Guide d'utilisation de NetXtreme® BCM57XX de Broadcom®

Dernière révision : février 2015

2CS57XX-CDUM513-R

Dernière révision : février 2015

2CS57XX-CDUM513-R

Sommaire

Section 1 : Caractéristiques et fonctionnalités

Description du fonctionnement

Les cartes Gigabit Ethernet de NetXtreme Broadcom permettent de connecter un système compatible PCI Express™ à un réseau Gigabit Ethernet. Les cartes Gigabit Ethernet NetXtreme de Broadcom utilisent une technologie qui permet de transférer des données à un débit maximum d'un gigabit par seconde, soit 10 fois la vitesse d'une carte Fast Ethernet.

Grâce au logiciel de regroupement de Broadcom, vous pouvez séparer votre réseau en réseaux locaux virtuels (VLAN) et regrouper plusieurs cartes réseau en équipes pour obtenir des fonctionnalités d'équilibrage de charge du réseau et de tolérance aux pannes. Voir Regroupement et Broadcom Gigabit Ethernet Teaming Services pour obtenir des informations détaillées sur le regroupement. Voir Réseaux locaux virtuels (VLAN) pour obtenir une description des réseaux locaux virtuels. Consultez la rubrique Configuration du regroupement pour obtenir des instructions sur la configuration du regroupement et la création de réseaux locaux virtuels sous Windows.

Spécifications

La liste suivante présente les caractéristiques de la carte Gigabit Ethernet NetXtreme de Broadcom pour tous les systèmes d'exploitation pris en charge :

- Emetteurs-récepteurs SerDes quad 10/100/1000BASE-T intégrés et quad 1000BASE-X/SGMII 1,25 Gbaud
- EEE (Energy Efficient Ethernet™) conforme IEEE 802.3az-2010
- Clause 73 IEEE 802.3ap (négociation automatique)
- MAC duplex intégral/semi-duplex Quad 10/100/1000BASE-T
- MAC duplex intégral/semi-duplex Quad 1000BASE-X/SGMII
- PCI Express v2.0 mode MDIX (Automatic MDI Crossover)
- x4 à 5 GT/s ou 2,5 GT/s
- Capacités MSI et MSI-X jusqu'à 17 vecteurs MSIX
- Prise en charge d'I/O Virtualization pour VMware NetQueue et Microsoft VMQ
  - 17 files d'attente de réception et 16 files d'attente de transmission
  - 17 vecteurs MSI-X prenant en charge les interruptions par file d'attente
- Vecteur MSI-X souple pour l'association de file d'attente de transmission/réception
- ECN TPH (TLP Processing Hint) selon la spécification de base PCI Express v2.0
- Réinitialisation du niveau de fonctionnement
- RSS (Receive Side Scaling) avec prise en charge des vecteurs MSI-X par file d'attente et du type de hachage RSS UDP
- TSS (Transmit Side Scaling) et file d'attente multi-Tx avec prise en charge des vecteurs MSI-X par file d'attente
- Prise en charge des trames Jumbo jusqu'à 9 600 octets de données utiles
- Prise charge VLAN (Virtual LAN)— Identification VLAN IEEE 802.1q
- Déchargement de somme de contrôle TCP, IP, UDP
- LSO (Large Send Offload), TSO (TCP Segmentation Offload)
- Assistance matérielle pour les implémentations de synchronisation de l'heure IEEE 1588 et IEEE 802.1AS
- Contrôle de flux IEEE 802.3x
- Interface SMBus 2.0
- Statistiques pour SNMP MIB II, MIB de type Ethernet et MIB Ethernet (IEEE 802.3z, clause 30)
- Conformité de la gestion de l'alimentation ACPI
- Gestion avancée de l'alimentation (APM) par CPMU (Central Power Management Unit)
- Contrôleur efficace de régulateur de commutation
- Moniteur de température incorporé
- Prise en charge de CLKREQ PCI Express
- Déchargement de la gestion de l'alimentation
- Prise en charge des mémoires Flash et EEPROM NVRAM série ; configuration automatique de la mémoire Flash
- Détection et correction des erreurs ECC sur SRAM interne
- Prise en charge de JTAG (méthode Boundary Scan)

Gestion d'état d'alimentation

Prise en charge de la fonction WOL (Wake on LAN) (paquet magique, trame de réveil, configuration spécifique)

Remarque : La vitesse de connexion de la carte lorsque le système est arrêté et qu'il attend un signal de réveil est de 10 Mbit/s ou de 100 Mbit/s, mais peut être rétablie à 1 000 Mbit/s quand le système fonctionne et qu'il est connecté à un commutateur prenant en charge 1 000 Mbit/s. Les systèmes comptant utiliser WOL (Wake on LAN) doivent être connectés à un commutateur ayant les capacités nécessaires pour les vitesses de 1 000 et de 10/100 Mbit/s.

Fréquence d'interruption adaptative

Le pilote de la carte ajuste intelligemment la fréquence d'interruption du serveur en fonction des conditions d'écoulement du trafic, de façon à augmenter le débit global de l'application. Lorsque le trafic est faible, le pilote de la carte interrompt le serveur pour chaque paquet reçu, réduisant ainsi le temps d'attente. Lorsque le trafic est important, la carte émet une interruption du serveur pour plusieurs paquets entrants consécutifs, préservant les cycles de l'ordinateur central d'accueil.

Voies doubles DMA

L'interface PCI sur les cartes Gigabit Ethernet NetXtreme de Broadcom comporte deux voies DMA indépendantes pour effectuer des opérations de lecture et d'écriture simultanément.

ASIC avec processeur RISC intégré

La fonction principale des cartes Gigabit Ethernet NetXtreme de Broadcom réside dans un ASIC de haute performance, étroitement intégré. L'ASIC comprend un processeur RISC. Cette fonctionnalité offre la possibilité d'ajouter de nouvelles fonctionnalités à la carte et de l'adapter aux exigences ultérieures du réseau via le téléchargement de logiciels.

NetXtremeLes opérations de gestion de Broadcom telles que DMTF, SMASH, DASH et le relais NC-SI s'exécutent sur un moteur de processeur d'application (APE) de haute performance, distinct du moteur de traitement réseau traditionnel.

Broadcom Advanced Control Suite

Composant du logiciel de regroupement Broadcom, Broadcom Advanced Control Suite (BACS) est un utilitaire intégré qui fournit des informations utiles sur toutes les cartes réseau installées sur votre système. L'utilitaire BACS permet également de réaliser des tests détaillés, des diagnostics et des analyses sur chaque carte, ainsi que de modifier les valeurs des propriétés et d'afficher des statistiques du trafic pour chaque carte. BACS est utilisé pour configurer des regroupements et ajouter des réseaux locaux virtuels sous les systèmes d'exploitation Windows. Voir Utilisation de l'application Broadcom Advanced Control Suite pour obtenir des informations et des instructions plus détaillées.

Systèmes d'exploitation pris en charge

La carte Gigabit Ethernet NetXtreme de Broadcom prend en charge les systèmes d'exploitation suivants :

- Microsoft® Windows® (32 bits et 64 bits étendus)
- Linux® (32 bits et 64 bits étendus)
- VMware
- Oracle Solaris

Indication de liaison au réseau et d'activité du réseau

Pour les connexions Ethernet en fil de cuivre, l'état de la liaison au réseau et de l'activité est indiqué par les voyants sur les connecteurs RJ-45, tel que décrit dans le Tableau 1 : « Liaison au réseau et activité indiqués par les voyants de port RJ-45 » à la page 14. Broadcom Advanced Control Suite fournit également des informations sur l'état de la liaison au réseau et de l'activité du réseau (voir Pour consulter des informations sur une carte).

Tableau 1 : Liaison au réseau et activité indiqués par les voyants de port RJ-45

Voyant de port	*Etat du voyant*	*Etat du réseau*
Voyant de liaison	Désactivé	Pas de liaison (câble déconnecté)
	Allumé (sans clignotement)	raccourci
Voyant d'activité	Désactivé	Aucune activité réseau
	Clignotement	Activité réseau

Section 2 : Regroupement

Remarque : voir Broadcom Gigabit Ethernet Teaming Services pour des informations détaillées sur les points suivants :

- Glossaire des termes et acronymes employés
- Concepts de regroupement
- Composants logiciels
- Configuration matérielle requise
- Fonctionnalités prises en charge selon le type d'équipe
- Sélection d'un type d'équipe
- Mécanismes de regroupement
- Architecture
- Types d'équipe
- Prise en charge du pilote selon le système d'exploitation
- Vitesses de regroupement prises en charge
- Regroupement et autres fonctionnalités réseau avancées
- Informations générales sur le réseau
- Informations sur l'application
- Résolution des problèmes de regroupement
- Foire aux questions
- Messages du journal des événements

Présentation

Le regroupement de cartes permet de regrouper n'importe quelles cartes réseau pour qu'elles fonctionnent sous forme d'équipe. De tels regroupements permettent l'adhésion à des réseaux locaux virtuels, l'équilibrage de charge entre les cartes et la tolérance aux pannes. Vous pouvez combiner ces avantages de façon à associer la fonction d'équilibrage de charge pour les éléments d'équilibrage de charge et l'utilisation d'une carte de reprise en attribuant l'équipe à différents réseaux locaux virtuels.

BASP (Broadcom Advanced Server Program) est le logiciel de regroupement de Broadcom. Sur les systèmes d'exploitation Windows, BASP se configure via l'utilitaire Broadcom Advanced Control Suite (BACS). Sous Linux, le regroupement passe par l'agrégation de canaux.

BASP prend en charge quatre types d'équipe d'équilibrage de charge :

- Smart Load Balancing and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique
- SLB (désactivation de la reprise automatique)

Equilibrage de charge et tolérance aux pannes

Le regroupement de cartes assure l'équilibrage de la charge du trafic et la tolérance aux pannes (mise en service des cartes auxiliaires en cas de défaillance de la connexion réseau). Lorsque plusieurs cartes sont installées sur le même système, elles peuvent être regroupées en un maximum de seize équipes.

Chaque équipe peut comprendre jusqu'à huit cartes, dont une utilisée comme carte auxiliaire pour les types d'équipe Smart Load Balancing and Failover (SLB) ou SLB (désactivation de la reprise automatique). Si l'écoulement du trafic n'est pas identifié sur une carte quelconque, élément de l'équipe, en raison d'une défaillance de la carte, du câble ou du commutateur, la charge est distribuée aux éléments restants de l'équipe sur une connexion active. Dans le cas où toutes les cartes primaires sont défaillantes, le trafic est distribué à la carte auxiliaire. Les sessions existantes sont maintenues et la défaillance n'a aucune répercussion sur l'utilisateur.

Types d'équipe

Les types d'équipe disponibles pour les systèmes d'exploitation pris en charge sont indiqués dans le tableau suivant :

Tableau 2 : Types d'équipe

Système d'exploitation	Types d'équipe disponibles
Windows Server 2008 et Windows Server 2012	Smart Load Balancing and Failover Link Aggregation (802.3ad) Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique SLB (désactivation de la reprise automatique) **REMARQUE** : Windows Server 2012 fournit une prise en charge du regroupement intégrée, appelée « regroupement NIC ». Il n'est pas recommandé que les utilisateurs activent des équipes via le regroupement NIC et BASP simultanément sur les mêmes cartes.
Linux	Regroupement de cartes à l'aide du module de noyau d'agrégation et d'une interface d'agrégation de canaux. Pour plus d'informations, consultez votre documentation Linux.

Smart Load Balancing™ and Failover

Smart Load Balancing™ and Failover est la mise en œuvre de l'équilibrage de charge par Broadcom basée sur le trafic IP. Cette fonction prend en charge l'équilibrage du trafic IP s'écoulant par plusieurs cartes (par ex., éléments d'équipe) dans les deux sens. Dans ce type d'équipe, toutes les cartes de l'équipe ont des adresses MAC distinctes. Il permet une détection automatique des défaillances et une reprise dynamique par un autre élément de l'équipe ou par la carte auxiliaire en réplique synchrone. Cette reprise est assurée indépendamment du protocole de couche 3 (IP) et fonctionne même avec les commutateurs des couches 2 et 3 existantes. Aucune configuration de commutateur (telle que trunk ou link aggregation) n'est nécessaire pour que ce type d'équipe fonctionne.

Remarque :

- si vous n'activez pas LiveLink™ lors de la configuration d'équipes SLB, il est recommandé de désactiver le protocole STP au niveau du commutateur ou du port. Ceci permet de minimiser le temps d'interruption nécessaire à la détermination de la boucle de l'arbre maximal lors d'une reprise. LiveLink réduit ce genre de problèmes.
- Lorsque la liaison d'un élément de l'équipe est à 1000 Mbit/s et que la liaison d'un autre élément est à 100 Mbit/s, la majeure partie du trafic est prise en charge par l'élément dont la liaison est de 1000 Mbit/s.

Link Aggregation (802.3ad)

Ce mode prend en charge le Link Aggregation (regroupement de liaisons). Il est conforme à la spécification IEEE 802.3ad (LACP). Le logiciel de configuration permet de configurer dynamiquement les cartes que vous voulez attribuer à une équipe donnée. Si votre partenaire de liaison n'est pas configuré correctement, conformément à la spécification 802.3ad, des erreurs sont détectées et notées. Dans ce mode, toutes les cartes de l'équipe sont configurées de façon à recevoir des paquets pour la même adresse MAC. Le procédé d'équilibrage de volume dans le sens de la sortie est déterminé par le pilote BASP. Le partenaire de liaison de l'équipe détermine le procédé d'équilibrage de charge des paquets dans le sens de l'entrée. Dans ce mode, au moins un des partenaires de la liaison doit être en mode actif.

Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique

Le type d'équipe Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique est très semblable au type Link Aggregation (802.3ad), dans ce sens que toutes les cartes de l'équipe sont configurées pour recevoir des paquets à la même adresse MAC. En revanche, ce type d'équipe ne prend pas en charge le protocole LACP ou le protocole du marqueur. Ce type d'équipe prend en charge divers environnements dans lesquels les partenaires de liaison des cartes sont configurés statiquement pour prendre en charge un procédé exclusif de gestion des liaisons. Par exemple, ce type d'équipe peut être utilisé pour prendre en charge OpenTrunk de Lucent ou Fast EtherChannel (FEC) de Cisco. En fait, il s'agit d'une version simplifiée du type d'équipe Link Aggregation (802.3ad). Cette méthode est bien plus simple, car il n'existe pas de protocole formalisé de contrôle de regroupement de liaisons (LACP). Comme avec les autres types d'équipe, la création des équipes et l'affectation des cartes physiques à diverses équipes sont réalisées statiquement au moyen du logiciel de configuration utilisateur.

Le type d'équipe Generic Trunking (FEC/GEC/Projet 802.3ad en mode statique) prend en charge l'équilibrage de charge et la reprise du trafic entrant et sortant.

SLB (désactivation de la reprise automatique)

Le type d'équipe SLB (désactivation de la reprise automatique) est identique au type d'équipe Smart Load Balancing (Equilibrage de volume intelligent) et Failover (Compensation), à l'exception suivante : lorsque l'élément auxiliaire est actif, si un élément principal se remet en ligne, l'équipe continue à utiliser l'élément auxiliaire plutôt que de revenir à l'élément principal.

Si une carte primaire attribuée à une équipe est désactivée, l'équipe fonctionne comme une équipe de type Smart Load Balancing and Failover dans lequel des reprises automatiques peuvent survenir.

Toutes les interfaces primaires d'une équipe participent à l'équilibrage de charge en envoyant et en recevant une partie du trafic total. Les interfaces auxiliaires reprennent le contrôle dans le cas où toutes les interfaces primaires ont perdu leur liaison.

Le regroupement de reprise assure l'équilibrage de la charge du trafic et la mise en service des cartes auxiliaires (tolérance aux pannes) en cas de défaillance de la connexion réseau. Si la carte primaire d'une équipe se déconnecte à cause de sa défaillance ou de celle du câble ou du port de commutation, l'élément secondaire de l'équipe devient actif, redirigeant le trafic entrant et sortant, affecté en premier lieu à la carte primaire. Les sessions existantes sont maintenues et la défaillance n'a aucune répercussion pour l'utilisateur.

Limites des types d'équipe Smart Load Balance et Fail Over et SLB (désactivation de la reprise automatique)

Smart Load-Balancing™ (SLB) est un code propre au protocole.

Tableau 3 : Smart Load Balancing

Système d'exploitation	***Défaillance/Reprise — Tout Broadcom***	***Défaillance/Reprise — Multi-fournisseur***
Protocole	***IP***	***IP***
Windows Server 2008	O	O
Windows Server 2008 R2	O	O
Windows Server 2012	O	O
Système d'exploitation	***Equilibrage de volume — Tout Broadcom***	***Equilibrage de volume — Multi-fournisseur***
Protocole	***IP***	***IP***
Windows Server 2008	O	O
Windows Server 2008 R2	O	O
Windows Server 2012	O	O
Windows Server 2012 R2	O	O

Légende : O = oui
N = non
N/C = non pris en charge

Le type d'équipe SLB (Equilibrage de charge intelligent) fonctionne avec tous les commutateurs Ethernet sans configuration préalable des ports de commutation selon un mode de liaison particulier. Seule la charge de trafic IP est équilibrée dans les sens d'entrée et de sortie. D'autres paquets de protocole sont envoyés et reçus via une interface primaire uniquement. Seules les cartes réseau de Broadcom prennent en charge la reprise des trafics non IP. Dans le type d'équipe Generic Trunking, le commutateur Ethernet doit prendre en charge un type de mode de liaison de port (Gigabit EtherChannel de Cisco ou un mode Link Aggregation d'un autre constructeur de commutateurs). Ce type d'équipe n'est pas lié à un type de protocole particulier. L'ensemble du trafic doit être équilibré et tolérant aux pannes.

Remarque : Si vous n'activez pas LiveLink™ lors de la configuration d'équipes, il est recommandé de désactiver le protocole STP au niveau du commutateur. Ceci permet de minimiser le temps d'interruption nécessaire à la détermination de la boucle de l'arbre maximal lors d'une reprise. LiveLink réduit ce genre de problèmes.

Fonctionnalité LiveLink™

LiveLink™ est une fonctionnalité de BASP disponible uniquement pour le type de regroupement Smart Load Balancing™ and Failover. L'objectif de LiveLink est de détecter la connectivité réseau située au-delà du commutateur et d'acheminer le trafic uniquement via les éléments d'équipe dont la liaison fonctionne. Cette fonction est effectuée via le logiciel de regroupement (voir Configuration de LiveLink pour une équipe de type Smart Load Balancing and Failover (Equilibrage de charge intelligent et reprise) ou SLB (désactivation de la reprise automatique)). Le logiciel de regroupement teste périodiquement une ou plusieurs cartes cibles du réseau (il émet un paquet de liaison à partir de chaque élément de l'équipe). Les cibles testées envoient une réponse à la réception du paquet de liaison. Si un élément de l'équipe ne détecte pas de réponse dans un laps de temps et après un nombre de tentatives définis, le logiciel de regroupement cesse de transmettre du trafic via cet élément. Par la suite, si cet élément détecte une réponse d'une cible de test, cela signifie que la liaison est rétablie et le logiciel de regroupement reprend automatiquement la transmission du trafic par cet élément. LiveLink fonctionne uniquement avec TCP/IP.

La fonctionnalité LiveLink™ est prise en charge par les systèmes d'exploitation Windows 32 bits et 64 bits. Pour plus d'informations sur la prise en charge de cette fonctionnalité sous Linux, reportez-vous à la documentation relative à l'agrégation de canaux dans votre documentation Linux.

Regroupement et prise en charge de Large Send Offload et Checksum Offload

Les propriétés Large Send Offload (Déchargement important à l'émission) et Checksum Offload (Déchargement de la somme de contrôle) sont uniquement activées pour une équipe lorsque tous ses membres prennent en charge la fonctionnalité et sont configurés en conséquence.

Section 3 : Broadcom Gigabit Ethernet Teaming Services

Introduction

Cette section présente les considérations liées à la technologie et à la mise en œuvre que vous devez garder à l'esprit lors de l'utilisation des services de regroupement réseau proposés par le logiciel Broadcom fourni avec les systèmes. L'objectif des services de regroupement Broadcom est d'offrir une tolérance aux pannes et des possibilités d'agrégation de liaisons sur un ensemble de deux cartes ou plus. Les informations contenues dans ce document sont destinées à aider les équipes informatiques lors du déploiement et du dépannage des applications système qui requièrent une tolérance aux pannes et un équilibrage de charge sur le réseau.

Glossaire

Tableau 4 : Glossaire

L'élément	Définition
ARP	Address Resolution Protocol
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program (pilote intermédiaire)
DNS	Service de noms de domaine
G-ARP	Gratuitous Address Resolution Protocol
Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique	Type d'équipe d'équilibrage de charge intelligent et de reprise dépendant du commutateur où le pilote intermédiaire gère le trafic sortant et où le commutateur gère le trafic entrant.
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Protocole Internet
LACP	Link Aggregation Control Protocol
Link Aggregation (802.3ad)	Type d'équipe d'équilibrage de charge intelligent et de reprise dépendant du commutateur avec LACP où le pilote intermédiaire gère le trafic sortant et où le commutateur gère le trafic entrant.
LOM	LAN on Motherboard
MAC	Contrôle d'accès support
NDIS	Network Driver Interface Specification
NLB	Network Load Balancing (Microsoft)
PXE	Preboot Execution Environment
RAID	Redundant Array of Inexpensive Disks

Tableau 4 : Glossaire

L'élément	Définition
Smart Load Balance and Failover	Type d'équipe de reprise indépendant du commutateur où l'élément d'équipe principal gère le trafic entrant et sortant tandis que l'élément d'équipe auxiliaire reste en attente d'un événement de reprise (par exemple, une perte de lien). Le pilote intermédiaire (BASP) gère le trafic entrant et sortant.
Smart Load Balancing (SLB)	Type d'équipe d'équilibrage de charge et de reprise indépendant du commutateur où le pilote intermédiaire gère le trafic entrant et sortant.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WINS	Service de noms Windows
WLBS	Windows Load Balancing Service

Concepts de regroupement

Adressage réseau

Pour comprendre comment fonctionne ce regroupement, il est important d'avoir une bonne connaissance du fonctionnement de la communication des nœuds dans un réseau Ethernet. Ce document est conçu pour des lecteurs familiers avec les bases des communications des réseaux Ethernet et IP. Les informations suivantes offrent un aperçu avancé des concepts d'adressage réseau utilisés dans un réseau Ethernet.

Chaque interface de réseau Ethernet d'une plate-forme hôte (par exemple, un ordinateur) nécessite une adresse de couche 2 globale unique et au moins une adresse de couche 3 globale unique. La couche 2 est la couche de liaison des données et la couche 3 est la couche réseau comme définie dans le modèle OSI. L'adresse de couche 2 est affectée au matériel. Elle est souvent appelée adresse MAC ou adresse physique. Cette adresse est préprogrammée en usine et est stockée dans la mémoire NVRAM d'une interface réseau ou sur la carte mère du système dans le cas d'une interface LAN intégrée. Les adresses de couche 3 sont souvent appelées adresse logique ou adresse de protocole. Elles sont affectées à la pile de logiciel. IP est un exemple de protocole de couche 3. La couche 4 (couche de transport) utilise quant à elle les numéros de port de chaque protocole réseau de niveau supérieur, comme Telnet ou FTP. Ces numéros de port sont utilisés pour différencier les flux de trafic entre les applications. Les protocoles de couche 4 (par exemple, TCP ou UDP) sont souvent utilisés dans les réseaux actuels. La combinaison de l'adresse IP et du numéro de port TCP est appelée « socket » ou interface de connexion.

Les périphériques Ethernet communiquent entre eux en utilisant l'adresse MAC et non l'adresse IP. Toutefois, la plupart des applications fonctionnent avec un nom d'hôte traduit en adresse IP par un service de noms tel que WINS ou DNS. Il est donc nécessaire de pouvoir identifier l'adresse MAC attribuée à l'adresse IP. Le protocole ARP (Address Resolution Protocol) propose cette fonction dans le cadre d'un réseau IP. Une adresse de monodiffusion correspond à une seule adresse MAC ou à une seule adresse IP. Une adresse de diffusion est envoyée à tous les périphériques d'un réseau.

Regroupement et adresses réseau

Une équipe de cartes fonctionne comme une interface de réseau virtuel unique et est semblable à une carte non groupée pour les autres périphériques réseau. Une carte réseau virtuelle annonce une seule adresse de couche 2 et une ou plusieurs adresses de couche 3. Lorsque le pilote de regroupement est initialisé, il sélectionne une adresse MAC appartenant à l'une des cartes physiques. Cette adresse devient l'adresse MAC de l'équipe. Cette adresse correspond généralement à celle de la première carte initialisée par le pilote. Lorsque le système qui héberge l'équipe reçoit une requête ARP, il sélectionne une adresse MAC parmi les cartes physiques de l'équipe à utiliser comme adresse MAC source pour la réponse ARP. Sur les systèmes d'exploitation Windows, la commande IPCONFIG /all affiche les adresses IP et MAC de la carte virtuelle et non celles de chaque carte physique. L'adresse IP de protocole est attribuée à l'interface réseau virtuelle et non à chaque carte physique.

Pour les modes de regroupement indépendants du commutateur, toutes les cartes physiques formant une carte virtuelle doivent utiliser l'adresse MAC unique qui leur a été attribuée lors de la transmission de données. Les trames renvoyées par chaque carte physique de l'équipe doivent utiliser une adresse MAC unique pour être compatible IEEE. Il est important de noter que les entrées du cache ARP ne sont pas découvertes à partir des trames reçues, mais uniquement à partir des requêtes et des réponses ARP.

