1
Serveur Web	webzone3	web3	111	10.1.111.0	e1000g2
Serveur d'authentification	authzone3	auth3	112	10.1.112.0	e1000g2

Pour créer la configuration illustrée dans la figure, reportez-vous à l'[Exemple 13–1](#).

### Noms significatifs pour les VLAN

Dans Oracle Solaris, vous pouvez affecter des noms significatifs aux interfaces VLAN. Les noms de VLAN sont constitués d'un nom de lien et du numéro de VID, par exemple, `sales0`. Vous devez attribuer des noms personnalisés lorsque vous créez des VLAN. Pour plus d'informations sur les noms personnalisés, reportez-vous à la section [“Noms des périphériques réseau et des liaisons de données” à la page 26](#). Pour plus d'informations sur les noms personnalisés valides, reportez-vous à la section [“Règles applicables aux noms de lien valides” à la page 30](#).

## Administration de VLAN (liste des tâches)

Le tableau ci-dessous contient des liens vers les différentes tâches d'administration des VLAN.

Tâche	Description	Voir
Planification d'un réseau local virtuel (VLAN)	Réalisez les tâches de planification requises avant la création du VLAN.	<a href="#">“Procédure de planification de la configuration de VLAN” à la page 255</a>

Tâche	Description	Voir
Configuration d'un VLAN	Créez des VLAN sur votre réseau.	<a href="#">“Procédure de configuration d'un VLAN” à la page 256</a>
Configuration d'un VLAN sur un groupement	Déployez des technologies combinées qui associent les VLAN et les groupements de liens.	<a href="#">“Configuration de réseaux VLAN via un groupement de liens” à la page 259</a>
Affichage des informations concernant le VLAN	Obtenez des informations sur un VLAN et ses composants.	<a href="#">“Procédure d'affichage des informations du VLAN” à la page 261</a>
Suppression d'un VLAN	Sélectionnez un VLAN à supprimer parmi plusieurs VLAN configurés sur une liaison de données.	<a href="#">“Procédure de suppression d'un VLAN” à la page 262</a>

## Planification de plusieurs VLAN sur un réseau

Pour planifier la configuration des VLAN de votre réseau, suivez la procédure ci-dessous :

### ▼ Procédure de planification de la configuration de VLAN

- 1 **Observez la topologie du réseau local et déterminez les emplacements appropriés pour créer des VLAN.**

La [Figure 13–1](#) illustre un exemple simple de topologie de réseau.

- 2 **Créez un schéma de numérotation pour les VID et assignez un VID à chaque VLAN.**

---

**Remarque** – Votre réseau dispose peut-être déjà d'un tel schéma de numérotation. Dans ce cas, créez des VID compris dans le schéma de numérotation existant.

---

- 3 **Sur chaque système, déterminez quelles interfaces seront membres de quel VLAN.**

- a. **Déterminez les interfaces configurées sur un système.**

```
# dladm show-link
```

- b. **Déterminez les VID associés aux liaisons de données du système.**

- c. **Créez le VLAN à l'aide de la commande `dladm create-vlan`.**

- 4 **Vérifiez les connexions des interfaces sur les commutateurs du réseau.**

Notez le VID de chaque interface ainsi que le port du commutateur auquel elle est connectée.

- 5 **Configurez chaque port du commutateur avec le même VID que celui de l'interface à laquelle il est connecté.**

Reportez-vous aux instructions fournies par le fabricant du commutateur pour de plus amples informations sur la configuration.

## Configuration des VLAN

La procédure suivante décrit comment créer et configurer un réseau VLAN. Dans Oracle Solaris, tous les périphériques Ethernet prennent en charge les VLAN. Cependant, certaines restrictions existent avec certains périphériques. Pour connaître ces exceptions, reportez-vous à la section “[VLAN sur les périphériques hérités](#)” à la page 260.

### ▼ Procédure de configuration d'un VLAN

#### Avant de commencer

Des liaisons de données doivent déjà être configurées dans votre système avant de pouvoir créer des VLAN. Reportez-vous à la section “[Configuration d'une interface IP](#)” à la page 183.

- 1 **Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Déterminez les types de liens utilisés sur votre système.**

```
# dladm show-link
```

- 3 **Créez un lien de VLAN sur une liaison de données.**

```
# dladm create-vlan -l link -v VID vlan-link
```

*link*                Spécifie le lien sur lequel l'interface de VLAN est créée.

*VID*                Indique le numéro d'ID d'un VLAN

*vlan-link*        Spécifie le nom du VLAN, qui peut également être un nom choisi par l'administrateur.

- 4 **Vérifiez la configuration du VLAN.**

```
# dladm show-vlan
```

- 5 **Créez une interface IP sur le VLAN.**

```
# ipadm create-ip interface
```

où *interface* utilise le nom du VLAN.

- 6 **Configurez l'interface IP à l'aide d'une adresse IP.**

```
# ipadm create-addr -T static -a IP-address addrobj
```

où *addrobj* utilise la convention d'attribution de nom *interface/user-defined-string*.



### Exemple 13–1 Configuration d'un VLAN

Cet exemple crée la configuration de VLAN illustrée dans la [Figure 13–2](#). Cet exemple suppose que vous avez déjà configuré les différentes zones du système. Pour plus d'informations sur la configuration des zones, reportez-vous à la section [Partie II, “Oracle Solaris Zones” du manuel Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources](#).

```
global# dladm show-link
LINK          CLASS    MTU    STATE    BRIDGE    OVER
e1000g0       phys     1500   up       --        --
e1000g1       phys     1500   up       --        --
e1000g2       phys     1500   up       --        --

global# dladm create-vlan -l e1000g0 -v 111 web1
global# dladm create-vlan -l e1000g0 -v 112 auth1
global# dladm create-vlan -l e1000g0 -v 113 app1
global# dladm create-vlan -l e1000g1 -v 111 web2
global# dladm create-vlan -l e1000g1 -v 112 auth2
global# dladm create-vlan -l e1000g1 -v 113 app2
global# dladm create-vlan -l e1000g2 -v 111 web3
global# dladm create-vlan -l e1000g2 -v 112 auth3

global# dladm show-vlan
LINK    VID    OVER    FLAGS
web1    111    e1000g0  ----
auth1    112    e1000g0  ----
app1    113    e1000g0  ----
web2    111    e1000g1  ----
auth2    112    e1000g1  ----
app2    113    e1000g1  ----
web3    111    e1000g2  ----
auth3    113    e1000g2  ----
```

Lorsque les informations de lien s'affichent, les VLAN sont inclus dans la liste.

```
global# dladm show-link
LINK          CLASS    MTU    STATE    BRIDGE    OVER
e1000g0       phys     1500   up       --        --
e1000g1       phys     1500   up       --        --
e1000g2       phys     1500   up       --        --
web1          vlan     1500   up       --        e1000g0
auth1         vlan     1500   up       --        e1000g0
app1          vlan     1500   up       --        e1000g0
web2          vlan     1500   up       --        e1000g1
auth2         vlan     1500   up       --        e1000g1
app2          vlan     1500   up       --        e1000g1
web3          vlan     1500   up       --        e1000g2
auth3         vlan     1500   up       --        e1000g2
```

Les VLAN sont assignés à leurs zones respectives. Par exemple, lorsque vous recherchez des informations de réseau pour des zones individuelles, des données similaires à ce qui suit s'affichent pour chaque zone :

```
global# zonecfg -z webzone1 info net
net:
    address not specified
    physical: web1

global# zonecfg -z authzone1 info net
net:
    address not specified
    physical: auth1

global# zonecfg -z appzone2 info net
net:
    address not specified
    physical: app2
```

La valeur de la propriété `physical` indique le VLAN défini pour la zone donnée.

Connectez-vous à chaque zone non globale pour configurer le VLAN à l'aide d'une adresse IP.

Dans `webzone1` :

```
webzone1# ipadm create-ip web1
webzone1# ipadm create-addr -T static -a 10.1.111.0/24 web1/v4
```

Dans `webzone2` :

```
webzone2# ipadm create-ip web2
webzone2# ipadm create-addr -T static -a 10.1.111.0/24 web2/v4
```

Dans `webzone3` :

```
webzone3# ipadm create-ip web3
webzone3# ipadm create-addr -T static -a 10.1.111.0/24 web3/v4
```

Dans `authzone1` :

```
authzone1# ipadm create-ip auth1
authzone1# ipadm create-addr -T static -a 10.1.112.0/24 auth1/v4
```

Dans `authzone2` :

```
authzone2# ipadm create-ip auth2
authzone2# ipadm create-addr -T static -a 10.1.112.0/24 auth2/v4
```

Dans `authzone3` :

```
authzone3# ipadm create-ip auth3
authzone3# ipadm create-addr -T static -a 10.1.112.0/24 auth3/v4
```

Dans `appzone1` :

```
appzone1# ipadm create-ip app1
appzone1# ipadm create-addr -T static -a 10.1.113.0/24 app1/v4
```

Dans appzone2 :

```
appzone2# ipadm create-ip app2
appzone2# ipadm create-addr -T static -a 10.1.113.0/24 app2/v4
```

## ▼ Configuration de réseaux VLAN via un groupement de liens

De la même manière que vous configurez des réseaux VLAN par le biais d'une interface, vous pouvez également créer des VLAN via un groupement de liens. Les groupements de liens sont décrits dans le [Chapitre 12, “Administration de groupements de liens”](#). Cette section décrit la configuration des réseaux VLAN et les groupements de liens.

### Avant de commencer

Créez d'abord le groupement de liens et configurez-le avec une adresse IP valide. Pour créer des groupements de liens, reportez-vous à la section “[Procédure de création d'un groupement de liens](#)” à la page 245.

#### 1 Répertoriez les groupements qui sont configurés dans le système.

```
# dladm show-link
```

#### 2 Pour chaque VLAN que vous souhaitez créer sur le groupement, exécutez la commande suivante.

```
# dladm create-vlan -l link -v VID vlan-link
```

où

*link* Spécifie le lien sur lequel l'interface de VLAN est créée. Dans ce cas spécifique, le lien fait référence au groupement de liens.

*VID* Indique le numéro d'ID d'un VLAN

*vlan-link* Spécifie le nom du VLAN, qui peut également être un nom choisi par l'administrateur.

#### 3 Créez des interfaces IP sur les VLAN.

```
# ipadm create-ip interface
```

où *interface* utilise le nom du VLAN.

#### 4 Configurez les interfaces IP sur les VLAN avec des adresses IP valides.

```
# ipadm create-addr -T static -a IP-address addrobj
```

où *addrobj* doit utiliser la convention d'attribution de nom *vlan-int/user-defined-string*

**Exemple 13-2** Configuration de plusieurs réseaux locaux virtuels via un groupement de liens

Dans cet exemple, deux réseaux VLAN sont configurés sur un groupement de liens. Les identifiants VLAN (VID) 193 et 194 sont respectivement assignés aux réseaux VLAN.

```
# dladm show-link
LINK          CLASS      MTU      STATE      BRIDGE      OVER
subvideo0     phys       1500     up         --          ----
subvideo1     phys       1500     up         --          ----
video0        aggr       1500     up         --          subvideo0, subvideo1

# dladm create-vlan -l video0 -v 193 salesregion1
# dladm create-vlan -l video0 -v 194 salesregion2

# ipadm create-ip salesregion1
# ipadm create-ip salesregion2

# ipadm create-addr -T static -a 192.168.10.5/24 salesregion1/v4static
# ipadm create-addr -T static -a 192.168.10.25/24 salesregion2/v4static
```

## VLAN sur les périphériques hérités

Certains périphériques hérités gèrent uniquement les paquets dont la taille de trame maximale est de 1514 octets. Les paquets dont la taille de l'image dépasse la limite maximale sont refusés. Pour de tels cas, suivez la procédure décrite à la section [“Procédure de configuration d'un VLAN” à la page 256](#). Toutefois, lors de la création du VLAN, utilisez l'option -f pour forcer la création du VLAN.

La procédure générale à suivre est la suivante :

1. Créez le VLAN avec l'option -f.

```
# dladm create-vlan -f -l link -v VID [vlan-link]
```

2. Définissez une taille inférieure pour l'unité de transmission maximale (MTU), 1496 octets par exemple.

```
# dladm set-linkprop -p default_mtu=1496 vlan-link
```

La valeur inférieure de MTU permet de réserver de l'espace pour la couche de liaison pour insérer l'en-tête de VLAN avant la transmission.

3. Effectuez la même procédure pour définir la même valeur inférieure de taille de MTU pour chaque nœud dans le VLAN.

Pour plus d'informations sur la modification des valeurs de propriété de lien, reportez-vous à la section [“Configuration des liaisons de données \(tâches\)” à la page 157](#).

## Autres tâches d'administration sur les VLAN

Cette section décrit l'utilisation des nouvelles sous-commandes d'adm pour les autres tâches de VLAN. Ces commandes d'adm fonctionnent également avec les noms de lien.

### ▼ Procédure d'affichage des informations du VLAN

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

#### 2 Affichez les informations concernant le VLAN.

```
# dladm show-vlan [vlan-link]
```

Si vous ne spécifiez pas de lien VLAN, la commande affiche des informations sur tous les VLAN configurés.

### Exemple 13–3 Affichage des informations du VLAN

L'exemple suivant est basé sur le système doté de plusieurs VLAN illustré par la [Figure 13–2](#) et montre les VLAN disponibles dans le système.

```
# dladm show-vlan
LINK      VID      OVER      FLAGS
web1      111      e1000g0   ----
auth1     112      e1000g0   ----
app1      113      e1000g0   ----
web2      111      e1000g1   ----
auth2     112      e1000g1   ----
app2      113      e1000g1   ----
web3      111      e1000g2   ----
auth3     113      e1000g2   ----
```

Les VLAN configurés s'affichent également lors de l'exécution de la commande d'adm show-link. Dans la sortie de commande, les VLAN sont identifiés dans la colonne CLASS.

```
# dladm show-link
LINK      CLASS    MTU      STATE    BRIDGE    OVER
e1000g0   phys     1500     up       --        --
e1000g1   phys     1500     up       --        --
e1000g2   phys     1500     up       --        --
web1      vlan     1500     up       --        e1000g0
auth1     vlan     1500     up       --        e1000g0
app1      vlan     1500     up       --        e1000g0
web2      vlan     1500     up       --        e1000g1
auth2     vlan     1500     up       --        e1000g1
app2      vlan     1500     up       --        e1000g1
web3      vlan     1500     up       --        e1000g2
auth3     vlan     1500     up       --        e1000g2
```

## ▼ Procédure de suppression d'un VLAN

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Déterminez le VLAN que vous souhaitez supprimer.

```
# dladm show-vlan
```

### 3 Démontez l'interface IP du VLAN.

```
# ipadm delete-ip vlan-interface
```

où *vlan-interface* est l'interface IP qui est configurée sur le VLAN.

---

**Remarque** – Vous ne pouvez pas supprimer un VLAN qui est en cours d'utilisation.

---

### 4 Supprimez le VLAN en suivant l'une des procédures suivantes :

- Pour supprimer le VLAN temporairement, utilisez l'option `-t` comme suit :

```
# dladm delete-vlan -t vlan
```

- Pour que la suppression soit persistante, procédez comme suit :

- a. Supprimez le VLAN.

```
# dladm delete-vlan vlan
```

## Exemple 13–4 Suppression d'un VLAN

```
# dladm show-vlan
LINK      VID      OVER      FLAGS
web1      111      e1000g0   ----
auth1     112      e1000g0   ----
app1      113      e1000g0   ----
web2      111      e1000g1   ----
auth2     112      e1000g1   ----
app2      113      e1000g1   ----
web3      111      e1000g2   ----
auth3     113      e1000g2   ----

# ipadm delete-ip web1
# dladm delete-vlan web1
```

## Association de tâches de configuration réseau et utilisation de noms personnalisés

Cette section fournit un exemple qui combine toutes les procédures décrites dans les chapitres précédents à propos de la configuration de liens, de groupements de liens et de VLAN tout en utilisant des noms personnalisés. Pour obtenir une description des autres scénarios de mise en réseau qui utilisent des noms personnalisés, consultez l'article à l'adresse <http://www.oracle.com/us/sun/index.htm>.

### EXEMPLE 13-5 Configuration de liens, de VLAN et de groupements de liens

Dans cet exemple, un système qui utilise 4 NIC doit être configuré afin d'être un routeur pour 8 sous-réseaux séparés. Pour atteindre cet objectif, 8 liens seront configurés, un pour chaque sous-réseau. Tout d'abord, un groupement de liens est créé sur les 4 NIC. Ce lien non marqué devient le sous-réseau non marqué par défaut pour le réseau vers lequel pointe le routage par défaut.

Ensuite, les interfaces de VLAN sont configurées sur le groupement de liens pour les autres sous-réseaux. Les sous-réseaux sont nommés suivant un plan de code de couleurs. En conséquence, les noms de VLAN sont également nommés afin de correspondre à leurs sous-réseaux respectifs. La configuration finale comporte 8 liens pour les 8 sous-réseaux : 1 lien non marqué et 7 liens de VLAN marqués.

Pour conserver les configurations après les redémarrages, les mêmes procédures s'appliquent comme dans les versions précédentes d'Oracle Solaris. Par exemple, les adresses IP doivent être ajoutées aux fichiers de configuration comme `/etc/inet/ndpd.conf`. Ou encore, les règles de filtrage pour les interfaces doivent être incluses dans un fichier de règles. Ces dernières étapes ne sont pas incluses dans l'exemple. Pour obtenir des informations sur ces étapes, consultez les chapitres correspondants du document *Administration d'Oracle Solaris : Services IP*, en particulier *TCP/IP Administration* et *DHCP*.

```
# dladm show-link
LINK          CLASS      MTU  STATE  BRIDGE  OVER
nge0          phys      1500  up     --      --
nge1          phys      1500  up     --      --
e1000g0       phys      1500  up     --      --
e1000g1       phys      1500  up     --      --

# dladm show-phys
LINK          MEDIA      STATE  SPEED  DUPLEX  DEVICE
nge0          Ethernet  up     1000Mb full   nge0
nge1          Ethernet  up     1000Mb full   nge1
e1000g0       Ethernet  up     1000Mb full   e1000g0
e1000g1       Ethernet  up     1000Mb full   e1000g1

# ipadm delete-ip nge0
# ipadm delete-ip nge1
# ipadm delete-ip e1000g0
```

## EXEMPLE 13-5 Configuration de liens, de VLAN et de groupements de liens (Suite)

```
# ipadm delete-ip e1000g1

# dladm rename-link nge0 net0
# dladm rename-link nge1 net1
# dladm rename-link e1000g0 net2
# dladm rename-link e1000g1 net3

# dladm show-link
LINK      CLASS      MTU  STATE  BRIDGE  OVER
net0      phys      1500  up    --      --
net1      phys      1500  up    --      --
net2      phys      1500  up    --      --
net3      phys      1500  up    --      --

# dladm show-phys
LINK      MEDIA          STATE      SPEED  DUPLEX  DEVICE
net0      Ethernet      up        1000Mb full   nge0
net1      Ethernet      up        1000Mb full   nge1
net2      Ethernet      up        1000Mb full   e1000g0
net3      Ethernet      up        1000Mb full   e1000g1

# dladm create-aggr -P L2,L3 -l net0 -l net1 -l net2 -l net3 default0

# dladm show-link
LINK      CLASS      MTU  STATE  BRIDGE  OVER
net0      phys      1500  up    --      --
net1      phys      1500  up    --      --
net2      phys      1500  up    --      --
net3      phys      1500  up    --      --
default0  aggr      1500  up    --      net0 net1 net2 net3

# dladm create-vlan -v 2 -l default0 orange0
# dladm create-vlan -v 3 -l default0 green0
# dladm create-vlan -v 4 -l default0 blue0
# dladm create-vlan -v 5 -l default0 white0
# dladm create-vlan -v 6 -l default0 yellow0
# dladm create-vlan -v 7 -l default0 red0
# dladm create-vlan -v 8 -l default0 cyan0

# dladm show-link
LINK      CLASS      MTU  STATE  BRIDGE  OVER
net0      phys      1500  up    --      --
net1      phys      1500  up    --      --
net2      phys      1500  up    --      --
net3      phys      1500  up    --      --
default0  aggr      1500  up    --      net0 net1 net2 net3
orange0   vlan      1500  up    --      default0
green0    vlan      1500  up    --      default0
blue0     vlan      1500  up    --      default0
white0    vlan      1500  up    --      default0
yellow0   vlan      1500  up    --      default0
red0      vlan      1500  up    --      default0
cyan0     vlan      1500  up    --      default0

# dladm show-vlan
```



**EXEMPLE 13-5** Configuration de liens, de VLAN et de groupements de liens (Suite)

LINK	VID	OVER	FLAGS
orange0	2	default0	----
green0	3	default0	----
blue0	4	default0	----
white0	5	default0	----
yellow0	6	default0	----
red0	7	default0	----
cyan0	8	default0	----

```
# ipadm create-ip orange0
# ipadm create-ip green0
# ipadm create-ip blue0
# ipadm create-ip white0
# ipadm create-ip yellow0
# ipadm create-ip red0
# ipadm create-ip cyan0

# ipadm create-addr -T static -a IP-address orange0/v4
# ipadm create-addr -T static -a IP-address green0/v4
# ipadm create-addr -T static -a IP-address blue0/v4
# ipadm create-addr -T static -a IP-address white0/v4
# ipadm create-addr -T static -a IP-address yellow0/v4
# ipadm create-addr -T static -a IP-address red0/v4
# ipadm create-addr -T static -a IP-address cyan0/v4
```



## Présentation d'IPMP

---

Le multipathing sur réseau IP (IPMP, IP Network Multipathing) fournit une détection des défaillances des interfaces physiques, un basculement d'accès réseau transparent et une répartition de la charge de paquets pour les systèmes dotés de plusieurs interfaces qui sont connectés à un réseau local (LAN) particulier.

Le présent chapitre contient les informations suivantes :

- “Nouveautés d'IPMP ” à la page 267
- “Déploiement d'IPMP” à la page 268
- “Composants IPMP dans Oracle Solaris” à la page 278
- “Types de configurations d'interface IPMP” à la page 279
- “Adressage IPMP” à la page 280
- “Détection de défaillance et de réparation dans IPMP ” à la page 281
- “IPMP et reconfiguration dynamique” à la page 286
- “Terminologie et concepts IPMP” à la page 288

---

**Remarque** – Tout au long de la description d'IPMP dans ce chapitre et dans le [Chapitre 15, “Administration d'IPMP”](#), toutes les références au terme *interface* signifient *interface IP*. A moins qu'un processus de qualification n'indique explicitement une autre utilisation du terme, telle que carte réseau (NIC), le terme se réfère toujours à l'interface qui est configurée sur la couche IP.

---

## Nouveautés d'IPMP

Les fonctions suivantes différencient l'implémentation actuelle d'IPMP de l'implémentation précédente :

- Un groupe IPMP est représenté comme une interface IP IPMP. Cette interface est considérée comme n'importe quelle autre interface de la couche IP de la pile réseau. Toutes les tâches administrative IP, tables de routage, tables protocole de résolution d'adresse (ARP), règles de pare-feu et autres procédures liées aux IP fonctionnent avec un groupe IPMP faisant référence à l'interface IPMP.
- Le système devient responsable de la distribution d'adresses de données entre les interfaces actives sous-jacentes. Dans la précédente implémentation d'IPMP, l'administrateur détermine initialement la liaison d'adresses de données aux interfaces correspondantes lorsque le groupe IPMP est créé. Dans l'implémentation actuelle, lorsque le groupe IPMP est créé, les adresses de données appartiennent à l'interface IPMP sous forme de pool d'adresses. Le noyau lie alors automatiquement et aléatoirement les adresses de données aux interfaces actives sous-jacentes du groupe.
- L'outil `ipmpstat` est présenté comme l'outil principal pour obtenir plus d'informations sur les groupes IPMP. Cette commande fournit des informations sur tous les aspects de la configuration d'IPMP, tels que les interfaces IP sous-jacentes du groupe, les adresses de données et de test, les types de détection de défaillance en cours d'utilisation, et les interfaces qui ont échoué. Les fonctions `ipmpstat`, les options que vous pouvez utiliser et les sorties que chaque option génère sont toutes décrites dans [“Contrôle des informations d'IPMP” à la page 319](#).
- L'interface IPMP peut se voir attribuer un nom personnalisé pour identifier le groupe IPMP plus facilement dans votre configuration réseau. Pour les procédures à suivre pour configurer les groupes IPMP avec des noms personnalisés, reportez-vous à n'importe quelle procédure décrivant la création d'un groupe IPMP dans [“Configuration de groupes IPMP” à la page 302](#).

---

**Remarque** – Pour utiliser IPMP, assurez-vous que le `DefaultFixed` est activé sur le système. Pour plus d'informations sur les procédures, reportez-vous à la section [“Profils et des outils de configuration” à la page 154](#). Pour plus d'informations sur la configuration réseau géré par profil, reportez-vous au [Chapitre 4, “Configuration de profil NWAM \(tâches\)”](#).

---

## Déploiement d'IPMP

Cette section décrit différents sujets sur l'utilisation de groupes IPMP.

### Avantages d'IPMP

Différents facteurs peuvent faire qu'une interface devient inutilisable. Généralement, une interface IP peut échouer. Ou, une interface peut être mis hors ligne pour maintenance matérielle. Dans de tels cas, sans un groupe IPMP, le système ne peut plus être contacté à l'aide d'une des adresses IP qui sont associés à cette interface inutilisable. En outre, les connexions existantes qui utilisent ces adresses IP sont interrompues.

Avec IPMP, une ou plusieurs interfaces IP peuvent être configurées dans un *groupe IPMP*. Le groupe fonctionne comme une interface IP avec des adresses de données pour envoyer ou recevoir le trafic réseau. Si une interface sous-jacente dans le groupe échoue, les adresses de données sont réparties entre les autres interfaces actives sous-jacentes du groupe. Ainsi, le groupe permet de maintenir la connectivité réseau malgré un échec de l'interface. Avec IPMP, la connectivité réseau est toujours disponible, à condition qu'au moins une interface soit utilisable pour le groupe.

En outre, IPMP répartit le trafic réseau sortant sur l'ensemble des interfaces du groupe IPMP, ce qui permet d'améliorer les performances réseau globales. On parle de *répartition de charge* sortante. De plus, le système contrôle indirectement la répartition de charge entrante en effectuant une sélection des adresses source pour les paquets dont l'adresse IP source n'a pas été spécifiée par l'application. Cependant, si l'application a explicitement choisi une adresse IP source, le système ne doit pas en changer.

## Quand utiliser IPMP

La configuration d'un groupe IPMP est déterminée par vos configurations système. Respectez les règles suivantes :

- Plusieurs interfaces IP sur le même réseau local ou LAN doivent être configurées dans un groupe IPMP. Le terme LAN fait référence de manière général à une variété de configurations réseau locales, dont les VLAN (réseaux locaux virtuels) et les réseaux locaux avec et sans fil dont les noeuds appartiennent au *même domaine de diffusion de couche liaison*.

---

**Remarque** – Si plusieurs groupes IPMP appartiennent au même domaine de diffusion (L2), ces groupes ne sont pas pris en charge. Un domaine de diffusion L2 est généralement mappé à un sous-réseau spécifique. Par conséquent, vous ne devez configurer qu'un seul groupe IPMP par sous-réseau.

---

- Les interfaces IP sous-jacentes d'un groupe IPMP ne doivent pas s'étendre sur plusieurs réseaux locaux.

Par exemple, supposons qu'un système avec trois interfaces est connecté à deux LAN séparés. Deux interfaces IP sont liées à un LAN alors qu'une interface IP unique se connecte à l'autre. Dans ce cas, les deux interfaces IP se connectant au premier LAN doivent être configurées en tant que groupe IPMP, comme requis par la première règle. En conformité avec la deuxième règle, l'interface IP unique qui se connecte au second LAN ne peut pas devenir membre de ce groupe IPMP. Aucune configuration d'IPMP n'est requise pour l'interface IP unique. Cependant, vous pouvez configurer l'interface unique au sein d'un groupe IPMP pour surveiller la disponibilité de l'interface. La configuration IPMP à interface unique est abordée plus en détail dans la section [“Types de configurations d'interface IPMP” à la page 279](#).

Prenons un autre cas où le lien vers le premier LAN se compose de trois interfaces IP alors que l'autre lien se compose de deux interfaces. Cette installation requiert la configuration de deux groupes IPMP : un groupe à trois interfaces qui effectue un lien vers le premier LAN et un groupe à deux interfaces pour connecter au second.

## Comparaison d'IPMP et du groupement de liens

IPMP et le groupement de liens sont des technologies différentes pour obtenir une amélioration des performances du réseau, ainsi que maintenir la disponibilité du réseau. En général, vous pouvez déployer le groupement de liens pour obtenir de meilleures performances du réseau, tandis que vous utilisez IPMP afin d'assurer une haute disponibilité.

Le tableau suivant présente une comparaison générale entre le groupement de liens et IPMP.

	IPMP	Groupement de liens
Type de technologie réseau	Couche 3 (couche IP)	Couche 2 (couche de liaison)
Outil de configuration	ipadm	dladm
Détection de défaillance basée sur les liaisons	Pris en charge	Pris en charge
Détection de défaillance basée sur sonde	Basé sur ICMP, ciblant n'importe quel système défini dans le même sous-réseau IP en tant qu'adresses de test, sur plusieurs niveaux de commutateurs de couche 2 qui suivent.	Basé sur le protocole LACP (Link Aggregation Control Protocol), cible l'hôte ou le commentateur pair le plus proche.
Utilisation d'interfaces de réserve	Pris en charge	Non pris en charge
Extension sur plusieurs commutateurs	Pris en charge	Généralement non pris en charge ; certains fournisseurs proposent des solutions propriétaires et non interopérables pour s'étendre sur plusieurs commutateurs.
Support matériel	Non requis	Requis Par exemple, un groupement de liens dans le système qui exécute Oracle Solaris nécessite que les ports correspondant aux commutateurs soient également groupés.
Couche de liaison requise	Prenant en charge la diffusion	Spécifique à Ethernet
Structure de pilotes requise	Aucun	Doit utiliser une structure GLDv3

	IPMP	Groupe de liens
Prise en charge de la répartition de charge	Présente, contrôlée par noyau. La répartition de charge entrante est indirectement affectée par sélection des adresses source.	Contrôle de grain plus fin de l'administrateur sur la répartition de charge du trafic sortant à l'aide de la commande d'adm. Répartition de charge entrante prise en charge.

Dans les groupements de liens, le trafic entrant est réparti sur les liens multiples qui composent le groupement. Par conséquent, les performances réseau sont améliorées avec l'installation de plus de cartes réseau pour ajouter des liens au groupement. Le trafic d'IPMP utilise les adresses de données de l'interface IPMP alors qu'elles sont liées aux interfaces actives disponibles. Si, par exemple, tout le trafic de données circule uniquement entre deux adresses IP mais pas nécessairement sur la même connexion, alors l'ajout de plusieurs cartes réseau n'améliore pas les performances avec IPMP car seules deux adresses IP restent utilisables.

Ces deux technologies se complètent et peuvent être déployées simultanément pour fournir les avantages combinés de performance et de disponibilité du réseau. Par exemple, sauf dans les cas où des solutions propriétaires sont fournies par certains fournisseurs, les groupements de liens ne peuvent actuellement pas s'étendre sur plusieurs commutateurs. Par conséquent, un commutateur devient un point d'échec unique pour un groupement de liens entre le commutateur et un hôte. Si le commutateur tombe en panne, le groupement de liens est également perdu, et les performances réseau diminuent. Les groupes IPMP ne rencontrent pas ce problème de limitation des commutateurs. Par conséquent, dans le cas d'un LAN utilisant plusieurs commutateurs, les groupements de liens qui se connectent à leurs commutateurs respectifs peuvent être combinés en un groupe IPMP sur l'hôte. Avec cette configuration, de meilleures performances du réseau ainsi qu'une haute disponibilité sont obtenues. Dans le cas d'un commutateur en panne, les adresses de données du groupement de liens vers ce commutateur en panne redistribuées parmi les autres groupements de liens du groupe.

Pour en savoir plus sur les groupements de liens, reportez-vous au [Chapitre 12](#), “Administration de groupements de liens”.

## Utilisation de noms de liaison flexibles sur une configuration d'IPMP

Grâce à la prise en charge des noms de liaison personnalisés, la configuration de liaison n'est plus liée à la carte réseau physique à laquelle la liaison est associée. L'utilisation de noms de liaison personnalisés vous permet de disposer d'une plus grande souplesse dans les interfaces IP d'administration. Cette flexibilité s'étend également à l'administration IPMP. Si une interface sous-jacente d'un groupe IPMP échoue et qu'il nécessite un remplacement, les procédures pour remplacer l'interface sont grandement facilitées. La carte réseau de remplacement, à condition qu'il s'agisse du même type, peut être renommée pour hériter de la configuration de la carte réseau ayant échoué. Vous n'avez pas à créer de nouvelles configurations avant d'ajouter une

nouvelle interface dans le groupe IPMP. Après avoir affecté le nom de la liaison de la carte réseau ayant échoué à la nouvelle carte réseau, celle-ci est configurée avec les mêmes paramètres que l'interface défaillante. Le démon de multipathing déploie alors l'interface en fonction de la configuration IPMP des interfaces actives et de réserve.

Par conséquent, pour optimiser votre configuration réseau et faciliter l'administration d'IPMP, vous devez employer des noms de liaison flexibles pour vos interfaces en leur affectant des noms génériques. Dans la section suivante, [“Fonctionnement d'IPMP” à la page 272](#), tous les exemples utilisent des noms de liaison flexibles pour le groupe IPMP et ses interfaces sous-jacentes. Pour plus d'informations sur le processus derrière les remplacements de carte réseau dans un environnement de réseau qui utilise des noms de liaison personnalisés, reportez-vous à la section [“IPMP et reconfiguration dynamique” à la page 286](#). Pour obtenir un aperçu de la pile réseau et de l'utilisation de noms de liaison personnalisés, reportez-vous à la section [“Pile réseau dans Oracle Solaris” à la page 22](#).

## Fonctionnement d'IPMP

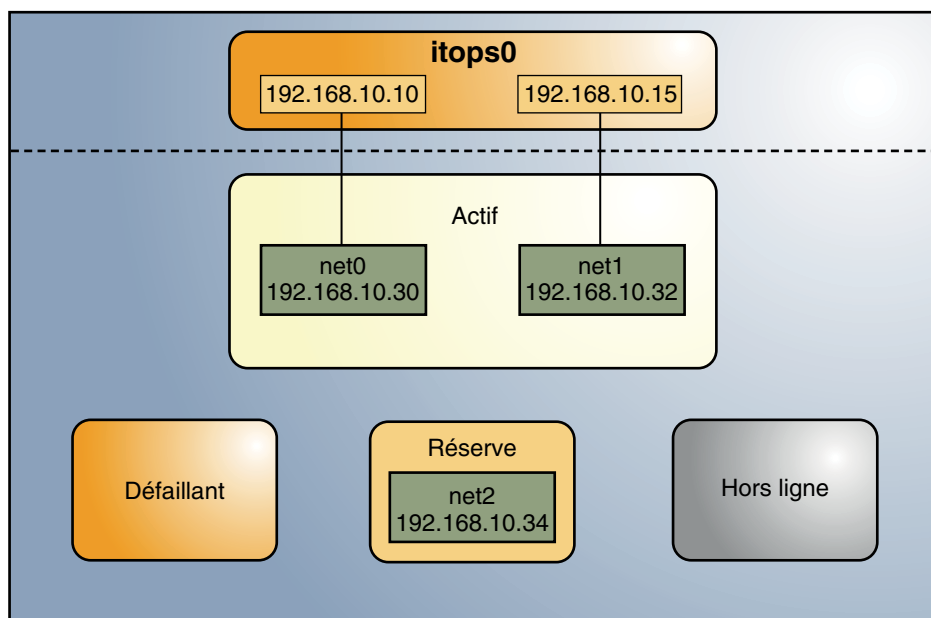
IPMP permet de maintenir la disponibilité du réseau en essayant de conserver le nombre initial d'interfaces actives et de réserve lorsque le groupe a été créé.

La détection de défaillance d'IPMP peut être basé sur les liaisons, les sondes ou les deux pour déterminer la disponibilité d'une l'interface IP sous-jacente spécifique dans le groupe. Si IPMP détermine qu'une interface sous-jacente a échoué, alors cette interface est marquée comme ayant échoué et n'est plus utilisable. L'adresse IP de données qui a été associée à l'interface défaillante est ensuite redistribuées à une autre interface opérationnelle du groupe. Si elle est disponible, une interface de réserve est également déployée pour maintenir le nombre initial d'interfaces actives.

Considérez un groupe IPMP à trois interfaces `itops0` avec une configuration active-de réserve, comme illustré dans la [Figure 14–1](#).



FIGURE 14-1 Configuration IPMP active-de réserve



Le groupe `itops0` est configuré comme suit :

- Deux adresses de données sont affectées au groupe : `192.168.10.10` et `192.168.10.15`.
- Deux interfaces sous-jacentes sont configurées en tant qu'interfaces actives et des noms de liaison flexibles leur sont affectés : `net0` et `net1`.
- Le groupe possède une interface de réserve, également avec un nom de liaison flexible : `net2`.
- La détection de défaillance par sonde est utilisée, et par conséquent les interfaces actives et de réserve sont configurées avec des adresses de test, comme suit :
  - `net0`: `192.168.10.30`
  - `net1`: `192.168.10.32`
  - `net2`: `192.168.10.34`

**Remarque** – Les zones Active, Offline, Reserve, et Failed des figures indiquent uniquement l'état des interfaces sous-jacentes, et non des emplacements physiques. Aucun mouvement physique d'interfaces ou d'adresses, ou transfert d'interfaces IP ne se produit au sein de cette implémentation d'IPMP. Les zones servent uniquement à montrer comment une interface sous-jacente change d'état suite à une panne ou une réparation.

Vous pouvez utiliser la commande `ipmpstat` avec différentes options pour afficher des types spécifiques d'informations à propos de groupes IPMP existants. Pour d'autres exemples, reportez-vous à la section [“Contrôle des informations d'IPMP” à la page 319](#).

La configuration d'IPMP dans la [Figure 14–1](#) peut être affichée en utilisant la commande `ipmpstat` suivante:

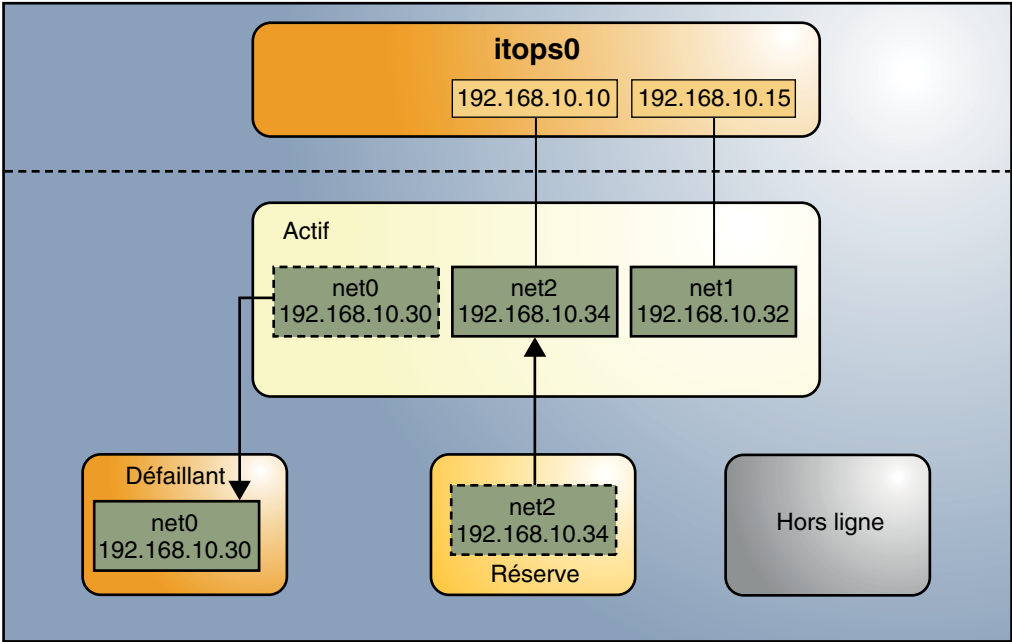
```
# ipmpstat -g
GROUP      GROUPNAME    STATE    FDT      INTERFACES
itops0     itops0       ok       10.00s   net1 net0 (net2)
```

Pour afficher des informations sur les interfaces sous-jacentes du groupe, vous devez saisir les informations suivantes :

```
# ipmpstat -i
INTERFACE  ACTIVE    GROUP    FLAGS    LINK     PROBE    STATE
net0       yes      itops0   - - - - - up       ok       ok
net1       yes      itops0   - - mb - - up       ok       ok
net2       no       itops0   is - - - - up       ok       ok
```

IPMP permet de maintenir la disponibilité du réseau en gérant les interfaces sous-jacentes afin de conserver le nombre initial d'interfaces actives. Par conséquent, si `net0` échoue, alors `net2` est déployée pour s'assurer que le groupe continue d'avoir deux interfaces actives. L'activation de `net2` apparaît dans la [Figure 14–2](#).

FIGURE 14-2 Panne d'interface dans IPMP



**Remarque** – Le mappage bi-univoque d'adresses de données sur des interfaces actives dans la [Figure 14-2](#) ne sert qu'à simplifier l'illustration. Le module de noyau IP permet d'affecter des adresses de données au hasard sans nécessairement adhérer à une relation bi-univoque entre des adresses de données et des interfaces.

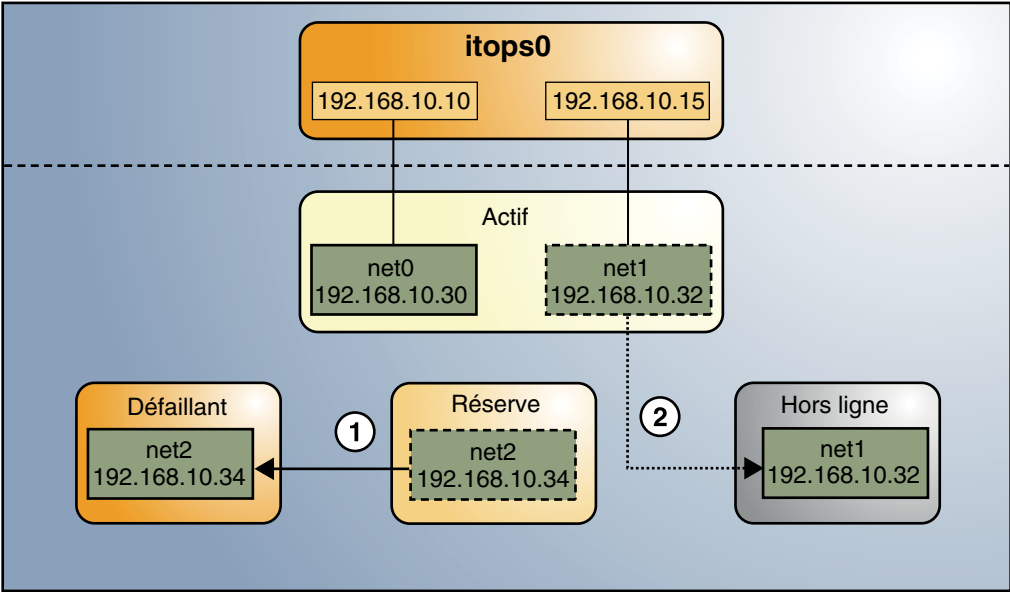
L'utilitaire `ipmpstat` affiche les informations dans la [Figure 14-2](#) comme suit :

```
# ipmpstat -i
INTERFACE  ACTIVE  GROUP   FLAGS   LINK    PROBE   STATE
net0       no      itops0  - - - - up      failed  failed
net1       yes     itops0  - - m b - up      ok      ok
net2       yes     itops0  - s - - - up      ok      ok
```

Une fois que `net0` est réparée, elle revient à son état d'interface active. A son tour, `net2` revient à son état initial d'attente.

Un autre scénario de panne est affichée dans la [Figure 14-3](#), où l'interface de réserve `net` échoue (1), et par la suite, une interface active, `net1`, est mise hors ligne par l'administrateur (2). Le résultat est que le groupe IPMP est laissé avec une seule interface opérationnelle, `net0`.

FIGURE 14-3 Panne d'interface de réserve dans IPMP

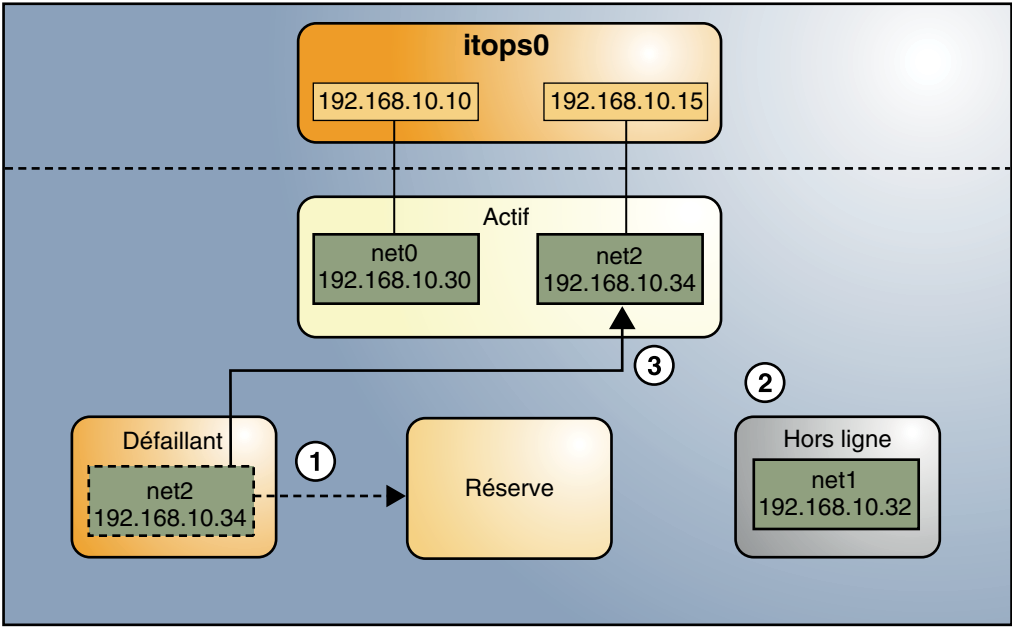


L'utilitaire `ipmpstat` affichera les informations illustrées par la [Figure 14-3](#) comme suit :

```
# ipmpstat -i
INTERFACE  ACTIVE  GROUP   FLAGS    LINK    PROBE    STATE
net0       yes    itops0  - - - - -  up      ok       ok
net1       no     itops0  - - m b - d -  up      ok       offline
net2       no     itops0  i s - - - -  up      failed  failed
```

Pour cette panne, la récupération après réparation d'une interface se comporte différemment. Le processus de restauration dépend du nombre initial d'interfaces actives du groupe IPMP par rapport à la configuration après réparation. Le processus de récupération est représentée graphiquement dans la [Figure 14-4](#).

FIGURE 14-4 Processus de restauration IPMP



Dans la [Figure 14-4](#), lorsque **net2** est réparée, elle doit normalement revenir à son état d'origine d'interface de réserve (1). Cependant, le groupe IPMP ne reflète toujours pas le nombre initial de deux interfaces actives, car **net1** est toujours hors ligne (2). Par conséquent, IPMP déploie **net2** comme une interface active (3).

L'utilitaire `impstat` affiche le scénario IPMP post-réparation comme suit :

```
# impstat -i
INTERFACE  ACTIVE  GROUP   FLAGS   LINK    PROBE   STATE
net0       yes    itops0  ----- up       ok      ok
net1       no     itops0  --mb-d- up       ok      offline
net2       yes    itops0  -s----- up       ok      ok
```

Une séquence de restauration similaire se produit si l'incident implique une interface active qui est également configurée en mode `FAILBACK=no`, où une interface active en panne ne revient pas automatiquement à l'état actif après réparation. Supposons que **net0** dans la [Figure 14-2](#) soit configurée en mode `FAILBACK=no`. Dans ce mode, une **net0** réparée est passée à un état de réserve en tant qu'interface de réserve, même si elle était initialement une interface active. L'interface **net2** demeure active afin de maintenir le nombre initial de deux interfaces actives du groupe IPMP. L'utilitaire `impstat` affiche les informations de récupération comme suit :

```
# impstat -i
INTERFACE  ACTIVE  GROUP   FLAGS   LINK    PROBE   STATE
net0       no     itops0  i----- up       ok      ok
net1       yes    itops0  --mb---  up       ok      ok
```

```
net2          yes          itops0      -s-----  up          ok          ok
```

Pour plus d'informations sur ce type de configuration, reportez-vous à la section “[Mode FAILBACK=no](#)” à la page 285.

## Composants IPMP dans Oracle Solaris

Oracle Solaris IPMP comprend les logiciels suivants :

Le *démon de multipathing* `in.mpathd` détecte les pannes et réparations d'interface. Le démon procède à la détection de défaillance basée sur les liaisons et la détection de défaillance basée sur les sondes si les adresses de test sont configurées pour les interfaces sous-jacentes. Selon le type de méthode de détection de défaillance employée, le démon définit ou supprime les indicateurs appropriés sur l'interface afin d'indiquer si l'interface a échoué ou a été réparé. Le démon peut également être configuré pour surveiller la disponibilité de toutes les interfaces, y compris celles qui ne sont pas configurées pour appartenir à un groupe IPMP. Pour obtenir une description de la détection de défaillance, reportez-vous à la section “[Détection de défaillance et de réparation dans IPMP](#)” à la page 281.

Le démon `in.mpathd` contrôle également la désignation des interfaces actives dans le groupe IPMP. Le démon tente de conserver le même nombre d'interfaces initialement configuré lorsque le groupe IPMP a été créé. Par conséquent, `in.mpathd` active ou désactive les interfaces sous-jacentes selon les besoins pour être cohérent avec la stratégie configurée de l'administrateur. Pour plus d'informations sur la manière dont le démon `in.mpathd` gère l'activation des interfaces sous-jacentes, reportez-vous à la section “[Fonctionnement d'IPMP](#)” à la page 272. Pour plus d'informations sur le démon, reportez-vous à la page de manuel `in.mpathd(1M)`.

Le *module de noyau IP* gère la répartition de charge sortante en distribuant l'ensemble des adresses IP disponibles dans le groupe sur l'ensemble des interfaces IP sous-jacentes disponibles dans le groupe. Le module effectue également une sélection d'adresses source pour gérer la répartition de charge entrante. Les deux rôles du module IP améliorent les performances du trafic réseau.

Le *fichier de configuration IPMP* `/etc/default/mpathd` sert à configurer le comportement du démon. Par exemple, vous pouvez spécifier la manière dont le démon effectue la détection de défaillance basée sur sonde en définissant la durée d'analyse d'une cible pour détecter des défaillances ou les interfaces à analyser. Vous pouvez également spécifier de quelle façon l'état d'une interface défaillante doit être une fois que l'interface est réparée. Vous pouvez également définir les paramètres de ce fichier pour spécifier si le processus doit surveiller toutes les interfaces IP du système, et pas uniquement celles qui sont configurées pour faire partie de groupes IPMP. Pour plus d'informations sur les procédures de modification du fichier de configuration, reportez-vous à la “[Procédure de configuration du comportement du démon IPMP](#)” à la page 316.

L'utilitaire *ipmpstat* fournit différents types d'informations sur l'état d'IPMP dans son ensemble. L'outil affiche également d'autres informations spécifiques sur les interfaces IP sous-jacentes pour chaque groupe, ainsi que des adresses de données et de test qui ont été configurées pour le groupe. Pour plus d'informations sur l'utilisation de cette commande, reportez-vous à la section [“Contrôle des informations d'IPMP” à la page 319](#) et la page de manuel *ipmpstat(1M)*.

