Gestion des liaisons de données réseau dans Oracle® Solaris 11.2

Référence: E53794-02
Septembre 2014

ORACLE®

Table des matières

Utilisation de la présente documentation

- **Aperçu** fournit un aperçu de des fonctionnalités avancées qui servent à gérer les liaisons de données réseau pour améliorer les performances réseau. Décrit comment combiner des combiner des liens en agrégations en utilisant le regroupement de jonction ou DLMP, diviser votre réseau en sous-réseau en utilisant des réseaux virtuels locaux, connecter des segments de réseau séparés en utilisant des ponts, échanger des informations de connectivité de réseau avec Link Lien Layer Discovery Protocol et gérer des réseaux convergents en utilisant data center bridging.
- **Public visé** : administrateurs système.
- Certaines **connaissances requises : expérience de** base connaissances en matière d'administration réseau avancés et.

Bibliothèque de la documentation des produits

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=E36784.

Accès aux services de support 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 si vous êtes malentendant.

Commentaires en retour

Faites part de vos commentaires sur cette documentation à l'adresse : http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

Introduction à Managing Network Datalinks

Ce chapitre présente les fonctionnalités avancées permettant de gérer les liaisons de données réseau, qui sont décrites dans les chapitres restants de ce manuel. La mise en oeuvre des différentes technologies décrites dans ce manuel dépend de circonstances spécifiques. De même, certaines configurations matérielles peuvent imposer l'utilisation d'un type spécifique de fonctionnalité. Inutile de suivre l'intégralité des procédures de configuration de ce manuel. Sélectionnez puis déployez les technologies qui répondent aux exigences de votre réseau.

Avant de mettre en place l'une des configurations décrites dans ce manuel, vous devez avoir effectué les tâches basiques de configuration et vous devez avoir une certaine expérience en matière de configuration de liaisons de données. Pour plus d'informations sur la configuration de base du réseau, reportez-vous à “ Configuration et administration des composants réseau dans Oracle Solaris 11.2 ”. Pour plus d'informations sur les éléments de la gestion de la liaison de données, reportez-vous au Chapitre 2, “ Administration de la configuration de liaisons de données dans Oracle Solaris ” du manuel “ Configuration et administration des composants réseau dans Oracle Solaris 11.2 ”.

Pour obtenir un récapitulatif des fonctionnalités de configuration dans Oracle Solaris, reportez-vous auChapitre 1, “ Récapitulatif de l’administration réseau d’Oracle Solaris ” du manuel “ Stratégies pour l’administration réseau dans Oracle Solaris 11.2 ”.

Ce chapitre aborde les sujets suivants :

Nouveautés dans Gestion des liaisons de données de réseau dans Oracle Solaris 11.2

Pour les clients existants, cette section met en évidence les changements majeurs dans cette version :

- **Détection de défaillance basée sur sonde dans une agrégation DLMP** détecte les pertes des liens et de la connectivité entre liens agrégés DLMP et cibles configurées. Ce type de détection de défaillance répond aux limites de votre mécanisme de détection de défaillance basée sur les liaisons, qui peut détecter uniquement les pannes dues à la perte de la connexion directe entre la liaison de données et l'instruction switch de saut suivant. Pour plus d'informations, reportez-vous à la section “Détection de défaillance dans un groupement DLMP” à la page 23.
- **Transmission des valeurs recommandées de la sélection de transmission améliorée (ETS)** dans Data Center Bridging (DCB) permet d'activer l'hôte Oracle Solaris pour recommander les partages de bande passante au noeud suivant dans le commutateur DCB. Pou plus d'informations, reportez-vous à “Recommandation de la configuration ETS aux homologues” à la page 117, “Définition des propriétés ETS de la liaison de données” à la page 114, et Exemple 6-8, “Affichage de la capacité de synchronisation des informations ETS de l'hôte local”.
- **Affichage de la valeur effective des propriétés de la liaison de données** – La sous-commande`dladm show-linkprop` a été améliorée et permet désormais afficher le champ `EFFECTIVE`pour certaines des propriétés de liaisons de données. Les valeurs correspondant au champ`EFFECTIVE` sont déterminées par le système en fonction de la disponibilité de la ressource périphérique, de la capacité du périphérique concerné sous-jacent ou par les négociations avec le pair. La valeur effective n'a pas besoin d'être identique aux valeurs configurées. Une liaison de données peur avoir une valeur effective, même si la propriété n'est pas configurée avec une valeur. Pour obtenir un exemple de l'affichage du champ `EFFECTIVE`, reportez-vous à “Définition des propriétés de liaison de données” à la page 111 etExemple 6-7, “Affichage des propriétés de liaison de données associées à ETS”.
- **Affichage des statistiques de pont** – La sous-commande `dlstat show-bridge` affiche les statistiques du pont et les statistiques des liens connectés à chaque pont ainsi que la vue imbriquée des statistiques du pont. Pour plus d'informations, reportez-vous à “Affichage des informations sur les ponts configurés” à la page 76.

Fonctionnalités et composants permettant de gérer les liaisons de données de réseau

La gestion des performances du réseau fait référence à l'utilisation de ces fonctions et technologies afin d'affiner le mode de traitement du trafic réseau par les systèmes. Les systèmes configurés à l'aide de ces technologies peuvent mieux gérer le trafic, ce qui contribue à améliorer les performances globales du réseau. Bien que ces fonctions concernent divers types d'opérations sur le réseau, ces résultats donnent la connectivité des avantages communs, tel que le réseau et l'efficacité d'administration réseau.

Groupement de liaisons

Les groupements de liaisons vous permettent de réunir plusieurs ressources de liaisons de données en vue de les administrer comme une seule unité. Vous pouvez améliorer la bande passante et garantir la haute disponibilité aux applications en combinant plusieurs cartes d'interface réseau physiques ensemble. Le groupement de liaisons des liaisons de données réseau permet de s'assurer qu'un système a un accès permanent au réseau. Le groupement de tronçons et le groupement DLMP forment les deux types de groupement de liaisons.

Le groupement de tronçon fournit une bande passante consolidée des liaisons de données sous-jacentes consolidées pour les clients configurés sur le groupement. Un groupement DLMP permet d'accroître la disponibilité sur plusieurs commutateurs pour les clients configurés sur le groupement. Groupement DLMP prend également en charge la détection de défaillance basée sur les liaisons et la détection de défaillance basée sur sonde afin de garantir une disponibilité continue du réseau pour envoyer et recevoir du trafic. Pour plus d'informations sur les différents types de groupement de liaisons et les procédures à suivre pour configurer et administrer les groupements de liaisons, reportez-vous au Chapitre 2, Configuration de la haute disponibilité à l'aide de groupements de liaisons.

Réseau local virtuel

Les réseaux locaux virtuels permettent de diviser le réseau en sous-réseaux sans avoir à ajouter de matériel dans l'environnement réseau physique. Par conséquent, les sous-réseaux sont virtuels et vous utilisez les mêmes ressources réseau physiques. Les réseaux VLAN fournissent des applications avec des sous-réseaux isolés de sorte que seules les applications dans le même VLAN puissent communiquer entre elles. Vous avez la possibilité de configurer plusieurs réseaux virtuels au sein d'une seule et même unité (comme un commutateur) en combinant des VLAN et Zones Oracle Solaris. Pour plus d'informations sur les procédures de configuration et de réseaux locaux virtuels (VLAN) et l'administration des VLAN, reportez-vous au chapitre Chapitre 3, Réseaux virtuels à l'aide de la configuration de réseaux locaux virtuels.

Passerelle Networks

Les ponts permettent de connecter des segments de réseau distincts, qui eux-mêmes relient des noeuds. Dans le cas d'une connexion par pont, les segments réseau reliés communiquent comme s'ils formaient un seul et même segment réseau. Les ponts utilisent un mécanisme de transmission de paquets pour connecter des sous-réseaux et activer un système pour transmettre des paquets à leur destination par le biais des routes de connexion les plus courtes. Pour plus d'informations sur les réseaux pontés et procédures d'administration d'administration, reportez-vous au Chapitre 4, Administration de fonctionnalités de pontage.

Lien Layer Discovery Protocol

LLDP Layer Discovery Protocol (lien) permet l'échange de la connectivité et la gestion des informations entre les systèmes du réseau dans le but d'en découvrir la topologie. Ces informations peuvent inclure les capacités du système, les adresses de gestion et d'autres informations relatives aux opérations du réseau. Le réseau de diagnostic utilise LLDP pour détecter les problèmes de service qui peuvent entraîner une connectivité réseau limitée ou dégradée. Pour plus d'informations sur LLDP et les procédures nécessaires à la configuration LLDP, reportez-vous au Chapitre 5, Echange d'informations sur la connectivité réseau avec Link Layer Discovery Protocol.

Data Center Bridging

La technologie Data Center Bridging (DCB) sert à gérer la bande passante , la priorité relative et le contrôle de flux partageant le même type de trafic lors du partage du même lien de réseau, par exemple, lors du partage d'une liaison de donnée entre les protocoles de réseau et de stockage. DCB permet des échanges d'informations avec les systèmes homologues sur les fonctions qui prennent en charge le réseau convergent avec LLDP. Les informations désignent les configurations qui modifient l'intégrité des paquets réseau, notamment dans les environnements soumis à un trafic important, comme les centres de données. DCB offre une infrastructure réseau efficace grâce à la consolidation du réseau SAN (Storage Area Network) et du réseau local (LAN) et réduit les coûts opérationnels et de gestion dans les centres de données.

Vous pouvez configurer les fonctions DCB, telles que le contrôle de flux basé sur la priorité (PFC) pour la prévention de perte de paquets et la sélection de transmission améliorée (ETS) pour le partage de bande passante entre les paquets en fonction des priorités de classe de service (CoS). Pour plus d'informations, reportez-vous auChapitre 6, Gestion des réseaux convergents avec Data Center Bridging.

♦ ♦ ♦ CHAPITRE 2

Configuration de la haute disponibilité à l'aide de groupements de liaisons

Ce chapitre fournit une présentation de groupements de liaisons et décrit les procédures pour configurer et administrer les groupements de liaisons.

Ce chapitre aborde les sujets suivants :

Présentation des groupements de liaisons

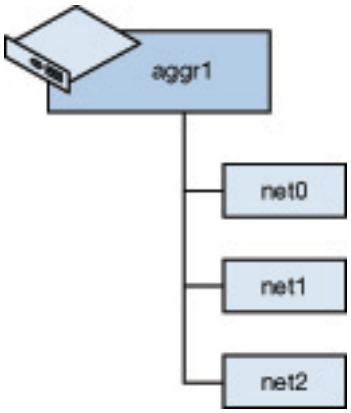
Le groupement de liaisons est la manière d'associer plusieurs liaisons de données sur un système physique afin d'améliorer la bande passante aux applications. Ces liaisons de données physiques sont configurées en une seule unité logique pour accroître le débit de trafic réseau ainsi que pour atteindre la haute disponibilité au la couche de liaison de données.

Vous pouvez inclure n'importe quel groupement de liaisons indiqué dans les cartes VNIC disponibles en tant qu'interface individuelle à l'aide d'Oracle Enterprise Manager Ops

Center. Vous pouvez également afficher les détails de l'agrégation DLMP en exécutant Oracle Enterprise Manager Ops Center. Pour plus d'informations sur Oracle Enterprise Manager Ops Center, reportez-vous à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=oc122&id=OPCCM.

Le schéma suivant illustre un groupement de liaisons configuré sur un système.

FIGURE 2-1 Configuration d'un groupement de liaisons



L'image illustre le groupement `aggr1` qui se compose de trois liaisons de données sous-jacentes, `net0`, `net1` et `net2`. Ces liaisons de données sont dédiées au trafic qui traverse le système par le biais du groupement. Les applications externes n'ont pas connaissance des liaisons sous-jacentes. Seule la liaison de données logique `aggr1` est accessible.

Avantages du groupement de liaisons

Le groupement de liaisons présente les avantages suivants :

- **Plus grande bande passante** – Les capacités de plusieurs liens sont réunies en un seul lien logique.
- **Le basculement et le rétablissement automatiques** : Le trafic sur un lien rompu est automatiquement commuté vers les autres liaisons actives du groupement, de façon à atteindre la haute disponibilité.
- **Amélioration de l'administration** : toutes les liaisons sous-jacentes sont administrées de manière unifiée.
- **Réduction du nombre de drains dans le pool d'adresses réseau** – Le groupement entier peut être assigné à une seule adresse IP.

Parce que les groupes de groupement de liaisons sont réunis une seule liaison de données logique, les fonctionnalités de liaisons de données comme la protection des liaisons et la gestion des ressources fonctionne correctement avec les groupements de liaisons. Pour plus d'informations sur la protection des jonctions, reportez-vous au Chapitre 1, “ Utilisation de la protection des liens dans des environnements virtualisés ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”. Pour plus d'informations sur la gestion des ressources, reportez-vous auChapitre 7, “ Gestion des ressources réseau ” du manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Certains des groupement de liaisons surmontent les problèmes qui surviennent lors de l'utilisation de fonctions de haute disponibilité grâce à la virtualisation du réseau, par exemple IPMP. Avec le groupement de liaisons, vous devez d'abord créer l'agrégation dans une zone globale, puis les indiquer en tant que lien sous-jacent lorsque vous configurez la zone non globale. Dès que la zone est initialisée, elle est affectée à une carte VNIC sur l'agrégation de liaison. Contrairement à IPMP, qui doit être configuré dans chaque zone non globale, les groupements de liaisons sont configurées dans les zones globales uniquement sur des VNIC afin de fournir hautement disponible et des zones non globales. La zone globale peut également configurer les propriétés (bande passante, par exemple) sur les cartes VNIC assignée à la zone.

Remarque - Les groupements de liaisons exécutent des fonctions similaires à la fonctionnalité de chemins d'accès multiples de réseau IP (IPMP) pour améliorer les performances et la disponibilité du réseau. Pour une comparaison de ces deux technologies, reportez-vous à l'Annexe A, Groupement de liaisons et IPMP : comparaison des fonctionnalités.

Les types de groupements de liaisons suivants sont pris en charge :

- Groupements de jonctions
- Groupements DLMP (Datalink Multipathing)

Pour plus d'informations sur les différences entre ces deux types d'agrégation de liaison, voir“Comparaison entre un groupement de jonctions et un groupement DLMP” à la page 42.

Groupements de jonctions

Les groupements de tronçons sont basées sur les normes IEEE 802.3ad et fonctionnent en permettant de répartir plusieurs flux de trafic sur un ensemble de ports agrégés. IEEE 802.3ad nécessite la configuration de commutateur et des extensions propriétaires de fournisseurs de commutateur afin de fonctionner sur plusieurs commutateurs. Dans les agrégations de tronçons, les clients configurés sur les agrégations obtiennent une bande passante consolidée des liens sous-jacents car chaque port de réseau est associé à chaque lien de donnée configurée de l'agrégation. Lorsque vous créez un groupement de liaisons par défaut, le groupement est créé en mode trunk. Vous pouvez utiliser un groupement de jonctions dans les cas suivants :

- Par exemple, si un système du réseau exécute des applications avec un fort trafic distribué, il convient de dédier un groupement de jonctions au trafic de ces applications pour profiter de la bande passante disponible.
- Pour les sites avec un espace d'adressage IP limité qui nécessite une grande bande-passante, vous avez besoin d'une seule adresse IP pour le groupement de jonctions des liens de données.
- Sur les sites sur lesquels il faut masquer tout lien de donnée interne, l'addresse IP du groupement de jonction masque ces liens de données des applications externes.
- Pour les applications qui ont besoin de groupement de jonctions fiable protège une connexion réseau, par rapport à un échec de liaison connexions réseau.

Le groupement de jonctions prend en charge les fonctionnalités suivantes :

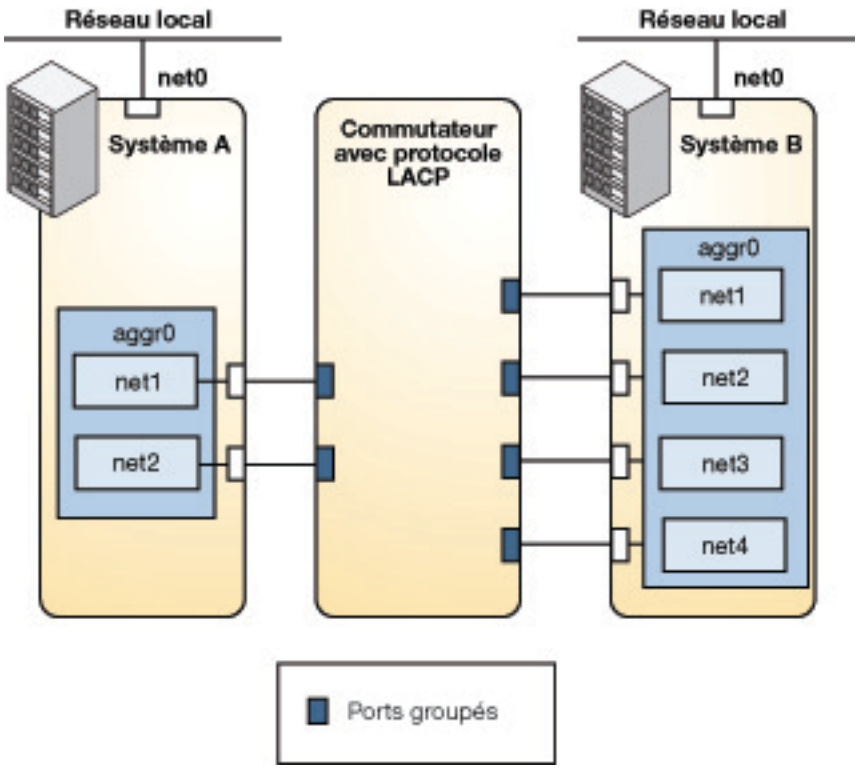
- Utilisation d'un commutateur
- L'utilisation d'un commutateur avec le LACP (Link Aggregation Control Protocol)
- Configuration dos-à-dos du groupement de jonction
- Stratégies et équilibrage de la charge

Les sections suivantes décrivent les fonctionnalités les groupements de jonctions.

Utilisation d'un commutateur

En règle générale, les systèmes configurés avec des groupements de jonctions utilisent également un commutateur externe pour se connecter à d'autres systèmes. La figure ci-après illustre un réseau local constitué de deux systèmes sur lesquels chaque système possède un groupement de jonctions configuré.

FIGURE 2-2 Groupement de jonctions utilisant un commutateur

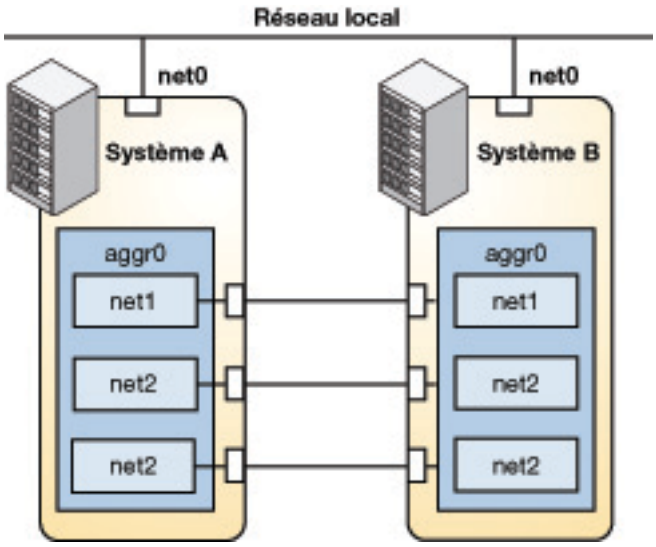


Les deux systèmes sont connectés par un commutateur. Le système A a un groupement de jonction composé de deux liens de données, `net1` et `net2`. Ces interfaces sont connectées au commutateur par le biais de ports groupés. Le système B possède un groupement de jonctions de quatre liaisons de données, `net1` à `net4`. Ces interfaces sont également connectées au commutateur par le biais de ports groupés. Dans cette topologie de groupement de jonctions, le commutateur doit prendre en charge les normes IEEE 802.3ad et les ports de commutateur doivent être configurés pour cette agrégation. Reportez - vous à la documentation du fabricant du commutateur pour configurer le commutateur.

Configuration dos-à-dos du groupement de jonction

Les groupements de jonctions prennent également en charge la configuration dos à dos. Au lieu d'utiliser un commutateur, deux systèmes sont connectés directement pour exécuter deux groupements parallèles, comme l'illustre le schéma suivant.

FIGURE 2-3 Configuration dos-à-dos du groupement de jonction



La figure illustre le groupement de jonctions `trunk0` du système A directement connecté au groupement de jonctions `trunk0` du système B par le biais de liaisons correspondantes entre leurs liaisons de données sous-jacentes respectives. Cette configuration permettent aux systèmes A et B d'assurer la redondance, la haute disponibilité, et la communication haut-débit entre les deux systèmes. Chaque système possède une interface `net0` dédiée au flux du trafic au sein du réseau local.

Les applications les plus courantes d'un groupement de jonctions dos à dos de groupement de jonctions est la configuration de serveurs de basée de données en miroir dans les centres de données. Il faut impérativement mettre à jour les deux serveurs en même temps, ce qui nécessite une large bande passante, un flux de trafic haut débit et une grande fiabilité.

Utilisation d'un commutateur avec le protocole de contrôle de groupement de liaisons

Si la configuration d'un groupement de jonctions a une bascule et le commutateur prend en charge le LACP, vous pouvez activer LACP pour le commutateur et le système. Reportez - vous à la documentation du fabricant du commutateur pour configurer le commutateur.

LACP permet à une unité de données la détection de liaison de données plus fiable qu'en cas d'échec. Sans LACP, le groupement de liaisons s'appuie uniquement sur l'état de la liaison signalé par le pilote du périphérique pour détecter la panne d'une liaison de données agrégée. Sans LACP, les LACPDU sont échangées à intervalles réguliers afin de vous assurer que les liaisons de données agrégées peuvent envoyer et recevoir du trafic. LACP détecte également certains cas de configuration incorrecte , par exemple, lorsque le regroupement des liaisons de données ne correspond pas entre les deux pairs.

LACP échange des trames d'échange spéciales (LACPDU) entre l'agrégation et le commutateur si LACP est activé sus le système. LACP utilise ses LACPDU pour maintenir l'état des liens de données agrégés.

La commande `dladm create-aggr` est utilisée pour configurer le LACP d'un groupement en un des trois modes suivants :

- `off` : mode par défaut des groupements. Le système ne génère aucun LACPDU.
- `active` : le système génère des unités de données LACP à intervalles réguliers.
- `passive` : le système génère une unité de données LACP uniquement quand il en reçoit une du commutateur. Si le commutateur et le groupement sont définis sur le mode `passive`, ils ne peuvent échanger aucun LACPDU.

  Pour plus d'informations sur la configuration LACP, reportez-vous à “Création d'un groupement de liaisons” à la page 27.

Définition de stratégies de groupement à des fins d'équilibrage de charge

Vous pouvez définir une stratégie pour le trafic sortant qui indique comment répartir la charge entre les différentes liaisons disponibles dans le cadre d'un groupement, établissant ainsi un équilibrage de charge. Vous pouvez utiliser les spécificateurs de charge suivants pour renforcer les diverses stratégies d'équilibrage de la charge :

- L2 : détermine la liaison sortante en hachant l'en-tête MAC (L2) de chaque paquet.
- L3 : détermine la liaison sortante en hachant l'en-tête IP (L3) de chaque paquet.

- L4 : détermine la liaison sortante 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.

Groupements DLMP (Datalink Multipathing)

Groupement DLMP est un type de groupement de liaisons qui assure la haute disponibilité sur plusieurs commutateurs sans qu'il soit nécessaire de configuration du commutateur. Groupement DLMP prend en charge la détection de défaillance basée sur les liaisons et la détection de défaillance basée sur sonde afin de garantir une disponibilité continue du réseau pour envoyer et recevoir du trafic.

Avantages de groupement DLMP

Le groupement DLMP offre les avantages suivants :

- Les normes IEEE 802.3ad implémentée par les groupements de honctions n'ont pas de provisions à répartir sur plusieurs commutateurs. Permettre le basculement entre plusieurs commutateurs en mode jonction (trunk) nécessite plusieurs extensions propriétaires de commutateurs qui ne sont pas compatibles entre les fournisseurs. Les groupements DLMP permettent le basculement entre plusieurs commutateurs sans nécessiter d'extension propriétaire.
- Utiliser IPMP pour la haute disponibilité dans le contexte de la virtualisation du réseau est très complexe. Un groupe IPMP ne peut pas être assigné directement dans une zone. Lorsque des cartes d'interface réseau (NIC) doivent être partagées entre plusieurs zones, vous devez configurer les VNIC de manière à ce que chaque zone obtienne une VNIC de chaque NIC physique. Chaque zone doit grouper ses VNIC dans un groupe IPMP pour obtenir une haute disponibilité. La complexité augmente au fur et à mesure que vous adaptez les configurations, dans un scénario qui inclut un grand nombre de systèmes, zones, cartes réseau, cartes réseau virtuelles (VNIC) et groupes IPMP, par exemple. Avec les groupements DLMP, vous créez une VNIC ou configurez la ressource `anet` d'une zone au-dessus de l'agrégation, et la zone voit une VNIC à haut niveau de disponibilité.
- Le groupement DLMP vous permet d'utiliser les fonctionnalités de couche de liaison comme la protection des liaisons, les flux définis par l'utilisateur et la personnalisation des propriétés de liaisons telles que la bande passante par exemple.

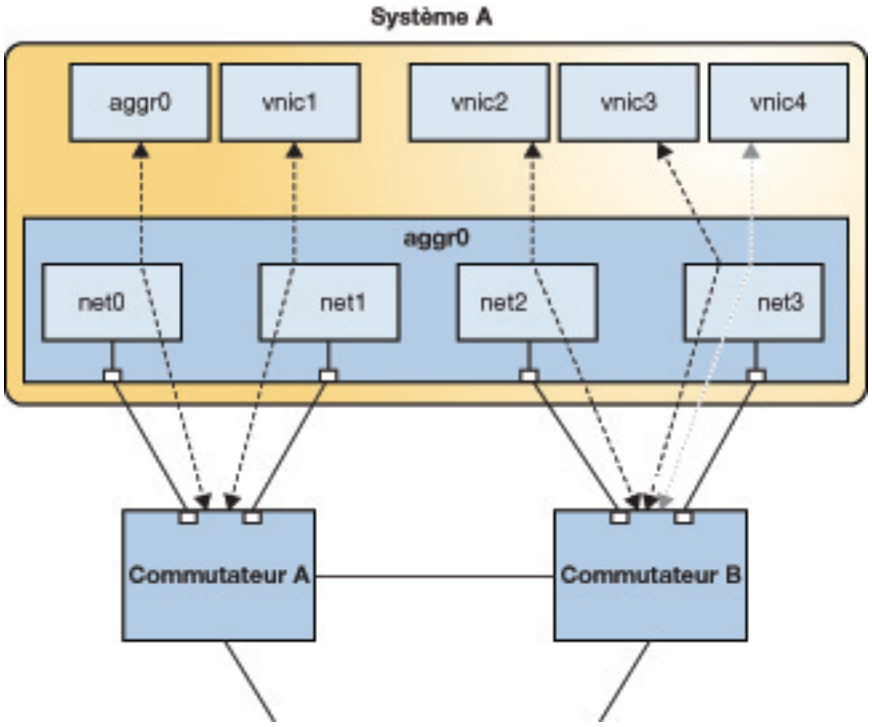
Remarque - IPMP vous ne devez pas configurer un groupe sur un groupement DLMP. Cependant, vous pouvez configurer un groupe sur un groupement de jonctions IPMP.