Description des types de regroupement

Il existe trois méthodes de classification des types de regroupement pris en charge :

- La première dépend de la correspondance ou de la non-correspondance de la configuration du port de commutation avec le type de regroupement de la carte.
- La deuxième est basée sur la fonctionnalité de l'équipe, si celle-ci prend en charge l'équilibrage de charge et la reprise ou uniquement la reprise.
- La troisième dépend de l'utilisation ou non du protocole LACP (protocole de contrôle de regroupement de liaison).

Le Tableau 5 reprend les types de regroupement et leur classification.

Tableau 5 : Types de regroupement disponibles

Type de regroupement	Dépendante du commutateur (le commutateur doit prendre en charge un type d'équipe spécifique)	La prise en charge du protocole Link Aggregation Control Protocol est requise sur le commutateur	Equilibrage de charge	Reprise
Smart Load Balancing and Failover (avec 2 à 8 éléments d'équipe d'équilibrage de charge)			•	•
SLB (désactivation de la reprise automatique)				•
Link Aggregation (802.3ad)	•	•	•	•
Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique	•		•	•

Smart Load Balancing and Failover

Le type d'équipe Smart Load Balancing™ and Failover (équilibrage de charge intelligent et reprise) assure l'équilibrage de charge et la reprise lorsqu'il est configuré pour l'équilibrage de charge et uniquement la reprise lorsqu'il est configuré pour la tolérance aux pannes. Ce type d'équipe est compatible avec n'importe quel commutateur Ethernet et ne requiert aucune configuration de gestion des liaisons sur le commutateur. L'équipe annonce plusieurs adresses MAC et une ou plusieurs adresses IP (lors de l'utilisation d'une adresse IP secondaire). L'adresse MAC de l'équipe est sélectionnée à partir de la liste des éléments d'équilibrage de charge. Lorsque le système reçoit une requête ARP, la pile de mise en réseau des logiciels envoie toujours une réponse ARP avec l'adresse MAC de l'équipe. Pour lancer le processus d'équilibrage de charge, le pilote de regroupement modifie cette réponse ARP en changeant l'adresse MAC source afin qu'elle corresponde à celle d'une des autres cartes physiques.

Smart Load Balancing vous permet d'équilibrer la charge en émission et en réception en fonction de l'adresse IP de couche 3 ou 4 et du numéro de port TCP/UDP. L'équilibrage de charge ne se fait donc pas au niveau des octets ou des trames, mais par session TCP/UDP. Le recours à cette méthode est nécessaire pour conserver l'ordre de transmission des trames appartenant à la même communication par socket. L'équilibrage de charge est pris en charge sur 2 à 8 ports. Ces ports peuvent inclure toute combinaison de cartes complémentaires et de périphériques LOM (LAN on Motherboard). L'équilibrage de charge en émission se fait en créant un tableau de hachage à l'aide des adresses IP source et cible ainsi que des numéros de port TCP/UDP. Une même combinaison d'adresses IP source et cible et de numéros de port TCP/UDP génère normalement un indice de hachage identique et renvoie par conséquent au même port de l'équipe. Lorsqu'un port est sélectionné pour acheminer toutes les trames d'un socket donné, l'adresse MAC unique de la carte physique (et non l'adresse MAC de l'équipe) est incluse dans la trame. Cette étape est requise pour la conformité à la norme IEEE 802.3. Si deux cartes effectuent des transmissions en utilisant la même adresse MAC, il survient un conflit d'adresse MAC que le commutateur ne peut pas gérer.

L'équilibrage de charge en réception est réalisé via un pilote intermédiaire par l'envoi d'ARP gratuits client par client en utilisant l'adresse de monodiffusion de chaque client comme adresse cible de la requête ARP (cette opération est également connue sous le nom d'ARP dirigé). Il s'agit alors d'un équilibrage de charge par client et non d'un équilibrage de charge de trafic. Lorsque le pilote intermédiaire détecte un déséquilibre notable de la charge dans une équipe SLB, il génère des G-ARP afin de redistribuer les trames entrantes. Le pilote intermédiaire (BASP) ne répond pas aux requêtes ARP. Seule la pile de protocole logiciel fournit la réponse ARP requise. Il est important de comprendre que l'équilibrage de charge en réception est fonction du nombre de clients qui se connectent au système via l'interface de l'équipe.

L'équilibrage de charge en réception SLB tente d'équilibrer le trafic entrant pour les ordinateurs client via les ports physiques de l'équipe. Cette fonction utilise un ARP gratuit modifié pour annoncer une autre adresse MAC pour l'adresse IP de l'équipe dans l'adresse physique et de protocole de l'expéditeur. Cet ARP gratuit (G-ARP) est en monodiffusion pour les adresses MAC et IP d'un ordinateur client, dans l'adresse physique cible et dans l'adresse de protocole cible. Le client cible doit alors mettre à jour son cache ARP avec un nouveau mappage d'adresse MAC vers l'adresse IP de l'équipe. Les G-ARP ne sont pas diffusés car tous les clients enverraient alors leur trafic vers un même port. Les avantages de l'équilibrage de charge par client seraient alors nuls et la transmission des trames serait trop retardée. Ce processus d'équilibrage de charge en réception fonctionne tant que tous les clients et le système groupé utilisent le même sous-réseau ou domaine de diffusion.

Lorsque les clients et le système utilisent des sous-réseaux différents et que le trafic entrant doit traverser un routeur, le trafic reçu et destiné au système n'est pas équilibré. La carte physique sélectionnée par le pilote intermédiaire pour l'acheminement du flux IP acheminera l'ensemble du trafic. Lorsque le routeur envoie une trame vers l'adresse IP de l'équipe, il diffuse une requête ARP (sauf dans le cache ARP). La pile de logiciel serveur génère une réponse ARP avec l'adresse MAC de l'équipe, mais le pilote intermédiaire modifie la réponse ARP et l'envoie vers une carte physique donnée, établissant ainsi le flux pour cette session.

ARP n'est en effet pas un protocole routable. Il ne contient pas d'en-tête IP et n'est donc pas envoyé vers le routeur ou la passerelle par défaut. ARP n'est qu'un protocole de sous-réseau local. De plus, G-ARP n'étant pas un paquet de diffusion, le routeur ne le traite pas et ne met pas à jour son propre cache ARP.

La seule méthode permettant au routeur de traiter un ARP destiné à un autre périphérique réseau est la suivante : il faut que Proxy ARP soit activé et que l'hôte ne dispose d'aucune passerelle par défaut. Peu utilisée, cette méthode est déconseillée pour la plupart des applications.

Le trafic sortant acheminé via un routeur fait l'objet d'un équilibrage de charge car l'équilibrage de charge en émission est basé sur les adresses IP source et cible et le numéro de port TCP/UDP. Comme les routeurs ne modifient pas les adresses IP source et cible, l'algorithme d'équilibrage de charge fonctionne comme prévu.

La configuration de routeurs pour le protocole HSRP (Hot Standby Routing Protocol) ne permet pas l'équilibrage de charge en réception dans l'équipe de cartes. En général, HSRP permet à deux routeurs d'agir comme un seul routeur, en annonçant une adresse IP virtuelle et une adresse MAC virtuelle. Un routeur physique est l'interface active quand l'autre est en veille.

Bien que HSRP puisse également charger des nœuds de partage (en utilisant différentes passerelles par défaut sur les nœuds hôtes) sur plusieurs routeurs dans les groupes HSRP, il pointe toujours vers l'adresse MAC principale de l'équipe.

Generic Trunking

Generic Trunking est un mode de regroupement assisté par commutateur et nécessite que les ports soient configurés à chaque extrémité de la liaison : interfaces serveur et ports de commutation. Il y est souvent fait référence sous les noms Cisco Fast EtherChannel ou Gigabit EtherChannel. De plus, Generic Trunking prend en charge des mises en œuvre similaires d'autres fabricants de commutateurs comme Extreme Networks Load Sharing et Bay Networks ou le mode statique IEEE 802.3ad Link Aggregation. Dans ce mode, l'équipe annonce une adresse MAC et une adresse IP lorsque la pile de protocole répond aux requêtes ARP. De plus, chaque carte physique de l'équipe utilise la même adresse MAC pour l'équipe lors de la transmission de trames. Ceci est possible car le commutateur situé à l'autre extrémité de la liaison reconnaît le mode de regroupement et peut gérer l'utilisation d'une adresse MAC unique par tous les ports de l'équipe. La table de transmission du commutateur présente l'ensemble comme un port virtuel unique.

Dans ce mode de regroupement, le pilote intermédiaire contrôle l'équilibrage de charge et la reprise pour le trafic sortant uniquement. Le trafic entrant est géré par les composants matériels et le microprogramme du commutateur. Comme c'est le cas pour Smart Load Balancing, le pilote intermédiaire BASP utilise les adresses source et cible IP/TCP/UDP pour équilibrer le trafic sortant du serveur. La plupart des commutateurs implémentent un hachage XOR des adresses MAC source et cible.

Link Aggregation (IEEE 802.3ad LACP)

Le type d'équipe Link Aggregation est semblable au type Generic Trunking, à la différence qu'il utilise le protocole LACP (Link Aggregation Control Protocol) pour définir les ports formant l'équipe. LACP doit être activé aux deux extrémités de la liaison pour que l'équipe puisse fonctionner. Si LACP n'est pas disponible aux deux extrémités de la liaison, 802.3ad propose une agrégation manuelle qui nécessite uniquement que les deux extrémités de la liaison soient à l'état établissement de liaison. L'agrégation manuelle permet l'activation d'une liaison d'élément sans échange de messages LACP. Cette méthode n'est donc pas aussi fiable et solide qu'une liaison LACP négociée. LACP détermine automatiquement les liaisons d'élément pouvant être agrégées avant de procéder à leur agrégation. Il assure l'ajout et la suppression contrôlés de liaisons physiques dans le cadre de l'agrégation, afin qu'aucune trame ne soit perdue ou dupliquée. La suppression d'éléments de liaison agrégés est assurée par le protocole du marqueur qui peut éventuellement être activé pour les liens agrégés compatibles avec le protocole LCAP (Link Aggregation Control Protocol).

Le groupe Link Aggregation annonce une adresse MAC unique pour tous les ports de l'ensemble. L'adresse MAC du service d'agrégation peut être l'une des adresses MAC formant le groupe. Le protocole LACP et le protocole du marqueur utilisent une adresse cible de multidiffusion.

La fonction de contrôle Link Aggregation détermine les liaisons pouvant être agrégées. Il lie ensuite les ports à une fonction d'agrégation dans le système et surveille les conditions pour déterminer si une modification est requise dans le groupe d'agrégation. L'agrégation de liaisons permet de regrouper les capacités individuelles de plusieurs liaisons afin de créer une liaison virtuelle hautes performances. La défaillance ou le remplacement d'une liaison dans un ensemble LACP n'entraînera aucune perte de connectivité. Le trafic sera simplement reporté sur les liaisons restantes de l'ensemble.

SLB (désactivation de la reprise automatique)

Ce type d'équipe est identique au type Smart Load Balance and Failover, à l'exception suivante : lorsque l'élément d'équilibrage est actif, si un élément principal se remet en ligne, l'équipe continue à utiliser l'élément d'équilibrage plutôt que de revenir à l'élément principal. Ce type d'équipe est pris en charge uniquement dans les situations où le câble réseau est déconnecté et reconnecté à la carte réseau. Il n'est pas pris en charge dans les situations où la carte est supprimée ou installée via un gestionnaire de périphériques ou des périphériques PCI enfichables à chaud.

Si une carte primaire attribuée à une équipe est désactivée, l'équipe fonctionne comme une équipe de type Smart Load Balancing and Failover dans lequel des reprises automatiques peuvent survenir.

Composants logiciels

Le regroupement est mis en œuvre via un pilote intermédiaire NDIS dans l'environnement Windows. Ce composant logiciel fonctionne avec le pilote miniport, la couche NDIS et la pile de protocole pour activer l'architecture de regroupement (voir Figure 1). Le pilote miniport contrôle directement le contrôleur de réseau local hôte afin d'activer des fonctions telles que l'envoi, la réception et l'interruption du traitement. Le pilote intermédiaire se situe entre le pilote miniport et la couche de protocole. Il assure le multiplexage de plusieurs instances de pilote miniport et crée une carte virtuelle considérée comme une carte unique par la couche NDIS. NDIS fournit un ensemble de fonctions de bibliothèque pour permettre la communication entre des pilotes miniport ou des pilotes intermédiaires d'une part et la pile de protocole d'autre part. Une adresse de protocole (une adresse IP, par exemple) est attribuée à chaque instance de périphérique miniport, mais, lorsqu'un pilote intermédiaire est installé, l'adresse de protocole est attribuée à la carte virtuelle d'équipe, et non à chaque périphérique miniport formant l'équipe.

La prise en charge de regroupement proposée par Broadcom est fournie par trois composants logiciels qui fonctionnent ensemble et sont pris en charge comme un tout. Lorsqu'un composant est mis à niveau, les autres composants doivent être mis à niveau vers une version prise en charge. Tableau 6 décrit les trois composants logiciels et leurs fichiers associés pour les systèmes d'exploitation pris en charge.

Tableau 6 : Composants logiciels du regroupement Broadcom

Composant logiciel	Nom Broadcom	Windows	Linux
Pilote miniport	Broadcom Base Driver	b57nd60X.sys	tg3
Pilote intermédiaire	Broadcom Advanced Server Program (BASP)	Basp.sys	bonding
Interface utilisateur de configuration	Broadcom Advanced Control Suite (BACS)	BACS	BACS CLI
Pilote NDIS 6	Pilote x86 Windows Vista et versions ultérieures Pilote x64 Windows Vista et versions ultérieures	b57nd60x.sys b57nd60a.sys	S/O

L'utilitaire Broadcom Advanced Control Suite (BACS) est conçu pour fonctionner avec les systèmes d'exploitation Windows Server 32 bits et 64 bits. BACS est utilisé pour configurer le regroupement pour l'équilibrage de charge et la tolérance aux pannes, ainsi que les VLAN. De plus, cet utilitaire affiche l'adresse MAC, la version du pilote et les informations d'état de chaque carte réseau. BACS comprend également plusieurs outils de diagnostic, comme les diagnostics matériels, le test de câble et le test de topologie réseau.

Configuration matérielle requise

- Commutateur Ethernet
- Routeur

Les différents modes de regroupement décrits dans ce document imposent certaines restrictions concernant l'équipement réseau utilisé pour connecter les clients aux systèmes groupés. Chaque type de technologie d'interconnexion réseau a une incidence sur le regroupement comme indiqué à la section suivante.

Commutateur Ethernet

Les commutateurs Ethernet permettent de décomposer un réseau Ethernet en plusieurs domaines de diffusion. Le commutateur assure la transmission des paquets Ethernet entre les hôtes à partir des adresses MAC Ethernet uniquement. Une carte réseau physique reliée à un commutateur peut fonctionner en mode semi-duplex ou duplex intégral.

Pour prendre en charge Generic Trunking et 802.3ad Link Aggregation, un commutateur doit prendre en charge explicitement ces fonctionnalités. Si le commutateur ne prend pas en charge ces protocoles, il peut tout de même être utilisé pour l'équilibrage de charge.

Routeur

Conçus pour acheminer le trafic réseau à partir du protocole de couche 3 ou supérieur, les routeurs fonctionnement également souvent comme des périphériques de couche 2 avec fonction de commutation. Le regroupement de ports connectés directement à un routeur n'est pas pris en charge.

Fonctionnalités prises en charge selon le type d'équipe

Tableau 7 propose une comparaison des fonctions pour les différents types d'équipe pris en charge par les cartes réseau Broadcom. Utilisez ce tableau pour déterminer le type d'équipe le mieux adapté à votre configuration. Le logiciel de regroupement accepte jusqu'à huit ports dans une même équipe et jusqu'à 16 équipes par système. Ces équipes peuvent être constituées de n'importe quelle combinaison de types de regroupement pris en charge, mais chaque équipe doit se situer sur un réseau ou un sous-réseau différent.

Tableau 7 : Comparaison des types d'équipes

Type d'équipe	Tolérance aux pannes	Equilibrage de charge	Gestion de liaisons statique dépendante du commutateur	Agrégation de liaison dynamique indépendante du commutateur (IEEE 802.3ad)
Fonction	SLB avec réplique synchrone[a]	SLB	Generic Trunking	Link Aggregation
Nombre de ports par équipe (même domaine de diffusion)	2–8	2–8	2–8	2–8
Nombre d'équipes	16	16	16	16
Tolérance aux pannes de la carte		Oui	Oui	Oui

Tableau 7 : Comparaison des types d'équipes (Suite)

Type d'équipe	Tolérance aux pannes	Equilibrage de charge	Gestion de liaisons statique dépendante du commutateur	Agrégation de liaison dynamique indépendante du commutateur (IEEE 802.3ad)
Tolérance aux pannes de la liaison du commutateur (même domaine de diffusion)	Oui	Oui	Dépendante du commutateur	Dépendante du commutateur
Equilibrage de charge en émission	Non	Oui	Oui	Oui
Equilibrage de charge en réception	Non	Oui	Oui (effectué par le commutateur)	Oui (effectué par le commutateur)
Requiert un commutateur compatible	Non	Non	Oui	Oui
Pulsations pour vérifier la connectivité	Non	Non	Non	Non
Supports divers (cartes avec différents supports)	Oui	Oui	Oui (dépendante du commutateur)	Oui
Vitesses mixtes (cartes ne prenant pas en charge des vitesses communes, mais pouvant fonctionner à différentes vitesses)	Oui	Oui	Non	Non
Vitesses mixtes (cartes prenant en charge des vitesses communes, mais pouvant fonctionner à différentes vitesses)	Oui	Oui	Non (la vitesse doit être identique)	Oui
Equilibrage de charge TCP/IP	Non	Oui	Oui	Oui
Regroupement multi-fournisseur	Oui[b]	Oui[b]	Oui[b]	Oui[b]
Equilibrage de charge non IP	Non	Oui (trafic IPX sortant uniquement)	Oui	Oui
Même adresse MAC pour tous les éléments de l'équipe	Non	Non	Oui	Oui
Même adresse IP pour tous les éléments de l'équipe	Oui	Oui	Oui	Oui
Equilibrage de charge par adresse IP	Non	Oui	Oui	Oui
Equilibrage de charge par adresse MAC	Non	Oui (utilisé en l'absence d'IP/IPX)	Oui	Oui

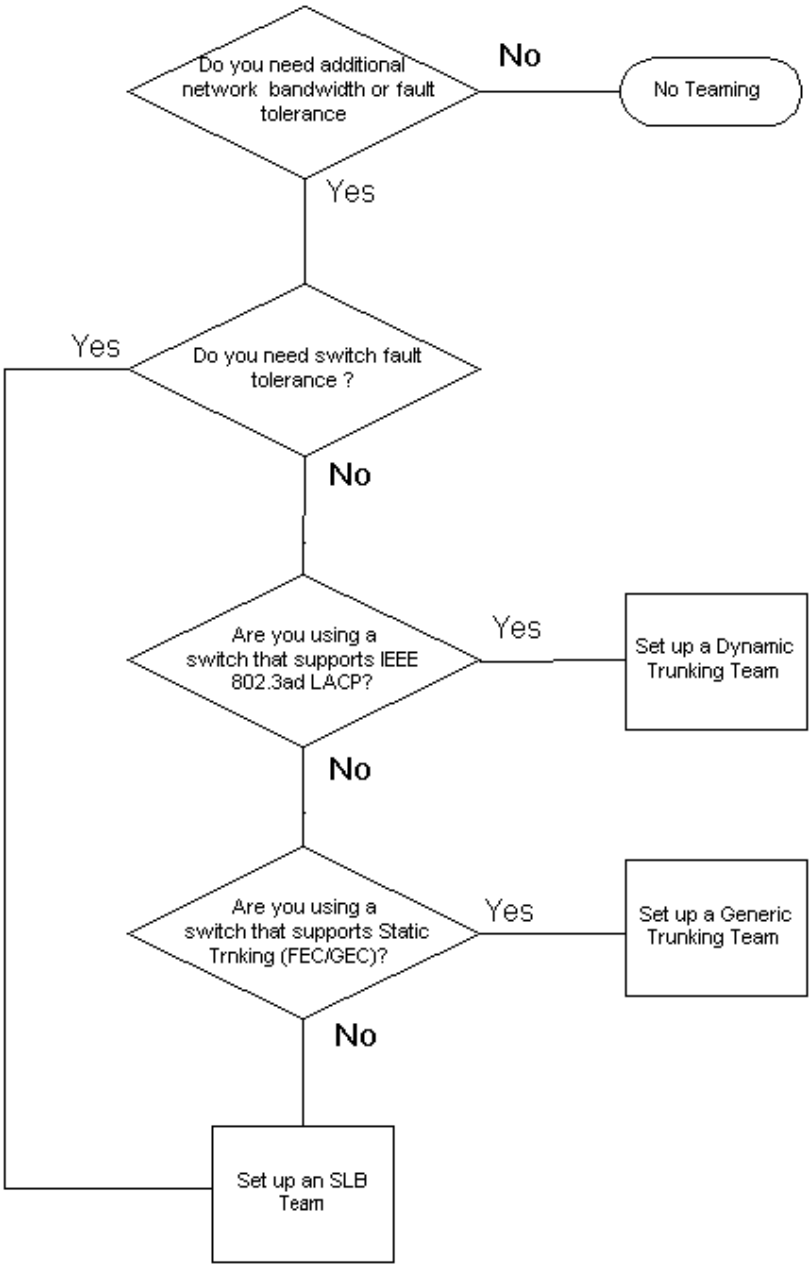
[a] SLB avec un élément primaire et un élément auxiliaire.

[b] Requiert au moins une carte Broadcom dans l'équipe.

Sélection d'un type d'équipe

Le tableau suivant indique le processus décisionnel lors de la planification du regroupement. Le motif de regroupement principal est le besoin en bande passante réseau supplémentaire et la nécessité d'une tolérance aux pannes. Le regroupement permet l'agrégation des liaisons et la tolérance aux pannes et répond donc à ces deux exigences. Le choix s'effectue dans l'ordre suivant : Link Aggregation en premier, Generic Trunking en deuxième et regroupement SLB en troisième en cas d'utilisation de commutateurs non gérés ou de commutateurs ne prenant pas en charge les deux premières options. Si la tolérance aux pannes de commutation est requise, SLB s'impose comme le seul choix possible (voir Figure 1).

Figure 1 : Processus de sélection d'un type d'équipe

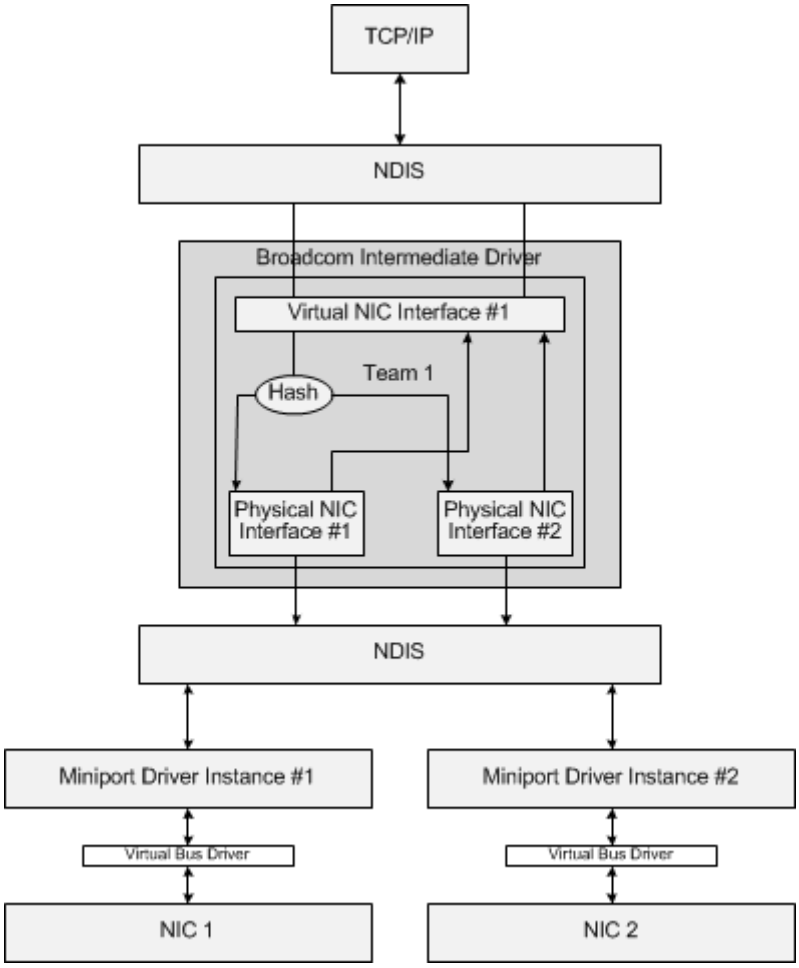


Mécanismes de regroupement

Architecture

Broadcom Advanced Server Program est implémenté en tant que pilote intermédiaire NDIS (voir Figure 2). Il fonctionne sous les piles de protocole telles que TCP/IP et fait office de carte virtuelle. Cette carte virtuelle hérite de l'adresse MAC du premier port initialisé de l'équipe. Une adresse de couche 3 doit également être configurée pour la carte virtuelle. La fonction principale de BASP est d'équilibrer le trafic entrant (pour SLB) et sortant (pour tous les modes de regroupement) parmi les cartes physiques installées sur le système faisant l'objet du regroupement. Les algorithmes d'entrée et de sortie sont indépendants et orthogonaux l'un par rapport à l'autre. Le trafic sortant pour une session spécifique peut être attribué à un port donné alors que le trafic entrant correspondant peut être attribué à un port différent.