## Types de configurations d'interface IPMP

En règle générale, la configuration d'IPMP se compose d'au moins deux interfaces physiques situées sur le même système et connectées au même LAN. Ces interfaces peuvent appartenir à un groupe IPMP dans l'une des configurations suivantes :

- Configuration active-active : groupe IPMP dans lequel les interfaces sont actives. Une *interface active* est une interface IP qui est actuellement disponible pour l'utilisation par le groupe IPMP. Par défaut, une interface sous-jacente devient active lorsque vous la configurez pour faire partie d'un groupe IPMP. Pour plus d'informations sur les interfaces actives et autres termes d'IPMP, reportez-vous à la section [“Terminologie et concepts IPMP” à la page 288](#).
- Configuration active-de réserve : groupe IPMP dans lequel au moins une interface est administrativement configuré comme étant de réserve. L'interface de réserve est appelée *interface de réserve*. Bien qu'inactive, l'interface IP de réserve est surveillée par le démon de multipathing pour effectuer le suivi de la disponibilité de l'interface, en fonction de sa configuration. Si la notification de défaillance de liaison est prise en charge par l'interface, la détection de défaillance basée sur les liaisons est utilisé. Si l'interface est configurée avec une adresse de test, la détection de défaillance basée sur sonde est également utilisée. Si une interface active échoue, l'interface de réserve est déployée automatiquement en fonction des besoins. Vous pouvez configurer autant d'interfaces de réserve que vous le souhaitez pour un groupe IPMP.

Vous pouvez aussi configurer une interface unique dans son propre groupe IPMP. Le groupe IPMP à interface unique se comporte de la même façon qu'un groupe IPMP avec plusieurs interfaces. Cependant, cette configuration IPMP ne fournit pas de haute disponibilité pour le trafic réseau. Si l'interface sous-jacente échoue, le système perd toute capacité à envoyer ou recevoir du trafic. L'intérêt de configurer un groupe IPMP à une interface est de surveiller la disponibilité de l'interface en utilisant la détection de défaillance. En configurant une adresse de test sur l'interface, vous pouvez configurer le démon pour effectuer le suivi de l'interface à l'aide de la détection de défaillance basée sur sonde. En règle générale, une configuration de groupe IPMP à une interface est utilisée en conjonction avec d'autres technologies qui ont de plus grandes capacités de basculement, comme le logiciel Oracle Solaris Cluster. Le système peut continuer à surveiller l'état de l'interface sous-jacente. Mais le logiciel Oracle Solaris Cluster fournit les fonctionnalités permettant de garantir la disponibilité du réseau lorsqu'une panne survient. Pour plus d'informations sur le logiciel Oracle Solaris Cluster, reportez-vous à la section [Sun Cluster Overview for Solaris OS](#).

Un groupe IPMP sans interfaces sous-jacente peut également exister, tel qu'un groupe dont les interfaces ont été supprimées. Le groupe IPMP n'est pas détruit, mais il ne peut pas être utilisé pour envoyer et recevoir du trafic. Les interfaces IP sous-jacentes sont mises en ligne pour le groupe, puis les adresses de données de l'interface IPMP sont allouées à ces interfaces et le système reprend l'hébergement du trafic réseau.

## Adressage IPMP

Vous pouvez configurer la détection de défaillance d'IPMP sur des réseaux IPv4 ainsi que sur des réseaux IPv4 et IPv6 double pile. Les interfaces configurées avec IPMP prennent deux types d'adresses en charge :

- Les *adresses de données* sont les adresses IPv4 et IPv6 conventionnelles qui sont allouées à une interface IP dynamiquement pendant l'initialisation par le serveur DHCP ou manuellement avec la commande `ipadm`. Les adresses de données sont affectées à l'interface IPMP. Le trafic de paquets standard IPv4 et, le cas échéant, IPv6, est considéré comme du *trafic de données*. Le flux de trafic de données utilise les adresses de données qui sont hébergées sur l'interface IPMP et le flux à travers les interfaces actives de ce groupe.
- Les *adresses de test* sont spécifiques à IPMP et utilisées par le démon `in.mpathd` pour effectuer une détection de défaillance et de réparation basée sur sonde. Des adresses de test peuvent également être affectées de façon dynamique par le serveur DHCP, ou manuellement avec la commande `ipadm`. Bien que les adresses de données soient affectées à l'interface IPMP, seules les adresses de test sont affectées aux interfaces sous-jacentes du groupe. Dans le cas d'une interface sous-jacente sur un réseau double pile, vous pouvez configurer une adresse de test IPv4, IPv6 ou les deux. Lorsqu'une interface sous-jacente échoue, l'adresse de test de l'interface continue d'être utilisée par le démon `in.mpathd` pour la détection de défaillance basée sur sonde pour vérifier la réparation qui suit.

---

**Remarque** – La configuration des adresses test n'est requise que si vous souhaitez utiliser spécifiquement la détection de défaillance basée sur sonde. Dans le cas contraire, vous pouvez activer le test transitif pour détecter la défaillance sans utiliser des adresses de test. Pour de plus amples informations sur la détection de défaillance basée sur sonde avec ou sans adresses de test, reportez-vous à la section “[Détection de défaillance basée sur sonde](#)” à la page 282.

---

Dans les précédentes implémentations d'IPMP, les adresses de test devraient être marquées comme étant DEPRECATED pour éviter d'être utilisées par les applications en particulier au cours des défaillances d'interface. Dans l'implémentation actuelle, des adresses de test se trouvent dans les interfaces sous-jacentes. Par conséquent, ces adresses ne peuvent plus être accidentellement utilisées par des applications qui ne sont pas conscientes d'IPMP. Cependant, pour vous assurer que ces adresses ne sont pas considérées comme une source possible pour les paquets de données, le système les marque automatiquement avec l'indicateur NOFAILOVER ainsi que DEPRECATED.



## Adresses test IPv4

En règle générale, vous pouvez utiliser l'adresse IPv4 de votre choix sur votre sous-réseau en tant qu'adresse de test. Il n'est pas nécessaire que les adresses test IPv4 soient acheminables. Dans la mesure où les adresses IPv4 sont une ressource limitée pour de nombreux sites, il est préférable dans certains cas d'utiliser des adresses privées RFC 1918 non acheminables en tant qu'adresses test. Notez que le démon `in.mpathd` n'échange que des sondes ICMP avec d'autres hôtes situés sur le même sous-réseau que l'adresse test. Si vous utilisez des adresses test de type RFC 1918, veillez à configurer d'autres systèmes, des routeurs de préférence, sur le réseau avec des adresses situées sur le sous-réseau RFC 1918. Le démon `in.mpathd` peut ensuite échanger les sondes avec des systèmes cible. Pour plus d'informations sur les adresses privées RFC 1918, reportez-vous au document [RFC 1918, Address Allocation for Private Internets](http://www.ietf.org/rfc/rfc1918.txt?number=1918) (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>) (en anglais).

## Adresses test IPv6

La seule adresse test IPv6 valide correspond à l'adresse lien-local d'une interface physique. Vous n'avez pas besoin d'utiliser une adresse IPv6 en tant qu'adresse test IPMP. L'adresse IPv6 lien-local est basée sur l'adresse MAC (Media Access Control) de l'interface. Les adresses lien-local sont configurées automatiquement lorsque l'interface devient compatible IPv6 lors du démarrage ou lorsque l'interface est configurée manuellement via `ipadm`.

Pour de plus amples informations sur les adresses lien-local, reportez-vous à la section “[Link-Local Unicast Address](#)” du manuel *System Administration Guide: IP Services*.

Lorsqu'IPv4 et IPv6 sont montés sur la totalité des interfaces d'un groupe IPMP, il est inutile de configurer des adresses test IPv4 distinctes. Le démon `in.mpathd` peut utiliser des adresses IPv6 lien-local en tant qu'adresses test.

# Détection de défaillance et de réparation dans IPMP

Afin de garantir une disponibilité continue du réseau pour envoyer ou recevoir le trafic, IPMP effectue une détection de défaillance sur les interfaces d'IP sous-jacentes du groupe IPMP. Les interfaces défaillantes sont inutilisables jusqu'à ce qu'elles soient réparées. Les interfaces actives restantes continuent de fonctionner et les interfaces de réserve sont déployées en fonction des besoins.

## Types de détection de défaillance dans IPMP

Le démon `in.mpathd` gère les types de détection de défaillance suivants :

- Détection de défaillance basée sur sonde, de deux types :
  - Aucune adresse de test n'est configurée (test transitif).

- Des adresses de test sont configurées.
- Détection de défaillance basée sur les liaisons, si la prise en charge est assurée par le pilote de la carte d'interface réseau.

## Détection de défaillance basée sur sonde

La détection de défaillance basée sur sonde consiste à utiliser des sondes ICMP pour vérifier si une interface a échoué. L'implémentation de cette méthode de détection de défaillance dépend de l'utilisation d'adresses de test.

## Détection de défaillance basée sur sonde sans utiliser d'adresses de test

Sans adresse de test, cette méthode est implémentée à l'aide de deux types de sondes :

- Sondes ICMP

Les sondes ICMP sont envoyées par les interfaces actives dans le groupe pour tester les cibles qui sont définies dans la table de routage. Une interface *active* est l'interface sous-jacente qui peut recevoir les paquets IP entrants qui sont adressés à l'adresse de couche liaison (L2) de l'interface. La sonde ICMP utilise l'adresse de données comme adresse source de la sonde. Si la sonde ICMP atteint sa cible et obtient une réponse à partir de la cible, alors l'interface active est opérationnelle.

- Sondes transitives

Les sondes transitives sont envoyées par les interfaces alternatives dans le groupe pour tester l'interface active. Une interface alternative est une interface sous-jacente qui n'est ne reçoit pas activement des paquets IP entrants.

Par exemple, prenons le cas d'un groupe IPMP composé de quatre interfaces sous-jacentes. Le groupe est configuré avec une adresse de données mais aucune adresse de test. Dans cette configuration, les paquets sortants peuvent utiliser toutes les interfaces sous-jacentes. Cependant, les paquets entrants peuvent uniquement être reçus par l'interface à laquelle l'adresse de données est liée. Les trois autres interfaces sous-jacentes qui ne peuvent pas recevoir les paquets entrants sont les interfaces *alternatives*.

Si une interface alternative réussit à envoyer une sonde à une interface active et à recevoir une réponse, alors l'interface active est fonctionnelle, et par déduction, l'interface alternative qui a envoyé la sonde également.

---

**Remarque** – Vous devez activer le test transitif pour utiliser cette méthode de détection de défaillance qui n'exige pas d'adresses de test.

---

## Détection de défaillance basée sur sonde avec des adresses de test

Cette méthode de détection de défaillance repose sur l'envoi et la réception de messages de sonde ICMP utilisant des adresses de test. Ces messages, également appelés *trafic de sonde* ou *trafic de test*, partent de l'interface vers un ou plusieurs systèmes cible sur le même réseau local.

Le démon examine toutes les cibles séparément à travers toutes les interfaces qui ont été configurées pour la détection de défaillance basée sur sonde. Si, après cinq tests consécutifs sur une interface donnée, aucune réponse n'est obtenue, `in.mpathd` considère que l'interface est défaillante. La fréquence des tests dépend du *temps de détection de défaillance*. Le temps de détection de défaillance par défaut est de 10 secondes. Cependant, vous pouvez régler le temps de détection de défaillance dans le fichier de configuration d'IPMP. Pour plus d'informations, reportez-vous à la section [“Procédure de configuration du comportement du démon IPMP” à la page 316](#). Pour optimiser la détection de défaillance basée sur sonde, vous devez définir plusieurs systèmes cible pour recevoir les sondes à partir du démon de multipathing. En présence de plusieurs systèmes cibles, vous pouvez mieux déterminer la nature d'une défaillance signalée. Par exemple, l'absence d'une réponse de la part de l'unique système défini peut indiquer une défaillance dans le système cible ou dans l'un des interfaces du groupe IPMP. En revanche, si un seul système entre plusieurs systèmes cible ne répond pas à une sonde, alors la défaillance l'échec est probablement dans le système cible plutôt que dans le groupe IPMP lui-même.

Le démon `in.mpathd` permet de déterminer les systèmes cible à analyser dynamiquement. Tout d'abord le démon recherche dans la table de routage les systèmes cibles sur le même sous-réseau que les adresses de test qui sont associées à l'interface du groupe IPMP. Si de telles cibles sont trouvées, le démon les utilise comme cibles pour les tests. Si aucune cible n'est trouvée sur le même sous-réseau, `in.mpathd` envoie des paquets de multidiffusion pour tester les hôtes voisins sur le lien. Le paquet multidiffusion envoyé à toutes les adresses d'hôtes multidiffusion, `224.0.0.1` dans IPv4 et `ff02::1` dans IPv6, pour déterminer les hôtes à utiliser en tant que systèmes cible. Les cinq premiers hôtes qui répondent aux paquets d'écho sont sélectionnés en tant que cibles pour les sondes. Si `in.mpathd` ne trouve aucun routeur ou hôte ayant répondu aux sondes multidiffusion, puis aux paquets d'écho ICMP, `in.mpathd` ne pourra pas détecter les défaillances basées sur sonde. Dans ce cas, l'utilitaire `ipmpstat -i` signale l'état de la sonde comme `unknown`.

Vous pouvez utiliser des routes d'hôte afin de configurer de façon explicite une liste de systèmes cible en vue d'une utilisation par `in.mpathd`. Pour plus d'instructions, reportez-vous à la section [“Configuration pour la détection de défaillance basée sur sonde” à la page 314](#).

## Défaillance de groupe

Une *défaillance de groupe* survient lorsque la totalité des interfaces d'un groupe IPMP sont défaillantes au même Dans ce cas, aucune interface sous-jacente n'est utilisable. De même, lorsque l'ensemble des systèmes cibles tombe en panne au même moment et que la détection de défaillance basée sur sonde est activée, le démon `in.mpathd` vide tous ses systèmes cibles et test de nouveaux systèmes cibles.

Dans un groupe IPMP qui n'a aucune adresse de test, une interface unique qui peut tester l'interface active sera désignée comme "prober". Cette interface désignée porte les indicateurs FAILED et PROBER. L'adresse de données est liée à cette interface qui permet à l'interface de continuer le test de la cible pour détecter une restauration.

## Détection de défaillance basée sur les liaisons

La détection de défaillance basée sur les liaisons est toujours activée, à condition que l'interface prenne ce type de détection en charge.

Pour déterminer si une interface tierce prend en charge la détection de défaillance basée sur les liaisons, utilisez la commande `ipmpstat -i`. Si la sortie d'une interface donnée comprend un état `unknown` pour sa colonne `LINK`, alors que l'interface ne prend pas en charge la détection de défaillance basée sur les liaisons. Reportez-vous à la documentation du fabricant pour obtenir des informations plus spécifiques sur le périphérique.

Ces pilotes réseau, qui prennent en charge la détection de défaillance basée sur les liaisons, contrôlent l'état de la liaison de l'interface et notifient le sous-système de mise en réseau en cas de modification de l'état. En fonction de la situation, le sous-système de mise en réseau définit ou efface alors l'indicateur `RUNNING` de cette interface. Si le démon `in.mpathd` détecte que l'indicateur `RUNNING` de l'interface a été effacé, il déclenche immédiatement une défaillance de l'interface.

## Détection de défaillance et fonction de groupe anonyme

IPMP prend en charge la détection de défaillance dans un groupe anonyme. Par défaut, IPMP surveille l'état uniquement d'interfaces qui appartiennent à des groupes IPMP. Cependant, le démon IPMP peut être configuré de façon à également assurer le suivi du statut des interfaces qui n'appartiennent à aucun groupe IPMP. Par conséquent, ces interfaces sont considérées comme faisant partie d'un "groupe anonyme." Lorsque vous exécutez la commande `ipmpstat -g`, le groupe anonyme est affiché sous forme de double-tirets (`--`). Dans les groupes anonymes, les adresses de données des interfaces fonctionnerait également comme adresse de test. Comme ces interfaces n'appartiennent pas à un groupe IPMP nommé, ces adresses sont visibles pour les applications. Pour activer le suivi des interfaces qui ne font pas partie d'un groupe IPMP, reportez-vous à la section [“Procédure de configuration du comportement du démon IPMP”](#) à la page 316.

## Détection de réparation d'interface physique

Le *temps de détection de réparation* est le double du temps de détection de défaillance. Le temps de détection de défaillance par défaut est de 10 secondes. Par conséquent, le temps de détection de réparation par défaut est de 20 secondes. Une fois qu'une interface défaillante est de nouveau marquée par l'indicateur `RUNNING` et que la méthode de détection de défaillance l'a détecté comme réparée, `in.mpathd` efface l'indicateur `FAILED` de l'interface. L'interface réparée est redéployée en fonction du nombre d'interfaces actives que l'administrateur a définies à l'origine.

Lorsqu'une interface sous-jacente échoue et que la détection de défaillance basée sur sonde est utilisé, le démon `in.mpathd` poursuit le test, par le biais du `prober` désigné lorsqu'aucune adresse de test n'est configurée ou à l'aide de l'interface de l'adresse de test. Au cours d'une réparation d'interface, la restauration se poursuit en fonction de la configuration d'origine de l'interface défaillante :

- L'interface défaillante était une interface active à l'origine. L'interface réparée reprend son état actif initial. L'interface de réserve qui a fonctionné comme remplacement lors de la défaillance est passé en état de réserve si suffisamment d'interfaces sont actives pour le groupe, tel que défini par l'administrateur système.

---

**Remarque** – Une exception à cette étape sont les cas où l'interface active réparée est également configurée avec le mode FAILBACK=no. Pour plus d'informations, reportez-vous à la section [“Mode FAILBACK=no” à la page 285](#).

---

- L'interface défaillante était à l'origine une interface de réserve : l'interface réparée revient à son état de réserve d'origine, à condition que le groupe IPMP reflète le nombre initial d'interfaces actives. Dans le cas contraire, l'interface de réserve est activée pour devenir une interface active.

Pour voir une présentation graphique du comportement d'IPMP pendant la défaillance et la réparation d'une interface, reportez-vous à la section [“Fonctionnement d'IPMP” à la page 272](#).

## Mode FAILBACK=no

Par défaut, les interfaces actives qui ont échoué et ont ensuite été réparées, redeviennent automatiquement des interfaces actives dans le groupe. Ce comportement est contrôlé par la définition du paramètre FAILBACK dans le fichier de configuration du démon. Cependant, même les perturbations insignifiantes, qui se produisent lorsque les adresses de données sont remappées pour réparer des interfaces, peuvent ne pas être acceptable pour certains administrateurs. Les administrateurs peuvent préférer autoriser une interface secondaire activée pour continuer comme interface active. IPMP permet aux administrateurs d'ignorer le comportement par défaut pour empêcher une interface de devenir automatiquement active lors d'une réparation. Ces interfaces doivent être configurées dans le mode FAILBACK=no. Pour connaître les procédures connexes, reportez-vous à la section [“Procédure de configuration du comportement du démon IPMP” à la page 316](#).

Lorsqu'une interface active en mode FAILBACK=no échoue et est ensuite réparée, le démon IPMP restaure la configuration d'IPMP comme suit :

- Le démon conserve l'état INACTIVE de l'interface, à condition que le groupe IPMP reflète la configuration d'origine des interfaces actives.
- Si la configuration d'IPMP au moment de la réparation ne reflète pas la configuration d'origine du groupe des interfaces actives, puis l'interface réparée est redéployée comme interface active, nonobstant l'état FAILBACK=no.

---

**Remarque** – Le mode FAILBACK=NO est défini pour l'ensemble du groupe IPMP. Il ne s'agit pas d'un paramètre réglable par interface.

---

# IPMP et reconfiguration dynamique

La fonctionnalité de reconfiguration dynamique permet de reconfigurer le matériel système, notamment les interfaces, lorsque le système est en cours d'exécution. La reconfiguration dynamique peut être utilisée uniquement sur les systèmes qui prennent en charge cette fonctionnalité.

En règle générale, la commande `cfgadm` permet d'effectuer des opérations de reconfiguration dynamique. Cependant, certaines plates-formes fournissent d'autres méthodes. Assurez-vous de consulter la documentation de votre plate-forme pour plus de détails sur l'utilisation de la reconfiguration dynamique. Pour les systèmes qui utilisent Oracle Solaris, vous trouverez des informations spécifiques relatives à la reconfiguration dynamique dans les ressources répertoriées dans le [Tableau 14-1](#). Des informations actuelles sur la reconfiguration dynamique est également disponible sur le site <http://www.oracle.com/technetwork/indexes/documentation/index.html> et peuvent être obtenues par la recherche de la rubrique "dynamic reconfiguration."

TABLEAU 14-1 Ressources documentaires sur la DR

Description	Référence
Informations détaillées sur la commande <code>cfgadm</code>	Page de manuel <code>cfgadm(1M)</code> .
Informations spécifiques sur la reconfiguration dynamique dans l'environnement Oracle Solaris Cluster	<i>Guide d'administration système d'Oracle Solaris Cluster</i>
Informations spécifiques sur la reconfiguration dynamique dans les serveurs Sun d'Oracle	Reportez-vous à la documentation fournie avec votre serveur spécifique
Introduction à la DR et à la commande <code>cfgadm</code>	Chapitre 6, "Configuration dynamique des périphériques (tâches)" du manuel <i>Administration d'Oracle Solaris : Périphériques et systèmes de fichiers</i>
Tâches d'administration de groupes IPMP sur un système prenant en charge la DR	"Restauration d'une configuration d'IPMP avec la reconfiguration dynamique" à la page 317

Les sections qui suivent expliquent comment la reconfiguration dynamique interagit avec IPMP.

Dans un système prenant en charge la reconfiguration dynamique des cartes d'interface réseau, IPMP permet de préserver la connectivité et d'éviter toute perturbation des connexions existantes. IPMP est intégré à la structure du RCM (Reconfiguration Coordination Manager, gestionnaire de coordination de reconfiguration). Par conséquent, vous pouvez en toute sécurité connecter, déconnecter ou reconnecter les cartes réseau et le RCM assure la gestion de la reconfiguration dynamique des composants système.

## Connexion de nouvelles cartes réseau

Avec la prise en charge de la reconfiguration dynamique, vous pouvez joindre, monter, puis ajouter de nouvelles interfaces aux groupes IPMP existants. Le cas échéant, vous pouvez également configurer les nouvelles interfaces ajoutées dans leur propre groupe IPMP. Pour plus d'informations sur les procédures de configuration des groupes IPMP, reportez-vous à la section [“Configuration de groupes IPMP” à la page 302](#). Une fois ces interfaces configurées, elles sont immédiatement disponibles pour l'utilisation par IPMP. Toutefois, pour bénéficier des avantages de l'utilisation de noms de liaison personnalisés, vous devez affecter des noms de liaisons génériques pour remplacer les noms de liaisons basés sur le matériel. Vous créez ensuite les fichiers de configuration correspondant à l'aide du nom générique que vous venez d'attribuer. Pour plus d'informations sur les procédures de configuration d'une interface unique à l'aide de noms de liaison personnalisés, reportez-vous à la section [“Configuration d'une interface IP” à la page 183](#). Une fois que vous avez attribué un nom de liaison générique à l'interface, assurez-vous de toujours faire référence au nom générique lorsque vous effectuez une configuration supplémentaire sur l'interface comme à l'aide de l'interface pour IPMP.

## Déconnexion de cartes d'interface réseau

Toutes les requêtes de déconnexion de composants système contenant des cartes d'interface réseau sont d'abord vérifiées afin de garantir un connectivité ininterrompue. Ainsi, par défaut, il est impossible de déconnecter une carte d'interface réseau ne faisant pas partie d'un groupe IPMP. La déconnexion est également impossible dans le cas d'une carte d'interface réseau qui contient les seules interfaces en état de fonctionnement d'un groupe IPMP. Cependant, si vous devez retirer le composant système, l'option `-f` de `cfgadm` permet de contourner ce comportement ; vous trouverez une explication à la page de manuel [cfgadm\(1M\)](#).

Si les vérifications sont réussies, le démon définit l'indicateur `OFFLINE` sur l'interface. Toutes les adresses de test sur les interfaces ne sont pas configurées. Ensuite, la carte d'interface réseau est démontée du système. En cas d'échec de l'une de ces étapes, ou de défaillance de la reconfiguration dynamique ou autre matériel sur le même composant système, l'état d'origine de la configuration précédente est restauré. Un message d'état de cet événement s'affiche. Dans le cas contraire, la demande de déconnexion est traitée. Vous pouvez retirer le composant du système. Aucune connexion existante n'est interrompue.

## Remplacement de cartes réseau

Lorsqu'une interface sous-jacente d'un groupe IPMP échoue, une solution classique consiste à remplacer l'interface défaillante en connectant une nouvelle carte réseau. Le RCM enregistre les informations de configuration associées à toute carte d'interface réseau déconnectée d'un système en cours d'exécution. Si vous remplacez une carte réseau avec un carte réseau *identique*, alors RCM configure automatiquement l'interface en fonction de la configuration permanente qui avait été précédemment définie avec la commande `ipadm`.

Par exemple, supposons que vous remplaciez une interface `bge0` défaillante par une autre interface `bge0`. Les paramètres de configuration de l'interface `bge0` défaillante qui ont été définis à l'aide de la commande `ipadm` sont des paramètres persistants. Une fois que vous connectez la carte réseau `bge`, RCM monte et configure ensuite l'interface `bge0` en fonction de ces paramètres persistants. Ainsi, l'interface est correctement configurée avec l'adresse de test et est ajoutée au groupe IPMP.

Vous pouvez remplacer une carte réseau défaillante par une autre carte réseau, à condition que les deux soient du même type, tel qu'Ethernet. Dans ce cas, le RCM monte la nouvelle interface une fois qu'elle est connectée. Si vous n'avez pas utilisé de noms de liaison personnalisés lorsque vous avez configuré pour la première fois des interfaces, vous devrez configurer la nouvelle carte d'interface réseau pour pouvoir ajouter l'interface au groupe IPMP.

Toutefois, si vous avez utilisé noms de liaison personnalisés, les étapes de configuration supplémentaires sont inutiles. Par la réaffectation du nom de liaison de l'interface défaillante à la nouvelle interface, cette dernière acquiert la configuration spécifiée dans les paramètres persistants de l'interface supprimée. RCM configure ensuite l'interface en fonction de ces paramètres. Pour plus d'informations sur les procédures de restauration de votre configuration d'IPMP à l'aide de DR lorsqu'une interface échoue, reportez-vous à la section [“Restauration d'une configuration d'IPMP avec la reconfiguration dynamique” à la page 317](#).

## Terminologie et concepts IPMP

Cette section présente les termes et concepts utilisés dans les chapitres relatifs à IPMP dans ce manuel.

interface active

Fait référence à une interface sous-jacente qui peut être utilisée par le système pour envoyer ou recevoir le trafic de données. Une interface est active si les conditions suivantes sont remplies :

- Au moins une adresse IP est UP dans l'interface. Voir l'adresse UP.
- Les indicateurs `FAILED`, `INACTIVE` ou `OFFLINE` ne sont pas définis sur l'interface.
- L'interface n'a pas été marquée comme ayant un double adresse matérielle.

Comparée à interface inutilisable, interface `INACTIVE`.

adresse de données

Fait référence à une adresse IP pouvant servir d'adresse source ou cible de données. Une adresse de données permet l'envoi et la



réception de données sur toutes les interfaces du groupe IPMP auquel elle appartient. En outre, le jeu d'adresses de données dans un groupe IPMP peut être utilisé de manière continue à condition qu'une interface du groupe soit en cours de fonctionnement. Dans les précédentes implémentations d'IPMP, les adresses de données étaient hébergées sur les interfaces sous-jacentes d'un groupe IPMP. Dans l'implémentation actuelle, les adresses de données sont hébergées sur l'interface IPMP.

#### adresse DESAPPROUEE

Fait référence à une adresse IP ne pouvant être utilisée en tant qu'adresse source pour les données. En règle générale, les adresses de test IPMP, qui ont l'indicateur NOFAILOVER, sont également automatiquement marquées comme DEPRECATED par le système. Toutefois, toute adresse peut être indiquée comme adresse DESAPPROUEE en vue d'empêcher son utilisation en tant qu'adresse source.

#### Reconfiguration dynamique

Fait référence à une fonction permettant de reconfigurer un système en cours d'exécution sans incidence ou presque sur les opérations en cours. La reconfiguration dynamique n'est pas prise en charge par toutes les plates-formes Sun d'Oracle. Certaines plates-formes ne prennent en charge que la reconfiguration dynamique de certains types de matériel. Sur les plates-formes qui prennent en charge la reconfiguration dynamique de cartes d'interface réseau, IPMP peut être utilisé pour accéder au réseau sans interruption au système lors de la reconfiguration dynamique.

Pour obtenir des informations supplémentaires sur la prise en charge de la reconfiguration dynamique par IPMP, reportez-vous à la section [“IPMP et reconfiguration dynamique”](#) à la page 286.

création d'interface IPMP explicite

S'applique uniquement à l'implémentation d'IPMP actuelle. Le terme fait référence à la méthode de création d'une interface IPMP en utilisant la commande `ipadm create-ipmp` en commande. La création d'interface IPMP explicite est la méthode recommandée pour créer des groupes IPMP. Cette méthode permet à l'administrateur de définir les noms d'interface IPMP et de groupe IPMP.

Comparée à la création d'interface IPMP implicite.

mode FAILBACK=no

Fait référence à un paramètre d'une interface sous-jacente qui minimise le fait de relier des adresses entrantes à des interfaces en évitant la redistribution au cours d'une réparation d'interface. Plus précisément, lorsqu'une réparation d'interface est détectée, l'indicateur FAILED est effacé. Toutefois, si le mode de l'interface réparée est FAILBACK=no, alors l'indicateur INACTIVE est également défini pour empêcher l'utilisation de l'interface, à condition qu'une deuxième interface opérationnelle existe également. Si la deuxième interface du groupe IPMP échoue, L'interface INACTIVE peut prendre le relais. Bien que le concept de rétablissement ne s'applique plus dans l'implémentation d'IPMP actuelle, le nom de ce mode est conservé pour assurer la compatibilité administrative.

interface FAILED

Indique une interface que le démon `in.mpathd` a déterminé défaillante. La détermination est obtenue par une détection de défaillance basée sur les liaison ou sur sonde. L'indicateur FAILED est défini sur n'importe quelle interface défaillante.

détection de défaillance

Fait référence au processus de détection intervenant lorsqu'une interface ou le chemin d'une interface vers un périphérique de couche Internet ne fonctionne plus. Deux formes de défaillance sont implémentées : basée sur les liaisons et basée sur sonde.

création d'interface IPMP implicite

Fait référence à la méthode de création d'une interface IPMP à l'aide de la commande `ifconfig` pour placer une interface sous-jacente dans un groupe IPMP qui n'existe pas. La création d'interface IPMP implicite est prise en charge pour des raisons de rétrocompatibilité avec l'implémentation d'IPMP dans les précédentes versions d'Oracle Solaris. Par conséquent, cette méthode ne permet pas de définir le nom d'interface IPMP ou le nom de groupe IPMP. La création d'interface IPMP implicite n'est pas prise en charge par la commande `ipadm`.

Comparée à la création d'interface IPMP explicite.

interface INACTIVE

Fait référence à une interface qui fonctionne mais n'est pas utilisée en fonction de la stratégie administrative. L'indicateur `INACTIVE` est défini sur n'importe quelle interface `INACTIVE`.

Comparée à l'interface active, interface inutilisable.

prise en charge des groupes anonymes IPMP

Indique une fonction d'IPMP dans laquelle le démon d'IPMP suit l'état de toutes les interfaces réseau du système, qu'elles appartiennent ou non à un groupe IPMP. Toutefois, si les interfaces ne sont pas réellement dans un groupe IPMP, les adresses sur ces interfaces ne sont pas disponibles en cas de défaillances de l'interface.

Groupe IPMP

Fait référence à un ensemble d'interfaces réseau que le système considère interchangeables afin d'améliorer la disponibilité du réseau et de l'utilisation. Chaque groupe IPMP dispose d'un ensemble d'adresses de données que le système peut associer à n'importe quel ensemble d'interfaces actives dans le groupe. L'utilisation de ce jeu d'adresses de données maintient la disponibilité réseau et améliore

interface de groupe IPMP	<p>l'utilisation du réseau. L'administrateur peut sélectionner les interfaces à placer dans un groupe IPMP. Cependant, toutes les interfaces d'un même groupe doivent partager un ensemble commun de propriétés, telles qu'être connectées à la même liaison et configurées avec le même ensemble de protocoles (par exemple, IPv4 et IPv6).</p>
nom de groupe IPMP	<p>Voir interface IPMP.</p> <p>Fait référence au nom d'un groupe IPMP, qui peut être affecté avec la sous-commande <code>ipadm set -i fprop</code>. Toutes les interfaces sous-jacentes avec le même nom de groupe IPMP sont définis dans le cadre du même groupe IPMP. Dans l'implémentation actuelle, les noms de groupe IPMP perdent en importance en faveur des noms d'interface IPMP. Les administrateurs sont invités à utiliser le même nom à la fois pour l'interface IPMP et le groupe à l'aide la sous-commande <code>ipadm create -i mp</code> pour créer le groupe IPMP.</p>
interface IPMP	<p>S'applique uniquement à l'implémentation d'IPMP actuelle. Le terme fait référence à l'interface IP qui représente un certain groupe IPMP, tout ou partie des interfaces sous-jacentes de l'interface et toutes les adresses de données. Dans l'implémentation actuelle d'IPMP, l'interface IPMP est le principal composant de gestion d'un groupe IPMP et est utilisée dans les tables de routage, tables ARP, règles de pare-feu, etc.</p>
nom d'interface IPMP	<p>Indique le nom d'une interface IPMP. Ce document utilise la convention de nommage <code>ipmpn</code>. Le système utilise aussi la même convention de nommage dans la création d'interface IPMP implicite. Toutefois, l'administrateur peut choisir n'importe quel nom en utilisant une création d'interface IPMP explicite.</p>

singleton IPMP

Fait référence à une configuration d'IPMP utilisée par le logiciel Oracle Solaris Cluster qui permet à une adresse de données d'agir également comme une adresse de test. Cette configuration s'applique, par exemple, lorsqu'une seule interface appartient à un groupe IPMP.

détection de défaillance basée sur les liaisons

Spécifie une forme passive de détection de défaillance, dans laquelle l'état de liaison de la carte réseau est surveillé pour déterminer l'état d'une interface. La détection de défaillance basée sur les liaisons vérifie uniquement si la liaison est active. Ce type de détection de défaillance n'est pas pris en charge par tous les pilotes de carte réseau. La détection de défaillance basée sur les liaisons ne nécessite aucune configuration explicite et fournit une détection de défaillance de liaison instantanée.

Comparée à la détection de défaillance basée sur sonde.

répartition de charge

Fait référence au processus consistant à distribuer le trafic entrant et sortant au sein d'un groupe d'interfaces. Contrairement à l'équilibrage de charge, la répartition de charge ne garantit pas que la charge soit répartie de manière égale. La répartition de charge permet d'augmenter le rendement. Elle ne se produit que lorsque le trafic réseau se dirige vers plusieurs destinations utilisant plusieurs connexions.

La répartition de charge entrante indique le processus de distribution du trafic entrant sur l'ensemble des interfaces d'un groupe IPMP. La répartition de charge entrante ne peuvent pas être contrôlée directement avec IPMP. Le processus est indirectement manipulé par l'algorithme de sélection de d'adresse source.

La répartition de charge sortante fait référence au processus de distribution du trafic sortant sur l'ensemble des interfaces d'un groupe

	<p>IPMP. La répartition de charge sortante est effectuée sur un système par destination par le module IP et est ajustée si nécessaire en fonction de l'état et des membres des interfaces dans le groupe IPMP.</p>
adresse NOFAILOVER	<p>S'applique uniquement à l'implémentation d'IPMP précédente. Fait référence à une adresse associée à une interface sous-jacente et qui reste donc indisponible si l'interface sous-jacente échoue. Toutes les adresses NOFAILOVER portent l'indicateur NOFAILOVER. Les adresses de test IPMP doivent être désignées comme NOFAILOVER, tandis que les adresses de données IPMP ne doivent jamais être désignées comme NOFAILOVER. Le concept de basculement n'existe pas dans l'implémentation d'IPMP. Cependant, le terme NOFAILOVER reste pour des raisons de compatibilité administrative.</p>
interface OFFLINE	<p>Indique une interface qui a été désactivée du système par l'administrateur, généralement en préparation de sa suppression du système. Ce type d'interfaces porte l'indicateur OFFLINE. La commande <code>if_mpadm</code> peut être utilisée pour faire passer une interface à un état hors ligne.</p>
interface physique	<p>Voir : interface sous-jacente</p>
sonde	<p>Fait référence à un paquet ICMP, similaire à l'envoi de paquets qui utilisés par la commande <code>ping</code>. Cette sonde sert à tester les chemins d'envoi et de réception d'une interface donnée. Des paquets de test sont envoyés par le démon <code>in.mpathd</code> si la détection de défaillance basée sur sonde est activée. Un paquet de sonde utilise une adresse de test IPMP comme adresse source.</p>
détection de défaillance basée sur sonde	<p>Indique une forme active de détection de défaillance, dans laquelle les sondes sont échangées avec les cibles de sondes pour déterminer l'état d'une interface. Lorsque cette option est activée, la détection de défaillance basée sur sonde teste l'ensemble du chemin</p>

	<p>d'envoi et de réception de chaque interface. Toutefois, ce type de détection nécessite que l'administrateur configure explicitement chaque interface avec une adresse de test.</p> <p>Comparée à la détection de défaillance basée sur les liaisons.</p>
cible de sonde	<p>Fait référence à un système sur la même liaison qu'une interface dans un groupe IPMP. La cible est sélectionnée par le démon <code>in.mpathd</code> pour aider à vérifier l'état d'une interface donnée à l'aide de la détection de défaillance basée sur sonde. La cible de sonde peut être n'importe quel hôte sur la liaison capable d'envoyer et de recevoir des sondes ICMP. Les cibles de sondes sont généralement des routeurs. Plusieurs cibles de sondes sont généralement utilisées pour isoler la détection de défaillance de défaillances des cibles de sondes elles-mêmes.</p>
sélection d'adresse source	<p>Fait référence au processus de sélection d'une adresse de données dans le groupe IPMP comme adresse source pour un paquet particulier. La sélection d'adresse source est effectuée par le système lorsqu'une application n'a pas spécialement sélectionné une adresse source à utiliser. Etant donné que chaque adresse de données est associée à une seule adresse matérielle, la sélection d'adresse source contrôle indirectement la répartition de charge entrante.</p>
interface STANDBY	<p>Indique une interface qui a été administrativement configurée pour être utilisée uniquement lorsqu'une autre interface du groupe a échoué. Toutes interfaces STANDBY porte l'indicateur STANDBY.</p>
système cible	<p>Voir cible de sonde.</p>
adresse de test	<p>Fait référence à une adresse IP à utiliser comme adresse source ou cible de test et non comme adresse source ou cible du trafic des données. Les adresses test sont associées à une</p>

	<p>interface sous-jacente. Si une interface sous-jacente est configurée avec une adresse de test UP, le démon <code>in.mpathd</code> surveille cette adresse à l'aide de la détection de défaillance basée sur sonde. Toutes les adresses de test doivent être désignées comme <code>NOFAILOVER</code>. Ces adresses sont également automatiquement marquées <code>DEPRECATED</code> par le système pour s'assurer qu'elles ne sont considérées comme de possibles adresses source pour les paquets de données.</p>
interface sous-jacente	<p>Spécifie une interface IP qui fait partie d'un groupe IPMP et est directement associée à un véritable périphérique réseau. Si, par exemple, <code>ce0</code> et <code>ce1</code> sont placées dans le groupe IPMP <code>imp0</code>, alors <code>ce0</code> et <code>ce1</code> constituent les interfaces sous-jacentes de <code>imp0</code>. Dans l'implémentation précédente, les groupes IPMP sont constitués uniquement d'interfaces sous-jacentes. Cependant, dans l'implémentation actuelle, ces interfaces sont sous-jacentes à l'interface IPMP (par exemple, <code>imp0</code>) qui représente le groupe, d'où le nom.</p>
opération annuler-hors ligne	<p>Fait référence à l'acte d'activer administrativement une interface précédemment hors ligne pour être utilisée par le système. La commande <code>if_mpadm</code> peut être utilisée pour effectuer une opération annuler-hors ligne.</p>
interface inutilisable	<p>Fait référence à une interface sous-jacente qui ne peut pas être utilisé du tout pour envoyer ou recevoir du trafic de données dans sa configuration actuelle. Une interface inutilisable diffère d'une interface <code>INACTIF</code>, qui n'est pas actuellement utilisée, mais peut être utilisée si une interface active dans le groupe devient inutilisable. Une interface est inutilisable si l'une des conditions suivantes existe :</p> <ul style="list-style-type: none"><li>■ L'interface n'a aucune adresse UP.</li></ul>



adresse UP

- L'indicateur FAILED ou OFFLINE a été défini pour l'interface.
- L'interface a été marqué comme ayant la même adresse matérielle comme une autre interface du groupe.

Fait référence à une adresse qui a été rendu administrativement disponible au système en définissant l'indicateur UP. Une adresse qui n'est pas UP est traitée comme n'appartenant pas au système et donc n'est jamais prise en compte pendant la sélection d'adresse source.



## Administration d'IPMP

---

Ce chapitre décrit les tâches relatives à l'administration des groupes d'interfaces avec IPMP (multipathing sur réseau IP). Les rubriques traitées sont les suivantes :

- “Liste des tâches d'administration d'IPMP” à la page 299
- “Configuration de groupes IPMP” à la page 302
- “Maintenance de groupes IPMP” à la page 310
- “Configuration pour la détection de défaillance basée sur sonde ” à la page 314
- “Restauration d'une configuration d'IPMP avec la reconfiguration dynamique ” à la page 317
- “Contrôle des informations d'IPMP” à la page 319

### Liste des tâches d'administration d'IPMP

Dans Oracle Solaris, la commande `impstat` est l'outil préféré à utiliser pour obtenir des informations sur le groupe IPMP. Dans ce chapitre, la commande `impstat` remplace certaines fonctions de la commande `ifconfig` qui ont été utilisées dans les précédentes versions d'Oracle Solaris pour fournir des informations IPMP.

Pour plus d'informations sur les différentes options pour la commande `impstat`, reportez-vous à la section “[Contrôle des informations d'IPMP](#)” à la page 319.

Les sections qui suivent fournissent des liens vers les tâches décrites dans ce chapitre.

## Création et configuration de groupe IPMP (liste des tâches)

Tâche	Description	Voir
Planification d'un groupe IPMP.	Répertorie la totalité des informations complémentaires et des tâches requises préalables à la configuration d'un groupe IPMP.	<a href="#">“Procédure de planification pour un groupe IPMP” à la page 302</a>
Configuration d'un groupe IPMP à l'aide du DHCP.	Fournit une méthode alternative pour configurer les groupes IPMP à l'aide du DHCP.	<a href="#">“Procédure de configuration d'un groupe IPMP à l'aide du protocole DHCP ” à la page 304</a>
Configuration d'un groupe IPMP actif-actif.	Configure un groupe IPMP dans lequel toutes les interfaces sous-jacentes sont déployées pour héberger le trafic réseau.	<a href="#">“Procédure de configuration manuelle d'un groupe IPMP actif-actif” à la page 306</a>
Configuration d'un groupe IPMP active-de réserve.	Configure un groupe IPMP dans lequel une interface sous-jacente est gardée inactive comme réserve.	<a href="#">“Procédure de configuration manuelle d'un groupe IPMP actif-de réserve” à la page 308</a>

## Maintenance des groupes IPMP (liste des tâches)

Tâche	Description	Voir
Ajout d'une interface à un groupe IPMP	Configuration d'une nouvelle interface en tant que membre d'un groupe IPMP existant.	<a href="#">“Procédure d'ajout d'une interface à un groupe IPMP” à la page 310</a>
Retrait d'une interface d'un groupe IPMP	Retire une interface d'un groupe IPMP.	<a href="#">“Procédure de suppression d'une interface d'un groupe IPMP” à la page 310</a>
Ajout d'adresses IP ou suppression d'adresses IP d'un groupe IPMP	Ajoute ou supprime des adresses d'un groupe IPMP.	<a href="#">“Procédure d'ajout ou de suppression d'adresses IP ” à la page 311</a>
Modification de l'appartenance d'une interface IPMP	Déplace des interfaces au sein de groupes IPMP.	<a href="#">“Procédure de déplacement d'une interface d'un groupe IPMP vers un autre” à la page 312</a>
Suppression d'un groupe IPMP	Supprime un groupe IPMP qui n'est plus nécessaire.	<a href="#">“Procédure de suppression d'un groupe IPMP” à la page 313</a>

Tâche	Description	Voir
Remplacement de cartes ayant échoué	Supprime ou remplace des cartes réseau défaillantes d'un groupe IPMP.	<a href="#">“Procédure de remplacement d'une carte physique qui a échoué” à la page 318</a>

## Configuration de la détection de défaillance basée sur sonde (liste des tâches)

Tâche	Description	Voir
Spécification manuelle de systèmes cible	Identifie et ajoute des systèmes à cibler pour la détection de défaillance basée sur sonde.	<a href="#">“Procédure de spécification manuelle de systèmes cible pour la détection de défaillance basée sur sonde” à la page 315</a>
Configuration du comportement de la détection de défaillance basée sur sonde	Modifie les paramètres pour déterminer le comportement de la détection de défaillance basée sur sonde.	<a href="#">“Procédure de configuration du comportement du démon IPMP ” à la page 316</a>

## Contrôle des groupes IPMP (liste des tâches)

Tâche	Description	Voir
Obtention d'informations de groupe	Affiche des informations sur un groupe IPMP.	<a href="#">“Procédures d'obtention d'informations sur le groupe IPMP” à la page 320</a>
Obtention d'informations sur les adresses de données	Affiche des informations sur les adresses de données qui sont utilisées par un groupe IPMP.	<a href="#">“Procédures d'obtention d'informations sur les adresses de données IPMP” à la page 321</a>
Obtention d'informations sur les interfaces IPMP	Affiche des informations sur les interfaces sous-jacentes d'interfaces ou de groupes IPMP.	<a href="#">“Procédure d'obtention d'informations sur les interfaces IP sous-jacentes d'un groupe ” à la page 322</a>
Obtention d'informations sur les cibles de sonde	Affiche d'informations sur les cibles de sonde de la détection de défaillance basée sur sonde.	<a href="#">“Procédures d'obtention d'informations sur les cibles de sonde IPMP ” à la page 323</a>
Obtention d'informations sur les sondes	Affiche des informations en temps réel sur les sondes en cours dans le système.	<a href="#">“Procédure d'observation des sondes IPMP ” à la page 325</a>

Tâche	Description	Voir
Personnalisation de l’affichage des informations de contrôle des groupes IPMP	Détermine les informations d’IPMP à afficher.	<a href="#">“Procédure de personnalisation de la sortie de la commande <code>ipmpstat</code> dans un script” à la page 326</a>

# Configuration de groupes IPMP

Cette section décrit les procédures qui sont utilisées pour planifier et configurer des groupes IPMP. La présentation du [Chapitre 14, “Présentation d’IPMP”](#) décrit l’implémentation du groupe IPMP en tant qu’interface. Par conséquent, les termes *groupe IPMP* et *interface IPMP* sont utilisés de façon interchangeable.

## ▼ Procédure de planification pour un groupe IPMP

La procédure suivante inclut les tâches de planification et les informations requise à collecter préalablement à la configuration du groupe IPMP. Il n’est pas obligatoire de réaliser les tâches dans l’ordre dans lequel elles sont décrites.

---

**Remarque** – Vous ne devez configurer qu’un seul groupe IPMP pour chaque sous-réseau ou domaine de diffusion L2. Pour plus d’informations, reportez-vous à la section [“Quand utiliser IPMP” à la page 269](#).

---

### 1 Déterminer la configuration générale d’IPMP qui correspondrait à vos besoins.

Votre configuration d’IPMP dépend de ce dont votre réseau d’entreprise a besoin pour gérer le type de trafic qui est hébergé sur votre système. IPMP répartit les paquets réseau sortants sur l’ensemble des interfaces du groupe IPMP et améliore donc le débit du réseau. Toutefois, pour une connexion TCP donnée, le trafic entrant suit généralement un seul chemin d’accès physique pour minimiser le risque de traiter des paquets hors-service.

Par conséquent, si votre réseau traite un gros volume de trafic sortant, la configuration d’un grand nombre d’interfaces dans un groupe IPMP peut améliorer les performances du réseau. Si au lieu de cela, le système héberge un trafic entrant important, le nombre d’interfaces dans le groupe n’améliore pas nécessairement les performances en répartissant la charge le trafic. Toutefois, le fait de disposer de plus d’interfaces sous-jacentes permet de garantir la disponibilité du réseau lors d’une défaillance d’interface.

### 2 Pour les systèmes SPARC, vérifiez que chaque interface du groupe dispose d’une adresse MAC unique.

Pour configurer une adresse MAC unique pour chaque interface du système, reportez-vous à la section [“SPARC : Garantie de l’unicité de l’adresse MAC d’une interface” à la page 181](#).

### 3 Assurez-vous que le même ensemble de modules STREAMS est déplacé et configuré sur toutes les interfaces du groupe IPMP.

Toutes les interfaces d'un même groupe doivent disposer de modules STREAMS configurés selon le même ordre.

#### a. Vérifiez l'ordre des modules STREAMS sur toutes les interfaces du groupe IPMP futur.

Vous pouvez imprimer une liste de modules STREAMS à l'aide de la commande `ifconfig interface modlist`. Voici un exemple de sortie de la commande `ifconfig` pour une interface `net0` :

```
# ifconfig net0 modlist
0 arp
1 ip
2 e1000g
```

Comme le montre la sortie, les interfaces existent normalement en tant que pilotes réseau directement sous le module IP. Aucune configuration supplémentaire ne devrait être nécessaire pour ces interfaces.

Cependant, certaines technologies s'insèrent sous la forme d'un module STREAMS entre le module IP et le pilote de réseau. Dans le cas d'un module STREAMS avec état, des comportements inattendus peuvent être observés lors du basculement, même en cas de déplacement d'un même module sur toutes les interfaces d'un groupe. Cependant, vous pouvez utiliser des modules STREAMS sans état, à condition que vous les déplaçiez selon le même ordre sur toutes les interfaces du groupe IPMP.

#### b. Déplacez les modules d'une interface selon l'ordre standard pour le groupe IPMP.

```
ifconfig interface modinsert module-name@position
```

```
ifconfig net0 modinsert vpnmod@3
```

### 4 Utilisez le même format d'adressage IP sur toutes les interfaces du groupe IPMP.

Si une interface est configurée pour IPv4, toutes les interfaces du groupe doivent être configurées pour IPv4. Si par exemple, vous ajoutez l'adressage IPv6 à une interface, toutes les interfaces du groupe IPMP doivent être configurées pour la prise en charge d'IPv6.

### 5 Déterminez le type de détection de défaillance que vous souhaitez implémenter.

Par exemple, si vous voulez implémenter la détection de défaillance basée sur sonde, vous devez configurer les adresses de test sur les interfaces sous-jacentes. Pour plus d'informations, reportez-vous à la section [“Types de détection de défaillance dans IPMP”](#) à la page 281.

### 6 Assurez-vous que toutes les interfaces du groupe IPMP sont connectées au même réseau local.

Par exemple, vous pouvez configurer les commutateurs Ethernet sur le même sous-réseau IP dans un groupe IPMP. Vous pouvez configurer le nombre d'interfaces de votre choix dans un groupe IPMP.

**Remarque** – Vous pouvez également configurer un groupe IPMP à interface unique, par exemple, si le système ne dispose que d'une interface physique. Pour plus d'informations, reportez-vous à la section [“Types de configurations d'interface IPMP” à la page 279](#).

---

**7 Assurez-vous que le groupe IPMP ne contient pas d'interfaces avec différents types de média réseau.**

Les interfaces regroupées doivent être du même type, comme défini dans `/usr/include/net/if_types.h`. Par exemple, vous ne pouvez pas combiner les interfaces Ethernet et Token ring dans un groupe IPMP. En outre, vous ne pouvez pas combiner un bus d'interfaces Token avec des interfaces ATM (Asynchronous Transfer Mode, mode de transfert asynchrone) dans le même groupe IPMP.