Fonctionnement du groupement DLMP

Dans un groupement de jonctions, chaque port est associé à chaque liaison de données configurée dans le groupement. Dans un groupement DLMP, un port est associé à l'une des du groupement de liaisons de données configurées.

Le schéma suivant illustre le fonctionnement d'un groupement DLMP.

FIGURE 2-4 Groupement DLMP



La figure illustre le système A, qui inclut le groupement de liaisons `aggr0`. Ce groupement se compose de quatre liaisons sous-jacentes (de `net0` à `net3`). Les cartes VNIC `vnic0` à `vnic4` sont configurées sur le groupement. Le groupement est connecté aux commutateurs A et B, eux-mêmes connectés aux autres systèmes de destination au sein du réseau élargi.

Les VNIC sont associées aux ports groupés via les jonctions sous-jacentes. Par exemple, dans la figure, `vnic0` à `vnic3` sont associées aux ports groupés sont via les liaisons sous-jacentes `net0`

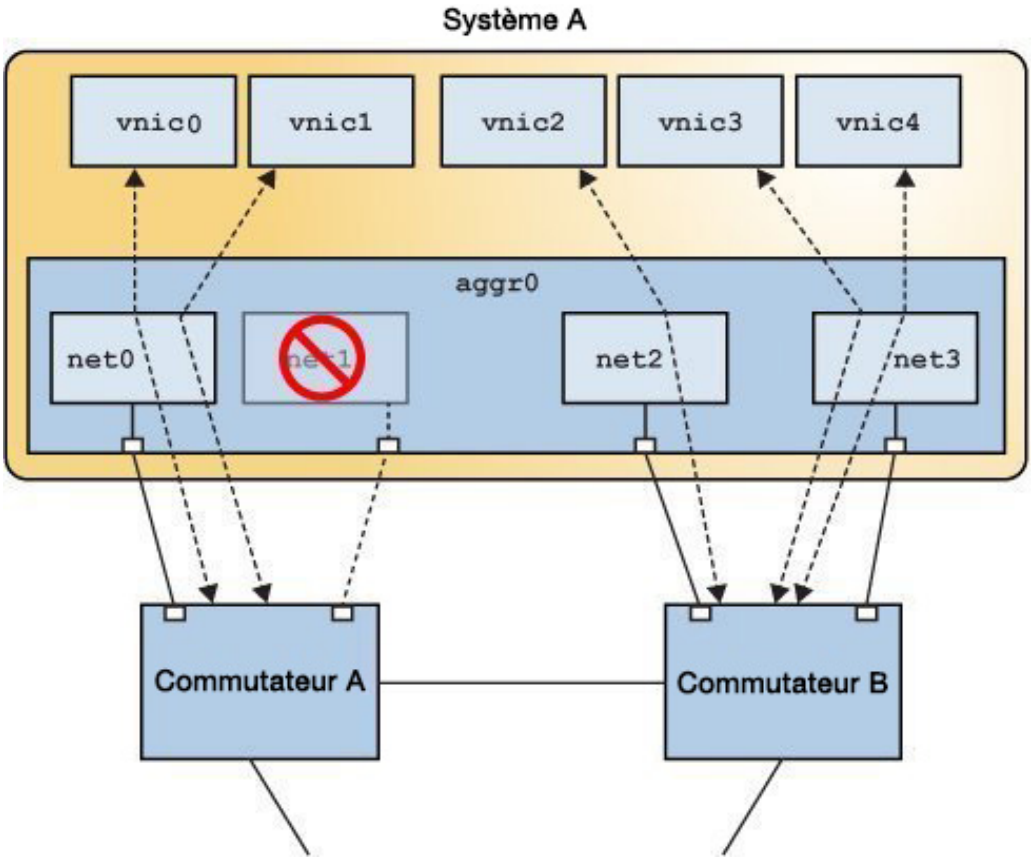
via net3. C'est - à - dire si le nombre de cartes réseau virtuelles et le nombre de liaisons sous-jacentes sont identiques, chaque port est associé à un jonction sous-jacent .

Si le nombre de cartes réseau virtuelles dépasse le nombre de liaisons sous-jacentes, un port individuel est associé à plusieurs liaisons de données. Par exemple, dans la figure le nombre total de cartes réseau virtuelles dépasse le nombre de liaisons sous-jacentes . Par conséquent, vnic4 partage un port avec vnic3.

Lorsqu'un port tombe en panne, tous les agrégées liaisons de données qui l'utilisent sont réparties sur les autres ports réseau haute disponibilité lors du changement de base. Par exemple, si net0 échoue, le port d'un groupement DLMP partage les ports restant net1 parmi les autres cartes VNIC. La distribution sur les ports du groupement se produit de manière transparente et indépendamment des commutateurs externes connectés au groupement.

La figure ci-dessous montre comment fonctionne quand un port d'un groupement DLMP échoue. Dans la figure, net1 a échoué, et la liaison avec net1 est hors service. vnic1 partage un port avec vnic0 via net0.

FIGURE 2-5 Groupement DLMP lorsqu'un port échoue



Détection de défaillance dans un groupement DLMP

La détection de défaillance dans un groupement DLMP est une méthode permettant de détecter l'échec des ports groupés. Un port est considéré comme étant en échec lorsqu'il ne réussit pas à envoyer ou recevoir du trafic. Le port peut échouer en raison des raisons suivantes :

- Sur les chemins de câbles ou des dommages de coupure
- Port de commutateur tombe en panne

- Chemin d'accès réseau en cas d'échec d'en amont

Groupement DLMP effectue une détection de défaillance sur les ports groupés afin de garantir une disponibilité continue du réseau pour envoyer ou recevoir le trafic. Quand un port échoue, les clients associés à ce port font l'objet d'un basculement vers un port actif. Les interfaces défaillantes restent inutilisables jusqu'à ce qu'elles soient réparées. Les interfaces actives restantes continuent de fonctionner et les interfaces de secours sont déployées en fonction des besoins. Après que le port en panne est rétabli après la défaillance, les clients d'autres ports actifs peuvent lui être associés.

DLMP basée sur les liaisons d'agrégation et prend en charge à la fois la détection de défaillance basée sur sonde.

Détection de défaillance basée sur les liaisons

La détection de défaillance basée sur les liaisons détecte la panne ou lorsque le câble de laquelle le commutateur signature et de port est down (arrêté). Par conséquent, il ne peut détecter les pannes dues aux la perte de la connexion directe entre (prochain saut) en liaison de données et de l'instruction switch. La détection de défaillance basée sur les liaisons est activée par défaut si un groupement DLMP est créé.

Détection de défaillance basée sur sonde

La détection de défaillance basée sur sonde de fin détecte les défaillances entre un hôte et le cibles configurées. Les limitations connues cette fonctionnalité de surmonte les la détection de défaillance basée sur les liaisons. La détection de défaillance basée sur sonde est utile lorsqu'un routeur par défaut est arrêté ou lorsque le réseau devient inaccessible. Le détecte la panne d'un groupement DLMP sonde via l'envoi et la réception de paquets.

Pour activer la détection de défaillance basée sur sonde dans groupement DLMP, vous devez configurer la propriété `probe-ip`.

Remarque - Dans un groupement DLMP, si `probe-ip` n'est configurée, la détection de défaillance basée sur sonde est désactivée ; seules la détection de défaillance basée sur les liaisons est utilisée.

Lors de la création de la première groupement DLMP, le service `svc:/network/dlmp:default` est activée automatiquement. Ce service démarre le démon `in.dlmpd` qui effectue la détection de défaillance basée sur sonde dans les groupements DLMP. Ce service est désactivé lorsqu'il n'y a pas de se trouve dans le système d'un groupement DLMP. Pour plus d'informations, reportez-vous à “Configuration de la détection de défaillance basée sur sonde pour un groupement DLMP” à la page 33.

La détection de défaillance basée sur sonde s'effectue à l'aide de la combinaison de deux types de sondes : ICMP (Internet Control Message Protocol, protocole sondes (L3)) (L2) et les sondes transitives, qui sont utilisées conjointement pour déterminer l'état d'une consolidation liaisons de données physiques.

- **Sondage ICMP**

  Vous pouvez configurer une liste séparée par des virgules de source cible les adresses IP et, éventuellement, une adresse IP ou le nom d'hôte. Adresse IP doit être la cible sur le même sous-réseau que l'adresse IP source indiqué. Vous pouvez spécifier l'origine dans quatre différentes formes adresse IP. Pour plus d'informations, reportez-vous à “Configuration de la détection de défaillance basée sur sonde pour DLMP” à la page 33

  Le sondage ICMP utilise les adresses IP sources configurées de la `probe-ip` uniquement si l'adresse IP est associée à des clients tels que les VNIC. Un port est associé à un client uniquement lorsqu'un port VNIC reçoit le trafic entrant et la transmet le trafic sortant pour ce client. A une heure donnée, le trafic de réception fonctionnel entrant ou sortant pour un client passe toujours par un seul port sous-jacent du groupement DLMP. Les adresses IP la propriété `probe-ip` sont utilisées pour surveiller l'état des ports que si les adresses IP sont associées à ce port.

  Pour chaque adresse, le démon `in.dlmpd` envoie périodiquement des paquets monodiffusion ICMP dirigés vers les cibles configurées. Si les adresses IP cibles ne sont pas configurés, `in.dlmpd` utilise la table de routage sur le même sous-réseau que l'adresse IP indiquée et utilise le prochain saut d'adresse comme adresse IP cible.

  Le trafic de sonde ICMP est envoyé uniquement par le biais du port associé avec ce client IP en question. Le port est marqué comme *ICMP failed* dans toutes les cibles devenir inaccessible pour ce port particulier. Le port est marqué comme*ICMP active* si au moins l'une des cibles est accessible depuis que le port par le biais d'une sonde ICMP.

- **Test transitif**

  Le test transitif est effectué lorsque l'état de l'état pour tous les ports réseau ne peut pas être déterminée par l'envoi de sondes ICMP. Par conséquent, le test transitif est exécuté lorsque le port n'est pas associé à l'adresse IP source configurée pour la propriété `probe-ip`. Par exemple, le test transitif est exécuté lorsque le un port IP n'est pas associé avec un client IP ou quand nombre d'adresses IP configurées de la propriété `probe-ip` est inférieur au nombre total de ports groupés. Des paquets de test sont envoyés à intervalles réguliers à partir des ports qui ne sont associés à aucun port client IP au pair. Si un port ICMP est en mesure d'accéder à port, ce port est considéré comme *L2 active*.

  Les paquets inclut Oracle Solaris pour les tests transitifs protocole exclusif qui sont transmis via le réseau. Pour plus d'informations, reportez-vous Annexe B, Format de paquet des sondes transitives.

La détection de défaillance basée sur sonde est effectuée dans la zone globale lorsque les VNIC sur un groupement sont créés dans la zone globale et sont affectées aux zones non globales. Trafic peut être toutefois, bien différenciées sonde la zone non globale à l'aide des VLAN. Par exemple, lorsque le trafic est exécuté sur un seul sonde dans une zone globale VLAN, la zone non globale du trafic VLAN peut être exécuté sur un autre.

Conditions requises pour créer des groupements de liaisons

la configuration des groupements de liaisons répond aux critères suivants :

- Les liaisons de données à configurer dans une agrégation ne doit pas comporter d'interface configurée via les IP.
- Vous pouvez créer des groupements de liaisons uniquement depuis la zone globale. Vous ne pouvez pas utiliser pour créer un groupement de liaisons de données à partir d'une zone non globale, même si vous ne disposez d'aucune interface IP configurée sur les liaisons de données. Groupement de liaisons de données. elle combine plusieurs cartes d'interface réseau physiques, mais uniquement dans une zone non globale toutes les interfaces sont virtuels. Par conséquent, vous ne pouvez pas créer un groupement de liaisons de la zone non globale.
- Toutes les liaisons de données du groupement doivent s'exécuter à la même vitesse et en mode duplex intégral.
- Dans un groupement DLMP, au moins un commutateur doit connecter le groupement aux ports d'autres systèmes. Vous ne pouvez pas établir une configuration dos à dos lors de la création d'un groupement DLMP.
- Sur les systèmes SPARC, chaque liaison de données doit posséder sa propre adresse MAC unique. Pour plus d'informations, reportez-vous à“ Garantie de l’unicité de l’adresse MAC de chaque interface ” du manuel “ Configuration et administration des composants réseau dans Oracle Solaris 11.2 ”.
- Les périphériques doivent prendre en charge les notifications relatives à l'état des liaisons (comme indiqué dans la norme IEEE 802.3ad de groupement de liaisons) pour qu'un port puisse se connecter ou se déconnecter d'un groupement. 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 “Création d'un groupement de liaisons” à la page 27.

Création d'un groupement de liaisons

Ports regroupe les sous-jacente groupement de liaisons dans un seul groupe logique. Ports l'agrégation exclusivement utilise ces sous-jacentes ; vous ne pouvez effectuer aucune autre opération telles que la configuration des adresses IP des cartes d'interface réseau virtuelles ou l'assignation à ces ports. Toutefois, vous pouvez configurer les VNIC sur l'agrégation des ports individuels sont et qui ne sont pas associées au port.

Vous devez préalablement lever les éventuels sur ces ports d'interface IP avant de créer le groupement de liaisons.

Vous pouvez également configurer un VLAN et créer des VNIC sur le groupement de liaisons que vous avez créées. Pour plus d'informations sur la création des VLAN sur groupements, reportez-vous à “Configuration de VLAN par le biais d'un groupement de liaisons” à la page 54.

Remarque - Les groupements de jonctions ne fonctionnent qu'avec des jonctions de même vitesse, en mode duplex intégral et point à point. Assurez-vous que les interfaces de votre groupement répondent à ces critères.

▼ Création d'un groupement de liaisons

Avant de commencer

Si vous créez un groupement de jonctions à un commutateur figure dans l'agrégation, configurez les ports du commutateur doivent pouvoir être utilisés en tant qu'agrégation sur le commutateur. Si le commutateur prend en charge le LACP, celui-ci doit être configuré en mode `active` ou `passive`

Reportez - vous à la documentation du fabricant du commutateur pour configurer le commutateur.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Afficher la liaison de données des informations permettant d'identifier les liaisons de données physiques pour l'agrégation.**

   ```
   # dladm show-phys
   ```

3. **Assurez-vous que la liaison de données que vous avez l'intention de mode "aggregate storage" ne sont pas utilisée par aucune application.**

   Par exemple, si une interface IP est créée sur la liaison de données, commencez par la supprimer.

   a. **Déterminer l'état de la liaison.**

      ```
      # ipadm show-if
      IFNAME       CLASS        STATE     ACTIVE     OVER
      lo0          loopback     ok        yes        --
      net0         ip           ok        no         --
      ```

      La sortie indique qu'une interface IP est configurée sur la liaison de données `net0`.

   b. **Supprimez l'interface IP.**

```
# ipadm delete-ip interface
```

Remplacez *interface* par le nom de l'interface IP configurée sur la liaison. Pour plus d'informations, reportez-vous à la page de manuel ipadm(1M).

4. Créez un groupement de liaisons.

```
# dladm create-aggr [-f] [-m mode] [-P policy]  [-L LACP-mode] \
[-T time] [-u address] -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.
`-m` *mode*	Mode doit être défini sur l'une des valeurs suivantes. Le mode par défaut est tronçon `trunk`. ■ `trunk` : groupement de liaisons mode norme IEEE 802.3ad ■ `dlmp` : mode liaison de données d'accès multiples (fonctionnalité multipathing) DLMP
`-P` *policy*	(Uniquement pour groupement de jonctions) Spécifie la stratégie d'équilibrage de la charge du groupement. Les valeurs prises en charge sont `L2`, `L3` et `L4`. Pour plus d'informations, reportez-vous à la section “Définition de stratégies de groupement à des fins d'équilibrage de charge” à la page 19.
`-L` *LACP-mode*	(Tronçon Spécifie le mode d'agrégation de uniquement LACP) s'il est utilisé. Les valeurs prises en charge sont `off`, `active` ou `passive`. Pour plus d'informations sur les modes, reportez-vous à “Utilisation d'un commutateur” à la page 16.
`-T` *time*	Tronçon d'agrégation (LACP uniquement) : indique la valeur de l'horloge LACP. Les valeurs prises en charge sont `short` ou `long`.
`-u` *address*	Spécifie l'adresse unicast fixe du groupement.
`-l` *linkn*	Spécifie les liaisons de données que vous souhaitez regrouper.
aggr	Spécifie le nom du groupement (n'importe quel nom personnalisé). Pour plus d'informations sur les règles pour affecter des noms, reportez-vous à “ Règles d’affectation de noms de liaison valides ” du manuel “ Configuration et administration des composants réseau dans Oracle Solaris 11.2 ”.

5. (Facultatif) Vérifiez le statut du groupement que vous venez de créer.

- Les groupements et jonctions avec les informations de statut affichées.

```
# dladm show-link
```

- Afficher le statut et la par groupement possède des informations sur les ports.

```
# dladm show-aggr -x
```

L'état du groupement doit être en fonctionnement `up`.

Exemple 2-1 Création d'un groupement de jonctions

Cet exemple montre les commandes utilisées pour créer un groupement de liaisons avec deux liaisons de données sous-jacentes, `net0` et `net1`. Le groupement est également configuré pour transmettre des paquets LACP. Dans cet exemple, il faut commencer par supprimer les interfaces IP configurées sur les liaisons de données sous-jacentes.

```
# ipadm show-if
IFNAME       CLASS        STATE     ACTIVE     OVER
lo0          loopback     ok        yes        --
net0         ip           ok        no         --
# ipadm delete-ip net0
# dladm create-aggr -L active -l net0 -l net1 trunk0
# dladm show-aggr -x
LINK       PORT           SPEED DUPLEX   STATE     ADDRESS            PORTSTATE
trunk0     --             1000Mb full    up        8:0:27:49:10:b8    --
           net0           1000Mb full    up        8:0:27:49:10:b8    attached
           net1           1000Mb full    up        8:0:27:e4:d9:46    attached
```

Exemple 2-2 Création d'un groupement DLMP et à la section Configuring an IP Interface en haut du d'agrégation

Cet exemple illustre la création d'un groupement DLMP. Comprenant trois liaisons de données sous-jacentes, `net0`, `net1` et `net2`. Une interface IP est créée par-dessus du groupement `aggr0` et une VNIC `vnic1` est créée au-dessus.

```
# dladm create-aggr -m dlmp -l net0 -l net1 -l net2 aggr0
# dladm show-link
LINK      CLASS     MTU     STATE   OVER
net0      phys      1500    up      --
net1      phys      1500    up      --
net2      phys      1500    up      --
aggr0     aggr      1500    up      net0 net1 net2
# dladm show-aggr -x
LINK       PORT           SPEED DUPLEX   STATE     ADDRESS            PORTSTATE
aggr0      --             1000Mb full    up        8:0:27:49:10:b8    --
           net0           1000Mb full    up        8:0:27:49:10:b8    attached
           net1           1000Mb full    up        8:0:27:e4:d9:46    attached
           net2           1000Mb full    up        8:0:27:38:7a:97    attached
# ipadm create-ip aggr0
# ipadm create-addr -T static -a local=10.10.10.1 aggr0/v4
```

```
# dladm create-vnic -l aggr0 vnic1
```

Étapes suivantes Vous pouvez le configurer plus précisément, telles que la création d'interfaces IP d'agrégation et des VNIC. Vous pouvez utiliser le groupement créé pour la configuration à la fois des zones non globales et de noyau zones.

- Pour plus d'informations sur la création d'interfaces IP, reportez-vous au Chapitre 3, " Configuration et administration des interfaces et adresses IP dans Oracle Solaris " du manuel " Configuration et administration des composants réseau dans Oracle Solaris 11.2 ".
- Pour plus d'informations sur la configuration des VLAN sur un groupement de liaisons, reportez-vous à "Configuration de réseaux VLAN via un groupement de liaisons" à la page 54.
- Pour plus d'informations sur la configuration des cartes d'interface réseau virtuelles, reportez-vous à " Configuration des cartes VNIC et des etherstubs " du manuel " Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ".
- Pour plus d'informations sur la configuration des zones, reportez-vous à " Création et utilisation des zones Oracle Solaris ".

Ajout d'une liaison à un groupement

Vous pouvez inclure d'autres liaisons de données à une agrégation existante. Si vous ajoutez des liaisons de données pour un groupement de jonctions, il peut être nécessaire de reconfigurer le commutateur pour s'adapter aux autres liaisons de données même si LACP est configuré sur le commutateur.

▼ Ajout d'une liaison à un groupement

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Assurez-vous qu'aucun des interfaces IP sont configurées sur la liaison. Interface IP est le cas échéant, supprimez cette interface IP configurée.**

   ```
   # ipadm show-if
   # ipadm delete-ip interface
   ```

   Remplacez *interface* par l'interface IP configurée sur la liaison de données.

3. **Ajoutez la liaison au groupement.**

```
# dladm add-aggr -l link [-l link] [...] aggr
```

Remplacez *link* par la liaison de données à ajouter au groupement et *aggr* par le nom du groupement.

4. **Les groupements (tronçon) Si nécessaire, reconfigurez le commutateur.**
Vous devrez éventuellement reconfigurer le commutateur pour s'adapter aux autres liaisons de données en fonction de la manière dont est configuré, même si commutateur est activé sur le commutateur LACP.
Reportez-vous à la documentation du commutateur pour effectuer les tâches de reconfiguration du commutateur.

Exemple 2-3 Ajout d'une liaison à un groupement

Cet exemple illustre comment ajouter une liaison au groupement `aggr0`.

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1
net3     phys      1500    up        --
# ipadm delete-ip net3
# dladm add-aggr -l net3 aggr0
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1 net3
net3     phys      1500    up        --
```

Retrait d'une liaison d'un groupement

Vous pouvez supprimer les liaisons de données individuelles associées à un groupement à l'aide de la commande `dladm remove-aggr`. Vous devez effectuez la reconfiguration du commutateur lorsque vous supprimez des jonctions de l'agrégation.

Connectez - vous en tant qu'administrateur et utilisez la commande suivante :

```
# dladm remove-aggr -l link aggr
```

EXEMPLE 2-4 Retrait d'une liaison d'un groupement

Cet exemple illustre comment retirer une liaison du groupement `aggr0`.

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1 net3
net3     phys      1500    up        --
# dladm remove-aggr -l net3 aggr0
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1
net3     phys      1500    unknown   --
```

Modification d'un groupement de jonctions

Vous pouvez modifier les attributs sélectionnés comme`policy`, `lacpmode` et `time` pour le groupement de jonctions. Ces attributs ne sont pas pris en charge dans les groupements DLMP.

- Pour modifier la stratégie d'équilibrage de charge du groupement, connectez-vous en tant qu'administrateur et exécutez la commande suivante :

  # dladm modify-aggr -P *policy aggr*

  policy — Représente une ou plusieurs des règles d'équilibrage de charge telles que L2, L3 et L4 expliquées dans l"Définition de stratégies de groupement à des fins d'équilibrage de charge" à la page 19.

  aggr — Spécifie le groupement dont vous souhaitez modifier la stratégie.

- Pour modifier le mode LACP du groupement, connectez-vous en tant qu'administrateur et utilisez la commande suivante :

  # dladm modify-aggr -L *LACP-mode* **-T** *time aggr*

  -L *LACP-mode* — Indique le mode dans lequel le groupement LACP doivent être compatibles. Les valeurs de cette variable sont les suivantes : `active`, `passive` et `off`.

  -T *time* — Indique la valeur de l'horloge du LACP (`short` ou `long`).

  aggr — Spécifie le groupement dont vous souhaitez modifier le mode LACP.

EXEMPLE 2-5 Modification d'un groupement de jonctions

Cet exemple montre comment modifier la stratégie d'équilibrage de charge due groupement de liaisons `aggr0` sur L2 et comment modifier le mode LACP et à l'état `active`.

```
# dladm modify-aggr -P L2 aggr0
# dladm modify-aggr -L active -T short aggr0
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   trunk      L2      auto            active         short
```

Configuration de la détection de défaillance basée sur sonde pour un groupement DLMP

Vous devez configurer la propriété `probe-ip` pour un groupement DLMP pour activer les sondes. Dans le cas contraire, un Cross-Probing uniquement est désactivée par défaut et la détection de défaillance basée sur les liaisons est utilisée. Pour plus d'informations, reportez-vous à la section “Détection de défaillance dans un groupement DLMP” à la page 23.

Les propriétés de liaison de données suivantes permettent de configurer la détection de défaillance basée sur sonde, procédez comme suit :

- `probe-ip` :cette option permet de spécifierdes adresses IP source en les séparant par des virgules et l'adresse IP a cible ou le nom d'hôte. Utilisation d'adresses de la source pour ICMP IP sondes. La liste des adresses IP source est suivi d'une adresse de cible optionnelles. Adresse IP doit être la cible sur le même sous-réseau que l'adresse IP source indiqué.

  Vous pouvez utiliser le signe + pour séparer les source à partir de la cible. Vous pouvez indiquer les cibles en tant qu'adresse IP ou le nom d'hôte de la cible. Pour plus d'informations sur la façon d'indiquer les adresses source et de l'adresse cible, reportez-vous à “Configuration de la détection de défaillance basée sur sonde pour DLMP” à la page 33.
- `probe-fdt` : cette option permet de spécifier le temps de détection de défaillance. Vous pouvez configurer le temps de détection de défaillance attendue de la valeur en secondes. La valeur par défaut est 10 secondes.

▼ Configuration de la détection de défaillance basée sur sonde pour DLMP

Avant de commencer

Création d'un groupement DLMP. Pour plus d'informations, reportez-vous à“Création d'un groupement de liaisons” à la page 27.

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **(Facultatif) Afficher toutes les d'agrégation agrégations existantes pour la configuration pour identifier la détection de défaillance basée sur sonde.**

   ```
   # dladm show-aggr
   ```

3. **Définir les cibles pour le groupement sonde pour lequel vous souhaitez configurer la détection de défaillance basée sur sonde.**

   ```
   # dladm set-linkprop -p probe-ip=IP-address[/prefix-length]|hostname+[target] aggr
   ```

   Les adresses source et de destination pour la propriété `probe-ip` peuvent être définies comme suit :

   - `probe-ip=`*IP-address*[/*prefix-length*]|*hostname*+[*target*]

     Adresse IP et sa longueur de préfixe. Par exemple, `10.130.10.1/24+`.
   - `probe-ip=`*addr-obj-name*+[*target*]

     Nom d'objet d'adressage. Par exemple, `vnic1/addr1+192.168.0.1`.
   - `probe-ip=`*interface-name*+[*target*]

     Nom d'interface. il peut s'agir d'un nom du groupement VNIC lui-même ou n'importe quelle interface configurée sur le groupement. Par exemple, `[aggr1]+`.
   - `probe-ip=+`[*target*]

     Aucun vous indiquez une adresse IP. Lorsque les données d'origine vous n'avez pas indiqué l'adresse IP, toutes les adresses IP et configuré sur le pris en compte d'agrégation en tant que les cartes VNIC sont des adresses IP d'origine potentiel de sondes ICMP. Par exemple : `+10.130.10.1`.

4. **(Facultatif) Définir le temps de détection de défaillance.**

   ```
   # dladm set-linkprop -p probe-fdt=fdt aggr
   ```

   Où *fdt* est le temps de détection de défaillance exprimé en secondes. La valeur par défaut est 10 secondes.

5. **(Facultatif) Reportez - vous à la affichage sonde le groupement afin de les informations connexes.**

   ```
   # dlstat show-aggr -n -P [[t],[i],[all]]
   ```

Exemple 2-6 Configuration de la détection de défaillance basée sur sonde

1. Afficher les agrégations existantes.