Figure 2 : Pilote intermédiaire



Trafic sortant

Le pilote intermédiaire Broadcom gère le trafic sortant pour tous les modes de regroupement. Pour le trafic sortant, chaque paquet est réparti dans un flux, puis distribué à la carte physique sélectionnée pour transmission. La classification de flux implique un hachage efficace sur les champs de protocoles connus. La valeur de hachage obtenue est indexée dans un tableau de hachage de flux sortant. L'entrée sélectionnée dans le tableau comprend l'indice des cartes physiques sélectionnées chargées de la transmission de ce flux. L'adresse MAC source des paquets est ensuite remplacée par l'adresse MAC de la carte physique sélectionnée. Le paquet modifié est ensuite transmis à la carte physique sélectionnée pour transmission.

Les paquets TCP et UDP sortants sont classés à l'aide des informations d'en-tête de couche 3 et 4. Ce processus améliore la distribution de charge pour les services de protocole Internet les plus courants qui utilisent des ports connus, comme HTTP et FTP. Ainsi, BASP effectue l'équilibrage de charge par session TCP et non paquet par paquet.

Dans les entrées du tableau de hachage de flux sortant, les compteurs statistiques sont également mis à jour après classification. Le moteur d'équilibrage de charge consulte ces compteurs pour distribuer régulièrement les flux via les ports groupés. Le chemin de code de sortie a été conçu pour optimiser l'accès simultané lorsque de nombreux accès concurrents au tableau de hachage de flux sortant sont autorisés.

Pour les protocoles autres que TCP/IP, la première carte physique est toujours sélectionnée pour les paquets sortants. La seule exception est le protocole ARP (Address Resolution Protocol), qui est traité de façon différente pour permettre l'équilibrage de charge du trafic entrant.

Trafic entrant (SLB uniquement)

Le pilote intermédiaire Broadcom gère le trafic entrant pour le mode de regroupement SLB. Contrairement à l'équilibrage de charge du trafic sortant, l'équilibrage de charge du trafic entrant s'applique uniquement aux adresses IP situées dans le même sous-réseau que le serveur d'équilibrage de charge. L'équilibrage de charge du trafic entrant exploite une caractéristique unique du protocole ARP (RFC0826) : chaque hôte IP utilise son propre cache ARP pour encapsuler le datagramme IP dans une trame Ethernet. BASP manipule prudemment la réponse ARP pour diriger chaque hôte IP afin qu'il envoie le paquet IP entrant vers la carte physique souhaitée. Ainsi, l'équilibrage de charge du trafic entrant est un processus planifié à l'avance, basé sur l'historique des statistiques des flux entrants. Les nouvelles connexions d'un client vers le serveur surviennent toujours sur la carte physique primaire (car la réponse ARP générée par la pile de protocole du système d'exploitation associe toujours l'adresse IP logique à l'adresse MAC de la carte physique primaire).

Comme pour le flux sortant, il existe un tableau de hachage de tête de flux entrant. Chaque entrée du tableau dispose d'une liste à lien unique et chaque lien (entrées de flux entrant) représente un hôte IP situé sur le même sous-réseau.

Lorsqu'un datagramme IP entrant arrive, l'entrée de tête de flux entrant est localisée par hachage de l'adresse IP source du datagramme IP. Les deux compteurs statistiques stockés dans l'entrée sélectionnée sont également mis à jour. Ces compteurs sont utilisés de la même façon que les compteurs de sortie par le moteur d'équilibrage de charge, afin de réattribuer régulièrement les flux à la carte physique.

Dans le chemin de code entrant, le tableau de hachage de tête de flux entrant est également conçu pour accepter les accès concurrents. Les listes de liens des entrées de flux entrant sont uniquement référencées en cas de traitement des paquets ARP et de l'équilibrage de charge régulier. Il n'existe aucune référence par paquet pour les entrées de flux entrant. Même si les listes de liens ne sont pas associées, le temps système de traitement de chaque paquet non ARP est toujours une constante. Le traitement des paquets ARP, entrants et sortants, dépend toutefois du nombre de liens au sein de la liste de liens correspondante.

Sur le chemin de traitement entrant, le filtrage est également utilisé pour empêcher que les paquets de diffusion n'effectuent une boucle avec retour dans le système à partir d'autres cartes physiques.

Prise en charge de protocole

Les flux ARP et IP/TCP/UDP bénéficient de l'équilibrage de charge. Si le paquet utilise uniquement le protocole IP (par exemple, ICMP ou IGMP), toutes les données à destination d'une adresse IP donnée passent par la même carte physique. Si le paquet utilise TCP ou UDP pour le protocole de couche 4, le numéro de port est ajouté à l'algorithme de hachage, afin que deux flux de couche 4 puissent être acheminés via deux cartes physiques vers la même adresse IP.

Par exemple, supposons que l'adresse IP du client est 10.0.0.1. L'ensemble du trafic IGMP et ICMP circule via la même carte physique, car seule l'adresse IP est utilisée pour le hachage. Le flux peut ressembler au schéma suivant :

IGMP ------> PhysAdapter1 ------> 10.0.0.1

ICMP ------> PhysAdapter1 ------> 10.0.0.1

Si le serveur envoie également un flux TCP et UDP vers la même adresse (10.0.0.1), ils peuvent être sur la même carte physique que IGMP et ICMP ou sur des cartes physiques totalement différentes de ICMP et IGMP. Le flux peut ressembler au schéma suivant :

IGMP ------> PhysAdapter1 ------> 10.0.0.1

ICMP ------> PhysAdapter1 ------> 10.0.0.1

TCP------> PhysAdapter1 ------> 10.0.0.1

UDP------> PhysAdatper1 ------> 10.0.0.1

Les flux peuvent également ressemble au schéma suivant :

IGMP ------> PhysAdapter1 ------> 10.0.0.1

ICMP ------> PhysAdapter1 ------> 10.0.0.1

TCP------> PhysAdapter2 ------> 10.0.0.1

UDP------> PhysAdatper3 ------> 10.0.0.1

La répartition entre les cartes peut évoluer avec le temps, mais tout protocole non basé sur TCP/UDP passe par la même carte physique, car seule l'adresse IP est utilisée pour le hachage.

Performances

Les cartes d'interface réseau modernes offrent de nombreuses fonctions matérielles qui réduisent l'utilisation de l'UC en déchargeant ce dernier de diverses opérations exigeantes en ressources (voir Regroupement et autres propriétés de réseau avancées). En revanche, le pilote intermédiaire BASP est une fonction purement logicielle qui doit étudier chaque paquet reçu des piles de protocole et réagir à leur contenu avant de l'expédier via une interface physique donnée. Bien que le pilote BASP puisse traiter tout paquet sortant en temps quasi constant, certaines applications susceptibles d'être déjà liées à l'UC peuvent subir des répercussions négatives si elles sont utilisées via une interface groupée. Pour ce type d'application, il est préférable d'exploiter les fonctions de reprise du pilote intermédiaire plutôt que les fonctionnalités d'équilibrage de charge. Ces applications peuvent également fonctionner plus efficacement sur une carte physique unique proposant une fonction matérielle spéciale, comme Large Send Offload (Déchargement important à l'émission).

Prise en charge du pilote selon le système d'exploitation

Comme indiqué précédemment, le BASP est pris en charge dans les environnements Windows Server 2008 et 2012.

Les différentes fonctions de mode de regroupement sont résumées dans le tableau ci-dessous.

Tableau 8 : Fonctions du mode de regroupement

Spécifications	Prise en charge de Windows
Smart Load Balancing™	
Interface utilisateur	BACS[a]
Nombre d'équipes	16
Nombre de cartes par équipe	8
Remplacement à chaud	Oui
Ajout à chaud	Oui
Suppression à chaud	Oui
Prise en charge de la vitesse de liaison	Vitesses diverses
Protocole de trame	IP
Gestion des paquets entrants	BASP
Gestion des paquets sortants	BASP
Evénement de reprise	Perte de liaison ou événement LiveLink
Délai de la reprise	<500 ms
Délai de reprise automatique	1,5 s[b] (environ)
Prise en charge de LiveLink	Oui
Adresse MAC	Différente
Regroupement multi-fournisseur	Oui
Generic Trunking	
Interface utilisateur	BACS
Nombre d'équipes	16
Nombre de cartes par équipe	8
Remplacement à chaud	Oui
Ajout à chaud	Oui
Suppression à chaud	Oui
Prise en charge de la vitesse de liaison	Vitesses diverses
Protocole de trame	Tous
Gestion des paquets entrants	Commutateur
Gestion des paquets sortants	BASP
Evénement de reprise	Perte de liaison uniquement
Délai de la reprise	500 ms
Délai de reprise automatique	1,5 s[b] (environ)
Adresse MAC	Identique pour toutes les cartes
Regroupement multi-fournisseur	Oui
Dynamic Trunking	
Interface utilisateur	BACS

Tableau 8 : Fonctions du mode de regroupement (Suite)

Spécifications	Prise en charge de Windows
Nombre d'équipes	16
Nombre de cartes par équipe	8
Remplacement à chaud	Oui
Ajout à chaud	Oui
Suppression à chaud	Oui
Prise en charge de la vitesse de liaison	Vitesses diverses
Protocole de trame	Tous
Gestion des paquets entrants	Commutateur
Gestion des paquets sortants	BASP
Evénement de reprise	Perte de liaison uniquement
Délai de la reprise	<500 ms
Délai de reprise automatique	1,5 s[b] (environ)
Adresse MAC	Identique pour toutes les cartes
Regroupement multi-fournisseur	Oui

[a] Broadcom Advanced Control Suite
[b] Vérifiez que le mode Port Fast ou Edge Port est activé

Vitesses de regroupement prises en charge

Les diverses vitesses de liaison prises en charge pour chaque type d'équipe sont présentées dans le Tableau 9. Le terme « vitesse mixte » fait référence à la capacité des cartes de regroupement qui fonctionnent à différentes vitesses de liaison.

Tableau 9 : Vitesses de liaison dans le regroupement

Type d'équipe	*Vitesse de liaison*	*Direction du trafic*	*Vitesse prise en charge*
SLB	10/100/1000	Entrant/sortant	Vitesse mixte
FEC	100	Entrant/sortant	Vitesse identique
GEC	1000	Entrant/sortant	Vitesse identique
IEEE 802.3ad	10/100/1000	Entrant/sortant	Vitesse mixte

Regroupement et autres propriétés de réseau avancées

Avant de créer une équipe, d'ajouter ou de supprimer des éléments ou de modifier les paramètres avancés d'un élément de l'équipe, vérifiez que tous les éléments de l'équipe ont été configurés de la même manière. Les paramètres à vérifier incluent les VLAN et l'identification de paquets QoS, les trames Jumbo et les divers types de déchargement. Les propriétés avancées de la carte et la prise en charge du regroupement sont répertoriées dans le Tableau 10.

Tableau 10 : Propriétés avancées de la carte et prise en charge du regroupement

Propriété de la carte	Prise en charge par une carte virtuelle groupée
Checksum Offload (Déchargement de la somme de contrôle)	Oui
IEEE 802.1p QoS Tagging (Identification QoS IEEE 802.1p)	Non
Large Send Offload (Déchargement important à l'émission)	Oui[a]
Jumbo Frames (Trames Jumbo)	Oui[b]
IEEE 802.1Q VLANs (VLAN IEEE 802.1Q)	Oui
Wake On LAN (Réseau local de réveil)	Non
Preboot Execution Environment (PXE)	Oui[c]

[a] Toutes les cartes de l'équipe doivent prendre en charge cette fonction. Certaines cartes peuvent ne pas prendre en charge cette fonction si IPMI est également activé.
[b] Doit être prise en charge par toutes les cartes de l'équipe.
[c] Comme serveur PXE uniquement, pas comme application client.

Checksum Offload (Déchargement de la somme de contrôle)

Checksum Offload (Déchargement de la somme de contrôle) est une propriété des cartes réseau Broadcom qui permet aux sommes de contrôle d'envoi et de réception de trafic TCP/IP/UDP d'être calculées par la carte physique plutôt que par l'UC hôte. Lorsque le trafic est très important, cette fonction peut permettre à un système de gérer plus de connexions plus efficacement que si l'UC hôte devait calculer les sommes de contrôle. Il s'agit d'une propriété matérielle par nature qui ne tirerait pas parti d'une mise en œuvre uniquement logicielle. Une carte prenant en charge le déchargement de la somme de contrôle informe le système d'exploitation de l'existence de cette fonction. Ainsi, la somme de contrôle n'a pas à être calculée dans la pile de protocole. Le pilote intermédiaire étant situé directement entre la couche de protocole et le pilote miniport, la couche de protocole ne peut pas décharger de sommes de contrôle.

IEEE 802.1p QoS Tagging (Identification QoS IEEE 802.1p)

La norme IEEE 802.1p comporte un champ de 3 bits (prenant en charge 8 niveaux de priorité au maximum), qui permet de hiérarchiser le trafic. Le pilote intermédiaire BASP ne prend pas en charge l'identification QoS IEEE 802.1p.

Large Send Offload (Déchargement important à l'émission)

Large Send Offload (Déchargement important à l'émission) est une fonction fournie par les cartes réseau Broadcom qui empêche qu'un protocole de niveau supérieur comme TCP ne divise un paquet de données important en une série de paquets plus petits en lui ajoutant des en-têtes. La pile de protocole n'a besoin de générer qu'un seul en-tête pour un paquet de données de 64 Ko maximum et la carte matérielle divise le tampon en trames Ethernet de taille appropriée avec un en-tête correctement ordonné (en fonction de l'en-tête unique fourni au départ).

Jumbo Frames (Trames Jumbo)

Le pilote intermédiaire BASP prend en charge les trames Jumbo, dans la mesure où toutes les cartes physiques de l'équipe les prennent également en charge et où la même taille est définie sur toutes les cartes de l'équipe.

IEEE 802.1Q VLAN (VLAN IEEE 802.1Q)

La norme IEEE 802.3ac définit des extensions de format de trame pour la prise en charge de l'identification des réseaux locaux virtuels utilisant des ponts sur les réseaux Ethernet comme indiqué dans la spécification IEEE 802.1Q. Le protocole VLAN permet d'insérer une balise dans une trame Ethernet pour identifier le VLAN auquel appartient une trame. Si elle est présente, la balise VLAN de 4 octets est insérée dans la trame Ethernet entre l'adresse MAC source et le champ longueur/type. Les deux premiers octets de la balise VLAN correspondent au type de balise IEEE 802.1Q, alors que les 2 octets suivants incluent un champ de priorité utilisateur et l'identificateur de VLAN (VID). Les réseaux locaux virtuels (VLAN) permettent à l'utilisateur de partager son réseau local physique en sous-parties logiques. Chaque VLAN défini se comporte comme un réseau indépendant, son trafic et ses diffusions étant isolés des autres réseaux, ce qui assure une meilleure efficacité de la bande passante au sein de chaque groupe logique. Les VLAN permettent également à l'administrateur de mettre en application des politiques de sécurité et de qualité de service (QoS). Le BASP prend en charge la création de

64 VLAN par équipe ou carte : 63 identifiés et 1 non identifié. Toutefois, le système d'exploitation et les ressources du système limitent le nombre de VLAN. La prise en charge des VLAN est assurée conformément à la norme IEEE 802.1q, aussi bien dans un environnement de regroupement que sur une seule carte. Notez que les VLAN sont pris en charge exclusivement dans un regroupement homogène et non dans un environnement de regroupement multi-fournisseur. Le pilote intermédiaire BASP prend en charge l'identification des VLAN. Un ou plusieurs VLAN peuvent être liés à une même instance du pilote intermédiaire.

Wake On LAN (Réseau local de réveil)

Le réseau local de réveil est une fonction permettant à un système de sortir de veille à l'arrivée d'un paquet spécifique sur l'interface Ethernet. Dans la mesure où les cartes virtuelles sont implémentées en tant que périphérique logiciel, elles ne disposent pas des fonctions matérielles permettant de mettre en œuvre le réseau local de réveil. Il est donc impossible de sortir le système d'un état de veille en utilisant la carte virtuelle. Les cartes physiques, en revanche, prennent en charge cette propriété, même lorsque la carte fait partie d'une équipe.

Preboot Execution Environment (PXE)

Preboot Execution Environment (PXE) permet à un système de démarrer à partir d'une image du système d'exploitation sur le réseau. Par définition, PXE est appelé avant le chargement du système d'exploitation. Pour cette raison, le pilote intermédiaire BASP ne peut pas charger ni activer d'équipe. Ainsi, le regroupement n'est pas pris en charge comme client PXE, bien qu'une carte physique faisant partie d'une équipe lors du chargement du système d'exploitation puisse être utilisée comme client PXE. Une carte groupée ne peut être utilisée comme client PXE. Cependant, elle peut être utilisée pour un serveur PXE, qui fournit des images de système d'exploitation à des clients PXE en utilisant les protocoles DHCP (Dynamic Host Control Protocol) et TFTP (Trivial File Transfer Protocol). Ces deux protocoles fonctionnent sur IP et sont pris en charge par tous les modes de regroupement.

Informations générales sur le réseau

Regroupement de cartes reliées à des commutateurs différents

Le regroupement SLB peut être configuré sur des commutateurs différents. Cependant, les commutateurs doivent être connectés entre eux. Generic Trunking et Link Aggregation ne fonctionnent pas sur des commutateurs différents car leur mise en œuvre exige que toutes les cartes physiques d'une équipe partagent la même adresse MAC Ethernet. Notez bien que SLB ne peut détecter que la perte de liaison entre les ports d'une équipe et leur partenaire de liaison le plus proche. SLB ne peut réagir par rapport à d'autres pannes matérielles des commutateurs et ne peut détecter de perte de liaison sur d'autres ports.

Activation de la tolérance aux pannes de liaison des commutateurs

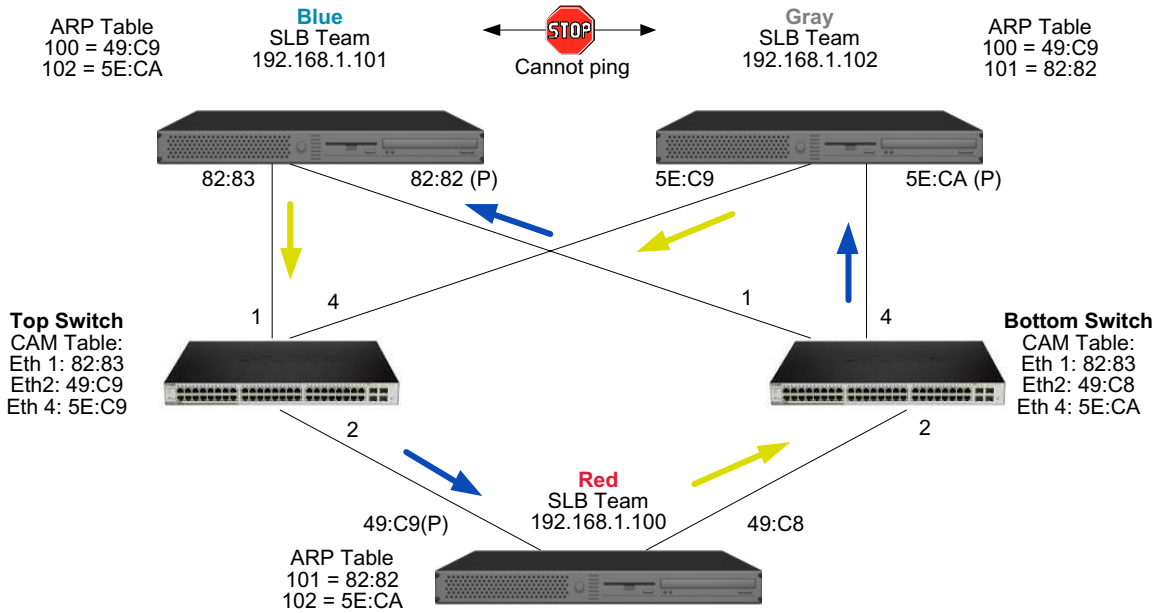
Les diagrammes ci-dessous décrivent le fonctionnement d'une équipe SLB lorsque la tolérance aux pannes de liaison des commutateurs est activée. Ils présentent la correspondance entre la requête ping et les réponses ping dans une équipe SLB où deux éléments sont actifs. Tous les serveurs (Bleu, Gris et Rouge) échangent des pings de façon continue.La Figure 3 présente une installation sans câble de connexion entre les deux commutateurs.Sur la Figure 4, le câble de connexion est en place. La Figure 5 illustre un événement de reprise lorsque le câble de connexion est en place. Ces scénarios décrivent le comportement de regroupement entre les deux commutateurs et l'importance de la liaison d'interconnexion.

Ces diagrammes présentent l'élément secondaire de l'équipe en train d'envoyer les requêtes écho ICMP (flèches jaunes) tandis que l'élément primaire reçoit les réponses écho ICMP correspondantes (flèches bleues). C'est là une caractéristique importante du logiciel de regroupement. Les algorithmes d'équilibrage de charge ne synchronisent pas l'équilibrage des trames pendant leur envoi ou leur réception. Cela signifie que les trames d'une communication donnée peuvent être émises et reçues sur différentes interfaces de l'équipe. C'est le cas de tous les types de regroupement pris en charge par Broadcom. Pour cette raison, une liaison d'interconnexion doit être assurée entre les commutateurs qui se connectent aux ports de la même équipe.

Dans la configuration ne comportant pas d'interconnexion, une demande ICMP de Bleu (Blue) à Gris (Gray) part du port 82:83 à destination du port Gris 5E:CA, mais le commutateur supérieur (Top Switch) ne peut l'envoyer à cet endroit car il ne peut pas passer par le port 5E:C9 sur Gris. Un scénario similaire a lieu lorsque Gris tente d'émettre un ping sur Bleu. Une demande ICMP part de 5E:C9 à destination de Bleu 82:82, mais ne peut y parvenir. Le commutateur supérieur ne possède pas d'entrée pour 82:82 dans son tableau CAM car il n'y a pas d'interconnexion entre les deux commutateurs. Cependant, les pings circulent entre Rouge (Red) et Bleu et entre Rouge et Gris.

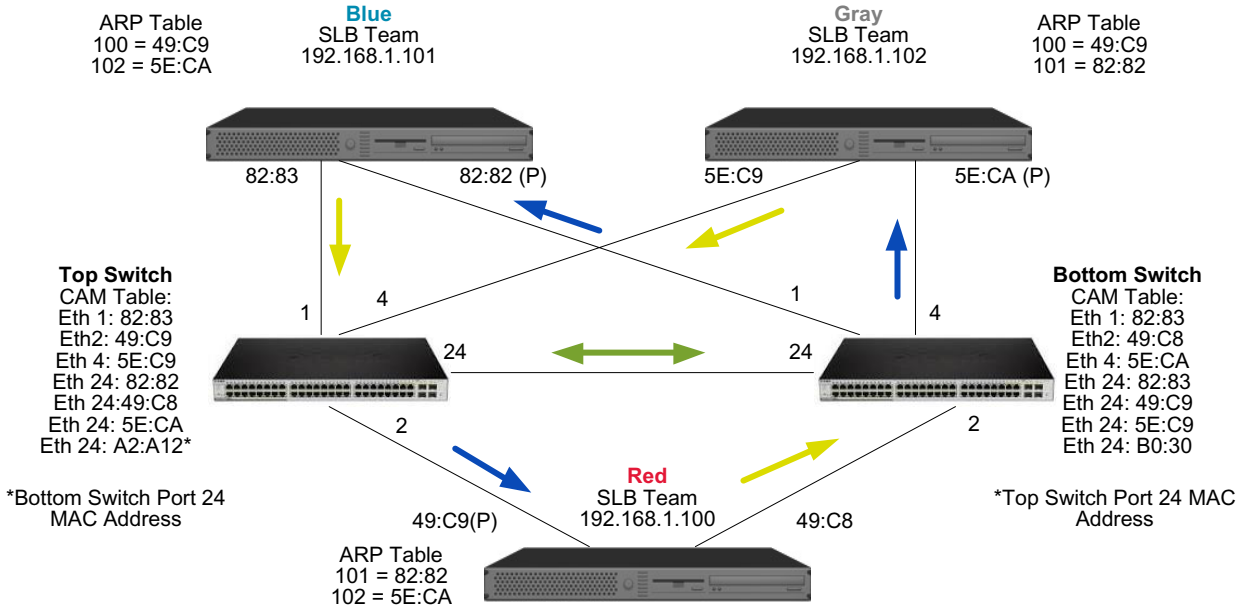
De plus, un événement de reprise pourrait entraîner des pertes de connectivité supplémentaires. Prenons l'exemple d'un câble déconnecté sur le commutateur supérieur, au port 4. Dans ce cas, Gris envoie la demande ICMP à Rouge 49:C9 mais, dans la mesure où le commutateur inférieur n'a pas d'entrée pour 49:C9 dans son tableau CAM, la trame est acheminée vers tous ses ports mais ne peut atteindre 49:C9.