**8 En cas d'IPMP avec interfaces ATM, configurez les interfaces ATM en mode d'émulation LAN.**

IPMP n'est pas pris en charge par les interfaces préférant l'IP classique à l'ATM.

## ▼ **Procédure de configuration d'un groupe IPMP à l'aide du protocole DHCP**

Dans l'implémentation actuelle d'IPMP, des groupes IPMP peuvent être configurés avec le protocole DHCP (Dynamic Host Configuration Protocol), prise en charge.

Un groupe IPMP à plusieurs interfaces peut être configuré à l'aide d'interfaces actives-actives ou actives-de réserve. Pour plus d'informations, reportez-vous à la section [“Types de configurations d'interface IPMP” à la page 279](#). La procédure suivante décrit les étapes de configuration d'un groupe IPMP active-de réserve à l'aide du protocole DHCP.

**Avant de commencer**

Assurez-vous que les interfaces IP qui seront dans le groupe IPMP ont été correctement configurées sur les liaisons de données du système. Vous pouvez créer une interface IPMP même si des interfaces IP sous-jacentes n'existent pas encore. Cependant, les configurations suivantes sur cette interface IPMP échoueront.

Pour plus d'informations sur les procédures de configuration de liaisons et d'interfaces IP, reportez-vous à la section [“Configuration d'interfaces IP \(tâches\)” à la page 181](#). Pour plus d'informations sur les interfaces IPv6, reportez-vous à la section [“Configuration d'une interface IPv6” du manuel \*Administration d'Oracle Solaris : Services IP\*](#).

En outre, si vous utilisez un système SPARC, configurer une adresse MAC unique pour chaque interface. Pour obtenir les procédures, reportez-vous à la section [“SPARC : Garantie de l'unicité de l'adresse MAC d'une interface” à la page 181](#).

Enfin, si vous utilisez DHCP, assurez-vous que les interfaces sous-jacentes ont des baux infinis. Sinon, dans le cas d'une défaillance de groupe, les adresses de test expirent et le démon d'IPMP désactive la détection de défaillance basée sur sonde et la détection de défaillance basée sur les



liaisons sera utilisée. Si la détection de défaillance basée sur les liaisons découvre que l'interface fonctionne, le démon peut incorrectement signaler que l'interface a été réparée. Pour plus d'informations sur la configuration DHCP, reportez-vous au [Chapitre 13, “Planning for DHCP Service \(Tasks\)”](#) du manuel *System Administration Guide: IP Services*.

---

**Remarque** – Vous ne pouvez pas utiliser IPMP si le profil réseau actif sur le système est un profil réactif. Avant de configurer les groupes IPMP, activez si nécessaire le profil `DefaultFixed` pour passer à un profil de configuration réseau fixe. Pour plus d'informations sur les procédures, reportez-vous à la section “[Profils et des outils de configuration](#)” à la page 154.

---

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Créez une interface IPMP.

```
# ipadm create-ipmp ipmp-interface
```

où

*ipmp-interface* spécifie le nom de l'interface IPMP. Vous pouvez attribuer n'importe quel nom significatif à l'interface IPMP. Comme avec n'importe quelle interface IP, le nom est constitué d'une chaîne de caractères et d'un chiffre, comme `ipmp0`.

### 3 Créer les interfaces IP sous-jacentes si elles n'existent pas encore.

```
# ipadm create-ip under-interface
```

où *under-interface* fait référence à l'interface IP que vous allez ajouter au groupe IPMP.

### 4 Ajoutez des interfaces IP sous-jacentes qui contiendront des adresses de test au groupe IPMP.

```
# ipadm add-ipmp -i under-interface1 [-i under-interface2 ...] ipmp-interface
```

Vous pouvez créer autant d'interfaces IP pour le groupe IPMP qu'il y en a de disponibles dans le système.

### 5 Faites configurer et gérer les adresses de données par DHCP sur l'interface IPMP.

```
# ipadm create-addr -T dhcp addrobj
```

*addrobj* représente un objet adresse et utilise le format *interface/string*. L'*interface* dans cette étape est l'interface IPMP. La chaîne peut être n'importe quelle chaîne définie par l'utilisateur. Par conséquent, si vous avez plusieurs adresses de données sur l'interface IPMP, les objets adresse correspondants sont *ipmp-interface/string1*, *ipmp-interface/string2*, *ipmp-interface/string3*, et ainsi de suite.

## 6 Faites gérer les adresses de test par DHCP dans les interfaces sous-jacentes.

Vous devez exécuter la commande suivante pour chaque interface sous-jacente du groupe IPMP.

```
# ipadm create-addr -T dhcp addrobj
```

*addrobj* représente un objet adresse et utilise le format *interface/string*. L'*interface* dans cette étape est l'interface sous-jacente. La chaîne peut être n'importe quelle chaîne définie par l'utilisateur. Par conséquent, si vous avez plusieurs adresses sous-jacentes pour le groupe IPMP, les objets adresse correspondants sont *under-interface/string1*, *under-interface /string2*, *under-interface/ string3*, et ainsi de suite.

### Exemple 15–1 Configuration d'un groupe IPMP avec DHCP

Cet exemple montre comment configurer un groupe IPMP active-de réserve sur le serveur DHCP et est basé sur le scénario suivant :

- Trois interfaces sous-jacentes pour le groupe IPMP seront configurées sur leurs liaisons de données respectives. *net0*, *net1*, et *net2* sont désignées membres du groupe IPMP.
- L'interface IPMP *itops0* partage le même nom avec le groupe IPMP.
- *net2* est désignée comme l'interface de réserve.
- Pour utiliser la détection de défaillance basée sur sonde, toutes les interfaces sous-jacentes se voient affecter des adresses de test.

```
# ipadm create-ipmp itops0

# ipadm create-ip net0
# ipadm create-ip net1
# ipadm create-ip net2

# ipadm add-ipmp -i net0 -i net1 -i net2 itops0

# ipadm create-addr -T dhcp itops0/dhcp0
# ipadm create-addr -T dhcp itops0/dhcp1

# ipadm create-addr -T dhcp net0/test
# ipadm create-addr -T dhcp net2/test
# ipadm create-addr -T dhcp net3/test

# ipadm set-ifprop -p standby=on net2
```

## ▼ Procédure de configuration manuelle d'un groupe IPMP actif-actif

La procédure ci-après décrit les étapes de configuration manuelle d'un groupe IPMP actif-actif.

**Avant de commencer**

Assurez-vous que les interfaces IP qui seront dans le groupe IPMP potentiel ont été correctement configurées sur les liaisons de données du système. Pour plus d'informations sur les procédures de configuration de liaisons et d'interfaces IP, reportez-vous à la section [“Configuration d'interfaces IP \(tâches\)” à la page 181](#). Pour plus d'informations sur les interfaces IPv6, reportez-vous à la section [“Configuration d'une interface IPv6” du manuel \*Administration d'Oracle Solaris : Services IP\*](#). Vous pouvez créer une interface IPMP même si des interfaces IP sous-jacentes n'existent pas encore. Cependant, les configurations suivantes sur cette interface IPMP échoueront.

En outre, si vous utilisez un système SPARC, configurer une adresse MAC unique pour chaque interface. Pour obtenir les procédures, reportez-vous à la section [“SPARC : Garantie de l'unicité de l'adresse MAC d'une interface” à la page 181](#).

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

**2 Créez une interface IPMP.**

```
# ipadm create-ipmp ipmp-interface
```

où

*ipmp-interface* spécifie le nom de l'interface IPMP. Vous pouvez attribuer n'importe quel nom significatif à l'interface IPMP. Comme avec n'importe quelle interface IP, le nom est constitué d'une chaîne de caractères et d'un chiffre, comme *ipmp0*.

**3 Ajoutez interfaces IP sous-jacentes au groupe.**

```
# ipadm add-ipmp -i under-interface1 [-i underinterface2 ...] ipmp-interface
```

où *under-interface* fait référence à l'interface sous-jacente du groupe IPMP. Vous pouvez ajouter autant interfaces IP qu'il y en a de disponibles dans le système.

---

**Remarque** – Dans un environnement à double pile, si l'on place l'instance IPv4 d'une interface dans un groupe particulier, l'instance IPv6 est automatiquement placée dans ce même groupe.

---

**4 Ajoutez des adresses de données à l'interface IPMP.**

```
# ipadm create-addr -T static IP-address addrobj
```

L'*IP-address* peut être en notation CIDR.

*addrobj* doit utiliser la convention de nommage *ipmp-interface/any-string*. Par conséquent, si le nom de l'interface IPMP est *ipmp0*, *addrobj* peut être *ipmp0/dataaddr*.

**5 Ajoutez des adresses de test aux interfaces sous-jacentes.**

```
# ipadm create-addr -T static IP-address addrobj
```

L'*IP-address* peut être en notation CIDR.

*addrobj* doit utiliser la convention de nommage *under-interface/any-string*. Par conséquent, si le nom d'une interface sous-jacente est *net0*, *addrobj* peut être *net0/testaddr*.

---

**Remarque** – La configuration d'une adresse test est nécessaire uniquement si vous souhaitez utiliser la détection de défaillance basée sur sonde sur une interface spécifique.

Toutes les adresses IP test d'un groupe IPMP doivent utiliser le même préfixe de réseau. Les adresses IP test doivent appartenir à un sous-réseau IP unique.

---

## ▼ Procédure de configuration manuelle d'un groupe IPMP actif-de réserve

Pour plus d'informations sur interfaces de réserve, reportez-vous à la section “[Types de configurations d'interface IPMP](#)” à la page 279. La procédure suivante permet de configurer un groupe IPMP où l'une interface est maintenue en réserve. Cette interface est déployée uniquement lorsqu'une interface active dans le groupe échoue.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Créez une interface IPMP.

```
# ipadm create-ipmp ipmp-interface
```

où

*ipmp-interface* spécifie le nom de l'interface IPMP. Vous pouvez attribuer n'importe quel nom significatif à l'interface IPMP. Comme avec n'importe quelle interface IP, le nom est constitué d'une chaîne de caractères et d'un chiffre, comme *ipmp0*.

### 3 Ajoutez interfaces IP sous-jacentes au groupe.

```
# ipadm add-ipmp -i under-interface1 [-i underinterface2 ...] ipmp-interface
```

où *under-interface* fait référence à l'interface sous-jacente du groupe IPMP. Vous pouvez ajouter autant interfaces IP qu'il y en a de disponibles dans le système.

---

**Remarque** – Dans un environnement à double pile, si l'on place l'instance IPv4 d'une interface dans un groupe particulier, l'instance IPv6 est automatiquement placée dans ce même groupe.

---

### 4 Ajoutez des adresses de données à l'interface IPMP.

```
# ipadm create-addr -T static IP-address addrobj
```

L'*IP-address* peut être en notation CIDR.

*addrobj* doit utiliser la convention de nommage *ipmp-interface/any-string*. Par conséquent, si le nom de l'interface IPMP est *ipmp0*, *addrobj* peut être *ipmp0/dataaddr*.

## 5 Ajoutez des adresses de test aux interfaces sous-jacentes.

```
# ipadm create-addr -T static IP-address addrobj
```

L'*IP-address* peut être en notation CIDR.

*addrobj* doit utiliser la convention de nommage *under-interface/any-string*. Par conséquent, si le nom d'une interface sous-jacente est *net0*, *addrobj* peut être *net0/testaddr*.

---

**Remarque** – La configuration d'une adresse test est nécessaire uniquement si vous souhaitez utiliser la détection de défaillance basée sur sonde sur une interface spécifique.

Toutes les adresses IP test d'un groupe IPMP doivent utiliser le même préfixe de réseau. Les adresses IP test doivent appartenir à un sous-réseau IP unique.

---

## 6 Configurez l'une des interfaces sous-jacentes en tant qu'interface de réserve.

```
# ipadm set-ifprop -p standby=yes under-interface
```

### Exemple 15–2 Configuration d'un groupe IPMP active-de réserve

Cet exemple montre comment créer manuellement une configuration d'IPMP active-de réserve. L'exemple commence par créer les interfaces sous-jacentes.

```
# ipadm create-ip net0
# ipadm create-ip net1
# ipadm create-ip net2

# ipadm create-ipmp itops0

# ipadm add-ipmp -i net0 -i net1 -i net2 itops0
# ipadm create-addr -T static -a 192.168.10.10/24 itops0/v4add1
# ipadm create-addr -T static -a 192.168.10.15/24 itops0/v4add2

# ipadm create-addr -T static -a 192.168.85.30/24 net0/test
# ipadm create-addr -T static -a 192.168.85.32/24 net1/test
# ipadm create-addr -T static -a 192.168.85.34/24 net2/test

# ipadm set-ifprop -p standby=yes net2

# ipmpstat -g
GROUP      GROUPNAME  STATE      FDT        INTERFACES
itops0     itops0     ok         10.00s     net0 net1 (net2)

# ipmpstat -t
INTERFACE  MODE      TESTADDR   TARGETS
net0       routes    192.168.10.30  192.168.10.1
net1       routes    192.168.10.32  192.168.10.1
net2       routes    192.168.10.34  192.168.10.5
```

# Maintenance de groupes IPMP

Cette section décrit les tâches relatives à la maintenance de groupes IPMP existants et des interfaces qui composent ces groupes. Cette tâche suppose que vous avez déjà configuré un groupe IPMP, tel que décrit dans la section “[Configuration de groupes IPMP](#)” à la page 302.

## ▼ Procédure d'ajout d'une interface à un groupe IPMP

### Avant de commencer

Assurez-vous que l'interface que vous ajoutez au groupe respecte toutes les contraintes pour être dans le groupe. Pour obtenir la liste des exigences d'un groupe IPMP, reportez-vous à la section “[Procédure de planification pour un groupe IPMP](#)” à la page 302.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Si l'interface IP sous-jacente n'existe pas encore, créez l'interface.

```
# ipadm create-ip interface
```

#### 3 Ajoutez l'interface IP au groupe IPMP.

```
# ipadm add-ipmp -i under-interface ipmp-interface
```

### Exemple 15–3 Ajout d'une interface à un groupe IPMP

Pour ajouter l'interface net4 au groupe IPMP itops0, vous devez taper les commandes suivantes :

```
# ipadm create-ip net4
# ipadm add-ipmp -i net4 itops0
# ipmpstat -g
GROUP  GROUPNAME  STATE  FDT  INTERFACES
itops0 itops0     ok     10.00s  net0 net1 net4
```

## ▼ Procédure de suppression d'une interface d'un groupe IPMP

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Supprimez l'interface du groupe IPMP.

```
# ipadm remove-ipmp -i under-interface[, -i under-interface, ...] ipmp-interface
```

Vous pouvez supprimer autant d'interfaces sous-jacentes dans une seule commande selon les besoins. La suppression de toutes les interfaces sous-jacentes ne supprime pas l'interface IPMP. Existe plutôt comme interface ou groupe IPMP.

#### Exemple 15–4 Suppression d'une interface d'un groupe

Pour supprimer l'interface `net4` du groupe IPMP `itops0`, vous devez taper les commandes suivantes :

```
# ipadm remove-ipmp net4 itops0
# ipmpstat -g
GROUP    GROUPNAME    STATE    FDT    INTERFACES
itops0   itops0       ok       10.00s net0 net1
```

## ▼ Procédure d'ajout ou de suppression d'adresses IP

Vous utilisez la sous-commande `ipadm create-addr` pour ajouter des adresses ou la sous-commande `ipadm delete-addr` pour supprimer des adresses des interfaces. Dans l'implémentation actuelle d'IPMP, des adresses de test sont hébergées sur les IP sous-jacentes interface, tandis que les adresses de données sont affectées à l'interface IPMP. Les procédures ci-après décrivent comment ajouter ou supprimer des adresses IP qui sont des adresses de test ou des adresses de données.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Ajoutez ou supprimez des adresses de données.

- Pour ajouter des adresses de données au groupe IPMP, tapez la commande suivante :

```
# ipadm create-addr -T static -a ip-address addrobj
addrobj utilise la convention de nommage ipmp-interface/user-string.
```

- Pour supprimer une adresse du groupe IPMP, tapez la commande suivante :

```
# ipadm delete-addr addrobj
addrobj utilise la convention de nommage ipmp-interface/user-string.
```

### 3 Ajoutez ou supprimez des adresses de test.

- Pour affecter une adresse de test à une interface sous-jacente du groupe IPMP, tapez la commande suivante :

```
# ipadm create-addr -T static ip-address addrobj
```

- Pour supprimer une adresse de test d'une interface sous-jacente du groupe IPMP, tapez la commande suivante :

```
# ipadm delete-addr addrobj
```

### Exemple 15–5 Suppression d'une adresse de test d'une interface

L'exemple suivant utilise la configuration d'`itops0` dans l'[Exemple 15–2](#). L'étape supprime l'adresse de test de l'interface `net1`. Dans cet exemple, supposez que l'adresse de test soit nommée `net1/test1`

```
# ipmpstat -t
INTERFACE      MODE      TESTADDR      TARGETS
net1           routes    192.168.10.30  192.168.10.1

# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0          static    ok         127.0.0.1/8
...
net1/test1    static    ok         192.168.10.30

# ipadm delete-addr net1/test1
```

## ▼ Procédure de déplacement d'une interface d'un groupe IPMP vers un autre

Vous pouvez placer une interface dans un nouveau groupe IPMP lorsque l'interface appartient à un groupe IPMP. Il est inutile de supprimer l'interface du groupe IPMP actuel. Lorsque vous placez l'interface dans un nouveau groupe, l'interface est automatiquement retirée de tout groupe IPMP existant.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Déplacez l'interface vers un nouveau groupe IPMP.

```
# ipadm add-ipmp -i under-interface ipmp-interface
```

où *under-interface* fait référence à l'interface sous-jacente que vous souhaitez déplacer et *ipmp-interface* fait référence à l'interface ou au groupe IPMP dans lequel vous voulez placer l'interface sous-jacente.

Si vous placez l'interface dans un nouveau groupe, elle est automatiquement retirée de tout groupe existant.

### Exemple 15–6 Déplacement d'une interface vers un autre groupe IPMP

Cet exemple suppose que les interfaces sous-jacentes de votre groupe soient `net0`, `net11` et `net2`. Pour vous déplacer `net0` vers le groupe IPMP `cs-link1`, vous devez saisir la commande suivante :



```
# ipadm add-ipmp -i net0 ca-link1
```

Cette commande supprime l'interface `net0` du groupe IPMP `itops0` et met ensuite `net0` à `cs-link1`.

## ▼ Procédure de suppression d'un groupe IPMP

Utilisez cette procédure si vous n'avez plus besoin d'un groupe IPMP spécifique.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Identifiez le groupe IPMP et les interfaces IP sous-jacentes.

```
# ipmpstat -g
```

### 3 Supprimez toutes les interfaces IP qui appartiennent au groupe IPMP.

```
# ipadm remove-ipmp -i under-interface[, -i under-interface, ...] ipmp-interface
```

---

**Remarque** – Pour supprimer une interface IPMP, aucune interface IP ne doit exister en tant que partie du groupe IPMP.

---

### 4 Supprimer l'interface IPMP.

```
# ipadm delete-ipmp ipmp-interface
```

Une fois que vous avez supprimé l'interface IPMP, n'importe quelle adresse IP qui n'est associée à l'interface est supprimée du système.

## Exemple 15–7 Suppression d'une interface IPMP

Pour supprimer l'interface `itops0` qui a les interfaces IP sous-jacentes `net0` et `net1`, vous devez taper les commandes suivantes :

```
# ipmpstat -g
GROUP  GROUPNAME  STATE  FDT  INTERFACES
itops0  itops0     ok     10.00s  net0 net1

# ipadm remove-ipmp -i net0 -i net1 itops0

# ipadm delete-ipmp itops0
```

## Configuration pour la détection de défaillance basée sur sonde

La détection de défaillance basée sur sonde nécessite l'utilisation de systèmes cible, comme expliqué dans la section [“Détection de défaillance basée sur sonde” à la page 282](#). Pendant l'identification des cibles pour la détection de défaillance basée sur sonde, le démon `in.mpathd` fonctionne en deux modes : mode cible routeur ou mode cible multidiffusion. En mode cible routeur, le démon de multipathing test les cibles qui sont définies dans la table de routage. Si aucune cible n'est définie, le démon s'exécute en mode cible multidiffusion, où les paquets de multidiffusion sont envoyés tester les hôtes voisins sur le réseau local.

De préférence, vous devez définir les cibles d'hôte à tester par le démon `in.mpathd`. Pour certains groupes IPMP, le routeur par défaut est suffisant comme cible. Cependant, pour certains groupes IPMP, il est nécessaire de configurer des cibles spécifiques pour la détection de défaillance basée sur sonde. Pour spécifier les cibles, définissez des routes hôte dans la table de routage comme cibles de sonde. Les routes hôte configurées dans la table de routage figurent dans la liste avant le routeur par défaut. IPMP utilise les routes hôte définies explicitement pour la sélection de cibles. Par conséquent, vous devez définir des routes hôte afin de configurer des cibles de sondes plutôt que d'utiliser le routeur par défaut.

Pour définir des routes hôte dans la table de routage, utilisez la commande `route`. Vous pouvez utiliser l'option `-p` avec cette commande pour ajouter des routes permanentes. Par exemple, `route -p add` ajoute une route qui reste dans la table de routage même après la réinitialisation du système. L'option `-p` vous permet donc d'ajouter des routes persistantes sans avoir besoin de scripts spéciaux pour recréer ces routes à chaque démarrage du système. Pour mieux utiliser la détection de défaillance basée sur sonde, assurez-vous que vous avez défini plusieurs cibles pour recevoir les sondes.

L'exemple de procédure qui suit présente la syntaxe exacte pour ajouter des routes persistantes vers des cibles de détection de défaillance basée sur sonde. Pour plus d'informations sur les options pour la commande `route`, reportez-vous à la page de manuel [route\(1M\)](#).

Tenez compte des critères suivants lorsque vous devez sélectionner les hôtes de votre réseau les plus adaptés en tant que cibles.

- Assurez-vous que les cibles potentielles sont disponibles et en cours d'exécution. Etablissez la liste de leurs adresses IP.
- Assurez-vous que les interfaces cible se trouvent sur le même réseau que le groupe IPMP configuré.
- Le masque de réseau et l'adresse de diffusion des systèmes cible doivent être les mêmes que ceux du groupe IPMP.
- L'hôte cible doit pouvoir répondre aux requêtes ICMP provenant de l'interface qui utilise la détection de défaillance basée sur sonde.

## ▼ Procédure de spécification manuelle de systèmes cible pour la détection de défaillance basée sur sonde

- 1 Connectez-vous à l'aide de votre compte utilisateur au système dans lequel vous configurez la détection de défaillance basée sur sonde.
- 2 Ajoutez une route à un hôte spécifique, à utiliser en tant que cible dans le cadre de la détection de défaillance basée sur sonde.

```
$ route -p add -host destination-IP gateway-IP -static
```

où *destination-IP* et *gateway-IP* sont les adresses IPv4 de l'hôte à utiliser en tant que cible. Par exemple, saisissez ce qui suit afin de spécifier le système cible 192.168.10.137 qui se trouve sur le même sous-réseau que les interfaces du groupe IPMP `itops0`:

```
$ route -p add -host 192.168.10.137 192.168.10.137 -static
```

Cette nouvelle route est configurée automatiquement chaque fois que le système est redémarré. Si vous souhaitez définir une seule route temporaire à un système cible pour la détection de défaillance basée sur sonde, n'utilisez pas l'option `-p`.

- 3 Ajoutez les routes vers les hôtes supplémentaires du réseau à utiliser en tant que systèmes cible.

## ▼ Procédure de sélection de méthode de détection de défaillance à utiliser

Par défaut, la détection de défaillance basée sur sonde peut uniquement être exécutée en utilisant des adresses de test. Si le pilote de la carte réseau la prend en charge, la détection de défaillance basée sur les liaisons est également activée automatiquement.

Vous ne pouvez pas désactiver la détection de défaillance basée sur les liaisons si cette méthode est prise en charge par le pilote de la carte réseau. Cependant, vous pouvez sélectionner le type de la détection de défaillance basée sur sonde à implémenter.

- 1 Pour n'utiliser que le test transitif, effectuez les opérations suivantes :

- a. Utilisez les commandes SMF pour passer sur la propriété IPMP `transitive-probing`.

```
# svccfg -s svc:/network/ipmp setprop config/transitive-probing=true
# svcadm refresh svc:/network/ipmp:default
```

Pour plus d'informations sur la configuration de cette propriété, reportez-vous à la page de manuel [in.mpathd\(1M\)](#).

- b. Supprimez toutes les adresses de test existantes ayant été configurées pour le groupe IPMP.

**2 Pour n'utiliser que des adresses de test pour le test de défaillance, effectuez les opérations suivantes :**

**a. Si nécessaire, désactivez le test transitif.**

```
# svccfg -s svc:/network/ipmp setprop config/transitive-probing=false
# svcadm refresh svc:/network/ipmp:default
```

**b. Attribuer des adresses de test pour les interfaces sous-jacentes du groupe IPMP.**

## ▼ Procédure de configuration du comportement du démon IPMP

Le fichier de configuration IPMP `/etc/default/mpathd` permet de configurer les paramètres système suivants des groupes IPMP.

- `FAILURE_DETECTION_TIME`
- `TRACK_INTERFACES_ONLY_WITH_GROUPS`
- `FAILBACK`

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Modifiez le fichier `/etc/default/mpathd`.**

Modifiez la valeur par défaut d'au moins un des trois paramètres.

**a. Saisissez la nouvelle valeur du paramètre `FAILURE_DETECTION_TIME`.**

```
FAILURE_DETECTION_TIME=n
```

où *n* correspond à la durée en secondes nécessaire aux sondes ICMP pour la détection d'une éventuelle défaillance d'interface. La valeur par défaut est de 10 secondes.

**b. Saisissez la nouvelle valeur du paramètre `FAILBACK`.**

```
FAILBACK=[yes | no]
```

- *yes* – La valeur *yes* correspond au comportement de basculement par défaut d'IPMP. En cas de détection de réparation d'une interface défaillante, l'accès réseau est rétabli à l'aide de l'interface réparée, tel que décrit dans la section “[Détection de réparation d'interface physique](#)” à la page 284.
- *no* – La valeur *no* indique que le trafic de données n'est pas rétabli sur une interface réparée. En cas de détection d'une interface réparée, l'indicateur `INACTIVE` est défini pour celle-ci. L'indicateur indique qu'il est actuellement impossible d'utiliser l'interface pour le trafic de données. Il est cependant possible de l'utiliser pour le trafic de sondes.

Par exemple, le groupe IPMP `imp0` se compose de deux interfaces, `net0` et `net1`. Dans le fichier `/etc/default/mpathd`, le paramètre `FAILBACK=no` est défini. Si `net0` échoue, elle est marquée comme étant `FAILED` et devient inutilisable. Après réparation, l'interface est marquée comme étant `INACTIVE` et reste inutilisable en raison du paramètre `FAILBACK=no`.

Si `net1` échoue et qu'uniquement `net0` est dans l'état `INACTIVE`, `net0` voit son indicateur `INACTIVE` effacé et l'interface devient utilisable. Si le groupe IPMP dispose d'autres interfaces qui sont également dans l'état `INACTIVE`, alors n'importe laquelle de ces interfaces `INACTIVE`, et pas nécessairement `net0`, peut être effacée et devenir utilisable lorsque `net1` échoue.

**c. Saisissez la nouvelle valeur du paramètre `TRACK_INTERFACES_ONLY_WITH_GROUPS`.**

```
TRACK_INTERFACES_ONLY_WITH_GROUPS=[yes | no]
```

---

**Remarque** – Pour plus d'informations sur ce paramètre et la fonction de groupe anonyme, reportez-vous à la section “[Détection de défaillance et fonction de groupe anonyme](#)” à la page 284.

---

- *yes* – La valeur *yes* correspond au comportement par défaut d'IPMP. Ce paramètre permet à IPMP d'ignorer les interfaces réseau qui ne sont pas configurées dans un groupe IPMP.
- *no* – La valeur *no* définit la détection de défaillance et de réparation pour *toutes* les interfaces réseau, qu'elles soient configurées ou non dans un groupe IPMP. Cependant, lorsqu'une défaillance ou une réparation est détectée sur une interface non configurée dans un groupe IPMP, aucune action n'est déclenchée dans IPMP pour maintenir les fonctions réseau de cette interface. Par conséquent, la valeur *no* est utile uniquement pour les rapports de défaillances et n'améliore pas directement la disponibilité du réseau.

**3 Redémarrez le démon `in.mpathd`.**

```
# pkill -HUP in.mpathd
```

## Restauration d'une configuration d'IPMP avec la reconfiguration dynamique

Cette section décrit les procédures relatives à l'administration de systèmes prenant en charge la reconfiguration dynamique (DR).

## ▼ Procédure de remplacement d'une carte physique qui a échoué

Cette procédure explique la méthode de remplacement d'une carte physique d'un système prenant la DR en charge. La procédure suppose que les conditions suivantes :

- Le NCP actif de votre système est `DefaultFixed`. Reportez-vous à la section *Dynamic Reconfiguration and Network Configuration Profiles* in “[Fonctionnement de NWAM avec d'autres technologies de mise en réseau Oracle Solaris](#)” à la page 43 for information about using DR if your system's active NCP is not `DefaultFixed`.
- Les interfaces IP du système sont `net0` et `net1`.
- Les deux interfaces appartiennent au groupe IPMP, `itops0`.
- L'interface sous-jacente `net0` contient une adresse de test.
- L'interface sous-jacente `net0` a échoué, et vous devez supprimer la carte de `net0`, bge.
- Vous remplacez la carte bge par une carte `e1000g`.

### Avant de commencer

Les procédures d'exécution DR varie en fonction du type de système. Par conséquent, vérifiez les éléments suivants :

- Assurez-vous que votre système prend en charge la reconfiguration dynamique.
- Consultez le manuel approprié décrivant les procédures DR sur votre système. Pour le matériel Sun d'Oracle, tous les systèmes qui prennent en charge la reconfiguration dynamique sont des serveurs. Pour localiser la documentation sur la reconfiguration dynamique sur les systèmes Sun, recherchez "dynamic reconfiguration" à l'adresse suivante : <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

---

**Remarque** – Les étapes de la procédure suivante font uniquement référence aux aspects de la DR qui sont spécifiquement liés à IPMP et l'utilisation des noms de liaisons. La procédure ne comporte pas l'ensemble des étapes nécessaires pour effectuer la DR. Par exemple, certaines couches au-delà de la couche IP nécessitent quelques étapes de configuration manuelle, tel que pour ATM et d'autres services, si la configuration n'est pas automatisée. Consultez la documentation relative à la DR appropriée pour votre système.

Pour obtenir la procédure détaillée de remplacement de cartes réseau, reportez-vous à la section “[Procédure de remplacement d'une NIC avec la reconfiguration dynamique](#)” à la page 173.

---

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Suivez les étapes DR appropriées pour supprimer la carte réseau défaillante du système.**

Par exemple, vous pouvez supprimer la carte bge.

**3 Connectez la carte réseau de remplacement au système.**

Par exemple, vous devez installer la carte e1000g sur le même emplacement que la carte bge occupait. La liaison de données de e1000g prend le nom net0 et hérite de la configuration de cette liaison de données.

**4 Terminez le processus de reconfiguration dynamique en activant les nouvelles ressources de la NIC pour qu'elles soient disponibles pour une utilisation.**

Par exemple, vous utilisez la commande `cfgadm` pour effectuer cette étape. Pour plus d'informations, reportez-vous à la page de manuel [cfgadm\(1M\)](#).

Après cette étape, la nouvelle interface est configurée avec l'adresse de test ajoutée comme interface sous-jacente du groupe IPMP et déployée comme interface active ou de réserve, en fonction des configurations persistantes de net0. Le noyau peut allouer des adresses de données pour cette nouvelle interface en fonction des configurations permanentes de l'interface IPMP, `itops0`.

## Contrôle des informations d'IPMP

Les procédures suivantes utilisent la commande `ipmpstat`, ce qui vous permet de contrôler les différents aspects des groupes IPMP sur le système. Vous pouvez observer l'état du groupe IPMP dans son ensemble ou de ses interfaces IP sous-jacentes. Vous pouvez également vérifier la configuration des adresses de données et de test pour le groupe. La commande `ipmpstat` permet également d'obtenir plus d'informations sur la détection de défaillance. Pour plus d'informations sur la commande `ipmpstat` et ses options, reportez-vous à la page de manuel [ipmpstat\(1M\)](#).

Par défaut, les noms d'hôte sont affichés sur la sortie au lieu des adresses IP numériques, à condition que les noms d'hôtes existent. Pour afficher la liste des adresses IP numériques dans la sortie, utilisez l'option `-n` avec d'autres options pour afficher des informations spécifiques sur le groupe IPMP.

---

**Remarque** – Dans les procédures suivantes, l'utilisation de la commande `ipmpstat` ne nécessite pas privilèges d'administrateur système, sauf indication contraire.

---

## ▼ Procédures d'obtention d'informations sur le groupe IPMP

Utilisez cette procédure pour répertorier l'état des différents groupes IPMP sur le système, y compris l'état de leurs interfaces sous-jacentes. Si la détection de défaillance basée sur sonde est activée pour un groupe spécifique, la commande inclut également le temps de détection de défaillance pour ce groupe.

### ● Affichage d'informations relatives au groupe IPMP

```
$ ipmpstat -g
GROUP  GROUPNAME  STATE      FDT          INTERFACES
itops0  itops0      ok         10.00s       net0 net1
acctg1  acctg1      failed    --          [net3 net4]
field2  field2      degraded  20.00s       net2 net5 (net7) [net6]
```

GROUP	Spécifie le nom de l'interface IPMP. Dans le cas d'un groupe anonyme, ce champ est vide. Pour plus d'informations sur les groupes anonymes, reportez-vous à la page de manuel <a href="#">in.mpathd(1M)</a> .
GROUPNAME	Spécifie le nom du groupe IPMP. Dans le cas d'un groupe anonyme, ce champ est vide.
STATE	Indique l'état actuel d'un groupe, qui peut être l'un des suivants : <ul style="list-style-type: none"><li>■ <code>ok</code> indique que toutes les interfaces sous-jacentes du groupe IPMP sont utilisables.</li><li>■ <code>degraded</code> indique que certaines interfaces sous-jacentes du groupe sont inutilisables.</li><li>■ <code>failed</code> indique que toutes les interfaces du groupe sont inutilisables.</li></ul>
FDT	Indique le temps de détection de défaillance, si la détection de défaillance est activée. Si la détection de défaillance est désactivée, ce champ sera vide.
INTERFACES	Spécifie les interfaces sous-jacentes qui appartiennent à ce groupe. Dans ce champ, les interfaces actives sont répertoriées en premier, suivies des interfaces inactives et enfin des interfaces inutilisables. L'état de l'interface est indiqué par la manière dont elle est répertoriée : <ul style="list-style-type: none"><li>■ <i>interface</i> (sans parenthèses ou des crochets) indique une interface active. Les interfaces actives sont celles qui sont en cours d'utilisation par le système pour envoyer ou recevoir le trafic de données.</li><li>■ <i>(interface)</i> (avec des parenthèses) indique une interface fonctionnelle mais inactive. L'interface n'est pas en cours d'utilisation comme défini par la stratégie d'administration.</li><li>■ <i>[interface]</i> (avec des crochets) indique que l'interface est inutilisable car elle a échoué ou qu'elle a été mise hors ligne.</li></ul>



## ▼ Procédures d'obtention d'informations sur les adresses de données IPMP

Utilisez cette procédure pour afficher les adresses de données et le groupe auquel chaque adresse appartient. Les informations affichées incluent également les adresses disponibles pour l'utilisation, selon qu'elles ont été activées ou désactivées par la commande `ipadm [up-addr/down-addr]`. Vous pouvez également déterminer sur quelle interface entrante ou sortante une adresse peut être utilisée.

### ● Affichage d'informations relatives à l'adresse IPMP

```
$ ipmpstat -an
ADDRESS      STATE      GROUP      INBOUND      OUTBOUND
192.168.10.10 up         itops0     net0  net0  net1
192.168.10.15 up         itops0     net1  net0  net1
192.0.0.100  up         acctg1     --      --
192.0.0.101  up         acctg1     --      --
128.0.0.100  up         field2     net2      net2 net7
128.0.0.101  up         field2     net7      net2 net7
128.0.0.102  down       field2     --      --
```

- ADDRESS**      Spécifie le nom d'hôte ou l'adresse de données, si l'option `-n` est utilisée avec l'option `-a`.
- STATE**        Indique si l'adresse sur l'interface IPMP est up, et donc utilisable, ou down, et donc inutilisable.
- GROUP**        Spécifie l'interface IP IPMP qui héberge une adresse de données spécifique.
- INBOUND**      Identifie l'interface qui reçoit des paquets pour une adresse donnée. Les informations du champ peuvent changer en fonction des événements externes. Par exemple, si une adresse de données est arrêtée ou si aucune interface IP active ne reste dans le groupe IPMP, ce champ est vide. Le champ vide indique que le système n'accepte pas les paquets IP qui sont destinés à l'adresse indiquée.
- OUTBOUND**     Identifie l'interface qui envoie des paquets qui utilisent une adresse donnée comme adresse source. De la même manière que pour le champ **INBOUND**, le champ d'information **OUTBOUND** peut également différer selon les événements externes. Un champ vide indique que le système n'envoie pas de paquets à l'adresse source. Le champ peut être vide parce que l'adresse est arrêtée ou parce qu'il ne reste pas d'interfaces IP active dans le groupe.

# ▼ Procédure d'obtention d'informations sur les interfaces IP sous-jacentes d'un groupe

Utilisez cette procédure pour afficher des informations sur les interfaces IP sous-jacentes d'un groupe IPMP. Pour obtenir une description de la relation correspondante entre la carte réseau, la liaison de données et l'interface IP, reportez-vous à la section “[Pile réseau dans Oracle Solaris](#)” à la page 22.

## ● Affichage d'informations relatives à l'interface IPMP

```
$ ipmpstat -i
INTERFACE  ACTIVE  GROUP   FLAGS    LINK     PROBE    STATE
net0       yes    itops0  --mb---  up       ok       ok
net1       yes    itops0  - - - - -  up       disabled ok
net3       no     acctg1  - - - - -  unknown  disabled offline
net4       no     acctg1  is - - - -  down    unknown  failed
net2       yes    field2  --mb---  unknown  ok       ok
net6       no     field2  - i - - - -  up      ok       ok
net5       no     filed2  - - - - -  up      failed  failed
net7       yes    field2  --mb---  up      ok       ok
```

- INTERFACEIndique chaque interface sous-jacente de chaque groupe IPMP.
- ACTIVEIndique si l'interface fonctionne et en cours d'utilisation (yes) ou non (no).
- GROUPSpécifie le nom de l'interface IPMP. Dans le cas de groupes anonymes, ce champ est vide. Pour plus d'informations sur les groupes anonymes, reportez-vous à la page de manuel [in.mpathd\(1M\)](#).
- FLAGSIndique l'état de l'interface sous-jacente, qui peut être un ou n'importe quelle combinaison des éléments suivants :
  - i indique que l'indicateur INACTIVE est défini pour l'interface et par conséquent l'interface n'est pas utilisée pour envoyer ou recevoir le trafic de données.
  - s indique que l'interface est configurée pour être une interface de réserve.
  - m indique que l'interface est désignée par le système pour envoyer et recevoir le trafic de multidiffusion IPv4 pour le groupe IPMP.
  - b indique que l'interface est désignée par le système pour recevoir le trafic de diffusion pour le groupe IPMP.
  - M indique que l'interface est désignée par le système pour envoyer et recevoir le trafic de multidiffusion IPv6 pour le groupe IPMP.
  - d indique que l'interface est hors service et par conséquent inutilisable.
  - h indique que l'interface physique partage une adresse matérielle physique double avec une autre interface et a été mise hors ligne. L'indicateur h signifie que l'interface est inutilisable.

LINK	<p>Indique l'état de la détection de défaillance basée sur les liaisons, qui est l'un des états suivants :</p> <ul style="list-style-type: none"> <li>▪ up ou down indique la disponibilité ou l'indisponibilité d'une liaison.</li> <li>▪ unknown indique que le pilote ne prend pas en charge la notification si une liaison est up ou down et par conséquent ne détecte pas les changements d'état de liaison.</li> </ul>
PROBE	<p>Spécifie l'état de détection de défaillance basée sur sonde pour les interfaces qui ont été configurées avec une adresse test, comme suit :</p> <ul style="list-style-type: none"> <li>▪ ok indique que la sonde est fonctionnelle et active.</li> <li>▪ failed indique que la détection de défaillance basée sur sonde a détecté que l'interface n'est pas opérationnelle.</li> <li>▪ unknown indique qu'aucune cibles de sondes adéquate n'a été trouvée, et par conséquent les sondes ne peuvent pas être envoyées.</li> <li>▪ disabled indique qu'aucune adresse test IPMP n'est configurée sur l'interface. Par conséquent la détection de défaillance basée sur sonde est désactivée.</li> </ul>
STATE	<p>Spécifie l'état global de l'interface, comme suit :</p> <ul style="list-style-type: none"> <li>▪ ok indique que l'interface est en ligne et fonctionne normalement sur la base de la configuration des méthodes de détection de défaillance.</li> <li>▪ failed indique que l'interface ne fonctionne pas car la liaison de l'interface est hors service ou la détection de sonde a déterminé que l'interface n'est pas en mesure d'envoyer ou de recevoir le trafic.</li> <li>▪ offline indique que l'interface n'est pas disponible pour utilisation. En général, l'interface est passée hors ligne dans les circonstances suivantes : <ul style="list-style-type: none"> <li>▪ L'interface est en cours de test.</li> <li>▪ La reconfiguration dynamique est en cours d'exécution.</li> <li>▪ L'interface partage une adresse matérielle double avec une autre interface.</li> </ul> </li> <li>▪ unknown indique que l'état de l'interface IPMP ne peut pas être déterminé car aucune cible de sonde n'est trouvable pour la détection de défaillance basée sur sonde.</li> </ul>

## ▼ Procédures d'obtention d'informations sur les cibles de sonde IPMP

Utilisez cette procédure pour contrôler les cibles de sondes qui sont associées à chaque interface IP dans un groupe IPMP.

● Affichage des cibles de sondes IPMP

```
$ ipmpstat -nt
INTERFACE  MODE          TESTADDR      TARGETS
net0        routes        192.168.85.30  192.168.85.1 192.168.85.3
net1        disabled     --            --
net3        disabled     --            --
net4        routes        192.1.2.200    192.1.2.1
net2        multicast    128.9.0.200    128.0.0.1 128.0.0.2
net6        multicast    128.9.0.201    128.0.0.2 128.0.0.1
net5        multicast    128.9.0.202    128.0.0.1 128.0.0.2
net7        multicast    128.9.0.203    128.0.0.1 128.0.0.2
```

```
$ ipmpstat -nt
INTERFACE  MODE          TESTADDR      TARGETS
net3        transitive    <net1>         <net1> <net2> <net3>
net2        transitive    <net1>         <net1> <net2> <net3>
net1        routes        172.16.30.100  172.16.30.1
```

INTERFACE      Spécifie les interfaces sous-jacentes du groupe IPMP.

- MODE            Spécifie la méthode d'obtention des cibles de sonde.
- routes indique que la table de routage du système est utilisée pour rechercher des cibles de sondes.
  - mcast indique que des sondes ICMP multidiffusion sont utilisées pour rechercher des cibles.
  - disabled indique que la détection de défaillance basée sur sonde a été désactivée pour l'interface.
  - transitive indique qu'un test transitif est utilisé pour détecter une défaillance, comme indiqué dans le deuxième exemple. Notez que vous ne pouvez pas implémenter la détection de défaillance basée sur sonde en utilisant simultanément des sondes transitives et des adresses de test. Si vous ne souhaitez pas utiliser d' adresses test, vous devez alors passer au test transitif Si vous ne souhaitez pas utiliser le test transitif, vous devez configurer des adresses test. Pour obtenir une présentation générale, reportez-vous à la section “[Détection de défaillance basée sur sonde](#)” à la page 282.

TESTADDR       Spécifie le nom d'hôte ou, si l'option -n est utilisée avec l'option -t, l'adresse IP qui est assignée à l'interface pour envoyer et recevoir les sondes.

Si le test transitif est utilisé le nom de l'interface fait référence aux interfaces IP sous-jacentes qui ne sont pas activement utilisées pour recevoir des données. Les noms indiquent également que les sondes de test transitif sondes sont envoyées à l'adresse source de ces interfaces spécifiées. Pour que les interfaces IP sous-jacentes actives reçoivent des données, une adresse IP est affichée pour indiquer l'adresse source de sondes ICMP sortantes.

**Remarque** – Si une interface IP est configurée avec des adresses de test IPv4 et IPv6, les informations de cible de sonde sont affichées séparément pour chaque adresse de test.

**TARGETS** Répertorie les cibles de sondes actuelles dans une liste séparée par des espaces. Les cibles de sondes sont affichées en tant que noms d'hôte ou qu'adresses IP, si l'option `-n` est utilisée avec l'option `-t`.

## ▼ Procédure d'observation des sondes IPMP

Utilisez cette procédure pour observer les sondes en cours. Lorsque vous exécutez la commande pour observer des sondes, des informations sur l'activité des sondes sur le système sont constamment affichées jusqu'à ce que vous mettiez fin à la commande avec `Ctrl-C`. Vous devez disposer de privilèges d'administrateur principal pour exécuter cette commande.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel Administration d'Oracle Solaris : services de sécurité](#).

**2 Affichez les informations sur les sondes en cours**

```
# impstat -pn
TIME    INTERFACE  PROBE    NETRTT    RTT       RTTAVG    TARGET
0.11s   net0        589      0.51ms    0.76ms    0.76ms    192.168.85.1
0.17s   net4        612      --        --        --        192.1.2.1
0.25s   net2        602      0.61ms    1.10ms    1.10ms    128.0.0.1
0.26s   net6        602      --        --        --        128.0.0.2
0.25s   net5        601      0.62ms    1.20ms    1.00ms    128.0.0.1
0.26s   net7        603      0.79ms    1.11ms    1.10ms    128.0.0.1
1.66s   net4        613      --        --        --        192.1.2.1
1.70s   net0        603      0.63ms    1.10ms    1.10ms    192.168.85.3
^C
```

```
# impstat -pn
TIME    INTERFACE  PROBE    NETRTT    RTT       RTTAVG    TARGET
1.39s   net4        t28      1.05ms    1.06ms    1.15ms    <net1>
1.39s   net1        i29      1.00ms    1.42ms    1.48ms    172.16.30.1
```

**TIME** Spécifie l'heure à laquelle une sonde a été envoyé par rapport à l'heure à laquelle la commande `impstat` a été émise. Si une sonde a été lancée avant le démarrage de la commande `impstat`, l'heure s'affiche avec une valeur négative, par rapport au moment de l'émission de la commande.

**INTERFACE** Spécifie l'interface sur laquelle la sonde est envoyée.

PROBE	Spécifie l'identificateur qui représente la sonde. Si le test transitif est utilisé pour détecter les défaillances, l'identificateur est précédé de <code>t</code> pour les tests transitifs ou <code>i</code> pour les sondes ICMP.
NETRTT	Spécifie le temps total d'aller-retour réseau de la sonde en millisecondes. NETRTT couvre le temps entre le moment où le module IP envoie la sonde et le moment où le module IP reçoit les paquets ack à partir de la cible. Si le démon <code>in.mpathd</code> a déterminé que la sonde est perdue, le champ est vide.
RTT	Spécifie le temps total d'aller-retour de la sonde en millisecondes. RTT couvre l'intervalle de temps entre le moment où le démon exécute le code pour envoyer la sonde et le moment où le démon termine le traitement des paquets ack à partir de la cible. Si le démon <code>in.mpathd</code> a déterminé que la sonde est perdue, le champ est vide. Les pics qui se produisent dans RTT qui ne sont pas présents dans NETRTT peuvent indiquer que le système local est surchargé.
RTTAVG	Spécifie le temps moyen d'aller-retour de la sonde sur l'interface entre le système local et la cible. Le temps moyen d'aller-retour permet d'identifier les cibles lentes. Si les données sont insuffisantes pour calculer la moyenne, ce champ est vide.
TARGET	Spécifie le nom d'hôte ou, si l'option <code>-n</code> est utilisée avec l'option <code>-p</code> , l'adresse cible à laquelle la sonde est envoyée.

## ▼ Procédure de personnalisation de la sortie de la commande `ipmpstat` dans un script

Lorsque vous utilisez la commande `ipmpstat`, par défaut, les champs plus significatifs qui tiennent dans 80 colonnes sont affichés. Dans la sortie, tous les champs qui sont spécifiques à l'option que vous pouvez utiliser avec la commande `ipmpstat` sont affichés, sauf dans le cas de la syntaxe `ipmpstat -p`. Si vous voulez spécifier les champs à afficher, utilisez l'option `-o` en association avec d'autres options qui déterminent le mode de sortie de la commande. Cette option est particulièrement utile lorsque vous exécutez la commande à partir d'un script ou à l'aide d'un alias de commande

### ● Pour personnaliser la sortie, lancer l'une des commandes suivantes :

- Pour afficher les champs sélectionnés de la commande `ipmpstat`, utilisez l'option `-o` en combinaison avec l'option de sortie spécifique. Par exemple, pour afficher uniquement les champs `GROUPNAME` et `STATE` du mode de sortie de groupe, vous devez saisir la commande suivante :

```
$ ipmpstat -g -o groupname,state
```

```
GROUPNAME  STATE
itops0     ok
```

```
accgt1      failed
field2      degraded
```

- Pour afficher tous les champs d'une commande `impstat`, utilisez la syntaxe suivante :

```
# impstat -o all
```

## ▼ Procédure de génération d'une sortie analysable par machine pour la commande `impstat`

Vous pouvez générer des informations analysables par machine avec la syntaxe `impstat -P`. L'option `-P` est conçue pour être utilisée particulièrement dans les scripts. La sortie analysable par machine diffère de la sortie normale de l'une des façons suivantes :

- Les en-têtes sont omis.
- Les champs sont séparés par le signe deux-points (:).
- Les champs avec des valeurs vides sont vides plutôt que d'être remplis avec le double tiret (--).
- Dans le cas de plusieurs champs faisant l'objet d'une demande, si un champ contient un caractère deux-points littéral (:) ou une barre oblique inverse (\), ceux-ci peuvent être remplacés par des caractères d'échappement ou exclu en faisant précéder les caractères d'une barre oblique inverse (\).

Pour utiliser correctement la syntaxe `impstat -P`, respectez les règles suivantes :

- Utilisez `-o option fields` avec l'option `-P`.
- N'utilisez jamais `-o all` avec l'option `-P`.

Ignorer l'une ou l'autre de ces règles cause l'échec de la commande `impstat -P`.

- **Pour afficher au format analysable par machine le nom de groupe, le temps de détection de défaillance et les interfaces sous-jacentes, vous devez saisir les informations suivantes :**

```
$ impstat -P -o -g groupname,fdt,interfaces
itops0:10.00s:net0 net1
acctg1::[net3 net4]
field2:20.00s:net2 net7 (net5) [net6]
```

Le nom de groupe, le temps de détection de défaillance et les interfaces sous-jacentes sont des champs d'informations de groupe. Par conséquent, vous pouvez utiliser les options `-o -g` avec l'option `-P`.

### Exemple 15-8 Utilisation de `impstat -P` dans un script

Cet exemple de script affiche le temps de détection de défaillance d'un groupe IPMP.

```
getfdt() {  
    ippstat -gP -o group,fdt | while IFS=: read group fdt; do  
        [[ "$group" = "$1" ]] && { echo "$fdt"; return; }  
    done  
}
```



## Echange d'informations sur la connectivité réseau à l'aide du protocole LLDP

---

Ce chapitre explique comment activer les systèmes afin d'échanger des informations sur la connectivité réseau et le système sur l'ensemble du réseau local à l'aide du protocole LLDP (Link Layer Discovery Protocol).

### Présentation du protocole LLDP dans Oracle Solaris

Le protocole LLDP permet de diffuser des informations dans l'ensemble d'un réseau local afin d'en découvrir la topologie. Avec ce protocole, un système peut diffuser des informations sur la connectivité et la gestion à d'autres systèmes sur le réseau. Ces informations peuvent inclure la capacité du système, les adresses de gestion et autres informations pertinentes. Ce protocole permet également d'utiliser ce même système pour recevoir des informations similaires sur les autres systèmes sur le même réseau local.