```
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   dlmp       --      --              --             --
aggr1   dlmp       --      --              --             --
```

2. Définir les cibles pour la sonde `aggr1`.

```
# dladm set-linkprop -p probe-ip=+ aggr1
```

   Vu que l'adresse IP source n'est pas spécifiée, toutes les adresses IP configurées sur le groupement `aggr1` et toutes les cartes VNIC de deviennent des adresses IP sources des sondes ICMP.

3. Définir le temps de détection de défaillance.

```
# dladm set-linkprop -p probe-fdt=15 aggr1
```

4. Afficher les propriétés qui sont définies.

```
# dladm show-linkprop -p probe-ip,probe-fdt aggr1
LINK     PROPERTY         PERM   VALUE           EFFECTIVE    DEFAULT      POSSIBLE
aggr1    probe-ip         rw     192.168.85.137  --           --        --
aggr1    probe-fdt        rw     15              15           10          1-600
```

5. Les sondes les statistiques de l'affichage pour l'agrégation.

```
# dlstat show-aggr -n -P t,i aggr1
TIME   AGGR   PORT  LOCAL           TARGET          PROBE  NETRTT     RTT
0.45s  aggr1  net0  net0            net1            t16148  --         --
0.45s  aggr1  net0  net0            net1            t16148  0.63ms     0.81ms
1.08s  aggr1  net1  net1            net0            t16148  --         --
1.08s  aggr1  net1  net1            net0            t16148  0.72ms     0.99ms
2.07s  aggr1  net1  192.168.85.137  192.168.85.137  i15535  --         --
2.07s  aggr1  net1  192.168.85.137  192.168.85.137  i15535  0.18ms     0.54ms
```

Surveillance de la détection de défaillance basée sur sonde

Vous pouvez surveiller la détection de défaillance basée sur sonde à l'aide des commandes `dladm show-aggr`, `dlstat show-aggr` et `ipadm show-addr`

EXEMPLE 2-7 La section Probe-Informations connexes l'affichage

L'exemple suivant affiche les statistiques des sondes pour un groupement DLMP. Avec l'option de type de sonde `-P`, vous pouvez fournir une liste d'arguments séparés par des virgules (`t` pour test transitif, `i` pour sonde ICMP et `all` pour sondes ICMP et tests transitifs) dans la commande`dlstat show-aggr` pour affichage du type les sondes de la sonde respective.

```
# dlstat show-aggr -n -P t,i aggr1
   TIME     AGGR     PORT   LOCAL        TARGET       PROBE  NETRTT     RTT
   0.53s    aggr1    net0   net0         net1         t16148  --         --
   0.53s    aggr1    net0   net0         net1         t16148  0.62ms     0.87ms
   1.17s    aggr1    net1   net1         net0         t16148  --         --
   1.17s    aggr1    net1   net1         net0         t16148  0.72ms     0.99ms
   2.24s    aggr1    net1   192.168.0.1  192.168.0.2  i15535  --         --
   2.24s    aggr1    net1   192.168.0.1  192.168.0.2  i15535  0.11ms     0.55ms
```

`TIME` L'heure auxquelles la sonde est envoyée en secondes. Cette information concerne l'heure à laquelle vous envoyez la commande `dlstat`. Si la sonde est envoyée avant d'exécuter la commande `dlstat`, le temps est négatif.

`aggr` Nom de l'agrégation pour lequel l'échantillon est envoyé.

`LOCAL` Adresse IP ICMP de sondes : les sondes source.

Nom de port des sondes transitives à partir de laquelle le : sonde transitive provient.

`TARGET` Adresse IP ICMP de sondes : les sondes de destination.

Nom de port des sondes transitives sonde : qui cible de la.

`PROBE` Sonde représentant le numéro d'identifiant. Le préfixe `t` est le préfixe pour les tests transitifs pour et le préfixe `i` est pour les sondes ICMP.

`NETRTT` Temps d'aller-retour réseau pour la sonde. Cette valeur est la période de temps s'écoulant entre l'envoi de la sonde et la réception de l'accusé de réception par le groupement DLMP.

`RTT` Temps total d'aller-retour réseau pour la sonde. Cette valeur est la période de temps s'écoulant entre l'envoi de la sonde d'accusé de réception et à l'exécution de la par le processus groupement DLMP.

Pour plus d'informations, reportez-vous à la page de manuel `dlstat`(1M).

EXEMPLE 2-8 Affichage des informations détaillées sur la agrégés port

L'exemple suivant affiche les informations d'agrégation détaillées sur chaque port sous-jacent .

```
# dladm show-aggr -x
LINK        PORT    SPEED   DUPLEX   STATE    ADDRESS            PORTSTATE
aggr1       --      100Mb   full     up       1e:34:db:fa:50:a2  --
            net0    100Mb   full     up       1e:34:db:fa:50:a2  attached
            net1    100Mb   full     up       b2:c0:6a:3e:c5:b5  attached
```

Pour plus d'informations, reportez-vous à la page de manuel `dladm`(1M).

EXEMPLE 2-9 L'affichage des ports de l'état du agrégés

L'exemple suivant indique l'état de l'les ports cible du groupement et des adresses IP des ports.

```
# dladm show-aggr -S -n
LINK       PORT       FLAGS   STATE    TARGETS        XTARGETS
aggr1      net1       u--3    active   192.168.0.2    net0
--         net0       u-2-    active   --             net1
```

EXEMPLE 2-10 Affichage des valeurs de propriété `probe-ip`

L'exemple suivant affiche des informations détaillées pour une propriété de jonction `probe-ip` pour le groupement DLMP spécifié.

```
# dladm show-linkprop -p probe-ip aggr1
LINK     PROPERTY         PERM   VALUE         EFFECTIVE    DEFAULT      POSSIBLE
aggr1    probe-ip         rw     192.168.0.2   192.168.0.2  --           --
```

EXEMPLE 2-11 En affichant la boîte de l'adresse IP et le département du d'agrégation

L'exemple suivant illustre l'affichage et l'état d'adresse IP de l'agrégation.

```
# ipadm show-addr aggr1
ADDROBJ           TYPE     STATE        ADDR
aggr1/local1      static   ok           192.168.0.1/24
```

Suppression d'un groupement de liaisons

Vous pouvez supprimer un groupement de liaisons à l'aide de la commande `dladm delete-aggr`. Vous devez supprimer l'interface IP et sur le groupement de liaisons les cartes VNIC configurées avant de supprimer l'agrégation.

▼ Suppression d'un groupement de liaisons

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Supprimez l'interface IP configurée sur le groupement de liaisons.**

   ```
   # ipadm delete-ip IP-aggr
   ```

Remplacez *IP-aggr* par l'interface IP configurée sur le groupement de liaisons.

3. **Supprimez le groupement de liaisons.**

```
# dladm delete-aggr aggr
```

Exemple 2-12 Suppression d'un groupement de liaisons

Cet exemple illustre comment supprimer le groupement `aggr0`. La suppression est persistante.

```
# ipadm delete-ip aggr0
# dladm delete-aggr aggr0
```

Commutation entre des groupements de jonction et DLMP

Passer d'un groupement de jonctions à un groupement LDMP modifie la totalité de la configuration. Par conséquent, le groupement est plus affecté que par une simple modification des autres propriétés de groupement de liaisons.

▼ Transition d'un type de groupement de liaisons à l'autre

Avant de commencer

- Si vous passez d'un groupement de jonctions à un groupement DLMP, il faut supprimer la configuration de commutateur précédemment créée pour le groupement de jonctions.
- Si vous passez d'un groupement DLMP, vous devez vous assurer que toutes les jonctions se trouvent sur le même commutateur, et que le commutateur est configuré pour l'agrégation.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Déterminez le type de groupement de liaisons actuel.**

```
# dladm show-aggr
```

   Le champ `MODE` de la sortie indique le type de groupement actuel. La valeur de `MODE` est soit `standard` pour un groupement de jonctions, soit `haonly` pour un groupement DLMP.

3. **Bascule l'agrégation.**

```
# dladm modify-aggr -m mode aggr
```

où *mode* est `trunk` si vous passez à un groupement de jonctions ou `dlmp` si vous passez à un groupement DLMP, et *aggr* est le nom du groupement.

4. **Réglez le commutateur conformément aux exigences du nouveau type de groupement de liaisons.**
   Reportez - vous à la documentation du fabricant du commutateur pour la configuration du commutateur.

5. **(Facultatif) Groupement de liaisons vérifier cette configuration.**

```
# dladm show-aggr
```

Exemple 2-13 Transition d'un groupement de jonctions à un groupement DLMP

Cet exemple illustre comment passer d'un groupement de jonctions à un groupement DLMP.

```
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   trunk      L2      auto            active         short

# dladm modify-aggr -m dlmp aggr0
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   dlmp       --      --              --             --
```

Une fois l'agrégation n'est pas activé, vous devez supprimer la configuration du commutateur qui a été lettrée sur le groupement de jonctions.

Cas d'utilisation : configuration d'un groupement de liaisons

Les éléments suivants de bout en bout de cas d'emploi affiche sur la procédure à suivre pour réaliser les actions suivantes :

- Création d'un groupement DLMP.
- Ajouter des liaisons au groupement.
- Créer une interface IP sur le groupement.
- Configurer une VNIC sur le groupement.
- Configurer la détection de défaillance basée sur sonde pour l'agrégation.
- Adresse de configurer la cible dans la table de routage IP.
- Des sondes transitives ICMP et surveiller les.

1. Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. Affichez les informations concernant les liaisons pour identifier les liaisons de données dans le cadre de l'agrégation.

```
# dladm show-link
LINK      CLASS     MTU     STATE   OVER
net0      phys      1500    up      --
net1      phys      1500    up      --
net2      phys      1500    up      --
```

3. Assurez-vous que le mode "aggregate storage" liaisons de données que vous ne disposez pas, vous devez procéder comme suit les interfaces configurées sur la liaison IP. Supprimez l'interface si l'interface est configurée sur l'une des jonctions.

```
# ipadm show-if
IFNAME       CLASS        STATE     ACTIVE     OVER
lo0          loopback     ok        yes        --
net0         ip           ok        no         --
# ipadm delete-ip net0
```

4. Créez un groupement DLMP entre les jonctions `net0` et `net1`.

```
# dladm create-aggr -m dlmp -l net0 -l net1 aggr1
```

5. Ajoutez une autre jonction, `net2`, au groupement.

```
# dladm add-aggr -l net2 aggr1
```

Reconfigurez le commutateur pour s'adapter aux nouveaux jonctions si ceci est exigé par la configuration du commutateur. Reportez-vous à la documentation du fabricant du commutateur.

6. Configurez une interface IP sur le groupement `aggr1`.

```
# ipadm create-ip aggr1
# ipadm create-addr -T static -a local=10.10.10.1 aggr1/v4
```

7. Créer une VNIC au-dessus de l'agrégation.

```
# dladm create-vnic -l aggr1 vnic1
```

8. Configurer la détection de défaillance basée sur sonde pour l'agrégation.

```
# dladm set-linkprop -p probe-ip=+ aggr1
```

L'adresse IP source et l'adresse IP cible des sondes ne sont pas spécifiées. Vous devez donc configurer la cible dans la table de routage afin d'activer les sondes.

9. Configurer la cible dans la table de routage afin qu'il soit dans la même adresse IP sous-réseau que celui indiqué.

```
# route add -host 10.10.10.2 10.10.10.2 -static
```

10. Afficher l'état de la de ports groupés et les cibles.

```
# dladm show-aggr -S
LINK       PORT        FLAGS   STATE     TARGETS         XTARGETS
aggr1      net0        u--3    active    10.10.10.2      net2 net1
--         net1        u-2-    active       --           net2 net0
--         net2        u-2-    active       --           net0 net1
```

11. Surveiller les statistiques sonde ICMP.

```
# dlstat show-aggr -n -P i
   TIME     AGGR      PORT   LOCAL          TARGET        PROBE NETRTT  RTT
   1.16s    aggr1     net0   10.10.10.1     10.10.10.2    i33   --      --
   1.16s    aggr1     net0   10.10.10.1     10.10.10.2    i33   0.08ms  0.33ms
   2.05s    aggr1     net0   10.10.10.1     10.10.10.2    i34   --      --
   2.05s    aggr1     net0   10.10.10.1     10.10.10.2    i34   0.01ms  0.64ms
   4.05s    aggr1     net0   10.10.10.1     10.10.10.2    i35   --      --
   4.05s    aggr1     net0   10.10.10.1     10.10.10.2    i35   0.10ms  0.35ms
   5.54s    aggr1     net0   10.10.10.1     10.10.10.2    i36   --      --
   5.54s    aggr1     net0   10.10.10.1     10.10.10.2    i36   0.08ms  0.34ms
```

12. Surveiller les statistiques entre les ports sonde transitive.

```
 # dlstat show-aggr -n -P t
   TIME     AGGR   PORT        LOCAL       TARGET  PROBE NETRTT  RTT
   0.30s    aggr1  net2        net2        net0    t38   --      --
   0.30s    aggr1  net2        net2        net0    t38   0.46ms  0.59ms
   0.46s    aggr1  net0        net0        net1    t39   --      --
   0.46s    aggr1  net0        net0        net1    t39   0.46ms  0.50ms
   0.48s    aggr1  net1        net1        net0    t39   --      --
   0.48s    aggr1  net1        net1        net0    t39   0.34ms  0.38ms
   0.72s    aggr1  net2        net2        net1    t38   --      --
   0.72s    aggr1  net2        net2        net1    t38   0.38ms  0.42ms
   0.76s    aggr1  net0        net0        net2    t39   --      --
   0.76s    aggr1  net0        net0        net2    t39   0.33ms  0.38ms
   0.87s    aggr1  net1        net1        net2    t39   --      --
   0.87s    aggr1  net1        net1        net2    t39   0.32ms  0.38ms
   1.95s    aggr1  net2        net2        net0    t39   --      --
   1.95s    aggr1  net2        net2        net0    t39   0.36ms  0.42ms
   1.97s    aggr1  net2        net2        net1    t39   --      --
   1.97s    aggr1  net2        net2        net1    t39   0.32ms  0.38ms
   1.99s    aggr1  net0        net0        net1    t40   --      --
   1.99s    aggr1  net0        net0        net1    t40   0.31ms  0.36ms
   2.12s    aggr1  net1        net1        net0    t40   --      --
   2.12s    aggr1  net1        net1        net0    t40   0.34ms  0.40ms
   2.14s    aggr1  net0        net0        net2    t40   --      --
```

Le groupement `aggr0` avec une interface IP configurée par-dessus a été créé. La VNIC `vnic1` est configurée sur le groupement `aggr0`. La détection de défaillance basée sur sonde est

configuré sans adresse IP spécifiant le ou la cible source adresse de l'IP les sondes. Pour activer le sondage, la cible dans la table de routage est configurée avec une adresse IP `10.10.10.2` sur le même sous-réseau que l'adresse IP spécifiée, `10.10.10.1`. Les statistiques et transitive la sonde ICMP sont contrôlés.

Comparaison entre un groupement de jonctions et un groupement DLMP

Cette section présente une comparaison générale des deux types de groupement de liaisons.

TABLEAU 2-1 Et comparaison des fonctions des Tronçon groupement DLMP

Caractéristiques	Groupements de jonctions	Groupements DLMP
Détection de défaillance basée sur les liaisons	Pris en charge	Pris en charge
LACP	Pris en charge	Non prise en charge.
Utilisation d'interfaces de secours	Non prise en charge.	Non pris en charge[1]
Extension sur plusieurs commutateurs	Non pris en charge sauf en cas d'utilisation d'une solution propriétaire	Pris en charge
Configuration du commutateur	(obligatoire)	Pas nécessaire
Stratégies d'équilibrage de la charge	Pris en charge	Non applicable
Répartition de la charge sur tous les ports du groupement	Pris en charge	Limité[2]
Les flux définis par l'utilisateur pour la gestion des ressources	Pris en charge	Pris en charge
Protection de lien	Pris en charge	Pris en charge
Configuration dos à dos	Pris en charge	Non pris en charge[3]

[1]Chaque client DLMP est associé à un seul port. Les ports restants agissent en tant que ports disponibles pour les clients DLMP, mais vous ne pouvez pas configurer ces ports disponibles.

[2] Le groupement répartit ses VNIC sur tous les ports. Mais une carte VNIC individuelle ne peut pas répartir la charge sur plusieurs ports.

[3] Les groupements DLMP doivent toujours utiliser un commutateur intermédiaire pour envoyer des paquets à d'autres systèmes de destination. Cependant, aucune configuration de commutateur n'est exigée pour DLMP.

♦ ♦ ♦ CHAPITRE 3

Réseaux virtuels à l'aide de la configuration de réseaux locaux virtuels

Ce chapitre décrit les caractéristiques et les avantages des réseaux locaux virtuels (VLAN). Ce chapitre décrit également les procédures à suivre pour configurer et modifiez les VLAN.

Ce chapitre aborde les sujets suivants :

Présentation du déploiement de réseaux locaux virtuels (VLAN)

Un réseau local virtuel (VLAN) désigne une subdivision d'un réseau local au niveau de la couche de liaison de données de la pile de protocoles. Vous pouvez créer des VLAN pour tout réseau local utilisant la technologie de commutation. Vous pouvez également assigner les interfaces d'un même système à des VLAN différents.

Cas dans lesquels mettre en place des VLAN

Vous pouvez déployer VLAN pour réaliser les opérations suivantes :

- Création de divisions logiques de groupes de travail

  Par exemple, si tous les hôtes d'un étage d'un immeuble sont connectés à un commutateur basées sur réseau local, vous pouvez alors 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 attentes d'un service financier et d'un service informatique sont totalement différentes en matière de sécurité. Vous pouvez créer un VLAN distinct pour chaque service et appliquer la stratégie de sécurité qui convient pour chaque VLAN.
- Réduire la taille de domaine de diffusion et améliorer l'efficacité du réseau. Division de groupes de travail en domaines de diffusion gérables

  Par exemple, dans un domaine de diffusion composé de 25 utilisateurs, si le trafic de diffusion est prévu pour 12 utilisateurs seulement, paramétrer un VLAN séparé pour ces 12 utilisateurs permet de réduire le trafic et d'améliorer l'efficacité du réseau.

Affectation de noms aux VLAN

Les VLAN offrent l'avantage de porter des noms génériques ou personnalisés. Dans les versions précédentes, le réseau local virtuel était identifié par le point de connexion physique (PPA) qui exigeait la combinaison du nom matériel de la liaison de données et de l'ID du VLAN. Dans Oracle Solaris, vous pouvez choisir désormais un nom plus explicite pour identifier un VLAN. Ce nom doit respecter les règles de dénomination des liaisons de données présentées dans“ Règles d’affectation de noms de liaison valides ” du manuel “ Configuration et administration des composants réseau dans Oracle Solaris 11.2 ” Par exemple, vous pouvez leur attribuer un nom de VLAN personnalisé comme `sales0` ou `marketing1`.

Les noms de VLAN fonctionnent avec leur ID. Chaque VLAN d'un réseau local est identifié par un ID de VLAN, qui fait partie de la balise VLAN. L'ID de VLAN est attribué au réseau local virtuel lors de sa configuration. Lorsque vous configurez des commutateurs pour prendre en charge des VLAN, il faut attribuer un ID de VLAN à chaque port. L'ID de VLAN du port doit être identique à celui associé à l'interface connectée au port.

Par défaut, chaque port dispose d'un ID de VLAN appelé ID de VLAN de port. Les paquets appartenant à cet ID de VLAN ne sont pas marqués d'une étiquette VLAN. Dans Oracle Solaris, vous pouvez utiliser la propriété de liaison de données `default_tag` pour afficher et modifier l'ID d'un port VLAN sur une interface.

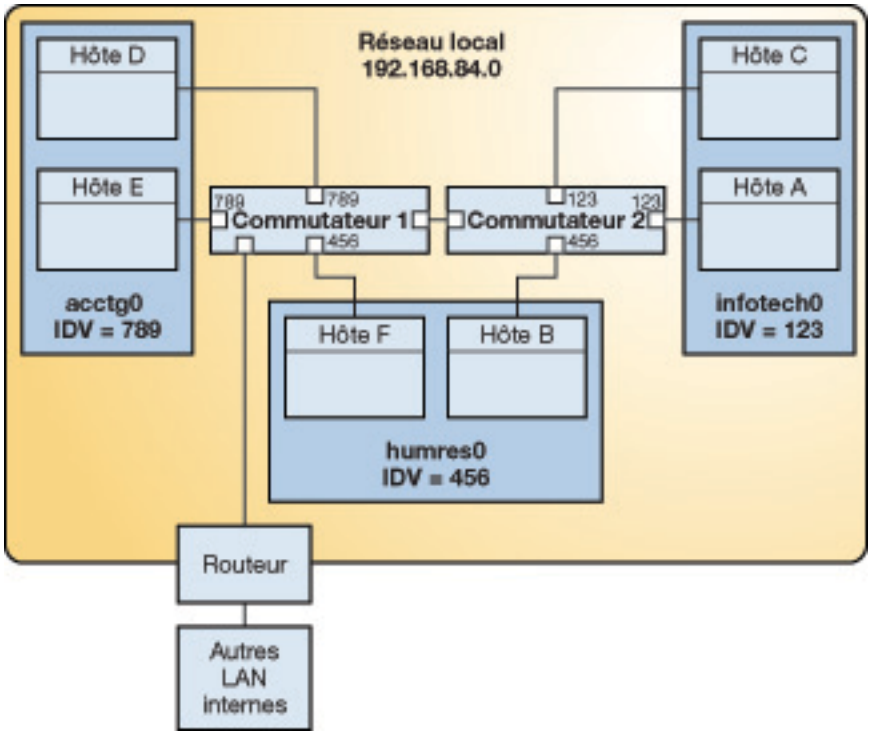
Topologie de réseau local virtuel

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.

Le schéma suivant illustre un réseau local divisé en trois VLAN.

FIGURE 3-1 Réseau local avec trois VLAN



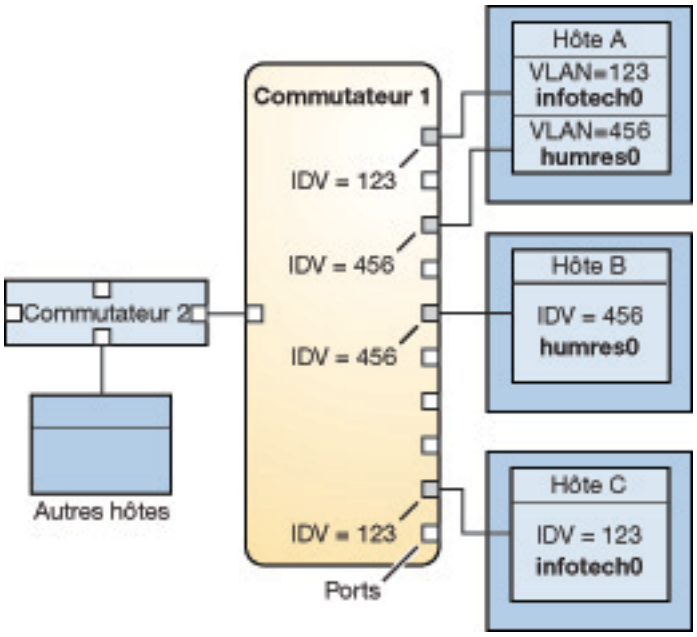
Dans le schéma, le LAN porte l'adresse de sous-réseau `192.168.84.0`.

Ce réseau local est divisé en trois VLAN afin de correspondre à trois groupes de travail :

- `acctg0` portant l'ID de VLAN `789` : Comptabilité. Ce groupe comprend les hôtes D et E.
- `humres0` portant l'ID de VLAN `456` : Ressources Humaines. Ce groupe comprend les hôtes B et F.
- `infotech0` portant l'ID de VLAN `123` : Informatique. Ce groupe comprend les hôtes A et C.

Une variante de la figure est indiquée dans la figure suivante, où un seul commutateur est utilisé et plusieurs hôtes appartenant à différents VLAN se connectent à cet unique commutateur.

FIGURE 3-2 Un commutateur connectant plusieurs hôtes VLAN différents



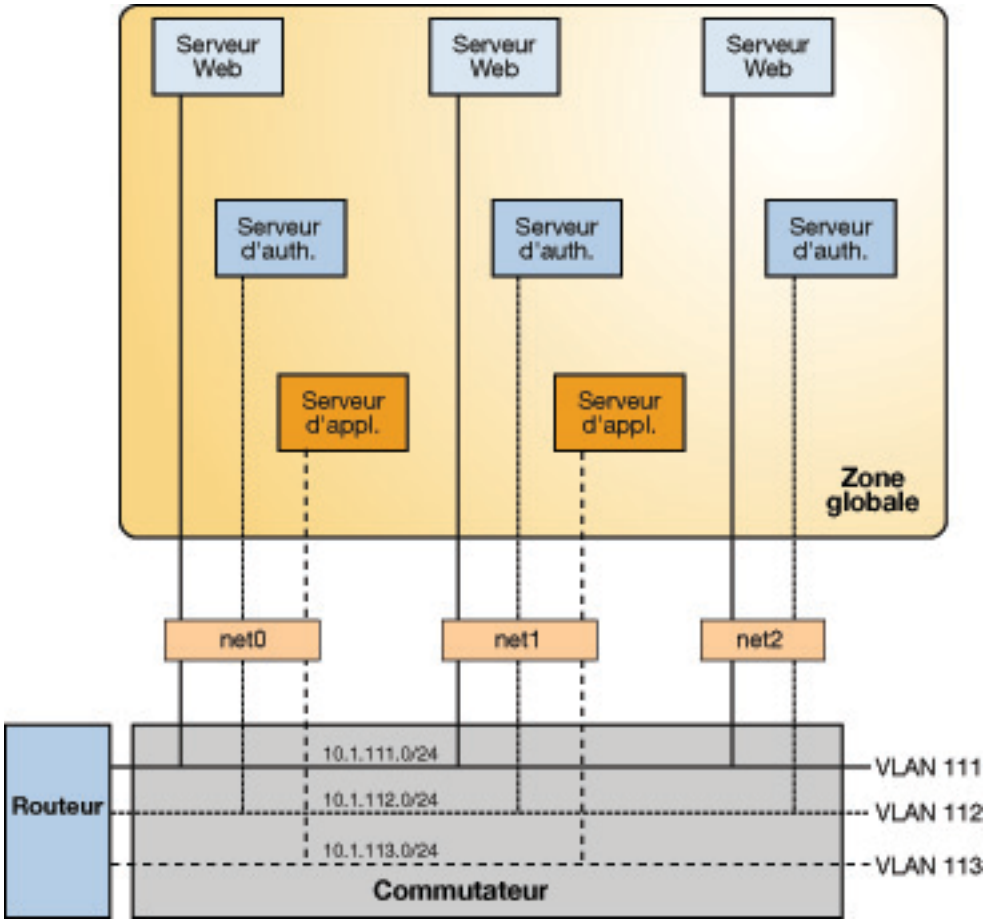
Dans la figure, les hôtes A et C font partie du VLAN du groupe Informatique portant l'ID VLAN `123`. Ainsi, une des interface de l'hôte A porte l'ID de VLAN `123`. Cette interface est connectée au port 1 du commutateur 1, qui porte également l'ID de VLAN `123`. L'hôte B est membre du VLAN Ressources humaines portant l'ID `456`. L'interface de l'hôte B est connectée au port 5 du commutateur 1, qui porte l'ID de VLAN `456`. Enfin, l'interface de l'hôte C porte l'ID de VLAN `123`. L'interface est connectée au port 9 du commutateur 1. Le port 9 porte également l'ID de VLAN `123`.

La figure montre également qu'un même hôte peut appartenir à plusieurs VLAN. Par exemple, l'hôte A comporte deux VLAN sont configurés sur l'interface de l'hôte. Le deuxième VLAN est configuré avec l'ID VLAN `456`, et il est connecté au port 3, qui porte également l'ID de VLAN `456`. Par conséquent, hôte A est membre des VLAN `infotech0` et `humres0`

Utilisation de VLAN avec des zones

Vous avez la possibilité de configurer plusieurs réseaux virtuels au sein d'une seule et même unité en combinant des VLAN et zones Oracle Solaris. La figure suivante fournit un aperçu d'un système possédant trois cartes réseau physiques : `net0`, `net1` et `net2`.

FIGURE 3-3 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. Avec les VLAN et les zones, vous pouvez réduire les huit systèmes et les configurer en tant que zones dans un système unique. Il faut ensuite attribuer des ID pour affecter un VLAN à chaque ensemble de zones qui effectue les mêmes fonctions. Le tableau suivant répertorie les informations fournies dans le schéma.

Fonction	Nom de zone	Nom de VLAN	ID du VLAN	Adresse IP	NIC
serveur Web	`webzone1`	`web1`	111	`10.1.111.0`	`net0`
Serveur d'authentification	`authzone1`	`auth1`	112	`10.1.112.0`	`net0`
Serveur d'application	`appzone1`	`app1`	113	`10.1.113.0`	`net0`
serveur Web	`webzone2`	`web2`	111	`10.1.111.1`	`net1`
Serveur d'authentification	`authzone2`	`auth2`	112	`10.1.112.1`	`net1`
Serveur d'application	`appzone2`	`app2`	113	`10.1.113.1`	`net1`
serveur Web	`webzone3`	`web3`	111	`10.1.111.2`	`net2`
Serveur d'authentification	`authzone3`	`auth3`	112	`10.1.112.2`	`net2`

Pour créer la configuration illustrée dans le schéma, reportez-vous à l'Exemple 3-2, “La configuration d'un VLAN comportant des zones”.

Planification d'une configuration VLAN

Configuration Planning a VLAN implique les étapes suivantes :

1. Observez la topologie du réseau local et déterminez les zones dans lesquelles il serait judicieux de créer des VLAN.

   Pour un exemple de topologie de réseau simple, reportez-vous à la Figure 3-1, “Réseau local avec trois VLAN”.
2. Créez un schéma de numérotation pour les ID de VLAN et attribuez un ID à chaque VLAN.

Remarque - Si un schéma de numérotation VLAN existe déjà sur le réseau, vous devez créer dans des ID de VLAN dans le schéma de numérotation VLAN existant.

---

3. Sur chaque système, déterminez les interfaces à inclure dans chaque VLAN.

   a. Déterminer les liens qui sont configurés sur le système à l'aide de la commande`dladm show-link`.

b. Déterminez les ID de VLAN à associer aux liaisons de données du système.
c. Créez le VLAN.

4. Vérifiez les connexions des liaisons de données aux commutateurs du réseau.

   Notez l'ID de VLAN de chaque interface ainsi que le port du commutateur auquel elle est connectée.

5. Attribuez à chaque port du commutateur le même ID de VLAN 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 d'un VLAN

La procédure suivante explique comment créer un VLAN sur une liaison de données à l'aide de la commande `dladm`. Vous pouvez créer une interface IP sur un VLAN et configurer l'interface avec une adresse IP à l'aide de la commande `ipadm`. Pour plus d'informations sur les commandes `dladm` et`ipadm`, reportez-vous aux pages de manuel `dladm`(1M) et `ipadm`(1M).

▼ Configuration d'un VLAN

Avant de commencer Cette procédure part du principe que les zones dont déjà créées sur le système. Pour plus d'informations sur la configuration des zones, reportez-vous au - Chapitre 1, “ Planification et configuration de zones non globales ” du manuel “ Création et utilisation des zones Oracle Solaris ”.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Déterminez les types de liaisons en cours d'utilisation sur le système.**

   ```
   # dladm show-link
   ```

3. **Configurez une liaison VLAN sur une liaison de données.**

   ```
   # dladm create-vlan -l link -v vid VLAN-link
   ```

   link Spécifie la liaison sur laquelle créer l'interface VLAN.

   vid Indique le numéro d'ID d'un VLAN.

vlan-link Spécifie le nom du VLAN, qui peut également être cohérente nom personnalisé. Pour plus d'informations sur les noms de VLAN, reportez-vous à “Affectation de noms aux VLAN” à la page 44.

4. **Vérifiez la configuration du VLAN.**