Figure 3 : Regroupement de cartes reliées à des commutateurs différents sans liaison inter-commutateur



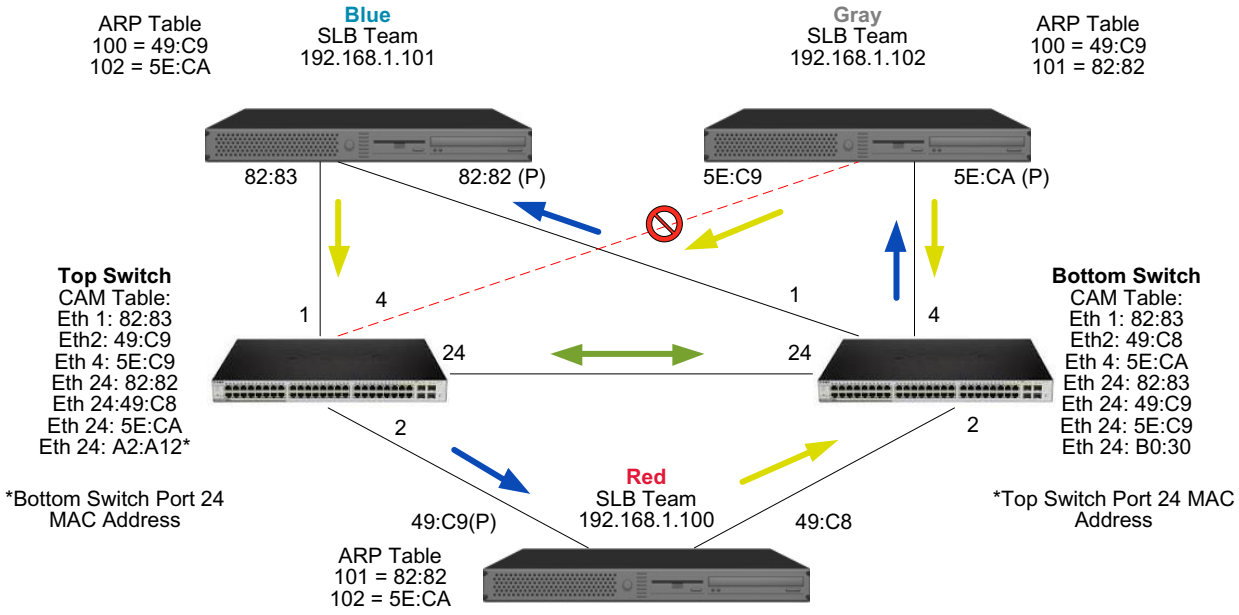
L'ajout d'une liaison entre les commutateurs permet au trafic entre Bleu et Gris et inversement de circuler sans problème. Notez les entrées supplémentaires dans le tableau CAM pour les deux commutateurs. La liaison d'interconnexion est cruciale pour que l'équipe fonctionne correctement. Par conséquent, il est fortement conseillé de disposer d'un ensemble d'agrégations de liaisons pour connecter les deux commutateurs afin de garantir une haute disponibilité de la connexion.

Figure 4 : Regroupement de cartes reliées à des commutateurs différents avec une interconnexion



La Figure 5 illustre un événement de reprise dans lequel le câble est débranché du commutateur supérieur, port 4. Cette reprise est réussie car tous les postes peuvent échanger des pings sans perdre de connectivité.

Figure 5 : Evénement de reprise



Spanning Tree Algorithm (algorithme d'arbre maximal)

- TCN (Topology Change Notice)
- Port Fast/Edge Port

Dans les réseaux Ethernet, un seul chemin actif peut exister entre deux ponts ou commutateurs. La présence de plusieurs chemins actifs risque en effet d'entraîner des boucles dans le réseau. En cas de boucle, certains commutateurs reconnaissent des postes situés des deux côtés du commutateur. Cette situation entraîne le dysfonctionnement de l'algorithme de transmission qui permet de transférer les trames. Les algorithmes d'arbre maximal fournissent des chemins redondants en définissant un arbre qui couvre tous les commutateurs d'un réseau étendu, puis fait passer des chemins de données à l'état attente (bloqué). A intervalle régulier, les commutateurs du réseau envoient et reçoivent des paquets de l'arbre maximal qu'ils utilisent pour identifier le chemin. Si un segment du réseau devient inaccessible ou que le délai requis par l'arbre maximal change, l'algorithme de l'arbre maximal reconfigure la topologie de l'arbre maximal et établit à nouveau la liaison en activant le chemin en attente. Le fonctionnement de l'arbre maximal est transparent pour les terminaux, qui ne détectent pas s'ils sont connectés à un seul segment LAN ou à un LAN commuté de plusieurs segments.

STP (Spanning Tree Protocol) est un protocole de couche 2 conçu pour fonctionner avec les ponts et les commutateurs. Les spécifications de STP sont définies dans IEEE 802.1d. Le principal objectif de STP est de vous éviter de vous retrouver dans une situation de boucle lorsque vous avez des chemins redondants sur le réseau. STP détecte/désactive les boucles réseau et fournit des liaisons de sauvegarde entre les commutateurs ou les ponts. Cela permet au périphérique d'interagir avec d'autres périphériques compatibles avec le protocole STP sur le réseau afin qu'il n'existe qu'un seul chemin entre deux postes du réseau.

Une fois qu'une topologie réseau stable a été établie, tous les ponts écoutent un message BPDU (Bridge Protocol Data Units) transmis du pont racine. Si un pont ne reçoit pas de message BPDU après un intervalle prédéfini (durée max), le pont

suppose que la liaison au pont racine est inactive. Ensuite, ce pont démarre des négociations avec d'autres ponts pour reconfigurer le réseau et établir à nouveau une topologie réseau valide. Le processus de création d'une nouvelle topologie peut prendre jusqu'à 50 secondes. Pendant ce temps, les communications de bout en bout sont interrompues.

L'utilisation d'un arbre maximal n'est pas recommandée pour les ports connectés aux terminaux car, par définition, un terminal ne crée pas de boucle dans un segment Ethernet. De plus, lorsqu'une carte groupée est connectée à un port alors que l'arbre maximal est activé, les utilisateurs peuvent être confrontés à des problèmes de connectivité inattendus. Prenons l'exemple d'une carte groupée dont l'une des cartes physiques a une liaison perdue. Si la carte physique est reconnectée (opération également appelée reprise automatique), le pilote intermédiaire détecte que la liaison a été établie à nouveau et commence à transmettre du trafic via le port. Le trafic est perdu si le port a été temporairement bloqué par le protocole STP.

TCN (Topology Change Notice)

Un pont/commutateur crée un tableau de transmission d'adresses MAC et de numéros de port en découvrant l'adresse MAC source reçue sur un port spécifique. Le tableau est utilisé pour transmettre des trames à un port spécifique plutôt que d'acheminer la trame vers tous les ports. Le délai d'expiration maximum des entrées du tableau est généralement de 5 minutes. Lorsqu'un hôte est silencieux depuis 5 minutes, son entrée est supprimée du tableau. Dans certains cas, il peut être intéressant de réduire le délai d'expiration. C'est le cas par exemple lorsqu'une liaison active passe à l'état bloqué ou de l'état bloqué à actif. Cette modification peut prendre jusqu'à 50 secondes. A l'issue du calcul STP, un nouveau chemin doit être disponible pour la communication entre les terminaux. Toutefois, dans la mesure où certaines des entrées du tableau de transmission restent basées sur l'ancienne topologie, les communications peuvent ne pas être établies à nouveau avant un délai de 5 minutes lorsque les entrées de port concernées sont supprimées du tableau. Le trafic est alors acheminé vers tous les ports et à nouveau découvert. Dans ce cas, il est intéressant de réduire le délai d'expiration. C'est l'objectif d'un TCN (Topology Change Notice) BPDU. Le TCN est envoyé du pont/commutateur concerné au pont/commutateur racine. Dès qu'un pont/commutateur détecte un changement de topologie (une liaison devenant inactive ou un port passant à l'état actif), il envoie un TCN au pont racine via son port racine. Le pont racine informe ensuite l'ensemble du réseau qu'un BPDU présente un changement de topologie. Chaque pont réduit alors la durée d'expiration du tableau MAC à 15 secondes pendant une durée spécifique. Cela permet au commutateur de découvrir à nouveau les adresses MAC dès la convergence du protocole STP.

Les TCN BPDU sont envoyés lorsqu'un port qui transmettait les changements (état actif) passe à l'état bloqué ou qu'un port passe à l'état actif. Un TCN BPDU ne lance pas de calcul STP. Il affecte exclusivement le délai d'expiration des entrées du tableau de transmission du commutateur. Il ne modifie pas la topologie du réseau et ne crée pas de boucle. Les nœuds finaux, notamment les serveurs ou les clients, déclenchent un changement de topologie lorsqu'ils s'arrêtent, puis redémarrent.

Port Fast / Edge Port

Pour limiter l'impact des TCN sur le réseau (par exemple, l'augmentation du trafic vers les ports de commutation), il est préférable que les nœuds finaux souvent arrêtés/redémarrés utilisent le paramètre Port Fast ou Edge Port sur le port de commutation auquel ils sont connectés. Port Fast ou Edge Port est une commande appliquée à des ports spécifiques qui provoque les effets suivants :

- Les ports passant de l'état de statut inactif à actif passent en mode STP actif plutôt que de passer de l'état écoute à l'état découverte, puis à l'état actif. STP fonctionne toujours sur ces ports.
- Le commutateur ne génère pas de TCN lorsque le port passe à l'état actif ou inactif.

Regroupement avec Microsoft NLB / WLBS

Le mode de regroupement SLB *ne fonctionne pas* avec l'équilibrage de charge du réseau Microsoft (NLB) en mode monodiffusion, mais en mode multidiffusion uniquement. En raison du mécanisme utilisé par le service NLB, la configuration de regroupement recommandée dans cet environnement est Failover (SLB avec NIC auxiliaire) étant donné l'équilibrage de charge est géré par NLB.

Informations sur l'application

Regroupement et mise en cluster-logiciel de mise en cluster Microsoft

Nous recommandons vivement aux clients d'installer au moins deux cartes réseau par nœud de cluster (les cartes embarquées sont acceptées). Ces interfaces ont deux objectifs. Une carte est utilisée exclusivement pour les communications *par pulsations* au sein d'un cluster. Cette carte, appelée *carte privée*, se situe généralement sur un sous-réseau privé indépendant. L'autre carte est utilisée pour les communications entre les clients et est appelée *carte publique*.

Plusieurs cartes peuvent être utilisées pour répondre à chacun des deux objectifs suivants : communications privées au sein d'un cluster et communications publiques externes entre les clients. Le logiciel de mise en cluster Microsoft prend en charge tous les modes de regroupement Broadcom, pour la carte publique uniquement. Le regroupement de cartes réseau privées n'est pas pris en charge. Microsoft indique que l'utilisation du regroupement sur l'interconnexion privée d'un cluster serveur n'est pas prise en charge car elle pourrait entraîner des délais dans la transmission et la réception de paquets de pulsations entre les nœuds. Pour des résultats optimaux, lorsque vous voulez obtenir une redondance pour l'interconnexion privée, désactivez le regroupement et utilisez les ports disponibles pour former une deuxième interconnexion privée. Vous obtenez le même résultat et cette méthode permet d'obtenir deux chemins de communications solides pour permettre aux nœuds de communiquer.

Pour le regroupement dans un environnement en clusters, les clients sont encouragés à utiliser des cartes de la même marque.

Remarque : Le logiciel de mise en cluster Microsoft ne prend pas en charge NLB de Microsoft.

Regroupement et sauvegarde réseau

Lorsque vous effectuez des sauvegardes réseau dans un environnement non groupé, le débit global de la carte du serveur de sauvegarde peut être influencé du fait d'un trafic excessif et d'une surcharge de la carte. En fonction du nombre de serveurs de sauvegarde, de flux de données et de la vitesse de la bande, le trafic de sauvegarde peut facilement utiliser un pourcentage élevé de la bande passante de liaison au réseau, affectant ainsi les données de production et les performances de sauvegarde de la bande magnétique. Les sauvegardes réseau sont généralement constituées d'un serveur de sauvegarde dédié fonctionnant avec un logiciel de sauvegarde sur bande tel que NetBackup, Galaxy ou Backup Exec. Le serveur de sauvegarde est associé soit à une unité de sauvegarde sur bande SCSI, soit à une bandothèque connectée via un SAN Fibre-Channel. Les systèmes sauvegardés sur le réseau sont généralement appelés clients ou serveurs distants et sont équipés d'un agent logiciel de sauvegarde sur bande.

Dans la mesure où il existe quatre serveurs client, le serveur de sauvegarde peut transmettre simultanément quatre tâches de sauvegarde (une par client) à un autochargeur multi-pilote. Cependant, du fait de la liaison unique entre le commutateur et le serveur de sauvegarde, une sauvegarde en 4 flux peut facilement saturer la carte et la liaison. Si la carte du serveur de sauvegarde fonctionne à 1 Gbit/s (125 Mo/s) et que chaque client peut transmettre des données en continu à 20 Mo/s pendant la sauvegarde sur bande, le débit entre le serveur de sauvegarde et le commutateur sera de 80 Mo/s (20 Mo/s x 4), ce qui correspond à 64 % de la bande passante du réseau. Bien que situé dans la plage de bande passante, 64 % est un pourcentage élevé, en particulier si d'autres applications partagent la même liaison.

Equilibrage de charge et reprise

Le débit global augmente à mesure que le nombre de flux de sauvegarde augmente. Cependant, chaque flux de données peut ne pas pouvoir conserver les mêmes performances dans un seul flux de sauvegarde à 25 Mo/s. En d'autres termes, bien qu'un serveur de sauvegarde puisse transmettre des données en continu à partir d'un client unique à 25 Mo/s, il est peu probable que 4 tâches de sauvegarde simultanées transmettent à 100 Mo/s (25 Mo/s x 4 flux). Bien que le débit global augmente à mesure que le nombre de flux de sauvegarde augmente, chaque flux de sauvegarde peut être affecté par les limitations du logiciel de sauvegarde sur bande ou de la pile réseau.

Pour qu'un serveur de sauvegarde sur bande utilise efficacement les performances de la carte et de la bande passante réseau lors de la sauvegarde de clients, une infrastructure réseau doit mettre en œuvre des fonctions de regroupement comme l'équilibrage de charge et la tolérance aux pannes. Les centres de données incluront les commutateurs redondants, l'agrégation des liaisons et la gestion des liaisons dans le cadre de leur solution de tolérance aux pannes. Bien que les pilotes de périphérique de regroupement agissent sur la circulation des données via les interfaces groupées et les chemins de reprise, cette opération est transparente pour les applications de sauvegarde sur bande et elle n'interrompt pas le processus de sauvegarde sur bande lors de la sauvegarde de systèmes distants sur le réseau.La Figure 6 représente une topologie réseau qui illustre une sauvegarde sur bande dans un environnement groupé Broadcom et indique comment l'équilibrage de charge intelligent peut *équilibrer la charge* des données de sauvegarde sur bande pour plusieurs cartes groupées.

Le serveur client peut utiliser quatre chemins pour envoyer des données au serveur de sauvegarde, mais un seul de ces chemins sera désigné pendant le transfert de données. Le serveur client Rouge peut notamment utiliser le chemin suivant pour envoyer des données au serveur de sauvegarde :

Exemple de chemin : le serveur client Rouge envoie des données via la carte A, le commutateur 1 et la carte du serveur de sauvegarde A.

Le chemin désigné est déterminé par deux facteurs :

1. Cache ARP du serveur client, qui pointe vers l'adresse MAC du serveur de sauvegarde. Ce facteur est déterminé par l'algorithme d'équilibrage de charge du trafic entrant du pilote intermédiaire Broadcom.
2. L'interface de la carte physique du serveur client Rouge est utilisée pour transmettre les données. Ce facteur est déterminé par l'algorithme d'équilibrage de charge du trafic sortant du pilote intermédiaire Broadcom (voir Trafic sortant et Trafic entrant (SLB uniquement).

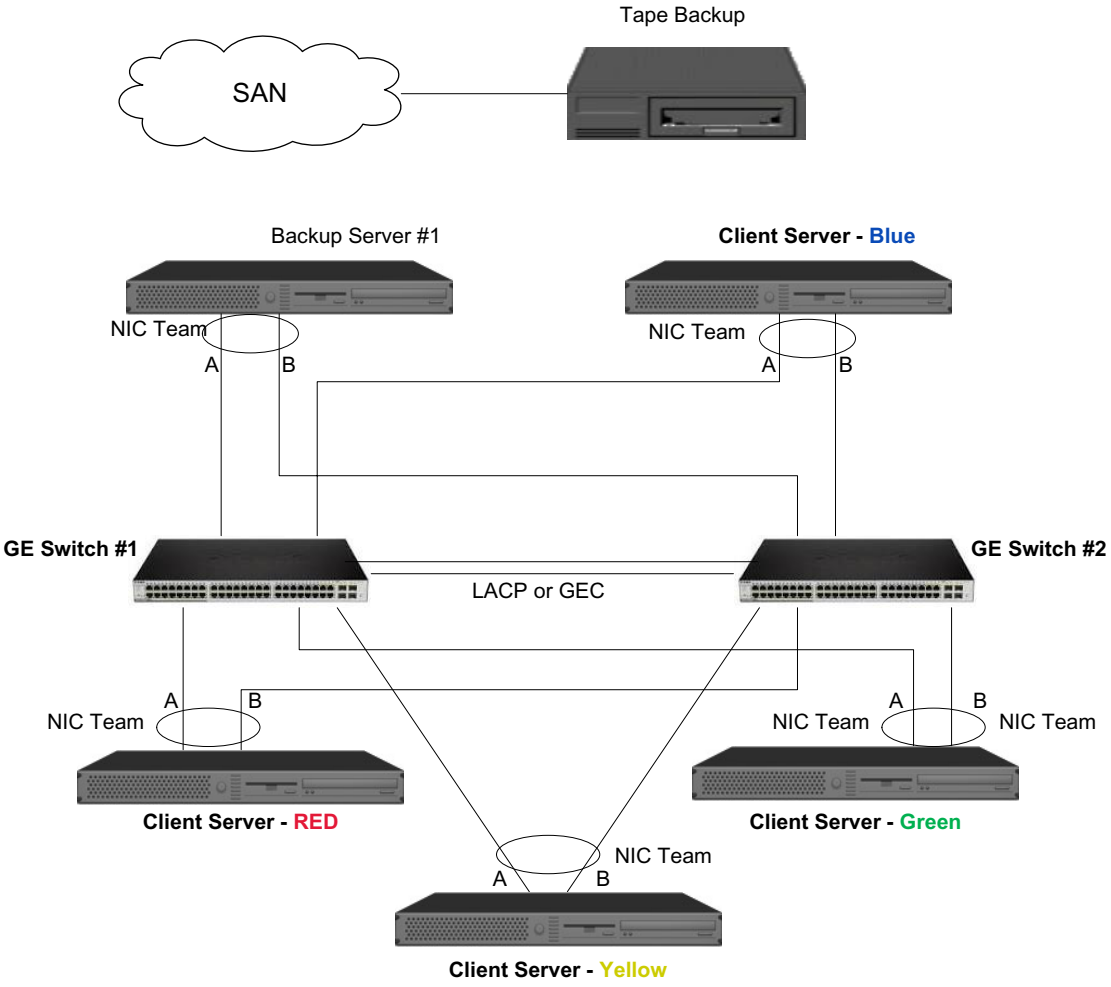
L'interface groupée du serveur de sauvegarde transmet un G-ARP (Gratuitous Address Resolution Protocol) au serveur client Rouge, qui, à son tour, entraîne la mise à jour du cache ARP du serveur client avec l'adresse MAC du serveur de sauvegarde. Le mécanisme d'équilibrage de charge de l'interface groupée détermine l'adresse MAC incorporée au G-ARP. L'adresse MAC sélectionnée sert principalement de destination au transfert de données depuis le serveur client. Sur le serveur client Rouge, l'algorithme de regroupement SLB détermine laquelle des deux interfaces de carte va être utilisée pour transmettre les données. Dans cet exemple, les données du serveur client Rouge sont reçues sur l'interface de la carte A du serveur de sauvegarde. Pour illustrer les mécanismes SLB lorsqu'une charge supplémentaire est placée sur l'interface groupée, examinez le scénario lorsque le serveur de sauvegarde lance une deuxième opération de sauvegarde : une vers le serveur client Rouge et une vers le serveur client Bleu. L'itinéraire emprunté par le serveur client Bleu pour envoyer des données au serveur de sauvegarde dépend de son cache ARP, qui pointe vers l'adresse MAC du serveur de sauvegarde. Dans la mesure où la carte A du serveur de sauvegarde subit déjà la charge de son opération de sauvegarde avec le serveur client Rouge, le serveur de sauvegarde appelle l'algorithme SLB afin d'*informer* le serveur client Bleu (via un G-ARP) de la nécessité de mettre à jour son cache ARP afin de refléter l'adresse MAC de la carte B. Lorsque le serveur client Bleu doit transmettre des données, il utilise l'une de ses interfaces de carte, déterminée par son propre algorithme SLB. Le principal est que les données du serveur client Bleu soient reçues par l'interface de la carte B du serveur de sauvegarde et non pas l'interface de la carte A. C'est important car, dans la mesure où les deux flux de sauvegarde circulent simultanément, le serveur de sauvegarde doit *équilibrer la charge* des flux de données provenant de différents clients. Lorsque les deux flux de sauvegarde circulent, chaque interface de carte du serveur de sauvegarde traite une charge égale, équilibrant ainsi la charge des données entre les deux interfaces de carte.

Le même algorithme s'applique si une troisième et une quatrième opération de sauvegarde sont lancées par le serveur de sauvegarde. L'interface groupée du serveur de sauvegarde transmet un G-ARP de monodiffusion aux clients de sauvegarde afin de les informer de la nécessité de mettre à jour leur cache ARP. Chaque client transmet ensuite les données de sauvegarde à l'adresse MAC cible du serveur de sauvegarde suivant un itinéraire donné.

Tolérance aux pannes

En cas de défaillance d'une liaison réseau lors des opérations de sauvegarde sur bande, le trafic entre le serveur de sauvegarde et le client s'arrête et les tâches de sauvegarde échouent. Toutefois, si la topologie réseau a été configurée à la fois pour SLB Broadcom et la tolérance aux pannes de commutation, les opérations de sauvegarde sur bande peuvent continuer sans interruption malgré la défaillance de la de liaison. Tous les processus de reprise au sein du réseau sont transparents pour les applications logicielles de sauvegarde sur bande. Pour comprendre comment les flux de données de sauvegarde sont dirigés lors du processus de reprise du réseau, examinez la topologie de la Figure 6. Le serveur client Rouge transmet des données au serveur de sauvegarde via le chemin 1, mais une défaillance de liaison se produit entre le serveur de sauvegarde et le commutateur. Les données ne pouvant plus être envoyées du commutateur 1 à l'interface de la carte A du serveur de sauvegarde, elles sont redirigées depuis le commutateur #1 vers l'interface de la carte B du serveur de sauvegarde par le biais du commutateur 2. L'application de sauvegarde n'est pas informée de ce changement, car toutes les opérations de tolérance aux pannes sont gérées par l'interface de l'équipe de cartes et les paramètres de gestion des liaisons des commutateurs. Quant au serveur client, il fonctionne toujours comme s'il transmettait des données par le chemin d'origine.

Figure 6 : Sauvegarde réseau avec regroupement SLB de cartes reliées à deux commutateurs



Résolution des problèmes de regroupement

Lorsqu'un analyseur de protocole est exécuté sur l'interface groupée d'une carte virtuelle, l'adresse MAC indiquée dans les trames transmises peut s'avérer incorrecte. L'analyseur n'indique pas les trames établies par BASP et indique l'adresse MAC de l'équipe et non l'adresse MAC de l'interface transmettant la trame. Nous vous recommandons d'utiliser le processus suivant pour surveiller une équipe :

1. Mettez en miroir les ports de liaison montante provenant de l'équipe au niveau du commutateur.
2. Si l'équipe occupe deux commutateurs, mettez également en miroir la gestion des liaisons d'interconnexion.
3. Echantillonnez tous les ports en miroir séparément.
4. Sur l'analyseur, utilisez une carte et un pilote qui ne filtrent pas les informations QoS et VLAN.

Conseils pour la configuration du regroupement

Lorsque vous résolvez des problèmes de connectivité réseau ou de regroupement, vérifiez les points suivants.

1. Pour une équipe SLB, il est recommandé d'adopter la même vitesse de liaison pour toutes les cartes.
2. Si LiveLink n'est pas activé, désactivez STP ou activez un mode STP qui contourne les phases initiales (par exemple, Port Fast, Edge Port) pour les ports de commutation connectés à une équipe.
3. Tous les commutateurs auxquels l'équipe est directement connectée doivent posséder la même version matérielle, micrologicielle et logicielle pour être pris en charge.
4. Pour être groupées, les cartes doivent faire partie du même VLAN. Si plusieurs équipes sont configurées, chaque équipe doit se trouver sur un réseau distinct.
5. Ne saisissez pas d'adresse de multidiffusion ou de diffusion dans le champ Locally Administered Address (Adresse administrée localement).
6. N'attribuez pas d'adresse administrée localement à une carte physique faisant partie d'une équipe.
7. Vérifiez que la gestion de l'alimentation est désactivée sur tous les éléments physiques d'une équipe (la case **Autoriser l'ordinateur à éteindre ce périphérique pour économiser l'énergie** de l'onglet **Gestion de l'alimentation** des **Propriétés** de la carte ne doit pas être activée ; voir Définition des options de gestion de l'alimentation dans « Installation des pilotes et des applications Windows »).
8. Supprimez toutes les adresses IP statiques des éléments physiques de l'équipe avant de mettre l'équipe en place.
9. Une équipe qui demande un débit maximum doit utiliser LACP ou GEC/FEC. Dans ce cas, le pilote intermédiaire n'est responsable que de l'équilibrage de charge du trafic sortant et le commutateur effectue l'équilibrage de charge du trafic entrant.
10. Les équipes agrégées (802.3ad \ LACP et GEC\FEC) doivent être connectées à un seul commutateur prenant en charge IEEE 802.3a, LACP ou GEC/FEC.
11. Il n'est pas conseillé de connecter une équipe à un concentrateur, car ce type d'équipement prend uniquement en charge le mode semi-duplex. Les concentrateurs peuvent être connectés à une équipe à des fins de dépannage uniquement. La désactivation du pilote de périphérique d'une carte réseau membre d'une équipe LACP ou GEC/FEC peut provoquer des effets inverses à ceux escomptés sur la connectivité du réseau. Afin d'éviter les pertes de connexion au réseau, Broadcom vous recommande, dans un premier temps, de déconnecter physiquement la carte du commutateur, puis de désactiver ensuite le pilote du périphérique.

12. Vérifiez que les pilotes de base (miniport) et d'équipe (intermédiaire) sont de la même version.

13. Testez la connectivité de chaque carte physique avant le regroupement.

14. Testez le comportement de reprise et de reprise automatique de l'équipe avant de la placer dans un environnement de production.