Dans Oracle Solaris, la prise en charge du protocole LLDP comprend également les fonctions DCB (Data Center Bridging) pour l'échange d'informations de configuration sur les fonctions DCB, telles que le contrôle de flux basé sur la priorité et la TLV d'application.

Grâce au protocole LLDP, l'administrateur système peut facilement détecter les configurations système défectueuses, notamment dans les réseaux complexes qui comprennent des réseaux locaux virtuels (VLAN), agrégations de liens et autres types de lien.

### Composants d'une implémentation LLDP

Le protocole LLDP est implémenté avec les composants suivants :

- Le package LLDP doit être installé pour activer la fonctionnalité LLDP. Ce package fournit le démon LLDP, des utilitaires de ligne de commande, le fichier manifeste et les scripts du service, ainsi que d'autres composants requis pour le bon fonctionnement du protocole LLDP.

- Le service `lldpd` est activé par la commande `svcadm`. Ce service gère le démon LLDP et est responsable du démarrage, de l'arrêt, du redémarrage ou de l'actualisation du démon. Il est désactivé par défaut. Par conséquent, pour utiliser le protocole LLDP, le service doit d'abord être activé à l'échelle globale du système. Une fois le service `lldpd` activé et le démon démarré, la fonctionnalité LLDP peut être activée sur des liens individuels, comme déterminé par l'administrateur système.
- La commande `lldpadm` gère le protocole LLDP sur des liens individuels et est utilisée, par exemple, pour configurer le mode de fonctionnement du protocole LLDP, indiquer les unités TLV (Type-Longueur-Valeur) qui seront transmises et configurer les informations relatives à l'application DCB. Plus précisément, la commande est utilisée pour définir les propriétés LLDP par agent, ainsi que les propriétés LLDP globales. Les sous-commandes générales de la commande `lldpadm` sont parallèles à celles des commandes `lcladm` et `ipadm`.
  - `lldpadm set -*` indique l'action à effectuer, dans laquelle une ou plusieurs valeurs sont définies pour une propriété LLDP donnée.
  - `lldpadm show -*` affiche les valeurs définies pour une propriété LLDP spécifiée.
  - `lldpadm reset -*` réinitialise la configuration d'une propriété LLDP spécifiée à ses valeurs par défaut.

L'utilisation de ces sous-commandes est illustrée dans les sections suivantes. Pour plus d'informations sur la commande `lldpadm`, reportez-vous à la page de manuel [lldpadm\(1M\)](#).

- La bibliothèque LLDP (`liblldp.so`) fournit des API qui peuvent être utilisées pour récupérer les informations LLDP sur un lien, analyser les paquets LLDP et exécuter d'autres fonctions.
- Les agents LLDP sont des instances LLDP associées avec les cartes d'interface réseau physiques sur lesquelles le protocole LLDP est activé. Un agent LLDP contrôle le comportement du protocole LLDP sur la carte d'interface réseau associée. Les agents LLDP peuvent uniquement être configurés sur les cartes d'interface réseau physiques.
- Le démon LLDP (`lldpd`) fonctionne en tant que responsable des agents LLDP sur le système. Il interagit avec `snmpd`, le démon du protocole SNMP (Simple Network Management Protocol), pour récupérer les informations LLDP reçues sur le système via SNMP. En outre, le démon poste des informations `sysevents` et répond aux requêtes de la bibliothèque LLDP.

La section suivante décrit l'agent LLDP plus en détail.

# Fonctionnalités de l'agent LLDP

L'agent LLDP transmet et reçoit des paquets LLDP, également appelés *unités de données de protocole*. L'agent gère et stocke les informations contenues dans ces paquets dans deux types de magasins de données :

- Base d'informations de gestion locale, ou MIB locale. Ce magasin de données contient les informations réseau relatives au lien spécifique sur lequel l'agent LLDP est activé. Une MIB locale contient à la fois les informations communes et uniques. Par exemple, l'ID du châssis fait partie des informations communes partagée entre tous les agents LLDP sur le système. Au contraire, les numéros de port sont différents pour les liaisons de données du système. Par conséquent, chaque agent gère sa propre MIB locale.
- MIB distante. Les informations stockées dans ce magasin de données se rapportent à d'autres systèmes sur le réseau local.

## Configuration du fonctionnement de l'agent LLDP

L'agent LLDP peut être configuré afin de fonctionner dans l'un des modes suivants :

- En mode de transmission uniquement (txonly), l'agent ne traite pas les paquets LLDP entrants. Par conséquent, la MIB distante est vide.
- En mode de réception uniquement (rxonly), l'agent ne traite que les paquets LLDP entrants et stocke les informations dans les MIB distantes. Cependant, aucune information provenant de la MIB locale n'est transmise.
- En mode de transmission et réception (both), l'agent transmet et reçoit les paquets LLDP. Les deux types de MIB sont utilisés. Ce mode active également automatiquement les fonctions DCB prises en charge par le lien sous-jacent.
- En mode désactivé (disable), l'agent n'existe pas.

### ▼ Activation du protocole LLDP

Cette procédure active le protocole LLDP sur votre système pour la première fois.

#### 1 Installez le package LLDP.

```
# pkg install lldp
```

---

**Remarque** – Pour obtenir un aperçu des packages Oracle Solaris et de leur installation, reportez-vous au [Chapitre 12, “Gestion des packages de logiciels \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

---

#### 2 Démarrez le service LLDP sur le système.

```
# svcadm enable svc:/network/lldp:default
```

- 3 Identifiez la liaison de données sur laquelle vous voulez activer le protocole LLDP.
- 4 Définissez le mode de fonctionnement pour l'agent LLDP sur cette liaison de données.

```
# lldpadm set-agentprop -p mode=value agent
```

où *value* peut être l'un des modes de fonctionnement, et *agent* utilise le nom de la liaison de données sur laquelle le protocole LLDP est activé.

---

**Remarque** – Les sous-commandes de la commande `lldpadm` peuvent être saisies sous forme abrégée afin de faciliter l'utilisation de la commande. Par exemple, `lldpadm set-agentprop` peut être saisi sous la forme `lldpadm set-ap`. Pour connaître les sous-commandes et leur forme abrégée, reportez-vous à la page de manuel [lldpadm\(1M\)](#).

---

- 5 Pour confirmer le mode de fonctionnement de l'agent LLDP, saisissez la commande suivante :

```
# lldpadm show-agentprop -p mode agent
```

- 6 Pour désactiver un agent LLDP, utilisez l'une des commandes suivantes :

- `lldpadm set-agentprop -p mode=disable agent`
- `lldpadm reset-agentprop -p mode agent`

- 7 Pour désactiver le protocole LLDP sur l'ensemble du système, saisissez la commande suivante :

```
# svcadm disable svc:/network/lldp:default
```

### Exemple 16-1 Activation du protocole LLDP sur plusieurs liaisons de données

Dans cet exemple, un système possède deux liaisons de données, `net0` et `net1`, et le protocole LLDP est activé dans différents modes pour chaque agent LLDP. Un agent transmet et reçoit les paquets LLDP, tandis que l'autre transmet uniquement les paquets LLDP.

```
# svcadm enable svc:/network/lldp:default
# lldpadm set-agentprop -p mode=both net0
# lldpadm set-agentprop -p mode=txonly net1
```

## Configuration des informations à diffuser

L'agent LLDP transmet des informations relatives au système et à la connectivité dans des paquets LLDP ou LLDPDU. Ces paquets contiennent des unités d'information individuellement formatées au format TLV (Type-Longueur-Valeur). Par conséquent, les unités d'information sont également appelées unités TLV. Certaines unités TLV sont obligatoires et sont incluses par défaut dans les paquets LLDP lorsque le protocole LLDP est activé. Les unités TLV suivantes sont obligatoires :

- ID de châssis

- ID de port
- Durée de vie
- Expiration de la PDU

L'ID de châssis correspond à l'information générée par la commande `host id`, tandis que l'ID de port est l'adresse MAC de la carte d'interface réseau physique. Plusieurs agents LLDP peuvent être activés sur un système unique, selon le nombre de liaisons. La combinaison des ID de châssis et de port identifie un agent de manière unique et le distingue des autres agents sur le système.

Vous ne pouvez pas utiliser la commande `lldpadm` pour exclure une unité TLV obligatoire des paquets LLDP.

Des unités TLV facultatives peuvent être ajoutées à un paquet LLDP. Ces unités TLV facultatives permettent aux fournisseurs d'insérer des unités TLV spécifiques au fournisseur devant être diffusées. Les unités TLV sont identifiées par des identifiants uniques d'organisme (OUI) individuels et sont saisies en fonction qu'elles répondent aux spécifications IEEE 802.1 ou IEEE 802.3. Les propriétés de l'agent LLDP correspondant à chaque type TLV sont créées de sorte que vous puissiez définir des valeurs pour chaque type.

Le tableau ci-dessous répertorie les types ou groupes TLV, les noms de propriété correspondantes, les unités TLV pour chaque propriété et leurs descriptions.

**TABEAU 16-1** Unités TLV pouvant être activée pour un agent LLDP

Type TLV	Nom de propriété	TLV	Description
Gestion de base	<code>basic-tlv</code>	<code>sysname</code> , <code>portdesc</code> , <code>syscapab</code> , <code>sysdesc</code> , <code>mgmtaddr</code>	Spécifie le nom du système, la description du port, la capacité du système, la description du système et l'adresse de gestion à diffuser
OUI 802.1	<code>dot1-tlv</code>	<code>vlannname</code> , <code>pvid</code> , <code>linkaggr</code> , <code>pfc</code> , <code>appln</code>	Spécifie le nom du réseau VLAN, l'ID VLAN, l'agrégation de liens, la description du port et l'unité TLV de l'application à diffuser
OUI 802.3	<code>dot3-tlv</code>	<code>max-framesize</code>	Spécifie la taille de trame maximale à diffuser
OUI spécifique à Oracle (défini comme <code>0x0003BA</code> )	<code>virt-tlv</code>	<code>vnic</code>	Spécifie la VNIC à diffuser si un réseau virtuel est configuré

Vous pouvez configurer n'importe laquelle de ces propriétés pour indiquer les unités TLV à inclure dans les paquets lorsque le protocole LLDP est activé.

▼ **Spécification des unités TLV pour les paquets LLDP**

Cette procédure montre comment ajouter une unité TLV à diffuser dans le paquet LLDP. Pour définir les unités TLV pour les paquets LLDP, vous utilisez la sous-commande `lldpadm set-agentprop`.

- 1 **Si nécessaire, identifiez la propriété de l'agent LLDP pouvant contenir l'unité TLV que vous voulez ajouter.**

Cette sous-commande affiche également les unités TLV déjà définies pour chaque propriété.

```
# lldpadm show-agentprop agent
```

Si vous ne spécifiez pas la propriété, cette sous-commande affiche toutes les propriétés de l'agent LLDP et leurs valeurs TLV.

- 2 **Ajoutez l'unité TLV à la propriété.**

```
# lldpadm set-agentprop -p property[+|-]=value[,...] agent
```

Les qualificatifs `+` ou `-` sont utilisés pour les propriétés qui acceptent plusieurs valeurs. Ils vous permettent d'ajouter (`+`) ou de supprimer (`-`) des valeurs de la liste. Si vous n'utilisez pas les qualificatifs, alors la valeur que vous avez définie remplace toutes les valeurs précédemment définies pour la propriété.

- 3 **(Facultatif) Affichez les nouvelles valeurs de la propriété.**

```
# lldpadm show-agentprop -p property agent
```

**Exemple 16–2** Ajout d'unités TLV facultatives au paquet LLDP

Dans cet exemple, l'agent LLDP `net0` est déjà configuré pour diffuser les informations VLAN dans le paquet. Vous souhaitez également inclure des informations relatives à la capacité du système, l'agrégation de liens et la virtualisation du réseau à diffuser. Cependant, vous souhaitez supprimer la description du VLAN du paquet.

```
# lldpadm show-agentprop net0
# lldpadm set-agentprop -p dot1-tlv+=linkaggr net0
```

AGENT	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
net0	mode	rw	both	disable	txonly, rxonly, both, disable
net0	basic-tlv	rw	sysname, sysdesc	none	none, portdesc, sysname, sysdesc, syscapab, mgmtaddr, all
net0	dot1-tlv	rw	vlanname, pvid, pfc	none	none, vlanname, pvid, linkaggr, pfc, appln, all
net0	dot3-tlv	rw	max-framesize	none	none, max-framesize,

```

net0    virt-tlv  rw      none          none      all
         none,vnic,all

# lldpadm set-agentprop -p basic-tlv+=syscapab,dot1-tlv+=linkaggr,virt-tlv=vnic net0
# lldpadm set-agentprop -p dot1-tlv-=pfc net0
# lldpadm show-agentprop -p net0
AGENT   PROPERTY  PERM   VALUE          DEFAULT    POSSIBLE
net0    mode         rw     both           disable    txonly,rxonly,both,
         disable
net0    basic-tlv   rw     sysname,       none       none,portdesc,
         sysdesc,
         syscapab
net0    dot1-tlv    rw     vllanname,     none       none,vllanname,pvid,
         pvid,
         linkaggr
net0    dot3-tlv    rw     max-framesize  none       none, max-framesize,
         all
net0    virt-tlv    rw     vnic           none       none,vnic,all

```

## Gestion des unités TLV

Chaque unité TLV possède des propriétés que vous pouvez configurer à l'aide de valeurs spécifiques. Lorsque qu'une unité TLV est activée en tant que propriété de l'agent LLDP, elle est alors diffusée sur le réseau uniquement avec les valeurs spécifiées. Prenons par exemple la valeur TLV syscapab, qui diffuse les capacités d'un système. Ces capacités peuvent éventuellement inclure la prise en charge des routeurs, des passerelles, répéteurs, téléphones et autres périphériques. Cependant, vous pouvez définir syscapab afin que seules les fonctions réellement prises en charge dans votre système, tels que les routeurs et les passerelles, soient diffusés.

La procédure de gestion des unités TLV varie selon que configurez les TLV à l'échelle globale ou par agent.

Les *TLV globales* s'appliquent à tous les agents LLDP sur le système. Le tableau suivant affiche les valeurs TLV globales et les configurations possibles correspondantes.

TABLEAU 16-2 TLV globales et leurs propriétés

Nom de la TLV	Nom de la propriété TLV	Valeurs possibles de la propriété	Description de la valeur
syscapab	supported	other, repeater, bridge, wlan-ap, router, telephone, docsis-cd, station, cvlan, sylvan, tpmr	Principales fonctions prises en charge du système. Les valeurs par défaut sont router, station et bridge.
	enabled	Sous-ensemble de valeurs répertoriées pour supported	Fonctions activées du système.

**TABEAU 16-2** TLV globales et leurs propriétés (Suite)

Nom de la TLV	Nom de la propriété TLV	Valeurs possibles de la propriété	Description de la valeur
mgmtaddr	ipaddr	ipv4 ou ipv6	Spécifie le type d'adresse IP qui sera associée à l'agent LLDP local. Les adresses seront utilisées pour atteindre les entités de couche supérieure et aider à la détection par la gestion du réseau. Un seul type peut être spécifié.

Les unités TLV qui ne peuvent pas avoir de valeurs globales sont gérées au niveau de l'agent LLDP. Avec les *unités TLV par agent*, les valeurs que vous fournissez sont utilisés lorsque l'unité TLV est activée pour transmission par un agent LLDP spécifique.

Le tableau suivant présente les valeurs TLV et les configurations possibles correspondantes pour un agent LLDP.

**TABEAU 16-3** Unités TLV par agent et leurs propriétés

Nom de la TLV	Nom de la propriété TLV	Valeurs possibles de la propriété	Description de la valeur
pfc	willing	on, off	Indique à un agent LLDP d'accepter ou de rejeter les informations de configuration issues d'un ordinateur distant.
appln	apt	Les valeurs sont extraites des informations définies dans le tableau de priorité des applications.	Configure le tableau de priorité des applications. Ce tableau contient la liste des unités TLV de l'application et leurs priorités. L'application est identifiée par la paire <code>id/selector</code> . Le contenu du tableau applique le format suivant :  <code>id/selector/priority</code>

La procédure suivante montre comment définir des valeurs TLV globales. Pour en savoir plus sur la définition des unités TLV par agent, reportez-vous à la section [“Data Center Bridging” à la page 337](#).

## ▼ Définition des valeurs TLV globales

Cette procédure montre comment fournir des valeurs globales pour des unités TLV spécifique. Pour définir des valeurs TLV globales, vous utilisez la sous-commande `lldpadm set -tlvprop`.



- 1 Configurez la propriété TLV appropriée afin qu'elle contienne les valeurs que vous souhaitez diffuser.  
Pour référence, reportez-vous au [Tableau 16–2](#).  
`# lldpadm set-tlvprop -p tlv-property=value[,value,value,...] tlv`
- 2 (Facultatif) Affichez les valeurs de la propriété que vous venez de configurer.  
`# lldpadm show-tlvprop`

**Exemple 16–3** Spécification de la capacité du système et de l'adresse IP de gestion

Cet exemple permet d'accomplir deux objectifs :

- Fournit des informations spécifiques sur les capacités du système à diffuser dans le paquet LLDP. Pour atteindre cet objectif, les propriétés `supported` et `enabled` de l'unité TLV `syscapab` doivent être configurées.
- Fournit l'adresse IP de gestion utilisée dans la diffusion.

```
# lldpadm set-tlvprop -p supported=bridge,router,repeater syscapab
# lldpadm set-tlvprop -p enabled=router syscapab
# lldpadm set-tlvprop -p ipaddr=192.168.1.2 mgmtaddr
# lldpadm show-tlvprop
```

TLVNAME	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
syscapab	supported	rw	bridge, router, repeater	bridge,router, station	other,router, repeater,bridge, wlan-ap,telephone, docis-cd,station, cvlan,svlan,tpmr
syscapab	enabled	rw	router	none	bridge,router, repeater
mgmtaddr	ipaddr	rw	192.162.1.2	none	--

## Data Center Bridging

Pour prendre en charge le trafic FCoE (Fibre Channel over Ethernet), l'implémentation du protocole LLDP dans Oracle Solaris inclut la prise en charge de la fonction Data Center Bridging (DCB).

Dans les réseaux qui utilisent un réseau Ethernet classique pour l'échange de trafic, il existe le risque que des paquets soient perdus lorsque le réseau est occupé. Une exigence essentielle pour le trafic FCoE est qu'aucun paquet ne doit être supprimé au cours de la transmission. Avec la prise en charge de la technologie Data Center Bridging Exchange (DCBx), la TLV de contrôle de flux basé sur la priorité (PFC) et la TLV d'application, la perte de paquets est évitée.

Le PFC étend la trame PAUSE standard afin d'inclure les informations relatives à la priorité des paquets. En règle générale, une trame PAUSE est envoyée sur un lien lorsque le trafic est important afin que le destinataire puisse traiter les paquets déjà reçus. Avec le PFC, au lieu de transmettre une trame PAUSE pour interrompre l'ensemble du trafic sur le lien, le trafic est mis

en pause en fonction des priorités définies pour les paquets. Une trame PFC peut être envoyée pour la priorité pour laquelle le trafic doit être interrompu. L'expéditeur arrête le trafic pour cette priorité spécifique, tandis que le trafic pour d'autres priorités n'est pas affecté. Après un délai spécifié, une autre trame PFC est envoyée pour signaler que le trafic mis en pause peut reprendre.

Les informations de configuration PFC sont échangées entre stations paires via la technologie DCBx. Si les pairs dans un échange de trafic possèdent des configurations PFC correspondantes, le PFC peut suspendre ou reprendre la transmission du trafic en fonction de vos besoins. Pour activer des priorités différentes à différents paquets, la TLV d'application est utilisée pour définir les informations de priorité. Si les pairs possèdent des configurations PFC qui ne correspondent pas, la TLV PFC peut être personnalisée pour accepter la configuration de l'autre pair, comme illustré dans la procédure suivante.

La fonction Data Center Bridging présente un cas particulier afin d'illustrer la configuration d'unités TLV par agent, comme expliqué à la section [“Gestion des unités TLV” à la page 335](#).

### ▼ Définition de valeurs TLV par agent

Cette procédure montre comment définir les valeurs TLV au niveau de l'agent LLDP à l'aide de la sous-commande `lldpdm set-agenttlvprop`.

- 1 **Configurez la propriété TLV appropriée afin qu'elle contienne les valeurs que vous souhaitez qu'un agent LLDP donné diffuse.**

Pour référence, reportez-vous au [Tableau 16–3](#).

```
# lldpdm set-agenttlvprop -p tlv-property[+|-]=value[,value,value,...] -a agent tlv-name
```

- 2 **(Facultatif) Affichez les valeurs de la propriété que vous venez de configurer.**

```
# lldpdm show-agenttlvprop
```

#### Exemple 16–4 Activation de l'agent LLDP afin qu'il accepte les informations et définitions des priorités d'application TLV

Cet exemple montre comment les valeurs TLV `pfc` et `appln` sont personnalisées. Les unités TLV dans cet exemple spécifient comment la fonction DCB fonctionne pour le trafic FCoE. Le système est configuré pour accepter la configuration PFC du pair dans l'hypothèse où la configuration locale ne correspond pas à la configuration du pair. L'exemple montre également comment la priorité est définie pour la TLV d'application de l'agent LLDP.

```
# lldpdm set-agenttlvprop -p willing=on -a net0 pfc
# lldpdm set-agenttlvprop -p apt=8906/1/4 -a net0 appln
# lldpdm show-agenttlvprop
AGENT  TLVNAME  PROPERTY  PERM  VALUE      DEFAULT  POSSIBLE
net0    pfc        willing   rw    on         off      on,off
net0    appln      apt       rw    8906/1/4   --      --
```

# Contrôle des agents LLDP

La sous-commande `lldpadm show-agent` affiche les informations complètes diffusées par un agent LLDP. Se rapportant à un système particulier, la diffusion peut consister d'informations sur le système local transmises au reste du réseau. La diffusion peut également se composer d'informations reçues par le système à partir d'autres systèmes sur le même réseau.

## ▼ Affichage des diffusions

Cette procédure montre comment afficher les informations diffusées par un agent LLDP. Les informations peuvent être locales ou distantes. Les informations *locales* proviennent du système local. Les informations *distantes* proviennent d'autres systèmes sur le réseau reçues par le système local.

- Utilisez la sous-commande `lldpadm show-agent` avec l'option appropriée pour afficher les informations de votre choix.
  - Pour afficher les informations locales diffusées par l'agent LLDP, saisissez la commande suivante :
 

```
# lldpadm show-agent -l agent
```
  - Pour afficher les informations distantes reçues par l'agent LLDP, saisissez la commande suivante :
 

```
# lldpadm show-agent -r agent
```
  - Pour afficher les informations locales ou distantes en détail, saisissez la commande suivante :
 

```
# lldpadm show-agent -[l|r]v agent
```

### Exemple 16-5 Obtention des informations diffusées par un agent LLDP

L'exemple ci-dessous montre comment afficher les informations qui sont diffusées localement ou à distance par un agent LLDP. Par défaut, les informations s'affichent sous forme abrégée. En utilisant l'option `-v`, vous pouvez vous obtenir des informations détaillées.

```
# lldpadm show-agent -l net0
AGENT  CHASSISID  PORTID
net0   004bb87f    00:14:4f:01:77:5d

# lldpadm show-agent -lv net0
          Agent: net0
Chassis ID Subtype: Local(7)
Port ID Subtype: MacAddress(3)
Port ID: 00:14:4f:01:77:5d
Port Description: net0
```

```

        Time to Live: 81 (seconds)
        System Name: hosta.example.com
    System Description: SunOS 5.11 dcb-clone-x-01-19-11 i86pc
Supported Capabilities: bridge,router
Enabled Capabilities: router
Management Address: 192.168.1.2
Maximum Frame Size: 3000
Port VLAN ID: --
VLAN Name/ID: vlan25/25
    VNIC PortID/VLAN ID: 02:08:20:72:71:31
Aggregation Information: Capable, Not Aggregated
    PFC Willing: --
        PFC Cap: --
        PFC MBC: --
        PFC Enable: --
Application(s) (ID/Sel/Pri): --
    Information Valid Until: 117 (seconds)

# lldpadm show-agent -r net0
AGENT  SYSNAME  CHASSISID  PORTID
net0    hostb    0083b390   00:14:4f:01:59:ab

# lldpadm show-agent -rv net0
        Agent: net0
        Chassis ID Subtype: Local(7)
        Port ID Subtype: MacAddress(3)
        Port ID: 00:14:4f:01:59:ab
        Port Description: net0
        Time to Live: 121 (seconds)
        System Name: hostb.example.com
        System Description: SunOS 5.11 dcb-clone-x-01-19-11 i86pc
Supported Capabilities: bridge,router
Enabled Capabilities: router
Management Address: 192.168.1.3
Maximum Frame Size: 3000
Port VLAN ID: --
VLAN Name/ID: vlan25/25
    VNIC PortID/VLAN ID: 02:08:20:72:71:31
Aggregation Information: Capable, Not Aggregated
    PFC Willing: --
        PFC Cap: --
        PFC MBC: --
        PFC Enable: --
Application(s) (ID/Sel/Pri): --
    Information Valid Until: 117 (seconds)

```

## ▼ Affichage des statistiques LLDP

Vous pouvez afficher des statistiques LLDP pour obtenir plus d'informations sur les paquets LLDP diffusés par le système local ou par des systèmes distants. Les statistiques font référence aux événements importants qui impliquent la transmission et la réception de paquets LLDP.

- 1 **Pour afficher toutes les statistiques relatives à la transmission et à la réception de paquets LLDP, utilisez la commande suivante :**

```
# lldpadm show-agent -s agent
```

## 2 Pour afficher les informations statistiques sélectionnées, utilisez l'option -o.

```
# lldpadm show-agent -s -o field[,field,...]agent
```

où *field* fait référence à un nom de champ dans la sortie de la commande `show-agent -s`.

### Exemple 16-6 Affichage de statistiques sur les paquets LLDP

Cet exemple montre comment afficher des informations sur la diffusion de paquets LLDP.

```
# lldpadm show-agent -s net0
AGENT IFRAMES IEER IDISCARD OFRAMES OLENERR TLVDISCARD TLVUNRECOG AGEOUT
net0      9      0          0      14          0          4          5          0
```

La sortie de la commande fournit les informations suivantes :

- AGENT spécifie le nom de l'agent LLDP, qui est identique à la liaison de données sur laquelle l'agent LLDP est activé.
- IFRAMES, IEER et IDISCARD affichent des informations concernant les paquets reçus, les paquets entrants avec des erreurs et les paquets entrants supprimés.
- OFRAMES et OLENERR se rapportent aux paquets sortants, ainsi qu'aux paquets qui présentent une erreur de longueur.
- TLVDISCARD et TLVUNRECOG affichent des informations sur les unités TLV supprimées, ainsi que sur celles qui ne sont pas reconnues.
- AGEOUT fait référence aux paquets dont le délai est dépassé.

L'exemple indique que sur 9 trames reçues dans le système, 5 TLV ne sont pas reconnues, peut-être parce qu'elles ne respectent pas les normes. L'exemple montre également que 14 trames ont été transmises au réseau par le système local.



## PARTIE III

# Virtualisation du réseau et gestion des ressources





# Introduction à la virtualisation du réseau et au contrôle des ressources (présentation)

---

Ce chapitre présente les concepts de base de la virtualisation du réseau et du contrôle des ressources. Il comprend les rubriques suivantes :

- Virtualisation du réseau
- Types de réseaux virtuels
- Machines virtuelles et zones
- Contrôle des ressources, notamment la gestion de flux
- Observabilité du réseau améliorée

Ces fonctions permettent de gérer le contrôle de flux, d'améliorer les performances du système et de configurer l'utilisation du réseau nécessaire pour garantir la virtualisation du système d'exploitation, l'utilisation des utilitaires et la consolidation des serveurs.

Pour des tâches spécifiques, reportez-vous aux chapitres suivants :

- [Chapitre 19, “Configuration des réseaux virtuels \(tâches\)”](#)
- [Chapitre 22, “Contrôle du trafic réseau et de l'utilisation des ressources”](#)
- [Chapitre 20, “Utilisation de la protection des liens dans les environnements virtualisés”](#)
- [Chapitre 21, “Gestion des ressources réseau”](#)

## Virtualisation du réseau et réseaux virtuels

La *virtualisation du réseau* consiste à combiner des ressources réseau matérielles et logicielles dans une seule unité administrative. L'objectif de la virtualisation du réseau est de fournir aux systèmes et utilisateurs un partage efficace, contrôlé et sécurisé des ressources réseau.

Le résultat de la virtualisation du réseau est un *réseau virtuel*. Les réseaux virtuels sont classés en deux grandes catégories : externes et internes. Les *réseaux virtuels externes* sont composés de plusieurs réseaux locaux administrés par le logiciel comme une entité unique. Les blocs de construction des réseaux virtuels externes standard sont le matériel de commutation et la technologie logicielle VLAN. Les réseaux virtuels externes comprennent par exemple les grands réseaux d'entreprise et les centres de données.

Un *réseau virtuel interne* se compose d'un système utilisant des machines virtuelles ou des zones configurées sur au moins une interface pseudo-réseau. Ces conteneurs peuvent communiquer les uns avec les autres comme sur le même réseau local, fournissant un réseau virtuel sur un seul hôte. Les blocs de construction du réseau virtuel sont les *cartes d'interface réseau virtuelles ou NIC virtuelles (VNIC)* et les commutateurs virtuels. La virtualisation de réseau Oracle Solaris propose la solution de réseau virtuel interne.

Vous pouvez combiner les ressources réseau pour configurer à la fois les réseaux interne et externe. Par exemple, vous pouvez configurer des systèmes individuels avec des réseaux virtuels internes sur des réseaux locaux appartenant à un grand réseau virtuel externe. Les configurations réseau décrites dans cette partie incluent des exemples de réseaux virtuels interne et externe combinés.

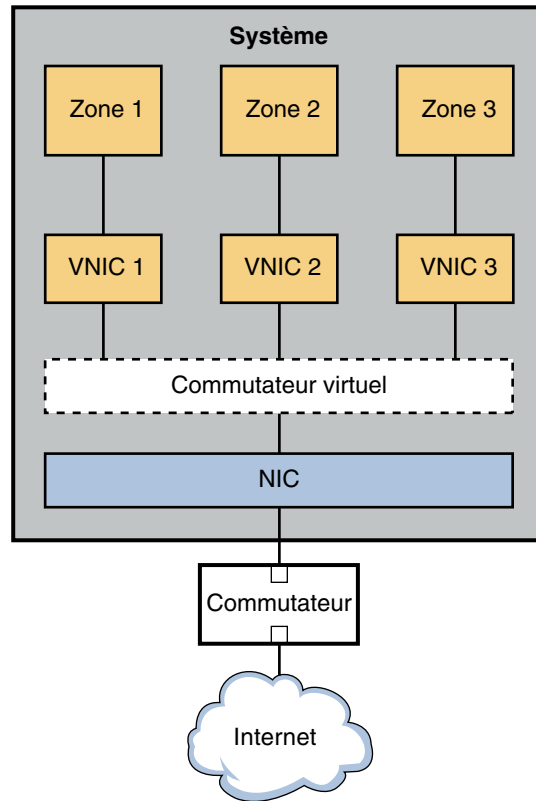
## Parties du réseau virtuel interne

Un réseau virtuel interne basé sur Oracle Solaris contient les éléments suivants :

- Au moins une carte d'interface réseau, ou NIC.
- Une carte d'interface réseau virtuelle, ou VNIC, configurée sur l'interface réseau.
- Un commutateur virtuel, configuré en même temps que la première carte d'interface réseau virtuelle sur l'interface.
- Un conteneur, tel qu'une zone ou une machine virtuelle, configuré sur la carte d'interface réseau virtuelle.

La figure suivante montre ces éléments et la manière dont ils se combinent dans un système unique.

FIGURE 17-1 Configuration VNIC pour une interface unique



La figure présente un système unique avec une carte d'interface réseau. La carte d'interface réseau (NIC) est configurée avec trois VNIC. Chaque carte d'interface réseau virtuelle prend en charge une seule zone. Par conséquent, la zone 1, la zone 2 et la zone 3 sont configurées sur la VNIC 1, la VNIC 2 et la VNIC 3, respectivement. Les trois VNIC sont virtuellement connectées à un commutateur virtuel. Celui-ci fournit la connexion entre les VNIC et la carte d'interface réseau physique sur lequel les VNIC sont basées. L'interface physique fournit le système avec sa connexion réseau externe.

Vous pouvez également créer un réseau virtuel basé sur l'etherstub. Les etherstub sont de simples logiciels qui ne nécessitent pas d'interface réseau comme base du réseau virtuel.

Une VNIC est un périphérique réseau virtuel avec la même interface de liaison de données comme interface physique. Vous configurez les VNIC sur une interface physique. Pour obtenir la liste actuelle des interfaces physiques prenant en charge les VNIC, reportez-vous à la [foire aux questions sur la virtualisation du réseau et le contrôle des ressources](http://hub.opensolaris.org/bin/view/Project+crossbow/faq) (<http://hub.opensolaris.org/bin/view/Project+crossbow/faq>). Vous pouvez configurer jusqu'à 900 VNIC sur une interface physique unique. Lorsque les VNIC sont configurées, elles se

comportent comme des cartes d'interface réseau physiques. En outre, les ressources du système traitent les VNIC comme s'il s'agissait de cartes d'interface réseau physiques.

Chaque carte d'interface réseau virtuelle est implicitement connectée à un *commutateur virtuel* qui correspond à l'interface physique. Le commutateur virtuel fournit la même connectivité entre les VNIC sur un réseau virtuel que le matériel de commutation pour les systèmes connectés aux ports d'un commutateur.

Conformément à la conception Ethernet, si un port de commutateur reçoit un paquet sortant depuis l'hôte connecté à ce port, ce paquet ne peut pas accéder à une destination sur le même port. Cette conception est un inconvénient pour les systèmes configurés avec des zones ou des machines virtuelles. Sans virtualisation du réseau, les paquets sortants émis depuis une machine virtuelle ou une zone avec une pile exclusive ne peuvent pas être transmis à une autre machine virtuelle ou zone sur le même système. Les paquets sortants passent par un port de commutateur sur le réseau externe. Les paquets entrants ne peuvent pas atteindre leur zone ou machine virtuelle de destination car les paquets ne peuvent pas revenir via le port par lequel ils ont été envoyés. Par conséquent, lorsque des machines virtuelles et des zones sur le même système ont besoin de communiquer, un chemin d'accès aux données entre les conteneurs doit être ouvert sur l'ordinateur local. Les commutateurs virtuels fournissent ces conteneurs avec la méthode de transmission de paquets.

## Transit des données dans un réseau virtuel

La [Figure 17–1](#) illustre une configuration VNIC simple pour un réseau virtuel sur un système unique.

Lorsque le réseau virtuel est configuré, une zone envoie le trafic vers un hôte externe de la même manière qu'un système sans réseau virtuel. Le trafic circule, par l'intermédiaire de la carte d'interface réseau virtuelle, de la zone vers le commutateur virtuel, puis vers l'interface physique, qui envoie les données sur le réseau.

Mais que se passe-t-il si une zone sur un réseau virtuel veut envoyer les paquets à une autre zone sur le réseau virtuel, compte tenu des restrictions Ethernet précédemment mentionnées ? Comme illustré dans la [Figure 17–1](#), supposons que la Zone 1 doit envoyer le trafic vers la Zone 3. Dans ce cas, les paquets sont envoyés à partir de la Zone 1 par l'intermédiaire de sa VNIC 1 dédiée. Le trafic passe ensuite à travers le commutateur virtuel vers VNIC 3. VNIC 3 transmet alors le trafic à la Zone 3. Le trafic ne quitte jamais le système, et ne viole donc pas les restrictions Ethernet.

## Responsables de l'implémentation des réseaux virtuels

Si vous avez besoin de consolider des ressources sur des serveurs Sun d'Oracle, envisagez l'implémentation de VNIC et de réseaux virtuels. Les groupeurs des fournisseurs d'accès

Internet, les entreprises de télécommunication et les grandes institutions financières peuvent utiliser les fonctions de virtualisation de réseau suivantes pour améliorer les performances de leurs serveurs et réseaux.

- Matériel NIC, y compris les nouvelles interfaces matérielles puissantes qui prennent en charge les anneaux matériels
- Plusieurs adresses MAC pour les VNIC
- Grande quantité de bande passante fournie par les interfaces les plus récentes

Vous pouvez remplacer de nombreux systèmes par un système unique mettant en oeuvre l'exécution de plusieurs zones ou machines virtuelles, sans perte significative de la séparation, la sécurité ou la flexibilité.

## Définition du contrôle des ressources

Le *contrôle des ressources* est le processus consistant à affecter les ressources du système de manière contrôlée. La fonction de contrôle des ressources d'Oracle Solaris active la bande passante afin qu'elle soit partagée entre les VNIC sur le réseau virtuel d'un système. Vous pouvez également utiliser les fonctions de contrôle des ressources pour allouer et gérer la bande passante sur une interface physique sans VNIC ni machine virtuelle. Cette section présente les principales fonctionnalités de contrôle des ressources et explique brièvement comment elles fonctionnent.

## Fonctionnement de la gestion de la bande passante et du contrôle de flux

Le site [Searchnetworking.com](http://searchnetworking.techtarget.com) (<http://searchnetworking.techtarget.com>) définit la bande passante comme "la quantité de données pouvant être transmise d'un point à un autre dans une période donnée (en général, une seconde)". La *gestion de la bande passante* vous permet d'affecter une partie de la bande passante disponible d'une carte d'interface réseau physique à un consommateur, par exemple en tant qu'application ou client. Vous pouvez contrôler la bande passante sur la base d'une application, d'un port, d'un protocole et d'une adresse. La gestion de la bande passante garantit une utilisation efficace de la grande quantité de bande passante disponible à partir des nouvelles interfaces réseau GLDv3.

Les fonctions de contrôle des ressources permettent d'implémenter une série de contrôles sur la bande passante disponible d'une interface. Par exemple, vous pouvez définir une *garantie* de bande passante d'une interface pour un consommateur particulier. Cette garantie est la quantité minimale de bande passante garantie allouée à l'application ou l'entreprise. La partie allouée de la bande passante est désignée comme un *partage*. En définissant des garanties, vous pouvez allouer suffisamment de bande passante aux applications qui peuvent fonctionner correctement sans une certaine quantité de bande passante. Par exemple, la diffusion de contenu multimédia

en temps réel et la voix sur IP consomment une grande quantité de bande passante. Vous pouvez utiliser les fonctions de contrôle de ressources pour garantir que ces deux applications disposent de suffisamment de bande passante pour s'exécuter correctement.

Vous pouvez également définir une *limite* sur le partage. La limite est l'allocation maximale de bande passante que le partage peut consommer. Grâce aux limites, vous pouvez empêcher les services non critiques de voler de la bande passante aux services critiques.

Enfin, vous pouvez définir l'ordre de priorité entre les divers partages alloués aux consommateurs. Vous pouvez accorder la priorité absolue au trafic critique, par exemple aux paquets de pulsation d'un cluster, et une priorité inférieure aux applications de moindre importance.

Par exemple, les fournisseurs d'applications hébergées (ASP) peuvent offrir à leurs clients des niveaux de service basés sur des frais dépendant du partage de bande passante acheté par le client. Dans le cadre de l'accord de niveau de service (SLA), une quantité de bande passante est alors garantie à chaque partage, afin de ne pas dépasser la limite achetée. (Pour plus d'informations sur les accords de niveau de service, reportez-vous à la section [“Implémentation des accords de niveau de service”](#) du manuel *Administration d'Oracle Solaris : Services IP*. Les contrôles de priorité peuvent être basés sur différents niveaux de l'accord de niveau de service, ou sur différents prix payés par le client du SLA.

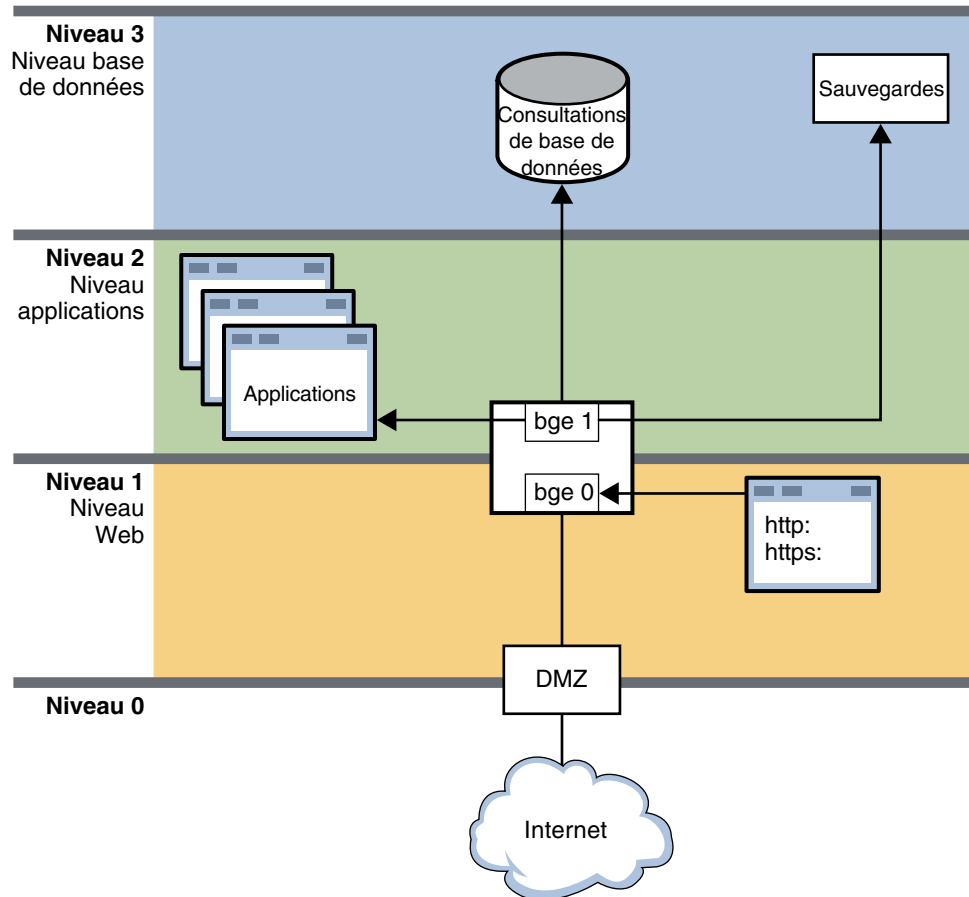
L'utilisation de la bande passante est contrôlée par la gestion des flux. Un *flux* est un flux de paquets qui possèdent tous certaines caractéristiques, telles que le numéro de port ou l'adresse de destination. Ces flux sont gérés par transport, service ou machine virtuelle, y compris les zones. Les flux ne peuvent pas dépasser la quantité de bande passante garantie pour l'application ou le partage acheté par le client.

Lorsqu'une garantie est affectée à une carte d'interface réseau virtuelle ou un flux, la carte d'interface réseau virtuelle est assurée de recevoir sa bande passante définie même si d'autres flux ou VNIC utilisent également l'interface. Cependant, les garanties affectées peuvent uniquement être utilisées si elles ne dépassent pas la bande passante maximale de l'interface physique.

## Allocation du contrôle des ressources et de la gestion de la bande passante sur un réseau

La figure suivante montre une topologie de réseau d'entreprise utilisant le contrôle des ressources pour gérer diverses applications.

FIGURE 17-2 Réseau avec des contrôles de ressources en place



Cette figure présente une topologie de réseau standard qui utilise des contrôles de ressources afin d'améliorer l'efficacité et les performances du réseau. Le réseau n'implémente pas de VNIC ni de conteneurs, tels que des zones exclusives et des machines virtuelles. Cependant, les VNIC et les conteneurs pourraient être utilisés sur ce réseau à des fins de consolidation, entre autres.

Le réseau est divisé en quatre niveaux :

- Le **niveau 0** est la zone démilitarisée (DMZ). Il s'agit d'un petit réseau local qui contrôle l'accès à partir de et vers le monde extérieur. Le contrôle des ressources n'est pas utilisé sur les systèmes de la DMZ.
- Le **niveau 1** est le niveau Web et comprend deux systèmes. Le premier système est un serveur proxy qui effectue le filtrage. Ce serveur dispose de deux interfaces, bge0 et bge1. Le lien bge0 connecte le serveur proxy à la zone démilitarisée (DMZ) sur le niveau 0. Le lien bge1 connecte également au serveur proxy au second système, le serveur Web. Les services

http et https partagent la bande passante du serveur Web avec d'autres applications standard. En raison de la taille et de la nature critique des serveurs Web, les partages de http et https nécessitent des garanties et la définition de priorités.

- Le **niveau 2** est le niveau des applications et comprend également deux systèmes. La deuxième interface du serveur proxy, bge1, établit la connexion entre le niveau Web et le niveau des applications. Grâce à un commutateur, un serveur d'applications se connecte à bge1 sur le serveur proxy. Le serveur d'applications nécessite le contrôle des ressources afin de gérer les partages de la bande passante attribués aux différentes applications exécutées. Les applications critiques qui ont besoin d'une grande quantité de bande passante doivent disposer de garanties et de priorités supérieures aux applications plus petites ou de moindre importance.
- Le **niveau 3** est le niveau de base de données. Les deux systèmes sur ce niveau se connectent par le biais d'un commutateur à l'interface bge1 du serveur proxy. Le premier système, un serveur de base de données, doit pouvoir fournir des garanties et définir l'ordre de priorité des différents processus impliqués dans les recherches dans la base de données. Le deuxième système est un serveur de sauvegarde pour le réseau. Ce système doit utiliser une grande quantité de bande passante pendant les sauvegardes. Cependant, les activités de sauvegarde sont généralement effectuées pendant la nuit. En utilisant le contrôle des ressources, vous pouvez contrôler le moment où les processus de sauvegarde disposent des garanties de bande passante et des priorités les plus élevées.

## Responsable de l'implémentation des fonctions de contrôle des ressources

Tout administrateur système souhaitant améliorer l'efficacité et les performances d'un système doit envisager d'implémenter les fonctions de contrôle des ressources. Les groupeurs peuvent déléguer les partages de bande passante en combinaison avec les VNIC afin d'équilibrer la charge des serveurs les plus importants. Les administrateurs de serveurs peuvent utiliser les fonctionnalités d'allocation de partage afin d'implémenter des accords de niveau de service, tels que ceux proposés par les fournisseurs d'applications hébergées. Les administrateurs système traditionnels peuvent utiliser les fonctions de gestion de la bande passante pour isoler et donner la priorité à certaines applications. Enfin, grâce à l'allocation de partage, rien de plus facile que d'observer l'utilisation de la bande passante par les consommateurs individuels.

## Fonctions d'observabilité pour la virtualisation du réseau et le contrôle des ressources

La virtualisation du réseau et le contrôle des ressources incluent des fonctions d'observabilité afin de vous aider à visualiser l'utilisation des ressources avant de configurer des contrôles, pour les VNIC et les flux par exemple. Associées avec la comptabilisation étendue d'Oracle Solaris, les



fonctionnalités d'observabilité du contrôle des ressources vous permettent de consigner les statistiques systèmes dans des journaux. Les fonctionnalités d'observabilité de la virtualisation du réseau et du contrôle des ressources sont les suivantes :

- Possibilité de contrôler un système en cours d'exécution.
- Possibilité de consigner et établir des rapports sur les statistiques.
- Fonctionnalités de comptabilisation étendue pour la consignation des données d'historique.

La nouvelle commande `flowadm` et les extensions des commandes `dladm` et `netstat` implémentent les fonctions d'observabilité de la virtualisation du réseau. Vous pouvez utiliser ces commandes pour surveiller l'utilisation courante du système et rassembler des données statistiques dans des journaux.

En analysant les journaux d'historique, vous pouvez déterminer les éléments suivants :

- Où les ressources réseau peuvent être consolidées de plusieurs systèmes en un système unique, éventuellement avec une bande passante supérieure via la nouvelle génération d'interfaces réseau. Effectuez cette opération avant de configurer les VNIC et machines virtuelles ou zones exclusives.
- Les applications qui consomment le plus de bande passante. Ces informations peuvent vous aider à configurer la gestion de la bande passante, de sorte que le maximum de bande passante soit garanti aux applications essentielles pendant un créneau horaire particulier. Par exemple, vous pouvez garantir à un flux vidéo la plus grande quantité de bande passante d'une interface 20 heures par jour. Pendant quatre heures définies chaque jour, vous pouvez accorder la priorité absolue au programme de sauvegarde du système. Effectuez ces opérations dans le cadre de l'implémentation de la gestion de la bande passante.
- Combien facturer aux clients pour la bande passante utilisée. Les fournisseurs d'applications hébergées et autres entreprises qui louent de l'espace système peuvent utiliser les fonctionnalités d'observabilité du contrôle des ressources pour déterminer l'utilisation par les clients payants. Certaines entreprises proposent à leurs clients des accords de niveau de service, dans lesquels le client achète un pourcentage garanti de bande passante au fournisseur. Les fonctions d'observabilité vous permettent de savoir quelle quantité de bande passante chaque client utilise et de facturer les excédents potentiels. D'autres entreprises proposent à leurs clients la bande passante sur la base de l'utilisation. Dans ce cas, les fonctions d'observabilité aident directement à la facturation. Effectuez cette opération après avoir implémenté le contrôle des ressources et, éventuellement, les VNIC et machines virtuelles sur un système.

Le chapitre suivant, [Chapitre 18, “Planification de la virtualisation du réseau et du contrôle des ressources”](#), contient des scénarios qui indiquent où les fonctions d'observabilité sont utilisées pour la consolidation de la planification et le contrôle des ressources.



## Planification de la virtualisation du réseau et du contrôle des ressources

---

Ce chapitre contient des informations et scénarios d'exemple pour vous aider à évaluer et concevoir les solutions de virtualisation du réseau et de contrôle des ressources pour votre site. Ce chapitre aborde les scénarios suivants :

- “Réseau virtuel basique sur un système unique” à la page 356
- “Réseau privé virtuel sur un système unique” à la page 358
- “Contrôle des ressources basé sur l'interface pour un réseau classique” à la page 362

Chaque scénario contient des suggestions de "meilleur usage" qui présentent les types de réseaux les plus adaptés à un cas particulier.

### Liste des tâches de virtualisation du réseau et de contrôle des ressources

Le tableau suivant décrit les tâches de configuration d'un réseau virtuel et d'implémentation des contrôles de ressources sur le réseau.

Tâche	Description	Voir
Conception et planification d'un réseau virtuel sur un hôte unique	<p>Consolidez les services réseau et les applications proposés par le réseau local sur un hôte unique.</p> <p>Ce scénario est particulièrement utile pour les groupeurs et les fournisseurs de services.</p>	“Planification et conception d'un réseau virtuel” à la page 356

Tâche	Description	Voir
Planification et conception d'un réseau virtuel privé sur un hôte unique	Exécutez un réseau virtuel qui n'autorise pas l'accès public.  Ce scénario est recommandé pour les administrateurs système qui doivent exécuter un environnement de développement.	<a href="#">“Réseau privé virtuel sur un système unique” à la page 358</a>
Gestion de la bande passante et contrôle des ressources pour les systèmes sur la base d'une interface	Isolez, définissez des priorités et affectez une quantité spécifique de bande passante d'interface pour le trafic de paquets.  Ce scénario est utile dans le cas de systèmes qui gèrent un trafic important pour certains services, tels qu'un service Web ou un serveur de base de données.	<a href="#">“Contrôle des ressources basé sur l'interface pour un réseau classique” à la page 362</a>

## Planification et conception d'un réseau virtuel

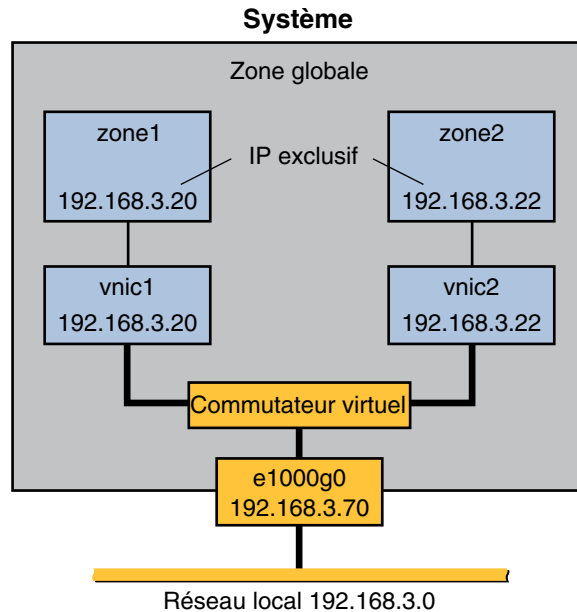
Cette section décrit deux scénarios différents pour la configuration d'un réseau virtuel. Consultez les scénarios afin de vous aider à déterminer le plus approprié à vos besoins. Utilisez ensuite ce scénario pour concevoir votre propre solution de virtualisation. Les deux scénarios sont les suivants :

- Réseau virtuel basique de deux zones, particulièrement utile pour consolider les services réseau à partir du réseau local sur un hôte unique.
- Réseau virtuel privé, utile pour un environnement de développement dans lequel vous isolez des applications et services du réseau public.