```
# dladm show-vlan
```

5. **Créez une interface IP sur le VLAN.**

```
# ipadm create-ip interface
```

où*interface* fournit le nom du VLAN.

6. **Configurez l'interface IP à l'aide d'une adresse IP.**

```
# ipadm create-addr -a address interface
```

Exemple 3-1 Création d'un VLAN

Cet exemple illustre comment créer la configuration VLAN présentée dans la Figure 3-1, “Réseau local avec trois VLAN”.

1. Vérifiez les liaisons disponibles et créez le VLAN sur les liaisons spécifiques.

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
net2     phys      1500    up        --
```

2. L'hôte A, procédez comme suit :

```
# dladm create-vlan -l net0 -v 123 infotech0
```

C de l'hôte, procédez comme suit :

```
# dladm create-vlan -l net0 -v 123 infotech0
```

Hôte F :

```
# dladm create-vlan -l net0 -v 456 humres0
```

L'hôte B, procédez comme suit :

```
# dladm create-vlan -l net0 -v 456 humres0
```

Hôte D :

```
# dladm create-vlan -l net0 -v 789 acctg0
```

Hôte E :

```
# dladm create-vlan -l net0 -v 789 acctg0
```

3. Afficher les VLAN créés.

```
# dladm show-vlan
LINK            VID     OVER        FLAGS
infotech0       123     net0        ----
infotech0       123     net0        ----
humres0         456     net0        ----
humres0         456     net0        ----
acctg0          789     net0        ----
acctg0          789     net0        ----
```

Exemple 3-2 La configuration d'un VLAN comportant des zones

Cet exemple illustre comment créer la configuration VLAN présentée dans la Figure 3-3, “Système comportant plusieurs VLAN”. 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 “ Création et utilisation des zones Oracle Solaris ”.

1. L'administrateur commence par contrôler les liaisons disponibles pour configurer des VLAN, puis procède à la création des VLAN sur les liaisons spécifiques.

```
global# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
net2     phys      1500    up        --

global# dladm create-vlan -l net0 -v 111 web1
global# dladm create-vlan -l net0 -v 112 auth1
global# dladm create-vlan -l net0 -v 113 app1
global# dladm create-vlan -l net1 -v 111 web2
global# dladm create-vlan -l net1 -v 112 auth2
global# dladm create-vlan -l net1 -v 113 app2
global# dladm create-vlan -l net2 -v 111 web3
global# dladm create-vlan -l net2 -v 112 auth3

global# dladm show-vlan
LINK      VID     OVER        FLAGS
web1      111     net0        ----
auth1     112     net0        ----
app1      113     net0        ----
web2      111     net1        ----
```

```
auth2     112     net1        ----
app2      113     net1        ----
web3      111     net2        ----
auth3     113     net2        ----
```

Lorsque les informations relatives aux liaisons s'affichent, les VLAN sont inclus dans la liste.

```
global# dladm show-link
LINK      CLASS    MTU      STATE     OVER
net0      phys     1500     up        --
net1      phys     1500     up        --
net2      phys     1500     up        --
web1      vlan     1500     up        net0
auth1     vlan     1500     up        net0
app1      vlan     1500     up        net0
web2      vlan     1500     up        net1
auth2     vlan     1500     up        net1
app2      vlan     1500     up        net1
web3      vlan     1500     up        net2
auth3     vlan     1500     up        net2
```

2. Les VLAN sont assignés à leurs zones respectives et affiche des informations pour chaque zone semblable à ce qui suit :

```
global# zonecfg -z webzone1 info net
net:
address not specified
physical: web1
net:
address not specified
physical: web2
net:
address not specified
physical: web3

global# zonecfg -z authzone1 info net
net:
address not specified
physical: auth1
net:
address not specified
physical: auth2
net:
address not specified
physical: auth3

global# zonecfg -z appzone2 info net
```

```
net:
address not specified
physical: app1
net:
address not specified
physical: app2
```

La valeur de la propriété `physical` indique le VLAN défini pour la zone donnée.

3. Afficher les VLAN attribués dans les zones.

```
global# dladm show-vlan
LINK            VID  OVER  FLAGS
webzone1/web1   111  net0  --
authzone1/auth1 112  net0  --
appzone1/app1   113  net0  --
webzone1/web2   111  net1  --
authzone1/auth2 112  net1  --
appzone1/app2   113  net1  --
webzone1/web3   111  net2  --
authzone2/auth3 111  net2  --
```

4. Connectez-vous à chaque zone non globale pour configurer le VLAN à l'aide d'une adresse IP.

   Dans la zone `webzone1` :

```
webzone1# ipadm create-ip web1
webzone1# ipadm create-addr -a 10.1.111.0/24 web1
ipadm: web1/v4
```

   Dans la zone `webzone2` :

```
webzone2# ipadm create-ip web2
webzone2# ipadm create-addr -a 10.1.111.1/24 web2
ipadm: web2/v4
```

   Dans la zone `webzone3` :

```
webzone3# ipadm create-ip web3
webzone3# ipadm create-addr -a 10.1.111.2/24 web3
ipadm: web3/v4
```

   Dans la zone `authzone1` :

```
authzone1# ipadm create-ip auth1
authzone1# ipadm create-addr -a 10.1.112.0/24 auth1
ipadm: auth1/v4
```

   Dans la zone `authzone2` :

```
authzone2# ipadm create-ip auth2
autzone2# ipadm create-addr -a 10.1.112.1/24 auth2
ipadm: auth2/v4
```

Dans la zone `authzone3` :

```
authzone3# ipadm create-ip auth3
authzone3# ipadm create-addr -a 10.1.112.2/24 auth3
ipadm: auth3/v4
```

Dans la zone `appzone1` :

```
appzone1# ipadm create-ip app1
appzone1# ipadm create-addr -a 10.1.113.0/24 app1
ipadm: app1/v4
```

Dans la zone `appzone2` :

```
appzone2# ipadm create-ip app2
appzone2# ipadm create-addr -a 10.1.113.1/24 app2
ipadm: app2/v4
```

Une fois que des adresses IP ont été attribuées à tous les VLAN, la configuration est terminée. Les trois VLAN sont opérationnels et peuvent héberger du trafic dans leurs zones respectives.

Configuration de réseaux VLAN via un groupement de liaisons

Vous pouvez créer des VLAN sur un groupement de liaisons de manière similaire à vous configurez des réseaux locaux virtuels sur une interface. Les groupements de liaisons sont décrits dans Chapitre 2, Configuration de la haute disponibilité à l'aide de groupements de liaisons. Cette section décrit la configuration combinée de VLAN et de groupements de liaisons.

▼ Configuration de VLAN par le biais d'un groupement de liaisons

Avant de commencer Créez le groupement de liaisons. Pour créer des groupements de liaisons, reportez-vous à “Création d'un groupement de liaisons” à la page 27.

1. **Répertoriez les groupements de liaisons configurés sur le système.**

```
# dladm show-aggr
```

2. **Pour chacun des VLAN à créer sur le groupement de liaisons, exécutez la commande suivante :**

   # dladm create-vlan -l *link* **-v** *vid VLAN-link*

   link Spécifie la liaison sur laquelle créer l'interface VLAN.

   Remarque - Dans cette procédure, "link" fait référence au groupement de liaisons.

   vid Indique le numéro d'ID d'un VLAN.

   vlan-link Spécifie le nom du VLAN.

3. **Créez une interface IP sur chacun des VLAN créés à l'étape précédente.**

   # ipadm create-ip *interface*

   où *interface* utilise le nom du VLAN.

4. **Attribuez une adresse IP valide à chacune des interfaces IP d'un VLAN.**

   # ipadm create-addr -a *address interface*

Exemple 3-3 Configuration de plusieurs réseaux locaux virtuels sur un groupement de liaisons

Dans cet exemple, deux VLAN sont configurés sur un groupement de liaisons. Ils portent respectivement l'ID 193 et 194.

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1

# dladm create-vlan -l aggr0 -v 193 acctg0
# dladm create-vlan -l aggr0 -v 194 humres0

# ipadm create-ip acctg0
# ipadm create-ip humres0

# ipadm create-addr -a 192.168.10.0/24 acctg0
ipadm: acctg0/v4
# ipadm create-addr -a 192.168.20.0/24 humres0
ipadm: humres0/v4
```

Configuration de VLAN sur un périphérique hérité

Certains périphériques hérités gèrent uniquement les paquets dont l'unité de transmission maximale (MTU) ou taille de trame est fixée à 1514 octets. Les paquets dont la taille de 'image dépasse la limite maximale sont refusés. Pour de tels cas, suivez la procédure décrite à la section “Configuration d'un VLAN” à la page 49. Toutefois, lors de la création du VLAN, utilisez l'option `-f` pour forcer la création du VLAN.

▼ Configuration de VLAN sur un périphérique hérité

1. **Créez le VLAN avec l'option `-f`.**

   ```
   # dladm create-vlan -f -l link -v vid VLAN-link
   ```

`-f`	Forcer la création du VLAN. Utilisez cette option lorsque vous êtes en train de créer un VLAN sur les dispositifs qui n'autorisent pas les tailles d'image VLAN assez large pour inclure un en-tête .
`-l` *link*	Spécifie la liaison sur laquelle créer l'interface VLAN. Dans cette procédure, "link" fait référence au périphérique hérité.
`-v` *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.

2. **Définissez une taille inférieure pour l'unité de transmission maximale (`MTU`).**

   Dans l'exemple suivant, `mtu` est défini sur `1496`.

   ```
   # dladm set-linkprop -p 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. **Répétez l'étape 2 pour définir une valeur pour chaque noeud MTU du VLAN.**

   Pour plus d'informations sur la modification des valeurs de propriété de liaison, reportez-vous à “ Administration des propriétés de liaison de données ” du manuel “ Configuration et administration des composants réseau dans Oracle Solaris 11.2 ”

Affichage des informations du VLAN

Vous pouvez utiliser la commande `dladm show-link` pour afficher des informations sur VLAN, car ces derniers sont des liaisons de données. Utilisez la commande `dladm show-vlan` pour obtenir des informations spécifiques sur les VLAN.

L'exemple ci-dessous compare le type d'information que vous pouvez obtenir à l'aide de la commande. `dladm show-link` ou de la commande`dladm show-vlan`. La sortie de la commande `dladm show-link` affiche toutes les liaisons de données du système, y compris celles qui ne constituent pas des VLAN. La sortie de la commande `dladm show-vlan` affiche un sous-ensemble d'informations relatives aux VLAN.

```
# dladm show-link
LINK     CLASS    MTU      STATE     OVER
net0     phys     1500     up        --
net1     phys     1500     up        --
net2     phys     1500     up        --
web1     vlan     1500     up        net0
auth1    vlan     1500     up        net0
app1     vlan     1500     up        net0
web2     vlan     1500     up        net1
auth2    vlan     1500     up        net1
app2     vlan     1500     up        net1
web3     vlan     1500     up        net2
auth3    vlan     1500     up        net2

# dladm show-vlan
LINK      VID     OVER     FLAGS
web1      111     net0     ----
auth1     112     net0     ----
app1      113     net0     ----
web2      111     net1     ----
auth2     112     net1     ----
app2      113     net1     ----
web3      111     net2     ----
auth3     113     net2     ----
```

Modification des VLAN

Vous pouvez modifier un VLAN à l'aide de la commande `dladm modify-vlan` de l'une des manières suivantes :

- Modifier l'ID de VLAN d'un VLAN
- Migrer un VLAN vers une autre liaison sous-jacente

Modification de l'ID de VLAN d'une carte VNIC

Pour modifier l'ID d'un VLAN, exécutez l'une des commandes suivantes :

- `dladm modify-vlan -v` *vid* `-L` *datalink*

  Dans cette commande, *vid* représente le nouvel ID de VLAN que vous affectez à la carte VNIC. Le paramètre *datalink* désigne la liaison de données sous-jacente sur laquelle la carte VNIC est configurée.

Remarque - Vous pouvez utiliser la syntaxe `dladm modify-vlan -v` *vid*`-L`*datalink*de commande seulement si un seul VLAN figure sur la liaison de données. La commande échoue si vous l'exécutez sur une liaison de données sur laquelle sont configurés plusieurs VLAN car ces derniers doivent porter des ID uniques.

Si vous modifiez l'ID du VLAN sur le lien, vous devez également configurer le port de commutateur pour le nouvel ID de VLAN.

- `dladm modify-vlan -v` *vid vlan*

  Exécutez cette commande pour modifier l'ID unique de plusieurs VLAN configurés sur une seule liaison de données. Chaque VLAN sur la liaison de données possède son propre ID de VLAN, vous devez donc modifier les ID de VLAN un par un. Au cours de la configuration illustrée dans Figure 3-3, “Système comportant plusieurs VLAN”, il convient de remplacer les ID de VLAN de `web1`, `auth1` et `app1` configurés sur `net0` comme suit :

```
# dladm modify-vlan -v 123 web1
# dladm modify-vlan -v 456 app1
# dladm modify-vlan -v 789 auth1
```

Migration d'un VLAN vers une autre liaison sous-jacente

Vous pouvez migrer un VLAN d'une liaison de données sous-jacente à une sans pour autant supprimer ou reconfigurer ce réseau. La liaison sous-jacente peut prendre la forme d'une liaison physique, d'un groupement de liaisons ou d'un etherstub. Pour plus d'informations, reportez-vous à “ Composants d’un réseau virtuel ” du manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Pour assurer la réussite de la migration d'un VLAN, la liaison de données sous-jacente vers laquelle est déplacé le VLAN doit pouvoir s'adapter aux propriétés de liaison de données du VLAN. Si ces propriétés ne sont pas prises en charge, la migration échoue et l'utilisateur en est

informé. Après la migration effective du VLAN, toutes les applications qui l'utilisent continuent de fonctionner normalement, à condition que le VLAN reste connecté au réseau.

Certaines propriétés dépendantes du matériel peuvent changer après la migration d'un VLAN. Par exemple, un VLAN partage toujours la même adresse MAC que sa liaison de données sous-jacente. Par conséquent, lors de la migration d'un VLAN, son adresse MAC est remplacée par l'adresse MAC principale de la liaison de données cible. D'autres propriétés peuvent être concernées, comme l'état de la liaison de données, son débit, la taille MTU, etc. Néanmoins, les applications fonctionnent sans interruption.

Remarque - Un VLAN migré ne conserve pas les statistiques de couloir matériel de la liaison de données d'origine. Les couloirs matériels disponibles pour le VLAN sur la liaison de données cible deviennent la nouvelle source de statistiques. En revanche, les statistiques logicielles qui s'affichent par défaut en exécutant la commande `dlstat` sont préservées.

Vous pouvez procéder à la migration de VLAN de manière globale ou sélective.

Migration globale

La migration globale permet de migrer tous les VLAN qui sont configurées sur une liaison de données à une autre liaison de données. Pour effectuer une migration globale, vous devez uniquement spécifier la liaison de données source et la liaison de données cible. L'exemple suivant montre comment déplacez toutes les VLAN de `ether0` vers `net1`.

```
# dladm modify-vlan -l net1 -L ether0
```

`-l` Correspond à la liaison de données cible vers laquelle migrer les VLAN.

`-L` Correspond à la liaison de données d'origine sur laquelle les VLAN sont configurés.

Remarque - Il faut spécifier la liaison de données cible avant la liaison de données source.

Migration sélective

Sélective uniquement la migration sélectionné est utilisé pour migrer plusieurs VLAN. Pour procéder à une migration sélective de VLAN, il faut spécifier les réseaux à déplacer. Dans l'exemple suivant est basé sur la Figure 3-3, “Système comportant plusieurs VLAN”, les réseaux locaux virtuels (VLAN) sont déplacés de `net0` à `net3`.

```
# dladm modify-vlan -l net3 web1,auth1,app1
```

Remarque - Lors d'une migration sélective de VLAN, omettez l'option `-L` qui s'applique uniquement aux migrations globales.

Vous pouvez modifier l'ID de VLAN lors d'une migration. En vous basant sur la Figure 3-3, “Système comportant plusieurs VLAN”, l'exemple ci-dessous illustre comment migrer plusieurs VLAN et modifier leur ID en même temps.

```
# dladm show-vlan
LINK    VID      OVER     FLAGS
web1    111      net0     -----
auth1   112      net0     -----
app1    113      net0     -----

# dladm modify-vlan -l net3 -v 123 web1
# dladm modify-vlan -l net3 -v 456 auth1
# dladm modify-vlan -l net3 -v 789 app1
# dladm show-vlan
LINK    VID      OVER     FLAGS
web1    123      net3     -----
auth1   456      net3     -----
app1    789      net3     -----
```

Remarque - Une sous-commande parallèle `dladm modify-vnic` permet de migrer les cartes réseau virtuelles configurées en tant que VLAN. Il faut exécuter la sous-commande appropriée selon que vous migrez des VLAN ou des cartes réseau virtuelles configurées en tant que VLAN. Exécutez la sous-commande `modify-vlan` sur les VLAN répertoriés par la commande `dladm show-vlan`. Exécutez la sous-commande `modify-vnic` sur les cartes réseau virtuelles, y compris celles portant un ID de VLAN, répertoriées par la commande `dladm show-vnic`. Pour plus d'informations sur la procédure pour modifier des cartes réseau virtuelles, reportez-vous à “ Modification des ID de VLAN des VNIC ” du manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Suppression d'un VLAN

Exécutez la commande `dladm delete-vlan` pour supprimer des configurations de VLAN du système.

Remarque - Il faut commencer par supprimer les configurations IP existantes du VLAN concerné. Si des interfaces IP figurent sur un VLAN, sa suppression échoue.

EXEMPLE 3-4 Suppression d'une configuration de VLAN

Cet exemple montre comment supprimer une configuration VLAN.

```
# dladm show-vlan
LINK      VID     OVER     FLAGS
web1      111     net0     ----
```

```
auth1     112     net0     ----
app1      113     net0     ----
web2      111     net1     ----
auth2     112     net1     ----
app2      113     net1     ----
web3      111     net2     ----
auth3     113     net2     ----

# ipadm delete-ip web1
# dladm delete-vlan web1
```

Etude de cas : combinaison de groupements de liaisons et de configurations VLAN

Cette section fournit un exemple illustrant la création d'une combinaison de configurations réseau qui utilise des groupements de liaisons et des VLAN sur lesquels sont créées des interfaces IP.

Dans l'exemple ci-dessous, il faut configurer un système comprenant quatre cartes réseau virtuelles en tant que routeur pour huit sous-réseaux distincts. Par conséquent, huit liaisons sont configurés, un pour chaque sous-réseau . Tout d'abord, un groupement de liaisons est créé sur chacune des cartes réseau virtuelles. Cette liaison non marquée qui ne comporte pas de balise dans le cadre sortant VLAN devient le sous-réseau non marqué par défaut pour le réseau vers lequel pointe le routage par défaut.

Ensuite, les interfaces VLAN sont configurées sur le groupement de liaisons pour les autres sous-réseaux. Les sous-réseaux sont nommés en fonction d'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 huit liaisons pour les huit sous-réseaux : une liaison non marquée et sept liaisons VLAN marquées. L'exemple commence par vérifier si des interfaces IP figurent déjà sur les liaisons de données. Il faut impérativement supprimer ces interfaces pour pouvoir combiner les liaisons de données en groupement.

1. L'administrateur commence par supprimer toutes les interfaces IP configurées sur les liaisons de données.

```
# ipadm show-if
IFNAME    CLASS      STATE   ACTIVE   OVER
lo0       loopback   ok      yes      --
net0      ip         ok      yes      --
net1      ip         ok      yes      --
net2      ip         ok      yes      --
net3      ip         ok      yes      --

# ipadm delete-ip net0
```

```
# ipadm delete-ip net1
# ipadm delete-ip net2
# ipadm delete-ip net3
```

2. Créez le groupement de jonctions `default0`.

```
# dladm create-aggr -P L2,L3 -l net0 -l net1 -l net2 -l net3 default0

# dladm show-link
LINK        CLASS     MTU   STATE    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
```

3. Créer une interface IP sur le groupement.

```
# ipadm create-ip default0
# ipadm create-addr -a 10.2.3.4/24 default0
```

4. Créez les réseaux VLAN sur `default0`.

```
# 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    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
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    -----
```

5. Créez des interfaces IP sur les liens VLAN et attribuent des adresses IP aux interfaces.

```
# 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 -a 10.2.3.5/24 orange0
# ipadm create-addr -a 10.2.3.6/24 green0
# ipadm create-addr -a 10.2.3.7/24 blue0
# ipadm create-addr -a 10.2.3.8/24 white0
# ipadm create-addr -a 10.2.3.9/24 yellow0
# ipadm create-addr -a 10.2.3.10/24 red0
# ipadm create-addr -a 10.2.3.11/24 cyan0
```

♦ ♦ ♦ CHAPITRE 4

Administration de fonctionnalités de pontage

Vous pouvez utiliser le pontage est utilisé pour connecter des segments du réseau afin qu'ils puissent communiquer les uns comme s'il s'agissait d'un seul et même segment réseau. Ce chapitre décrit comment configurer et administrer les réseaux pontés.

Ce chapitre aborde les sujets suivants :

Présentation des réseaux pontés

Les ponts réseau connectent différents noeuds du réseau dans un réseau unique. Le segment du réseau à l'autre partagent un réseau unique de diffusion et communiquent comme s'ils formaient un seul et même segment réseau lorsque vous êtes connecté. Par conséquent, chaque noeud peut atteindre les autres noeuds par le biais de protocoles réseau (comme IP) et non de 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.

Bien que le pontage et le routage puissent être utilisés pour distribuer des informations sur l'emplacement des ressources réseau, ces techniques diffèrent en plusieurs points. 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.

Le pontage est utilisé pour distribuer des informations sur l'emplacement des ressources sur le réseau. En revanche, les destinations des paquets transmis sont déterminées par l'examen

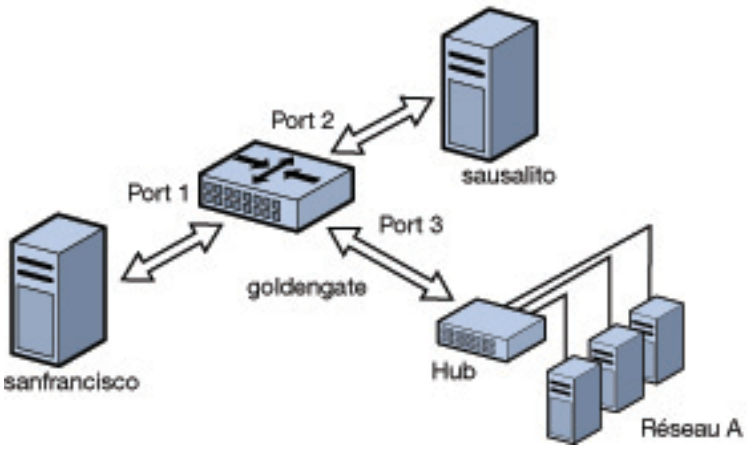
du trafic sur le réseau, reçu sur les liaisons reliées au pont. Une passerelle protocoles, tels les protocoles réseau a recours au protocole STP (Spanning Tree Protocol) et (Transparent Interconnection of Lots of Links TRILL). Pour plus d'informations, reportez-vous à “Protocoles de pontage” à la page 69

Attention - Ne définissez pas la propriété `local-mac-address?` sur `false` à l'aide de la commande `eeprom` sur les systèmes basés sur SPARC® utilisant le pontage. Ces systèmes utiliseraient alors de manière erronée la même adresse MAC sur plusieurs ports et sur le même réseau.