15. Lorsque vous déplacez une équipe d'un réseau hors production vers un réseau de production, nous vous recommandons fortement de tester à nouveau la reprise et la reprise automatique.

16. Testez les performances de l'équipe avant de la placer dans un environnement de production.

Procédures de dépannage

Avant d'appeler le support technique, assurez-vous d'avoir effectué les étapes suivantes de résolution des problèmes de connectivité réseau lorsque le serveur utilise le regroupement de cartes.

1. Vérifiez que le voyant de liaison Ethernet de chaque carte est allumé et que tous les câbles sont connectés.

2. Vérifiez que les pilotes de base et intermédiaire correspondants appartiennent à la même version et qu'ils sont correctement chargés.

3. Vérifiez la présence d'une adresse IP valide à l'aide de la commande **ipconfig** pour Windows.

4. Vérifiez que STP est désactivé, que Edge Port/Port Fast est activé sur les ports de commutation connectés à l'équipe ou que LiveLink est utilisé.

5. Vérifiez que les cartes et les commutateurs sont configurés de la même manière pour les fonctions Vitesse de liaison et Duplex.

6. Si possible, décomposez l'équipe et vérifiez séparément la connectivité de chaque carte pour confirmer que le problème est directement lié au regroupement.

7. Vérifiez que tous les ports de commutation connectés à l'équipe se trouvent sur le même VLAN.

8. Vérifiez que les ports de commutation sont configurés correctement pour le type d'équipe Generic Trunking (FEC/GEC)/ Projet 802.3ad en mode statique et que ce type correspond au type de regroupement de cartes. Si le système est configuré pour un type d'équipe SLB, assurez-vous que les ports de commutation correspondants *ne sont pas* configurés pour les types d'équipes Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique.

Foire aux questions

Question :	Dans quels cas l'équilibrage de charge du trafic n'est pas effectué ? Pourquoi l'équilibrage de charge du trafic est-il inégal entre les éléments d'une équipe ?
Réponse :	La majorité du trafic n'utilise pas IP/TCP/UDP ou la majorité des clients se trouvent dans un autre réseau. L'équilibrage de charge en réception ne dépend pas de la quantité de trafic, mais du nombre de clients connectés au système.

Question :	Quels sont les protocoles réseau pour lesquels un équilibrage de charge est effectué dans une équipe ?
Réponse :	Le logiciel de regroupement Broadcom prend uniquement en charge le trafic IP/TCP/UDP. Les autres types de trafic sont transférés vers la carte primaire.

Question :	Avec SLB, pour quels protocoles l'équilibrage de charge est-il effectué et pour lesquels ne l'est-il pas ?
Réponse :	L'équilibrage de charge est effectué dans les deux sens pour les protocoles IP/TCP/UDP uniquement : en émission et en réception.

Question :	Puis-je grouper un port fonctionnant à 100 Mbit/s et un port fonctionnant à 1 000 Mbit/s ?
Réponse :	L'utilisation de vitesses mixtes dans une équipe est seulement prise en charge pour les équipes Smart Load Balancing™ et 802.3ad, comme indiqué ci-dessus.

Question :	Puis-je grouper une carte fibre optique et une carte cuivre Gigabit Ethernet ?
Réponse :	Oui pour SLB et oui si le commutateur le permet dans FEC/GEC et 802.3ad.

Question :	Quelle est la différence entre l'équilibrage de charge de la carte et NLB (Network Load Balancing) de Microsoft ?
Réponse :	L'équilibrage de charge de la carte est effectué au niveau d'une session réseau, alors que NLB est effectué au niveau de l'application système.

Question :	Puis-je connecter les cartes groupées aux ports d'un routeur ?
Réponse :	Non. Tous les ports d'une équipe doivent se trouver sur le même réseau ; dans un routeur, en revanche, chaque port se trouve par définition sur un réseau distinct. Tous les modes de regroupement demandent à ce que le partenaire de liaison soit un commutateur de niveau 2.

Question :	Puis-je utiliser le regroupement avec Microsoft Cluster Services ?
Réponse :	Oui. Le regroupement est pris en charge exclusivement sur le réseau public et non sur le réseau privé utilisé pour la liaison par pulsations.

Question :	PXE peut-il fonctionner sur une carte virtuelle (équipe) ?
Réponse :	Un client PXE fonctionne dans un environnement avant que le système d'exploitation ne soit chargé, ce qui signifie que les cartes virtuelles n'ont pas encore été activées. Si la carte physique prend en charge PXE, elle peut être utilisée comme client PXE, qu'elle fasse partie ou non d'une carte virtuelle lors de chargement du système d'exploitation. Les serveurs PXE peuvent fonctionner sur une carte virtuelle.

Question :	Le réseau local de réveil peut-il fonctionner sur une carte virtuelle (équipe) ?
Réponse :	La fonction Réseau local de réveil fonctionne dans un environnement avant que le système d'exploitation ne soit chargé. Elle se déclenche lorsque le système est éteint ou en attente, aucune équipe n'est donc configurée.

Question :	Quel est le nombre maximum de ports pouvant être groupés ?
Réponse :	Jusqu'à 8 ports peuvent être associés à une équipe.

Question :	Quel est le nombre maximum d'équipes pouvant être configurées sur le même système ?
Réponse :	Jusqu'à 16 équipes peuvent être configurées sur le même système.

Question :	Pourquoi mon équipe perd-elle de la connectivité durant les 30 à 50 secondes suivant la restauration (reprise automatique) de la carte primaire ?
Réponse :	Parce que STP fait passer le port de l'état bloqué à l'état actif. Vous devez activer Port Fast ou Edge Port sur les ports de commutation connectés à l'équipe ou utiliser LiveLink pour rendre compte du délai lié au protocole STP.

Question :	Puis-je connecter une équipe de cartes reliées à des commutateurs différents ?
Réponse :	Smart Load Balancing peut être utilisé avec plusieurs commutateurs car chaque carte physique du système utilise une seule adresse MAC Ethernet. Link Aggregation et Generic Trunking ne peuvent pas fonctionner entre plusieurs commutateurs car ces modes demandent à ce que toutes les cartes physiques partagent la même adresse MAC Ethernet.

Question :	Comment mettre à niveau le pilote intermédiaire (BASP) ?
Réponse :	Le pilote intermédiaire ne peut être mis à niveau via les propriétés de la connexion locale. Il doit être mis à niveau à l'aide du programme d'installation.

Question :	Comment déterminer les statistiques de performances sur une carte virtuelle (équipe) ?
Réponse :	Dans Broadcom Advanced Control Suite, cliquez sur l'onglet Statistiques BASP de la carte virtuelle.

Question :	Puis-je configurer simultanément NLB et le regroupement ?
Réponse :	Oui, mais seulement lorsque NLB est exécuté en mode multidiffusion (NLB n'est pas pris en charge avec MS Cluster Services).

Question :	Le système de sauvegarde et les systèmes client sauvegardés doivent-ils être groupés ?
Réponse :	Dans la mesure où le système de sauvegarde subit la charge de données la plus importante, il doit toujours être groupé pour l'agrégation de liaisons et la reprise. Cependant, un réseau entièrement redondant exige que les commutateurs et les clients de sauvegarde soient groupés pour la tolérance aux pannes et l'agrégation de liaisons.

Question :	Lors des opérations de sauvegarde, l'algorithme de regroupement de cartes équilibre-t-il les charges des données au niveau de l'octet ou au niveau de la session ?
Réponse :	Lorsque le regroupement de cartes est utilisé, l'équilibrage de charge des données n'est effectué qu'au niveau de la session et non au niveau de l'octet afin d'éviter les trames mal classées. L'équilibrage de charge du regroupement de cartes ne fonctionne pas de la même manière que d'autres mécanismes d'équilibrage de charge de stockage comme EMC PowerPath.

Question :	Est-il nécessaire de configurer de manière spécifique le logiciel ou le matériel de sauvegarde sur bande pour qu'ils fonctionnent avec le regroupement de cartes ?
Réponse :	Aucune configuration spécifique n'est nécessaire pour que le logiciel de sauvegarde sur bande fonctionne avec le regroupement. Le regroupement est transparent pour les applications de sauvegarde sur bande.

Question :	Comment puis-je savoir quel pilote j'utilise actuellement ?
Réponse :	Dans tous les systèmes d'exploitation, la meilleure manière pour vérifier la version du pilote est de repérer physiquement le fichier du pilote et d'en vérifier les propriétés.

Question :	SLB peut-il détecter une défaillance de commutation si la tolérance aux pannes est activée ?
Réponse :	Non. SLB ne peut détecter que la perte de liaison entre le port groupé et son partenaire de liaison le plus proche. SLB ne peut détecter les défaillances de liaison sur d'autres ports. Reportez-vous à Fonctionnalité LiveLink™ pour plus de renseignements.

Question :	Où puis-je surveiller les statistiques en temps réel d'une équipe de cartes dans un système Windows ?
Réponse :	Utilisez Broadcom Advanced Control Suite (BACS) pour contrôler les compteurs généraux, IEEE 802.3 et personnalisés.

Messages du journal des événements

Messages du journal des événements sous Windows

Les messages d'état du journal des événements Windows du pilote de base et du pilote intermédiaire connus pour les cartes Gigabit Ethernet NetXtreme de Broadcom sont répertoriés dans la section suivante. Lors du chargement d'un pilote de carte Broadcom, Windows indique un code d'état dans l'observateur d'événements système. Ces codes d'événement peuvent être répartis en deux types d'entrées si les deux pilotes sont chargés (une série pour le pilote de base ou miniport et une autre série pour le pilote intermédiaire ou de regroupement).

Pilote de base (carte physique / miniport)

Le Tableau 11 répertorie les messages du journal des événements pris en charge par le pilote de base, explique la cause du message et indique l'action recommandée.

Tableau 11 : Messages du journal des événements du pilote de base

L'e-mail Numéro	L'e-mail	Cause	Action corrective
1	Failed to allocate memory for the device block. (Echec de l'allocation de mémoire pour le bloc du périphérique.) Check system memory resource usage. (Vérifiez l'utilisation des ressources mémoire système.)	Le pilote ne peut pas affecter de mémoire à partir du système d'exploitation.	Fermez les applications en cours pour libérer de la mémoire
2	Failed to allocate map registers. (Echec de l'allocation des registres de mappage.)	Le pilote ne peut pas allouer de registres de mappage à partir du système d'exploitation.	Déchargez d'autres pilotes pouvant allouer des registres de mappage.
3	Failed to access configuration information. (Echec de l'accès aux informations de configuration.) Reinstall the network driver. (Réinstallez le pilote réseau.)	Le pilote ne peut pas accéder aux registres de l'espace de configuration PCI sur la carte.	Pour les cartes complémentaires : réinstallez la carte dans le logement, déplacez la carte vers un autre logement PCI ou bien remplacez la carte.
4	The network link is up. (La liaison réseau est inactive.) Check to make sure the network cable is properly connected. (Assurez-vous que le câble réseau est correctement connecté.)	La carte a perdu sa connexion avec son partenaire de liaison.	Assurez-vous que le câble réseau est connecté, qu'il s'agit du bon type de câble et que le partenaire de liaison (par exemple, le commutateur ou le concentrateur) fonctionne correctement.

Tableau 11 : Messages du journal des événements du pilote de base (Suite)

L'e-mail Numéro	L'e-mail	Cause	Action corrective
5	The network link is up. (La liaison réseau est active.)	La carte a établi une liaison.	Message d'information uniquement. Aucune action requise.
6	Network controller configured for 10Mb half-duplex link. (Le contrôleur réseau est configuré pour une liaison semi-duplex de 10 Mbit.)	La carte a été configurée manuellement pour la vitesse de transmission et le duplex sélectionnés.	Message d'information uniquement. Aucune action requise.
7	Network controller configured for 10Mb full-duplex link. (Le contrôleur réseau est configuré pour une liaison duplex intégral de 10 Mbit.)	La carte a été configurée manuellement pour la vitesse de transmission et le duplex sélectionnés.	Message d'information uniquement. Aucune action requise.
8	Network controller configured for 100Mb half-duplex link. (Le contrôleur réseau est configuré pour une liaison semi-duplex de 100 Mbit.)	La carte a été configurée manuellement pour la vitesse de transmission et le duplex sélectionnés.	Message d'information uniquement. Aucune action requise.
9	Network controller configured for 100Mb full-duplex link. (Le contrôleur réseau est configuré pour une liaison duplex intégral de 100 Mbit.)	La carte a été configurée manuellement pour la vitesse de transmission et le duplex sélectionnés.	Message d'information uniquement. Aucune action requise.
10	Network controller configured for 1Gb half-duplex link. (Le contrôleur réseau est configuré pour une liaison semi-duplex de 1 Gbit.)	La carte a été configurée manuellement pour la vitesse de transmission et le duplex sélectionnés.	Message d'information uniquement. Aucune action requise.
11	Network controller configured for 1Gb full-duplex link. (Le contrôleur réseau est configuré pour une liaison duplex intégral de 1 Gbit.)	La carte a été configurée manuellement pour la vitesse de transmission et le duplex sélectionnés.	Message d'information uniquement. Aucune action requise.
12	Medium not supported. (Support non pris en charge.)	Le système d'exploitation ne prend pas en charge le support IEEE 802.3.	Redémarrez le système d'exploitation, lancez une analyse antivirus, lancez une analyse du disque (à l'aide de la commande chkdsk) et réinstallez le système d'exploitation.
13	Unable to register the interrupt service routine. (Impossible d'enregistrer le sous-programme du service d'interruption.)	Le pilote du périphérique ne peut pas installer le gestionnaire d'interruption.	Redémarrez le système d'exploitation ; retirez les autres pilotes de périphérique qui partagent le même IRQ.
14	Unable to map IO space. (Impossible de mapper l'espace E/S.)	Le pilote du périphérique ne peut pas affecter d'E/S mappées en mémoire pour accéder à des registres de pilote.	Retirez les autres cartes du système, réduisez la quantité de mémoire physique installée et remplacez la carte.
15	Driver initialized successfully. (Le pilote a été initialisé.)	Le pilote a été chargé.	Message d'information uniquement. Aucune action requise.

Tableau 11 : Messages du journal des événements du pilote de base (Suite)

L'e-mail Numéro	L'e-mail	Cause	Action corrective
16	NDIS is resetting the miniport driver. (NDIS réinitialise le pilote miniport.)	La couche NDIS a détecté un problème d'envoi/de réception de paquets et réinitialise le pilote pour résoudre le problème.	Exécutez les diagnostics de Broadcom Advanced Control Suite ; vérifiez que le câble réseau fonctionne.
18	Unknown PHY detected. (PHY inconnu détecté.) Using a default PHY initialization routine. (Utilisation d'une routine d'initialisation PHY par défaut.)	Le pilote n'a pas pu lire l'ID de PHY.	Remplacez la carte.
19	This driver does not support this device. (Ce pilote ne prend pas ce périphérique en charge.) Upgrade to the latest driver. (Passez à la dernière version du pilote.)	Le pilote ne reconnaît pas la carte installée.	Passez à une version de pilote prenant en charge cette carte.
20	Driver initialization failed. (L'initialisation du pilote a échoué.)	Echec non spécifié pendant l'initialisation du pilote.	Réinstallez le pilote, effectuez la mise à niveau vers un pilote plus récent, exécutez les diagnostics de Broadcom Advanced Control Suite ou remplacez la carte.
21	VEthernet@WireSpeed est activé et n'a pas pu négocier la vitesse maximale de la liaison.	Connexion ou câble probablement défectueux.	Rebranchez le câble ou changez-le.
22	Impossible d'installer le pilote de périphérique d'un contrôleur réseau obsolète pour ce système d'exploitation.	Le dernier pilote de boîte d'envoi ne prend plus en charge le périphérique obsolète.	Utilisez le pilote fourni ou remplacez le périphérique.
256	Mémoire physique contiguë insuffisante pour la fusion de pool.	Le pilote ne peut pas allouer suffisamment de mémoire partagée pour la fusion des tampons des paquets.	Supprimez/désactivez une autre carte du système ou augmentez la mémoire système.

Pilote intermédiaire (carte virtuelle / équipe)

Le Tableau 12 répertorie les messages du journal des événements pris en charge par le pilote intermédiaire, explique la cause du message et indique l'action recommandée.

Tableau 12 : Messages du journal des événements du pilote intermédiaire

Evénement système Numéro du message	L'e-mail	Cause	Action corrective
1	Unable to register with NDIS. (Impossible d'enregistrer avec NDIS.)	Le pilote ne peut pas s'enregistrer auprès de l'interface NDIS.	Déchargez d'autres pilotes NDIS.

Tableau 12 : Messages du journal des événements du pilote intermédiaire (Suite)

Evénement système Numéro du message	L'e-mail	Cause	Action corrective
2	Unable to instantiate the management interface. (Impossible d'instancier l'interface de gestion.)	Le pilote ne peut pas créer d'instance de périphérique.	Redémarrez le système d'exploitation.
3	Unable to create symbolic link for the management interface. (Impossible de créer de lien symbolique pour l'interface de gestion.)	Un autre pilote a entraîné un conflit de nom de périphérique.	Déchargez le pilote de périphérique à l'origine du conflit qui utilise le nom *Blf*.
4	Broadcom Advanced Server Program Driver has started. (Le pilote BASP a démarré.)	Un autre pilote a entraîné un conflit de nom de périphérique.	Message d'information uniquement. Aucune action requise.
5	Broadcom Advanced Server Program Driver has stopped. (Le pilote BASP s'est arrêté.)	Le pilote s'est arrêté.	Message d'information uniquement. Aucune action requise.
6	Could not allocate memory for internal data structures. (Impossible d'allouer de la mémoire pour les structures de données internes.)	Le pilote ne peut pas affecter de mémoire à partir du système d'exploitation.	Fermez les applications en cours pour libérer de la mémoire
7	Could not bind to adapter. (Impossible d'effectuer la liaison à la carte.)	Le pilote n'a pas pu ouvrir l'une des cartes physiques de l'équipe.	Déchargez et rechargez le pilote de la carte physique, installez un pilote de carte physique mis à jour ou remplacez la carte physique.
8	Successfully bind to adapter. (Liaison à la carte effectuée.)	Le pilote a pu ouvrir la carte physique.	Message d'information uniquement. Aucune action requise.
9	Network adapter is disconnected. (La carte réseau est déconnectée.)	La carte physique n'est pas connectée au réseau (elle n'a pas établi de liaison).	Assurez-vous que le câble réseau est connecté, qu'il s'agit du bon type de câble et que le partenaire de liaison (le commutateur ou le concentrateur) fonctionne correctement.
10	Network adapter is connected. (La carte réseau est connectée.)	La carte physique est connectée au réseau (elle a établi une liaison).	Message d'information uniquement. Aucune action requise.
11	Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System. (Le pilote BASP n'est pas conçu pour fonctionner sur cette version de système d'exploitation.)	Le pilote ne prend pas en charge le système d'exploitation sur lequel il est installé.	Consultez les notes de version du pilote, puis installez-le sur un système d'exploitation pris en charge ou bien mettez-le à jour.

Tableau 12 : Messages du journal des événements du pilote intermédiaire (Suite)

Evénement système Numéro du message	L'e-mail	Cause	Action corrective
12	Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter. (La carte auxiliaire en réplique synchrone est sélectionnée comme carte primaire pour une équipe ne disposant pas de carte d'équilibrage de charge.)	Une carte auxiliaire a été activée.	Remplacez la carte physique défaillante.
13	Network adapter does not support Advanced Failover. (La carte réseau ne prend pas en charge la reprise avancée.)	La carte physique ne prend pas charge Broadcom NIC Extension (NICE).	Remplacez la carte par une autre qui prend en charge NICE.
14	Network adapter is enabled via management interface. (La carte réseau est activée via l'interface de gestion.)	Le pilote a pu activer une carte physique via l'interface de gestion.	Message d'information uniquement. Aucune action requise.
15	Network adapter is disabled via management interface. (La carte réseau est désactivée via l'interface de gestion.)	Le pilote a pu désactiver une carte physique via l'interface de gestion.	Message d'information uniquement. Aucune action requise.
16	Network adapter is activated and is participating in network traffic. (La carte réseau est activée et participe au trafic réseau.)	Une carte physique a été ajoutée ou activée dans une équipe.	Message d'information uniquement. Aucune action requise.
17	Network adapter is de-activated and is no longer participating in network traffic. (La carte réseau est désactivée et ne participe plus au trafic réseau.)	Le pilote ne reconnaît pas la carte installée.	Message d'information uniquement. Aucune action requise.

Section 4 : Réseaux locaux virtuels (VLAN)

Présentation de VLAN

Les VLAN vous permettent de partager votre réseau local physique en parties logiques, en vue de créer une segmentation logique des groupes de travail et de mettre en application des politiques de sécurité dans chaque segment logique. Chaque VLAN défini se comporte comme un réseau indépendant, son trafic et ses diffusions étant isolés des autres réseaux, ce qui assure une meilleure efficacité de la bande passante au sein de chaque groupe logique. Il est possible de définir jusqu'à 64 VLAN (63 identifiés et 1 non identifié) pour chaque carte Broadcom de votre serveur, en fonction de la quantité de mémoire disponible sur votre système.

Il est possible d'ajouter des réseaux locaux virtuels à une équipe de façon à obtenir plusieurs réseaux locaux virtuels ayant différentes identités de réseau. Une carte virtuelle est créée pour chaque réseau local ajouté.

Bien que les VLAN soient généralement utilisés pour créer des domaines de diffusion individuels et/ou des sous-réseaux IP indépendants, il est parfois utile qu'un serveur soit simultanément en liaison avec plusieurs VLAN. Les cartes Broadcom prennent en charge plusieurs VLAN par port d'accès ou par équipe, offrant ainsi une très grande souplesse de configuration du réseau.

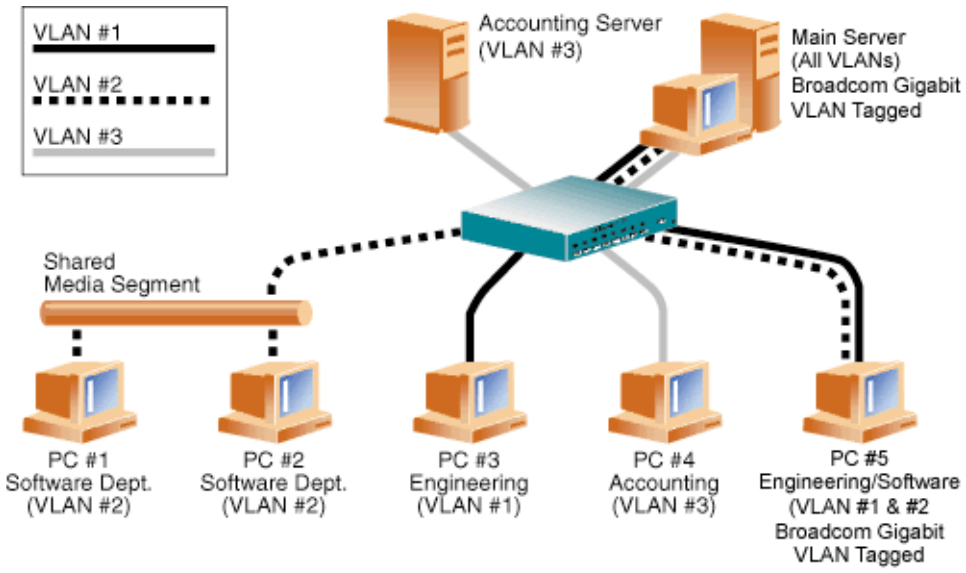


Figure 7 : Exemple de serveurs prenant en charge plusieurs VLAN avec référencement

La Figure 7 présente un exemple de réseau qui utilise des VLAN. Dans ce réseau type, le réseau local physique est composé d'un commutateur, de deux serveurs et de cinq clients. Le réseau local est organisé logiquement en trois VLAN, chacun représentant un sous-réseau IP particulier. Les fonctionnalités de ce réseau sont décrites dans le Tableau 13 :

Tableau 13 : Topologie d'un réseau local virtuel type

Composant	*Commentaires*
VLAN #1	Un sous-réseau IP constitué du serveur principal, du PC #3 et du PC #5. Ce sous-réseau représente un groupe Ingénierie.
VLAN #2	Comprend le serveur principal, les PC #1 et #2 reliés par le concentrateur commun et le PC #5. Ce VLAN est un groupe de développement de logiciels.
VLAN #3	Comprend le serveur principal, le serveur de comptabilité et le PC #4. Ce VLAN est un groupe de comptabilité.
Serveur du nom primaire	Un serveur à usage intensif qui doit être accessible depuis tous les VLAN et les sous-réseaux IP. Une carte Broadcom est installée sur le serveur principal. Les trois sous-réseaux sont accessibles par le biais de la carte physique unique qui sert d'interface. Le serveur est relié à un des ports de commutation qui est configuré pour les VLAN #1, #2 et #3. Le référencement est activé sur la carte et le port de commutation connecté. Grâce aux possibilités de référencement de VLAN de ces deux dispositifs, le serveur peut communiquer sur les trois sous-réseaux IP de ce réseau, mais continue à maintenir une diffusion distincte.
Serveur de comptabilité	Disponible pour le VLAN #3 uniquement. Le serveur de comptabilité est isolé du trafic des VLAN #1 et #2. Le référencement du port de commutation connecté au serveur est désactivé.
PC #1 et #2	Reliés à un concentrateur commun qui est ensuite connecté au commutateur. Les PC #1 et #2 appartiennent au VLAN #2 uniquement et se trouvent logiquement dans le même sous-réseau IP que le serveur principal et le PC #5. Le référencement n'est pas activé sur le port de commutation connecté.
PC #3	Un élément du VLAN #1, le PC #3 peut communiquer uniquement avec le serveur principal et le PC #5. Le référencement n'est pas activé sur le port de commutation de ce PC #3.
PC #4	Un élément de VLAN #3, PC #4 peut communiquer uniquement avec les serveurs. Le référencement n'est pas activé sur le port de commutation du PC #4.
PC #5	Un élément des VLAN #1 et #2, le PC #5 comporte une carte Broadcom. Il est connecté au port de commutation #10. La carte et le port de configuration sont configurés pour les VLAN #1 et #2 et le référencement est activé.