### Réseau virtuel basique sur un système unique

La [Figure 18–1](#) présente le réseau virtuel basique, ou "Network-In-a-Box (NIB)", utilisé dans les exemples de la section [“Configuration de composants de virtualisation réseau dans Oracle Solaris” à la page 368](#).

FIGURE 18-1 Réseau virtuel sur un hôte unique



Ce réseau virtuel se compose des éléments suivants :

- Une seule interface réseau GLDv3 `e1000g0`. Cette interface se connecte au réseau public `192.168.3.0/24`. L'interface `e1000g0` possède l'adresse IP `192.168.3.70`.
- Un commutateur virtuel, qui est automatiquement configuré lors de la création de la première carte d'interface réseau virtuelle.
- Deux cartes d'interface réseau virtuelles (VNIC). `vnic1` possède l'adresse IP `192.168.3.20` et `vnic2` l'adresse IP `192.168.3.22`.
- Deux zones IP exclusives auxquelles les VNIC sont affectées. `vnic1` est affectée à `zone1` et `vnic2` à `zone2`.

Les VNIC et les zones dans cette configuration permettent d'accéder au réseau public. Par conséquent, les zones peuvent transmettre le trafic au-delà de l'interface `e1000g0`. De même, les utilisateurs sur des réseaux externes peuvent atteindre les applications et les services offerts par les zones.

## Meilleurs exemples d'utilisation du réseau virtuel de base

Le scénario du réseau prêt à l'emploi vous permet d'isoler les applications et processus dans des machines virtuelles individuelles ou des zones sur un hôte unique. En outre, ce scénario peut être développé afin d'inclure de nombreux conteneurs, chacun d'entre eux pouvant exécuter un

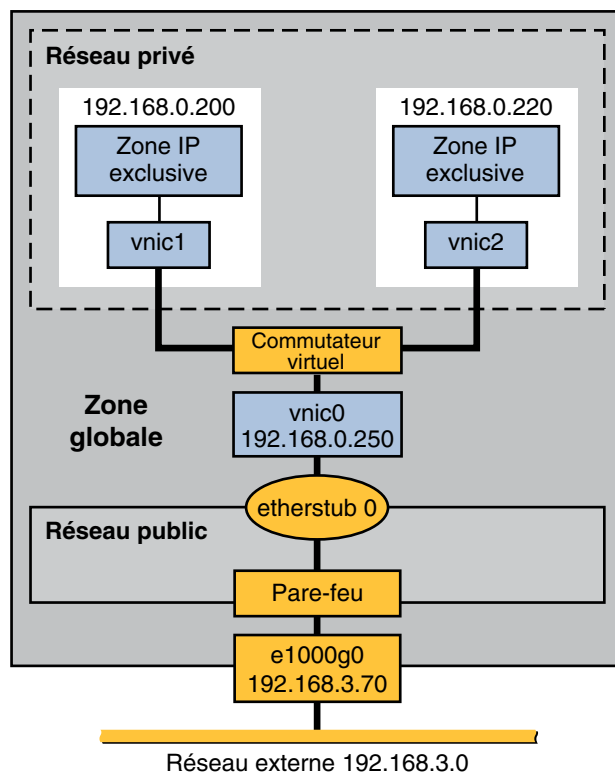
ensemble entièrement isolé d'applications. Le scénario améliore l'efficacité d'un système et, par extension, l'efficacité du réseau local. Par conséquent, ce scénario est idéal pour les utilisateurs suivants :

- Groupeurs réseau et autres personnes souhaitant consolider les services d'un réseau local dans un système unique.
- Tout site louant des services aux clients. Vous pouvez louer des zones individuelles ou des machines virtuelles, observer le trafic et recueillir des statistiques à des fins de mesure des performances ou de facturation sur chaque zone dans le réseau virtuel.
- Tout administrateur qui souhaite isoler les applications et processus pour séparer les conteneurs et améliorer l'efficacité du système.

## Réseau privé virtuel sur un système unique

La [Figure 18–2](#) présente un système unique avec un réseau privé derrière le logiciel de filtrage de paquets qui effectue une traduction des adresses réseau (NAT). Cette figure illustre le scénario développé dans l'[Exemple 19–5](#).

FIGURE 18-2 Réseau privé virtuel sur un hôte unique



La topologie comprend un système unique avec un réseau public, y compris un pare-feu, et un réseau privé construit sur une pseudo-interface etherstub. Le réseau public est exécuté dans la zone globale et se compose des éléments suivants :

- Interface réseau GLDv3 e1000g0 avec l'adresse IP 192 . 168 . 3 . 70.
- Pare-feu implémenté dans le logiciel IP Filter. Pour une introduction à IP Filter, reportez-vous à la section [“Introduction à IP Filter”](#) du manuel *Administration d'Oracle Solaris : Services IP*.
- etherstub0, pseudo-interface sur laquelle la topologie de réseau virtuel est construite. Les etherstubs offrent la possibilité de créer un réseau virtuel sur un hôte. Ce réseau est totalement isolé du réseau externe.

Le réseau privé est constitué des éléments suivants :

- Un commutateur virtuel qui permet le transfert de paquets entre les VNIC du réseau privé.
- vnic0, qui est la carte d'interface réseau virtuelle pour la zone globale, et possède l'adresse IP 192 . 168 . 0 . 250.

- vnic1 avec l'adresse IP 192.168.0.200 et vnic2 avec l'adresse IP 192.168.0.220. Les trois VNIC sont configurées sur etherstub0.
- vnic1 est affectée à zone1 et vnic2 à zone2.

## Meilleurs exemples d'utilisation d'un réseau privé virtuel

Envisagez la création d'un réseau virtuel privé pour un hôte utilisé dans un environnement de développement. En utilisant la structure etherstub, vous pouvez complètement isoler le logiciel ou les fonctions en cours de développement des conteneurs du réseau privé. En outre, vous pouvez utiliser le logiciel de pare-feu pour la traduction d'adresses réseau des paquets sortants qui proviennent des conteneurs du réseau privé. Le réseau privé est une version réduite de l'environnement de déploiement final.

## Pour plus d'informations

- Pour plus d'informations sur les procédures de configuration d'un réseau virtuel et l'implémentation des scénarios décrits dans ce chapitre, reportez-vous à la section [“Création d'un réseau virtuel privé”](#) à la page 383.
- Pour plus d'informations d'ordre conceptuel sur les cartes d'interfaces réseau virtuelles et les réseaux virtuels, reportez-vous à la section [“Virtualisation du réseau et réseaux virtuels”](#) à la page 345.
- Pour plus d'informations d'ordre conceptuel sur les zones, reportez-vous au [Chapitre 15, “Introduction à Oracle Solaris Zones”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.
- Pour plus d'informations sur IP Filter, reportez-vous à la section [“Introduction à IP Filter”](#) du manuel *Administration d'Oracle Solaris : Services IP*.

# Implémentation des contrôles sur les ressources réseau

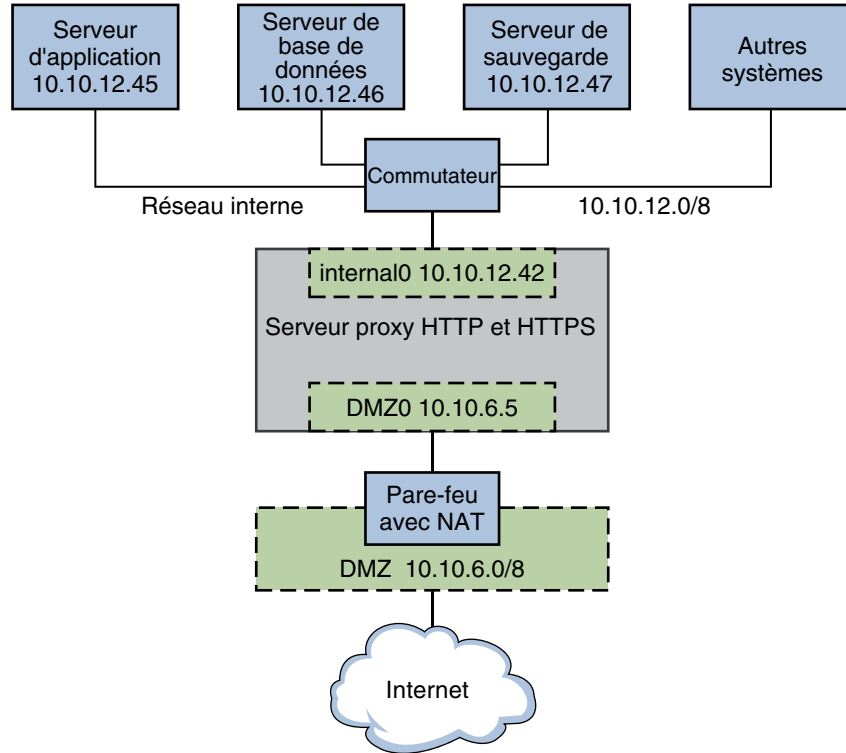
La virtualisation du réseau permet d'implémenter votre configuration réseau plus efficacement et à moindre coût en créant un réseau NIB (Network-In-a-Box). Pour augmenter l'efficacité, vous pouvez également implémenter des contrôles pour déterminer la façon dont les ressources sont utilisées par les processus réseau. Les propriétés de lien spécifiquement liées aux ressources réseau, telles que les anneaux, CPU, etc., peuvent être personnalisées afin de traiter les paquets réseau. En outre, vous pouvez également créer des flux pour gérer l'utilisation du réseau. Le contrôle des ressources réseau est évoqué en détails dans le [Chapitre 21, “Gestion des ressources réseau”](#).

La [Figure 18–3](#) montre la topologie du réseau pour une petite entreprise qui a besoin de gérer la bande passante sur son serveur proxy. Le serveur proxy propose un site Web public ainsi qu'un proxy pour les clients internes qui nécessitent des services provenant de différents serveurs sur le réseau interne du site.



**Remarque** – Ce scénario n'indique pas comment configurer le contrôle des flux d'un réseau virtuel, et, par conséquent, n'inclut pas de VNIC. Afin de contrôler le flux de données sur un réseau virtuel, reportez-vous à la section Contrôle de flux d'un réseau virtuel.

FIGURE 18-3 Contrôle des ressources pour un serveur proxy sur un réseau classique



La figure montre que la société dispose d'un réseau public, `10.10.6.0/8`, qui sert également une zone démilitarisée (DMZ). Un système de la zone démilitarisée (DMZ) fournit la traduction nom/adresse (NAT) par le biais d'un pare-feu IP Filter. La société possède un grand système qui fonctionne comme le serveur proxy. Le système dispose de deux interfaces câblées et de 16 jeux de processeurs avec les ID 0 à 16. Ce système est connecté au réseau public via l'interface `nge0`, avec l'adresse IP `10.10.6.5`. Le nom du lien pour l'interface est `DMZ0`. Via `DMZ0`, le serveur proxy fournit les services HTTP et HTTPS par le biais du site Web public de la société.

La figure illustre également le réseau interne de la société, `10.10.12.0/24`. Le serveur proxy se connecte au réseau `10.10.12.0/8` interne via l'interface `nge1`, avec l'adresse IP `10.10.12.42`. Le nom du lien pour cette interface est `internal0`. Par l'intermédiaire de la liaison de données

internal0, le serveur proxy fonctionne pour le compte des clients internes qui requièrent les services d'un serveur d'applications, 10.10.12.45, d'un serveur de base de données, 10.10.12.46 et d'un serveur de sauvegarde, 10.10.12.47.

## Contrôle des ressources basé sur l'interface pour un réseau classique

### Meilleure utilisation du contrôle des ressources basé sur l'interface sur un réseau classique

Envisagez d'établir un contrôle de flux pour les systèmes très utilisés, en particulier ceux avec les interfaces GLDv3 les plus récentes et une quantité importante de bande passante disponible. Le contrôle de flux basé sur l'interface permet d'améliorer l'efficacité de l'interface, le système, et, éventuellement, le réseau. Vous pouvez appliquer le contrôle de flux à n'importe quel système sur n'importe quel type de réseau. En outre, si votre objectif est d'améliorer l'efficacité du réseau, vous pouvez séparer divers services dans des flux individuels. Cette action permet d'affecter des ressources matérielles et logicielles séparées aux flux individuels, les isolant ainsi d'autres services sur un système particulier. Une fois les flux établis, vous pouvez observer le trafic de chacun d'entre eux et collecter des statistiques. Par la suite, vous pouvez affecter la quantité de bande passante adaptée et des priorités d'utilisation afin de contrôler l'utilisation sur les interfaces.

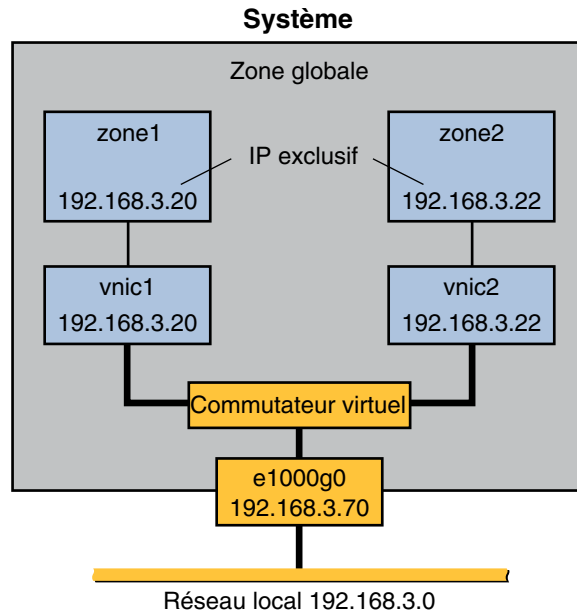
### Pour plus d'informations

- Pour en savoir plus sur les tâches d'implémentation du contrôle de flux, reportez-vous au [Chapitre 21, “Gestion des ressources réseau”](#).
- Pour des informations d'ordre conceptuel sur la gestion de la bande passante et le contrôle des ressources, reportez-vous à la section [“Définition du contrôle des ressources”](#) à la page 349
- Pour obtenir des informations techniques, reportez-vous aux pages de manuel [dladm\(1M\)](#) and [flowadm\(1M\)](#).

## Contrôle de flux pour le réseau virtuel

Ce scénario illustre la manière dont le contrôle de flux est utilisé au sein d'un réseau virtuel, par exemple le réseau virtuel de base présenté à la section [“Réseau virtuel basique sur un système unique”](#) à la page 356.

FIGURE 18-4 Réseau virtuel de base avec contrôles de flux



La topologie est décrite à la section [“Réseau virtuel basique sur un système unique” à la page 356](#). Ici, un hôte possède une interface réseau, `e1000g0`, avec deux VNIC, `vnic1` et `vnic2`. `zone1` est configuré sur `vnic1`, et `zone2` sur `vnic2`. La gestion des ressources pour le réseau virtuel implique la création de flux sur une base par VNIC. Ces flux définissent et isolent les paquets avec des caractéristiques similaires, telles que le numéro de port ou l'adresse IP de l'hôte émetteur. Vous pouvez affecter la bande passante en fonction de la politique d'utilisation du système.

Une autre utilisation très courante des contrôles de flux du trafic VNIC est celle des sociétés qui louent des zones. Vous devez créer différents contrats de niveau de service pour les clients, et louer les zones avec une quantité garantie de bande passante. Lorsque vous créez des flux sur la base de zones, vous pouvez isoler et observer le trafic de chaque client et contrôler l'utilisation de la bande passante. Si votre contrat de niveau de service est strictement basé sur l'utilisation, vous pouvez utiliser des statistiques et fonctions de comptabilisation pour facturer les clients.

Les contrôles de flux sont efficaces pour n'importe quel réseau qui requiert la gestion de la bande passante pour le trafic sur les zones. Les entreprises de taille plus importante, comme les fournisseurs d'applications hébergées (ASP) ou les fournisseurs d'accès Internet (FAI), peuvent tirer parti du contrôle des ressources sur les VNIC pour les centres de données et systèmes multiprocesseurs. Les zones individuelles peuvent être louées aux clients avec différents niveaux de service. Par conséquent, vous pouvez louer `zone1` au prix standard et offrir une bande passante standard. Vous pouvez ensuite louer `zone2` à un prix supérieur et donner au client en question un niveau élevé de bande passante.

## ▼ Création d'une politique d'utilisation des applications sur un réseau virtuel

- 1 **Dressez la liste des applications que vous voulez exécuter sur l'hôte.**
- 2 **Déterminez les applications qui ont toujours utilisé le plus de bande passante ou nécessitent la plus grande quantité de bande passante.**

Par exemple, l'application `telnet` peut ne pas consommer de grandes quantités de bande passante sur votre système, mais être très utilisée. À l'inverse, les applications de base de données consomment une grande quantité de bande passante, mais elles peuvent uniquement être utilisées de façon sporadique. Envisagez de contrôler le trafic pour ces applications avant de les affecter à des zones. Vous pouvez utiliser l'option de statistiques de la commande `dladm show-link` pour recueillir des statistiques, comme décrit à la section [“Collecte de statistiques relatives au trafic réseau sur les liaisons”](#) à la page 427.
- 3 **Affectez ces applications à des zones séparées.**
- 4 **Créez des flux pour toutes les applications s'exécutant dans zone1 dont vous souhaitez isoler et contrôler le trafic.**
- 5 **Affectez la bande passante à des flux en fonction des politiques d'utilisation en place pour votre site.**

## ▼ Création d'un accord de niveau de service pour le réseau virtuel

- 1 **Concevez une stratégie qui propose différents niveaux de services à des prix différents.**

Par exemple, vous pouvez créer des niveaux de service basiques, supérieurs et de haut niveau, dont le prix varie en conséquence.
- 2 **Décidez si vous voulez facturer des clients sur une base mensuelle, selon le niveau de service ou selon la bande passante réellement consommée.**

Si vous optez pour cette dernière structure de prix, vous avez besoin de recueillir des statistiques sur l'utilisation de chaque client.
- 3 **Créez un réseau virtuel sur un hôte, avec des conteneurs pour chaque client.**

Une implémentation très courante consiste à donner à chaque client sa propre zone exécutée sur une carte d'interface réseau virtuelle.

**4 Créez des flux qui isolent le trafic pour chaque zone.**

Pour isoler l'ensemble du trafic de la zone, utilisez l'adresse IP affectée à la VNIC de la zone.

**5 Affectez suffisamment de bande passante à chaque carte d'interface réseau virtuelle basée sur le niveau de service souscrit par le client attribuée à la zone de cette VNIC.**



## Configuration des réseaux virtuels (tâches)

Ce chapitre contient les tâches de configuration des réseaux virtuels internes, ou "réseaux en boîte." Les sujets traités comprennent :

- “Réseaux virtuels (liste des tâches)” à la page 367
- “Configuration de composants de virtualisation réseau dans Oracle Solaris” à la page 368
- “Utilisation de VNIC et de zones ” à la page 373

### Réseaux virtuels (liste des tâches)

Ce tableau répertorie les tâches de configuration d'un réseau virtuel, ainsi que des liens vers les tâches spécifiques. Notez que toutes les tâches ne s'appliquent pas à votre scénario de réseau virtuel.

Tâche	Description	Voir
Création de VNIC dans le système	Créez une ou plusieurs interfaces réseau virtuelles (VNIC). Les VNIC sont les pseudo-interfaces sur lesquelles vous construisez le réseau virtuel	<a href="#">“Procédure de création d'interface réseau virtuelle” à la page 369</a>
Création d'etherstubs dans le système	Créez un ou plusieurs etherstubs. Les etherstubs sont des commutateurs virtuels qui vous permettent de créer un réseau virtuel privé qui est isolé du réseau de plus grande taille.	<a href="#">“Création d'etherstubs ” à la page 371</a>

Tâche	Description	Voir
Création de zones pour utiliser des VNIC	Créez des VNIC et de nouvelles zones, et configurez-les pour créer un réseau virtuel de base.	<a href="#">“Création de nouvelles zones pour l'utiliser avec des VNIC” à la page 373</a>
Modification de zones pour utiliser des VNIC	Modifiez une zone existante pour créer un réseau virtuel.	<a href="#">“Modification de la configuration de zones existantes pour utiliser des VNIC” à la page 379</a>
Création d'un réseau virtuel privé	Configurez un réseau privé qui est isolé du réseau de plus grande taille en utilisant des etherstubs et des VNIC.	<a href="#">“Création d'un réseau virtuel privé” à la page 383</a>
Suppression de VNIC	Supprimez des VNIC qui ont été affectées à une zone sans supprimer la zone elle-même.	<a href="#">“Procédure de suppression du réseau virtuel sans suppression des zones” à la page 385</a>

# Configuration de composants de virtualisation réseau dans Oracle Solaris

Cette section présente les tâches de configuration des blocs de construction de virtualisation réseau dans Oracle Solaris. Les éléments suivants constituent les composants de base :

- Cartes réseau virtuelles (VNIC)
- Etherstubs

Les *VNIC* sont des pseudo-interfaces que vous créez au-dessus des liaisons de données. Une VNIC a généré automatiquement l'adresse MAC. Selon l'interface réseau en cours d'utilisation, vous pouvez explicitement attribuer à VNIC à une adresse MAC autre que l'adresse par défaut, comme décrit dans la page de manuel [dladm\(1M\)](#). Vous pouvez créer autant de VNIC sur une liaison de données que vous le souhaitez.

Les *Etherstubs* sont des pseudo-cartes réseau Ethernet qui sont gérées par l'administrateur système. Vous pouvez créer des VNIC sur des etherstubs plutôt que sur des liaisons physiques. Les VNIC sur un etherstub deviennent indépendantes des cartes réseau physiques dans le système. Avec des etherstubs, vous pouvez construire un réseau virtuel privé qui est isolé des autres réseaux virtuels dans le système et du réseau externe. Par exemple, vous souhaitez créer un environnement réseau dont l'accès est limité aux développeurs de votre entreprise plutôt qu'au réseau global. Etherstubs peut servir à créer un tel environnement.

Les etherstubs et les VNIC ne sont uniquement qu'une partie des fonctionnalités de virtualisation d'Oracle Solaris. En général, ces composants sont utilisés avec les conteneurs ou



les zones d'Oracle Solaris. En affectant des VNIC ou des etherstubs pour l'utilisation par des zones, vous pouvez créer un réseau au sein d'un système unique.

## ▼ Procédure de création d'interface réseau virtuelle

Cette procédure montre comment créer une carte réseau virtuelle (VNIC).

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 (Facultatif) Pour afficher les informations concernant les interfaces physiques disponibles du réseau, tapez la commande suivante :

```
# dladm show-phys
```

Cette commande affiche les cartes réseau physiques sur le système et leurs noms de liaison de données correspondants. A moins de créer des noms personnalisés pour vos liaisons de données, la liaison de données a le même nom que le nom du périphérique d'interface réseau. Par exemple, le périphérique `e1000g0` utilise le nom de liaison de données `e1000g0` jusqu'à ce que vous remplacez le nom de liaison avec un autre nom. Pour plus d'informations sur les noms de liaison de données personnalisés, reportez-vous à la section [“Noms des périphériques réseau et des liaisons de données”](#) à la page 26.

### 3 (Facultatif) Pour afficher les informations concernant les liaisons de données du système, tapez la commande suivante :

```
# dladm show-link
```

Cette commande répertorie les liaisons de données et leur état actuel. Assurez-vous que le champ STATE d'une liaison de données indique que la liaison de données est up. Vous pouvez configurer des VNIC uniquement sur des liaisons de données dont l'état est up.

### 4 (Facultatif) Pour visualiser les informations de l'adresse IP sur les interfaces configurées, tapez la commande suivante :

```
# ipadm show-addr
```

Cette commande répertorie les interfaces configurées sur votre système, y compris leurs adresses IP correspondantes.

### 5 Créez une VNIC sur une liaison de données.

```
# dladm create-vnic -l link vnic
```

- `link` est le nom de la liaison sur laquelle la VNIC est configurée.
- `vnic` est la VNIC à laquelle vous pouvez attribuer une étiquette avec un nom personnalisé.

**6 Créez une interface IP VNIC sur la liaison.**

```
# ipadm create-ip vnic
```

**7 Configurez la VNIC avec une adresse IP valide.**

Si vous affectez une adresse IP statique, utilisez la syntaxe suivante :

```
# ipadm create-addr -T static -a address addrobj
```

où *addrobj* utilise le format de nommage *interface/user-defined-string*, tel que *e1000g0/v4globalz*. Pour d'autres options lors de l'utilisation de cette commande, reportez-vous à la page de manuel [ipadm\(1M\)](#).

**8 Si vous utilisez une adresse IP statique, ajoutez les informations d'adresse dans le fichier `/etc/hosts`.**

**9 (Facultatif) Pour afficher la configuration d'adresse de la carte réseau virtuelle, saisissez la commande suivante :**

```
# ipadm show-addr
```

**10 (Facultatif) Pour afficher des informations relatives à la VNIC, tapez la commande suivante :**

```
# dladm show-vnic
```

**Exemple 19–1 Créez des interfaces réseau virtuelles**

Cet exemple contient les commandes permettant de créer des VNIC. Vous devez vous connecter au système en tant que superutilisateur ou un rôle équivalent pour exécuter les commandes.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED DUPLEX    DEVICE
net0      Ethernet   up         1000 full    e1000g0
net1      Ethernet   unknown    0      half     e1000g1

# dladm show-link
LINK      CLASS      MTU      STATE      BRIDGE      OVER
net0      phys       1500     up         --          --
net1      phys       1500     unknown    --          --

# ipadm show-if
IFNAME     CLASS      STATE      ACTIVE      OVER
lo0        loopback   ok         yes         --
net0       ip         ok         yes         --

# ipadm show-addr
ADDROBJ    TYPE      STATE      ADDR
lo0/?      static    ok         127.0.0.1/8
net0/v4addr static    ok         192.168.3.70/24

# dladm create-vnic -l net0 vnic0
# dladm create-vnic -l net0 vnic1
```

```
# dladm show-vnic
LINK      OVER      SPEED  MACADDRESS      MACADDRTYPE
vnic0     net0      1000  Mbps  2:8:20:c2:39:38  random
vnic1     net0      1000  Mbps  2:8:20:5f:84:ff  random
#
# ipadm create-ip vnic0
# ipadm create-ip vnic1

# ipadm create-addr -T static -a 192.168.3.80/24 vnic0/v4address
# ipadm create-addr -T static -a 192.168.3.85/24 vnic1/v4address
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/?        static    ok         127.0.0.1/8
net0/v4addr   static    ok         192.168.3.70/24
vnic0/v4address static    ok         192.168.3.80/24
vnic1/v4address static    ok         192.168.3.85/24
```

Le fichier `/etc/hosts` du système contient des informations similaires à celles figurant ci-dessous :

```
# cat /etc/hosts
#
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost    #For e1000g0
192.168.3.80 vnic1
192.168.3.85 vnic2
```

## ▼ Création d'etherstubs

Les etherstubs servent à isoler le réseau virtuel du reste des réseaux virtuels dans le système ainsi que du réseau externe auquel le système est connecté. Vous ne pouvez pas utiliser un etherstub tout seul. Au lieu de cela, les VNIC utilisés avec un etherstub pour créer des réseaux virtuelles privés ou isolés. Vous pouvez créer autant d'etherstubs que vous le souhaitez. Vous pouvez également créer autant de VNIC sur chaque etherstub que nécessaire.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 Créez un etherstub.

```
# dladm create-etherstub etherstub
```

### 3 Créez une VNIC sur l'etherstub.

```
# dladm create-vnic -l etherstub vnic
```

### 4 Configurez la VNIC avec une adresse privée.

---

**Remarque** – Pour isoler le réseau pour lequel vous configurez la VNIC sur un etherstub, assurez-vous d'utiliser une adresse IP privée qui ne peut pas être transmise au routeur par défaut du réseau externe. Par exemple, supposons que l'interface physique a l'adresse 192.168.3.0/24 qui indique que le système se trouve sur un réseau 192.168.3.x. Par conséquent, vous affectez une autre adresse qui n'est pas connu du routeur par défaut, comme 192.168.0.x.

---

**5 (Facultatif) Pour afficher des informations relatives aux VNIC, tapez la commande suivante :**

```
# dladm show-vnic
```

Cette commande répertorie toutes les VNIC du système et les données ou etherstubs sur lesquels les VNIC sont créées.

**6 (Facultatif) Pour afficher des informations relatives à l'ensemble des liaisons physiques et virtuelles sur le système, tapez la commande suivante :**

```
# dladm show-link
```

## Exemple 19–2 Création d'un etherstub

L'exemple suivant montre comment créer un etherstub puis configurer une VNIC sur l'etherstub. Cet exemple développe l'exemple précédent en ajoutant une troisième VNIC qui est configurée sur l'etherstub.

Vous devez vous connecter au système en tant que superutilisateur ou un rôle équivalent pour exécuter les commandes suivantes.

```
# dladm create-etherstub stub0
#
# dladm show-vnic
LINK      OVER      SPEED  MACADDRESS      MACADDRTYPE
vnic1     net9      1000 Mbps  2:8:20:c2:39:38  random
vnic2     net0      1000 Mbps  2:8:20:5f:84:ff  random
#
# dladm create-vnic -l stub0 vnic3
# ipadm create-vnic vnic3
# ipadm create-addr -T static -a 192.168.0.10/24 vnic3/privaddr
#
# dladm show-vnic
LINK      OVER      SPEED  MACADDRESS      MACADDRTYPE
vnic1     net0      1000 Mbps  2:8:20:c2:39:38  random
vnic2     net0      1000 Mbps  2:8:20:5f:84:ff  random
vnic3     stub0      1000 Mbps  2:8:20:54:f4:74  random
#
# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/?     static    ok         127.0.0.1/8
net0/v4addr static    ok         192.168.3.70/24
vnic1/v4address static    ok         192.168.3.80/24
vnic2/v4address static    ok         192.168.3.85/24
vnic3/privaddr static    ok         192.168.0.10/24
```

Le fichier `/etc/hosts` du système contient des informations similaires à celles figurant ci-dessous :

```
# cat /etc/hosts
#
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost   #For e1000g0
192.168.3.80 vnic1
192.168.3.85 vnic2
192.168.0.10 vnic3
```

## Utilisation de VNIC et de zones

Cette section vous explique comment déployer les composants de virtualisation réseau en les configurant pour être utilisés par zones. Cette section propose deux approches lors du travail avec des zones pour utiliser des VNIC :

- Création de zones entièrement nouvelles et configuration de VNIC sur ces zones
- Modification des configurations de zone existantes pour utiliser des VNIC

Lorsque vous vous connectez pour la première fois à un système, vous êtes automatiquement dans sa *zone globale*. Vous créez des VNIC sur la zone globale. Ensuite, vous configurez ces VNIC selon qu'elles doivent être utilisées par la zone globale ou les zones non globales de type exclusif. Pour une introduction aux zones, reportez-vous à la section “[Présentation des zones](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

## Création de nouvelles zones pour l'utiliser avec des VNIC

Utilisez cette approche si aucune zone configurée n'existe dans le système ou si vous souhaitez créer des zones pour utiliser des VNIC.

Pour utiliser des VNIC, une zone doit être configurée comme zone IP exclusive. Les étapes qui suivent configurent `zone1` avec `vnic1`. Vous devez effectuer les mêmes étapes pour configurer `zone2`. Pour plus de clarté, les invites indiquent dans quelle zone une commande spécifique est émise. Cependant, le chemin réel que les invites affichent peut varier en fonction des paramètres d'invite de votre système.

### ▼ Procédure de création et de configuration de la zone IP exclusive

Lorsque vous créez des zones, vous pouvez définir plusieurs paramètres. Les procédures de zone tout au long de ce chapitre se concentrent uniquement sur les paramètres qui sont pertinents pour faire fonctionner la zone avec des VNIC. Pour plus d'informations sur la

configuration des zones, reportez-vous à la section [Partie II, “Oracle Solaris Zones” du manuel \*Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources\*](#).

**Avant de commencer**

Assurez-vous que vous avez effectué les opérations suivantes :

- Création des VNIC pour les zones, comme expliqué dans la section [“Procédure de création d'interface réseau virtuelle”](#) à la page 369.
- Définition des noms de zone.
- Détermination des répertoires d'accueil de zone.
- Détermination de la carte réseau virtuelle à associer à une zone spécifique.
- Détermination des adresses IP pour les VNIC.
- Obtention d'autres informations réseau telles que l'adresse de routeur à fournir à la zone.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Pour chaque zone que vous créez, effectuez les étapes suivantes :**

**a. Démarrez l'utilitaire de configuration de zone et créez la zone.**

```
global# zonecfg -z zone
zonecfg:zone> create
```

**b. Définissez le répertoire personnel en définissant le paramètre zonepath.**

```
zonecfg:zone> set zonepath=/home/export/zone
```

**c. Activez l'initialisation automatique.**

```
zonecfg:zone> set autoboot=true
```

**d. Configurez la zone en mode IP exclusif.**

```
zonecfg:zone> set ip-type=exclusive
```

**e. Définir l'interface de la zone pour être une VNIC désignée.**

```
zonecfg:zone> add net
zonecfg:zone:net> set physical=vnic
zonecfg:zone:net> end
zonecfg:zone>
```

**f. Vérifiez et validez les paramètres, puis quittez l'utilitaire de configuration de zone.**

```
zonecfg:zone> verify
zonecfg:zone> commit
zonecfg:zone> exit
global#
```

- g. (Facultatif) Pour vérifier que les informations de la zone sont correctes, saisissez les informations suivantes :**

```
global# zonecfg -z zone info
```

---

**Remarque** – Vous pouvez afficher les mêmes informations tout en exécutant l'utilitaire de configuration de zone en tapant la commande suivante :

```
zonecfg:zone> info
```

---

### **3 Installez la zone.**

```
global# zoneadm -z zone install
```

---

**Remarque** – Le processus d'installation peut prendre un certain temps.

---

### **4 (Facultatif) Une fois la zone complètement installée, vérifiez l'état de la zone.**

```
zoneadm list -iv
```

---

**Remarque** – L'option `-iv` répertorie toutes les zones configurées indépendamment du fait qu'elles sont en cours d'exécution ou non. A ce stade, l'état de la zone que vous venez de créer sera "installed" plutôt que "running." Si vous utilisez l'option `-v`, seules les zones qui sont en cours d'exécution sont répertoriées et la zone que vous venez de créer est exclue.

---

### **5 Démarrez la zone.**

```
global# zoneadm -z zone boot
```

### **6 (Facultatif) Vérifiez que la zone est maintenant en cours d'exécution.**

```
global# zoneadm list -v
```

### **7 Une fois que la zone a complètement démarré, connectez-vous à la console de la zone.**

```
# zlogin -C zone
```

### **8 Fournissez les informations demandées.**

Certaines de ces informations sont le type de terminal, la région, la langue, etc. La plupart de ces informations sont fournies par la sélection d'une liste d'options. En règle générale, les options par défaut conviennent à moins que votre configuration système ne requière autre chose.

Les informations suivantes sont applicables à la procédure en cours que vous devez fournir ou vérifier :

- Nom d'hôte de la zone, par exemple zone1.
- Adresse IP de la zone qui est basée sur l'adresse IP sur la VNIC de la zone.
- Si IPv6 doit être activé.

- Si le système avec le réseau virtuel fait partie d'un sous-réseau.
- Masque de réseau de l'adresse IP.
- Route par défaut, qui peut être l'adresse IP de l'interface physique sur lequel le réseau virtuel est construit.

Une fois que vous avez fourni les informations requises pour la zone, la zone n'est pas redémarrée.

### Exemple 19–3 Configuration d'un réseau virtuel de base en créant des zones et des VNIC

Cet exemple permet de consolider toutes les étapes qui ont été précédemment fournies à la création de zones et de VNIC pour configurer le réseau virtuel. L'exemple utilise zone1 comme exemple de zone.

L'exemple est basé sur les hypothèses suivantes :

- VNIC : vnic1
- Noms de zone : zone1
- Répertoires personnels de zone : /home/exporter/zone-name .
- Affectations de zone de VNIC : vnic1 pour zone1
- Adresses IP : vnic1 utilise 192.168.3.80
- Adresse IP de l'interface physique : 192.168.3.70
- Adresse du routeur : 192.168.3.25

```
global# dladm show-phys
LINK    MEDIA      STATE      SPEED  DUPLEX    DEVICE
net0    Ethernet    up         1000   full     e1000g0
net1    Ethernet    unknown    1000   full     bge0

global# dladm show-lnk
LINK    CLASS      MTU      STATE      BRIDGE    OVER
net0    phys        1500     up         --         --
net1    phys        1500     unknown    --         --

global# ipadm show-if
IFNAME   CLASS      STATE      ACTIVE      OVER
lo0      loopback   ok         yes         --
net0     ip         ok         yes         --

global # ipadm show-addr
ADDROBJ  TYPE      STATE      ADDR
lo0/?    static    ok         127.0.0.1/8
net0/v4addr static    ok         192.168.3.70/24

global # dladm create-vnic -l net0 vnic1

global # dladm show-vnic
LINK    OVER      SPEED      MACADDRESS      MACADDRTYPE
vnic1   net0      1000 Mbps   2:8:20:5f:84:ff random

global # ipadm create-ip vnic1
```



```

global # ipadm create-addr -T static -a 192.168.3.80/24 vnic1/v4address
global # ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/?        static    ok         127.0.0.1/8
net0/v4addr   static    ok         192.168.3.70/24
vnic1/v4address static    ok         192.168.3.80/24

global # cat /etc/hosts
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost    #For net0
192.168.3.80 zone1     #using vnic1

global # zonecfg -z zone1
zonecfg:zone1> create
zonecfg:zone1> set zonepath=/export/home/zone1
zonecfg:zone1> seet autoboot=true
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic1
zonecfg:zone1:net> end
zonecfg:zone1> verify

zonecfg:zone1> info
zonename: zone1
zonepath: /export/home/zone1
brand:     native
autoboot:  true
net:
    address not specified
    physical: vnic1

zonecfg:zone1> commit
zonecfg:zone1> exit
global#
global# zoneadm -z zone1 verify
WARNING: /export/home/zone1 does not exist, so it could not be verified.
When 'zoneadm install' is run, 'install' will try to create
/export/home/zone1, and 'verify' will be tried again,
but the 'verify' may fail if:
the parent directory of /export/home/zone1 is group- or other-writable
or
/export/home/zone1 overlaps with any other installed zones.

global# zoneadm -z zone1 install
Preparing to install zone <zone1>
Creating list of files to copy from the global zone.
.
.
Zone <zone1> is initialized.

global# zoneadm list -iv
ID NAME      STATUS    PATH                                BRAND    IP
0  global     running   /                                    native   shared
-  zone1      installed /export/home/zone1                 native   excl

global# zoneadm -z zone1 boot
global# zoneadm list -v
ID NAME      STATUS    PATH                                BRAND    IP

```

```
0 global running / native shared
1 zone1 running /export/home/zone1 native excl
```

**zlogin -C zone1**

What type of terminal are you using?

.

.

.

8) Sun Workstation

9) Televideo 910

10) Televideo 925

11) Wyse Model 50

12) X Terminal Emulator (xterms)

13) CDE Terminal Emulator (dtterm)

14) Other

Type the number of your choice and press Return: **13**

.

(More prompts)

..

Fournissez les informations quand vous y êtes invité. Pour obtenir des informations sur les réseaux, fournissez les éléments suivants :

Hostname: **zone1**

IP address: **192.168.3.80**

System part of a subnet: **Yes**

Netmask: 255.255.255.0

Enable IPv6: **No**

Default route: **192.168.3.70**

Router IP address: **192.168.3.25**

**Étapes suivantes** Vous pouvez utiliser différents outils pour observer le trafic réseau et prendre les statistiques sur l'utilisation de la zone.

- Pour vérifier que votre réseau est correctement configuré, reportez-vous au [Chapitre 5, “Administration d’un réseau TCP/IP”](#) du manuel *Administration d’Oracle Solaris : Services IP*.
- Pour observer le trafic sur le réseau, reportez-vous à la section “[Contrôle du transfert des paquets à l’aide de la commande snoop](#)” du manuel *Administration d’Oracle Solaris : Services IP*.
- Pour gérer la façon dont le réseau utilise les ressources système, reportez-vous au [Chapitre 21, “Gestion des ressources réseau”](#).
- Pour obtenir des statistiques à des fins comptables, reportez-vous au [Chapitre 22, “Contrôle du trafic réseau et de l'utilisation des ressources”](#).

Si vous avez besoin de désassembler le réseau virtuel, reportez-vous à la section “[Procédure de suppression du réseau virtuel sans suppression des zones](#)” à la page 385.

# Modification de la configuration de zones existantes pour utiliser des VNIC

Utilisez cette méthode si vous souhaitez que les zones existantes utilisent des VNIC. Dans ce cas, les zones ont déjà des noms de zone et leurs répertoires personnels ou `zonpath` sont déjà définis.

## ▼ Avant de commencer

### Procédure de reconfiguration d'une zone pour qu'elle utilise une VNIC

Assurez-vous que vous avez effectué les opérations suivantes :

- Création des VNIC pour les zones, comme expliqué dans la section [“Procédure de création d'interface réseau virtuelle”](#) à la page 369.
- Détermination de la carte réseau virtuelle à associer à une zone spécifique.
- Détermination des adresses IP pour les VNIC.
- Obtention d'autres informations réseau telles que l'adresse de routeur à fournir à la zone.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Assurez-vous que les zones sont correctement configurées et en cours d'exécution sur le système.

```
global# zoneadm list -v
```

---

**Remarque** – L'option `-v` répertorie uniquement les zones qui sont en cours d'exécution. Pour répertorier toutes les zones configurées y compris celles qui n'ont pas été démarrées, utilisez l'option `-iv`.

---

#### 3 Pour chaque zone que vous souhaitez configurer avec des VNIC, effectuez les opérations suivantes :

##### a. Vérifiez les informations relatives à la zone.

```
global# zonecfg -z zone info
```

Vérifiez les informations relatives au type d'IP et d'interface réseau. L'interface réseau est désignée par le paramètre *physique*. Pour qu'une zone soit configurée avec une carte réseau virtuelle, la zone doit être une zone IP exclusive et l'interface réseau doit spécifier la VNIC.

##### b. Si nécessaire, changez la zone partagée en zone IP exclusive.

```
global# zonecfg -z zone
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1>
```

**c. Changez l'interface de la zone pour qu'elle utilise une VNIC.**

```
zonecfg:zone1> remove net physical=non-vnic-interface
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic
zonecfg:zone1:net> end
zonecfg:zone1>
```

**d. Changez d'autres valeurs de paramètres comme il convient.**

**e. Vérifiez et validez les changements que vous avez implémentés, puis quitter la zone.**

```
zonecfg:zone1 verify
zonecfg:zone1> commit
zonecfg:zone1> exit
global#
```

**f. Réinitialisez la zone.**

```
global# zoneadm -z zone reboot
```

**g. Une fois la zone redémarrée, vérifiez que ses informations `ip-type` et `physical` sont correctes.**

```
global# zonecfg -z zone info ip-type
global# zonecfg -z zone info net
```

L'information doit indiquer que le type d'IP de la zone est exclusif et qu'elle utilise la VNIC désignée.

**4 Connectez-vous à la zone.**

```
global# zlogin zone
```

**5 Configurez la VNIC avec une adresse IP valide.**

Si vous affectez une adresse statique à la carte réseau virtuelle, vous devez saisir la commande suivante :

```
zone# ipadm create-addr -T static -a address addrobj
```

où *address* peut utiliser la notation CIDR alors que *addrobj* suit la convention de nommage *interface/user-defined-string*.

**6 (Facultatif) Vérifiez la configuration de l'interface au sein de la zone.**

```
zone# ipadm show-if
```

ou

```
zone# ipadm show-addr
```

### Exemple 19–4 Configuration d'un réseau virtuel de base en modifiant la configuration de zone pour qu'elle utilise des VNIC

Cet exemple utilise le même système et fonctionne sur les mêmes hypothèses que dans l'exemple précédent. Supposons que dans ce système, zone2 existe déjà comme une zone partagée. Vous souhaitez modifier zone2 pour utiliser vnic2.

```
global# dladm show-link
LINK    CLASS    MTU    STATE    BRIDGE    OVER
net0    phys      1500    up      --      --
net1    phys      1500    unknown --      --
vnic1   vnic      1500    up      --      e1000g0

global# ipadm show-if
IFNAME   CLASS    STATE    ACTIVE    OVER
lo0      loopback ok       yes      --
net0     ip       ok       yes      --
vnic1    ip       ok       yes      --

global # ipadm show-addr
ADDROBJ   TYPE    STATE    ADDR
lo0/?     static  ok       127.0.0.1/8
net0/v4addr static  ok       192.168.3.70/24
vnic1/v4address static  ok       192.168.3.80/24

global # dladm create-vnic -l net0 vnic2
global # dladm show-vnic
LINK    OVER    SPEED    MACADDRESS    MACADDRTYPE
vnic1    net0    1000 Mbps  2:8:20:5f:84:ff  random
vnic2    net0    1000 Mbps  2:8:20:54:f4:74  random

global# zoneadm list -v
ID NAME    STATUS    PATH                    BRAND    IP
0  global  running  /                       native   shared
1  zone1   running  /export/home/zone1     native   excl
2  zone2   running  /export/home/zone2     native   shared

global# zonecfg -z zone2 info
zonename: zone2
zonepath: /export/home/zone2
brand: native
autoboot: true
bootargs:
pool: z2-pool
limitpriv:
scheduling-class:
ip-type: shared
hostid:
inherit-pkg-dir:
    dir: /lib
inherit-pkg-dir:
    dir: /platform
inherit-pkg-dir:
    dir: /sbin
inherit-pkg-dir:
    dir: /usr
inherit-pkg-dir:
```

```

        dir: /etc/crypto
net:
    address not specified
    physical: e1000g0
    defrouter not specified
global#

global# zonecfg -z zone2
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> remove net physical=net0
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic2
zonecfg:zone1:net> end
zonecfg:zone1> verify
zonecfg:zone1> commit
zonecfg:zone1> exit
global#

global# zonecfg -z zone2 info ip-type
ip-type: exclusive
global#

global# zonecfg -z zone2 info net
net:
    address ot specified
    physical: vnic2
    defrouter not specified
global#

global# zlogin zone2
zone2# ipadm create-ip vnic2
zone2# ipadm create-addr -T static -a 192.168.3.85/24 vnic2/v4address

zone2# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4        static    ok         127.0.0.1/8
vnic2/v4address static    ok         192.168.3.85/24

zone1# exit
global#

global# vi /etc/hosts
#
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost    #For e1000g0
192.168.3.80 zone1      #using vnic1
192.168.3.85 zone2      #using vnic2

```

**Étapes suivantes** Vous avez la possibilité de configurer l'installation réseau encore plus afin de personnaliser l'utilisation des ressources système ou vous pouvez utiliser différents outils pour observer le trafic réseau et collecter des statistiques sur l'utilisation des ressources.

- Pour vérifier que votre réseau est correctement configuré, reportez-vous au
- Pour observer le trafic sur le réseau, reportez-vous à
- Pour gérer la façon dont le réseau utilise des ressources système, reportez-vous au

- Pour obtenir des statistiques à des fins de comptabilisation, reportez-vous au

Si vous avez besoin de désassembler le réseau virtuel, reportez-vous à la section “[Procédure de suppression du réseau virtuel sans suppression des zones](#)” à la page 385.

## Création d'un réseau virtuel privé

L'exemple de cette section vous montre comment configurer un *réseau virtuel privé* sur un système unique. Les réseaux virtuels privés sont différents des réseaux privés virtuels (VPN). Un logiciel VPN crée une liaison point à point sécurisée entre deux systèmes d'extrémité. Le réseau privé configuré par les tâches dans cette section est un réseau virtuel sur une boîte qui n'est pas accessible par les systèmes externes.

Pour autoriser les zones d'un réseau privé à envoyer des paquets au-delà de l'hôte, configurez un périphérique NAT. NAT traduit les adresses IP privées de la VNIC vers les adresses IP routables de l'interface réseau physique, mais sans exposer les adresses IP privées au réseau externe. La configuration du routage est également évoquée dans l'exemple suivant.

### EXEMPLE 19-5 Création d'une configuration de réseau virtuel privé

Cet exemple utilise le même système et fonctionne sur les mêmes hypothèses que dans les exemples précédents. Plus précisément, zone1 et zone2 sont maintenant configurées en tant que réseaux virtuels. Supposons que zone3 existe déjà dans le système. Vous allez modifier zone3 afin d'en faire un réseau privé isolé du reste du réseau. Ensuite, vous allez configurer NAT et la transmission IP pour autoriser le réseau privé virtuel à envoyer des paquets à l'extérieur de l'hôte mais tout en cachant son adresse privée au réseau externe.

```
global# dladm create-etherstub stub0

global# dladm create-vnic -l etherstub0 vnic3
global# dladm show-vnic
LINK      OVER      SPEED      MACADDRESS      MACADDRTYPE
vnic1     net0      1000 Mbps   2:8:20:5f:84:ff   random
vnic2     net0      1000 Mbps   2:8:20:54:f4:74   random
vnic3     stub0      0 Mbps      2:8:20:6b:8:ab    random

global# vi /etc/hosts
#
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost      #For e1000g0
192.168.3.80 zone1        #using vnic1
192.168.3.85 zone2        #using vnic2
```

A ce stade, vous pouvez modifier zone3 pour obtenir une zone IP exclusive sur vnic3.