Réseau ponté simple

La figure ci-dessous illustre une configuration réseau de ponts simple.

FIGURE 4-1 Réseau ponté simple

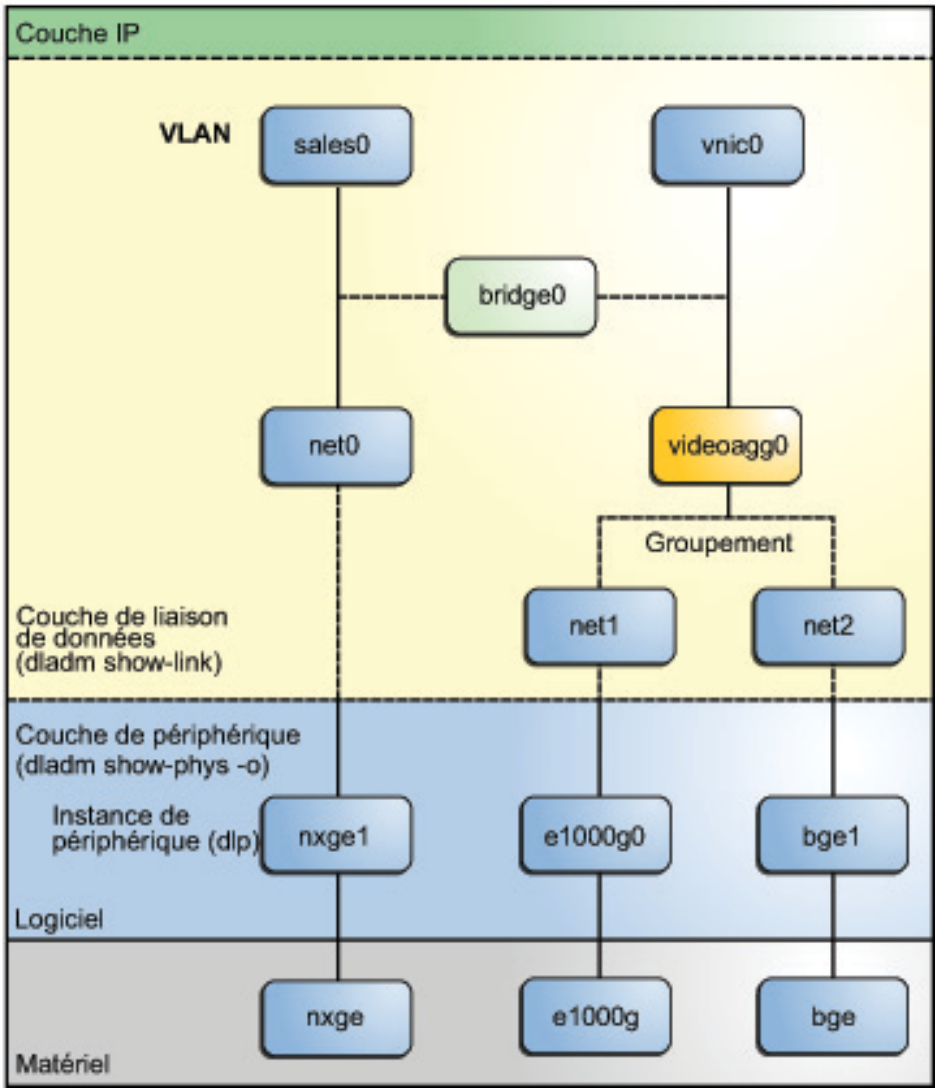


Le pont `goldengate` est un système Oracle Solaris configuré avec les fonctionnalités de pontage. Les systèmes `sanfrancisco` et `sausalito` sont connectés physiquement au pont. Le réseau A utilise un hub physiquement connecté au pont d'un côté et à des systèmes informatiques de l'autre côté. Les ports de pont sont les liens `net0`, `net1` et `net2`.

Implémentation des ponts Oracle Solaris dans la pile réseau

Dans Oracle Solaris, vous pouvez configurer des ponts sur la couche de liaison de données de la même implémentation de pile réseau, comme le montre la figure suivante.

FIGURE 4-2 Ponts de la pile réseau pour Oracle Solaris

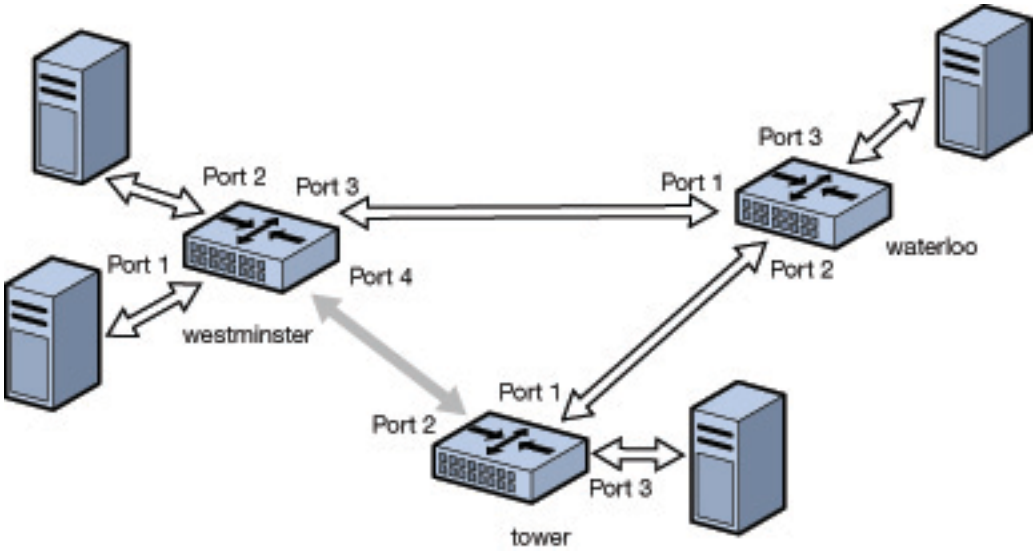


Deux interfaces (`net0` et `videoagg0`) sont configurées en tant que pont (`bridge0`). Les paquets reçus sur une interface sont transmis à l'autre interface. Après avoir configuré le pont, vous pouvez encore configurer des VLAN et des interfaces IP par le biais des deux interfaces.

Réseau ponté en anneau

Il est possible de former des réseaux pontés en anneau qui relient physiquement plusieurs ponts. La figure ci-dessous illustre une configuration de pont.

FIGURE 4-3 Réseau ponté en anneau



Le schéma suivant illustre un réseau ponté configuré en anneau. La configuration présente trois ponts. Deux systèmes sont connectés physiquement au pont `westminster`. Un système est connecté physiquement au pont `waterloo`, et un système est connecté physiquement au pont `tower`. Les ponts sont connectés physiquement les uns aux autres par le biais de ports.

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 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.

Fonctionnement d'un réseau ponté

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 réseau ponté. Au fil du temps, tous les ponts au sein du réseau "apprennent" quelle liaison 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. Les anciennes entrées de transfert sont également vidées à intervalle régulier. Lorsqu'une liaison est restaurée, les paquets reçus via cette liaison sont traités comme des nouveaux paquets. Le processus d'apprentissage démarre à nouveau, en fonction de l'adresse source d'un paquet. Ce processus permet au pont de transférer correctement des paquets sur cette liaison lorsque l'adresse est utilisée comme adresse de destination.

Protocoles de pontage

Les réseaux pontés utilisent les protocoles suivants :

- Spanning Tree Protocol (STP)

  La valeur par défaut STP est utilisé par le protocole que les réseaux pontés est. Par conséquent, le pontage utilise le mécanisme STP (Spanning Tree Protocol) pour éviter les boucles réseau qui rendraient les sous-réseaux inutilisables. 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.

Attention - 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.

Ces problèmes de performances ont une incidence uniquement sur les liaisons configurées pour faire partie d'un pont. 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.

- Transparent Interconnection of Lots of Links (TRILL)

  Oracle Solaris prend en charge l'amélioration de la protection TRILL, ce qui permet d'éviter les boucles sans désactiver des liens. Permet d'équilibrer la charge TRILL le trafic entre plusieurs chemins à la destination.

Lorsque STP est utilisé, la boucle physique est atténuée en empêchant une des connexions dans la boucle de transmettre des paquets. Dans la Figure 4-3, “Réseau ponté en anneau”, la liaison physique entre les ponts `westminster` et `tower` ne sert pas à transmettre des paquets.

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 noeud TRILL au sein du réseau et les utilise pour transférer les paquets vers différentes destinations.

Vous pouvez utiliser TRILL en spécifiant l'option `-P trill` dans les commandes `dladm create-bridge` ou `dladm modify-bridge` Pour plus d'informations, reportez-vous“Création d'un pont” à la page 72 et “Modification du type de protection d'un pont” à la page 73.

Pour plus d'informations sur le protocole STP, reportez-vous au document IEEE 802.1D-1998. 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).

Démon STP

Chaque pont créé à l'aide de la commande `dladm create-bridge` est représenté comme une instance de service de l'utilitaire de gestion des services (SMF) qui porte le même nom (`svc:/network/bridge`). Chaque instance exécute une copie du démon `/usr/lib/bridged`, qui met en oeuvre le protocole STP.

L'exemple de commande ci-dessous crée un pont nommé `pontevecchio`

```
# dladm create-bridge pontevecchio
```

Le système crée une instance de service SMF nommée `svc:/network/bridge:pontevecchio` et un noeud d'observabilité nommé `/dev/net/pontevecchio0`. Le noeud d'observabilité est destiné à être utilisé avec la commande `snoop` et l'analyseur de paquets `wireshark`. Vous pouvez utiliser la commande`dlstat` pour obtenir les statistiques d'exécution du pont.

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 un port particulier n'est pas connecté à un autre pont (car le port établit une connexion point à point directe à un système hôte, par exemple), vous pouvez désactiver administrativement STP sur ce port. Même si sur tous les ports d'un pont STP est désactivé, le démon STP continue de s'exécuter 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 lorsqu'elle 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 ci-dessous crée un pont nommé `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` .

Création d'un pont

Dans Oracle Solaris, il faut exécuter la commande `dladm` et l'utilitaire SMF pour administrer les ponts. Vous pouvez tirer parti des commandes SMF pour activer, désactiver et surveiller les instances de pont à l'aide de l'identifiant FMRI (Fault-Managed Resource Identifier) de l'instance (`svc:/network/bridge`). Vous pouvez exécuter la commande `dladm` pour créer ou détruire des ponts, mais aussi pour associer des liaisons aux ponts ou en retirer. Les liaisons affectées au pont doivent être de type Ethernet (médias 802.3 et 802.11 compris).

Pour configurer un pont entre des liaisons, il faut 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 d'un pont maximum.

La commande `dladm create-bridge` crée une instance de pont et affecte éventuellement 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 Solari ne crée pas de ponts entre les liaisons réseau.

Pour créer un pont, utilisez la commande suivante :

```
# dladm create-bridge [–P protect] [–p priority] [–d forward-delay] [–l link...] bridge-name
```

`-P` *protect* — Indique la méthode de protection. Mode doit être défini sur l'une des valeurs suivantes.

- `stp` : méthode de protection STP (valeur par défaut)
- `trill` : méthode de protection TRILL

`-p` *priority* — Indique une valeur de priorité STP IEEE pour un pont afin de déterminer le noeud de pont root dans le réseau. La valeur par défaut est `32768`. Les valeurs valides sont comprises entre `0` (priorité la plus élevée) et `61440` (priorité la plus basse), par incréments de 4096.

`-d` *forward-delay* — Paramètre spécifie le délai STP pour le pont, qui se trouve au-dessous . Lorsque le pont créé est le noeud root, tous les ponts du réseau utilisent cette horloge pour séquencer les états de liaison lorsqu'un port est activé. La valeur par défaut est `15` secondes. Les valeurs valides sont comprises entre `4` et `30` secondes.

`-l` *link* — Ajoute une liaison à un pont. Si l'une des liaisons indiquées ne peut pas être ajoutée, la commande échoue et le pont n'est pas créé.

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'inclut aucune séquence d'échappement, ce qui signifie qu'il ne peut contenir ni espaces ni caractères de contrôle ASCII ni les caractères suivants :

```
; / ? : @ & = + $ , % < > # "
```

Le nom `default` et les noms commençant par la chaîne `SUNW`sont réservés. Les noms contenant des chiffres de fin sont réservés à la création des périphériques d'observabilité qui servent au débogage. En raison de l'utilisation de périphériques d'observabilité, les noms d'instances de pont valides doivent également être des noms `dlpi` valides. 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.

Pour plus d'informations sur les options de création de pont, reportez-vous à la description de la commande `dladm create-bridge` dans la page de manuel dladm(1M).

EXEMPLE 4-1 Création d'un pont

L'exemple ci-dessous illustre comment créer le pont `brooklyn` en connectant les liaisons `net0` et `net1`.

```
# dladm create-bridge -P stp -d 12 -l net0 -l net1 brooklyn
# dladm show-bridge
BRIDGE       PROTECT ADDRESS           PRIORITY DESROOT
goldengate   stp     32768/8:0:20:bf:f 32768    8192/0:d0:0:76:14:38
brooklyn     stp     32768/8:0:20:e5:8 32768    8192/0:d0:0:76:14:38
```

L'exemple suivant illustre comment créer le pont `westminister` en connectant les liaisons `net0` et `net1`

```
# dladm create-bridge -P trill -l net0 -l net1 westminister
# dladm show-bridge
BRIDGE       PROTECT ADDRESS           PRIORITY DESROOT
goldengate   stp     32768/8:0:20:bf:f 32768    8192/0:d0:0:76:14:38
westminister trill   32768/8:0:20:e5:8 32768    8192/0:d0:0:76:14:38
```

Modification du type de protection d'un pont

STP est un mécanisme permettant d'éviter les boucles réseau qui peut rendre les sous-réseaux inutilisables. Outre l'utilisation de STP Oracle Solaris prend en charge pour les ponts, 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.

Pour modifier le type de protection de STP en TRILL ou de TRILL en STP, utilisez la commande suivante :

```
# dladm modify-bridge -P protection-type bridge-name
```

L'option `-P` *protection-type* spécifie le type de protection à utiliser, notamment `stp` (valeur par défaut) ou `trill`.

EXEMPLE 4-2 Modification du type de protection d'un pont

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
```

L'exemple suivant indique comment modifier le type de protection pour le pont `brooklyn` en remplaçant la valeur TRILL par STP.

```
# dladm modify-bridge -P stp brooklyn
```

Ajout de liaisons à un pont existant

Une liaison peut être membre d'un pont tout au plus. Par conséquent, si vous souhaitez déplacer une liaison d'une instance de pont à une autre, il faut commencer par supprimer la liaison du pont actuel avant de l'ajouter à un autre.

Les liaisons associées au même pont doivent toutes posséder la même valeur MTU. Bien que cela soit possible sur une liaison existante MTU valeur, l'instance de pont passe à l'état de maintenance jusqu'à ce que vous supprimiez ou modifiiez les liaisons affectées, de sorte que les valeurs MTU correspondent avant le redémarrage du pont.

Remarque - 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'un groupement ou les liaisons qui constituent elles-mêmes des groupements peuvent être affectées à un pont.

Pour ajouter une nouvelle liaison à un pont existant, utilisez la commande suivante :

```
# dladm add-bridge -l new-link bridge-name
```

L'exemple ci-dessous illustre comment ajouter la liaison `net2` au pont `rialto`.

```
# dladm add-bridge -l net2 rialto
```

Suppression des liaisons d'un pont

Avant de supprimer une pont, tous les liens correspondants doit d'abord être supprimé. Pour supprimer les liaisons, utilisez la commande suivante :

```
# dladm remove-bridge [-l link]... bridge-name
```

L'exemple ci-dessous illustre comment supprimer les liaisons `net0`, `net1` et `net2` du pont `charles`.

```
# dladm remove-bridge -l net0 -l net1 -l net2 charles
```

Paramétrage des propriétés de liaisons d'un pont

Vous pouvez définir le : les propriétés de liaison suivantes pour les ponts

`default_tag`	ID la valeur par défaut pour les paquets sans étiquette VLAN sont envoyées à l'une des rubriques ci-dessous et reçus à partir d'un lien. Les valeurs valides sont comprises entre `0` et `4094`. La valeur par défaut est `1`.
`forward`	Active ou désactive le transfert 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`.
`stp`	Active ou 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.
`stp_cost`	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.
`stp_edge`	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`.
`stp_p2p`	Spécifie le type de mode de connexion. Les valeurs valides sont `true`, `false` et `auto`. La valeur par défaut est `auto`.
`stp_priority`	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`.

Pour plus d'informations, reportez-vous à la page de manuel `dladm`(1M).

Pour modifier les propriétés de lien d'un pont, utilisez la commande suivante :

`dladm set-linkprop -p` *prop=value link*

EXEMPLE 4-3 Paramétrage des propriétés de liaisons d'un pont

L'exemple suivant montre comment désactiver la transmission du trafic et définissez le type de mode de connexion. Pour définir les propriétés pour le pont, vous devez définir ses propriétés sur les liens qui connectent les pont.

```
# dladm create-bridge -P stp -d 12 -l net0 -l net1 brooklyn
# dladm set-linkprop -p forward=0 net0
# dladm set-linkprop -p stp_p2p=true net1
```

L'exemple suivant décrit la réinitialisation de plusieurs propriétés d'un pont.

```
# dladm reset-linkprop -p default_tag,stp_priority brooklyn
```

Affichage des informations de configuration de pont

Vous pouvez afficher les informations de configuration de pont à l'aide de la commande `dladm show-bridge`.

Affichage des informations sur les ponts configurés

Vous pouvez utiliser les commandes `dladm show-bridge` et `dlstat show-bridge`pour afficher différents types d'informations sur les ponts configurés.

Les options de la commande dans le tableau ci-dessous :

- Afficher la liste des ponts :

  ```
  # dladm show-bridge
  ```

  ```
  # 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
  ```

- Pour afficher le lien d'un pont état relatives aux :

  ```
  # dladm show-bridge -l bridge-name
  ```

- Afficher les statistiques sur les liaisons du pont :

  ```
  # dlstat show-bridge 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
  ```

- Pour afficher les statistiques de chaque pont et les statistiques du pont liens : connectées les unes aux

```
# dlstat show-bridge

BRIDGE     LINK       IPKTS    RBYTES     OPKTS    OBYTES     DROPS  FORWARDS
rbblue0     --        1.93K   587.29K     2.47K     3.30M         0         0
           simblue1     72     4.32K     2.12K     2.83M         0        --
           simblue2  1.86K   582.97K       348   474.04K         0        --
stbred0     --         975   976.69K     3.44K     1.13M         0        38
           simred3    347   472.54K     1.86K   583.03K         0        --
           simred4    628   504.15K     1.58K   551.51K         0        --
```

- Chaque pour afficher toutes les statistiques du pont et les statistiques du pont liens : connectées les unes aux

```
# dlstat show-bridge -o all
```

Pour plus d'informations sur les options de la commande `dladm show-bridgee`, reportez-vous à la page de manuel dladm(1M), et pour plus d'informations sur les options de commande `dlstat show-bridge`, reportez-vous à la page de manuel dlstat(1M).

EXEMPLE 4-4 Affichage des informations du pont

Les exemples suivants illustrent l'utilisation de la commande avec diverses options`dladm show-bridge`.

- La commande ci-dessous affiche les informations d'état relatives aux liaisons d'une seule instance de pont (`tower`). Pour afficher les propriétés configurées, exécutez la commande `dladm show-linkprop`.

```
# dladm show-bridge -l tower
LINK         STATE        UPTIME   DESROOT
net0         forwarding   117      8192/0:d0:0:76:14:38
net1         forwarding   117      8192/0:d0:0:76:14:38
```

- La commande ci-dessous affiche les entrées de transfert au niveau du noyau du pont spécifié, `avignon` :

```
# dladm show-bridge -f avignon
DEST              AGE     FLAGS  OUTPUT
8:0:20:bc:a7:dc   10.860  --     net0
8:0:20:bf:f9:69   --      L      net0
8:0:20:c0:20:26   17.420  --     net0
8:0:20:e5:86:11   --      L      net1
```

- La commande ci-dessous affiche les informations TRILL relatives au pont spécifié,`key` :

```
# dladm show-bridge -t key
NICK   FLAGS LINK        NEXTHOP
38628  --    london      56:db:46:be:b9:62
```

```
58753  L     --          --
```

Affichage des données de configuration sur les liaisons de pont

Vous utilisez la commande `dladm show-link` avec l'option `-o all` pour afficher le champ `BRIDGE` dans la sortie. Si une liaison est membre d'un pont, ce champ identifie le nom du pont dont il est membre. 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 `dladm show-link` sous forme de liaison distincte. Pour ce noeud, le champ `OVER` répertorie les liaisons membres du pont.

Utilisez la commande suivante pour afficher les données de configuration sur une liaison membre d'un pont.

```
# dladm show-link [-p]
```

L'option `-p` génère une sortie dans un format analysable.

Suppression d'un pont du système

Avant de supprimer un pont, vous devez d'abord supprimer tous les liens reliées au pont.

▼ Suppression d'un pont du système

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Supprimer tous les liens reliées au pont.**

   ```
   # dladm remove-bridge [-l link]... bridge-name
   ```

3. **Supprimez le pont du système.**

   ```
   # dladm delete-bridge bridge-name
   ```

Exemple 4-5 Suppression d'un pont du système

L'exemple ci-dessous illustre comment retirer les liaisons `net0`, `net1` et `net2` du pont `coronado` avant de supprimer le pont lui-même.