Remarque : Il est nécessaire d'activer le référencement des VLAN uniquement sur les ports de commutation qui créent des liaisons communes avec d'autres commutateurs ou sur les ports connectés pouvant référencer les terminaux, tels que les serveurs ou les postes de travail avec les cartes Broadcom.

Ajout de réseaux locaux virtuels (VLAN) à des équipes

Chaque équipe peut prendre en charge jusqu'à 64 VLAN (63 identifiés et 1 non identifié). Avec plusieurs VLAN sur une carte, un serveur comportant une seule carte peut être en liaison logique avec plusieurs sous-réseaux IP. Lorsqu'une équipe comporte plusieurs VLAN, un serveur peut être en liaison logique avec plusieurs sous-réseaux IP et bénéficier de l'équilibrage de volume et de la reprise de trafic en cas de défaillance. Pour obtenir des instructions sur l'ajout d'un VLAN à une équipe, reportez-vous à la section Ajout d'un réseau local virtuel pour les systèmes d'exploitation Windows.

Remarque : Les cartes qui appartiennent à l'équipe de reprise peuvent être configurées pour prendre en charge les VLAN. Etant donné que les VLAN ne sont pas pris en charge pour un réseau local sur carte NIC tierce si une carte NIC tierce appartient à une équipe de reprise, les VLAN ne peuvent pas être configurés pour cette équipe.

Section 5 : Gérabilité

CIM

Common Information Model (CIM) est une norme de l'industrie définie par le groupement Distributed Management Task Force (DMTF). Microsoft met en oeuvre CIM sur les plates-formes Windows telles que Windows Server 2008. Broadcom prend en charge CIM sur les plates-formes Windows Server 2008.

La mise en oeuvre de CIM par Broadcom introduit diverses classes permettant de fournir des informations à l'utilisateur par le biais d'applications client CIM. Notez que le serveur CIM Broadcom fournit uniquement des données ; l'utilisateur peut choisir son logiciel client CIM préféré pour parcourir les informations mises à sa disposition par le serveur CIM Broadcom.

Le serveur CIM Broadcom fournit des informations par le biais de la carte BRCM_NetworkAdapter et des classes BRCM_ExtraCapacityGroup. La classe BRCM_NetworkAdapter fournit des informations sur la carte réseau, relatives à un groupe de cartes, y compris les contrôleurs Broadcom et ceux d'autres constructeurs. La classe BRCM_ExtraCapacityGroup fournit une configuration du groupe pour le programme BASP (Broadcom Advanced Server Program). La mise en oeuvre actuelle permet de fournir des informations sur l'équipe et sur les cartes réseau physiques de l'équipe.

Le programme Broadcom Advanced Server Program fournit des événements par le biais des journaux d'événements. L'utilisateur peut employer l'outil « Observateur d'événements » fourni par Windows Server 2008 ou utiliser CIM pour vérifier ou contrôler ces événements. Le serveur CIM Broadcom fournit également des informations sur les événements par le biais du modèle générique d'événements CIM. Ces événements sont __InstanceCreationEvent, __InstanceDeletionEvent et __InstanceModificationEvent. Ils sont définis par CIM. Selon CIM, l'application client doit enregistrer les événements en provenance de l'application client. A cette fin, elle procèdera à des interrogations comme l'indiquent les exemples ci-dessous, afin de recevoir les événements correctement.

```
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "BRCM_ExtraCapacityGroup"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "BRCM_ActsAsSpare"
SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "BRCM_ActsAsSpare"
```

Pour obtenir des informations détaillées sur ces événements, consultez la documentation CIM à l'adresse : http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf.

SNMP

Sous-agent BASP

Le sous-agent BASP, baspmgnt.dll, est conçu pour le service SNMP de Windows Server. Il est nécessaire pour réaliser l'installation du service SNMP avant celle du sous-agent BASP.

Le sous-agent BASP permet au logiciel du gestionnaire SNMP de contrôler activement les configurations et la qualité d'exécution des fonctionnalités du serveur Broadcom Advanced Server. Le sous-agent fournit également un filtre d'avertissement au gestionnaire SNMP pour l'informer de toutes modifications relatives à l'état du composant of BASP.

Le sous-agent BASP permet de contrôler les configurations et les statistiques des groupes BASP, des cartes NIC physiques appartenant à un groupe et des cartes NIC virtuelles créées à la suite du regroupement. Les cartes NIC qui ne sont pas groupées, ne sont alors pas contrôlées. La configuration BASP inclut des informations relatives à l'ID du groupe, les ID des cartes de l'équipe/VLAN/physiques/virtuelles, les descriptions des cartes de l'équipe/VLAN/physiques/virtuelles et les adresses MAC des cartes.

Les statistiques comprennent des informations détaillées relatives aux paquets de données transmises et reçues pour les cartes du groupe/VLAN/physiques/virtuelles.

Le filtre d'avertissement envoie des informations sur les modifications apportées à la configuration des cartes physiques appartenant à un groupe, telles que la liaison haut/bas de la carte physique et les événements installés/supprimés de la carte.

Pour contrôler ces informations, le gestionnaire SNMP doit charger les fichiers de la base de données MIB du BASP Broadcom, pour permettre le contrôle des informations décrites ci-dessus. Les fichiers ci-dessous figurent sur le support source du pilote :

baspcfg.mib

baspstat.mib

basptrap.mib

Agent extensible BASP

L'agent extensible SNMP d'informations détaillées sur le contrôleur NetXtreme Gigabit Ethernet de Broadcom (bcmif.dll) est conçu pour le service SNMP de Windows Server 2008.

L'agent extensible permet au logiciel du gestionnaire SNMP de contrôler activement les configurations de la carte Broadcom NetXtreme. Il est destiné à compléter les informations déjà fournies par l'interface réseau de gestion SNMP standard.

L'agent extensible fournit des informations approfondies sur la carte NetXtreme de Broadcom, telles que :

- l'adresse MAC
- son adresse IP liée
- le masque de sous-réseau IP
- l'état de liaison physique
- l'état de la carte
- le taux d'émission

- le mode duplex
- la plage de capacité mémoire
- le réglage de l'interruption
- le numéro du bus
- le numéro du dispositif
- le numéro de fonction

Pour contrôler ces informations, le gestionnaire SNMP doit charger le fichier MIB d'informations détaillées de Broadcom, pour pouvoir contrôler les informations décrites ci-dessus. Ce fichier, bcmif.mib, se trouve sur le CD d'installation de la carte NetXtreme de Broadcom.

Le poste de travail contrôlé requiert d'une part l'installation de l'agent extensible SNMP d'informations détaillées de Broadcom, bcmif.dll et d'autre part, l'installation et le chargement du service SNMP de Microsoft Windows Server 2008.

Section 6 : Installation du matériel

Remarque : Cette section s'applique uniquement aux modèles NIC complémentaires des cartes Gigabit Ethernet NetXtreme de Broadcom.

Mesures de sécurité

Attention : la carte est installée dans un système fonctionnant à une tension risquant d'être mortelle. Avant de retirer le capot de votre système, vous devez prendre les mesures suivantes afin de vous protéger et d'éviter tout risque de destruction des composants du système.

- Enlevez les objets métalliques ou les bijoux que vous portez aux mains et aux poignets.
- Veillez à utiliser uniquement des outils isolés ou non conducteurs.
- Vérifiez que le système est hors tension et que la prise est débranchée avant de toucher tout composant interne.
- Installez ou enlevez les cartes dans un environnement exempt d'électricité statique. Le port d'un bracelet antistatique correctement relié à la terre ou de tout autre dispositif antistatique ainsi que l'utilisation d'un tapis antistatique sont vivement conseillés.

Liste de vérification avant l'installation

1. Vérifiez que votre serveur utilise le BIOS le plus récent.
2. Si votre système est démarré à partir d'un système d'exploitation, arrêtez correctement le système d'exploitation.
3. Une fois le système arrêté, coupez l'alimentation secteur et débranchez la prise de l'ordinateur.
4. En tenant la carte par les bords, enlevez-la de son emballage d'expédition et placez-la sur une surface antistatique.
5. Vérifiez que la carte ne présente aucun signe de détérioration, en particulier sur le connecteur de bord. N'essayez jamais d'installer une carte abîmée.

Installation de la carte

Les instructions suivantes concernent l'installation de la carte Gigabit Ethernet NetXtreme de Broadcom (NIC complémentaire) sur la plupart des serveurs. Reportez-vous aux manuels fournis avec votre serveur pour toute précision sur la réalisation de ces tâches sur votre serveur spécifique.

1. Consultez les Mesures de sécurité et la Liste de vérification avant l'installation. Avant d'installer la carte, assurez-vous que le système est hors tension et débranché. Veillez à ce que les procédures de mise à la terre aient été suivies correctement.
2. Ouvrez le boîtier du système et sélectionnez un logement PCI Express vide.
3. Enlevez la platine avant nue (lame d'obturation) du logement sélectionné.
4. Alignez le bord du connecteur de la carte sur le logement du connecteur dans le système.
5. En exerçant une pression égale sur les deux coins de la carte, enfoncez celle-ci dans le logement jusqu'à ce qu'elle soit bien positionnée. Une fois la carte correctement positionnée, le connecteur du port de la carte est aligné sur l'ouverture du logement et sa platine avant se trouve dans l'alignement du châssis du système.

Attention : n'exercez pas de pression excessive lorsque vous calez la carte, car vous pourriez endommager le système ou la carte. Si vous avez du mal à enfoncer la carte, retirez-la, réalignez-la et recommencez.

6. Fixez la carte avec son clip ou sa vis.
7. Refermez le boîtier du système et détachez les dispositifs antistatiques.

Connexion des câbles réseau

Cuivre

La carte Gigabit Ethernet NetXtreme de Broadcom comporte un ou plusieurs connecteur(s) RJ-45 permettant de fixer le système à un segment de fil en cuivre Ethernet.

Remarque : La carte Gigabit Ethernet NetXtreme de Broadcom prend en charge le mode MDIX (Automatic MDI Crossover), qui permet de ne pas utiliser des câbles croisés lors de la connexion d'ordinateurs de manière consécutive. Un câble direct catégorie 5 permet aux ordinateurs de communiquer quand ils sont connectés directement.

1. Sélectionnez le câble approprié. Le Tableau 14. « Caractéristiques du câble 10/100/1000BASE-T » recense les caractéristiques du câble assurant une connexion aux ports 10/100/1000BASE-T :

Tableau 14 : Caractéristiques du câble 10/100/1000BASE-T

Type de port	*Connecteur*	*Type de câble*	*Longueur maximum*
10BASE-T	RJ-45	Paires torsadées non blindées (UTP) de catégorie 3, 4 ou 5	100 mètres
100/1000BASE-T[1]	RJ-45	Catégorie 5[2] UTP	100 mètres

[1]Conformément aux normes ISO/IEC 11801:1995 et EIA/TIA-568-A (1995), le support 1000BASE-T exige la connexion de quatre paires torsadées de catégorie 5, qui ont été testées selon les procédures d'essai définies dans TIA/EIA TSB95.

[2]CAT 5 est la configuration minimale requise. Les configurations CAT 5e et CAT 6 sont entièrement prises en charge.

2. Connectez une extrémité du câble à la carte.
3. Connectez l'autre extrémité du câble à un port RJ-45 du réseau Ethernet.

Remarque : dès que le câble est connecté correctement aux deux extrémités, les voyants du port de la carte doivent fonctionner. Voir Tableau 14 : « Caractéristiques du câble 10/100/1000BASE-T » à la page 67 pour obtenir une description des indicateurs de liaison au réseau et d'activité.

Section 7 : Création d'une disquette pilote

Pour les instructions de création d'une disquette pilote, reportez-vous à la documentation fournie avec votre système.

Section 8 : Logiciel pilote pour Boot Agent de Broadcom

Présentation

Les cartes Gigabit Ethernet NetXtreme de Broadcom prennent en charge l'environnement PXE (Preboot Execution Environment), RPL (Remote Program Load), l'initialisation iSCSI et BootP (Bootstrap Protocol). Multi-Boot Agent (MBA) est un module logiciel qui permet à votre système réseau de démarrer avec les images fournies par des systèmes distants par le biais du réseau. Le pilote MBA Broadcom est conforme à la spécification PXE 2.1 et est fourni avec des images monolithiques et des images binaires démultipliées. Il assure ainsi une souplesse d'exploitation dans divers environnements où la carte mère ne dispose pas toujours d'un code de base intégré.

Le module MBA fonctionne dans un environnement client/système. Un réseau comprend un ou plusieurs systèmes d'amorçage qui fournissent des images d'amorçage à de multiples systèmes du réseau. La mise en œuvre du module MBA a été testée avec succès dans les environnements suivants :

- **Serveur Linux® Red Hat® PXE.** Les clients PXE de Broadcom peuvent amorcer à distance les ressources du réseau pour les exploiter (montage NFS, etc.) et pour installer Linux. Dans le cas d'un amorçage à distance, le pilote universel Linux s'associe de façon transparente à l'interface UNDI (Universal Network Driver Interface) de Broadcom et fournit une interface réseau dans l'environnement client amorcé à distance par Linux.
- **Intel® APITEST.** Le pilote PXE de Broadcom PXE a subi avec succès toutes les séries de tests de conformité API.
- **Windows Deployment Service (WDS)**. Pour Windows Server, RIS a été remplacé par WDS, qui propose un client PXE Broadcom pour installer les systèmes d'exploitation Windows, notamment Windows Server 2008.

Configuration de MBA dans un environnement client

Pour les NIC complémentaires, suivez la procédure suivante. Pour les LOM, reportez-vous au guide du système de votre ordinateur.

La configuration de MBA dans un environnement client fait appel à la procédure suivante :

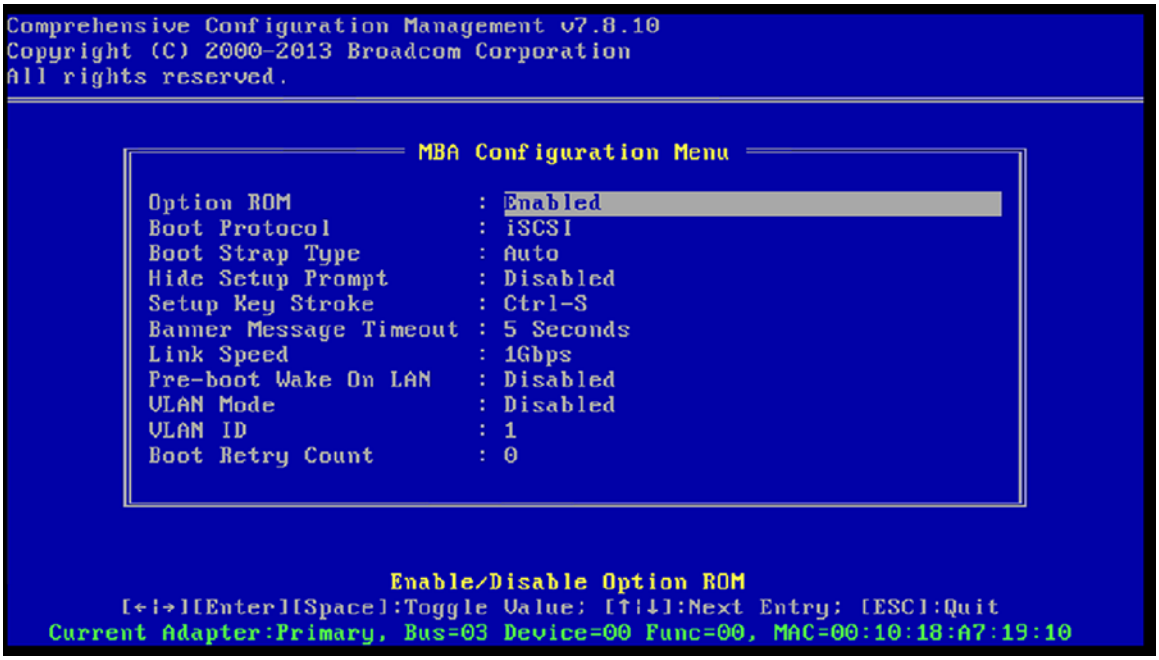
1. Configuration du pilote MBA
2. Configuration de l'ordre d'amorçage dans le BIOS

Configuration du pilote MBA

Cette section traite de la configuration du pilote MBA sur des modèles NIC complémentaires de la carte réseau Broadcom. Pour savoir comment configurer le pilote MBA sur des modèles LOM de la carte réseau Broadcom, reportez-vous à la documentation de votre système.

Avec CCM

1. Redémarrez votre système.
2. Appuyez sur les touches **CTRL+S** dans les 4 secondes suivant le moment où vous y êtes invité. La liste des cartes apparaît.
   a. Sélectionnez la carte à configurer et appuyez sur **Entrée**. Le menu principal apparaît.
   b. Sélectionnez **Configuration MBA** pour afficher le menu de configuration MBA.



3. Utilisez les flèches de direction HAUT et BAS pour sélectionner l'élément de menu Boot Protocol (Protocole d'amorçage). Puis, utilisez la touche DROITE ou GAUCHE pour sélectionner le protocole d'amorçage de votre choix si

des protocoles d'amorçage autres que PXE (Preboot Execution Environment) sont disponibles. S'ils sont disponibles, les autres protocoles d'amorçage incluent RPL (Remote Program Load) et BOOTP (Bootstrap Protocol).

Remarque : Pour certaines cartes LOM prenant en charge l'initialisation iSCSI, le protocole d'amorçage est défini via le BIOS. Pour plus d'informations, consultez la documentation de votre système.

Remarque : Si plusieurs cartes sont installées sur votre système et que vous ne savez pas avec certitude quelle carte vous êtes en train de configurer, appuyez sur **CTRL+F6** : les voyants de port de la carte se mettent à clignoter.

4. Utilisez les touches HAUT, BAS, GAUCHE et DROIT pour sélectionner et modifier les valeurs des autres éléments de menu, comme vous le souhaitez.
5. Appuyez sur **F4** pour enregistrer vos paramètres.
6. Appuyez sur **ECHAP** lorsque vous avez terminé.

Avec uEFI

1. Redémarrez votre système.
2. Entrez dans le menu Configuration du système ou Configuration de périphérique.
3. Sélectionnez le périphérique sur lequel vous souhaitez apporter des modifications aux paramètres MBA.
4. Sélectionnez **Menu de configuration MBA**.
5. Utilisez le menu déroulant pour sélectionner le protocole d'amorçage de votre choix, si des protocoles en dehors de Preboot Execution Environment (PXE) sont disponibles. S'ils sont disponibles, les autres protocoles d'amorçage incluent iSCSI et BOOTP (Bootstrap Protocol).

Remarque : Pour certaines cartes LOM prenant en charge l'initialisation iSCSI, le protocole d'amorçage est défini via le BIOS. Pour plus d'informations, consultez la documentation de votre système.

6. Utilisez les touches HAUT, BAS, GAUCHE et DROIT pour sélectionner et modifier les valeurs des autres éléments de menu, comme vous le souhaitez.
7. Sélectionnez **Retour** pour aller dans le menu principal
8. Sélectionnez **Terminer** pour enregistrer et quitter.

Configuration du BIOS

Pour amorcer le système avec le MBA depuis le réseau, désignez la carte MBA comme premier périphérique amorçable dans le BIOS. Cette procédure varie selon l'implémentation BIOS du système. Consultez le manuel d'utilisation du système pour obtenir des instructions.

Configuration de MBA dans un environnement serveur

Serveur Linux PXE

Linux comporte une prise en charge du serveur PXE. Il permet de réaliser à distance une installation Linux complète par l'intermédiaire du réseau. L'utilitaire de distribution est accompagné d'images d'amorçage - noyau d'amorçage (vmlinuz) et d'un disque virtuel initial (initrd) qui se trouvent sur le disque #1 :

/images/pxeboot/vmlinuz

/images/pxeboot/initrd.img

Consultez la documentation Linux pour savoir comment installer le serveur PXE sur Linux.

Il n'est pas nécessaire d'avoir le pilote réseau standard de Linux pour la carte Gigabit Ethernet NetXtreme de Broadcom pour réaliser un amorçage à distance. Après que le client PXE a téléchargé le noyau Linux et le disque virtuel initial, le pilote universel de Linux accompagnant l'utilitaire de distribution de Linux s'associe au code UNDI du PXE pour constituer un pilote réseau Linux.

Section 9 : Protocole iSCSI

Initialisation iSCSI

Les cartes Gigabit Ethernet NetXtreme de Broadcom prennent en charge l'initialisation iSCSI afin de permettre le démarrage réseau de systèmes d'exploitation sur des systèmes sans disque. L'initialisation iSCSI permet le démarrage d'un système d'exploitation Windows ou Linux à partir d'un ordinateur cible iSCSI se trouvant sur un réseau IP standard distant.

Pour les systèmes d'exploitation Windows et Linux, l'initialisation iSCSI peut être configurée de manière à lancer le démarrage à l'aide des paramètres généraux indiqués dans Tableau 15.

Systèmes d'exploitation pris en charge pour l'initialisation iSCSI

Les cartes Gigabit Ethernet NetXtreme de Broadcom prennent en charge l'initialisation iSCSI sur les systèmes d'exploitation suivants :

- Système d'exploitation Windows Server
- Distribution Enterprise Linux

Configuration du démarrage iSCSI

Le démarrage iSCI n’est pas pris en charge en mode BIOS quand il existe un stockage local (notamment RAID) du fait de contraintes mémoire EBDA.

La configuration du démarrage iSCSI comprend les étapes suivantes :

- Configuration de la cible iSCSI
- Configuration des paramètres d'initialisation iSCSI
- Préparation de l'image de démarrage iSCSI
- Redémarrage

Configuration de la cible iSCSI

La configuration de la cible iSCSI varie en fonction des fournisseurs cibles. Pour plus d'informations sur la configuration de la cible iSCSI, reportez-vous à la documentation du fournisseur. Les étapes générales sont les suivantes :

1. Créez une cible iSCSI.
2. Créez un disque virtuel.
3. Mappez le disque virtuel à la cible iSCSI créée à l'étape 1.

4. Associez un initiateur iSCSI à la cible iSCSI.
5. Enregistrez le nom de la cible iSCSI, le numéro du port TCP, le numéro d'unité logique (LUN) iSCSI, le nom IQN de l'initiateur et les détails d'authentification CHAP.
6. Une fois la cible iSCSI configurée, notez les éléments suivants :
   - Nom IQN de la cible
   - Adresse IP cible
   - Numéro de port TCP de la cible
   - Numéro d'unité logique (LUN) de la cible
   - Nom IQN de l'initiateur
   - Réf. et clé secrète CHAP

Configuration des paramètres d'initialisation iSCSI

Configurez le logiciel de démarrage iSCSI de Broadcom de manière statique ou dynamique. Reportez-vous au Tableau 15 pour connaître les options de configuration disponibles depuis l'écran Paramètres généraux.

Le Tableau 15 répertorie les paramètres pour IPv4 et IPv6. Les paramètres spécifiques à IPv4 ou IPv6 sont notés.

Remarque : La disponibilité de l'initialisation iSCSI IPv6 dépend de la plate-forme/du périphérique.

Tableau 15 : Options de configuration

Option	*Commentaires*
Paramètres TCP/IP via DHCP	Cette option est spécifique à IPv4. Contrôle si le logiciel hôte de démarrage iSCSI obtient les informations d'adresse IP via DHCP (Activé) ou par le biais d'une configuration IP statique (Désactivé).
Configuration IP automatique	Cette option est spécifique à IPv6. Contrôle si le logiciel hôte de démarrage iSCSI configure une adresse lien-local sans état et/ou une adresse avec état si DHCPv6 est présent et utilisé (Activé). Des paquets de sollicitation du routeur sont envoyés jusqu'à trois fois à un intervalle de 4 secondes entre chaque tentative. Vous pouvez aussi utiliser une configuration IP statique (Désactivé).
Paramètres iSCSI via DHCP	Contrôle si le logiciel hôte de démarrage iSCSI obtient ses paramètres cibles iSCSI via DHCP (Activé) ou par le biais d'une configuration statique (Désactivé). Les informations statiques sont à indiquer dans l'écran iSCSI Initiator Parameters Configuration (Configuration des paramètres de l'initiateur iSCSI).
Authentification CHAP	Contrôle si le logiciel hôte de démarrage iSCSI utilise une authentification CHAP lors de sa connexion à la cible iSCSI. Si l'authentification CHAP est activée, la réf. et la clé secrète CHAP sont à indiquer dans l'écran iSCSI Initiator Parameters Configuration (Configuration des paramètres de l'initiateur iSCSI).
Réf. fournisseur DHCP	Contrôle de quelle façon le logiciel hôte de démarrage iSCSI interprète le champ Vendor Class ID (ID de la classe du fournisseur) utilisé avec DHCP. Si le champ Vendor Class ID (ID de la classe du fournisseur) du paquet de l'Offre DHCP correspond à la valeur du champ, le logiciel hôte de démarrage iSCSI recherche les extensions de démarrage iSCSI requises dans le champ Option DHCP 43. Si DHCP est désactivé, il n'est pas nécessaire de désactiver cette valeur.
Durée d'établissement de la liaison	Contrôle la durée d'attente du logiciel hôte de démarrage iSCSI, en secondes, une fois la liaison Ethernet établie, avant de transmettre des données sur le réseau. Les valeurs valides sont comprises entre 0 et 255. Par exemple, un utilisateur devra définir une valeur pour cette option si un protocole réseau, tel que STP, est activé sur l'interface de commutateur du système client.