```
global# zonecfg -z zone3
zonecfg:zone3> set ip-type=exclusive
zonecfg:zone3> remove net physical=e1000g0
```

**EXEMPLE 19-5** Création d'une configuration de réseau virtuel privé (Suite)

```

zonecfg:zone3> add net
zonecfg:zone3:net> set physical=vnic3
zonecfg:zone3:net> end
zonecfg:zone3> vereify
zonecfg:zone3> commit
zonecfg:zone3> exit
global#

global# zonecfg -z zone3 info ip-type
ip-type: exclusive
global#

global# zonecfg -z zone3 info net
net:
    address ot specified
    physical: vnic3
    defrouter not specified
global#

global# zlogin zone3
zone3# ipadm create-ip vnic3
zone3# ipadm create-addr -T static -a 192.168.0.10/24 vnic3/privaddr

zone3# ipadm show-addr
ADDROBJ          TYPE      STATE      ADDR
lo0/v4           static    ok         127.0.0.1/8
vnic3/privaddr   static    ok         192.168.0.10/24
zone3# exit

global# ipadm show-addr
ADDROBJ          TYPE      STATE      ADDR
lo0/v4           static    ok         127.0.0.1/8
net0/v4addr      static    ok         192.168.3.70/24
vnic1/v4address  static    ok         192.168.3.80/24
vnic2/v4address  static    ok         192.168.3.85/24
vnic3/privaddr   static    ok         192.168.0.10/24

global# vi /etc/hosts
::1             localhost
127.0.0.1       localhost
192.168.3.70    loghost    #For e1000g0
192.168.3.80    zone1      #using vnic1
192.168.3.85    zone2      #using vnic2
192.168.0.10    zone3      #using vnic3

global# routeadm

```

Configuration Option	Current Configuration	Current System State
IPv4 routing	enabled	enabled
IPv6 routing	disabled	disabled
IPv4 forwarding	disabled	disabled
IPv6 forwarding	disabled	disabled
Routing services	"route:default ripng:default"	



EXEMPLE 19-5   Création d'une configuration de réseau virtuel privé       (Suite)

```
global# ipadm set-ifprop -p forwarding=yes -m ipv4 e1000g0

global# vi /etc/ipf/ipnat.conf
map e1000g0 192.168.0.0/24 -> 0/32 portmap tcp/udp auto
map e1000g0 192.168.0.0/24 -> 0/32

global# svcadm enable network/ipfilter

global# zoneadm -z zone1 boot
global# zoneadm -z zone2 boot
global# zoneadm -z zone3 boot
```

▼ **Procédure de suppression du réseau virtuel sans suppression des zones**

La procédure suivante indique comment désactiver le réseau virtuel d'une zone tout en conservant cette dernière intacte.

Utilisez cette procédure si vous devez effectuer l'une des opérations suivantes :

- Utiliser les zones existantes dans une configuration différente. Par exemple, vous pouvez avoir besoin de configurer les zones comme faisant partie d'un réseau privé qui nécessiterait de créer la zone à l'aide d'un etherstub.
- Migrer les zones vers un autre réseau.
- Déplacer les zones vers un autre chemin de zone.
- Cloner les zones, comme expliqué dans la section “Clonage d’une zone non globale dans le même système” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

**Avant de commencer** Cette tâche suppose que vous disposez d'un réseau virtuel en cours d'exécution qui se compose de zones IP exclusives.

- 1 **Connectez-vous en tant qu'administrateur.**  
Pour plus d'informations, reportez-vous à la section “Procédure d'obtention des droits d'administration” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Vérifiez l'état des zones actuellement configurées.**

```
# zoneadm list -v
```

Des informations similaires à celles figurant ci-dessous s'affiche :

ID	NAME	STATUS	PATH	BRAND	IP
0	global	running	/	native	shared
1	zone1	running	/export/home/zone1	native	excl

2	zone2	running	/export/home/zone2	native	excl
3	zone3	running	/export/home/zone3	native	excl

**3 Arrêtez les zones IP exclusives du réseau virtuel.**

Exécutez la commande suivante séparément pour chaque zone à arrêter.

```
global# zoneadm -z zone-name halt
```

Lorsque vous arrêtez la zone, vous supprimez l'environnement d'application de la zone et arrêtez un certain nombre d'activités du système, comme expliqué dans la section “[Arrêt d’une zone](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

**4 Vérifiez que les zones sont arrêtées.**

```
# zoneadm list -iv
ID NAME          STATUS    PATH                                BRAND  IP
0  global         running   /                                  native shared
-  zone1          installed /export/home/zone1              native excl
-  zone2          installed /export/home/zone2              native excl
-  zone3          installed /export/home/zone3              native excl
```

Notez que les zones ne sont plus en cours d'exécution, mais restent installées. Pour réinitialiser une zone, reportez-vous à la section “[Initialisation d’une zone](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

**5 Répertoriez les VNIC qui ont été configurées pour les zones arrêtées.**

```
# dladm show-vnic
LINK    OVER          SPEED  MACADDRESS          MACADDRTYPE
vnic1   net0          1000 Mbps  2:8:20:5f:84:ff    random
vnic2   net1          1000 Mbps  2:8:20:54:f4:74    random
vnic3   stub0         1000 MBps  2:8:20:c2:39:38    random
```

Le résultat indique que les VNIC sont toujours configurées en tant que liaisons de données dans la zone globale. Cependant, leurs interfaces IP ont été créées et activées sur les zones avec lesquelles ces VNIC sont associées, et non pas sur la zone globale. Ces zones non globales sont maintenant arrêtées.

**6 Supprimez les VNIC.**

```
# dladm delete-vnic vnic
```

Par exemple, la commande suivante permet de supprimer les VNIC dans les zones de la [Figure 18–1](#).

```
# dladm delete-vnic vnic1
# dladm delete-vnic vnic2
```

## Utilisation de la protection des liens dans les environnements virtualisés

---

Ce chapitre décrit la protection des liens et leur configuration sur les systèmes Oracle Solaris. Ce chapitre se compose des sections suivantes :

- [“Présentation de la protection de liens” à la page 387](#)
- [“Configuration de la protection des liens \(liste des tâches\)” à la page 389](#)

### Présentation de la protection de liens

Avec la généralisation de la virtualisation dans les configurations système, l'administrateur de l'hôte peut donner un accès exclusif à un lien physique ou virtuel aux machines virtuelles (VM) invitées. Cette configuration améliore les performances du réseau, puisqu'elle permet d'isoler le trafic réseau de l'environnement virtuel du trafic général envoyé ou reçu par le système hôte. Dans le même temps, cette configuration peut exposer le système et l'ensemble du réseau au risque de paquets dangereux qu'un environnement invité peut générer.

La protection des liens vise à empêcher les dommages qui peuvent être causés au réseau par des machines virtuelles invitées potentiellement malveillantes. Cette fonction offre une protection contre les menaces basiques suivantes :

- Usurpation d'adresses IP et MAC
- Usurpation de trame L2, telles que les attaques Bridge Protocol Data Unit (BPDU)

---

**Remarque** – La protection des liens ne doit pas remplacer le déploiement d'un pare-feu, en particulier pour les configurations avec des exigences de filtrage complexes.

---

## Types de protection des liens

Par défaut, le mécanisme de protection des liens est désactivé. Pour activer la protection des liens, spécifiez un ou plusieurs des types de protection suivants en tant que valeurs pour la propriété de lien `protection` :

- |                          |   |
|--------------------------|---|
| <code>mac-nospoof</code> | Active la protection contre l'usurpation d'adresse MAC. L'adresse MAC source d'un paquet sortant doit correspondre à l'adresse MAC configurée de la liaison de données. Dans le cas contraire, le paquet est supprimé. Si le lien appartient à une zone, l'activation de <code>mac-nospoof</code> empêche le propriétaire de la zone de modifier l'adresse MAC du lien. |
| <code>ip-nospoof</code>  | Active la protection contre l'usurpation d'adresse IP. Tous les paquets IP, ARP ou NDP sortants doivent avoir un champ d'adresse qui correspond à une adresse IP configurée par DHCP ou à l'une des adresses répertoriées dans la propriété de lien <code>allowed-ips</code> . Dans le cas contraire, le paquet est supprimé.   |

La propriété de lien `allowed-ips` fonctionne avec le type de protection `ip-nospoof`. Par défaut, la liste spécifiée par cette propriété est vide. Si la propriété est vide ou non configurée, les adresses IP suivantes sont implicitement incluses dans la propriété. Ces adresses IP sont mises en correspondance avec l'adresse IP des paquets sortants afin de déterminer si les paquets sont autorisés à être transmis ou sont supprimés.

- Adresses IPv4 ou IPv6 configurées par DHCP apprises dynamiquement
- Liaison des adresses IPv6 locales conformes à la norme RFC 2464 et dérivées de l'adresse MAC du lien

La liste suivante indique un protocole et le champ d'adresse associé du paquet sortant correspondant, qui doit correspondre à une adresse dans la propriété `allowed-ips`. Si cette propriété est vide, l'adresse du paquet doit correspondre à une adresse IP configurée par DHCP.

- IP (IPv4 ou IPv6) : adresse source du paquet
- ARP : adresse du protocole émetteur du paquet

- |                         |   |
|-------------------------|---|
| <code>restricted</code> | Restreint les paquets sortants aux seuls paquets avec des protocoles de types IPv4, IPv6 et ARP. Les autres paquets qui ne sont pas des types répertoriés sont supprimés. Ce type de protection empêche le lien de générer des trames de contrôle L2 potentiellement nuisibles. |
|-------------------------|---|

**Remarque** – Les paquets supprimés en raison de la protection des liens font l'objet d'un suivi par les statistiques de noyau suivantes : `mac_spoofed`, `ip_spoofed` et `rest_reint`. Ces statistiques correspondent aux trois types de protection. Utilisez la commande `kstat` pour récupérer ces statistiques par lien. Pour plus d'informations sur la récupération de ces statistiques, reportez-vous à la page de manuel [kstat\(1M\)](#).

## Configuration de la protection des liens (liste des tâches)

Pour utiliser la protection des liens, vous utilisez l'une des options de la commande `dladm` pour définir les propriétés du lien. Si le type de protection fonctionne avec d'autres fichiers de configuration, par exemple, `ip-nospoof` avec `allowed-ips`, vous pouvez effectuer deux actions générales. Tout d'abord, activez la protection des liens. Ensuite, personnalisez le fichier de configuration afin de déterminer la manière dont la protection des liens fonctionne.

**Remarque** – Vous devez configurer la protection des liens dans la zone globale.

Les éléments suivants renvoient aux tâches que vous pouvez utiliser pour configurer la protection des liens sur un serveur Oracle Solaris.

Tâche	Description	Voir
Activation du mécanisme de protection des liens	Utilisez la commande <code>dladm set-linkprop</code> pour activer les types de protection des liens pour un lien.	<a href="#">“Activation du mécanisme de protection des liens” à la page 390</a>
Désactivation du mécanisme de protection des liens	Utilisez la commande <code>dladm reset-linkprop</code> pour désactiver la protection des liens.	<a href="#">“Désactivation de la protection des liens” à la page 390</a>
Personnalisation du type de protection des liens IP	Utilisez la commande <code>dladm set-linkprop</code> pour configurer ou modifier les valeurs dans la propriété <code>allowed-ips</code> .	<a href="#">“Spécification des adresses IP pour la protection contre l'usurpation d'adresse IP” à la page 390</a>
Affichage de la configuration de la protection des liens	Utilisez la commande <code>dladm show-linkprop</code> pour afficher la configuration de la protection des liens en spécifiant les noms de propriété <code>protection</code> et <code>allowed-ips</code> .	<a href="#">“Affichage de la configuration de la protection des liens” à la page 391</a>

## ▼ Activation du mécanisme de protection des liens

Cette procédure permet d'activer un ou plusieurs des types de protection des liens suivants : `mac-nospoof`, `ip-nospoof` et `restricted`.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Activez la protection des liens en spécifiant un ou plusieurs types de protection.

```
# dladm set-linkprop -p protection=value[,value,...] link
```

Dans l'exemple suivant, les trois types de protection des liens sont activés sur le lien `vnic0` :

```
# dladm set-linkprop -p protection=mac-nospoof,ip-nospoof,restricted vnic0
```

## ▼ Désactivation de la protection des liens

Cette procédure permet de réinitialiser la protection des liens aux valeurs par défaut, ce qui désactive la protection des liens.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Désactivez la protection des liens en réinitialisant la propriété `protection` à sa valeur par défaut.

```
# dladm reset-linkprop -p protection link
```

## ▼ Spécification des adresses IP pour la protection contre l'usurpation d'adresse IP

Notez que la propriété `allowed-ips` n'est utilisée que si la propriété `protection` active le type de protection `ip-nospoof`.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Assurez-vous d'avoir activé la protection contre l'usurpation d'adresses IP.

Si vous n'avez pas encore activé ce type de protection des liens, exécutez la commande suivante :

```
# dladm set-linkprop -p protection=ip-nospoof
```

**3 Indiquez une liste d'adresses IP en tant que valeurs pour la propriété de lien `allowed-ips` .**

```
# dladm set-linkprop -p allowed-ips=IP-addr[,IP-addr,...] link
```

L'exemple suivant montre comment spécifier les adresses IP 10.0.0.1 et 10.0.0.2 en tant que valeurs pour la propriété `allowed-ips` du lien `vnic0` :

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 vnic0
```

**▼ Affichage de la configuration de la protection des liens**

Les valeurs des propriétés `protection` et `allowed-ips` indiquent comment la protection des liens est configurée. Notez que la propriété `allowed-ips` n'est utilisée que si la propriété `protection` spécifie le type de protection `ip-nospoof`.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Affichez les valeurs de la propriété de protection des liens.**

```
# dladm show-linkprop -p protection,allowed-ips link
```

L'exemple suivant affiche les valeurs pour les propriétés `protection` et `allowed-ips` du lien `vnic0` :

```
# dladm show-linkprop -p protection,allowed-ips vnic0
```

LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
vnic0	protection	rw	ip-nospoof mac-nospoof restricted	--	--
vnic0	allowed-ips	rw	10.0.0.1, 10.0.0.2	--	--





## Gestion des ressources réseau

---

Ce chapitre explique comment gérer les ressources sur les liaisons de données, y compris les liaisons virtuelles telles que les VNIC. La gestion des ressources réseau implémente une qualité de service afin d'améliorer les performances en particulier dans le réseau virtuel.

Ce chapitre se compose des sections suivantes :

- “Présentation de la gestion des ressources réseau” à la page 393
- “Gestion des ressources réseau (liste des tâches)” à la page 396
- “Gestion des ressources sur liaisons de données” à la page 397
- “Gestion des ressources sur les flux” à la page 416

### Présentation de la gestion des ressources réseau

Cette section explique la gestion des ressources réseau en introduisant les couloirs réseau. Elle décrit également comment implémenter la gestion des ressources réseau en définissant des propriétés de liaisons de données. Les flux sont également définis comme une autre manière de définir des contrôles des ressources pour traiter le trafic réseau.

### Propriétés de liaisons de données pour le contrôle des ressources

Dans les précédentes versions d'Oracle Solaris, l'implémentation d'une qualité de service est un processus complexe. Le processus consiste à définir des disciplines mises en file d'attente, des classes et des règles de filtrage, et à indiquer les relations entre l'ensemble de ces composants. Pour plus d'informations, reportez-vous à la [Partie V](#), “Qualité de service IP (IPQoS)” du [manuel \*Administration d'Oracle Solaris : Services IP\*](#).

Dans cette version, la qualité de service est obtenue plus facilement et dynamiquement par la gestion de ressources réseau. La gestion des ressources réseau consiste à définir des propriétés de liaisons de données qui se rapportent aux ressources réseau. En définissant ces propriétés,

vous pouvez déterminer la quantité d'une ressource donnée à utiliser pour les processus réseau. Par exemple, une liaison peut être associée à un nombre spécifique de CPU qui sont réservées exclusivement pour les processus réseau. Ou, une liaison peut se voir attribuer une bande passante pour traiter un type spécifique de trafic réseau. Une fois qu'une propriété de ressource est définie, le nouveau paramètre prend effet immédiatement. Cette méthode permet une gestion flexible des ressources. Vous pouvez définir des propriétés de ressource lors de la création de la liaison. Vous pouvez également définir ces propriétés par la suite, par exemple, après avoir étudié l'utilisation des ressources dans le temps et déterminé comment mieux répartir les ressources. Les procédures d'allocation des ressources s'appliquent à l'environnement de réseau virtuel ainsi qu'au réseau physique traditionnel.

La gestion des ressources réseau est comparable à la création de couloirs réservés au trafic. Lorsque vous combinez différentes ressources pour traiter des types spécifiques de paquets réseau, ces ressources forment un *couloir réseau* pour ces paquets. Vous pouvez affecter des ressources différemment pour chaque couloir réseau. Par exemple, vous pouvez allouer davantage de ressources à un couloir où le trafic réseau est le plus lourd. En configurant des couloirs réseau, où les ressources sont distribuées selon le besoin réel, vous augmentez l'efficacité du système pour traiter les paquets. Pour plus d'informations à propos des couloirs réseau, reportez-vous à la section [“Présentation du flux de trafic réseau”](#) à la page 423.

La gestion des ressources réseau est utile pour les tâches suivantes :

- Approvisionnement réseau
- Etablissement de contrats de niveau de service
- Facturation de clients
- Diagnostic des problèmes de sécurité

Vous pouvez isoler, définir l'ordre de priorité, effectuer le suivi et contrôler le trafic de données sur un système individuel sans les définitions de règle QoS complexes se trouvant dans les versions précédentes.

## Gestion des ressources réseau à l'aide de flux

Un *flux* est un moyen personnalisé de catégoriser des paquets pour mieux contrôler la manière dont les ressources sont utilisées pour traiter ces paquets. Les paquets réseau peuvent être catégorisés en fonction d'un *attribut*. Les paquets qui partagent un attribut constituent un flux et sont étiquetés avec un nom de flux spécifique. Le flux peut ensuite être affecté à des ressources spécifiques.

Les attributs qui serviront de base pour créer les flux sont dérivés des informations de l'en-tête d'un paquet. Vous pouvez organiser le trafic en flux de paquets en fonction de l'un des attributs suivants :

- Adresse IP
- Nom du protocole de transport (UDP, TCP ou SCTP)

- Application du numéro de port, par exemple, le port 21 pour FTP
- Attribut de champ DS, qui est utilisé pour la qualité de service dans les paquets IPv6 uniquement. Pour plus d'informations sur le champ DS, reportez-vous à la section “[Point de code DS](#)” du manuel *Administration d'Oracle Solaris : Services IP*.

Un flux peut uniquement être basé sur un seul des attributs de la liste. Par exemple, vous pouvez créer un flux selon le port en cours d'utilisation, comme que le port 21 pour FTP, ou selon les adresses IP, comme des paquets à partir d'une adresse IP source. Toutefois, vous ne pouvez pas créer, à partir d'une adresse IP spécifiée, un flux de paquets qui sont reçus sur le port 21 (FTP). De même, vous ne pouvez pas créer un flux pour tout le trafic depuis l'adresse IP 192 . 168 . 1 . 10 puis créer un flux pour un trafic de couche transport sur 192 . 168 . 1 . 10. Ainsi, vous pouvez configurer plusieurs flux sur un système, avec chaque flux basé sur un attribut différent.

## Commandes pour la gestion des ressources réseau

La commande permettant d'allouer des ressources réseau dépend du fait que vous travailliez directement sur des liaisons de données ou des flux.

- Pour les liaisons de données, utilisez la sous-commande `dladm` appropriée selon que vous êtes en train de définir la propriété lors de la création de la liaison ou la définition de la propriété d'une liaison existante. Pour créer une liaison et allouer des ressources simultanément, utilisez la syntaxe suivante :

```
# dladm create-vnic -l link -p property=value[,property=value] vnic
```

où `link` peut être une liaison physique ou virtuelle.

Pour définir la propriété d'une liaison existante, utilisez la syntaxe suivante :

```
# dladm set-linkprop -p property=value[,property=value] link
```

Pour plus de détails sur la commande `dladm` et les propriétés que cette commande gère, reportez-vous à la page de manuel [dladm\(1M\)](#).

Voici les propriétés de liaison que vous pouvez définir pour l'allocation des ressources :

- Bande passante : vous pouvez limiter la bande passante d'un matériel pour l'utilisation d'une liaison.
- Anneaux de carte réseau (NIC) : si une carte réseau prend en charge l'allocation d'anneaux, ses anneaux de transmission et de réception peuvent être affectés par un usage dédié par les liaisons de données. Les anneaux de carte réseau sont abordés dans la section “[Transmission et réception d'anneaux](#)” à la page 397.
- Pools de CPU : les pools de CPU sont généralement créés et associés à des zones spécifiques. Ces groupes peuvent être assignés aux liaisons de données à réserver aux jeux de CPU pour gérer les processus réseau de leurs zones associées. Les CPU et les pools sont abordés dans la section “[Pools et CPU](#)” à la page 411.

- CPU : dans un système à plusieurs processeurs, vous pouvez consacrer un nombre donné de processeurs pour un traitement réseau spécifique.
- Pour les flux, utilisez les sous-commandes `flowadm`. Tout d'abord, créez le flux en utilisant la sous-commande `flowadm add -flow`. Ensuite, affectez des ressources au flux en utilisant la sous-commande `flowadm set -flowprop`. L'ensemble des attributs définis qui caractérise les flux ensemble constitue la *stratégie de contrôle de flux* du système.

**Remarque** – Les propriétés pour l'allocation des ressources qui peuvent être affectées à un flux sont les mêmes que les propriétés qui sont directement affectées à une liaison. Actuellement toutefois, seules les propriétés de bande passante peuvent être associées avec des flux. Bien que les commandes pour définir les propriétés soient différentes pour les liaisons de données et pour les flux, la syntaxe est similaire. Pour configurer les propriétés de bande passante, reportez-vous aux exemples de la section “[Procédure de configuration d'un flux](#)” à la page 417.

Pour plus d'informations, reportez-vous à la page de manuel `flowadm(1M)`.

## Gestion des ressources réseau (liste des tâches)

Le tableau ci-dessous répertorie les différents modes d'établissement des contrôles de ressources et de détermination de la manière dont ces ressources sont allouées pour le traitement réseau.

Tâche	Description	Voir
Allocation d'anneaux à des clients MAC	Configure des clients MAC sur une liaison de données pour utiliser des anneaux.	<a href="#">“Propriétés pour l'allocation anneaux” à la page 398</a>
Attribution d'un pool de CPU à une liaison de données	Utilise la propriété <code>pool</code> pour allouer un ensemble de CPU afin de gérer les processus réseau d'une zone.	<a href="#">“Procédure de configuration d'un processeur d'un pool de CPU pour une liaison de données ” à la page 413</a>
Attribution d'un ensemble de CPU à une liaison de données	Sur un système qui a plusieurs CPU, réserve un ensemble de CPU pour la mise en réseau.	<a href="#">“Procédure d'allocation de CPU à des liaisons” à la page 415</a>
Implémentation de la gestion des ressources réseau à l'aide de flux sur un réseau physique	Isole le trafic réseau dans des flux individuels. Affecte ensuite aux flux une quantité définie de bande passante d'interface parmi d'autres flux.	<a href="#">“Procédure de configuration d'un flux” à la page 417</a>

# Gestion des ressources sur liaisons de données

Cette section décrit des propriétés de liaisons que vous pouvez définir pour améliorer les performances du réseau pour un réseau physique ou un réseau virtuel.

## Transmission et réception d'anneaux

Sur les cartes réseau, les anneaux de réception (Rx) et de transmission (Tx) sont des ressources matérielles à travers lesquelles le système reçoit et envoie des paquets réseau, respectivement. Les sections suivantes fournissent une présentation des anneaux suivie des procédures qui sont utilisées pour allouer des anneaux pour les processus de mise en réseau. Des exemples sont également fournis pour afficher le fonctionnement du mécanisme lorsque vous exécutez des commandes pour allouer des anneaux.

### Clients MAC et allocation d'anneaux

Les clients MAC, tels que des VNIC et autre liaisons de données, sont configurés sur la carte réseau pour activer la communication entre un système et d'autres nœuds du réseau. Une fois qu'un client est configuré, il utilise à la fois des anneaux Rx et Tx pour transmettre ou recevoir des paquets réseau respectivement. Un client MAC peut être basé sur le matériel ou le logiciel. Un client basé sur le matériel répond à une des conditions suivantes :

- Il a l'usage exclusif d'un ou de plusieurs anneaux Rx.
- Il a l'usage exclusif d'un ou de plusieurs anneaux Tx.
- Il a l'usage exclusif d'un ou de plusieurs anneaux Rx et d'un ou de plusieurs anneaux Tx.

Les clients qui ne remplissent pas une de ces conditions sont appelés clients MAC logiciels.

Les clients matériels peuvent avoir des anneaux attribués pour une utilisation exclusive en fonction de la carte réseau. Les cartes réseau comme `nxge` prennent en charge l'*allocation dynamique d'anneaux*. Sur ces cartes réseau, vous pouvez non seulement configurer des clients matériels, mais vous avez également la possibilité de déterminer le nombre d'anneaux à allouer à ces clients, en supposant que ces anneaux restent disponibles pour l'allocation. L'utilisation d'anneaux est toujours optimisée pour l'interface principale, par exemple, `nxge0`. L'interface principale est également appelée *client principal*. Tout anneau disponible n'ayant pas été affecté pour une utilisation exclusive par d'autres clients est automatiquement affecté à l'interface principale.

D'autres cartes réseau comme `ixge` ne prennent en charge que l'*allocation statique d'anneaux*. Sur ces cartes réseau, vous ne pouvez créer que des clients matériels. Les clients sont configurés automatiquement avec un jeu fixe d'anneaux par client. Le jeu fixe est déterminé au cours de la configuration initiale du pilote de la carte réseau. Pour plus d'informations sur la configuration initiale du pilote pour l'allocation statique, reportez-vous à la section [Manuel de référence des paramètres réglables Oracle Solaris](#).

## Allocation d'anneaux dans les réseaux locaux virtuels

Avec les réseaux locaux virtuels, l'allocation d'anneaux se déroule différemment selon la façon dont le réseau local virtuel est créé. Les réseaux locaux virtuels sont créés de l'une des deux façons suivantes :

- En utilisant la sous-commande `dladm create-vlan` :

```
# dladm create-vlan -l link -v VID vlan
```

- En utilisant la sous-commande `dladm create-vnic` :

```
# dladm create-vnic -l link -v VID vnic
```

Un réseau local virtuel qui est créé par la sous-commande `dladm create-vlan` a la même adresse MAC que l'interface sous-jacente. Par conséquent, ce réseau local virtuel partage aussi les anneaux Rx et Tx de l'interface sous-jacente. Un réseau local virtuel créé sous forme de VNIC avec la commande `dladm create-vnic` possède une adresse MAC différente de son interface sous-jacente. L'allocation d'anneaux d'un tel réseau local virtuel est indépendante de l'allocation pour la liaison sous-jacente. Par conséquent, ce réseau local virtuel peut se voir attribuer ses propres anneaux dédiés, en supposant que la carte réseau prend en charge les clients matériels.

## Propriétés pour l'allocation anneaux

Pour administrer les anneaux, deux propriétés d'anneau peuvent être définies avec la commande `dladm` :

- `rxrings` fait référence au nombre d'anneaux Rx affectés à une liaison spécifique.
- `txrings` fait référence au nombre d'anneaux Tx affectés à une liaison spécifique.

Vous pouvez définir chaque propriété sur l'une des trois valeurs possibles :

- `sw` indique que vous êtes en train de configurer un client logiciel. Le client n'a pas une utilisation exclusive des anneaux. Au contraire, le client partage les anneaux avec tous les autres clients existants configurés de la même manière.
- $n > 0$  (nombre supérieur à zéro) s'applique à la configuration d'un client matériel uniquement. Le nombre indique la quantité d'anneaux que vous allouez au client pour son usage exclusif. Vous pouvez spécifier un nombre uniquement si la carte réseau sous-jacente prend en charge l'allocation dynamique d'anneaux.
- `hw` s'applique également à la configuration d'un client matériel. Toutefois, pour ce type de client, vous ne pouvez pas spécifier le nombre réel d'anneaux dédiés. Au lieu de cela, le nombre fixe d'anneaux par client est déjà défini par rapport à la configuration initiale du pilote la carte réseau. Vous définissez les propriétés `*rings` sur `hw` si la carte réseau sous-jacente prend uniquement en charge l'allocation statique d'anneaux.

Pour fournir des informations sur les affectations et l'utilisation d'anneaux en cours, les propriétés d'anneau en lecture seule supplémentaires suivantes sont disponibles :

- `rxrings-available` et `txrings-available` indiquent le nombre d'anneaux Rx et Tx disponibles pour l'allocation.
- `rxhwclnt-available` et `txhwclnt-available` indiquent le nombre de clients matériels Rx et Tx qui peuvent être configurés sur une carte réseau.

## Préparatifs de configuration de clients matériels

Avant de configurer des clients matériels, vous devez connaître les capacités d'allocation d'anneaux de la carte réseau de votre système. Pour obtenir les informations requises, utilisez la commande suivante :

```
# dladm show-linkprop link
```

où *lien* fait référence à la liaison de données de votre carte réseau spécifique.

Pour afficher des propriétés spécifiques, utilisez la commande suivante :

```
# dladm show-linkprop -p property[,property,...] link
```

Pour configurer correctement les clients matériels, vous devez déterminer les éléments suivants :

- Si la carte réseau prend en charge les clients matériels  
Les propriétés `rxrings` et `txrings` dans la sortie de la commande indique si une carte réseau prend en charge les clients matériels. A partir des mêmes données, vous pouvez également déterminer le type d'allocation d'anneaux qui est pris en charge par la carte d'interface réseau.
- La disponibilité d'anneaux à allouer aux clients matériels  
Les propriétés `rxrings-available` et `txrings-available` dans la sortie de la commande indique les anneaux Rx et Tx disponibles que vous pouvez allouer à un client matériel.
- La disponibilité des clients matériels que vous pouvez configurer sur la liaison  
Les anneaux sont alloués sous forme d'ensembles. Aucune correspondance bi-univoque n'existe entre le nombre d'anneaux disponibles et le nombre de clients qui peuvent utiliser des anneaux dédiés. Par conséquent, pour allouer des anneaux, vous devez non seulement vérifier la disponibilité d'anneaux mais également le nombre de clients matériels supplémentaires que vous pouvez toujours configurer pour utiliser des anneaux dédiés. Vous pouvez allouer des anneaux uniquement si des anneaux et des clients matériels sont disponibles.  
Les propriétés `rxhwclnt-available` et `txhwclnt-available` dans la sortie de la commande indiquent le nombre de clients matériels, que vous pouvez configurer, pouvant utiliser des anneaux Rx et Tx.

Si la carte d'interface réseau prend en charge l'allocation d'anneaux, et que des anneaux et des clients matériels sont disponibles, vous pouvez configurer ce type de client sur le système,

comme expliqué dans la section “[Procédure de configuration d'un client matériel](#)” à la page 402. Sinon, vous pouvez configurer un client logiciel, comme expliqué dans la section “[Procédure de création d'un client le logiciel](#)” à la page 403.

Les exemples suivants présentent des informations différentes qui s'affichent pour des propriétés de liaison liées aux anneaux d'une NIC nxge, une NIC ixgbe et une NIC e1000g.

**EXEMPLE 21-1** Informations d'anneaux de NIC nxge

L'exemple suivant montre des informations d'anneau pour une NIC nxge.

#	dladm	show-linkprop	nxge0				
LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE		
...							
nxge0	rxrings	rw	--	--	sw,<1-7>		
...							
nxge0	txrings	rw	--	--	sw,<1-7>		
...							
nxge0	rxrings-available	r-	5	--	--		
nxge0	txrings-available	r-	5	--	--		
nxge0	rxhwcCnt-available	r-	2	--	--		
nxge0	txhwcCnt-available	r-	2	--	--		
...							

Le champ POSSIBLE répertorie sw et <1-7> comme valeurs acceptables pour les propriétés rxrings et txrings. Ces valeurs indiquent que nxge prend en charge les clients matériels ainsi que les clients logiciels. L'intervalle <1-7> indique que le nombre d'anneaux Rx ou Tx que vous définissez doit être compris dans la plage indiquée. Vous pouvez également déduire de la plage que la NIC prend en charge l'allocation d'anneaux dynamique pour les côtés réception et transmission.

En outre, les propriétés \*rings-available indiquent que cinq anneaux Rx et cinq anneaux Tx sont disponibles pour l'allocation de clients matériels.

Cependant, en fonction des propriétés \*Cnt-available, vous pouvez configurer uniquement deux clients qui peuvent avoir l'exclusivité de l'utilisation d'anneaux Rx disponibles. De même, vous pouvez configurer uniquement deux clients qui peuvent avoir l'exclusivité de l'utilisation d'anneaux Tx disponibles.

**EXEMPLE 21-2** Informations d'anneaux de NIC ixgbe

L'exemple suivant montre des informations d'anneau pour une NIC ixgbe.

#	dladm	show-linkprop	ixgbe0				
LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE		
...							
ixgbe0	rxrings	rw	--	--	sw,hw		
...							
ixgbe0	txrings	rw	--	--	sw,hw,<1-7>		
...							
ixgbe0	rxrings-available	r-	0	--	--		
ixgbe0	txrings-available	r-	5	--	--		



EXEMPLE 21-2 Informations d'anneaux de NIC ixgbe (Suite)

```
ixgbe0 rxhwclnt-available r- 0 -- --
ixgbe0 txhwclnt-available r- 7 -- --
...
```

Le champ POSSIBLE pour les propriétés rxrings et txrings indique que les clients matériels et logiciels peuvent être configurés sur ixgbe0. Seule l'allocation d'anneaux statique est prise en charge pour les anneaux Rx, où le matériel affecte un jeu fixe d'anneaux Rx à chaque client matériel. Cependant, vous pouvez allouer des anneaux Tx dynamiquement, ce qui signifie que vous pouvez déterminer le nombre d'anneaux Tx à assigner à un client matériel, dans cet exemple, jusqu'à 7 anneaux.

En outre, les propriétés \*rings-available indiquent que cinq anneaux Tx sont disponibles pour être alloués à des clients matériels, mais aucun anneau Rx ne peut être assigné.

Enfin, en se basant sur les propriétés \*hwclnt-available, vous pouvez configurer sept clients Tx matériel pour qu'ils utilisent exclusivement des anneaux Tx. Cependant, l'allocation dynamique d'anneaux Rx n'est pas prise en charge dans des cartes ixgbe. Par conséquent, vous ne pouvez pas créer un client matériel avec un ensemble défini d'anneaux Rx dédiés.

Un zéro (0) sous le champ VALUE pour les propriétés \*rings-available peut signifier une des deux choses suivantes :

- Aucun anneau n'est disponible pour être alloué aux clients.
- L'allocation d'anneau dynamique n'est pas prise en charge.

Vous pouvez vérifier la signification du zéro en comparant le champ POSSIBLE pour rxrings et txrings et le champ VALUE pour rxrings-available et txrings-available.

Par exemple, supposons que txrings-available soit 0, comme suit :

```
# dladm show-linkprop ixgbe0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings          rw    --    --        sw,hw
ixgbe0    txrings          rw    --    --        sw,hw,<1-7>
ixgbe0    rxrings-available r-    0     --        --
ixgbe0    txrings-available r-    0     --        --
...
```

Dans cette sortie, le champ VALUE pour rxrings-available est 0 alors que le champ POSSIBLE pour rxrings est sw, hw. Les informations combinées signifient qu'aucun anneau Rx n'est disponible car la carte d'interface réseau ne prend pas en charge l'allocation dynamique d'anneaux. Côté transmission, le champ VALUE pour txrings-available est 0 alors que le champ POSSIBLE pour txrings est sw, hw, <1-7>. Les informations fusionnées indiquent qu'aucun anneau Tx n'est disponible car ils sont déjà tous affectés. Cependant, comme le champ POSSIBLE pour txrings l'indique, l'allocation dynamique d'anneaux est prise en charge. Par conséquent, vous pouvez allouer des anneaux Tx quand ils deviennent disponibles.

EXEMPLE 21-3 Informations d'anneaux de NIC e1000g

L'exemple suivant montre des informations d'anneau pour une NIC e1000g.

```
# dladm show-linkprop e1000g0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
e1000g0   rxrings        rw    --     --       --
...
e1000g0   txrings        rw    --     --       --
...
e1000g0   rxrings-available  r-    0      --       --
e1000g0   txrings-available  r-    0      --       --
e1000g0   rxhwcInt-available r-    0      --       --
e1000g0   txhwcInt-available r-    0      --       --
...
```

Le résultat indique que ni les anneaux ni les clients matériels ne peuvent être configurés car l'allocation d'anneaux n'est pas prise en charge dans les cartes d'interface réseau e1000g.

▼ Procédure de configuration d'un client matériel

Cette procédure indique comment configurer un client matériel sur une carte d'interface réseau qui prend en charge l'allocation dynamique d'anneaux ou sur une carte d'interface réseau qui prend en charge l'allocation d'anneaux statique.

Avant de commencer

Assurez-vous que vous avez obtenu les informations suivantes sur la carte d'interface réseau sur votre système :

- Si la carte réseau prend en charge les clients matériels
- Le type d'allocation d'anneaux que la carte d'interface réseau prend en charge
- La disponibilité d'anneaux à allouer aux clients matériels
- La disponibilité des clients matériels que vous pouvez configurer sur la liaison

Pour obtenir des informations, reportez-vous à la section “[Préparatifs de configuration de clients matériels](#)” à la page 399.

1 Effectuez l'une des actions suivantes en fonction du type d'allocation d'anneaux que votre carte d'interface réseau prend en charge :

- Si la carte d'interface réseau prend en charge l'allocation dynamique d'anneaux, utilisez la syntaxe suivante :

```
# dladm create-vnic -p rxrings=number[,txrings=number] -l link vnic
number
```

Fait référence au nombre d'anneaux Rx et Tx que vous allouez au client. Le nombre ne doit pas dépasser le nombre d'anneaux disponibles à l'allocation.

---

**Remarque** – Certaines cartes d'interface réseau prennent en charge l'allocation dynamique d'anneaux Rx ou Tx, mais pas les deux types. Spécifiez *number* sur le type d'anneau pour lequel l'allocation dynamique d'anneaux est prise en charge.

---

*link*      Fait référence à la liaison de données sur lequel vous créez le client.

*vnic*      Fait référence au client que vous configurez.

- Si la carte d'interface réseau prend en charge l'allocation statique d'anneaux, utilisez la syntaxe suivante :

```
# dladm create-vnic -p rxrings=hw[,txrings=hw] -l link vnic
```

---

**Remarque** – Certaines cartes d'interface réseau prennent en charge l'allocation statique d'anneaux Rx ou Tx, mais pas les deux types. Spécifiez *hw* sur le type d'anneau pour lequel l'allocation statique d'anneaux est prise en charge.

---

## 2 (Facultatif) Vérifiez les informations d'anneau du client qui vient d'être créé.

```
# dladm show-linkprop vnic
```

## ▼ Procédure de création d'un client logiciel

Un client logiciel n'a pas l'usage exclusif d'anneaux. Au lieu de cela, le client partage l'utilisation d'anneaux avec le client principal ou l'interface avec d'autres clients logiciels existants. Le nombre d'anneaux pour les clients logiciels dépend du nombre de clients matériels existants.

### ● Effectuez l'une des étapes suivantes :

- Pour créer un client logiciel, tapez la commande suivante :

```
# dladm create-vnic -p rxrings=sw[,txrings=sw] -l link vnic
```

*link*      Fait référence à la liaison de données sur lequel vous créez le client.

*vnic*      Fait référence au client que vous configurez.

- Pour configurer un client existant afin de partager des anneaux avec d'autres clients, tapez la commande suivante :

```
# dladm set-linkprop -p rxrings=sw[,txrings=sw] vnic
```

## Exemple 21–4 Configuration de clients matériels et de clients logiciels

Cet exemple montre comment configurer les clients matériels et les clients logiciels sur un système avec une carte d'interface réseau ixgbe. Pour montrer comment l'allocation d'anneaux

est implémentée, l'exemple est divisé en parties. Les informations liées aux anneaux s'affichent et sont expliquées à chaque étape du processus de configuration. La configuration se déroule comme suit :

1. Affichez les liaisons et l'utilisation d'anneaux sur le système avant de procéder à la configuration de clients.
2. Configurez le client principal.
3. Configurez un client logiciel.
4. Configurer un autre client sans anneaux dédiés.
5. Allouez statiquement des anneaux au client qui vient d'être configuré.
6. Configurez un troisième client avec des anneaux dédiés qui sont alloués dynamiquement.

Tout d'abord, affichez les liaisons, l'utilisation d'anneau et les propriétés liées aux anneaux.

```
# dladm show-link
LINK      CLASS  MTU    STATE  BRIDGE  OVER
ixgbe0    phys    1500   down   --       --

# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS  CLIENTS
ixgbe0    RX        0-1    <default,mcast>
ixgbe0    TX        0-7    <default>
ixgbe0    RX        2-3    --
ixgbe0    RX        4-5    --
ixgbe0    RX        6-7    --

# dladm show-linkprop ixgbe0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings          rw    --    --       sw,hw
ixgbe0    rxrings-effective r    --    --       --
ixgbe0    txrings          rw    --    --       sw,hw,<1-7>
ixgbe0    txrings-effective r    --    --       --
ixgbe0    txrings-available r-    7     --       --
ixgbe0    rxrings-available r-    0     --       --
ixgbe0    rxhwclnt-available r-    3     --       --
ixgbe0    txhwclnt-available r-    7     --       --
...
```

La sortie de la commande montre une liaison ixgbe0 unique sur le système, mais pas de clients existants. En outre, les informations suivantes sont également tirées de cette sortie :

- La carte d'interface réseau a huit anneaux Rx et huit anneaux Tx (anneaux 0 à 7).
- Pour les clients matériels, seule l'allocation statique d'anneaux est prise en charge pour les anneaux Rx, alors que les allocations d'anneaux statiques et dynamiques sont prises en charge pour les anneaux Tx.
- Les clients logiciels peuvent être configurés pour les anneaux Rx et Tx.

- Sept anneaux Tx, 1 de 7, sont disponibles pour être alloués dynamiquement à d'autres clients (l'anneau 0 est généralement réservé au client principal). Aucun anneau Rx n'est disponible car l'allocation dynamique d'anneaux n'est pas prise en charge pour les anneaux Rx.
- Trois clients matériels peuvent être configurés pour utiliser des anneaux Rx, tandis que sept clients matériels peuvent être configurés pour utiliser des anneaux Tx.

Pour obtenir une explication des propriétés `*rings-effective`, reportez-vous à la section [“Procédure d'identification des affectations d'anneaux dans l'allocation d'anneaux statique”](#) à la page 409.

Ensuite, configurez le client principal.

```
# ipadm create-ip ixgbe0
# ipadm create-addr -T static -a 192.168.10.10/24 ixgbe0/v4
# dladm show-phys -H ixgbe0
```

LINK	RINGTYPE	RINGS	CLIENTS
ixgbe0	RX	0-1	<default,mcast>
ixgbe0	TX	0-7	<default>ixgbe0
ixgbe0	RX	2-3	ixgbe0
ixgbe0	RX	4-5	--
ixgbe0	RX	6-7	--

```
# dladm show-linkprop ixgbe0
```

LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
...					
ixgbe0	rxrings	rw	--	--	sw,hw
ixgbe0	rxrings-effective	r	2	--	--
ixgbe0	txrings	rw	--	--	sw,hw,<1-7>
ixgbe0	txrings-effective	r	8	--	--
ixgbe0	txrings-available	r-	7	--	--
ixgbe0	rxrings-available	r-	0	--	--
ixgbe0	rxhwclnt-available	r-	3	--	--
ixgbe0	txhwclnt-available	r-	7	--	--
...					

La sortie fournit les informations suivantes :

- `ixgbe0`, le client principal, reçoit automatiquement deux anneaux Rx (anneaux 2 et 3) pour un usage dédié. Cependant, `ixgbe0` utilise tous les anneaux Tx. Par défaut, tous les anneaux inutilisés sont automatiquement affectés au client principal.
- Le nombre d'anneaux Tx disponibles qui peuvent être affectés à d'autres clients reste de sept.
- Le nombre de clients matériels disponibles qui peuvent être configurés avec des anneaux Rx reste de trois. Le nombre de clients matériels disponibles qui peuvent être configurés dynamiquement avec des anneaux Tx reste de sept.

Ensuite, créez une VNIC sous forme de client logiciel.

```
# dladm create-vnic -l ixgbe0 -p rxrings=sw,txrings=sw vnic0
# dladm show-phys -H ixgbe0
```

```

LINK      RINGTYPE  RINGS  CLIENTS
ixgbe0    RX        0-1    <default,mcast>,vnic0
ixgbe0    TX        0-7    <default>vnic0,ixgbe0
ixgbe0    RX        2-3    ixgbe0
ixgbe0    RX        4-5    --
ixgbe0    RX        6-7    --

# dladm show-linkprop vnic0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
vnic0     rxrings           rw    sw     --       sw,hw
...
vnic0     txrings           rw    sw     --       sw,hw,<1-7>
...

# dladm show-linkprop ixgbe0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings           rw    --     --       --
ixgbe0    rxrings-effective r     2      --     --
ixgbe0    txrings           rw    --     --       sw,hw,<1-7>
ixgbe0    txrings-effective r     --     --     --
ixgbe0    txrings-available r-    7      --     --
ixgbe0    rxrings-available r-    0      --     --
ixgbe0    rxhwclnt-available r-    3      --     --
ixgbe0    txhwclnt-available r-    7      --     --
...

```

La sortie fournit les informations suivantes :

- Sous forme d'un client logiciel, `vnic0` est automatiquement affectée pour utiliser les anneaux Rx 0 et 1. Les autres clients logiciels avec des anneaux Rx qui sont créés par la suite seront affectés pour utiliser cette paire par défaut. Par défaut, `vnic0` se voit également affectée l'utilisation des huit anneaux Tx (anneaux 0 de 7). Les autres clients logiciels avec des anneaux Tx qui sont créés par la suite seront affectés pour utiliser cet ensemble d'anneaux par défaut.
- En tant que client logiciel, les propriétés `rxrings` et `txrings` de `vnic0` sont définies en fonction de `sw`.
- Aucun anneau Tx n'est affecté. Par conséquent, le nombre d'anneaux Tx disponibles pouvant être affectés à d'autres clients reste de sept.
- Le nombre de clients matériels disponibles pouvant être configurés avec des anneaux Rx reste de trois. Le nombre de clients matériels disponibles pouvant être configurés avec des anneaux Tx reste de sept.

Ensuite, configurez un autre client sans allocation d'anneaux.

```

# dladm create-vnic -l ixgbe0 vnic1
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS  CLIENTS
ixgbe0    RX        0-1    <default,mcast>,vnic0
ixgbe0    TX        0,2-7  <default>vnic0,ixgbe0
ixgbe0    RX        2-3    ixgbe0
ixgbe0    RX        4-5    vnic1

```

```

ixgbe0  RX      6-7    --
ixgbe0  TX      1      vnic1

# dladm show-linkprop vnic1
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
vnic1     rxrings         rw    --    --        sw, hw
vnic1     rxrings-effective r-    2      --        --
vnic1     txrings         rw    --    --        sw, hw, <1-7>
vnic1     txrings-effective r-    --    --        --
...

# dladm show-linkprop ixgbe0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0     rxrings         rw    --    --        sw, hw
ixgbe0     rxrings-effective r-    2      --        --
ixgbe0     txrings         rw    --    --        sw, hw, <1-7>
ixgbe0     txrings-effective r-    --    --        --
ixgbe0     txrings-available r-    7      --        --
ixgbe0     rxrings-available r-    0      --        --
ixgbe0     rxhwcInt-available r-    3      --        --
ixgbe0     txhwcInt-available r-    7      --        --
...

```

La sortie fournit les informations suivantes :

- Quand l'allocation d'anneaux est prise en charge, un client qui est configuré est considéré comme un client matériel, même si les propriétés `rxrings` et `txrings` ne sont pas définies. Par conséquent, `vnic1` reçoit automatiquement deux anneaux Rx dédiés (anneaux 4 et 5) pour son usage. De la même manière, `vnic1` reçoit également un anneau Tx dédié (anneau 1).
- Des huit anneaux Tx, `ixgbe0` et `vnic0` partagent désormais sept anneaux (anneau 0 et anneaux 2 à 7). Anneau 1 est devenu un anneau Tx dédié pour `vnic1`.
- Aucun anneau Tx n'est affecté. Par conséquent, le nombre d'anneaux Tx disponibles pouvant être affectés à d'autres clients reste de sept.
- Le nombre de clients matériels disponibles pouvant être configurés avec des anneaux Rx reste de trois. Le nombre de clients matériels disponibles pouvant être configurés avec des anneaux Tx reste de sept.

Allouez ensuite statiquement des anneaux au client `vnic1` qui vient d'être configuré.

```

# dladm set-linkprop -p rxrings=hw,txrings=hw vnic1
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS      CLIENTS
ixgbe0    RX        0-1        <default,mcast>,vnic0
ixgbe0    TX        0,2-7      <default>vnic0,ixgbe0
ixgbe0    RX        2-3        ixgbe0
ixgbe0    RX        4-5        vnic1
ixgbe0    RX        6-7        --
ixgbe0    TX        1          vnic1

```

```
# dladm show-linkprop vnic1
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
vnic1     rxrings           rw    hw     --       sw, hw
vnic1     rxrings-effective r-    2      --       --
vnic1     txrings           rw    hw     --       sw, hw, <1-7>
vnic1     txrings-effective r-    --     --       --
...
# dladm show-linkprop ixgbe0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings           rw    --     --       sw, hw
ixgbe0    rxrings-effective r-    2      --       --
ixgbe0    txrings           rw    --     --       sw, hw, <1-7>
ixgbe0    txrings-effective r-    --     --       --
ixgbe0    txrings-available r-    6      --       --
ixgbe0    rxrings-available r-    0      --       --
ixgbe0    rxhwcInt-available r-    3      --       --
ixgbe0    txhwcInt-available r-    6      --       --
...
```

La sortie fournit les informations suivantes :

- La distribution d'anneaux Rx et Tx pour vnic1 reste la même que lorsque vnic1 a été créée sans allocation d'anneaux.
- De la même façon, les informations d'anneau reste les mêmes que lorsque vnic1 a été créée sans allocation d'anneaux.
- Les propriétés rxrings et txrings de vnic1 ont été explicitement définies sur hw. Par conséquent, le nombre d'anneaux Tx disponibles pour une allocation dynamique a été réduit à six. De même, le nombre de clients matériels disponibles pouvant être configuré a été réduit à six.

Ensuite, configurez un client matériel avec des anneaux Tx qui sont alloués dynamiquement.

```
# dladm create-vnic -l ixgbe0 -p txrings=2 vnic2
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS  CLIENTS
ixgbe0    RX        0-1    <default,mcast>,vnic0
ixgbe0    TX        0,4-7  <default>vnic0,ixgbe0
ixgbe0    RX        2-3    ixgbe0
ixgbe0    RX        4-5    vnic1
ixgbe0    RX        6-7    vnic2
ixgbe0    TX        1      vnic1
ixgbe0    TX        2-3    vnic2

# dladm show-linkprop vnic2
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
vnic2     rxrings           rw    --     --       sw, hw
vnic2     rxrings-effective r-    2      --       --
vnic2     txrings           rw    2      --       sw, hw, <1-7>
vnic2     txrings-effective r-    2      --       --
...
# dladm show-linkprop ixgbe0
```



LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
...					
ixgbe0	rxrings	rw	--	--	sw, hw
ixgbe0	rxrings-effective	r-	2	--	--
ixgbe0	txrings	rw	--	--	sw, hw, <1-7>
ixgbe0	txrings-effective	r-	--	--	--
ixgbe0	txrings-available	r-	4	--	--
ixgbe0	rxrings-available	r-	0	--	--
ixgbe0	rxhwcInt-available	r-	3	--	--
ixgbe0	txhwcInt-available	r-	5	--	--
...					

La sortie fournit les informations suivantes :

- Le matériel automatiquement affecté à une paire d'anneau Rx (anneaux 6 et 7) pour `vnic2` pour un usage exclusif. Cependant, les deux anneaux Tx dédiés de `vnic2` (anneaux 2 et 3) ont été attribués par l'administrateur.
- Avec deux anneaux Tx administrativement affectés à `vnic2`, le nombre d'anneaux Tx disponibles pouvant être affectés à d'autres clients a été réduit à quatre.
- Avec `vnic2` configuré comme un client matériel avec deux anneaux Tx, le nombre de clients disponibles pouvant être configurés a été réduit à cinq.

## ▼ Procédure d'identification des affectations d'anneaux dans l'allocation d'anneaux statique

Lorsque vous configurez un client matériel avec l'allocation statique d'anneaux, le matériel détermine le nombre d'anneaux à affecter. Toutefois, les propriétés `rxrings` et `txrings` sont définies sur `hw` et n'indiquent pas le nombre d'anneaux qui sont réellement affectés. Au lieu de cela, le numéro peut être obtenu en vérifiant les propriétés `rxrings-effective` et `txrings-effectif`.

### 1 Configurez un client matériel avec l'allocation statique d'anneaux en procédant de l'une des manières suivantes :

- Pour créer le client avec l'allocation statique d'anneaux, tapez la commande suivante :

```
# dladm create-vnic -l link -p rxrings=hw[,txrings=hw] vnic
```

*link*      Fait référence à la liaison de données sur lequel vous créez le client.

*vnic*      Fait référence au client que vous configurez.