```
# dladm remove-bridge -l net0 -l net1 -l net2 coronado
# dladm delete-bridge coronado
```

Administration des VLAN sur les réseaux pontés

Par défaut, les VLAN configurés sur le système répartissent les paquets sur tous les ports définis 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 des paquets du VLAN spécifié sur cette liaison de pont. Pour plus d'informations sur les réseaux VLAN, reportez-vous au Chapitre 3, Réseaux virtuels à l'aide de la configuration de réseaux locaux virtuels.

Pour configurer un VLAN sur une liaison et désactiver le transfert de paquets vers ou à partir d'autres liaisons sur le pont, il faut désactiver le transfert en définissant la propriété `forward` du VLAN avec la commande `dladm set-linkprop`. Pour plus d'informations, reportez-vous à “Paramétrage des propriétés de liaisons d'un pont” à la page 75.

▼ Configuration de VLAN sur une liaison de données qui fait partie d'un pont

Avant de commencer Cette procédure part du principe que le pont existe déjà. Pour plus d'informations sur la création d'un pont, reportez-vous à “Création d'un pont” à la page 72.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Répertorier les informations relatives aux liaisons du pont pour déterminer les liaisons de données faisant partie du pont.**

   ```
   # dladm show-bridge -l bridge-name
   ```

3. **Sur le lien pour créer le VLAN qui fait partie du pont.**

   ```
   # dladm create-vlan -l link -v vid VLAN-link
   ```

link Spécifie la liaison sur laquelle créer l'interface VLAN.

Remarque - Dans cette procédure, le pont doit partie du lien que vous avez créées.

vid Indique le numéro d'ID d'un VLAN.

vlan-link Spécifie le nom du VLAN.

4. **Répétez cette commande pour chaque VLAN que vous souhaitez créer. Créez une interface IP sur chacun des VLAN créés à l'étape précédente.**

   `# ipadm create-ip` *interface*

   où *interface* est le nom du VLAN.

5. **Attribuez une adresse IP valide à chacune des interfaces IP d'un VLAN.**

   `# ipadm create-addr -a` *IP-address interface*

Réseaux locaux virtuels (VLAN) et protocoles STP et TRILL

Les VLAN sont ignorés par le protocole 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 topologie arborescente 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 impérativement exécuter tous les VLAN en tout point de votre infrastructure de ponts ou examiner soigneusement toutes les liaisons redondantes.

Le protocole TRILL ne suit pas les règles STP complexes. Au contraire, TRILL encapsule automatiquement les paquets dont l'étiquette VLAN est intacte et les transmet via le réseau.

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`, par exemple `/dev/net/bridgeofsighs0`.

Le noeud d'observabilité est destiné à être utilisé avec la commande `snoop` et l'analyseur de paquets `wireshark`. Ce noeud fonctionne comme une interface Ethernet classique, à cette

exception près que les paquets sont silencieusement rejetés lors de leur transmission. Vous ne pouvez pas raccorder IP au-dessus d'un noeud d'observabilité, ni effectuer des demandes de liaison (`DL_BIND_REQ`), sauf si vous utilisez l'option `passive` qui vous permet uniquement d'recevoir des paquets et non pas de les envoyer.

Le noeud d'observabilité met une seule copie non modifiée de chaque paquet géré par le pont. Il est mis à disposition de l'utilisateur à la surveillance et à des fins de débogage. Ce comportement est similaire à celui d'un port de surveillance sur un pont traditionnel. Il est soumis aux règles habituelles de mode de promiscuité DLPI (Data Link Provider Interface). Vous pouvez également utiliser la commande `pfmod` ou les fonctionnalités de la commande `snoop` et de l'analyseur de paquets `wireshark` pour filtrer les paquets basés sur l'ID du VLAN.

Les paquets transmis, c'est - à - dire les paquets envoyés à l', représentent les données noeud d'observabilité reçues par le pont.

Remarque - Lorsque le pontage ajoute, supprime ou modifie une balise VLAN, les données affichées par la commande `snoop`et l'analyseur de paquets `wireshark` décrivent l'état qui précède paquet aux processus en cours. Ce cas rare peut être problématique si des valeurs `default_tag` distinctes sont définies 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.

Vous pouvez également obtenir les statistiques relatives à l'utilisation des ressources réseau par les paquets sur les liaisons en exécutant la commande `dlstat`. Pour plus d'informations, reportez-vous au Chapitre 8, “ Contrôle du trafic réseau et de l’utilisation des ressources ” du manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

♦ ♦ ♦ CHAPITRE 5

Echange d'informations sur la connectivité réseau avec Link Layer Discovery Protocol

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).

Ce chapitre aborde les sujets suivants :

Généralités sur LLDP

LLDP est utilisé par les systèmes dans un réseau local (LAN) pour l'échange des informations de configuration ou de gestion entre eux. Avec ce protocole, un système peut publier des informations sur la connectivité et la gestion à d'autres systèmes sur le réseau. Ces informations peuvent inclure les capacités du système, les adresses de gestion et d'autres informations relatives aux opérations du réseau. Ce protocole permet également d'utiliser un même système pour recevoir des informations similaires concernant d'autres systèmes sur le même réseau local.

Les composants individuels d'un réseau local (comme les systèmes et les commutateurs) ne sont pas configurés indépendamment les uns des autres. Pour héberger de manière efficace le trafic réseau, il faut en effet coordonner la configuration des systèmes.

Chaque lorsque vous procédez manuellement, configurer et d'autres systèmes, commutateurs, ce qui garantit la compatibilité des composants des composants est une question. En revanche, cette méthode est risquée et entraîne souvent des erreurs de configuration, en particulier si plusieurs administrateurs travaillent de façon indépendante sur différents systèmes. Une meilleure solution consiste à utiliser LLDP, ce qui permet aux systèmes de transmettre leurs

données de configuration aux systèmes homologues et permet de détecter les mauvaises configurations.

Prend en charge l'utilisation d'Oracle Solaris pour promouvoir l'échange des LLDP système et les informations de connectivité réseau entre les systèmes sur le réseau, ce qui permet de réduire les risques de configuré de manière incorrecte des ressources réseau.

Dans cette version, LLDP utilisées par le réseau de façon à détecter automatiquement diagnostic des problèmes de service, ce qui risque d'entraîner la connectivité réseau limitée ou ressources dégradés, ou les deux. L'activation du service LLDP réseau améliore la capacité pour effectuer des tests de diagnostic sur votre système Oracle Solaris. Pour plus d'informations sur le diagnostic du réseau, reportez-vous au Chapitre 4, “ Opérations de diagnostic réseau réalisées à l’aide de l’utilitaire de module de transport network-monitor ” du manuel “ Dépannage des problèmes d’administration réseau dans Oracle Solaris 11.2 ”.

Dans Oracle Solaris, le protocole LLDP permet également d'échanger des unités TLV DCBX (Data Center Bridging eXchange). La technologie DCBX fournit des données de configuration sur les fonctionnalités DCB, comme le contrôle de flux basé sur la priorité (PFC) et la sélection de transmission améliorée (ETS). Pour plus d'informations sur la technologie DCB, reportez-vous au Chapitre 6, Gestion des réseaux convergents avec Data Center Bridging.

Avec LLDP, l'administrateur système peut facilement détecter les configurations système défectueuses, notamment dans les réseaux complexes tels que des réseaux locaux virtuels (VLAN) et de groupements de liaisons. Il est possible d'obtenir facilement des informations sur la topologie sans qu'il soit nécessaire de tracer les connexions physiques entre les serveurs, les commutateurs et les autres périphériques qui composent le réseau.

Composants d'une implémentation LLDP

Le protocole LLDP est implémenté avec les composants suivants :

- **package LLDP** : ce package est installé pour activer le LLDP. Ce package fournit le démon LLDP, des utilitaires de ligne de commande, le manifeste et les scripts de service, ainsi que d'autres composants requis pour assurer le bon fonctionnement du protocole LLDP.
- **service LLDP** - Vous pouvez activer le service LLDP à l'aide de la commande `svcadm`. Ce service utilise l'identificateur de ressource de gestion des défaut (FMRI) de l'instance de service `svc:/network/lldp:default` de l'utilitaire de gestion des services (SMF), pour gérer le démon LLDP, `lldpd`. Ce service LLDP est responsable du démarrage, de l'arrêt, du redémarrage ou de l'actualisation du démon `lldpd`. Il est automatiquement activé lorsque vous installez le package LLDP.
- `lldpadm` **commande** : Vous pouvez exécuter cette commande pour administrer LLDP commande sur des liaisons individuelles et configurer le mode de fonctionnement de LLPD afin de spécifier les unités TLV LLDP qui sont transmises et pour configurer les unités TLV DCBX. Pour plus d'informations sur les unités TLV, reportez-vous à “Informations publiées par l'agent LLDP” à la page 86.

Vous devez utiliser cette commande pour définir les propriétés par agent et les propriétés LLDP globales anisi que pour obtenir les informations LLDP d'un agent particulier ou de son pair.

Les sous-commandes `lldpadm` sont décrites dans les sections suivantes. Pour plus d'informations sur la commande `lldpadm`, reportez-vous à la page de manuel `lldpadm`(1M).

- **démon LLDP** : Les services LLDP gèrent les agents LLPD définis sur le système. Ils interagissent également avec `snmpd`, le démon du protocole SNMP (Simple Network Management Protocol), pour récupérer les informations LLDP reçues sur le système via SNMP.
- **agents LLDP** : les agents LLDP sont des instances LLDP associées à une liaison de données physique sur laquelle le protocole LLDP est activé. Sur les agents LLDP pour transmettre les informations et la liaison de données qu'il gère les flux de données qui sont ses homologues (peer) du pair également. Vous pouvez configurer un agent LLDP doit être pris en charge pour les physique associé des informations spécifiques concernant la liaison de données. Vous pouvez activer physique LLDP uniquement sur les liaisons de données.

Sources d'informations de l'agent LLDP

L'agent LLDP transmet et reçoit des unités de données LLDP (LLDPDU). L'agent gère et stocke les informations contenues dans ces LLDPDU dans deux types de bases de données :

- **Base MIB (Management Information Base) locale** : cette base de données contient des informations réseau relatives à une liaison spécifique du système sur laquelle 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. Mais les ID de port sont différents pour les liaisons de données du système. Par conséquent, chaque agent gère sa propre MIB locale.
- **Base MIB distante** : les informations stockées dans cette base de données proviennent des agents LLDP activés sur les hôtes homologues.

Modes d'agent LLDP

L'agent LLDP peut fonctionner dans les modes suivants.

- En mode transmission uniquement (`txonly`), l'agent LLDP ne traite pas les LLDPDU entrantes. Par conséquent, la MIB distante est vide.
- En mode réception uniquement (`rxonly`), l'agent ne traite que les LLDPDU entrantes et stocke les informations dans des bases MIB distantes. Cependant, aucune information provenant de la base MIB locale n'est transmise.

- En mode transmission et réception (`both`), l'agent transmet des informations locales et traite que les LLDPDU entrantes, puis gère les bases MIB locales et distantes.
- En mode désactivé (`disable`), l'agent n'existe pas.

Pour plus d'informations sur la définition de l'agent LLDP, reportez-vous à “Activation de LLDP pour des ports spécifiques” à la page 91.

Informations publiées par l'agent LLDP

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 mises en forme individuellement au format TLV (type, longueur, valeur). Par conséquent, les unités d'information sont également appelées *unités TLV*.

Unités TLV obligatoires

Certaines unités TLV sont obligatoires et sont incluses par défaut dans les paquets LLDP lorsque le protocole LLDP est activé. Vous ne pouvez pas exécuter la commande `lldpadm` pour exclure une unité de cette nature.

Les unités TLV sont obligatoires suivants :

- Chassis ID : les informations générées par la commande `hostid`
- Port ID : Adresse MAC du port de l'ID de la NIC physique
- Durée de vie
- (Fin de PDU protocol data unit)

Il est possible d'activer plusieurs agents LLDP sur un même système en fonction du nombre de liaisons. La combinaison des ID de châssis et de port identifie un agent de manière unique et le distingue des autres agents définis sur le système.

EXEMPLE 5-1 ID et le port affichant les ID du châssis

L'exemple suivant affiche les ID et le port du châssis pour un agent LLDP.

```
# hostid
004e434e

# dladm show-phys -m net4
LINK                SLOT     ADDRESS            INUSE CLIENT
net4                primary  0:1b:21:87:8b:b4   yes   net4
```

```
# lldpadm show-agent -l net4
AGENT               CHASSISID           PORTID
net4                004e434e            00:1b:21:87:8b:b4
```

Les agents LLDP d'Oracle Solaris font appel à `hostid` comme ID de châssis et à l'adresse MAC comme l'ID de port.

Unités TLV facultatives

Des unités TLV facultatives peuvent être ajoutées à un paquet LLDP. Ces unités facultatives permettent aux fournisseurs d'insérer des unités TLV spécifiques à publier. Les unités TLV LLDP par permet de définir un supplémentaires à l'aide d'identifiants uniques d'organisme (OUI) individuels. Oui identifie la catégorie pour une unité TLV selon que le OUI suive la norme IEEE 802.1 ou la norme IEEE 802.3. Vous pouvez configurer des propriétés de l'agent LLDP pour activer ou désactiver la transmission de ces unités TLV facultatives.

Le tableau ci-dessous répertorie les types ou groupes TLV, les noms de propriétés correspondantes, les unités TLV pour chaque propriété et leurs descriptions. 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.

TABLEAU 5-1 LLDP facultatif de l'agent TLV Units for an

Groupe TLV	Nom de la TLV	Unités TLV	Description
Gestion de base	`basic-tlv`	`sysname`, `portdesc`, `syscapab`, `sysdesc`, `mgmtaddr`	Spécifie le nom du système, la description du port, les capacités du système, la description du système et l'adresse de gestion à publier.
OUI 802.1	`dot1-tlv`	`vlanname`, `pvid`, `linkaggr`, `pfc`, `appln`, `evb`, `etscfg`, `etsreco`	Spécifie le nom du réseau local virtuel, l'ID de VLAN du port, le groupement de liaisons, le contrôle de flux basé sur la priorité, l'application, la sélection de transmission améliorée et le pontage virtuel d'extrémité à publier.
OUI 802.3	`dot3-tlv`	`max-framesize`	Spécifie la taille de trame maximale à publier.
OUI spécifique à Oracle (défini comme `0x0003BA`)	`virt-tlv`	`vnic`	Spécifie la carte réseau virtuelle à publier si un réseau virtuel est configuré.

Propriétés de l'unité 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 d'un agent LLDP, elle est publiée sur le réseau uniquement avec les valeurs spécifiées. Prenons par exemple

la valeur TLV `syscapab`, qui publie 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 sur le système (comme les routeurs et les passerelles) soient publiées.

La procédure à suivre varie selon que vous configurez des *unités TLV globales* ou des *unités TLV par agent*. Pour plus d'informations sur la configuration, reportez-vous à "Spécification des unités TLV et valeurs pour un paquet LLDP d'un agent" à la page 93.

Les unités TLV globales s'appliquent à tous les agents LLDP du système. Le tableau suivant affiche les valeurs TLV globales et les configurations possibles correspondantes.

TABLEAU 5-2 Unités TLV globales et leurs propriétés

Unités TLV	Nom de la propriété	Valeurs possibles de la propriété	Description de la valeur
`syscapab`	`Prise en charge`	`autre`, `répétiteur`, `pont`, `wlan-ap`, `routeur`, `téléphone`, `docsis-cd`, `station`, `cvlan`, `sylvan`, `tpmr`	Principales fonctions prises en charge du système. Les valeurs par défaut sont `router`, `station` et `bridge`.
	`activé`	Sous-ensemble de valeurs répertoriées pour `supported`	Fonctions activées du système.
`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 sont propres à géré sur un agent LLDP par agent de base. Avec les unités TLV par agent , les valeurs que vous fournissez sont utilisées lorsque l'unité TLV est activée pour la transmission par un agent LLDP spécifique.

Le tableau suivant présente les valeurs TLV et les configurations possibles correspondantes pour un agent LLDP.

TABLEAU 5-3 Unités TLV par agent et leurs propriétés

Unités TLV	Nom de la propriété	Valeurs possibles de la propriété	Description de la valeur
`pfc`	`willing`	`on`, `off`	Indique à un agent LLDP d'accepter ou de rejeter les données de configuration d'un ordinateur distant qui ont trait au contrôle de flux basé sur la priorité.
`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 `id`/`selector`. Le contenu du tableau applique le format suivant :

Unités TLV	Nom de la propriété	Valeurs possibles de la propriété	Description de la valeur
			`id/selector/priority` Pour plus d'informations, reportez-vous à "Configurations de priorité d'application" à la page 113.
`etscfg`	`willing`	`on`, `off`	Indique à un agent LLDP d'accepter ou de rejeter les données de configuration d'un ordinateur distant qui ont trait à la sélection de transmission améliorée.

Pour plus d'informations sur les unités TLV, reportez-vous au Chapitre 6, Gestion des réseaux convergents avec Data Center Bridging.

Activation du protocole LLDP sur le système

Vous pouvez configurer LLDP de façon à ce qu'il échange des informations système avec des hôtes ou des homologues sur le réseau.

La propriété SMF `auto-enable-agents` contrôle le mode d'activation d'agents LLDP sur le système. Avec cette propriété, vous pouvez choisir d'activer le protocole LLDP à l'échelle globale (sur l'ensemble des liaisons physiques) ou sur une seule liaison physique à la fois.

La propriété `auto-enable-agents` peut avoir une des trois valeurs suivantes :

- `yes` pour activer le LLDP sur tous les ports en mode de transmission et réception (`both`) à condition que ce protocole n'ait pas configuré sur un port auparavant. Si une configuration existe déjà sur un port, elle est conservée. Par exemple, si un port a été configuré avec le protocole LLDP en mode `rxonly`, le service LLDP ne fait pas basculer l'agent en mode réception et transmission (`both`). Sur ce port, LLDP continue de fonctionner en mode `rxonly`. Il s'agit de la valeur par défaut de la propriété `auto-enable-agents`.
- `force` active le protocole LLDP en mode réception et transmission (`both`) sur tous les ports et remplace leur configuration LLDP existantes, le cas échéant. Par exemple, si un port a été précédemment configuré avec le protocole LLDP en mode `rxonly`, l'agent LLDP bascule en mode réception et transmission (`both`), le mode LLDP par défaut.
- `no` désactive la sélection automatique de LLDP sur tous les ports, sauf sur ceux qui ont été précédemment configurés avec ce protocole. Si une configuration LLDP existe déjà sur un port, elle est conservée.

Remarque - Notez que vous devez redémarrer le service SMF LLDP chaque fois que vous personnalisez la propriété `auto-enable-agents` pour que la nouvelle valeur soit prise en compte.

Installation du package LLDP

Le protocole LLDP est activé par défaut et prêt à utiliser au terme de l'installation du package LLDP.

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Installez le package.**

   ```
   # pkg install lldp
   ```

3. **Déterminez si le service LLDP a démarré.**

   ```
   # svcs lldp
   STATE          STIME    FMRI
   online         Jul_10   svc:/network/lldp:default
   ```

   Si le service LLDP est désactivé, démarrez-le en exécutant la commande suivante :

   ```
   # svcadm enable svc:/network/lldp:default
   ```

Activation de LLDP de manière globale

Avant de commencer Pour activer LLDP, vous devez au préalable installer le package LLDP. Pour plus d'informations, reportez-vous à "Installation du package LLDP" à la page 90.

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Modifiez la propriété SMF `auto-enable-agents` sur `yes` s'il est défini sur `no`.**

   ```
   # svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "yes"
   ```

   Par défaut, la valeur est de cette propriété sera `yes`.

3. **Redémarrez le service LLDP.**

   ```
   # svcadm restart svc:/network/lldp:default
   ```

4. **(Facultatif) Personnalisez les unités TLV globales.**

   ```
   # lldpadm set-tlvprop -p property=value  global-TLV
   ```

où *property* se réfère à la propriété de l'unité TLV globale.

Étapes suivantes

Pour plus d'informations sur les unités TLV globales, reportez-vous à n “Propriétés de l'unité TLV” à la page 87.

Pour afficher la liste des unités TLV globales, saisissez `lldpadm show-tlvprop` ou reportez-vous à Tableau 5-2, “Unités TLV globales et leurs propriétés”.

Pour obtenir des instructions sur la procédure permettant de définir des valeurs TLV, reportez-vous à “Définition des unités TLV” à la page 95.

Pour plus d'informations sur la commande `lldpadm`, reportez-vous à la page de manuel `lldpadm`(1M).

▼ Activation de LLDP pour des ports spécifiques

Avant de commencer

Pour activer LLDP, vous devez au préalable installer le package LLDP. Pour plus d'informations, reportez-vous à “Installation du package LLDP” à la page 90.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Modifiez la propriété SMF `auto-enable-agents` sur `no` si elle est paramétrée sur `yes`.**

   ```
   # svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
   ```

   Par défaut, la valeur est de cette propriété sera `yes`.

3. **Redémarrez le service LLDP si vous avez modifié la propriété SMF `auto-enable-agents` lors de l'étape 2.**

   ```
   # svcadm restart svc:/network/lldp:default
   ```

4. **Activez l'agent LLDP sur les ports ou les liaisons de votre choix.**

   ```
   # lldpadm set-agentprop -p mode=value agent
   ```

   où *agent* est l'agent LLDP et identifié par la liaison physique sur laquelle est activé l'agent. Par exemple, si vous activez LLDP sur `net0`, l'agent correspond à `net0`.

   Il est possible d'attribuer l'une des quatre valeurs suivantes à la propriété `mode`, représentant les modes de fonctionnement de l'agent LLDP : `tx`, `rx`, `both` ou `disable`. Pour plus d'informations sur ces valeurs, reportez-vous à la section “Modes d'agent LLDP” à la page 85.

5. **Spécifiez les unités TLV que l'agent LLDP doit publier.**

   ```
   # lldpadm set-agentprop -p property=value agent
   ```

   Pour plus d'informations sur les propriétés de l'agent LLDP, reportez-vous à la section “Informations publiées par l'agent LLDP” à la page 86.

   Pour afficher la liste des autres propriétés de l'agent LLDP, saisissez `lldpadm show-agentprop` ou reportez-vous à Tableau 5-1, “LLDP facultatif de l'agent TLV Units for an”.

   Pour obtenir des instructions sur la manière de spécifier paquet d'unités TLV pour un agent LLDP, reportez-vous à “Spécification des unités TLV d'un paquet LLDP d'un agent” à la page 94.

6. **(Facultatif) Personnaliser les unités TLV par agent.**

   ```
   # lldpadm set-agenttlvprop -p property=value -a agent per-agent-TLV
   ```

   où *property* se réfère à la propriété de l'unité TLV par agent.

   Pour plus d'informations sur les unités TLV par agent, reportez-vous à “Propriétés de l'unité TLV” à la page 87.

   Pour afficher la liste des unités TLV par agent, saisissez `lldpadm show-agenttlvprop` ou reportez-vous à Tableau 5-3, “Unités TLV par agent et leurs propriétés”.

   Pour obtenir des instructions sur la procédure permettant de définir des valeurs TLV, reportez-vous à “Définition des unités TLV” à la page 95.

   Pour plus d'informations sur la commande `lldpadm`, reportez-vous à la page de manuel `lldpadm`(1M).

Exemple 5-2 Personnalisation de la propriété SMF `auto-enable-agents`

L'exemple suivant illustre les différentes configurations du protocole LLDP si vous modifiez la valeur de la propriété SMF `auto-enable-agents`. Supposons que LLDP soit configuré sur deux ports sur un système qui en compte quatre, comme suit :

- `net0` : mode `both`
- `net1` : mode `rxonly`
- `net2` et `net3` : aucun mode

Si la propriété SMF `auto-enable-agents` a la valeur par défaut `yes`, LLDP est automatiquement activé sur `net2` et `net3`. Vous pouvez afficher la configuration comme indiqué ci-après : LLDP

```
# lldpadm show-agentprop -p mode
AGENT   PROPERTY   PERM   VALUE   DEFAULT   POSSIBLE
net0    mode       rw     both    disable   txonly,rxonly,both,disable
net1    mode       rw     rxonly  disable   txonly,rxonly,both,disable
net2    mode       rw     both    disable   txonly,rxonly,both,disable
```

```
net3    mode       rw     both    disable   txonly,rxonly,both,disable
```

Si vous modifiez la propriété SMF en lui attribuant la valeur `no`, la configuration change lorsque vous redémarrez le service.

```
# svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
# svcadm restart svc:/network/lldp:default
# lldpadm show-agentprop -p mode
AGENT   PROPERTY   PERM   VALUE    DEFAULT   POSSIBLE
net0    mode       rw     both     disable   txonly,rxonly,both,disable
net1    mode       rw     rxonly   disable   txonly,rxonly,both,disable
net2    mode       rw     disable  disable   txonly,rxonly,both,disable
net3    mode       rw     disable  disable   txonly,rxonly,both,disable
```

Dans l'exemple de sortie, `net2` et `net3`, dont le mode LLDP était précédemment activé automatiquement, sont à présent marquées comme désactivées. Cependant, aucune modification n'intervient sur les interfaces `net0` et `net1` sur lesquelles des agents LLDP ont été configurés précédemment.

Exemple 5-3 Activation du protocole LLDP sur plusieurs liaisons de données

Cet exemple illustre l'activation du protocole LLDP de façon sélective. Un système comprend deux liaisons de données (`net0` et `net1`). Pour définir `net0`, afin que l'agent transmette et reçoive des paquets LLDP sur `net1`, et afin que l'agent transmette uniquement des paquets LLDP, saisissez les commandes suivantes :

```
# svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
# svcadm restart svc:/network/lldp:default
# lldpadm set-agentprop -p mode=both net0
# lldpadm set-agentprop -p mode=txonly net1
# lldpadm show-agentprop -p mode
AGENT   PROPERTY   PERM   VALUE    DEFAULT   POSSIBLE
net0    mode       rw     both     disable   txonly,rxonly,both,disable
net1    mode       rw     txonly   disable   txonly,rxonly,both,disable
```

Spécification des unités TLV et valeurs pour un paquet LLDP d'un agent

Vous pouvez spécifier les unités TLV comme `dot1-tlv` et `basic-tlv` en tant que valeurs de propriété pour un agent LLDP. Vous pouvez également configurer ces valeurs de propriété. Utilisez la commande `lldpadm set-agentprop` pour spécifier les unités TLV. Pour plus d'informations, reportez-vous à la page de manuel `lldpadm`(1M). Lorsque l'unité TLV est spécifié sous la forme d'une propriété d'un agent LLDP, elle est alors diffusée sur le réseau uniquement avec les valeurs que vous avez indiqué pour les unités TLV. Pour plus d'informations sur les unités TLV et des propriétés, reportez-vous à “Propriétés de l'unité TLV” à la page 87.

Spécification des unités TLV d'un paquet LLDP d'un agent

Cette section indique comment spécifier les unités TLV à publier dans un paquet LLDP que transmet un agent.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **(Facultatif) Identifier les propriétés d'agent LLDP pouvant contenir l'unité TLV que vous souhaitez ajouter. pour ce faire, affichez les unités TLV**

   ```
   # lldpadm show-agentprop agent
   ```

   Reportez - vous à cette commande vous aide à les unités TLV déjà définies pour chaque propriété. Si vous n'indiquez pas de propriété, cette commande affiche toutes les propriétés de l'agent LLDP et leurs valeurs TLV. Pour obtenir la liste des propriétés de l'agent, reportez-vous àTableau 5-1, "LLDP facultatif de l'agent TLV Units for an".

3. **Ajouter ou supprimer l'unité TLV à partir de la propriété.**

   ```
   # lldpadm set-agentprop -p property[+|-]=value[,...] agent
   ```

   Vous pouvez utiliser des qualificatifs pour ajouter (+) ou supprimer (-) des valeurs de la liste de valeurs pour les propriétés qui acceptent plusieurs valeurs.

   Si vous n'utilisez pas les qualificatifs ajouter (+) ou supprimer (-), alors la valeur que vous avez définie remplace toutes les valeurs précédemment définies pour la propriété.

4. **(Facultatif) Affichez les nouvelles valeurs de la propriété.**

   ```
   # lldpadm show-agentprop -p property agent
   ```

Exemple 5-4 Ajout d'unités TLV facultatives à un paquet LLDP

Dans l'exemple suivant, l'agent LLDP VLAN possède une interface `net0` dédiée à la publication des informations VLAN dans son paquet LLDP. Le paquet est configuré de façon plus approfondie pour LLDP inclure les capacités du système, NIC groupement de liaisons en tant que virtuel, ainsi que les informations LLDP peut publier des éléments. Ultérieurement, la description, celui-ci est enlevé de VLAN du paquet.

1. Afficher les propriétés de l'agent existant.

   ```
   # lldpadm show-agentprop 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                  sysname,sysdesc,
                                                   syscapab,mgmtaddr,
                                                   all
net0    dot1-tlv   rw     vlanname,       none     none,vlanname,pvid,
                          pvid,pfc                 linkaggr,pfc,appln,
                                                   evb,etscfg,etsreco,all
net0    dot3-tlv   rw     max-framesize   none     none, max-framesize,
                                                   all
net0    virt-tlv   rw     none            none     none,vnic,all
```

La sortie contient les éventuels, par défaut et valeurs possibles pour chaque propriété de l'agent LLDP.

2. Groupement de liaisons ensemble, les capacités du système, et à la virtualisation du réseau en tant qu'articles doit être pris en charge pour les informations sur le réseau.

```
# lldpadm set-agentprop -p basic-tlv+=syscapab,dot1-tlv+=linkaggr,virt-tlv=vnic net0
```

3. Une description extraites de la supprimer le paquet VLAN.

```
# lldpadm set-agentprop -p dot1-tlv-=vlanname net0
```

4. Afficher les propriétés de l'agent.

```
# 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,                 sysname,sysdesc,
                          syscapab                 syscapab,mgmtaddr,
                                                   all
net0    dot1-tlv   rw     pvid,pfc        none     none,vlanname,pvid,
                          linkaggr                 linkaggr,pfc,appln,
                                                   evb,etscfg,etsreco,all
net0    dot3-tlv   rw     max-framesize   none     none, max-framesize,
                                                   all
net0    virt-tlv   rw     vnic            none     none,vnic,all
```

▼ Définition des unités TLV

Cette procédure indique comment attribuer des valeurs à des unités TLV spécifiques.

Astuce - Vous pouvez réinitialiser les propriétés sur leurs valeurs par défaut TLV à l'aide de la commande `lldpadm reset-tlvprop` pour les unités TLV globales et la commande `lldpadm reset-agenttlvprop` pour les unités TLV par agent.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Configurer une zone globale ou dans une unité TLV par agent.**

   - **Pour configurer une unité TLV globale, définissez la propriété TLV appropriée qui doit contenir les valeurs à publier.**

     ```
     # lldpadm set-tlvprop -p TLV-property=value[,value,value,...] TLV-name
     ```

     Remplacez *tlv-name* par le nom de l'unité TLV globale et *tlv-property* par sa propriété. Vous pouvez attribuer plusieurs valeurs à la propriété. Pour obtenir la liste des unités TLV globales et leurs propriétés, reportez-vous à Tableau 5-2, "Unités TLV globales et leurs propriétés".

   - **Pour configurer une unité TLV par agent, définissez la propriété TLV appropriée avec les valeurs que l'agent LLDP doit publier.**

     ```
     # lldpadm set-agenttlvprop -p TLV-property[+|-]=value[,value,value,...] -a agent TLV-name
     ```

     Remplacez *tlv-name* par le nom de l'unité TLV par agent et *tlv-property* par sa propriété. Vous pouvez attribuer plusieurs valeurs à la propriété. Pour obtenir la liste des unités TLV par agent et leurs propriétés, reportez-vous à Tableau 5-3, "Unités TLV par agent et leurs propriétés".

     Vous pouvez utiliser des qualificatifs pour ajouter (+) ou supprimer (-) des valeurs de la liste de valeurs pour les propriétés qui acceptent plusieurs valeurs.

3. **(Facultatif) Affichez les valeurs de la propriété TLV que vous venez de configurer.**

   - **Pour afficher les valeurs d'une propriété TLV globale, procédez comme suit :**

     ```
     # lldpadm show-tlvprop
     ```

   - **Pour afficher les valeurs des propriété TLV un agent, procédez comme suit :**

     ```
     # lldpadm show-agenttlvprop
     ```

Exemple 5-5 Définir des valeurs TLV pour les unités TLV `syscapab` et `mgmtaddr`

Dans l'exemple suivant, des informations spécifiques sur les capacités du système à publier dans le paquet IP LLDP adresse et de gestion est configuré.

1. Configurez les propriétés `supported` et `enabled` de l'unité TLV `syscapab`.

```
# lldpadm set-tlvprop -p supported=bridge,router,repeater syscapab
# lldpadm set-tlvprop -p enabled=router syscapab
```

2. Spécifiez l'adresse IP de l'unité TLV `mgmtaddr`.

```
# lldpadm set-tlvprop -p ipaddr=192.168.1.2 mgmtaddr
```

3. Afficher les valeurs TLV des propriétés de l'agent.