Tableau 15 : Options de configuration (Suite)

Option	*Commentaires*
Utiliser l'horodatage TCP	Contrôle si l'option d'horodatage TCP est activée ou désactivée.
Cibler comme premier disque dur	Permet de définir le lecteur cible iSCSI comme premier lecteur de disque dur du système.
Nombre d'essais de connexion à une unité logique occupée	Contrôle le nombre de tentatives de reconnexion effectué par l'initiateur de démarrage iSCSI lorsque le numéro d'unité logique de la cible iSCSI est occupé.
IP Version (Version IP)	Cette option est spécifique à IPv6. Permet de passer du protocole IPv4 au protocole IPv6. Tous les paramètres IP sont perdus lorsque vous basculez d'une version de protocole à une autre.

MBA Boot Protocol Configuration (Configuration du protocole de démarrage MBA)

Pour configurer le protocole de démarrage

1. Redémarrez votre système.
2. A partir de la bannière PXE, sélectionnez **CTRL+S**. Le menu de configuration MBA apparaît (voir Boot Agent de Broadcom).
3. Dans le menu de configuration MBA, utilisez les flèches de direction **HAUT** et **BAS** pour sélectionner l'option **Protocole d'amorçage**. Utiliser les flèches de direction **GAUCHE** et **DROITE** pour changer l'option **Protocole d'amorçage** par **iSCSI**.

Remarque : Pour les plates-formes sur lesquelles le protocole d'amorçage est défini via le BIOS, consultez la documentation système pour plus d'informations.

4. Sélectionnez **Configuration de l'initialisation iSCSI** dans le **menu principal**.

Remarque : Si le microprogramme d'initialisation iSCSI n'est pas programmé dans la carte réseau NetXtreme, la sélection de **Configuration de l'initialisation iSCSI** n'a aucun effet.

Configuration du démarrage iSCSI

- Configuration de l'initialisation iSCSI statique
- Configuration de l'initialisation iSCSI dynamique

Configuration de l'initialisation iSCSI statique

Dans le cadre d'une configuration statique, vous devez indiquer l'adresse IP du système, le nom IQN de l'initiateur du système et les paramètres cibles obtenus dans Configuration de la cible iSCSI. Pour plus d'informations sur la configuration des options, reportez-vous au Tableau 15.

Pour configurer les paramètres d'initialisation iSCSI par le biais d'une configuration statique

1. Dans l'écran **Menu des paramètres généraux**, définissez les éléments suivants :
   - **TCP/IP parameters via DHCP** (Paramètres TCP/IP via DHCP) : Désactivé. (Pour IPv4.)
   - **IP Autoconfiguration** (Configuration auto de l'IP) : Désactivé. (Pour IPv6)
   - **iSCSI parameters via DHCP** (Paramètres iSCSI via DHCP) : Désactivé.
   - **CHAP Authentication** (Authentification CHAP) : Désactivé.
   - **Boot to iSCSI target** (Initialisation sur la cible iSCSI) : Désactivé.

- **DHCP Vendor ID** (ID du fournisseur DHCP) :BRCM ISAN
- **Link Up Delay Time** (Délai de liaison active) : 0
- **Use TCP Timestamp** (Utiliser l'horodateur TCP) : Activé (pour certaines cibles telles que Dell/EMC AX100i, il est nécessaire d'activer **Use TCP Timestamp**(Utiliser l'horodateur TCP))
- **Target as First HDD** (Cibler comme premier lecteur de disque dur) : Désactivé.
- **LUN Busy Retry Count** (Nombre de tentatives si le numéro d'unité logique est occupé) : 0
- **IP Version** (Version IP) : IPv6. (Pour IPv6)

2. Appuyez sur **ECHAP** pour revenir au menu **principal**.
3. Dans le menu **principal**, sélectionnez **Paramètres de l'initiateur**.
4. Dans l'écran **Paramètres de l'initiateur**, entrez des valeurs pour les éléments suivants :
   - Adresse IP (les adresses IPv4 et IPv6 non spécifiées doivent être « 0.0.0.0 » et « :: », respectivement**)**
   - Préfixe de masque de sous-réseau
   - Passerelle par défaut
   - DNS principal
   - DNS secondaire
   - Nom iSCSI (correspond au nom de l'initiateur iSCSI devant être utilisé par le système client)

Remarque : Entrez soigneusement l'adresse IP. L'adresse IP ne fait l'objet d'aucune vérification en matière de duplication ou de segment/d'attribution réseau incorrects.

5. Appuyez sur **ECHAP** pour revenir au menu **principal**.
6. Dans le menu **principal**, sélectionnez **1st Target Parameters** (Paramètres de la 1ère cible).
7. Dans l'écran **1st Target Parameters** (Paramètres de la 1ère cible), activez **Connexion** pour vous connecter à la cible iSCSI. Pour les éléments suivants, entrez les valeurs utilisées lors de la configuration de la cible iSCSI :
   - Adresse IP
   - Port TCP
   - Numéro d'unité logique d'initialisation
   - Nom iSCSI
8. Appuyez sur **ECHAP** pour revenir au menu **principal**.
9. Appuyez sur **ECHAP** et sélectionnez **Exit and Save Configuration** (Quitter et enregistrer la configuration).
10. Appuyez sur **F4** pour enregistrer votre configuration MBA.

Configuration de l'initialisation iSCSI dynamique

Dans le cadre d'une configuration dynamique, il vous suffit uniquement de spécifier que l'adresse IP et les informations concernant la cible ou l'initiateur du système sont fournies par un serveur DHCP (voir les configurations IPv4 et IPv6 dans Configuration du serveur DHCP pour la prise en charge de l'initialisation iSCSI). Pour IPv4, à l'exception du nom iSCSI de l'initiateur, tous les paramètres des écrans Paramètres de l'initiateur, Paramètres de la 1re cible ou Paramètres de la 2e cible sont ignorés et il n'est pas nécessaire de les effacer. Pour IPv6, à l'exception de la réf. et de la clé secrète CHAP, tous les paramètres des écrans Initiator Parameters (Paramètres de l'initiateur), 1st Target Parameters (Paramètres de la 1re cible) ou 2nd Target Parameters (Paramètres de la 2e cible) sont ignorés et il n'est pas nécessaire de les effacer. Pour plus d'informations sur la configuration des options, reportez-vous au Tableau 15.

Remarque :

- Lors de l'utilisation d'un serveur DHCP, les entrées du serveur DNS sont écrasées par les valeurs provenant du serveur DHCP. Ce problème se pose même si les valeurs fournies localement sont valides et si le serveur DHCP ne transmet aucune information concernant le serveur DNS. Lorsque le serveur DHCP ne transmet aucune information concernant le serveur DNS, les valeurs des serveurs DNS principal et secondaire sont définies à 0.0.0.0. Lorsque le système d'exploitation Windows prend le contrôle, l'initiateur iSCSI Microsoft récupère les paramètres de l'initiateur iSCSI et configure les registres appropriés de manière statique. Il écrase alors tout élément configuré. Etant donné que le daemon DHCP s'exécute dans l'environnement Windows en tant que processus utilisateur, tous les paramètres TCP/IP doivent être configurés de manière statique avant que la pile apparaisse dans l'environnement d'initialisation iSCSI.
- Si l'Option DHCP 17 est utilisée, les informations sur la cible sont fournies par le serveur DHCP et le nom iSCSI de l'initiateur est récupéré à partir de la valeur programmée dans l'écran Initiator Parameters (Paramètres de l'initiateur). Si aucune valeur n'a été sélectionnée, le contrôleur utilise le nom par défaut :

```
iqn.1995-05.com.broadcom.<11.22.33.44.55.66>.iscsiboot
```

dans lequel la chaîne `11.22.33.44.55.66` correspond à l'adresse MAC du contrôleur.

Si l'Option DHCP 43 (IPv4 uniquement) est utilisée, tous les paramètres des écrans Initiator Parameters (Paramètres de l'initiateur), 1st Target Parameters (Paramètres de la 1re cible) ou 2nd Target Parameters (Paramètres de la 2e cible) sont ignorés et il n'est pas nécessaire de les effacer.

Pour configurer les paramètres d'initialisation iSCSI par le biais d'une configuration dynamique

1. Dans l'écran **Menu des paramètres généraux**, définissez les éléments suivants :
   - **TCP/IP parameters via DHCP** (Paramètres TCP/IP via DHCP) : Activé. (Pour IPv4.)
   - **IP Autoconfiguration** (Configuration auto de l'IP) : Activé. (Pour IPv6)
   - **iSCSI parameters via DHCP** (Paramètres iSCSI via DHCP) : Activé.
   - **CHAP Authentication** (Authentification CHAP) : Désactivé.
   - **Boot to iSCSI target** (Initialisation sur la cible iSCSI) : Désactivé.
   - **DHCP Vendor ID** (ID du fournisseur DHCP) :BRCM ISAN
   - **Link Up Delay Time** (Délai de liaison active) : 0
   - **Use TCP Timestamp** (Utiliser l'horodateur TCP) : Activé (pour certaines cibles telles que **Dell/EMC AX100i, il est nécessaire d'activer** Use TCP Timestamp (Utiliser l'horodateur TCP))
   - **Target as First HDD** (Cibler comme premier lecteur de disque dur) : Désactivé.
   - **LUN Busy Retry Count** (Nombre de tentatives si le numéro d'unité logique est occupé) : 0
   - **IP Version** (Version IP) : IPv6. (Pour IPv6)
2. Appuyez sur **ECHAP** pour revenir au menu **principal**.

Remarque : Les informations des écrans **Initiator Parameters** (Paramètres de l'initiateur) et **1st Target Parameters** (Paramètres de la 1ère cible) sont ignorées et il n'est pas nécessaire de les effacer.

3. Sélectionner **Exit and Save Configurations** (Quitter et enregistrer la configuration).

Activation de l'authentification CHAP

Assurez-vous que l'authentification CHAP est activée sur la cible.

Activer l'authentification CHAP

1. Dans l'écran **Paramètres généraux**, définissez **Authentification CHAP** sur Activé.
2. Dans l'écran **Paramètres de l'initiateur**, entrez des valeurs pour les éléments suivants :
   - Réf. CHAP (jusqu'à 128 octets)
   - Clé secrète CHAP (si l'authentification est nécessaire ; doit contenir au minimum 12 caractères)
3. Appuyez sur **ECHAP** pour revenir au menu **principal**.
4. Dans le menu **principal**, sélectionnez **1st Target Parameters** (Paramètres de la 1ère cible).
5. Dans l'écran **1st Target Parameters** (Paramètres de la 1ère cible), entrez les valeurs utilisées lors de la configuration de la cible iSCSI pour les éléments suivants :
   - Réf. CHAP (facultatif si CHAP bidirectionnel)
   - Clé secrète CHAP (facultatif si CHAP bidirectionnel ; doit contenir au minimum 12 caractères)
6. Appuyez sur **ECHAP** pour revenir au menu **principal**.
7. Appuyez sur **ECHAP** et sélectionnez **Exit and Save Configuration** (Quitter et enregistrer la configuration).

Configuration du serveur DHCP pour la prise en charge de l'initialisation iSCSI

Le serveur DHCP est un composant facultatif. Il est nécessaire uniquement si vous effectuez une configuration dynamique de l'initialisation iSCSI (voir Configuration de l'initialisation iSCSI dynamique).

La configuration du serveur DHCP pour la prise en charge de l'initialisation iSCSI est différente pour IPv4 et IPv6.

- Configuration DHCP pour l'initialisation iSCSI pour IPv4
- Configuration DHCP pour l'initialisation iSCSI pour IPv6

Configuration DHCP pour l'initialisation iSCSI pour IPv4

Le protocole DHCP englobe plusieurs options apportant des informations de configuration au client DHCP. Pour une initialisation iSCSI, les cartes Broadcom prennent en charge les configurations DHCP suivantes :

- Option DHCP 17, chemin d'accès
- Option DHCP 43, informations concernant le fournisseur

Option DHCP 17, chemin d'accès

L'option 17 permet de transmettre les informations concernant la cible iSCSI au client iSCSI.

Le format du chemin d'accès défini dans IETC RFC 4173 se présente de la manière suivante :

```
"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
```

Les paramètres sont définis ci-dessous.

Tableau 16 : Définition des paramètres de l'Option DHCP 17

Paramètre	*Définition*
`"iscsi:"`	Une chaîne littérale
`<servername>`	L'adresse IP ou le nom de domaine complet de la cible iSCSI
`":"`	Séparateur
`<protocol>`	Le protocole IP permettant d'accéder à la cible iSCSI. Seul TCP étant pris en charge actuellement, le protocole est 6.
`<port>`	Le numéro de port associé au protocole. Le numéro de port standard pour iSCSI est 3260.
`<LUN>`	Numéro d'unité logique à utiliser sur la cible iSCSI. La valeur du LUN doit être représentée à l'aide de caractères hexadécimaux. Un LUN dont l'identifiant est 64 doit être défini sur 40, dans l'option 17 du serveur DHCP.
`<targetname>`	Le nom de la cible au format IQN ou EUI (voir RFC 3720 pour des détails sur les formats IQN et EUI). Exemple de nom IQN : « iqn.1995-05.com.broadcom:iscsi-target ».

Option DHCP 43, informations concernant le fournisseur

L'Option DHCP 43 (informations concernant le fournisseur) offre davantage d'options de configuration au client iSCSI que l'Option DHCP 17. Dans le cadre de cette configuration, trois sous-options supplémentaires permettent d'attribuer le nom IQN de l'initiateur au client d'initialisation iSCSI, ainsi que deux noms IQN de cible iSCSI pouvant être utilisés pour l'initialisation. Le format du nom IQN de la cible iSCSI est identique à celui de l'Option DHCP 17, tandis que le nom IQN de l'initiateur iSCSI est tout simplement le nom IQN de l'initiateur.

Remarque : L'Option DHCP 43 est uniquement prise en charge pour IPv4.

Les sous-options sont définies ci-dessous.

Tableau 17 : Définition des sous-options de l'Option DHCP 43

Sous-option	*Définition*
201	Informations sur la première cible iSCSI sous la forme du chemin d'accès standard `"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Informations sur la deuxième cible iSCSI sous la forme du chemin d'accès standard `"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	Nom IQN de l'initiateur iSCSI

L'Option DHCP 43 requiert une configuration plus importante que l'Option DHCP 17, mais elle offre un environnement plus riche et comporte davantage d'options de configuration. Broadcom recommande à ses clients d'utiliser l'Option DHCP 43 lors de la réalisation de configurations dynamiques de l'initialisation iSCSI.

Configuration du serveur DHCP

Configurez le serveur DHCP de sorte qu'il prenne en charge l'option 17 ou l'option 43.

Remarque : Si vous utilisez l'option 43, vous devez également configurer l'option 60. La valeur de l'option 60 doit correspondre à celle de l'**ID du fournisseur DHCP**. La valeur de la **Réf. fournisseur DHCP** est BRCM ISAN, comme indiqué dans les **Paramètres généraux** du menu de configuration de l'initialisation iSCSI.

Configuration DHCP pour l'initialisation iSCSI pour IPv6

Le serveur DHCPv6 peut fournir plusieurs options, y compris la configuration IP sans état ou avec état, ainsi que des informations au client DHCPv6. Pour une initialisation iSCSI, les cartes Broadcom prennent en charge les configurations DHCP suivantes :

- Option DHCPv6 16, option de classe fournisseur
- Option DHCPv6 17, informations concernant le fournisseur

Remarque : L'option de chemin d'accès standard de DHCPv6 n'est pas encore disponible. Broadcom suggère d'utiliser l'option 16 ou 17 pour la prise en charge dynamique de IPv6 pour l'initialisation iSCSI.

Option DHCPv6 16, option de classe fournisseur

L'Option DHCPv6 16 (option de classe fournisseur) doit être présente et contenir une chaîne correspondant au paramètre configuré pour la **Réf. fournisseur DHCP**. La valeur de la **Réf. fournisseur DHCP** est BRCM ISAN, comme indiqué dans les **Paramètres généraux** du menu de configuration de l'initialisation iSCSI.

Le contenu de l'option 16 doit être <longueur de 2 octets> <Réf. fournisseur DHCP>.

Option DHCPv6 17, informations concernant le fournisseur

L'Option DHCPv6 17 (informations concernant le fournisseur) fournit d'autres options de configuration au client iSCSI. Dans le cadre de cette configuration, trois sous-options supplémentaires permettent d'attribuer le nom IQN de l'initiateur au client d'initialisation iSCSI, ainsi que deux noms IQN de cible iSCSI pouvant être utilisés pour l'initialisation.

Les sous-options sont définies ci-dessous.

Tableau 18 : Définition des sous-options de l'Option DHCP 17

Sous-option	*Définition*
201	Informations sur la première cible iSCSI sous la forme du chemin d'accès standard `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Informations sur la deuxième cible iSCSI sous la forme du chemin d'accès standard `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	Nom IQN de l'initiateur iSCSI

Remarque : Dans le Tableau 18, les crochets [ ] sont requis pour les adresses IPv6.

Le contenu de l'option 17 doit être <numéro d'option de 2 octets 201|202|203> <longueur de 2 octets> <données>.

Configuration du serveur DHCP

Configurez le serveur DHCP de sorte qu'il prenne en charge l'option 16 et l'option 17.

Remarque : Le format de l'Option DHCPv6 16 et de l'Option DHCPv6 17 est entièrement défini dans RFC 3315.

Préparation de l'image de démarrage iSCSI

Configuration du démarrage de Windows Server 2008 R2 et iSCSI SP2

Windows Server 2008 R2 et Windows Server 2008 SP2 prennent en charge l'initialisation iSCSI. La procédure suivante fait référence à Windows Server 2008 R2 mais est commune à Windows Server 2008 R2 et SP2.

Image CD/ISO requise :

- Windows Server 2008 R2 x64 avec les pilotes Broadcom injectés. Reportez-vous également à la rubrique KB974072 de la base de connaissances Microsoft à l'adresse support.microsoft.com.

Remarque : Reportez-vous au fichier *silent.txt* pour l'application du programme d'installation du pilote spécifique, afin d'obtenir des instructions sur l'extraction individuelle des pilotes Windows NetXtreme.

Autres logiciels nécessaires :

- Bindview.exe (Windows Server 2008 R2 uniquement ; voir KB976042)

Procédure :

1. Supprimez tous les lecteurs locaux du système à démarrer (le « système distant »).
2. Chargez les images de l'initialisation iSCSI et MBA Broadcom les plus récentes dans la NVRAM de la carte.
3. Configurez le BIOS du système distant de sorte à désigner le MBA Broadcom comme premier périphérique amorçable et le DVD-ROM comme second.
4. Configurez la cible iSCSI de sorte à autoriser une connexion depuis le périphérique distant. Assurez-vous que l'espace disque soit suffisant sur la cible pour contenir l'installation du nouveau système d'exploitation.
5. Démarrez le système distant. Quand la bannière PXE (Preboot Execution Environment) apparaît, appuyez sur **Ctrl+S** pour entrer dans le menu de PXE.
6. Dans le menu PXE, définissez le **Protocole de démarrage** sur **iSCSI**.
7. Entrez les paramètres de la cible iSCSI.
8. Dans Paramètres généraux, définissez le paramètre **Démarrer depuis la cible** sur **Désactivé une fois.**
9. Enregistrez les paramètres et redémarrez le système.

   Le système distant devrait se connecter à la cible iSCSI puis démarrer depuis le périphérique DVDROM.
10. Démarrez depuis le DVD et commencez l'installation.
11. Répondez correctement à toutes les questions de l'installation (désignez le système d'exploitation que vous souhaitez installer, acceptez les conditions d'utilisation de la licence, etc.).

    Dans la fenêtre **Où** souhaitez-vous installer Windows ?, le lecteur cible doit être visible. Il s'agit d'un lecteur connecté via le protocole de démarrage iSCSI, situé dans la cible iSCSI distante.
12. Sélectionnez **Suivant** pour passer à l'installation de Windows Server 2008 R2.

    Quelques minutes après le démarrage de la procédure d'installation de Windows Server 2008 R2 sur DVD, un redémarrage système a lieu. Après le redémarrage, la routine d'installation de Windows Server 2008 R2 devrait reprendre jusqu'à la finalisation de cette étape.
13. Après un nouveau redémarrage système, vérifiez que le système distant est capable de démarrer depuis l'ordinateur.

14. Après le démarrage de Windows Server 2008 R2, chargez le pilote et exécutez Bindview.exe.
    a. Sélectionnez **Tous les services**.
    b. Dans **Filtre léger WFP**, vous devez voir **Chemin de liaison** pour l'AUT. Cliquez avec le bouton droit et désactivez-les. Ensuite, fermez l'application.
15. Vérifiez que le SE et le système sont fonctionnels et en mesure de passer le trafic en envoyant une commande ping à une adresse IP du système distant, etc.

Configuration du démarrage iSCSI sous Windows Server 2012

Windows Server 2012 prend en charge l'initialisation et l'installation iSCSI. Broadcom nécessite l'utilisation d'un DVD intégré avec les pilotes Broadcom injectés les plus récents. Reportez-vous à la rubrique KB974072 de la base de connaissances Microsoft à l'adresse support.microsoft.com.

Remarque : Reportez-vous au fichier *silent.txt* pour l'application du programme d'installation du pilote spécifique, afin d'obtenir des instructions sur l'extraction individuelle des pilotes Windows NetXtreme.

La procédure suivante permet de préparer l'image pour l'installation et l'initialisation :

1. Supprimez tous les lecteurs locaux du système à démarrer (le « système distant »).
2. Chargez les images de l'initialisation iSCSI et MBA Broadcom les plus récentes dans la NVRAM de la carte.
3. Configurez le BIOS du système distant de sorte à désigner le MBA Broadcom comme premier périphérique amorçable et le DVD-ROM comme second.
4. Configurez la cible iSCSI de sorte à autoriser une connexion depuis le périphérique distant. Assurez-vous que l'espace disque soit suffisant sur la cible pour contenir l'installation du nouveau système d'exploitation.
5. Démarrez le système distant. Quand la bannière PXE (Preboot Execution Environment) apparaît, appuyez sur **Ctrl+S** pour entrer dans le menu de PXE.
6. Dans le menu PXE, définissez le **Protocole de démarrage** sur **iSCSI**.
7. Entrez les paramètres de la cible iSCSI.
8. Dans Paramètres généraux, définissez le paramètre **Démarrer depuis la cible** sur **Désactivé une fois**.
9. Enregistrez les paramètres et redémarrez le système.

   Le système distant devrait se connecter à la cible iSCSI puis démarrer depuis le périphérique DVDROM.
10. Démarrez depuis le DVD et commencez l'installation.
11. Répondez correctement à toutes les questions de l'installation (désignez le système d'exploitation que vous souhaitez installer, acceptez les conditions d'utilisation de la licence, etc.).

    Dans la fenêtre **Où** souhaitez-vous installer Windows ?, le lecteur cible doit être visible. Il s'agit d'un lecteur connecté via le protocole de démarrage iSCSI, situé dans la cible iSCSI distante.
12. Sélectionnez **Suivant** pour passer à l'installation de Windows 2012.

    Quelques minutes après le démarrage de la procédure d'installation de Windows 2012 sur DVD, un redémarrage système a lieu. Après le redémarrage, la routine d'installation de Windows 2012 devrait reprendre et terminer l'installation.
13. Après un nouveau redémarrage système, vérifiez que le système distant est capable de démarrer depuis l'ordinateur.
14. Après le démarrage de Windows 2012 comme SE, Broadcom recommande d'exécuter le programme d'installation du pilote pour finaliser l'installation des pilotes Broadcom et de l'application.

Configuration de l'initialisation iSCSI sous Linux

L’initialisation iSCSI sous Linux est prise en charge sur Red Hat Enterprise Linux 5.5 et version ultérieure et sur SUSE Linux Enterprise Server 11 SP1 et version ultérieure. Notez queSLES 10.x et SLES 11 prennent uniquement en charge le chemin sans déchargement.

1. Pour une mise à jour du pilote, procurez-vous le dernier CD de pilotes Linux Broadcom.
2. Configurez les paramètres de démarrage iSCSI pour l'installation directe depuis un DVD sur la cible en désactivant l'option Démarrer à partir de la cible sur la carte réseau.
3. Modifiez l'ordre de démarrage comme suit :
   a. Démarrez depuis la carte réseau.
   b. Démarrez depuis le lecteur CD/DVD.
4. Redémarrez le système.
5. Le système se connecte à la cible iSCSI, puis démarre depuis le lecteur CD/DVD.
6. Suivez les instructions correspondant au SE.
   a. RHEL 5.5 - Saisissez « linux dd » sur l'invite « boot: », puis appuyez sur Entrée
   b. SuSE 11.X - Choisissez **installation** et saisissez **withiscsi=1 netsetup=1** dans l'option de démarrage. Si le pilote doit être mis à jour, choisissez **OUI** pour l'option du pilote F6.
7. Si le pilote doit être mis à jour, suivez les instructions pour charger le CD de pilotes ; sinon, passez cette étape.
8. A l'invite « périphérique de mise en réseau », choisissez le port de la carte réseau désiré et appuyez sur **OK**.
9. A l'invite « configurer TCP/IP », configurez la manière dont le système acquiert l'adresse IP et appuyez sur **OK**.
10. Si c'est l'adresse IP statique qui a été choisie, vous devez entrer les informations IP de l'initiateur iscsi.
11. (RHEL) Choisissez d'ignorer le test des supports.
12. Continuez l'installation comme souhaité. A ce stade, un lecteur sera disponible. Après la fin de la copie des fichiers, retirez le CD/DVD et redémarrez le système.
13. Lorsque le système redémarre, activez « démarrer depuis la cible » dans Paramètres de démarrage iSCSI et poursuivez l'installation jusqu'à la fin.