- Pour allouer statiquement des anneaux à un client existant, tapez la commande suivante :

```
# dladm set-linkprop -p rxrings=hw[,txrings=hw] vnic
```

### 2 Pour identifier le nombre d'anneaux qui ont été alloués, effectuez les étapes suivantes :

#### a. Affichez les propriétés du client.

```
# dladm show-linkprop link
```

où *link* fait référence au client basé ou à la VNIC.

**b. Vérifiez la valeur de la propriété *\*rings-effective* qui correspond au type d'anneau que vous avez alloué statiquement.**

Si, par exemple, vous avez alloué statiquement des anneaux Rx, vérifiez la propriété *rxrings-effective*. Si vous avez alloué statiquement des anneaux Tx, vérifiez la propriété *txrings-effective*. Le nombre indique combien d'anneaux ont été alloués par le matériel.

**3 Pour vérifier quels anneaux ont été alloués statiquement, effectuez les sous-étapes suivantes :**

**a. Affichez l'utilisation d'anneaux de la carte d'interface réseau.**

```
# dladm show-phys -H link
```

où *link* fait référence au client principal.

**b. Dans la sortie de la commande, vérifiez que les anneaux Rx ou Tx ont été affectés au client matériel que vous avez configuré dans la première étape.**

### Exemple 21–5 Identification d'anneaux qui sont alloués statiquement

Cet exemple montre comment des anneaux Rx ont été alloués statiquement à un client qui est configuré sur une carte d'interface réseau *ixgbe*. Sur de telles cartes d'interface réseau, seule l'allocation statique est prise en charge pour les anneaux Rx. L'exemple se déroule comme suit :

1. Affichez les liaisons sur le système. Dans cet exemple, le système ne dispose que d'une liaison, qui est *ixgbe0*.
2. Créez *vnicl* comme client matériel avec des anneaux Rx qui sont alloués statiquement.
3. Affichez les informations d'anneau afin de connaître le nombre d'anneaux alloués par le matériel.
4. Afficher l'utilisation des anneaux pour identifier les anneaux qui ont été alloués.

```
# dladm show-link
LINK      CLASS  MTU    STATE   BRIDGE  OVER
ixgbe0    phys   1500   down    --       --

# dladm create-vnic -l ixgbe0 -p rxrings=hw vnic1
# dladm show-linkprop vnic1
LINK      PROPERTY              PERM  VALUE  DEFAULT  POSSIBLE
...
vnicl     rxrings                rw     hw     --       sw, hw
vnicl     rxrings-effective      r-     2      --       --
vnicl     txrings                rw     --     --       sw, hw, <1-7>
vnicl     txrings-effective      r-     --     --       --

# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS  CLIENTS
ixgbe0    RX         0-1    <default,mcast>
```

```

ixgbe0 TX      0,2-7    <default>
ixgbe0 RX      2-3     vnic1
ixgbe0 RX      4-5     --
ixgbe0 RX      6-7     --
ixgbe0 TX      1       vnic1
...

```

La sortie indique qu'après que vnic1 a été configurée avec des anneaux Rx, le matériel a alloué deux anneaux Rx dédiés, comme en témoigne la propriété `rxrings-effective`. En fonction de la sortie de la commande **dladm show-phys -H**, les anneaux Rx 2 et 3 ont été dédiés à l'usage de vnic1.

Comme il est configuré en tant que client, vnic1 reçoit également automatiquement l'anneau Tx 1 pour son usage exclusif. Toutefois, la propriété `txrings-effective` n'affiche aucune valeur car la propriété `txrings` n'est pas définie de façon explicite.

## Pools et CPU

Le *pool* est une propriété de liaison qui permet de lier le traitement réseau à un pool de CPU. Avec cette propriété, vous pouvez mieux intégrer la gestion des ressources réseau par la liaison CPU et l'administration dans des zones. Dans Oracle Solaris, l'administration de zones comprend la liaison de processus sans mise en réseau à un pool de ressources CPU à l'aide de la commande `zonecfg` ou `poolcfg`. Pour lier le même pool de ressources à la gestion de processus de réseau, vous pouvez utiliser la commande `dladm set-linkprop` pour configurer une propriété `pool` d'une liaison. Ensuite, assignez cette liaison à la zone.

En définissant la propriété `pool` d'une liaison et l'affectation de la liaison comme zone de l'interface réseau, alors cette liaison est également liée à un pool de zone. Si cette zone est définie pour devenir une zone exclusive, les ressources CPU dans le pool ne peuvent plus être utilisées par d'autres liaisons de données qui ne sont pas affectées à cette zone.

---

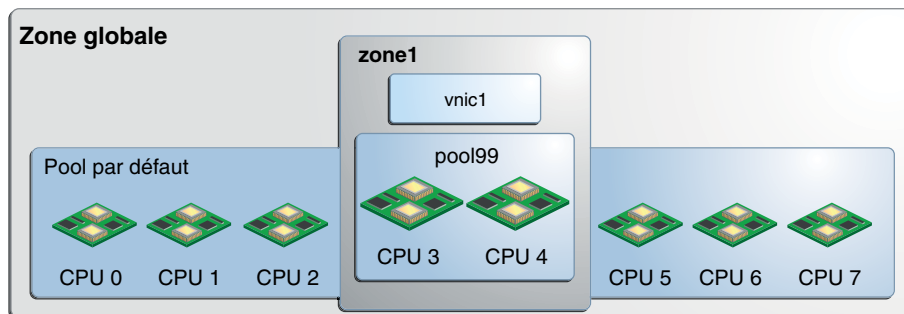
**Remarque** – Une propriété distincte, `cpu`, peut être définie pour affecter des CPU spécifiques à une liaison de données. Les deux propriétés, `cpu` et `pool`, s'excluent mutuellement. Vous ne pouvez pas définir les deux propriétés pour une liaison de données. Pour affecter des ressources à une liaison de données à l'aide de la propriété `cpu`, reportez-vous à la section [“Procédure d'allocation de CPU à des liaisons”](#) à la page 415.

---

Pour plus d'informations sur les pools au sein d'une zone, reportez-vous au [Chapitre 13, “Création et administration des pools de ressources \(tâches\)”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*. Pour plus d'informations sur la création de pools et l'affectation d'ensembles de CPU aux pools, reportez-vous à la page de manuel [poolcfg\(1M\)](#).

La figure suivante montre le fonctionnement des pools quand la propriété `pool` est affectée à une liaison de données.

FIGURE 21-1 Propriété `pool` d'une VNIC affectée à une zone

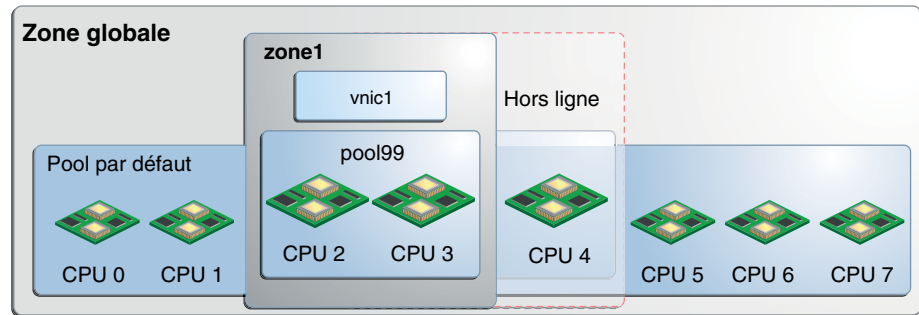


Dans la figure, le système dispose de huit CPU. Quand aucun pool n'est configuré sur le système, toutes les CPU appartiennent au *pool par défaut* et sont utilisées par la zone globale. Toutefois, dans cet exemple, le pool `pool99` a été créé et se compose des CPU 3 et CPU 4. Ce groupe est associé à la zone1, qui est une zone exclusive. Si `pool99` est défini comme une propriété de `vnic1`, `pool99` devient dédié pour également gérer les processus réseau de `vnic1`. Une fois que `vnic1` est affectée à l'interface réseau de la zone1, les CPU de `pool99` deviennent réservées pour gérer les traitements réseau et non-réseau de la zone1.

La propriété `pool` est de nature dynamique. Les pools de zone peuvent être configurés à l'aide d'une gamme de CPU, et le noyau détermine les CPU qui sont affectées à l'ensemble de CPU du pool. Les modifications apportées au pool sont automatiquement mises en place pour la liaison de données, ce qui simplifie l'administration du pool de cette liaison. En revanche, l'affectation de CPU spécifique à la liaison à l'aide de la propriété `cpu` exige que vous spécifiez la CPU à affecter. Vous devez définir la propriété `cpu` chaque fois que vous souhaitez modifier les composants de CPU du pool.

Par exemple, supposons que dans le système de la [Figure 21-1](#), CPU 4 est mis hors ligne. Dans la mesure où la propriété `pool` est dynamique, le logiciel associe automatiquement une autre CPU au pool. Par conséquent la configuration d'origine du pool de deux CPU est préservée. Pour `vnic1`, la modification est transparente. La configuration ajustée est illustrée dans la figure ci-après.

FIGURE 21-2 Reconfiguration automatique de la propriété pool



Les propriétés liées au pool supplémentaires donnent des informations sur l'utilisation d'une CPU ou d'un pool de CPU d'une liaison de données. Ces propriétés sont en lecture seule et ne peuvent pas être définies par l'administrateur.

- `pool-effective` affiche le pool en cours d'utilisation par les processus réseau.
- `cpus-effective` affiche la liste des CPU en cours d'utilisation par les processus réseau.

Pour gérer les ressources CPU d'une zone, la définition de la propriété `pool` d'une liaison de données n'est pas normalement exécutée en tant qu'étape initiale. Plus fréquemment, les commandes comme `zoncfg` et `poolcfg` sont utilisées pour configurer une zone afin d'utiliser un pool de ressources. Les propriétés de liaison `cpu` et `pool` elles-mêmes ne sont pas définies. Dans de tels cas, les propriétés `pool-effective` ainsi que `cpus-effective` de ces liaisons de données sont automatiquement définies en fonction de ces configurations de zone lorsque la zone est initialisée. Le pool par défaut est affiché sous `pool-effective`, tandis que la valeur de `cpus-effective` est sélectionnée par le système. Par conséquent, si vous utilisez la commande `dladm show-linkprop`, les propriétés `pool` et `cpu` seront vides, alors que les propriétés `pool-effective` et `cpus-effective` contiendront des valeurs.

La définition directe des propriétés `pool` et `cpu` d'une liaison de données est une étape alternative que vous pouvez utiliser pour lier le pool de CPU d'une zone pour les processus réseau. Une fois que vous avez configuré ces propriétés, leurs valeurs sont aussi reflétées dans les propriétés `pool-effective` et `cpus-effective`. Notez, cependant, que cette étape alternative est généralement moins utilisée pour gérer les ressources réseau d'une zone.

## ▼ Procédure de configuration d'un processeur d'un pool de CPU pour une liaison de données

Comme avec d'autres propriétés de liaison, la propriété `pool` peut être définie pour une liaison de données au moment où cette liaison est créée ou plus tard, quand elle requiert une configuration. Par exemple :

```
# dladm create-vnic -p pool=pool-name -l link vnic
```

Définit la propriété `pool` pendant que vous créez la VNIC. Pour définir la propriété `pool` d'une VNIC, utilisez la syntaxe suivante :

```
# dladm setlinkprop -p pool=pool-name vnic
```

La procédure ci-dessous présente les étapes de configuration d'un pool de CPU pour une VNIC.

**Avant de commencer**

Vous devez avoir effectué les opérations suivantes :

- Création d'un ensemble de processeurs avec son nombre de CPU affectés.
- Création d'un pool auquel l'ensemble de processeurs sera associé.
- Association du pool à l'ensemble de processeurs.

---

**Remarque** – Pour les instructions sur la réalisation de ces conditions préalables, reportez-vous à la section “[Modification d’une configuration](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*

---

**1 Définissez la propriété `pool` de la liaison sur le pool de CPU que vous avez créé pour la zone. Effectuez l'une des étapes ci-dessous en fonction de l'existence de la VNIC.**

- Si la VNIC n'a pas encore été créée, utilisez la syntaxe suivante :

```
# dladm create-vnic -l link -p pool=pool vnic
```

où *pool* fait référence au nom du pool créé pour la zone.

- Si la VNIC existe, utilisez la syntaxe suivante :

```
# dladm setlinkprop -p pool=pool vnic
```

**2 Définissez une zone pour utiliser la VNIC.**

```
zonecfg>zoneid:net> set physical=vnic
```

---

**Remarque** – Pour connaître toutes les étapes qui expliquent l'affectation d'une interface réseau à une zone, reportez-vous à la section “[Configuration, vérification et validation d'une zone](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

---

**Exemple 21–6 Affectation du pool de CPU d'une liaison à une zone avec un type d'IP exclusif**

Cet exemple montre comment un pool est affecté à une liaison de données d'une zone. Le scénario est basé sur la configuration de la [Figure 21–1](#). L'exemple part du principe qu'un pool

de CPU nommé `pool99` a déjà été configuré pour la zone. Le pool est alors affecté à une VNIC. Enfin, la zone non globale `zone1` est définie de manière à utiliser la VNIC comme interface réseau.

```
# dladm create-vnic -l e1000g0 -p pool99 vnic0

# zonecfg -c zone1
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> add net
zonecfg:zone1>net> set physical=vnic0
zonecfg:zone1>net> end
zonecfg:zone1> exit
```

## ▼ Procédure d'allocation de CPU à des liaisons

La procédure suivante explique comment affecter des CPU pour traiter le trafic traversant une liaison de données en configurant la propriété `cpu`.

### 1 Vérifiez les affectations de CPU pour l'interface.

```
# dladm show-linkprop -p cpus link
```

Par défaut, aucune CPU n'est affectée à une interface spécifique. Par conséquent, le paramètre `VALUE` dans la sortie de la commande ne contient aucune entrée.

### 2 Répertoriez les interruptions et les CPU avec lesquelles les interruptions sont associées.

```
# echo ::interrupts | mdb -k
```

La sortie affiche les paramètres de chaque liaison dans le système, y compris le nombre de CPU.

### 3 Affectez des CPU à la liaison.

Les CPU peuvent inclure celles avec lesquelles les interruptions de la liaison sont associées.

```
# dladm set-linkprop -p cpus=cpu1,cpu2,... link
```

où `cpu1` est le nombre de CPU à affecter à cette liaison. Vous pouvez affecter plusieurs CPU à la liaison.

### 4 Vérifiez l'interruption de liaison pour vérifiez les nouvelles affectations de CPU.

```
# echo ::interrupts | mdb -k
```

### 5 (Facultatif) Affichez les CPU associées à la liaison.

```
# dladm show-linkprop -p cpus link
```

## Exemple 21–7 Allocation de CPU à l'interface

Cet exemple montre comment dédier des CPU à l'interface `internal0` dans la [Figure 18–3](#).

Notez les informations suivantes dans la sortie générée par les différentes commandes. Pour plus de clarté, les informations significatives sont mises en évidence dans la sortie.

- Par défaut `internal0` n'a pas de CPU dédiée. Par conséquent `VALUE` est `--`.
- L'interruption d'`internal0` est associée avec la CPU 18.
- Une fois que des CPU sont allouées, `internal0` affiche une nouvelle liste de CPU sous `VALUE`.

```
# dladm show-linkprop -p cpus internal0
LINK          PROPERTY  PERM  VALUE  DEFAULT  POSSIBLE
internal0     cpus      rw    --     --        --

# echo ::interrupts | mdb -k
Device Shared Type MSG # State INO Mondo Pil CPU
external#0 no MSI 3 enbl 0x1b 0x1b 6 0
internal#0 no MSI 2 enbl 0x1a 0x1a 6 18

# dladm set-linkprop -p cpus=14,18,19,20 internal0

# dladm show-linkprop -p cpus internal0
LINK          PROPERTY  PERM  VALUE  DEFAULT  POSSIBLE
internal0     cpus      rw    14,18,19,20 --        --
```

L'ensemble des threads de référence, y compris l'interruption sont désormais limités à l'ensemble de CPU que vous venez d'affecter.

# Gestion des ressources sur les flux

Les flux sont constitués de paquets réseau qui sont organisés en fonction d'un attribut. Les flux permettent d'allouer des ressources réseau. Pour obtenir une présentation des flux, reportez-vous à la section [“Gestion des ressources réseau à l'aide de flux” à la page 394](#).

Pour utiliser les flux pour la gestion des ressources, effectuez les étapes générales suivantes :

1. Créez le flux à partir d'un attribut spécifique comme indiqué à la section [“Gestion des ressources réseau à l'aide de flux” à la page 394](#).
2. Personnalisez l'utilisation des ressources du flux en définissant des propriétés qui se rapportent aux ressources réseau. A l'heure actuelle, seule la bande passante pour le traitement des paquets peut être définie.

## Configuration de flux sur le réseau

Les flux peuvent être créés sur le réseau physique ainsi que le réseau virtuel. Pour configurer les flux, utilisez la commande `flowadm`. Pour obtenir des informations techniques précises, reportez-vous à la page de manuel [flowadm\(1M\)](#).



## ▼ Procédure de configuration d'un flux

- 1 (Facultatif) Déterminez la liaison sur laquelle vous allez configurer les flux.

```
# dladm show-link
```

- 2 Vérifiez que les interfaces IP sur la liaison sélectionnée sont correctement configurées avec des adresses IP.

```
# ipadm show-addr
```

- 3 Créez des flux en fonction de l'attribut que vous avez déterminé pour chaque flux.

```
# flowadm add-flow -l link -a attribute=value[,attribute=value] flow
```

*attribute* Fait référence à l'une des classifications suivantes en fonction de laquelle vous pouvez organiser les paquets réseau dans un flux :

- Adresse IP
- Protocole de transport (UDP, TCP ou SCTP)
- Numéro de port pour une application (par exemple le port 21 pour FTP)
- Attribut de champ DS, qui est utilisé pour la qualité de service dans les paquets IPv6 uniquement. Pour plus d'informations sur le champ DS, reportez-vous à la section “[Point de code DS](#)” du [manuel Administration d'Oracle Solaris : Services IP](#).

*flow* Fait référence au nom que vous attribuez au flux.

Pour plus d'informations sur les flux et attributs de flux, reportez-vous à la page de manuel [flowadm\(1M\)](#).

- 4 Implémentez des contrôles de ressources sur les flux en définissant les propriétés de flux appropriées.

```
# flowadm set-flowprop -p property=value[,property=value,...] flow
```

Vous pouvez spécifier les propriétés de flux suivantes qui contrôlent les ressources :

*maxbw* La quantité maximale de bande passante de la liaison que les paquets identifiés avec ce flux peuvent utiliser. La valeur que vous définissez doit être comprise dans la plage autorisée de valeurs pour la bande passante de la liaison. Pour afficher la plage possible de valeurs de la bande passante d'une liaison, vérifiez le champ POSSIBLE dans la sortie générée par la commande suivante :

```
# dladm show-linkprop -p maxbw link
```

---

**Remarque** – Actuellement, seule la bande passante d'un flux peut être personnalisée.

---

5 (Facultatif) Affichez les flux que vous avez créés sur la liaison.

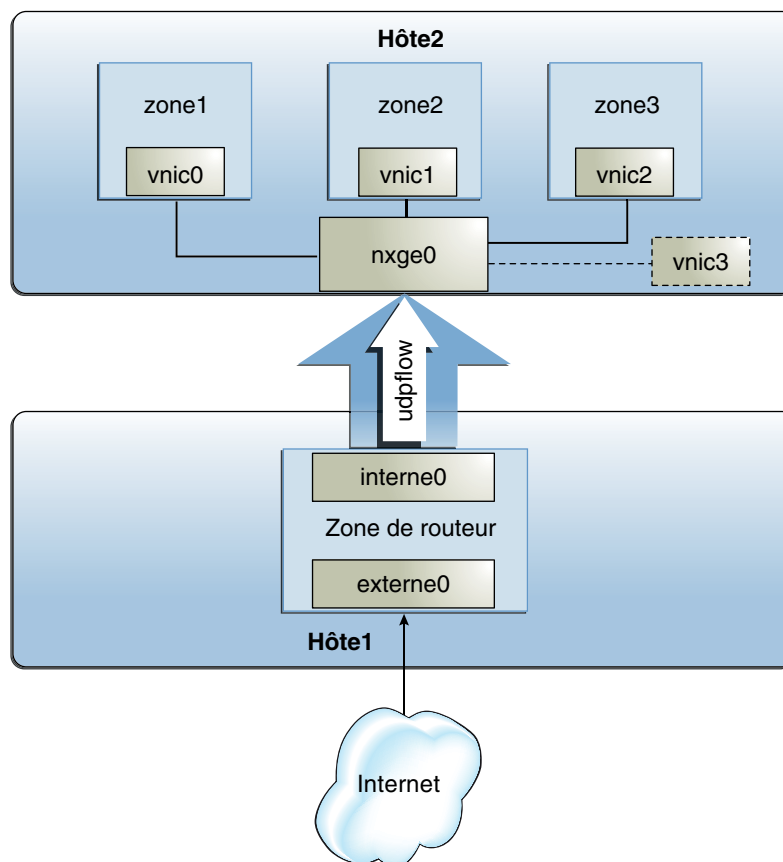
```
# flowadm show-flow -l link
```

6 (Facultatif) Affichez les paramètres de propriété d'un flux spécifique.

```
# flowadm show-flowprop flow
```

**Exemple 21–8** Gestion des ressources en définissant les propriétés de liaison et de flux

Cet exemple combine les étapes pour l'allocation de ressources réseau à des liaisons de données et des flux. L'exemple est basé sur la configuration présentée dans la figure ci-dessous.



La figure présente deux hôtes physiques qui sont reliés l'un à l'autre.

- Host1 a la configuration suivante :

- Il a une zone non globale qui fonctionne comme zone de routeur. Deux interfaces sont affectées à la zone : `external0` se connecte à Internet alors qu'`internal0` se connecte au réseau interne dont le deuxième hôte.
- Les interfaces IP ont été renommées pour utiliser des noms personnalisés. Bien que cela ne soit pas nécessaire, l'utilisation de noms personnalisés pour les liaisons et les interfaces est avantageuse quand vous administrez le réseau. Reportez-vous à la section [“Noms des périphériques réseau et des liaisons de données”](#) à la page 26.
- Un flux est configuré sur `internal0` afin d'isoler le trafic UDP et implémenter un contrôle sur la façon dont les paquets UDP utilisent les ressources. Pour plus d'informations sur la configuration des flux, reportez-vous à la section [“Gestion des ressources sur les flux”](#) à la page 416.
- Host2 a la configuration suivante :
  - Il dispose de trois zones non globales et de leurs VNIC. Les VNIC sont configurées sur une carte `nxge` prenant en charge l'allocation dynamique d'anneaux. Pour plus d'informations sur l'allocation d'anneaux, reportez-vous à la section [“Transmission et réception d'anneaux”](#) à la page 397.
  - La charge de traitement réseau de chaque zone est différente. Pour les besoins de cet exemple, la charge pour la zone1 est lourde, la charge pour la zone2 est moyenne et la charge pour la zone3 est légère. Les ressources sont affectées à ces zones en fonction de leur charge.
  - Une autre VNIC est configurée comme client logiciel. Pour obtenir un aperçu des clients MAC, reportez-vous à la section [“Clients MAC et allocation d'anneaux”](#) à la page 397.

Les tâches de cet exemple impliquent les éléments suivants :

- Création d'un flux et configuration de contrôles de flux : un flux est créé sur `internal0` pour créer des contrôles de ressources sur les paquets UDP reçus par Host2.
- Configuration des propriétés d'une ressource réseau pour les VNIC sur Host2 : basée sur la charge de traitement sur chaque zone, la VNIC de chaque zone est configurée avec un ensemble d'anneaux dédiés. Une autre VNIC est également configurée sans anneaux dédiés comme exemple de client logiciel.

Notez que l'exemple n'inclut aucune procédure de configuration de zone. Pour configurer des zones, reportez-vous au [Chapitre 17, “Planification et configuration de zones non globales \(tâches\)”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

Tout d'abord, affichez les informations sur les liaisons et les interfaces IP sur Host1.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED DUPLEX    DEVICE
internal0 Ethernet  up         1000 full    nge1
e1000g0   n          unknown    0      half     e1000g0
```

```
e1000g1      n      unknown      0      half      e1000g1
external0    Ethernet up      1000 full      nge0
```

#### # dladm show-link

```
LINK        CLASS    MTU    STATE    BRIDGE    OVER
internal0   phys      1500   up       --        nge1
e1000g0     phys      1500   unknown  --        --
e1000g1     phys      1500   unknown  --        --
external0   phys      1500   up       --        nge0
```

#### # ipadm show-addr

```
ADDROBJ     TYPE      STATE    ADDR
lo0/4       static    ok       127.0.0.1/8
external0   static    ok       10.10.6.5/24
internal0   static    ok       10.10.12.42/24
```

Ensuite, créez un flux sur `internal0` afin d'isoler le trafic UDP vers `Host2`. Implémentez des contrôles de ressources sur le flux.

```
# flowadm add-flow -l external0 -a transport=udp udpflow
# flowadm set-flowprop -p maxbw=80 udpflow
```

Vérifiez les informations sur le flux créé.

#### flowadm show-flow

```
FLOW        LINK        IPADDR    PROTO    PORT    DFSLD
udpflow     internal0 --        udp      --      --
```

```
# flowadm show-flowprop
SECURE OUTPUT FOR THIS
```

Sur `Host2`, configurez les VNIC sur `nxge0` pour chaque zone. Implémentez des contrôles de ressources sur chaque VNIC. Ensuite, affectez les VNIC à leurs zones respectives.

```
# dladm create-vnic -l nxge0 vnic0
# dladm create-vnic -l nxge0 vnic1
# dladm create-vnic -l nxge0 vnic2

# dladm set-prop -p rxrings=4,txrings=4 vnic0
# dladm set-prop -p rxrings=2,txrings=2 vnic1
# dladm set-prop -p rxrings=1,txrings=1 vnic2

# zone1>zonecfg>net> set physical=vnic0
# zone2>zonecfg>net> set physical=vnic1
# zone3>zonecfg>net> set physical=vnic2
```

Supposons que `pool1`, un ensemble de CPU dans `Host2`, ait été précédemment configuré pour une utilisation par `zone1`. Liez ce pool de CPU afin d'également gérer les processus réseau pour `zone1`, comme suit :

```
# dladm set-prop -p pool=pool01 vnic0
```

Enfin, créez un client logiciel qui partage des anneaux avec `nxge0`, l'interface principale.

```
dladm create-vnic -p rxrings=sw,txrings=sw -l nxge0 vnic3
```



## Contrôle du trafic réseau et de l'utilisation des ressources

---

Ce chapitre décrit les tâches de contrôle et de collecte d'informations statistiques sur l'utilisation des ressources du réseau dans un environnement de réseau physique ou virtuel. Ces informations peuvent vous aider à analyser l'allocation des ressources pour le provisioning, la consolidation et la facturation. Ce chapitre présente les deux commandes que vous utilisez pour afficher les statistiques : `d1stat` et `flowstat`.

Les sujets suivants sont abordés :

- “Présentation du flux de trafic réseau ” à la page 423
- “Contrôle du trafic et de l'utilisation des ressources (liste des tâches) ” à la page 426
- “Collecte de statistiques relatives au trafic réseau sur les liaisons” à la page 427
- “Collecte de statistiques relatives au trafic réseau sur les flux” à la page 433
- “Configuration de la comptabilisation du réseau” à la page 436

### Présentation du flux de trafic réseau

Les paquets traversent un chemin quand ils entrent ou sortent d'un système. A un niveau granulaire, les paquets sont reçus et transmis via des anneaux de réception (Rx) et des anneaux de transmission (Tx) d'une carte réseau. A partir de ces anneaux, les paquets reçus sont transmis à la pile réseau pour poursuivre le traitement pendant que les paquets sortants sont envoyés au réseau.

Le [Chapitre 21, “Gestion des ressources réseau”](#) introduit le concept de couloirs réseau. Une combinaison de ressources système allouées pour gérer le trafic sur le réseau constitue un couloir réseau. Par conséquent, les *couloirs réseau* sont des chemins personnalisés pour des types spécifiques de trafic réseau. Chaque couloir peut être *matériel* ou *logiciel* . En outre, chaque type de couloir peut être un couloir de *réception* ou de *transmission*. La distinction entre les couloirs matériels et logiciels est basée sur la capacité d'une carte réseau de prendre en charge l'allocation d'anneaux. Pour plus d'informations sur l'allocation d'anneaux, reportez-vous à la section [“Transmission et réception d'anneaux ” à la page 397](#). Ce chapitre se concentre principalement sur le trafic entrant qui est reçu par des couloirs de réception.

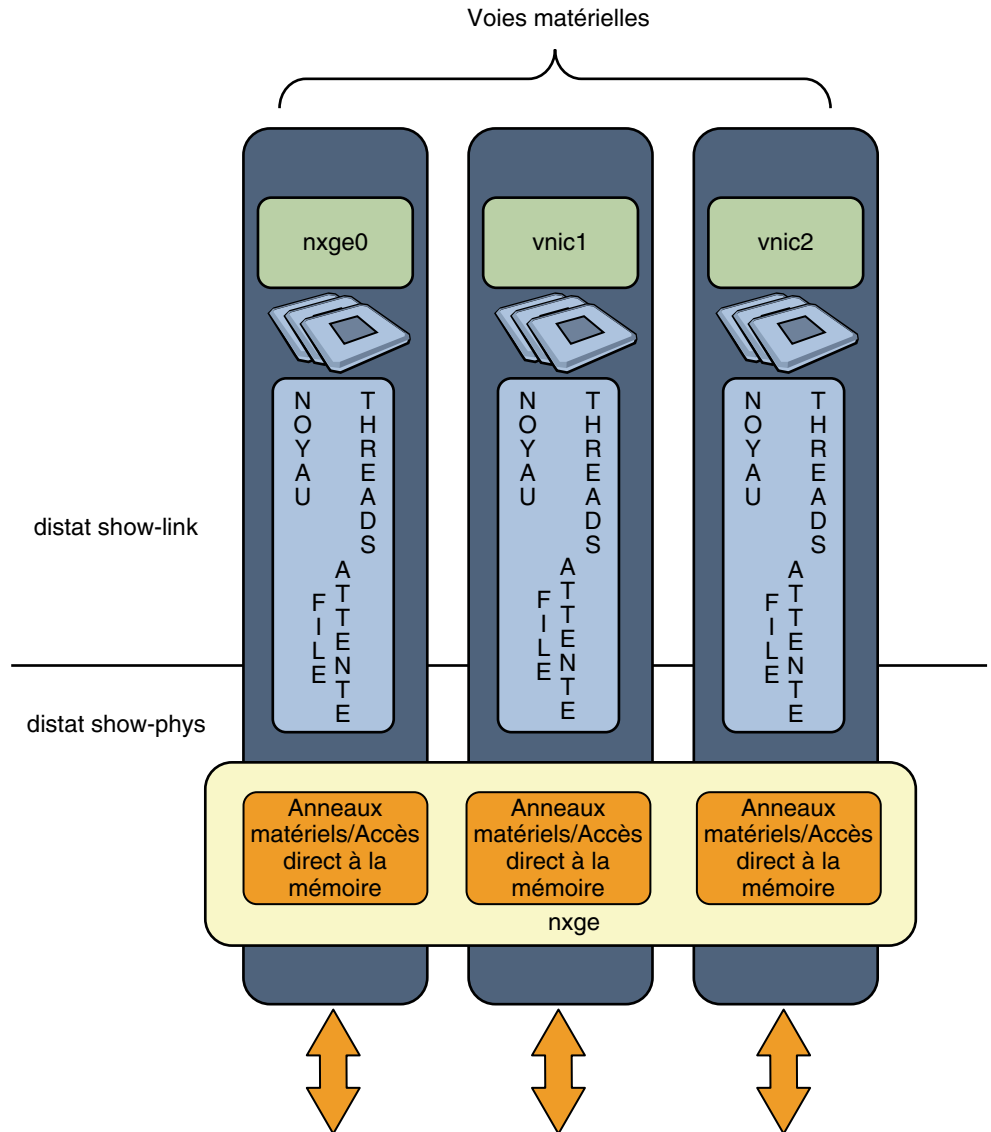
Sur les couloirs matériels, des anneaux sont dédiés aux paquets qui utilisent ces couloirs. En revanche, les anneaux sur les couloirs logiciels sont partagés entre des liaisons de données. Les liaisons de données sont configurées pour partager des anneaux pour les raisons suivantes :

- Raison administrative. La liaison de données n'exécute peut-être pas de processus intensifs nécessitant des anneaux dédiés.
- La carte réseau ne prend pas en charge l'allocation d'anneaux.
- Malgré la prise en charge de l'allocation d'anneaux, il ne reste plus d'anneaux à affecter pour un usage exclusif.

Observez la figure suivante qui présente les différents couloirs matériels :



FIGURE 22-1 Couloirs matériels



La figure montre la configuration suivante :

- Le système a une carte réseau unique, `nxge`.
- Des liaisons sont configurées sur le périphérique physique : `nxge0`, `vnic1` et `vnic2`. Notez qu'en tant que liaison de données, `nxge0` peut avoir un nom personnalisé. Cependant, dans la figure, la liaison conserve son nom de périphérique par défaut.

- Le système dispose de plusieurs processeurs.
- La carte réseau prend en charge l'allocation d'anneaux dynamique. Par conséquent, un ensemble d'anneaux matériels peut être affecté à chaque liaison pour constituer un couloir matériel. De plus, un ensemble de CPU est également affecté à chaque couloir.

# Contrôle du trafic et de l'utilisation des ressources (liste des tâches)

Vous pouvez obtenir des informations sur la manière dont les paquets utilisent les ressources réseau par l'observation du flux de paquets sur les couloirs réseau. La commande `dstat` fournit ces informations sur les liaisons de données. La commande `flowstat` exécute des fonctions similaires pour les flux existants.

Le tableau ci-dessous répertorie les différents modes que vous pouvez utiliser pour obtenir des statistiques sur le trafic réseau et l'utilisation des ressources dans le système.

Tâche	Description	Voir
Obtention d'informations statistiques sur le trafic réseau	Affiche le trafic entrant et sortant sur les interfaces réseau d'un système.	<a href="#">"Procédure d'obtention de statistiques de base sur le trafic réseau" à la page 428</a>
Obtention d'informations statistiques sur l'utilisation des anneaux	Visualise la manière dont le trafic entrant et sortant est distribué entre les anneaux d'une carte réseau.	<a href="#">"Procédure d'obtention de statistiques sur l'utilisation d'anneaux" à la page 430</a>
Obtention d'informations statistiques sur le trafic réseau de couloirs spécifiques	Visualise des informations détaillées sur le trafic entrant et sortant lorsque les paquets traversent des couloirs réseau, qui sont configurés sur les interfaces réseau d'un système.	<a href="#">"Procédure d'obtention de statistiques sur le trafic réseau sur des couloirs" à la page 431</a>
Obtention d'informations statistiques relatives au trafic sur les flux	Affiche les informations sur le trafic entrant et sortant traversant des flux définis par l'utilisateur.	<a href="#">"Procédure d'obtention de statistiques sur les flux" à la page 434</a>
Configuration de la comptabilisation du trafic réseau	Configure la comptabilisation réseau pour capturer des informations sur le trafic à des fins de comptabilisation.	<a href="#">"Procédure de configuration de la comptabilisation réseau étendue" à la page 436</a>

Tâche	Description	Voir
Obtention de statistiques historiques sur le trafic réseau	Extrait des informations du fichier journal de comptabilisation réseau étendu pour obtenir les statistiques historiques du trafic réseau sur des couloirs ainsi que des flux.	<a href="#">“Procédure d’obtention de statistiques historiques sur le trafic réseau” à la page 437</a>

Pour obtenir une description de la procédure de configuration des flux, reportez-vous à la section [“Gestion des ressources sur les flux” à la page 416](#). Pour plus d’informations sur ces deux commandes, reportez-vous aux pages de manuel [dlstat\(1M\)](#) et [flowstat\(1M\)](#).

## Collecte de statistiques relatives au trafic réseau sur les liaisons

Les commandes `dlstat` et `flowstat` sont des outils de contrôle et d’obtention de statistiques sur le trafic réseau sur des liaisons de données et des flux, respectivement. Ces commandes sont parallèles aux commandes `dladm` et `flowadm`. Le tableau suivant montre le parallélisme entre la paire de commandes `*adm` et la paire de commandes `*stat`, et leurs fonctions respectives :

Commandes d’administration		Commandes de contrôle	
Commande	Fonction	Commande	Fonction
Options de la commande <code>dladm</code>	Interface utilisateur et outil pour la configuration et l’administration des liaisons de données.	Options de la commande <code>dlstat</code>	Interface utilisateur et outil pour l’obtention de statistiques sur le trafic sur les liaisons de données.
Options de la commande <code>flowadm</code>	Interface utilisateur et outil pour la configuration et l’administration des flux.	Options de la commande <code>flowstat</code>	Interface utilisateur et outil pour l’obtention de statistiques sur le trafic sur les flux.

Les variantes suivantes de la commande `dlstat` peuvent être utilisées pour obtenir des informations sur le trafic réseau :

- `dlstat` : affiche des informations générales concernant les paquets qui sont en cours de réception ou de transmission par un système.
- `dlstat show-phys` : affiche des informations sur l’utilisation d’anneaux de réception et de transmission. Cette commande correspond à la commande `dladm show-phys`, qui affiche des informations sans rapport avec le trafic sur un périphérique physique du réseau. Pour une illustration au niveau du couloir réseau auquel cette commande s’applique, reportez-vous à la [Figure 22–1](#).

- `dlstat show-link` : affiche des informations détaillées relatives au flux de trafic sur un couloir. Le couloir est identifié par sa liaison de données. Cette commande correspond aux commandes `dladm show-link` et `dladm show-vnic`, qui affichent des informations sans rapport avec le trafic sur les liaisons de données. Pour une illustration au niveau du couloir réseau auquel la commande `dlstat show-link` s'applique, reportez-vous à la [Figure 22-1](#).
- `dlstat show-aggr` : affiche des informations sur l'utilisation des ports dans un groupement de liens. Cette commande correspond à la commande `dladm show-aggr`, qui affiche des informations sans rapport avec le trafic sur un groupement de liens.

## ▼ Procédure d'obtention de statistiques de base sur le trafic réseau

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Observez le flux de trafic de base sur toutes les liaisons de données.

```
# dlstat [-r|-t] [-i interval] [link]
```

<code>[-r -t]</code>	Affiche des statistiques uniquement du côté réception (option <code>-r</code> ) ou des statistiques uniquement du côté transmission (option <code>-t</code> ). Si vous n'utilisez pas ces options, les statistiques du côté réception et du côté transmission sont affichées.
<code>-i interval</code>	Spécifie la durée en secondes après laquelle vous souhaitez que les statistiques affichées soient actualisées. Si vous n'utilisez pas cette option, une sortie statique est affichée.
<code>link</code>	Indique que vous souhaitez contrôler les statistiques d'une la liaison de données spécifique uniquement. Si vous n'utilisez pas cette option, les informations de toutes les liaisons de données s'affichent.

Utilisée seule, la commande `dlstat` affiche des informations sur les paquets entrants et sortants sur toutes les liaisons de données configurées.

Les informations suivantes sont affichées par la plupart des options que vous pouvez utiliser avec la commande `dlstat` :

- Liaisons dans le système, qui ont été configurées avec des interfaces IP et qui peuvent recevoir ou transmettre le trafic
- Tailles de paquet et d'octet
- Interruptions et statistiques d'interrogation MAC
- Longueurs de chaîne de paquet

**Exemple 22-1** Affichage de statistiques de base côté réception et côté transmission

Cet exemple affiche des informations sur le trafic réseau qui est reçu ou envoyé sur toutes les liaisons de données configurées sur le système.

```
# dlstat
  LINK      IPKTS    RBYTES    OPKTS    OBYTES
e1000g0  101.88K    32.86M    40.16K    4.37M
nxge1     4.50M     6.78G     1.38M    90.90M
vnic1           8       336         0         0
```

**Exemple 22-2** Affichage des statistiques du côté réception à intervalles d'une seconde

Cet exemple affiche des informations sur le trafic qui est en cours de réception sur toutes les liaisons de données. L'information est actualisée chaque seconde. Pour arrêter l'actualisation de l'affichage, appuyez sur Ctrl-C.

```
# dlstat -r -i 1
  LINK      IPKTS    RBYTES    INTRS    POLLS    CH<10  CH10-50  CH>50
e1000g0  101.91K    32.86M    87.56K    14.35K    3.70K    205       5
nxge1     9.61M    14.47G     5.79M     3.82M   379.98K   85.66K   1.64K
vnic1           8       336         0         0         0         0
e1000g0           0         0         0         0         0         0
nxge1     82.13K  123.69M    50.00K    32.13K    3.17K    724      24
vnic1           0         0         0         0         0         0
...
^C
```

Dans cette sortie, les statistiques d'interruption (INTRS) sont significatives. Un faible nombre d'interruptions indique une plus grande efficacité en termes de performances. Si le nombre d'interruptions est élevé, vous pouvez avoir besoin d'ajouter davantage de ressources pour la liaison spécifique.

**Exemple 22-3** Affichage de statistiques du côté transmission à intervalles de cinq secondes

Cet exemple affiche des informations sur le trafic qui est en cours d'envoi sur toutes les liaisons de données. L'information est actualisée toutes les cinq secondes.

```
# dlstat -t -i 5
  LINK      OPKTS    OBYTES    BLKCNT  UBLKCNT
e1000g0   40.24K     4.37M         0         0
nxge1     9.76M   644.14M         0         0
vnic1           0         0         0         0
e1000g0           0         0         0         0
nxge1     26.82K     1.77M         0         0
vnic1           0         0         0         0
...
^C
```

# ▼ Procédure d'obtention de statistiques sur l'utilisation d'anneaux

## 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

## 2 Affichez les statistiques d'anneaux.

**# dlstat show-phys [-r|-t] [-i interval] [link]**

**[-r|-t]** Affiche des statistiques uniquement du côté réception (option -r) ou des statistiques uniquement du côté transmission (option -t). Si vous n'utilisez pas ces options, les statistiques du côté réception et du côté transmission sont affichées.

**-i interval** Spécifie la durée en secondes après laquelle vous souhaitez que les statistiques affichées soient actualisées. Si vous n'utilisez pas cette option, une sortie statique est affichée.

**link** Indique que vous souhaitez contrôler les statistiques de la liaison de données spécifique uniquement. Si vous n'utilisez pas cette option, les informations de toutes les liaisons de données s'affichent.

Utilisée seule, la commande `dlstat show-phys` affiche des informations sur les paquets entrants et sortants sur toutes les liaisons de données configurées.

### Exemple 22–4 Affichage des statistiques d'anneaux de réception pour une liaison de données

Cet exemple illustre l'utilisation d'anneaux de réception pour la liaison de données.

```
# dlstat show-phys -r nxge1
LINK TYPE INDEX  IPKTS  RBYTES
nxge1  rx      0      21    1.79K
nxge1  rx      1       0       0
nxge1  rx      2   1.39M    2.10G
nxge1  rx      3       0       0
nxge1  rx      4   6.81M   10.26G
nxge1  rx      5   4.63M    6.97G
nxge1  rx      6   3.97M    5.98G
nxge1  rx      7       0       0
```

Le périphérique `nxge` dispose de huit anneaux de réception, qui sont identifiés sous le champ `INDEX`. Une répartition égale des paquets par anneau est une configuration idéale qui indique que les anneaux sont correctement alloués à des liaisons en fonction de la charge des liaisons. Une répartition inégale peut indiquer une répartition disproportionnée des anneaux par liaison. La résolution dépend du fait que la carte réseau prenne ou non en charge l'allocation

dynamique d'anneaux, qui vous permet de redistribuer les anneaux par liaison. Pour plus d'informations sur l'allocation dynamique d'anneaux, reportez-vous à la section [“Transmission et réception d'anneaux”](#) à la page 397.

### Exemple 22-5 Affichage des statistiques d'anneaux de transmission d'une liaison de données

Cet exemple illustre l'utilisation d'anneaux de transmission pour la liaison de données.

```
# dlstat show-phys -t nxge1
LINK TYPE INDEX OPKTS OBYTES
nxge1 tx 0 44 3.96K
nxge1 tx 1 0 0
nxge1 tx 2 1.48M 121.68M
nxge1 tx 3 2.45M 201.11M
nxge1 tx 4 1.47M 120.82M
nxge1 tx 5 0 0
nxge1 tx 6 1.97M 161.57M
nxge1 tx 7 4.59M 376.21M
nxge1 tx 8 2.43M 199.24M
nxge1 tx 9 0 0
nxge1 tx 10 3.23M 264.69M
nxge1 tx 11 1.88M 153.96M
```

## ▼ Procédure d'obtention de statistiques sur le trafic réseau sur des couloirs

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Affichez les statistiques sur les couloirs réseau.

```
# dlstat show-link [-r [F]] [-t] [-i interval] [link]
```

**[-r] [-t]** Affiche des statistiques uniquement du côté réception (option -r) ou des statistiques uniquement du côté transmission (option -t). Si vous n'utilisez pas ces options, les statistiques du côté réception et du côté transmission sont affichées.

**-i interval** Spécifie la durée en secondes après laquelle vous souhaitez que les statistiques affichées soient actualisées. Si vous n'utilisez pas cette option, une sortie statique est affichée.

**link** Indique que vous souhaitez contrôler les statistiques d'une la liaison de données spécifique uniquement. Si vous n'utilisez pas cette option, les informations de toutes les liaisons de données s'affichent.

Si le groupement d'anneaux est pris en charge et que des anneaux dédiés ont été configurés, les statistiques de couloir matériel s'affichent. Si aucun anneau dédié n'est configuré, les statistiques de couloir logiciel s'affichent.

**Exemple 22-6** Affichage des statistiques du côté réception pour un couloir

Cet exemple affiche les informations suivantes :

- La manière dont les paquets sont reçus sur un couloir matériel
- La manière dont les paquets sont reçus sur un couloir logiciel
- La manière dont les paquets sont reçus sur un couloir logiciel et déployés aux CPU assignées

La commande suivante illustre les statistiques du côté réception pour la liaison spécifique. Les informations indiquent l'utilisation des anneaux. Toutefois, les données peuvent également refléter l'implémentation d'autres allocations de ressources, comme les limites de bande passante et le traitement des priorités.

```
# dlstat show-link -r nxge1
LINK TYPE ID INDEX IPKTS RBYTES INTRS POLLS CH<10 CH10-50 CH>50
nxge1 rx local -- 0 0 0 0 0 0
nxge1 rx hw 1 0 0 0 0 0
nxge1 rx hw 2 1.73M 2.61G 1.33M 400.22K 67.03K 7.49K 38
nxge1 rx hw 3 0 0 0 0 0 0
nxge1 rx hw 4 8.44M 12.71G 4.35M 4.09M 383.28K 91.24K 2.09K
nxge1 rx hw 5 5.68M 8.56G 3.72M 1.97M 203.68K 43.94K 854
nxge1 rx hw 6 4.90M 7.38G 3.11M 1.80M 168.59K 42.34K 620
nxge1 rx hw 7 0 0 0 0 0 0
```

La commande suivante illustre les statistiques du côté réception pour la liaison spécifique. Dans la sortie, le champ ID indique si des anneaux matériels sont affectés exclusivement ou partagés entre les clients. Dans la carte ixgbe, les anneaux Rx sont partagés si d'autres clients comme des VNIC sont configurés sur la liaison. Par conséquent, pour cet exemple spécifique, des anneaux Rx sont partagés, comme indiqué par la valeur sw et sous le champ ID.

```
# dlstat show-link -r ixgbe0
LINK TYPE ID INDEX IPKTS RBYTES INTRS POLLS CH<10 CH10-50 CH>50
ixgbe0 rx local -- 0 0 0 0 0 0
ixgbe0 rx sw -- 794.28K 1.19G 794.28K 0 0 0
```

La commande suivante illustre les statistiques d'utilisation du côté réception pour la liaison spécifique. De plus, avec l'utilisation de l'option -F dans la commande, la sortie fournit aussi des informations de déploiement. Plus précisément, le nombre de déploiements est de deux (0 et 1). Le trafic réseau qui est reçu sur le couloir matériel qui utilise l'anneau 0 est fractionné et transmis entre les deux déploiements. De même, le trafic réseau qui est reçu sur le couloir matériel qui utilise l'anneau 1 est également fractionné et répartis entre les deux déploiements.

```
# dlstat show-link -r -F nxge1
LINK ID INDEX FOUT IPKTS
```



```

nxge1  local  --  0  0
nxge1  hw    0  0 382.47K
nxge1  hw    0  1  0
nxge1  hw    1  0 367.50K
nxge1  hw    1  1 433.24K

```

### Exemple 22-7 Affichage des statistiques du côté transmission pour un couloir

L'exemple suivant affiche les statistiques relatives aux paquets sortants sur un couloir spécifique.

```

# dlstat show-link -t nxge1
LINK  TYPE  ID  INDEX  OPKTS  OBYTES  BLKCNT  UBLKCNT
nxge1  tx  hw    0      32    1.44K      0      0
nxge1  tx  hw    1      0      0      0      0
nxge1  tx  hw    2    1.48M    97.95M      0      0
nxge1  tx  hw    3    2.45M   161.87M      0      0
nxge1  tx  hw    4    1.47M    97.25M      0      0
nxge1  tx  hw    5      0     276      0      0
nxge1  tx  hw    6    1.97M   130.25M      0      0
nxge1  tx  hw    7    4.59M   302.80M      0      0
nxge1  tx  hw    8    2.43M   302.80M      0      0
nxge1  tx  hw    9      0      0      0      0
nxge1  tx  hw   10    3.23M   213.05M      0      0
nxge1  tx  hw   11    1.88M   123.93M      0      0

```

## Collecte de statistiques relatives au trafic réseau sur les flux

Les statistiques de flux vous aident à évaluer le trafic de paquets sur n'importe quel flux du système. Pour obtenir des informations sur les flux, utilisez la commande `flowstat`. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel [flowstat\(1M\)](#).

La syntaxe la plus courante de la commande `flowstat` est la suivante :

```
# flowstat [-r|-t] [-i interval] [-l link flow]
```

**`[-r|-t]`** Affiche des statistiques uniquement du côté réception (option `-r`) ou des statistiques uniquement du côté transmission (option `-t`). Si vous n'utilisez pas ces options, les statistiques du côté réception et du côté transmission sont affichées.

**`-i interval`** Spécifie la durée en secondes après laquelle vous souhaitez que les statistiques affichées soient actualisées. Si vous n'utilisez pas cette option, une sortie statique est affichée.

**`link`** Indique que vous souhaitez contrôler les statistiques pour tous les flux de la liaison de données. Si vous n'utilisez pas cette option, les informations relatives à tous les flux sur toutes les liaisons de données sont affichées.

*flow*

Indique que vous souhaitez contrôler les statistiques d'un flux spécifique uniquement. Si vous n'utilisez pas cette option, selon que vous avez spécifié une liaison, toutes les statistiques de flux sont affichées.

## ▼ Procédure d'obtention de statistiques sur les flux

### Avant de commencer

Vous pouvez utiliser la commande `flowstat` uniquement si des flux existent dans votre configuration réseau. Pour configurer les flux, reportez-vous au [Chapitre 21, “Gestion des ressources réseau”](#).

- 1 **Sur le système sur lequel vous avez déjà configuré le contrôle de flux, connectez-vous en tant qu'administrateur dans la zone globale.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 2 **Pour un échantillonnage de la manière d'observer le trafic réseau sur des flux, exécutez une des commandes suivantes :**

- Afficher des statistiques relatives aux paquets entrants et sortants sur tous les flux.

```
# flowstat
```

Cette commande fournit un affichage statique des informations sur le trafic sur tous les flux configurés.

- Afficher les statistiques relatives au trafic réseau de base sur tous les flux à un intervalle spécifié.

```
# flowstat -i interval
```

L'affichage des statistiques est actualisé à l'intervalle spécifié jusqu'à ce que vous arrêtiez la génération de la sortie en appuyant sur Ctrl+C.

- Afficher les statistiques relatives aux paquets entrants sur tous les flux qui sont configurés sur une liaison de données.