```
# lldpadm show-tlvprop
TLVNAME    PROPERTY    PERM  VALUE        DEFAULT         POSSIBLE
syscapab   supported   rw    bridge,      bridge,router,  other,router,
                             router,      station         repeater,bridge,
                             repeater                     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            --
```

La sortie inclut les valeurs par défaut des unités TLV ainsi que les valeurs que vous pouvez définir pour la propriété.

Pour plus d'informations sur la configuration des propriétés TLV par agent, reportez-vous au Chapitre 6, Gestion des réseaux convergents avec Data Center Bridging.

Désactivation de LLDP

Cette section décrit comment désactiver LLDP de façon sélective sur des ports individuels.

▼ Désactivation de LLDP

Pour désactiver le protocole LLDP à l'échelle globale sur l'ensemble des interfaces du système, suivez les étapes ci-après.

1. **Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Modifiez la propriété SMF LLDP à `no` afin de désactiver l'activation automatique de LLDP sur tous les ports à l'exception des configurations LLDP existantes.**

```
# svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
```

3. **Redémarrez le service LLDP.**

```
# svcadm restart svc:/network/lldp:default
```

4. **Désactivez LLDP sur chacun des ports sur lesquels une configuration précédente est conservée.**

   - **Cette commande désactive LLDP en modifiant le mode de l'agent.**

     ```
     # lldpadm set-agentprop -p mode=disable agent
     ```

     Remplacez *agent* par la liaison physique sur laquelle est activé l'agent LLDP. Par exemple, si vous activez LLDP sur `net0`, l'agent correspond à `net0`.

   - **Cette commande désactive LLDP en supprimant sa configuration du port.**

     ```
     # lldpadm reset-agentprop -p mode agent
     ```

     Dans cette commande, aucune valeur n'est attribuée à la propriété `mode`.

Attention - Si la propriété `auto-enable-agents` est définie sur `no`, puis est redéfinie sur `yes`, LLDP se comporte différemment que si l'agent défini sur ce port était simplement désactivé.

Contrôle des agents LLDP

La sous-commande `lldpadm show-agent` affiche toutes les informations publiées par un agent LLDP. Se rapportant à un système particulier, la publication peut se composer d'informations sur le système local transmises au reste du réseau ou des informations provenant d'autres systèmes sur le même réseau.

Affichage des informations publiées

Les informations peuvent être locales ou distantes. Les informations *locales* proviennent du système local. Les informations *distantes* proviennent d'autres agents définis sur le réseau LLDP et sont reçues par l'agent LLDP local.

Utilisez la commande`lldpadm show-agent` pour afficher les informations publiées.

```
# lldpadm show-agent -[l|r][v] agent
```

- `-l` affiche des informations locales publiées par l'agent LLDP local.
- `-r` affiche les informations distantes reçues par le agent LLDP.
- `-v` affiche les informations locales ou distantes détaillées.

EXEMPLE 5-6 Affichage d'informations publiées de l'agent LLDP

L'exemple ci-dessous illustre comment afficher les informations publiées 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.

Pour afficher les informations locales publiées par l'agent LLDP, entrez la commande suivante :

```
# lldpadm show-agent -l net0
AGENT   CHASSISID   PORTID
net0    004bb87f    00:14:4f:01:77:5d
```

Pour afficher les informations distantes LLDP publiées par l'agent, procédez comme suit :

```
# lldpadm show-agent -r net0
AGENT   SYSNAME   CHASSISID   PORTID
net0    hostb     0083b390    00:14:4f:01:59:ab
```

Pour afficher les informations locales en mode verbose, utilisez l'option -v :

```
# lldpadm show-agent -l -v net4
                                Agent: net4
                  Chassis ID Subtype: Local(7)
                          Chassis ID: 00843300
                     Port ID Subtype: MacAddress(3)
                             Port ID: 00:1b:21:89:03:d0
                    Port Description: --
                        Time to Live: 21 (seconds)
                         System Name: --
                   System Description: --
                Supported Capabilities: --
                  Enabled Capabilities: --
                     Management Address: --
                     Maximum Frame Size: --
```

```
                              Port VLAN ID: --
                              VLAN Name/ID: vlan1/22
                         VNIC PortID/VLAN ID: 02:08:20:63:2d:9d,02:08:20:e5:6c:af/21
                      Aggregation Information: --
                                  PFC Willing: On
                                      PFC Cap: 8
                                      PFC MBC: False
                                   PFC Enable: 4
                                  PFC Pending: True
                 Application(s)(ID/Sel/Pri): --
                                  ETS Willing: On
                           ETS Configured CBS: 0
                           ETS Configured TCS: 8
                           ETS Configured PAT: 0,1,2,3,4,5,6,7
                           ETS Configured BAT: 40,20,0,40,0,0,0,0
                           ETS Configured TSA: 2,2,2,2,2,2,2,2
                          ETS Recommended PAT: 0,1,2,3,4,5,6,7
                          ETS Recommended BAT: 40,20,0,40,0,0,0,0
                          ETS Recommended TSA: 2,2,2,2,2,2,2,2
                                     EVB Mode: Station
                               EVB GID (Station): Not Supported
                      EVB ReflectiveRelay REQ: Not Requested
                   EVB ReflectiveRelay Status: RR Not Enabled
                             EVB GID (Bridge): Not Supported
          EVB ReflectiveRelay Capable (RRCAP): Not Supported
          EVB ReflectiveRelay Control (RRCTR): Not Enabled
                        EVB max Retries (R): 0
        EVB Retransmission Exponent (RTE): 0
            EVB Remote or Local(ROL) and
                Resource Wait Delay (RWD): Local
            EVB Resource Wait Delay (RWD): 0
           EVB Remote or Local (ROL) and
                  Reinit Keep Alive (RKA): Local
              EVB Reinit Keep Alive (RKA): 0
                 Next Packet Transmission: 4 (seconds)
```

Pour afficher les informations distantes en mode verbose, utilisez l'option -v :

```
# lldpadm show-agent -r -v net4
                                    Agent: net4
                          Chassis ID Subtype: Local(7)
                                  Chassis ID: 00843300
                             Port ID Subtype: MacAddress(3)
                                     Port ID: 00:1b:21:89:03:d0
                           Port Description: --
                               Time to Live: 21 (seconds)
                                System Name: --
                           System Description: --
                        Supported Capabilities: --
                          Enabled Capabilities: --
                            Management Address: --
                            Maximum Frame Size: --
                                  Port VLAN ID: --
                                  VLAN Name/ID: vlan1/22
```

```
                VNIC PortID/VLAN ID: 02:08:20:63:2d:9d,02:08:20:e5:6c:af/21
             Aggregation Information: --
                         PFC Willing: On
                             PFC Cap: 8
                             PFC MBC: False
                          PFC Enable: 4
         Application(s)(ID/Sel/Pri): --
                         ETS Willing: On
                  ETS Configured CBS: 0
                  ETS Configured TCS: 8
                  ETS Configured PAT: 0,1,2,3,4,5,6,7
                  ETS Configured BAT: 40,20,0,40,0,0,0,0
                  ETS Configured TSA: 2,2,2,2,2,2,2,2
                ETS Recommended PAT: 0,1,2,3,4,5,6,7
                ETS Recommended BAT: 40,20,0,40,0,0,0,0
                ETS Recommended TSA: 2,2,2,2,2,2,2,2
                            EVB Mode: Station
                  EVB GID (Station): Not Supported
            EVB ReflectiveRelay REQ: Not Requested
         EVB ReflectiveRelay Status: RR Not Enabled
                   EVB GID (Bridge): Not Supported
EVB ReflectiveRelay Capable (RRCAP): Not Supported
EVB ReflectiveRelay Control (RRCTR): Not Enabled
                EVB max Retries (R): 0
  EVB Retransmission Exponent (RTE): 0
      EVB Remote or Local(ROL) and
          Resource Wait Delay (RWD): Local
      EVB Resource Wait Delay (RWD): 0
     EVB Remote or Local (ROL) and
            Reinit Keep Alive (RKA): Local
        EVB Reinit Keep Alive (RKA): 0
            Information Valid Until: 19 (seconds)
```

Affichage de statistiques sur les paquets LLDP

Vous pouvez afficher des statistiques LLDP pour obtenir plus d'informations sur les paquets LLDP publiés par le système local ou des systèmes distants. Les statistiques font référence aux événements importants qui impliquent la transmission et la réception de paquets LLDP.

- Pour afficher toutes les statistiques sur la transmission et la réception de paquets LLDP, procédez comme suit :

  ```
  # lldpadm show-agent -s agent
  ```

- 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 5-7 Affichage de statistiques sur les paquets LLDP

Cet exemple illustre comment afficher des informations sur la publication de paquets LLDP.

```
# lldpadm show-agent -s net0
AGENT IFRAMES IERR IDISCARD OFRAMES OLENERR TLVDISCARD TLVUNRECOG AGEOUT
net0        9    0        0      14       0          4          5      0
```

La sortie 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 unités TLV ne sont pas reconnues, peut-être parce qu'elles ne respectent pas les normes en vigueur. L'exemple montre également que 14 trames ont été transmises au réseau par le système local.

EXEMPLE 5-8 Affichage de statistiques sélectionnées sur les paquets LLDP

Cet exemple montre comment afficher les informations statistiques sélectionnées.

```
# # lldpadm show-agent -s -o iframes,oframes net4
IFRAMES  OFRAMES
0        10
```

♦ ♦ ♦ CHAPITRE 6

Gestion des réseaux convergents avec Data Center Bridging

Aujourd'hui encore, différents réseaux sont utilisés pour l'application de gestion du trafic de Fibre Channel, en fonction de répartition de la charge des exigences et le trafic réseau qui est en fonction de la bande passante disponible. Par exemple, LAN (Local Area Network) utilise Ethernet et SAN (Storage Area Network) utilise Fibre Channel. Toutefois, la technologie Data Center Bridging améliore l'Ethernet afin qu'il soit plus approprié pour différents types de trafic, c'est-à-dire le trafic convergent, mais aussi pour prendre en charge des fonctionnalités comme losslessness. DCB permet une infrastructure réseau efficace grâce à la consolidation de SAN et LAN et permet de réduire les coûts opérationnels et de gestion dans les centres de données.

Ce chapitre aborde les sujets suivants :

Présentation du Data Center Bridging (DCB)

Data Center Bridging est utilisé pour gérer la bande passante, la priorité relative et le contrôle de flux de plusieurs types de trafic réseau partageant la même liaison de réseau, par exemple, lors du partage d'une liaison de données entre les protocoles de mise en réseau et de stockage. Fibre Channel peut être consacré à l'hébergement de ce type de trafic. Toutefois, l'utilisation de

liaisons dédiées exclusivement au trafic Fibre Channel peut s'avérer coûteuse. C'est pourquoi le trafic FCoE (Fibre Channel over Ethernet) est employé plus fréquemment. DCB répond à la tendance de la technologie Fibre Channel à perdre des paquets lors de leur transmission via un réseau Ethernet.

DCB distingue le trafic en fonction des priorités, également appelés priorités de classe de service (CoS). L'hôte et le prochain saut utilisent le protocole d'échange DCBX pour négocier une configuration réseau, telles que l'absence de perte de trafic et un partage de bande passante minimal en fonction de priorités. Ce processus permet de traiter paquets à partir de différentes applications sur l'hôte et sur le réseau selon les priorités et de négocier la configuration correspondante en utilisant DCBX.

Chaque paquet du réseau DCB a un en-tête de VLAN qui contient une valeur de priorité DCB de 3 bits, c'est-à-dire une priorité DCB. Cette valeur de priorité 802.1p IEEE permet de distinguer chaque paquet Ethernet sur le réseau des autres paquets. Selon les valeurs de priorité des paquets, vous pouvez configurer DCB pour allouer à l'envoi de paquets de bande passante spécifique. Par exemple, tous les paquets dont la priorité est `1` doivent avoir PFC activé, et tous les paquets avec une priorité `2` doivent avoir PFC désactivé et disposer d'un partage de bande passante égal à 10%.

Vous pouvez configurer les fonctions DCB, telles que le contrôle de flux basé sur la priorité (PFC) et la sélection de transmission améliorée (ETS) en fonction de priorités. Pour plus d'informations sur PFC et ETS, reportez-vous à “Contrôle de flux basé sur la priorité (PFC)” à la page 105 et “Sélection de transmission améliorée” à la page 106

La propriété de la liaison de données `cos` DCB vous permet d'indiquer le CoS ou la priorité de la liaison de données. La valeur `cos` qui est définie sur une liaison de données principale ne s'applique pas aux cartes VNIC qui sont créés sur ce lien physique. Pour plus d'informations sur la personnalisation de PFC en fonction de la propriété `cos`, reportez-vous à “Personnalisation du contrôle de flux basée sur la priorité pour DCB” à la page 108. Pour plus d'informations sur la personnalisation d'ETS en fonction de la propriété `cos`, reportez-vous à “Personnalisation de la sélection de transmission améliorée pour DCB” à la page 114.

Dans Oracle Solaris, LLDP est utilisé pour échanger les unités type-longueur-valeur (TLV) DCBX. Pour plus d'informations sur LLDP, reportez-vous au Chapitre 5, Echange d'informations sur la connectivité réseau avec Link Layer Discovery Protocol. A condition que la NIC sous-jacente prend en charge les fonctions DCB, telles que le contrôle de flux basé sur la priorité et la sélection de transmission améliorée, les informations de configuration de ces fonctionnalités peuvent être partagés avec des hôtes homologues du réseau, comme suit :

- Le contrôle de flux basé sur la priorité (PFC) empêche la perte de paquets en mettant en oeuvre un mécanisme qui interrompt le flux de trafic des paquets de priorité CoS (classe de service) définie. Pour plus d'informations sur les classes de service, reportez-vous à la description de la propriété de liaison `cos` de la page de manuel `dladm`(1M).
- Permet de partager la bande passante ETS entre les paquets en fonction de CoS défini. Reportez-vous à la section “Sélection de transmission améliorée” à la page 106.

Eléments à prendre en compte lors de l'utilisation de la technologie DCB

Veuillez tenir compte des considérations suivantes concernant l'utilisation de DCB :

- La technologie DCB est prise en charge *uniquement* sur les NIC Intel Niantic physiques.

  Afin de vous assurer que le NIC prend en charge la technologie DCB, exécutez la commande suivante :

  ```
  # dladm show-linkprop -p ntcs agent
  ```

  Une valeur de propriété supérieure à zéro (`0`) indique que la carte réseau prend en charge DCB.
- Les ports DCB configurés en mode DCB ne peut pas être agrégés (Groupements tronçon ou DLMP).
- Comme DCB prend uniquement en charge la version IEEE de DCBX (et non des versions CEE ou CIN), les ponts externes doivent prendre en charge la norme IEEE dans le but d'interagir avec Oracle Solaris DCB.
- DCB prend en charge la configuration ETS et les recommandations TLV.
- DCB n'est pris en charge que dans 8 configurations de la classe de trafic.
- DCB ne prend pas en charge la notification de congestion (congestion).

Contrôle de flux basé sur la priorité (PFC)

Le contrôle de flux basé sur la priorité (PFC) étend le cadre 802.3x PAUSE standard pour inclure les valeurs de classe de service IEEE 802.1p. Grâce au contrôle de flux basé sur la priorité, l'ensemble du trafic sur la liaison n'est pas interrompu lorsqu'une trame PAUSE est envoyée, mais le trafic est suspendu uniquement en fonction des valeurs CoS activées dans la trame PFC. Une structure PFC est envoyée pour la priorité `cos` activée qui correspond au trafic à suspendre. L'hôte émetteur interrompt le trafic présentant cette valeur de la propriété `cos` tandis que le trafic pour d'autres valeurs de propriété `cos` désactivées n'est pas affecté. Au terme du délai spécifié dans la trame PFC, la transmission de paquets interrompus reprend.

La suspension basée sur des valeurs CoS garantit que les paquets ne sont pas supprimés pour cette valeur de la propriété `cos`. Pour les paquets sans valeur CoS définie ou avec des valeurs CoS qui n'ont pas PFC activé, aucun cadre PAUSE n'est envoyé. Ainsi, le trafic se poursuit en un flux continu et des paquets risquent d'être rejetés en cas de congestion. La gestion de paquets perdus dépend de la pile de protocole, par exemple TCP.

Il existe deux types d'informations DCB local sur l'hôte : des informations DCB distantes et des informations DCB. Pour que les fonctionnalités PFC soient opérationnelles, ces deux types d'informations DCB doivent être symétriques afin d'assurer le contrôle de flux basé sur

la priorité sur l'hôte. En règle générale, l'hôte local doit pouvoir mettre en correspondance les informations DCB qu'il reçoit de son homologue. Si vous activez DCB sur votre système, la technologie DCB synchronise les informations DCB avec le pair.

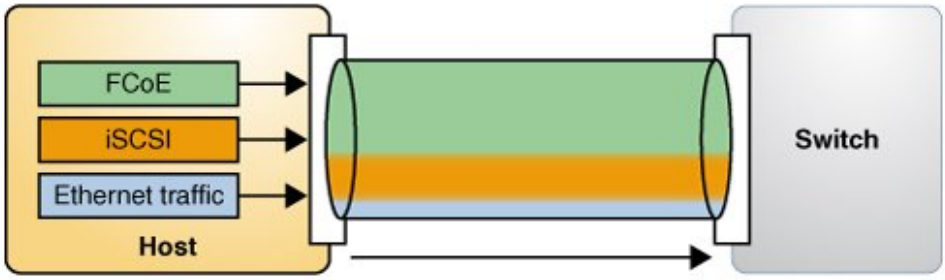
Dans la plupart des cas, la configuration par défaut de PFC suffit. Cette configuration est automatiquement définie lorsque vous activez LLDP. Toutefois, il est possible d'adapter différentes options lors de la configuration de PFC. Pour plus d'informations, reportez-vous à “Personnalisation du contrôle de flux basée sur la priorité pour DCB” à la page 108 et “Affichage des informations de configuration PFC” à la page 110.

Sélection de transmission améliorée

La sélection de transmission améliorée est une fonction DCB qui permet d'allouer de la bande passante sur une carte réseau à des applications en fonction de leur priorité DCB.

La figure suivante illustre la fonction d'ETS de DCB dans un réseau.

FIGURE 6-1 Slection de transmission améliorée dans DCB



L'hôte de la figure a différents types de trafic, tels que FCoE et iSCSI, qui partagent la même bande passante de liaison. Dans la figure, la priorité et une bande passante comme indiqué dans le tableau suivant ont été affectés à différents types de trafic.

Trafic	Priorité	Bande passante
FCoE	3	60%
iSCSI	4	30%
Trafic Ethernet (non iSCSI)	0	10%

Le protocole DCBX TLV ETS et l'allocation de bande passante ETS sont comme suit :

Priorité	0	1	2	3	4	5	6	7
Pourcentage d'allocation de la bande passante	10	0	0	60	30	0	0	0

Pour utiliser la fonction ETS, la fonction NIC doit la prendre en charge et s'exécuter en mode DCB. Lorsque vous activez LLDP, la configuration par défaut pour la fonction ETS est automatiquement configurée si le lien sous-jacent prend en charge DCB. Cependant, vous pouvez modifier la configuration par défaut. Pour plus d'informations, reportez-vous à “Personnalisation de la sélection de transmission améliorée pour DCB” à la page 114, “Recommandation de la configuration ETS aux homologues” à la page 117 et“Affichage des informations de configuration ETS” à la page 119.

Activation de DCBX

La prise en charge de DCBX est assurée automatiquement lorsque vous activez le protocole LLDP. La procédure ci-dessous présente les opérations à effectuer manuellement en cas d'échec de certains processus automatiques.

▼ Activation manuelle de la fonction d'échange Data Center Bridging

Avant de commencer Vérifiez que vous installez LLDP. Pour plus d'informations sur l'activation LLDP, reportez-vous à “Activation du protocole LLDP sur le système” à la page 89.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Assurez-vous que le service LLDP est en cours d'exécution.**

   ```
   # svcs lldp
   ```

   Si le service LLDP est désactivé, démarrez-le en exécutant la commande suivante :

   ```
   # svcadm enable svc:/network/lldp:default
   ```

3. **Vérifiez que l'agent LLDP s'exécute en mode réception et transmission.**

```
# lldpadm show-agentprop -p mode agent
```

Si l'agent LLDP ne fonctionne pas dans ces deux modes, entrez la commande suivante :

```
# lldpadm set-agentprop -p mode=both agent
```

Pour les autres configurations possibles des agents LLDP, reportez-vous à la section “Activation du protocole LLDP sur le système” à la page 89.

4. **Assurez-vous que la carte réseau sous-jacente prend en charge DCB.**

```
# dladm show-linkprop -p ntcs agent
```

Une valeur de propriété supérieure à zéro (`0`) indique que la carte réseau prend en charge DCB.

Personnalisation du contrôle de flux basée sur la priorité pour DCB

PFC et ETS sont activés par défaut et uniquement si la NIC sous-jacente est en mode DCB. Si vous préférez utiliser uniquement la fonctionnalité PFC, vous devez supprimer `etscfg` de la propriété `dot1 -tlv` de l'agent LLDP à l'aide de la commande suivante :

```
# lldpadm set-agentprop -p dot1-tlv-=etscfg net0
```

Pour consulter la liste des valeurs possibles pour `dot1–tlv`, reportez-vous à Tableau 5-1, “LLDP facultatif de l'agent TLV Units for an”.

Configuration des propriétés de liaisons de données liées à PFC

La fonction PFC de DCB fournit les propriétés de liaison de données suivantes :

- `pfcmap` : Fournit des informations sur les mises en correspondance et les définitions. La propriété `pfcmap` fait référence à un masque à 8 bits (`0`–`7`) qui représente les priorités. Le bit le plus faible représente la priorité `0`, et le bit le plus élevé la priorité `7`. Chaque bit de ce masque indique si la norme PFC est activée pour une priorité correspondante. Par défaut, la propriété `pfcmap` est définie sur `1111111`, ce qui signifie que la fonction PFC est activée pour toutes les priorités.
- `pfcmap-rmt-effective` : fait référence au mappage PFC en vigueur sur l'homologue distant. Cette propriété est en lecture seule.

Dans un réseau DCB, lorsqu'une récepteur est incapable de faire face au débit entrant du trafic, il envoie une trame PFC à l'expéditeur lui demandant de mettre en suspense le trafic pour les priorités possédant PFC activé. Pour tout paquet transmis via une liaison, DCB envoie une trame PFC à là l'hôte émetteur en cas de la congestion du trafic s'accumulant sur l'hôte récepteur. Pour envoyer les trames PFC correctement, les hôtes communiquant doivent disposer des informations de configuration DCB symétriques. Un système peut ajuster automatiquement sa configuration PFC pour qu'elle corresponde à celle de l'homologue distant. Vous pouvez déterminer le mappage PFC en vigueur sur l'hôte local au moyen de la commande `dladm show-linkprop` permettant d'afficher la valeur `EFFECTIVE` de la propriété `pfcmap`. Pour plus d'informations, reportez-vous à “Définition des propriétés de liaison de données” à la page 111.

▼ Personnalisation du contrôle de flux basé sur la priorité pour DCB

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Assurez-vous que la propriété `flowctrl` de la liaison de données est définie sur `pfc`.**

   ```
   # dladm show-linkprop -p flowctrl datalink
   ```

   Si la propriété n'est pas définie sur `pfc` ou `auto`, utilisez la commande suivante :

   ```
   # dladm set-linkprop -p flowctrl=pfc datalink
   ```

3. **Définissez la propriété `pfcmap`, sur une valeur différente de la valeur par défaut `11111111`.**

   ```
   # dladm set-linkprop -p pfcmap=value datalink
   ```

   Par exemple, pour activer la priorité CoS 6, entrez la commande suivante :

   ```
   # dladm set-linkprop -p pfcmap=01000000 net0
   ```

Unités hors main-d'oeuvre de la définition de la TLV PFC

DCB utilise les unités TLV PFC pour échanger des informations PFC entre les hôtes. Soit les hôtes doivent avoir la même valeur pour la propriété `pfcmap`, soit un hôte au moins doit être

disposé à accepter la configuration de ses pairs. Vous pouvez définir la propriété `pfcmap` à l'aide de la commande `dladm set-linkprop`.

La propriété TLV `willing` indique si l'hôte est prêt à accepter la configuration du pair, si la configuration de l'hôte est différente de la configuration du pair. Par défaut, la valeur de la propriété `willing` est définie sur `on`, ce qui indique que l'hôte accepte la configuration du pair.

Pour vérifier si l'hôte est en mesure de synchroniser ses informations PFC avec celles de l'homologue distant, vous devez déterminer si `willing` est défini sur `on` à l'aide de la commande suivante :

```
# lldpadm show-agenttlvprop -p willing -a agent pfc
```

Si la propriété TLV PFC `willing` est définie sur `off`, entrez la commande suivante pour configurer sur la propriété `willing` sur `on` et activez la fonction de synchronisation.

```
# lldpadm set-agenttlvprop -p willing=on -a agent pfc
```

où *agent* est la liaison de données sur laquelle est activé l'agent.

EXEMPLE 6-1 Activation de la synchronisation entre l'hôte et le pair

Afin de permettre la synchronisation pour une liaison de données `net0`, tapez la commande suivante :

```
# lldpadm set-agenttlvprop -p willing=on -a net0 pfc

# dladm show-linkprop -p pfcmap,pfcmap-rmt net0
LINK   PROPERTY    PERM  VALUE      EFFECTIVE  DEFAULT    POSSIBLE
net0   pfcmap      rw    11111111   00010000   11111111   00000000-11111111
net0   pfcmap-rmt  r-    --         00010000   11111111   --
```

Dans cet exemple, les propriétés `pfcmap` et `pfcmap-rmt` ont la valeur `00010000`. Cela indique que l'hôte local s'est synchronisé avec le pair. Par conséquent, la fonction PFC est activée avec une priorité `4` pour l'instance d'hôte et l'homologue.

Pour plus d'informations, reportez-vous à la page de manuel `lldpadm`(1M).

Affichage des informations de configuration PFC

Cette section décrit les commandes pour afficher des informations liées à PFC après LLDP et DCB et donne des exemples d'utilisation de ces commandes.

Définition des propriétés de liaison de données

La commande suivante affiche les définitions de priorité et les mappages PFC en vigueur sur la liaison de données :

```
# dladm show-linkprop -p pfcmap,pfcmap-rmt datalink
```

Dans une liaison de données avec des informations PFC concordantes entre les homologues local et distant, les valeurs la colonne `EFFECTIVE` des propriétés `pfcmap-lcl-effective` et `pfcmap-rmt-effective` sont identiques, quelle que soit la valeur attribuée à `pfcmap`. Si l'option de synchronisation est désactivée sur l'hôte local, le champ `EFFECTIVE` de la propriété `pfcmap` reflète la valeur de la propriété `pfcmap` de l'hôte local.

EXEMPLE 6-2 Affichage des propriétés de liaison de données associées à PFC

Cet exemple illustre comment afficher le statut des propriétés de liaison de données associées au contrôle de flux basé sur la priorité.

```
# dladm show-linkprop -p pfcmap,pfcmap-rmt net0
LINK   PROPERTY      PERM   VALUE      EFFECTIVE  DEFAULT    POSSIBLE
net0   pfcmap        rw     11111111   11111111   11111111   00000000-11111111
net0   pfcmap-rmt    r-     --         --         --         --
```

Dans l'exemple, le champ `value` pour la propriété `pfcmap` contient la valeur de `11111111`. La sortie montre que la valeur par défaut est attribuée au mappage PFC défini sur l'hôte local, c'est-à-dire que les huit priorités sont activées. Les valeurs `EFFECTIVE` pour les propriétés `pfcmap` et `pfcmap-rmt` sont `11111111` et `--`. La non-concordance des valeurs du champ `EFFECTIVE` indique que l'hôte local n'a pas synchronisé ses informations PFC avec celles de l'homologue distant.

Vous pouvez utiliser la commande `lldpadm show-agenttlvprop`pour vérifier la valeur de la propriété `willing` et la commande `lldpadm show-agent -r` pour vérifier les informations TLV PFC du pair.

Affichage de la capacité de synchronisation des informations PFC de l'hôte local

Cette commande affiche la propriété TLV PFC qui contrôle la capacité d'un hôte à synchroniser son mappage PFC avec un homologue.

```
# lldpadm show-agenttlvprop -a agent pfc
```

Remplacez *agent* par la liaison de données sur laquelle est activé le protocole LLDP.

EXEMPLE 6-3 Affichage de la capacité de synchronisation des informations PFC de l'hôte local

Cet exemple illustre comment afficher le statut actuel de la capacité de l'hôte à s'adapter à la configuration PFC de son homologue.

```
# lldpadm show-agenttlvprop -a net0 pfc
AGENT   TLVNAME   PROPERTY   PERM   VALUE   DEFAULT   POSSIBLE
net0    pfc       willing    rw     off     on        on,off
```

Pour plus d'informations, reportez-vous à "Unités hors main-d'oeuvre de la définition de la TLV PFC" à la page 109.

Informations sur la mise en correspondance de l'affichage PFC entre l'hôte et l'homologue

La valeur `PFC Pending` renvoie l'état `True` si les informations PFC de l'hôte et de l'homologue ne correspondent pas. Dès que ces informations sont synchronisées, le statut `PFC Pending` repasse à `False`.

Cette commande vous avertit de la non-concordance des informations de mappage PFC entre l'hôte local et l'homologue.

```
# lldpadm show-agent -lv -o "PFC Pending" agent
```

```
# lldpadm show-agent -lv -o "PFC Pending" agent
```

EXEMPLE 6-4 Vérification de la symétrie des informations PFC entre l'hôte et l'homologue

Cet exemple illustre comment vérifier en cours d'exécution si les informations PFC de l'hôte et de l'homologue sont synchronisées ou pas.

```
# lldpadm show-agent -lv -o "PFC Pending" net0
PFC Pending: True
```

Pour afficher toutes les informations qu'un agent publie, utilisez l'option -v (verbose) de la commande `lldpadm show-agent` :

```
# lldpadm show-agent -v net0
```

Affichage des définitions de priorité

Cette commande affiche des informations PFC sur la liaison physique, à savoir les priorités activées sur la carte réseau physique.

```
# dladm show-phys -D pfc datalink
```

EXEMPLE 6-5 Affichage des définitions de priorité CoS

Cet exemple illustre comment afficher les définitions de priorité CoS actuelles sur une liaison de données spécifique en fonction de la valeur de la propriété `pfcmap`. Supposons par exemple que la propriété `pfcmap` est configurée comme suit : `01000000`. Pour afficher les mappages de priorité correspondants sur la liaison physique, il faudrait exécuter la commande suivante :

```
# dladm show-phys -D pfc net0
LINK  COS    PFC   PFC_EFFECT   CLIENTS
net0   0     YES   NO           net0,vnic1
       1     YES   YES          vnic2
       2     YES   NO           vnic3
       3     YES   NO           vnic4
       4     YES   NO           vnic5
       5     YES   NO           vnic6
       6     YES   NO           vnic7
       7     YES   NO           vnic8
```

Sur la liaison physique `net0`, la priorité est activée pour tous les clients de la VNIC configurée sur la liaison de données. Cependant, l'hôte local ajuste son mappage PFC en fonction de celui de l'homologue, comme l'indiquent les valeurs du champ `PFC_EFFECT`, où la priorité est désactivée pour `COS`, `0` et `2-7`. Ainsi, aucune trame PFC n'est échangée dans le cadre du trafic sur les VNIC, à l'exception de la carte `vnic2`, quelles que soient les ressources disponibles. Dans cette configuration, le rejet de paquets est autorisé dans le cadre du flux de trafic sur toutes les cartes VNIC, sauf `vnic2`. Concernant le trafic sur la carte `vnic2`, des trames PAUSE PFC sont envoyées en cas de congestion pour éviter la perte de paquets sur ce client.

Configurations de priorité d'application

Les informations de priorité des DCBX échange les associés à l'application. Les unités TLV d'application qui sont échangées via DCBX contiennent des informations sur la priorité à associer à une application figurant sur l'hôte. La priorité est définie dans la table de priorité des applications. Chaque entrée de la table contient le nom de l'application et la priorité qui lui est associée. Lorsque vous définissez une priorité pour une application, tous les paramètres de l'le PFC DCB de cette priorité et ETS s'appliquent à l'application. L'unité TLV d'application transmet aux autres hôtes les informations de priorité des applications extraites de cette table.

Par défaut, l'application accepte les mappages de priorité du pair. La propriété `willing` de l'unité TLV d'application `appln` est similaire à PFC et permet d'échanger des informations entre les pairs.

Les entrées de cette table respectent le format suivant :

protocol-ID/*selector*/*priorité*

La paire *protocol-id*/*selector* identifie l'application. La priorité de l'application correspondante est identifiée par une priorité contenant une valeur comprise entre `0` et `7`.

Pour échanger les informations relatives à la priorité d'une application avec d'autres hôtes, il faut définir l'unité TLV de l'application comme suit :

```
# lldpadm set-agenttlvprop -p property=value -a agent appln
```

Par exemple, dans le cadre du trafic FCoE, l'ID de protocole est `0x8906` et l'ID de sélecteur est `1`. Supposons que la priorité `4` est associée à cette application. Selon Tableau 5-3, “Unités TLV par agent et leurs propriétés” où sont répertoriés les paramètres permettant de configurer une unité TLV d'application, entrez la commande suivante :

```
# lldpadm set-agenttlvprop -p apt=8906/1/4 -a net0 appln
# lldpadm show-agenttlvprop -a net0 appln
AGENT   TLVNAME   PROPERTY   PERM   VALUE      DEFAULT   POSSIBLE
net0    appln     apt        rw     8906/1/4   --        --
```

Personnalisation de la sélection de transmission améliorée pour DCB

La configuration par défaut est automatiquement définie lorsque LLDP est activé et la technologie DCB est prise en charge par le lien sous-jacent . Dans cette configuration par défaut, la valeur `cos 0` est affectée à toute la bande passante. Toutefois, vous pouvez utiliser la commande`dladm set-linkprop` pour configurer les valeurs `cos` sur une liaison de données afin d'affecter une partie de la bande passante à cette liaison de données.

Les TLV ETS et recommandation sont activés par défaut pour une NIC. Pour consulter la liste des valeurs possibles pour `dot1–tlv`, reportez-vous à Tableau 5-1, “LLDP facultatif de l'agent TLV Units for an”.

Si vous souhaitez supprimer la TLV `pfc`, tapez la commande suivante :

```
# lldpadm set-agenttlvprop -p dot1-tlv-=pfc agent
```

Définition des propriétés ETS de la liaison de données

Les propriétés de liaison de données qui font référence aux informations PFC s'appliquent à la prévention de perte de paquets en fonction des priorités CoS définies pour ces paquets. Les

propriétés ETS se rapportent à l'attribution de partages de la bande passante de liaisons sous-jacente de la liaison sous-jacente en fonction de priorités.

DCB fournit les propriétés liées à ETS suivantes :

- `cos` : spécifie la classe de service ou priorité de la liaison de données. La valeur de cette propriété est comprise entre `0` et `7`. La valeur par défaut est `0`. La valeur `cos` est définie dans la balise VLAN des paquets transmis sur ce lien.
- `etsbw-lcl` : indique le volume de bande passante ETS alloué à la transmission sur la liaison de données. Cette propriété est configurable uniquement si la NIC physique sous-jacente présente des capacités DCB et prend en charge ETS propriété, et la propriété `cos` de la liaison n'est pas défini sur `0`. Vous définissez une valeur pour cette propriété sur une liaison de données en spécifiant le pourcentage de la totalité de la bande passante du lien physique sous-jacent . La somme des valeurs pour la propriété `etsbw-lcl` pour toutes les liaisons de données NIC par le biais de la même physique ne doit pas dépasser 100%.

  Le pourcentage de bande passante défini dans `etsbw-lcl` n'est pas un volume réservé exclusivement à ce client secondaire. Si la bande passante allouée n'est pas consommée, d'autres clients configurés de la même manière peuvent l'utiliser. D'autre part, l'allocation de bande passante s'applique uniquement à la transmission dans le cadre du trafic sur l'hôte.
- `etsbw-rmt-advice` : spécifie la valeurde bande passante ETS recommandée envoyée vers le pair. Par défaut, la valeur configurée localement de la propriété `etsbw-lcl` est recommandée au pair. Toutefois, vous pouvez recommander une valeur différente de la valeur de la propriété `etsbw-lcl` en configurant explicitement la propriété de la liaison de données `etsbw-rmt-advice`.

  La configuration de la propriété `etsbw-rmt-advice` est utile si la bande passante affectée à une liaison de données est asymétrique, ce qui signifie que la réception (Rx) de la bande passante et la transmission (Tx) sont différentes. Lorsque vous définissez explicitement la propriété `etsbw-rmt-advice`, la transmission de la recommandation ETS TLV DCBX démarre automatiquement.
- `etsbw-lcl-advice` : spécifie le partage de bande passante recommandé pour la liaison de données qui est envoyé par le pair à l'hôte local. Il s'agit d'une propriété en lecture seule.
- `etsbw-rmt` : spécifie le partage de bande passante configuré sur le pair de la liaison de données. Il s'agit d'une propriété en lecture seule.

Pour définir la priorité et allouer une bande passante à la VNIC, utilisez les commandes suivantes :

- Pour définir la priorité à la VNIC, procédez comme suit :

  ```
  # dladm set-linkprop -p cos=value VNIC
  ```
- Pour allouer un pourcentage de la bande passante de la liaison physique sous-jacente à une VNIC, procédez comme suit :

  ```
  # dladm set-linkprop -p etsbw-lcl=value VNIC
  ```

La valeur que vous attribuez à la propriété `etsbw-lcl` représente le pourcentage de bande passante de la liaison sous-jacente. La somme de toutes les valeurs de bande passante allouée aux clients ne doit pas dépasser 100 %.

- Pour recommander de manière explicite une bande-passante envoyée à un pair :

```
# dladm set-linkprop -p etsbw-rmt-advice=value VNIC
```

Vous pouvez déterminer le partage de bande passante effectivement implémenté sur la liaison de données de l'hôte local et le partage de bande passante configuré sur le pair à l'aide de la commande `dladm show-linkprop`. La valeur dans le champ `EFFECTIVE` de la sortie des propriétés `etsbw-lcl` et `etsbw-rmt` indique le partage de bande passante effectivement implémenté. Pour plus d'informations, reportez-vous à “Affichage des informations de configuration ETS” à la page 119.

Pour déterminer le volume de bande passante adapté aux paquets présentant des priorités spécifiques, mieux vaut définir des informations ETS symétriques ou synchronisées entre les hôtes en communication. Plus précisément, le système local qui est en mesure d'adapter le partage de bande passante doit s'adapter à la valeur de `etsbw-lcl-advice`. Un système Oracle Solaris peut ajuster automatiquement sa configuration ETS pour qu'elle corresponde à celle recommandée par le pair.

Définition des unités TLV ETS

La configuration TLV ETS (`etscfg`) détermine la façon dont l'hôte réagit aux recommandations ETS issues de l'homologue. Cette unité TLV possède une seule propriété configurable : `willing`. Par défaut, cette propriété est définie sur `on` et autorise l'hôte local à synchroniser sa configuration ETS avec celle de l'homologue distant.

Pour vérifier que l'hôte est en mesure de synchroniser ses informations ETS avec celles du pair distant, utilisez la commande suivante :

```
# lldpadm show-agenttlvprop -p willing -a agent etscfg
```

Si la propriété `willing` est définie sur `off`, tapez la commande suivante pour établir synchronisation :

```
# lldpadm set-agenttlvprop -p willing=on -a agent etscfg
```

Si vous devez interdire à un agent spécifique de procéder à la synchronisation automatique de ces informations, attribuez la valeur `off` à la propriété `willing`, comme suit :

```
# lldpadm set-agenttlvprop -p willing=off -a agent etscfg
```

où *agent* est la liaison de données sur laquelle est activé l'agent.

Recommandation de la configuration ETS aux homologues

Les valeurs de bande passante ETS configurées (`etsbw-lcl`) pour chaque priorité peuvent être recommandés à l'homologue de sorte que celui-ci puisse configurer les mêmes valeurs. Vous devez activer la propriété `etsreco` dans le type `dot1-tlv` de l'agent LLDP sur la NIC afin de recommander les valeurs de bande passante ETS. Les valeurs recommandées peuvent être identiques aux valeurs ETS configurées localement ou vous pouvez également configurer de manière explicite les valeurs recommandées en définissant les nouvelles propriétés de liaisons de données `etsbw-rmt-advice` à l'aide de la commande `dladm set-linkprop`. La configuration de la propriété `etsbw-rmt-advice` est utile si la bande passante allouée pour une liaison de données est asymétrique, ce qui signifie que la réception (Rx) de la bande passante et la transmission (Tx) sont différentes.

Par défaut, les valeurs configurées de la propriété `etsbw-lcl` sont utilisées pour recommander des valeurs au pair. Toutefois, vous pouvez recommander un autre valeur ETS en définissant une valeur différente pour la propriété `etsbw-rmt-advice`. Par exemple, si le trafic sur le réseau se déroule plus sur Tx, vous pouvez configurer une valeur ETS plus élevée pour la propriété `etsbw-lcl` (Tx sur l'hôte) et une valeur plus faible pour la propriété `etsbw-rmt-advice` (Rx sur l'hôte).

EXEMPLE 6-6 Recommandation de la configuration ETS aux homologues

1. Assurez-vous que la propriété `etsreco` est activée en affichant la propriété de type `dot1-tlv` de l'agent LLDP pour `net5`.

```
# lldpadm show-agentprop -p dot1-tlv net5
AGENT        PROPERTY   PERM VALUE          DEFAULT        POSSIBLE
net5         dot1-tlv   rw   etsreco,etscfg none           none,vlanname,pvid,
                                                           linkaggr,pfc,appln,
                                                           evb,etscfg,etsreco,
                                                           all
```

2. Allouer une part de 20% de la bande passante sous-jacente de la liaison pour `vnic1`.

```
# dladm set-linkprop -p etsbw-lcl=20 vnic1
# dladm show-linkprop -p etsbw-lcl vnic1
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
vnic1    etsbw-lcl       rw   20           20           0         --
```

Par défaut, la même valeur est recommandée pour le pair.

```
# dladm show-linkprop -p etsbw-rmt-advice vnic1
LINK     PROPERTY         PERM VALUE  EFFECTIVE    DEFAULT   POSSIBLE
vnic1    etsbw-rmt-advice rw   --      20           0         --
```

3. Afficher les informations échangées par LLDP.

```
# lldpadm show-agent -l -v net5
```

4. Afficher la bande passante recommandée aux homologues.

```
# dladm show-phys -D ets -r net5
LINK      COS ETSBW_RMT_EFFECT ETSBW_RMT_ADVICE CLIENTS
--         0   0                80               net5
           1   0                0                --
           2   0                0                --
           3   0                20               vnic1
           4   0                0                --
           5   0                0                --
           6   0                0                --
           7   0                0                --
```

Par défaut, les valeurs configurées pour la propriété `etsbw-lcl` pour chaque priorité sur `net5` sont envoyées aux homologues comme les valeurs recommandées. `ETSBW_RMT_ADVICE` affiche les valeurs recommandées aux homologues. La sortie indique également que le pair n'a pas configuré de bande passante ETS à son extrémité. Vous pouvez également afficher la bande passante recommandé aux homologues à l'aide de la commande `lldpadm show-agent`.

5. Recommander une valeur différente aux homologues.

```
# dladm set-linkprop -p etsbw-rmt-advice=10 vnic1
# dladm show-linkprop -p etsbw-rmt-advice vnic1
LINK     PROPERTY          PERM VALUE     EFFECTIVE    DEFAULT   POSSIBLE
vnic1    etsbw-rmt-advice  rw   10         10           0         --
```

6. Afficher la bande passante recommandée aux homologues.

```
# dladm show-phys -D ets -r net5
LINK               COS ETSBW_RMT_EFFECT ETSBW_RMT_ADVICE CLIENTS
--                 0   0                90               net5
                   1   0                0                --
                   2   0                0                --
                   3   0                10               vnic2
                   4   0                0                --
                   5   0                0                --
                   6   0                0                --
                   7   0                0                --
```

Le champ `ETSBW_RMT_EFFECT` indique la valeur `0` pour `vnic2`, ce qui signifie que le pair n'a pas défini une bande passante de son côté, bien que vous ayez recommandée des valeurs de bande passante. Cela signifie que le pair n'a pas activé LLDP ou ne prend pas en charge ETS.

Affichage des informations de configuration ETS

Vous pouvez utiliser les commandes suivantes pour afficher les informations relatives à l'ETS.

- `# dladm show-linkprop -p etsbw-lcl,etsbw-rmt,etsbw-lcl-advice,etsbw-rmt-advice` *datalink*

  Cette commande affiche les informations relatives à la sélection de transmission améliorée sur un lien physique.

- `# dladm show-phys -D ets` *phys-link*

  Cette commande affiche la configuration ETS sur la liaison physique en matière d'allocation de bande passante et de distribution.

- `# lldpadm show-agenttlvprop -a` *agent* `etscfg`

  où *agent* est la liaison de données sur laquelle est activé le protocole LLDP. Cette commande affiche la propriété TLV ETS qui contrôle la capacité d'un hôte à synchroniser ses informations ETS avec un homologue.

EXEMPLE 6-7 Affichage des propriétés de liaison de données associées à ETS

Cet exemple illustre comment afficher le statut des propriétés de liaison de données associées au contrôle de flux basé sur la priorité.

```
# dladm show-linkprop -p cos,etsbw-lcl,etsbw-rmt,etsbw-lcl-advice, \
etsbw-rmt-advice vnic1
LINK    PROPERTY          PERM  VALUE  EFFECTIVE  DEFAULT    POSSIBLE
vnic1   cos               rw    2      2          0          0-7
vnic1   etsbw-lcl         rw    10     10         0          --
vnic1   etsbw-rmt         r-    20     20         --         --
vnic1   etsbw-lcl-advice  r-    20     20         --         --
vnic1   etsbw-rmt-advice  rw    10     10         0          --
```

La sortie indique que l'hôte a défini et recommandée une valeur ETS égale à 10 cos% pour `vnic1` avec une valeur `cos` de `2`. Cependant, le pair a défini et recommandé une valeur ETS de 20% avec une valeur `cos` de `2` pour `vnic1`. Vu que la synchronisation n'est pas activée (`willing` n'est pas activé) l'hôte n'a pas accepté la recommandation du pair, ce qui se retrouve dans la valeur , `EFFECTIVE` de la propriété `etsbw-lcl` (valeur configurée localement).

EXEMPLE 6-8 Affichage de la capacité de synchronisation des informations ETS de l'hôte local

Cet exemple illustre comment afficher le statut actuel de la capacité de l'hôte à s'adapter à la configuration ETS de son homologue.

```
# lldpadm show-agenttlvprop -a net0 etscfg
AGENT   TLVNAME   PROPERTY   PERM   VALUE   DEFAULT   POSSIBLE
net0    etscfg    willing    rw     off     on        on,off
```

Pour activer la synchronisation NTP, saisissez :

```
# lldpadm set-agenttlvprop -p willing=on -a net0 etscfg

# dladm show-linkprop -p  cos,etsbw-lcl,etsbw-rmt, \
etsbw-lcl-advice,etsbw-rmt-advice vnic1
LINK    PROPERTY           PERM  VALUE   EFFECTIVE  DEFAULT    POSSIBLE
vnic1   cos                rw    2       2          0          0-7
vnic1   etsbw-lcl          rw    10      20         0          --
vnic1   etsbw-rmt          r-    20      20         --         --
vnic1   etsbw-lcl-advice   r-    20      20         --         --
vnic1   etsbw-rmt-advice   rw    10      10         0          --
```

La synchronisation est activée (car la propriété `willing` est activée), l'hôte a accepté la recommandation du pair, ce qui est représentée dans la valeur `EFFECTIVE` de `etsbw-lcl`.

L'exemple suivant montre les valeurs ETS actuelles sur l'hôte et le pair pour chaque valeur de priorité sur le lien physique.

```
# dladm show-phys -D ets net4
LINK     COS ETSBW_LCL_EFFECT ETSBW_RMT_EFFECT ETSBW_LCL_SOURCE CLIENTS
net4      0   0                30               local            net4
          1   0                0                local            --
          2   0                0                local            --
          3   0                0                local            --
          4   0                70               local            --
          5   0                0                local            --
          6   0                0                local            --
          7   0                0                local            --
```

`ETSBW_LCL_EFFECT` Affiche le volume de bande passante ETS effectif sous la forme d'un pourcentage pour la priorité.

`ETSBW_RMT_EFFECT` Affiche le volume effectif de bande passante ETS sous la forme d'un pourcentage pour la valeur de priorité sur le pair.

`ETSBW_LCL_SOURCE` Indique l'origine pour la valeur `ETSBW_LCL_EFFECT`. Cette valeur peut être `local`, c'est-à-dire la valeur configurée ou `remote`, la valeur recommandée.

L'exemple suivant montre les informations ETS locales y compris les valeurs configurées localement, les valeurs effectives locales et les valeurs recommandées par le pair.

```
# dladm show-phys -D ets -l net5
LINK                COS ETSBW_LCL ETSBW_LCL_EFFECT ETSBW_LCL_ADVICE CLIENTS
--                  0   80        80               0                net5
                    1   0         0                0                --
                    2   0         0                0                --
                    3   20        20               0                vnic2
                    4   0         0                0                --
                    5   0         0                0                --
                    6   0         0                0                --
```

```
                    7   0         0               0               --
```

Etant donné que le pair n'a pas recommandé de valeurs, la valeur locale effective (`ETSBW_LCL_EFFECT`) est définie à l'aide de la valeur locale configurée (`ETSBW_LCL`).

L'exemple suivant affiche les informations relatives du pair.

```
# dladm show-phys -D ets -r net5
LINK                COS ETSBW_RMT_EFFECT ETSBW_RMT_ADVICE CLIENTS
--                  0   0                20                net5
                    1   0                0                 --
                    2   0                0                 --
                    3   0                80                vnic2
                    4   0                0                 --
                    5   0                0                 --
                    6   0                0                 --
                    7   0                0                 --
```

La sortie indique que le pair distant ne comporte aucune valeur définie dans le champ `ETSBW_RMT_EFFECT`, même si l'hôte avait recommandé au pair de définir 80% pour la priorité `3`.

♦ ♦ ♦ ANNEXE A

Groupement de liaisons et IPMP : comparaison des fonctionnalités

Le groupement de liaisons et IPMP constituent différentes technologies permettant d'améliorer les performances réseau et maintenir la disponibilité du réseau.

Le tableau suivant présente une comparaison générale entre le groupement de liaisons et IPMP.

Caractéristiques	Groupement de liaisons	IPMP
Type de technologie réseau	Couche 2 (couche de liaison)	Couche 3 (couche IP)
Outil de configuration	`dladm`	`ipadm`
Détection de défaillance basée sur les liaisons	Pris en charge.	Pris en charge.
Détection de défaillance basée sur sonde	Reposant sur LACP, cible le commutateur ou l'hôte homologue immédiat DLMP : pris en charge. 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 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
Utilisation d'interfaces de secours	Tronçon : non pris en charge. DLMP : non pris en charge.	Pris en charge. Les interfaces de secours peuvent être configurées.
Extension sur plusieurs commutateurs	Tronçon : n'est pris en charge. Toutefois, requiert fournisseur du commutateur extensions. DLMP : pris en charge.	Pris en charge.
Configuration du commutateur	Tronçon : Obligatoire. DLMP : facultatif.	Pas nécessaire.
Configuration dos à dos	Pris en charge.	Non pris en charge.
Types de médias pris en charge	Propre à Ethernet.	Prise en charge de la diffusion.
Prise en charge de la répartition de la charge	Tronçon : pris en charge et contrôlé par l'administrateur à l'aide de la commande	Pris en charge. Pris en charge, contrôlé par le noyau. La répartition de charge entrante est indirectement affectée par la sélection des adresses source

Caractéristiques	Groupement de liaisons	IPMP
	`dladm`. Répartition de charge entrante prise en charge. DLMP : pris en charge sur les clients et cartes VNIC de l'agrégation. Toutefois, la répartition de la charge par les clients individuels et les cartes VNIC sur le groupement n'est pas pris en charge.	
Niveau de prise en charge lors de l'intégration avec des cartes VNIC	Excellente prise en charge. L'agrégation est configurée dans le domaine de contrôle ou la zone globale uniquement et n'a pas d'incidence pour les zones.	Pris en charge. Toutefois, les propriétés des cartes VNIC, telles que la limite de bande passante, les anneaux Tx, Rx dédiés et la protection des liens IPMP ne peuvent pas être imposées pour un groupe. Nécessite plusieurs cartes VNIC à affecter aux zones et doit être configuré dans chaque zone.
Flux définis par l'utilisateur pour la gestion des ressources	Pris en charge.	Non pris en charge.
Protection de lien	Pris en charge.	Non pris en charge.
Exigences de protocole	Aucun.	Aucun.

Dans les groupements de liaisons, le trafic entrant est réparti sur plusieurs liaisons comprenant le groupement en mode trunk. Par conséquent, les performances réseau sont améliorées si vous installez davantage de cartes réseau pour ajouter des liaisons au groupement.

Les groupements DLMP s'étendent sur plusieurs commutateurs. En tant que technologie au niveau de la couche 2, les regroupements s'intègrent bien avec d'autres technologies de virtualisation Oracle Solaris.

Le trafic IPMP utilise les adresses de données de l'interface IPMP car 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.

♦ ♦ ♦ ANNEXE B

Format de paquet des sondes transitives

Le paquet de sonde transitive est un protocole propriétaire de type Ethernet `ETHERTYPE_ORCL` (`0x881b`). Pour plus d'informations sur les des sondes transitives reportez-vous à la rubrique “Détection de défaillance basée sur sonde” à la page 24 Pour obtenir un exemple pour afficher les statistiques des sondes reportez-vous à Exemple 2-7, “La section Probe-Informations connexes l'affichage”. La capture d'écran suivante présente le format de paquet sonde transitive.

FIGURE B-1 Transitive sonde de détection de paquets

Champ :	Description
MAC `de destination`	Adresse MAC de destination.
`src MAC`	Adresse MAC d'origine.
`Proto#`	Numéro du protocole. Les données traitées (payload) de la couche 2 des paquets `ETHERTYPE_ORCL` 2 doivent commencer par un numéro de 16 bits, notamment 1 pour le paquet de sonde transitive.
`Type`	Type de paquet de sonde. Le type de paquet de sonde est `0` pour la demande et 1pour une réponse.
`Pastille`	(Tous les n'est pas égal à zéro. le remplissage).

Champ :	Description
`Seq#`	Clés de sondes Mots-clés de numéro de séquence.
`Horodotage`	Clés de sondes Mots-clés horodatage.
`TL`	Les informations sur la cible de longueur. Pour Ethernet, la longueur source est 6 bits.(longueur de l'adresse MAC Ethernet).
`Cible`	Adresse MAC du port cible.
`SL`	Les informations relatives à l'origine de longueur. Pour Ethernet, la longueur source est 6 bits.
`Source`	Port source adresse MAC.

Index

E

G

R

S

T

U

V