```
# flowstat -r -l link
```

- Afficher les statistiques relatives aux paquets sortants sur un flux indiqué à un intervalle spécifié.

```
# flowstat -t -i interval flow
```

### Exemple 22–8 Affichage de statistiques de trafic pour tous les flux à intervalles d'une seconde

Cet exemple montre chaque seconde des informations sur le trafic entrant et sortant sur tous les flux configurés sur le système.

```
# flowstat -i 1
FLOW      IPKTS      RBYTES      IERRS      OPKTS      OBYTES      OERRS
flow1     528.45K    787.39M      0          179.39K    11.85M      0
flow2     742.81K    1.10G        0           0           0           0
flow3           0           0           0           0           0           0
flow1      67.73K    101.02M      0          21.04K     1.39M      0
flow2           0           0           0           0           0           0
flow3           0           0           0           0           0           0
...
^C
```

### Exemple 22-9 Affichage de statistiques du côté transmission pour tous les flux

```
# flowstat -t
FLOW      OPKTS      OBYTES      OERRS
flow1     24.37M     1.61G        0
flow2           0           0           0
flow1         4          216          0
```

### Exemple 22-10 Affichage de statistiques du côté réception pour tous les flux sur une liaison spécifiée

Cet exemple montre le trafic entrant dans les couloirs matériels dans tous les flux qui ont été créés sur la liaison de données net0.

```
# flowstat -r -i 2 -l net0
FLOW      IPKTS      RBYTES      IERRS
tcp-flow  183.11K    270.24M      0
udp-flow           0           0           0
tcp-flow  373.83K    551.52M      0
udp-flow           0           0           0
tcp-flow  372.35K    549.04M      0
udp-flow           0           0           0
tcp-flow  372.87K    549.61M      0
udp-flow           0           0           0
tcp-flow  371.57K    547.89M      0
udp-flow           0           0           0
tcp-flow  191.92K    282.95M      0
udp-flow  206.51K    310.70M      0
tcp-flow           0           0           0
udp-flow  222.75K    335.15M      0
tcp-flow           0           0           0
udp-flow  223.00K    335.52M      0
tcp-flow           0           0           0
udp-flow  160.22K    241.07M      0
tcp-flow           0           0           0
udp-flow  167.89K    252.61M      0
tcp-flow           0           0           0
udp-flow   9.52K     14.32M      0
...
^C
```

# Configuration de la comptabilisation du réseau

Vous pouvez utiliser l'utilitaire de comptabilisation étendue pour capturer des statistiques sur le trafic réseau dans un fichier journal. De cette manière, vous pouvez mettre à jour les enregistrements de trafic pour le suivi, le provisioning, la consolidation et la facturation. Plus tard, reportez-vous au fichier journal pour obtenir des informations sur l'utilisation du réseau sur une période de temps.

Pour configurer l'utilitaire de comptabilisation étendue, utilisez la commande `acctadm`.

## ▼ Procédure de configuration de la comptabilisation réseau étendue

- 1 Sur le système avec les interfaces dont vous voulez suivre l'utilisation du réseau, connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Affichez l'état de la comptabilisation réseau étendue dans le système.

```
# acctadm net
```

Quatre types de comptabilisation étendue peuvent être activés par la commande `acctadm` :

- Comptabilisation des processus
- Comptabilisation des tâches
- Comptabilisation des flux pour la qualité de service IP (IPQoS)
- Comptabilisation réseau des liaisons et des flux

La spécification `net` affiche l'état de la comptabilisation réseau. Si `net` n'est pas utilisée, l'état des quatre types de comptabilisation s'affiche.

---

**Remarque** – La comptabilisation réseau s'applique également aux flux qui sont gérés par les commandes `flowadm` et `flowstat` comme indiqué à la section “[Gestion des ressources sur les flux](#)” à la page 416. Par conséquent, pour configurer la comptabilisation de ces flux, utilisez l'option `net` avec la commande `acctadm`. N'utilisez *pas* l'option `flow` qui permet la comptabilisation des flux et qui s'applique aux configurations IPQoS.

---

- 3 Activez la comptabilisation étendue pour le trafic réseau.

```
# acctadm -e extended -f filename net
```

où *filename* comprend le chemin complet du fichier journal qui va capturer les statistiques de trafic réseau. Le fichier journal peut être créé dans n'importe quel répertoire que vous indiquez.

**4 Vérifiez que la comptabilisation réseau étendue est activée.**

```
# acctadm net
```

**Exemple 22-11 Configuration de la comptabilisation étendue pour le trafic réseau**

Cet exemple montre comment capturer et afficher des informations historiques sur le trafic réseau sur des liaisons de données et n'importe quel flux configuré sur le système.

Tout d'abord, affichez l'état de tous les types de comptabilisation, comme suit :

```
# acctadm
      Task accounting: inactive
      Task accounting file: none
      Tracked task resources: none
      Untracked task resources: extended
      Process accounting: inactive
      Process accounting file: none
      Tracked process resources: none
      Untracked process resources: extended,host
      Flow accounting: inactive
      Flow accounting file: none
      Tracked flow resources: none
      Untracked flow resources: extended
      Network accounting: inactive
      Network accounting file: none
      Tracked Network resources: none
      Untracked Network resources: extended
```

La sortie montre que la comptabilisation réseau n'est pas active.

Ensuite, activez la comptabilisation réseau étendue.

```
# acctadm -e extended -f /var/log/net.log net
# acctadm net
      Net accounting: active
      Net accounting file: /var/log/net.log
      Tracked net resources: extended
      Untracked net resources: none
```

Une fois que vous avez activé la comptabilisation réseau, vous pouvez utiliser les commandes `dlstat` et `flowstat` pour extraire des informations du fichier journal. La procédure suivante explique les étapes.

## ▼ Procédure d'obtention de statistiques historiques sur le trafic réseau

### Avant de commencer

Vous devez activer la comptabilisation étendue pour le réseau avant de pouvoir afficher les données d'historique sur le réseau. De plus pour afficher des données d'historique relatives au

trafic sur des flux, vous devez tout d'abord configurer les flux dans le système comme expliqué dans la section [“Gestion des ressources sur les flux”](#) à la page 416.

**1 Sur le système avec les interfaces dont que vous voulez suivre l'utilisation du réseau, connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Pour extraire et afficher des informations historiques sur l'utilisation des ressources sur les liaisons de données, utilisez la commande suivante :**

```
# dlstat show-link -h [-a] -f filename [-d date] [-F format] [-s start-time] [-e end-time] [link]
```

-h	Affiche un récapitulatif des informations historiques relatives à l'utilisation des ressources par paquets entrants et sortants sur les liaisons de données.
-a	Affiche l'utilisation des ressources sur toutes les liaisons de données, y compris celles qui ont déjà été supprimées après la capture de données.
-f <i>nomdefichier</i>	Spécifie le fichier journal qui a été défini quand la comptabilisation réseau a été activée avec la commande <code>acctadm</code> .
-d	Affiche les informations du journal pour des dates quand les informations sont disponibles.
-F <i>format</i>	Affiche les données dans un format spécifique. Actuellement, <code>gnuplot</code> est le seul format pris en charge.
-s <i>start-time</i> , -e <i>end-time</i>	Affiche les informations du journal disponibles pour une date et une période précises. Utilisez le format <code>MM/DD/YYYY, hh:mm:ss</code> . L'heure, hour (hh), doit utiliser la notation sur 24 heures. Si vous n'incluez pas la date, les données de la date en cours s'affichent.
<i>link</i>	Affiche les données historiques d'une liaison de données. Si vous n'utilisez pas cette option, les données réseau d'historique pour toutes les liaisons de données configurées s'affichent.

**3 Pour extraire et afficher des informations historiques relatives au trafic réseau sur des flux configurés, utilisez la commande suivante :**

```
# flowstat -h [-a] -f filename [-d date] [-F format] [-s start-time] [-e end-time] [flow]
```

-h	Affiche un récapitulatif des informations historiques relatives à l'utilisation des ressources par paquets entrants et sortants sur les liaisons de données.
-a	Affiche l'utilisation des ressources sur toutes les liaisons de données, y compris celles qui ont déjà été supprimées après la capture de données.

<code>-f nomdefichier</code>	Spécifie le fichier journal qui a été défini quand la comptabilisation réseau a été activée avec la commande <code>acctadm</code> .
<code>-d</code>	Affiche les informations du journal pour des dates quand les informations sont disponibles.
<code>-F format</code>	Affiche les données dans un format spécifique. Actuellement, <code>gnuplot</code> est le seul format pris en charge.
<code>-s start-time,</code> <code>-e end-time</code>	Affiche les informations du journal disponibles pour une date et une période précises. Utilisez le format <code>MM/DD/YYYY, hh:mm:ss</code> . hour (hh) doit utiliser la notation sur 24 heures. Si vous n'incluez pas la date, les données de la date en cours s'affichent.
<code>link</code>	Affiche les données historiques d'une liaison de données. Si vous n'utilisez pas cette option, les données réseau d'historique pour toutes les liaisons de données configurées s'affichent.
<code>flow</code>	Affiche les données historiques d'un flux. Si vous n'utilisez pas cette option, les données réseau d'historique pour tous les flux configurés s'affichent.

### Exemple 22-12 Affichage d'informations historiques relatives à l'utilisation des ressources sur les liaisons des données

L'exemple suivant présente les statistiques historiques sur le trafic réseau et son utilisation des ressources sur une liaison de données.

```
# dlstat show-link -h -f /var/log/net.log
LINK      DURATION  IPACKETS  RBYTES    OPACKETS  OBYTES    BANDWIDTH
e1000g0    80        1031      546908     0         0         2.44 Kbps
```

### Exemple 22-13 Affichage d'informations historiques relatives à l'utilisation des ressources sur les flux

Les exemples suivants montrent différentes manières d'afficher les statistiques historiques relatives au trafic réseau sur un flux et son utilisation des ressources.

Affichez les statistiques historiques de l'utilisation de ressources par le trafic sur un flux :

```
# flowstat -h -f /var/log/net.log
FLOW      DURATION  IPACKETS  RBYTES    OPACKETS  OBYTES    BANDWIDTH
flowtcp    100       1031      546908     0         0         43.76Kbps
flowudp    0         0         0          0         0         0.00Mbps
```

Affichez les statistiques historiques de l'utilisation de ressources par le trafic sur un flux à une date ou sur une période donnée.

```
# flowstat -h -s 02/19/2008,10:39:06 -e 02/19/2008,10:40:06 \  
-f /var/log/net.log flowtcp
```

FLOW	START	END	RBYTES	OBYTES	BANDWIDTH
flowtcp	10:39:06	10:39:26	1546	6539	3.23 Kbps
flowtcp	10:39:26	10:39:46	3586	9922	5.40 Kbps
flowtcp	10:39:46	10:40:06	240	216	182.40 bps
flowtcp	10:40:06	10:40:26	0	0	0.00 bps

Affichez les statistiques historiques de l'utilisation de ressources par le trafic sur un flux à une date ou sur une période donnée. Affichez les informations à l'aide du format gnuplot.

```
# flowstat -h -s 02/19/2008,10:39:06 -e 02/19/2008,10:40:06 \  
-F gnuplot -f /var/log/net.log flowtcp  
# Time tcp-flow  
10:39:06 3.23  
10:39:26 5.40  
10:39:46 0.18  
10:40:06 0.00
```



# Glossaire

---

<b>3DES</b>	Voir <a href="#">Triple-DES</a> .
<b>adresse à usage local</b>	Adresse unicast dont la portée du routage est exclusivement locale (au sein du sous-réseau ou d'un réseau d'abonnés). Cette adresse peut également avoir un caractère local ou global.
<b>adresse anycast</b>	Adresse IPv6 attribuée à un groupe d'interfaces (appartenant généralement à des noeuds différents). Un paquet envoyé à une adresse anycast est acheminé vers l'interface <i>la plus proche</i> possédant cette adresse. La route suivie par le paquet est conforme à la mesure de distance du protocole de routage.
<b>adresse CIDR</b>	Classless Inter-Domain Routing, routage inter-domaine sans classe. Format d'adresse IPv4 non basé sur les classes de réseau (classe A, B et C). Les adresses CIDR ont une longueur de 32 bits. Elles utilisent le format de notation décimal avec points IPv4 standard en plus d'un préfixe réseau. Ce préfixe définit le numéro de réseau et le masque de réseau.
<b>adresse de diffusion</b>	Adresses réseau IPv4 avec la partie hôte de l'adresse ne comportant que des zéros (10.50.0.0) ou des valeurs à un bit (10.50.255.255). Un paquet envoyé à une adresse de diffusion à partir d'un ordinateur situé sur le réseau local est transmis à tous les ordinateurs reliés au réseau.
<b>adresse de données</b>	Adresse IP pouvant servir d'adresse source ou cible de données. Une adresse de données permet l'envoi et la réception de données sur toutes les interfaces du groupe IPMP auquel elle appartient. En outre, le jeu d'adresses de données dans un groupe IPMP peut être utilisé de manière continue à condition qu'une interface du groupe soit en cours de fonctionnement.
<b>adresse de multidiffusion</b>	Adresse IPv6 identifiant un groupe d'interfaces d'une manière particulière. Un paquet envoyé à une adresse de multidiffusion est diffusé à toutes les interfaces du groupe. La fonctionnalité de l'adresse de multidiffusion IPv6 est similaire à celle de l'adresse de diffusion IPv4.
<b>adresse de site local (site-local-use)</b>	Désignation utilisée pour l'adressage sur un site unique.
<b>adresse de test</b>	Adresse IP dans un groupe IPMP à utiliser comme adresse source ou cible de test et non comme adresse source ou cible du trafic des données.
<b>adresse DESAPPROUEE</b>	Adresse IP ne pouvant pas servir d'adresse source pour les données d'un groupe IPMP. En règle générale, les adresses de test IPMP sont DESAPPROUEES . Toutefois, toute adresse peut être indiquée comme adresse DESAPPROUEE en vue d'empêcher son utilisation en tant qu'adresse source.
<b>adresse lien-local</b>	Dans IPv6, désignation utilisée en guise d'adresse d'une liaison simple lors d'une configuration d'adresse automatique, par exemple. Par défaut, l'adresse lien-local est créée à partir de l'adresse MAC du système.

<b>adresse privée</b>	Adresse IP impossible à acheminer via le réseau Internet. Les adresses privées peuvent être utilisées par des réseaux internes sur des hôtes n'ayant pas besoin d'établir une connexion Internet. Ces adresses sont définies dans <a href="http://www.ietf.org/rfc/rfc1918.txt?number=1918">Allocation d'adresses aux Internets privés (http://www.ietf.org/rfc/rfc1918.txt?number=1918)</a> et sont souvent appelées adresses "1918".
<b>adresse unicast</b>	Adresse IPv6 identifiant une interface unique sur un noeud IPv6. Le préfixe de site, l'ID du sous-réseau et l'ID de l'interface sont les trois composantes de l'adresse unicast.
<b>AES</b>	Standard de chiffrement avancé (Advanced Encryption Standard). Technique de chiffrement de données symétrique par blocs de 128 bits. Le gouvernement des Etats-Unis a adopté la variante Rijndael de l'algorithme comme norme de chiffrement en octobre 2000. AES remplace le chiffrement <a href="#">DES</a> comme norme administrative.
<b>association de sécurité</b>	SA, Security Association. Association définissant les propriétés en matière de sécurité entre un premier hôte et un deuxième hôte.
<b>attaque par réflexion</b>	Attaque consistant à envoyer à distance des paquets ICMP requête d'écho à une <a href="#">adresse de diffusion IP</a> ou à plusieurs adresses de diffusion dans le but de congestionner le réseau ou de provoquer de graves interruptions de service.
<b>attaque par jeu</b>	Dans IPsec, attaque impliquant la capture d'un paquet par un intrus. Le paquet stocké remplace ou réplique l'original par la suite. Pour se protéger contre ce type d'attaque, il suffit que le paquet contienne un champ qui s'incrémente pendant la durée de vie de la clé secrète assurant la sécurité du paquet.
<b>autorité de certification (CA)</b>	Organisation ou société "tiers de confiance" publiant des certificats numériques utilisés pour créer des signatures numériques et des bclés. L'Autorité de certification (CA) garantit l'identité d'une personne ayant reçu un certificat unique.
<b>base de données des stratégies de sécurité</b>	SPD, Security Policy Database. Base de données définissant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP afin de déterminer s'il est nécessaire de rejeter un paquet, de le transmettre en clair ou de le protéger avec IPsec.
<b>Blowfish</b>	Algorithme de chiffrement par bloc symétrique de longueur de clé variable (entre 32 et 448 bits). Son créateur, Bruce Schneier, affirme que Blowfish est optimisé pour les applications pour lesquelles la clé n'a pas besoin d'être régulièrement modifiée.
<b>CA</b>	Voir <a href="#">autorité de certification (CA)</a> .
<b>charge utile</b>	Données transportées dans un paquet. La charge utile n'inclut pas les informations d'en-tête nécessaires pour amener le paquet à destination.
<b>classe</b>	Dans IPQoS, groupe de flux de réseau dotés de caractéristiques identiques. Vous définissez les classes dans le fichier de configuration IPQoS.
<b>comptabilisation des flux</b>	Dans IPQoS, processus visant à collecter et à enregistrer les informations sur les flux de trafic. Pour ce faire, il convient de définir les paramètres du module <code>flowacct</code> dans le fichier de configuration IPQoS.
<b>compteur</b>	Module de l'architecture Diffserv mesurant le débit du trafic d'une classe particulière. L'implémentation IPQoS inclut deux compteurs, <code>tokenmt</code> et <code>tswtclmt</code> .
<b>configuration automatique</b>	Processus selon lequel un hôte configure automatiquement son adresse IPv6 à partir du préfixe de site et des adresses MAX locales.

<b>configuration automatique sans état</b>	Processus par lequel un hôte génère ses propres adresses IPv6 en combinant son adresse MAC et un préfixe IPv6 publié par un routeur IPv6 local.
<b>couche liaison</b>	Couche située immédiatement sous <a href="#">IPv4/IPv6</a> .
<b>cryptographie par clé asymétrique</b>	Système de chiffrement dans lequel l'expéditeur et le destinataire du message utilisent différentes clés pour chiffrer et déchiffrer le message. Les clés asymétriques servent à établir un canal sécurisé pour le chiffrement par clé symétrique. Le <a href="#">protocole Diffie-Hellman</a> est un exemple de protocole de clé asymétrique. Voir aussi <a href="#">cryptographie par clé symétrique</a> .
<b>cryptographie par clé publique</b>	Système cryptographique utilisant deux clés différentes : une clé publique connue de tous et une clé privée présentée exclusivement au destinataire du message. IKE fournit des clés publiques à IPsec.
<b>cryptographie par clé symétrique</b>	Système de chiffrement dans lequel l'expéditeur et le destinataire d'un message partagent une clé unique commune. Cette clé commune sert au chiffrement et au déchiffrement du message. Les clés symétriques permettent de chiffrer l'ensemble de la transmission de données dans IPsec. <a href="#">DES</a> est un exemple de système de cryptographie par clé symétrique.
<b>datagramme</b>	Voir <a href="#">datagramme IP</a> .
<b>datagramme IP</b>	Paquet d'informations transporté par IP. Un datagramme IP contient un en-tête et des données. L'en-tête inclut les adresses de la source et de la destination du datagramme. Les autres champs de l'en-tête permettent d'identifier et de recombinaison les données avec les datagrammes associés lorsqu'ils arrivent à destination.
<b>DES</b>	Standard de chiffrement de données (Data Encryption Standard). Méthode de chiffrement à clé symétrique mise au point en 1975 et normalisée par l'ANSI en 1981 car ANSI X.3.92. DES utilise une clé 56 bits.
<b>détection de défaillance</b>	Processus de détection intervenant lorsqu'une interface ou le chemin d'une interface vers un périphérique de couche Internet ne fonctionne plus. Le multipathing sur réseau IP (IPMP, IP Network Multipathing) inclut deux types de détection de défaillance : l'une utilise les liaisons (par défaut), l'autre les sondes (facultatif).
<b>détection de réparation</b>	Processus permettant de déterminer à quel moment une NIC ou le chemin de la carte vers un périphérique de couche 3 est de nouveau fonctionnel après un échec.
<b>détection de routeur</b>	Processus selon lequel les hôtes localisent des routeurs résidant sur une liaison directe.
<b>détection des voisins</b>	Mécanisme IP permettant à des hôtes de localiser d'autres hôtes résidant sur une liaison directe.
<b>DOI</b>	Un DOI (Domain of Interpretation, domaine d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.

<b>double pile</b>	Protocole TCP/IP intégrant IPv4 et IPv6 au niveau de la couche réseau, le reste de la pile étant identique. Lorsque vous activez le protocole IPv6 lors de l'installation d'Oracle Solaris, l'hôte reçoit la version double pile du protocole TCP/IP.
<b>DSA</b>	Algorithme de signature numérique (Digital Signature Algorithm). Algorithme de clé publique dont la longueur de clé varie de 512 à 4 096 bits. La norme du gouvernement américain, DSS, atteint 1 024 bits. L'algorithme DSA repose sur l'algorithme <a href="#">SHA-1</a> en entrée.
<b>DSCP</b>	DS Codepoint, point de code DS. Valeur de 6 bits qui, si elle figure dans le champ DS d'un en-tête IP, indique le mode de transfert d'un paquet.
<b>en-tête</b>	Voir <a href="#">en-tête IP</a> .
<b>en-tête d'authentification</b>	En-tête d'extension assurant l'authentification et l'intégrité des datagrammes IP, mais pas leur confidentialité.
<b>en-tête de paquet</b>	Voir <a href="#">en-tête IP</a> .
<b>en-tête IP</b>	Vingt octets de données identifiant de manière unique un paquet Internet. L'en-tête inclut l'adresse source et l'adresse de destination du paquet. Une partie facultative de l'en-tête permet d'insérer des octets supplémentaires.
<b>encapsulation</b>	Processus selon lequel un en-tête et une charge utile sont placés dans le premier paquet, puis insérés dans la charge utile du deuxième paquet.
<b>encapsulation IP-in-IP</b>	Mécanisme de mise en tunnel des paquets IP au sein de paquets IP.
<b>encapsulation minimal</b>	Forme facultative IPv4 de la mise en tunnel IPv4 prise en charge par les agents locaux, les agents étrangers et les noeuds mobiles. L'encapsulation permet d'économiser 8 ou 12 octets de surcharge par rapport à l'encapsulation IP-in-IP.
<b>filtrage de paquets</b>	Fonction de pare-feu pouvant être configurée pour autoriser ou interdire le transit de paquets particuliers via un pare-feu.
<b>filtre</b>	Ensemble de règles définissant les caractéristiques d'une classe dans le fichier de configuration IPQoS. Le système IPQoS sélectionne les flux de trafic conformes aux filtres du fichier de configuration IPQoS en vue de leur traitement. Voir <a href="#">filtrage de paquets</a> .
<b>filtre de paquets dynamique</b>	Voir <a href="#">filtre de paquets sans état</a> .
<b>filtre de paquets sans état</b>	<a href="#">filtrage de paquets</a> permettant de contrôler l'état des connexions actives et d'identifier, à l'aide des informations obtenues, les paquets du réseau autorisés à franchir le <a href="#">pare-feu</a> . En assurant le suivi et la coordination des requêtes et des réponses, un filtre de paquets sans état a la possibilité d'écarter une réponse non satisfaisante.
<b>gestion des clés</b>	La façon dont vous gérez les associations de sécurité.
<b>groupe anycast</b>	Groupe d'interfaces dotées de la même adresse anycast IPv6. L'implémentation du protocole IPv6 dans Oracle Solaris n'est pas compatible avec la création de groupes et d'adresses anycast. Cependant, les noeuds IPv6 Oracle Solaris peuvent assurer le transport du trafic vers des groupes anycast.

<b>groupe IPMP</b>	Groupe de multipathing sur réseau IP composé d'un jeu d'interfaces réseau et d'un jeu d'adresses de données que le système considère interchangeables afin d'améliorer la disponibilité et l'utilisation. Le groupe IPMP, y compris ses adresses de données et ses interfaces IP sous-jacentes, est représenté par une interface IPMP.
<b>HMAC</b>	Méthode de hachage à clé pour l'authentification de messages. HMAC est un algorithme d'authentification à clé secrète. HMAC est utilisé avec une fonction de repère cryptographique répétitive, telle que MD5 ou SHA-1, combinée avec une clé secrète partagée. La puissance cryptographique de HMAC dépend des propriétés de la fonction de repère sous-jacente.
<b>hôte</b>	Système qui n'effectue pas le transfert des paquets. Lors de l'installation d'Oracle Solaris, un système est désigné comme hôte par défaut et ne peut plus transmettre de paquets. Un hôte possède généralement une seule interface physique, mais peut également en avoir plusieurs.
<b>hôte multiréseau</b>	Système doté de plusieurs interfaces physiques et qui ne traite pas les paquets. Un hôte multiréseau peut exécuter des protocoles de routage.
<b>ICMP</b>	Internet Control Message Protocol, protocole Internet des messages de contrôle. Ce protocole sert à gérer les messages d'erreur ainsi que les messages de contrôle des échanges.
<b>ICMP requête d'écho</b>	Paquet transmis à une machine sur Internet en vue de solliciter une réponse. De tels paquets sont communément appelés paquets "ping".
<b>IKE</b>	Internet Key Exchange, échange de clé Internet. IKE automatise la mise en service de matériel d'identification authentifié pour les associations de sécurité IPsec.
<b>index du paramètre de sécurité</b>	SPI, Security Parameter Index. Nombre entier indiquant la rangée de la SADB qui permettra au récepteur de décrypter un paquet reçu.
<b>interface de réserve</b>	Interface physique prévue pour gérer le trafic des données uniquement en cas de défaillance d'une autre interface physique.
<b>interface physique</b>	Mode de raccordement d'un système à une liaison. Ce mode de raccordement est souvent mis en oeuvre sous la forme d'un pilote de périphérique et d'une NIC. Certaines cartes d'interface réseau (igb, par exemple) peuvent disposer de plusieurs points de connexion.
<b>interface réseau virtuelle (VNIC)</b>	Pseudo-interface offrant une connectivité réseau virtuelle qu'elle soit ou non configurée sur une interface réseau physique. Conteneurs tels que des zones IP exclusives ou des domaines xVM configurés sur des VNIC afin de former un réseau virtuel.
<b>IP</b>	Internet Protocol, protocole Internet. Méthode ou protocole utilisé pour envoyer les données d'un ordinateur à l'autre via Internet.
<b>IP</b>	Voir <a href="#">IP</a> , <a href="#">IPv4</a> , <a href="#">IPv6</a> .
<b>IPQoS</b>	Fonction logicielle qui permet l'implémentation du <a href="#">modèle Diffserv</a> standard en plus de la comptabilisation des flux et du marquage 802.1 D des réseaux locaux virtuels. A l'aide d'IPQoS, il est possible de fournir différents niveaux de services réseau aux clients et applications, comme indiqué dans le fichier de configuration IPQoS.
<b>IPsec</b>	Sécurité IP. Architecture de sécurité assurant la protection des datagrammes IP.

<b>IPv4</b>	Protocole Internet, version 4. IPv4 est parfois appelé IP. Cette version prend en charge un espace d'adressage à 32 bits.
<b>IPv6</b>	Protocole Internet, version 6. IPv6 prend en charge un espace d'adressage à 128 bits.
<b>liaison IP</b>	Utilitaire ou moyen de communication à l'aide duquel les noeuds peuvent communiquer dans la couche liaison. La couche liaison se trouve immédiatement sous IPv4/IPv6. Les réseaux Ethernet (simple ou reliés par un pont) ou les réseaux ATM sont des exemples de liaisons IP. Une liaison IP est définie par un ou plusieurs numéros ou préfixes de masque de sous-réseau IPv4. Un même numéro ou préfixe de masque de sous-réseau IPv4 ne peut pas être attribué à plusieurs liaisons IP. Dans le système ATM LANE, une liaison IP est un LAN à émulation simple. Lorsque vous utilisez le système ARP, la portée du protocole ARP correspond à une liaison IP simple.
<b>liste des certificats révoqués (LCR)</b>	Liste des certificats de clés publiques ayant fait l'objet d'une révocation par une CA. Les listes de certificats révoqués sont stockées dans la base de données des listes de certificats révoqués, gérée par IKE.
<b>MAC</b>	MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.
<b>marqueur</b>	<ol style="list-style-type: none"><li>1. Module de l'architecture diffserv et IPQoS attribuant une valeur au champ DS d'un paquet IP. Cette valeur indique la manière dont est traité le paquet. Dans l'implémentation IPQoS, le module du marqueur est ds cpmk.</li><li>2. Module dans l'implémentation IPQoS qui marque l'indicateur de réseau local virtuel d'un datagramme Ethernet par une valeur de priorité utilisateur. La valeur de priorité utilisateur indique comment les datagrammes sont transmis sur un réseau comportant des périphériques VLAN. Ce module est appelé dl cosmk.</li></ol>
<b>MD5</b>	Fonction de hachage cryptographique répétitive utilisée pour authentifier les messages, y compris les signatures numériques. Elle a été développée en 1991 par Rivest.
<b>modèle Diffserv</b>	Norme d'architecture du groupe IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet) destinée à l'implémentation de services différenciés sur les réseaux IP. Les modules principaux comprennent la classification, la mesure, le marquage, l'ordonnancement et le rejet. IPQoS implémente les modules de classification, de mesure et de marquage. Le modèle Diffserv est décrit dans le document RFC 2475, <i>An Architecture for Differentiated Services</i> .
<b>MTU</b>	Maximum Transmission Unit, unité de transmission maximale. Taille, exprimée en octets, des données pouvant être transmises via une liaison. Ainsi, la MTU d'une liaison Ethernet est de 1 500 octets.
<b>NAT</b>	Voir <a href="#">traduction d'adresses réseau</a> .
<b>NIC</b>	Network Interface Card, carte d'interface réseau. Carte réseau jouant le rôle d'interface d'un réseau. Certaines NIC ont plusieurs interfaces physiques. C'est le cas des cartes <i>igb</i> .
<b>noeud</b>	Dans IPv6, tout système IPv6, qu'il s'agisse d'un hôte ou d'un routeur.
<b>nom du keystore</b>	Nom qu'un administrateur attribue à une zone de stockage, ou keystore, sur une <a href="#">NIC</a> . Le nom du keystore est également appelé jeton ou ID de jeton.

<b>paquet</b>	Groupe d'informations transmis sous forme d'une unité sur les lignes de communications. Un paquet contient un <a href="#">en-tête IP</a> et une <a href="#">charge utile</a> .
<b>pare-feu</b>	Dispositif ou logiciel prévu pour isoler le réseau privé ou le réseau intranet d'une organisation d'Internet, afin de le protéger contre d'éventuelles intrusions. Un pare-feu peut inclure le filtrage de paquets, des serveurs proxy et les valeurs NAT (Network Address Translation, translation d'adresse réseau).
<b>périphérique VLAN</b>	Interface réseau permettant de renvoyer le trafic vers le niveau Ethernet (liaison de données) de la pile de protocole IP.
<b>PFS</b>	<p>Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.</p> <p>PFS s'applique à l'échange de clés authentifiées uniquement. Voir aussi <a href="#">protocole Diffie-Hellman</a>.</p>
<b>PHB</b>	Per-Hop Behavior, comportement par saut. Priorité accordée à une classe de trafic. Le comportement par saut indique la priorité des flux de cette classe par rapport aux autres classes de trafic.
<b>pile</b>	Voir <a href="#">pile IP</a> .
<b>pile de protocole</b>	Voir <a href="#">pile IP</a> .
<b>pile IP</b>	TCP/IP est souvent appelé une "pile". Ce terme fait référence aux couches (TCP, IP et parfois d'autres) par lesquelles transitent toutes les données aux extrémités client et serveur d'un échange de données.
<b>PKI</b>	Public Key Infrastructure, infrastructure de clé publique. Système de certificats numériques, d'autorités de certification et d'autres autorités d'enregistrement prévu pour vérifier et authentifier la validité de chaque partie impliquée dans une transaction Internet.
<b>priorité utilisateur</b>	Valeur de 3 bits ayant pour effet de mettre en oeuvre des marqueurs de classe de services, qui définissent la façon dont les datagrammes Ethernet sont transférés sur un réseau de périphériques VLAN.
<b>protocole de transport de contrôle de flux</b>	SCTP, Stream Control Transport Protocol. Protocole de la couche transport assurant des communications orientées connexion sous une forme similaire au protocole TCP. De plus, SCTP gère les multiréseaux (une des extrémités de la connexion peut être associée à plusieurs adresses IP).
<b>protocole Diffie-Hellman</b>	Egalement appelé cryptographie par clé publique. Protocole d'accord de clé cryptographique asymétrique mis au point par Diffie et Hellman en 1976. Ce protocole permet à deux utilisateurs d'échanger une clé secrète via un moyen non sécurisé sans secrets préalables. Diffie-Hellman est utilisé par le protocole IKE.
<b>protocole ESP</b>	Encapsulating Security Payload, association de sécurité. Extension de l'en-tête assurant l'intégrité et la confidentialité des datagrammes. ESP est l'un des cinq composants de l'architecture de sécurité IP (IPsec).
<b>publication des voisins</b>	Réponse à un message de sollicitation de voisinage ou processus selon lequel un noeud envoie des publications de voisinage non sollicitées pour signaler une modification de l'adresse de couche liaison.
<b>publication du routeur</b>	Processus selon lequel les routeurs annoncent leur présence (avec divers paramètres de connexion et paramètres Internet) de façon périodique ou en réponse à un message de sollicitation d'un routeur.

<b>reconfiguration dynamique</b>	Fonction permettant de reconfigurer un système en cours d'exécution sans incidence ou presque sur les opérations en cours. La reconfiguration dynamique n'est pas prise en charge par toutes les plates-formes Sun d'Oracle. Certaines plates-formes ne prennent en charge que la reconfiguration dynamique de certains types de matériel comme les NIC.
<b>redirection</b>	Dans un routeur, technique permettant de signaler à un hôte le meilleur noeud (prochain saut) en vue d'atteindre une destination particulière.
<b>reniflage</b>	Action d'espionner les communications des réseaux informatiques. Cette technique est fréquemment employée avec des programmes automatisés pour extirper hors ligne des informations telles que des mots de passe en clair.
<b>répartition de charge</b>	Processus consistant à distribuer le trafic entrant et sortant au sein d'un groupe d'interfaces. La répartition de charge permet d'augmenter le rendement. Elle ne se produit que lorsque le trafic réseau se dirige vers plusieurs destinations utilisant plusieurs connexions. Il existe deux types de répartition de charge : la répartition de charge entrante pour le trafic entrant et la répartition de charge sortante pour le trafic sortant.
<b>réseau virtuel</b>	Regroupement de ressources et fonctionnalités réseau logicielles et matérielles gérées en tant qu'entité logicielle unique. Un réseau virtuel <i>interne</i> regroupe les ressources réseau sur un seul système, parfois appelé "réseau en boîte".
<b>résultat</b>	Action à réaliser à l'issue de la mesure du trafic. Les compteurs IPQoS aboutissent à trois résultats signalés par la couleur rouge, jaune et verte. Vous définissez ces codes couleur dans le fichier de configuration IPQoS.
<b>routeur</b>	Système généralement composé de plusieurs interfaces ayant pour fonction d'exécuter des protocoles de routage et de transférer des paquets. Vous pouvez configurer un système à une seule interface en guise de routeur à condition que le système se trouve à l'extrémité d'une liaison PPP.
<b>RSA</b>	Méthode permettant d'obtenir des signatures numériques et des systèmes de cryptographie par clé publique. Cette méthode qui date de 1978 a été décrite par trois développeurs (Rivest, Shamir et Adleman).
<b>SA</b>	Voir <a href="#">association de sécurité</a> .
<b>SADB</b>	Security Associations Database, base de données des associations de sécurité. Table définissant les clés cryptographiques et les algorithmes cryptographiques. Les clés et les algorithmes ont pour intérêt de sécuriser la transmission des données.
<b>saut</b>	Mesure permettant l'identification du nombre de routeurs séparant deux hôtes. Si trois routeurs séparent une source et une destination, les hôtes se trouvent à quatre sauts l'un de l'autre.
<b>SCTP</b>	Voir protocole de transport de contrôle de flux.
<b>sélecteur</b>	Élément définissant de façon spécifique les critères à appliquer aux paquets d'une classe particulière en vue de sélectionner ce trafic dans le flux du réseau. Vous définissez les sélecteurs dans la clause de filtrage du fichier de configuration IPQoS.
<b>serveur proxy</b>	Serveur faisant l'interface entre une application client (telle qu'un navigateur Web) et un autre serveur. Ce type de serveur permet de filtrer les requêtes afin d'interdire l'accès à certains sites Web, par exemple.



<b>SHA-1</b>	Secure Hashing Algorithm, algorithme de hachage sécurisé. L'algorithme s'applique à toute longueur d'entrée inférieure à $2^{64}$ afin d'obtenir une synthèse des messages. L'algorithme SHA-1 sert d'entrée à l'algorithme DSA.
<b>signature numérique</b>	Code numérique associé à un message électronique qui identifie l'expéditeur de manière unique.
<b>sollicitation des voisins</b>	Sollicitation envoyée par un noeud afin de déterminer l'adresse de couche liaison d'un voisin. Une telle sollicitation consiste à vérifier qu'un voisin est toujours accessible par une adresse de couche liaison mise en cache.
<b>sollicitation du routeur</b>	Processus selon lequel les hôtes demandent à des routeurs de générer immédiatement des publications du routeur, et non pas lors de la prochaine exécution programmée.
<b>SPD</b>	Voir <a href="#">base de données des stratégies de sécurité</a> .
<b>SPI</b>	Voir <a href="#">index du paramètre de sécurité</a> .
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol, protocole de contrôle de la transmission/protocole Internet. TCP/IP est le langage de communication ou protocole de base sur Internet. Il peut également servir de protocole de communication sur un réseau privé (intranet ou extranet).
<b>traduction d'adresses réseau</b>	NAT, Network Address Translation. Traduction d'une adresse IP utilisée au sein d'un réseau sous une adresse IP différente connue au sein d'un autre réseau. Cette technique sert à limiter le nombre d'adresses IP globales nécessaires.
<b>Triple-DES</b>	Triple-Data Encryption, triple chiffrement des données. Méthode de chiffrement par clé symétrique. Elle nécessite une clé de 168 bits. L'abréviation de Triple-DES est 3DES.
<b>tunnel</b>	Chemin suivi par un <a href="#">datagramme</a> pendant son encapsulation. Voir <a href="#">encapsulation</a> .
<b>tunnel bidirectionnel</b>	Tunnel pouvant transmettre des datagrammes dans les deux directions.
<b>tunnel inverse</b>	Tunnel débutant à l'adresse d'hébergement du noeud mobile et se terminant au niveau de l'agent local.
<b>usurpation</b>	Action d'accéder par intrusion à un ordinateur en envoyant un message avec une adresse IP provenant prétendument d'un hôte de confiance. Pour ce faire, un pirate doit d'abord utiliser différentes techniques pour identifier l'adresse IP d'un hôte de confiance, puis modifier les en-têtes de paquets pour donner l'impression que les paquets proviennent de cet hôte.
<b>valeur de hachage</b>	Nombre généré à partir d'une chaîne de texte. Les fonctions de hachage garantissent que les messages transmis n'ont pas été sabotés. <a href="#">MD5</a> et <a href="#">SHA-1</a> sont des exemples de fonctions de hachage unidirectionnel.
<b>VPN</b>	Virtual Private Network, réseau privé virtuel. Réseau logique sécurisé utilisant des tunnels dans un réseau public tel qu'Internet.



# Index

---

## A

- Adresse lien-local, dans IPMP, 281
- Adresse MAC
  - Exigences pour IPMP, 302–304
  - Vérification de l'unicité, 181–183
- Adresses de données, *Voir* IPMP, adresses de données
- Adresses de test
  - Voir* IPMP, adresses de test
- Adresses IP, Propriétés, 187
- Agent LLDP, *Voir* LLDP, agents
- Allocation d'anneaux
  - Voir aussi* Groupement d'anneaux
  - Étapes d'implémentation, 399
  - Réseaux locaux virtuels, 398
- Allocation de CPU, 415–416
- Analyse de cibles dans IPMP, 278
- Anneau à jeton, Prise en charge d'IPMP, 303
- Anneaux, transmission et réception, 397–411
- Anneaux matériels, 397–411
- ATM, Prise en charge d'IPMP, 303

## B

- BSSID, *Voir* Wi-Fi

## C

- Carte d'interface réseau (NIC)
  - Paramètres de vitesse de liaison, 167–168
  - Paramètres Ethernet, 168–170

- Carte d'interface réseau (NIC) (*Suite*)
  - Propriétés publiques et privées des pilotes de NIC, 164
  - Remplacement, DR, 173
- Carte réseau (NIC)
  - Défaillance et basculement, 290
  - Reconfiguration dynamique, 289
  - Remplacement, avec la DR, 287–288, 317–319
- Cible de sonde, dans IPMP, Définition, 295
- Clients basés sur le matériel, 397
- Clients MAC, 397
  - Allocation d'anneaux, 399
  - Basé sur le logiciel, 397
  - Basé sur le matériel, 397
  - Configuration, 399
  - Logiciel, 403
  - Matériel, 399
- Configuration, Protection des liens, 389–391
- Configuration d'un commutateur
  - Mode de protocole LACP, 243
  - Topologie de groupement, 240
- Configuration de clé WEP, 219
- Configuration de commutateur, Modes de protocole LACP, 247
- Configuration de lien persistant, Création, 186
- Considérations de sécurité, Wi-Fi, 218
- Contrôle d'interface, Utilisation de la commande `ipadm`, 198
- Contrôle de l'utilisation du réseau, 423
- Contrôle des flux, *Voir* Flux
- Contrôle des ressources, *Voir* Gestion des ressources réseau

Couloirs réseau, 393

    Couloirs logiciels, 423

    Couloirs matériels, 423

CPU dédiés pour des interfaces, 415–416

CPU pool, propriété, 411

## D

Défaillances de groupe, IPMP, 283

Détection de défaillance, dans IPMP, 281, 290

    Basé sur sonde, 282–283

    Détection de défaillance basée sur les liaisons, 284

    Temps de détection, 282–283

Détection de défaillance basée sur les liaisons, 284

Détection de défaillance basée sur sonde, 282–283

*Voir aussi* IPMP, adresses de test

*Voir aussi* IPMP, sans adresse de test

    Adresses de test, 282–283

    Configuration de systèmes cible, 314–317

    Test transitif, 282

dladm, commande

    Configuration d'un VLAN, 256–259

    Configuration Wi-Fi, 213

    Gestion des ressources réseau, 395

    Liaisons de données

        Affichage d'attributs physiques, 161

        Affichage des informations, 162–163

        Modification de la taille de MTU, 165–167

        Renommage, 160

        Suppression de liaisons de données, 163

    Modification d'un groupement, 247

dlstat, commande, 423, 427

    show-phys, 430–431

## E

Équilibrage de charge, Groupement, 242

ESSID, *Voir* Wi-Fi

/etc/default/mpathd, fichier

*Voir* IPMP, fichier de configuration

## F

flowadm, commande, 416–421

    Gestion des ressources sur des flux, 395

flowstat, commande, 423

Flux, 394, 416–421

## G

Gestion des ressources réseau, 393

    Commandes dladm pour implémentation, 395

    Flux, 394

    Liaisons, 393

Groupe anonyme, 284, 291

Groupe IPMP, 291

*Voir aussi* Interface IPMP

    Affichage d'informations sur, 319–328

    Ajout d'une interface à un groupe, 310

    Ajout ou suppression d'adresses, 311–312

    Configuration avec DHCP, 304–306

    Connexion de nouvelles cartes réseau, via la  
        DR, 287

    Déconnexion de cartes réseau, via la DR, 287

    Défaillances de groupe, 283

    Déplacement d'une interface entre  
        groupes, 312–313

    Remplacement de cartes réseau, à l'aide de la  
        DR, 287–288

    Suppression d'une interface d'un groupe, 310–311

    Tâches de planification, 302–304

Groupement

    Conditions requises, 243

    Création, 245–247

    Définition, 239

    Fonction, 239

    Modification, 247

    Stratégie d'équilibrage de charge, 242

    Topologie

        Commutateur, 241

        Dos à dos, 241

Groupement d'anneaux

*Voir aussi* Allocation d'anneaux

    Dynamique and statique, 397–411

Groupement d'anneaux statique

*Voir* Groupement d'anneaux

## Groupement de liens, *Voir* Groupement

### Groupements

Suppression de liens, 249

#### Topologies

De base, 240

## I

### ifconfig, commande

et ipadm, commande, 204

Vérification de l'ordre des modules STREAMS, 303

in.mpathd, démon, *Voir* IPMP, in.mpathd, démon

### Interface

#### Configuration

Groupement, 245–247

Vérification de l'unicité d'une adresse

MAC, 181–183

VLAN, 251–265

### Interface de réserve

*Voir aussi* ifconfig, commande, options pour IPMP

Rôle dans un groupe IPMP, 279

### Interface inutilisable, 296

### Interface IPMP, 267–268, 292

Affichage d'informations sur, 319–328

Affiche d'informations à propos de, 272

Configuration pour groupes IPMP, 306–308

Panne d'interfaces sous-jacentes, 272

### Interface physique, 240–241

*Voir aussi* Interface

### Interface sous-jacente, 296

### Interfaces

#### Configuration

comme partie d'un VLAN, 256–259

Interfaces Wi-Fi, 212

Sur une liaison de données, 184

Création d'une configuration persistante, 186

De réserve, dans IPMP, 279

Détection de réparation avec IPMP, 284–286

Ordre des modules STREAMS sur une interface, 303

Types de configuration d'IPMP, 279

Types de Wi-Fi, 211

VLAN, 256–260

### Interfaces active-active, IPMP, 279

### Interfaces actives-actives

IPMP, 306–308, 308–309

Interfaces actives-de réserve, IPMP, 279

Interfaces sans fil, *Voir* Wi-Fi

ip-nospoof, Types de protection des liens, 388

### ipadm

set-addrprop, 187

show-addrprop, 187

ipadm, commande, Administration des propriétés

TCP/IP, 179

### ipadm, commande

Configuration d'interfaces IP, 183

Contrôle d'interfaces, 198

Création d'interfaces IPMP, 306–308

Définition des propriétés des adresses IP, 187

et ifconfig, commande, 204

Montage d'une interface, 184

Sous-commandes pour IPMP, 307

Suppression d'un interface, 245

### IPMP

Administration, 310–313

Adresses de données, 280

adresses de données, 288

Adresses de test, 280

Affichage d'informations avec ipmpstat, 319–328

Cible de sonde, 295

Composant logiciel, 278

Détection de défaillance, 281, 282–283, 290

Détection de réparation, 284–286

Exigences d'IP, 281

Exigences de base, 302–304

Fichier de configuration, 278, 316–317

Groupe anonyme, 284, 291

Groupement de liens, 270–271

in.mpathd, démon, 278, 283

Présentation, 268–269

Prise en charge d'Ethernet, 303

Prise en charge des anneaux à jeton, 303

Prise en charge du mode ATM, 303

Reconfiguration dynamique, 286–288, 289

Remplacement d'interfaces, DR, 317–319

Répartition de charge, 269, 293

Système cible, configuration, 315

Terminologie, 288

**IPMP (Suite)**

- Trafic de sondes, 282–283

- Types de configuration d'interface, 279

IPMP (multipathing sur réseau IP), *Voir* IPMP

ipmpstat, commande, 267–268, 279, 299, 319–328

**J**

Jumbo frames, Activation de la prise en charge, 165–167

**L**

LACP, Mode, 243

Liaisons de données

- Voir aussi* d'adm, commande

- Administration des propriétés de liaison, 158

- Affichage des informations, 162–163

- Configuration d'une interface IP via un lien, 184

- Conventions de nommage, 26–31

- Module STREAMS, 176–177

- MTU, tailles, 165–167

- Noms de liaison

  - Utilisation dans les configurations

    - IPMP, 271–272

- Noms de lien, 29–31

- Noms de liens, 26–31

- Paramètres de vitesse de liaison, 167–168

- Paramètres Ethernet, 168–170

- Règles d'utilisation des noms personnalisés, 30–31

- Renommage d'une liaison, 160

- Suppression de liaisons de données, 163

LLDP, 329

- Agents, 331–335

- Composants dans Oracle Solaris, 329–330

- Modes de fonctionnement, 331–335

- Unités TLV, 332–335

LLDPU, *Voir* LLDP, unités TLV

**M**

mac-nospoof, Types de protection des liens, 388

MIB, 331–335

Migration d'adresse, 268

- Voir aussi* IPMP, adresses de données

Mode de protocole LACP, Modification des modes de protocole LACP, 247

Mode FAILBACK=no, 285

MTU, *Voir* Unité de transmission maximale

MTU (Maximum Transmission Unit), 165–167

**N**

/net/if\_types.h, fichier, 303

netstat, commande, Vérification du flux de paquets sur un lien Wi-Fi, 217

Noms de liens, *Voir* Liaisons de données

Noms personnalisés, *Voir* Liaisons de données, noms de liens

Nouvelles fonctionnalités, Wi-Fi, 210

**P**

Paramètres TCP/IP, Paramétrage avec la commande ipadm, 179

Pile réseau, 22, 24

Planification des, VLAN, 255–256

Point actif, Wi-Fi

- Définition, 210

- Recherche de point actif, 211

Point d'accès, Wi-Fi, 210, 212

Point de connexion physique, 254

Ports privilégiés, Définition avec la commande ipadm, 194

Profil de configuration réseau (NCP, network configuration profile), 153–154

Protection des liens, 387–389

- Configuration, 389–391

**R**

Reconfiguration Coordination Manager (RCM, gestionnaire de coordination de reconfiguration), structure, 287–288

**Reconfiguration dynamique (DR)**

- Voir aussi* Carte d'interface réseau (NIC)
- Définition, 289
- Fonctionnant avec des interfaces, IPMP, 287
- Interopération avec IPMP, 286–288
- Remplacement des NIC, 173
- Utilisation avec des interfaces, IPMP, 287–288
- Utilisation des interfaces, IPMP, 317–319

**Reconfiguration dynamique (DR, Dynamic Reconfiguration), Flexibilité des noms de lien personnalisés, 31****Reconfiguration dynamique(DR), Interopération avec IPMP, 317–319****Répartition de charge, 269, 293****Ressource de pool de CPU, Affectation à des liaisons, 413****restricted, Types de protection des liens, 388****S****Statistique de trafic réseau, Par anneau, 430–431****Statistiques réseau, *Voir* Contrôle de l'utilisation du réseau****Stratégie pour le groupement, 242****STREAMS, modules, Liaisons de données, 176–177****Système cible, dans IPMP, Configuration manuelle, 315****T****Temps de détection de réparation, 284–286****Test transitif, 282****TLV, *Voir* LLDP, unités TLV****Trafic de sondes, 282–283****Trunking, *Voir* Groupement****Types de protection des liens, 388–389**

- ip-nospoof, 388
- mac-nospoof, 388
- restricted, 388

**U****Usurpation, Protection des liens, 387–389****V****Virtualisation et la qualité de service, 393****VLAN**

- Configuration, 251–265
- Création via groupement de liens, 259–260
- Définition, 251–265
- Exemple de scénario, 251
- Noms de VLAN, 254
- Piratage de point de connexion physique, 254
- Point de connexion physique, 254
- Topologie, 252–254

**VNIC**

- Affectation de ressources de pool de CPU, 413
- Montage, 379–383

**W****Wi-Fi**

- Basic Service Set ID (BSSID), 213
- Chiffrement d'une connexion, 218
- Connexion à un réseau Wi-Fi, 212, 213, 214
- Contrôle d'un lien, 216
- Définition, 210
- Exemple, définition de la vitesse d'un lien, 217
- Exemple de communication chiffrée, 220
- Exemple de configuration Wi-Fi, 215
- Extended Service Set ID (ESSID), 213
- Génération d'une clé WEP, 219
- Interfaces prises en charge, 211
- Liens Wi-Fi sécurisés, 218
- Norme IEEE 802.11, 210
- Point actif, 210
- Préparation d'un système pour l'exécution du Wi-Fi, 211
- Types de réseaux Wi-Fi, 210