A ce stade, la phase d'installation initiale est terminée. Le reste de la procédure s'applique pour créer une nouvelle image initrd personnalisée pour toute nouvelle mise à jour des composants :

14. Mettez à jour l'initiateur iscsi si nécessaire. Vous devez tout d'abord supprimer l'initiateur existant à l'aide de la commande **rpm -e**.
15. Assurez-vous que tous les Runlevels du service réseau sont activés :
    `chkconfig network on`
16. Assurez-vous que les Runlevels 2, 3 et 5 du service iscsi sont activés.
    `chkconfig -level 235 iscsi on`
17. Pour Red Hat 6.0, assurez-vous que le service Gestionnaire de réseau est arrêté et désactivé.
18. Installez iscsiuio si vous le souhaitez (non requis pour SuSE 10).
19. Installez le progiciel linux-nx2 si vous le souhaitez.
20. Installez le progiciel bibt.
21. Supprimez ifcfg-eth*.
22. Redémarrez.
23. Pour SUSE 11.1, suivez la solution d'installation à distance sur DVD illustrée ci-dessous.

24. Après le redémarrage du système, connectez-vous, passez au dossier /opt/bcm/bibt et exécutez le script iscsi_setup.sh pour créer les image initrd.

25. Copiez l’image initrd dans le dossier /boot.

26. Modifiez le menu grub pour qu'il pointe vers la nouvelle image initrd.

27. Vous devez modifier le fichier de configuration iscsid.conf pour pouvoir activer CHAP (Red Hat uniquement).

28. Redémarrez et modifiez les paramètres CHAP si désiré.

29. Continuez à démarrer dans l'image de l'initialisation iSCSI et choisissez l'image créée.

30. Pour IPv6, vous pouvez maintenant modifier l'adresse IP pour l'initiateur et la cible par l'adresse IPv6 de votre choix dans la NVRAM configuration.

Redémarrage

Une fois que le système est prêt pour une initialisation iSCSI et que le système d'exploitation se trouve sur la cible iSCSI, la dernière étape consiste à effectuer le démarrage lui-même. Le système démarrera Windows ou Linux sur le réseau et fonctionnera comme un lecteur de disque local.

1. Réinitialisez le serveur.

2. Sélectionnez **CTRL+S**.

3. Dans le menu **principal**, sélectionnez **Paramètres généraux** et définissez l'option **Démarrer depuis la cible iSCSI** sur **Activé**.

Si l'authentification CHAP est nécessaire, assurez-vous que le démarrage s'est effectué correctement avant de l'activer (voir Activation de l'authentification CHAP).

Autres facteurs d'initialisation iSCSI à prendre en compte

Il existe plusieurs autres facteurs devant être pris en compte lors de la configuration d'un système pour l'initialisation iSCSI.

Modification des paramètres Vitesse et Duplex dans les environnements Windows.

L'initialisation au moyen du chemin NDIS est prise en charge. Les paramètres Vitesse et Duplex peuvent être modifiés à l'aide de l'utilitaire de gestion BACS pour l'initialisation iSCI via le chemin NDIS.

Adresse administrée localement

Une adresse MAC définie par l'utilisateur attribuée par le biais de la propriété Adresse administrée localement de la section Avancé de l'onglet Configurations BACS n'est pas prise en charge par les périphériques compatibles avec l'initialisation iSCSI.

Réseaux locaux virtuels (VLAN)

L'identification VLAN n'est pas prise en charge pour l'initialisation iSCSI avec l'initiateur logiciel iSCSI Microsoft.

Dépannage de l'initialisation iSCSI

Les conseils de dépannage suivants peuvent s'avérer utiles pour l'initialisation iSCSI.

Problème : L'utilitaire iSCSI de vidage de la mémoire Broadcom ne capture pas correctement un vidage de la mémoire lorsque la vitesse de liaison de l'initialisation iSCSI est configurée pour 10 Mbit/s ou 100 Mbit/s.
Solution : L'utilitaire iSCI de vidage de la mémoire est pris en charge lorsque la vitesse de liaison de l'initialisation iSCSI est configurée pour 1 Gbit/s. Les valeurs 10 Mbit/s et 100 Mbit/s ne sont pas prises en charge.

Problème : Une cible iSCSI n'est pas reconnue en tant que cible d'installation lorsque vous essayez d'installer Windows Server 2008 en utilisant une connexion IPv6.
Solution : Il s'agit d'un problème connu de tierce partie. Consultez l'article 971443 de la base de connaissances Microsoft à l'adresse http://support.microsoft.com/kb/971443.

Problème : L'utilitaire de configuration iSCSI ne s'exécute pas.
Solution : Assurez-vous que le microprogramme de démarrage iSCSI est installé dans la NVRAM.

Problème : Après avoir configuré la LUN de démarrage iSCSI sur la valeur 255, un écran système bleu apparaît lors du démarrage iSCSI.
Solution : Bien que la solution iSCSI de Broadcom prenne en charge une plage de LUN comprise entre 0 et 255, l'initiateur logiciel iSCSI Microsoft ne prend pas en charge une LUN de 255. Pour y remédier, configurez une valeur de numéro d'unité logique comprise entre 0 et 254.

Problème : Impossible de mettre à jour un pilote intégré en l'absence d'ID matériel non intégré.
Solution : Créez une image DVD intégrée personnalisée avec des pilotes pris en charge présents sur le support d'installation.

Vidage sur incident iSCSI

Si vous utilisez l'utilitaire Broadcom iSCSI Crash Dump, il est essentiel de suivre la procédure d'installation du pilote iSCSI Crash Dump. Pour plus d'informations, voir Utilisation du programme d'installation.

Section 10 : Installation de l'application de gestion et du pilote Linux

Présentation

Le pilote Linux TG3 est fourni dans les formats de présentation (noms de fichier) suivants :

- RPM source (tg3-*version*.3dkms.src.rpm)
- RPM source (tg3-*version*.3dkms.noarch.rpm)
- Complémentaire (tg3_sup-*version*.tar.gz)
- Tar comprimé (tg3-*version*.tar.gz)

Des fichiers source identiques permettant de créer le pilote sont inclus dans les deux progiciels source RMP et TAR. Le fichier tar contient d'autres utilitaires, tels que des correctifs et des images de disquette pilote pour l'installation réseau.

Installation du logiciel pilote TG3

Installation du progiciel RPM source

Conditions préalables :

- Source du noyau Linux
- Compilateur C

Procédure :

1. Installez le progiciel RPM source.
   `rpm -ivh tg3-version.src.rpm`
2. Faites pointer le répertoire sur le chemin du RPM et construisez le pilote binaire pour le noyau (le chemin RPM varie en fonction des distributions Linux).
   ```
   cd /usr/src/redhat,OpenLinux,turbo,packages,rpm …
   rpm -bb SPECS/tg3.spec or rpmbuild -bb SPECS/tg3.spec
   rpmbuild -bb SPECS/tg3.spec (for RPM version 4.x.x)
   ```

   Remarque : Il se peut que le message suivant s'affiche lors de la tentative d'installation du progiciel RPM source :

   ```
   error: cannot create %sourcedir /usr/src/redhat/SOURCE
   ```

   La cause la plus probable de l'erreur est que le progiciel rpm-build n'a pas été installé. Recherchez le progiciel rpm-build sur le support d'installation Linux et installez-le à l'aide de la commande suivante :

   ```
   rpm -ivh rpm-build-version.i386.rpm
   ```

   Effectuez l'installation du logiciel RPM source.
3. Installez le progiciel que vous venez de construire (pilote et man page).
   `rpm -ivh RPMS/i386/tg3-version.i386.rpm`

   En fonction du noyau, le pilote est installé dans le chemin suivant :

   Noyaux 2.6.x :

   /lib/modules/*version_noyau*/kernel/drivers/net/tg3.ko
4. Chargez le pilote.
   ```
   modprobe tg3
   ```

Pour configurer le protocole et l'adresse réseau, consultez la documentation de la version appropriée de Linux.

Création du pilote à partir du fichier TAR source

1. Créez un répertoire (tg3-*version*) et extrayez les fichiers TAR dans ce répertoire.
   `tar xvzf tg3-version.tgz`
2. Construisez le pilote tg3.o sous forme de module chargeable pour le noyau d'exécution.
   `CD tg3-version`
   `make clean`
   `make; make install`
3. Testez le pilote en le chargeant.
   `rmmod tg3`
   `modprobe tg3`

   Aucun message n'est renvoyé si cette commande est exécutée correctement.

Remarque : voir les instructions RPM ci-dessus pour obtenir l'emplacement du pilote installé.

4. Pour configurer le protocole et l'adresse réseau, reportez-vous à la documentation fournie avec votre système d'exploitation.

Installations réseau

Pour les installations réseau via NFS, FTP ou HTTP (à l'aide d'une disquette d'amorçage réseau ou de PXE), utilisez le pilote tg3 qui fait partie de la distribution du système d'exploitation Linux.

Désinstallation et suppression du pilote TG3

Désinstallation et suppression du pilote provenant d'une installation RPM

Pour désinstaller le pilote, utilisez **ifconfig** pour fermer toutes les interfaces *ethX* ouvertes par le pilote, puis saisissez :

```
rmmod tg3
```

Si le pilote a été installé à l'aide de **rpm**, procédez ainsi pour le supprimer :

```
rpm -e tg3-<version>
```

Suppression du pilote provenant d'une installation TAR

Si le pilote a été installé à l'aide de make install à partir du fichier tar, le pilote tg3.o doit être supprimé manuellement du système d'exploitation. Voir Installation du progiciel RPM source pour connaître l'emplacement du pilote installé.

Si une interface de configuration est associée au pilote tg3, fermez d'abord cette interface en utilisant **ifconfig ethx down** puis **rmmod tg3**.

Messages du pilote

Vous trouverez ci-dessous des exemples de messages courants qui sont susceptibles d'être consignés dans le fichier */var/log/messages*. Utilisez **dmesg -n***level* pour contrôler le niveau auquel les messages apparaîtront sur la console. Pour la plupart, les systèmes sont réglés par défaut sur le niveau 6.

Ouverture de session du pilote

```
tg3.c:version (date)
```

NIC détecté

```
eth#: Tigon3 [partno (BCM95xxx) rev 4202 PHY (57xx) (PCI Express) 10/100/1000BaseT Ethernet
:00:xx:xx:xx:xx:xx
eth#: RXcsums [1] LinkChg REG [0] MIirq [0] ASF [0] Split [0] Wirespeed [1]TSOcap [1]
eth#: dma_rwctrl [76180000]
ACPI : PCI interrupt 0000:02:02.0 [A] -> GSI 26 (level,low) -> IRQ 233
```

Contrôle de flux :

```
tg3: eth#: Flow control is configured for TX and for RX.
```

Indication de liaison active et de vitesse

```
tg3: eth#: Link is up at 1000 Mbps, full duplex.
```

Indication de liaison inactive

```
tg3: eth#: Link is down.
```

Regroupement avec agrégation de canaux

Le pilote TG3 vous permet de regrouper des cartes à l'aide du module de noyau d'agrégation et d'une interface d'agrégation de canaux. Consultez votre documentation Linux pour plus d'informations sur la fonction d'agrégation de canaux de Linux.

Installation de l'application de gestion pour Linux

Présentation

Broadcom Advanced Control Suite version 4 (BACS4) est une application de gestion pour la configuration de la famille de cartes NetXtreme I. Le logiciel BACS4 fonctionne sur les systèmes d'exploitation de serveur et de client Windows et Linux.

Ce chapitre aborde l'installation de l'application de gestion BACS4 sur des systèmes Linux. Pour les systèmes Windows, un programme d'installation est fourni pour installer les pilotes Windows et les applications de gestion, y compris BACS4 (voir Installation de l'application de gestion et du pilote Windows pour connaître la procédure à suivre).

Il existe deux principaux composants de l'utilitaire BACS4 : le composant fournisseur et le logiciel du client. Un fournisseur est installé sur un serveur (ou « hôte géré ») contenant une ou plusieurs cartes réseau. Le fournisseur recueille des informations sur les cartes réseau et les rend disponibles pour la récupération depuis un ordinateur de gestion sur lequel le logiciel client est installé. Le logiciel client permet d'afficher les informations des fournisseurs et de configurer les cartes réseau. Le logiciel client BACS comprend une interface graphique et une interface de ligne de commande (CLI).

Protocoles de communication

Un protocole de communication permet l'échange d'informations entre le fournisseur et le logiciel client. Il s'agit d'implémentations propriétaires ou open-source des normes WBEM (Web-Based Enterprise Management) et CIM (Common Information Model) de la DMTF (Distributed Management Task Force). Les administrateurs réseau peuvent choisir l'option qui leur convient le mieux en fonction de la norme prévalant sur leur réseau.

Le tableau suivant indique les options disponibles suivant les systèmes d'exploitation installés sur l'hôte géré et le client.

Si le client utilise :	***Et l'hôte géré utilise :***	***BACS peut utiliser ces protocoles de communication :***
Windows	Windows	WMI WS-MAN (WinRM)
Windows	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)
Linux	Windows	WS-MAN (WinRM)
Linux	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)

Si le client utilise :	*Et l'hôte géré utilise :*	*BACS peut utiliser ces protocoles de communication :*
• WMI = Windows Management Instrumentation. • WS-MAN = Web Service-Management. WinRM est une implémentation Windows et OpenPegasus est une implémentation open-source qui fonctionne sous Linux. • CIM-XML = version XML d'OpenPegasus.		

Si votre réseau inclut une combinaison de clients Windows et Linux qui accèdent à des serveurs Windows et Linux, alors WS-MAN est un choix adapté. Si Linux est le seul système d'exploitation installé sur les serveurs, alors le choix du CIM-XML est envisageable. Si le réseau inclut uniquement des serveurs et des clients Windows, WMI est un choix envisageable. WMI est très simple à configurer mais n'est pris en charge que sur le système d'exploitation Windows. (voir Installation de l'application de gestion et du pilote Windows pour connaître la procédure d'installation et de configuration des protocoles Windows.)

L'installation de BACS couvre l'installation du composant fournisseur sur l'hôte géré et le logiciel client sur la station de gestion. Le processus d'installation varie suivant la combinaison des systèmes d'exploitation installés sur le client et l'hôte géré et le protocole de communication sélectionné.

Installation de WS-MAN ou de CIM-XML sur un serveur Linux

Etape 1 : Installer OpenPegasus

Sur le système d'exploitation Red Hat de Linux, deux options d'installation sont disponibles :

- A partir du RPM intégré (Red Hat uniquement)
- A partir de la source (Red Hat et SuSE)

Sur le système d'exploitation SUSE Linux Enterprise Server 11 (SLES11), vous devez utiliser le RPM source.

Remarque : Le RPM intégré ne prend pas en charge le protocole de communication WS-MAN. Pour utiliser WS-MAN, vous devez installer OpenPegasus à partir de la source.

A partir du RPM intégré (Red Hat uniquement)

Sous Red Hat de Linux, un RPM intégré OpenPegasus est disponibile sous `tog-pegasus-<version>.<arch>.rpm`.

1. Pour installer tog-pegasus, utilisez la commande suivante :
   `rpm -ivh tog-openpegasus-<version>.<arch>.rpm`
2. Pour démarrer Pegasus, utilisez la commande suivante :
   `/etc/init.d/tog-pegasus start`

Remarque : Sous SuSE de Linux, le RPM intégré d'OpenPegasus n'est pas disponible. OpenPegasus doit être installé à partir de la source, comme décrit dans la procédure suivante.

Notez que dans Pegasus intégré, le protocole HTTP n'est pas activé par défaut. Une fois que OpenPegasus intégré est installé correctement, si aucune autre configuration n'est requise, suivez les instructions de la section Etape 4 : Installer le fournisseur CMPI de Broadcom. Pour activer le protocole HTTP, reportez-vous à la section Activer HTTP.

A partir de la source (Red Hat et SuSE)

La source d'OpenPegasus est téléchargeable sur www.openpegasus.org.

Remarque : Si ce n'est pas déjà fait, téléchargez et installez les RPM openssl et libopenssl-devel. Cette étape est facultative et uniquement nécessaire si vous envisagez d'utiliser le protocole HTTPS pour connecter le client à l'hôte géré.

Configuration des variables d'environnement

Configurez les variables d'environnement pour la création d'OpenPegasus comme suit.

Variable d'environnement	*Commentaires*
PEGASUS_ROOT	L'emplacement de l'arborescence source de Pegasus
PEGASUS_HOME	L'emplacement de l'exécutable construit, le référentiel ; par ex. les sous-répertoires $PEGASUS_HOME/bin, PEGASUS_HOME/lib, $PEGAUS_HOME/repository et $PEGASUS_HOME/mof.
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Pour les systèmes Linux 32 bits : « LINUX_IX86_GNU » Pour les systèmes Linux 64 bits : « LINUX_X86_64_GNU »
PEGASUS_HAS_SSL	Facultatif. Défini sur « true » pour la prise en charge du protocole HTTPS.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Facultatif. Défini sur « true » pour la prise en charge du protocole WSMAN.

Paramètres supplémentaires

La variable $PEGASUS_HOME doit être configurée dans l'environnement du shell et $PEGASUS_HOME/bin doit être ajouté à l'environnement $PATH.

Exemples

- export PEGASUS_PLATFORM="LINUX_X86_64_GNU"
- export PEGASUS_CIM_SCHEMA="CIM222"
- export PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER=true
- export PEGASUS_ROOT="/share/pegasus-2.10-src"
- export PEGASUS_HOME="/pegasus"
- export PATH=$PATH:$PEGASUS_HOME/bin

Pour une prise en charge du SSL, ajoutez la variable d'environnement suivante :

- export PEGASUS_HAS_SSL=true

Pour une prise en charge de WS-MAN, ajoutez la variable d'environnement suivante :

- export PEGASUS_ENABLE_PROTOCOL_WSMAN=true

Dans OpenPegasus, CIM-XML et WSMAN utilisent les mêmes ports pour les protocoles HTTP et HTTPS. Les numéros de port par défaut pour les protocoles HTTP et HTTPS sont 5989 et 5989, respectivement.

Remarque : Vous pouvez ajouter ces exportations à la fin de .bash_profile. Ce fichier se trouve dans le répertoire /root.

- Les variables d'environnement seront créées quand un utilisateur se connecte à l'aide de PuTTY.
- Sous le système Linux lui-même, pour chaque terminal sur lequel les variables d'environnement ne sont pas configurées, exécutez la commande suivante :
  `source /root/.bash_profile`
- Quand vous vous déconnectez et vous reconnectez, les variables d'environnement seront définies.

Construire et installer OpenPegasus

A partir de $PEGASUS_ROOT (l'emplacement du répertoire racine source de Pegasus), exécutez les commandes suivantes :

```
make clean
make
make repository
```

Remarque : Quand OpenPegasus est construit à partir de la source, les valeurs par défaut sont rétablies pour toutes les configurations. Si vous reconstruisez OpenPegasus, vous devez refaire la configuration comme mentionné dans la section Etape 3 : Configurer OpenPegasus sur le serveur.

Etape 2 : Démarrer le serveur CIM sur le serveur

Utilisez la commande `cimserver` pour démarrer le serveur CIM. Pour arrêter le serveur CIM, utilisez la commande `cimserver -s`.

Pour vérifier si OpenPegasus a été installé correctement, entrez la commande suivante :

```
cimcli ei -n root/PG_Interop PG_ProviderModule
```

Remarque : Pour OpenPegasus compilé à partir de la source, PEGASUS_HOME doit être défini au démarrage du serveur CIM. Sinon, le serveur CIM ne charge pas le référentiel correctement. Pensez à configurer PEGASUS_HOME dans le fichier « .bash_profile ».

Etape 3 : Configurer OpenPegasus sur le serveur

Utilisez la commande `cimconfig` pour configurer OpenPegasus, comme indiqué dans le tableau suivant :

Commande	*Commentaires*
`cimconfig -l`	Répertorie tous les noms de propriété valides.
`cimconfig -l -c`	Répertorie tous les noms de propriété valides et leurs valeurs
`cimconfig -g <property name>`	Interroge une propriété particulière.
`cimconfig -s <property name>=<value> -p`	Configure une propriété particulière.
`cimconfig --help`	Affiche des informations complémentaires sur la commande.

Le serveur CIM doit être démarré avant d'exécuter `cimconfig` et pour que les modifications de configuration soient prises en compte, vous devez le redémarrer.

Activer l'authentification

Les propriétés suivantes d'OpenPegasus doivent être configurées comme décrit dans cette section. Sinon, le fournisseur CIM de Broadcom CIM ne fonctionnera pas correctement. Menez à bien les configurations qui suivent avant de lancer BACS et de vous connecter au fournisseur.

Démarrez le serveur CIM si ce n'est pas déjà fait. Puis, configurez les éléments suivants :

- `cimconfig -s enableAuthentication=true -p`
- `cimconfig -s enableNamespaceAuthorization=false -p`
- `cimconfig -s httpAuthType=Basic -p`
- `cimconfig -s passwordFilePath=cimserver.passwd -p`
- `cimconfig -s forceProviderProcesses=false -p`

Si vous souhaitez qu'un utilisateur root se connecte à distance :

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

Configuration utilisateur avec privilège : Les utilisateurs du système Linux sont utilisés pour l'authentification OpenPegasus. Les utilisateurs du système doivent être ajoutés à OpenPegasus avec `cimuser` pour une connexion via BACS :

- `cimuser -a -u` *<username>* `-w` *<password>*

  Exemple : `cimuser -a -u root -w linux1`

Activer HTTP

1. Si ce n'est pas déjà fait, démarrez le serveur CIM.
2. Utilisez la commande suivante pour configurer un port HTTP (facultatif) :
   `cimconfig -s httpPort=5988 -p`

   Cette propriété n'est pas disponible pour OpenPegasus intégré.
3. Utilisez la commande suivante pour activer la connexion HTTP :
   `cimconfig -s enableHttpConnection=true -p`
4. Utilisez les commandes `cimserver -s` et `cimserver`, respectivement, pour arrêter ou redémarrer le serveur CIM afin que la nouvelle configuration soit prise en compte.

Activer HTTPS

1. Si ce n'est pas déjà fait, démarrez le serveur CIM.
2. Configurez le port HTTPS avec la commande suivante (facultatif) :
   `cimconfig -s httpsPort=5989 -p`

Cette propriété n'est pas disponible pour OpenPegasus intégré.

3. Activez la connexion HTTPS avec la commande suivante :
   `cimconfig -s enableHttpsConnection=true -p`
4. Utilisez les commandes `cimserver -s` et `cimserver`, respectivement, pour arrêter ou redémarrer le serveur CIM afin que la nouvelle configuration soit prise en compte.

Etape 4 : Installer le fournisseur CMPI de Broadcom

Vérifiez qu'OpenPegasus est installé correctement avant d'installer le fournisseur CMPI.

Installer

Entrez la commande suivante pour installer le fournisseur CMPI de Broadcom.

```
% rpm -i BRCM_CMPIProvider-{version}.{arch}.rpm
```

Désinstaller

Entrez la commande suivante pour désinstaller le fournisseur CMPI de Broadcom :

```
% rpm -e BRCM_CMPIProvider
```

Etape 5 : Effectuer la configuration du pare-feu Linux, si besoin

Suivez ces procédures pour ouvrir les ports appropriés dans le pare-feu :

Red Hat

1. Cliquez sur **Système**, sélectionnez **Administration** puis **Pare-feu**.
2. Sélectionnez **Autres ports**.
3. Dans la boîte de dialogue Port et protocole, sélectionnez **Défini par l'utilisateur**.
4. Dans le champ **Port/Etendue du port**, ajoutez le numéro de port.
5. Dans le champ **Protocole**, ajoutez un protocole, TCP, UDP, par exemple.
6. Cliquez sur **Appliquer** pour que les règles de pare-feu soient prises en compte.

Exemples :

- Pour CIM-XML sur HTTP, le numéro de port est 5988 et le protocole est TCP.
- Pour CIM-XML sur HTTPS, le numéro de port est 5989 et le protocole est TCP.

SuSE

1. Cliquez sur **Calculer**, puis sur **YaST**.
2. Sélectionnez **Sécurité et utilisateurs** sur le volet gauche.
3. Sur le volet droit, double-cliquez sur **Pare-feu**.
4. Sélectionnez **Règles personnalisées** sur le volet gauche.
5. Sur le volet droit, cliquez sur **Ajouter**.
6. Entrez les valeurs suivantes :
   - **Réseau source** : 0/0 (signifie tous)
   - **Protocole** : TCP (ou le protocole approprié)
   - **Port de destination** : <*Numéro de port*> ou <*Plage de numéros de port*>
   - **Port source** : Laissez le champ vierge.
7. Cliquez sur **Suivant** puis sur **Terminer** pour que les règles de pare-feu soient prises en compte.

Exemples :

Pour CIM-XML, utilisez les valeurs suivantes :

- **Réseau source** : 0/0 (signifie tous)
- **Protocole** : TCP
- **Port de destination** : 5988:5989
- **Port source** : Laissez le champ vierge.

Etape 6 : Installer BACS et les applications de gestion associées

Voir Installation de l'application Broadcom Advanced Control Suite.

Installation de WS-MAN ou de CIM-XML sur un client Linux

Aucun composant logiciel particulier n'est requis sur le système client Linux pour utiliser le protocole HTTP mais vous devez installer l'application de gestion BACS. Toutefois, pour les installations WS-MAN, vous pouvez éventuellement configurer le protocole HTTPS à utiliser avec BACS.

Configurer HTTPS sur un client Linux

Suivez ces étapes si vous souhaitez utiliser HTTPS à la place de HTTP (WS-MAN uniquement) :

Générer un certificat auto-signé pour le serveur Windows/Linux :

OpenSSL sur Linux ou Windows peut être utilisé pour générer le certificat auto-signé, comme suit :

Remarque : Vous pouvez télécharger et installer openssl à partir de http://gnuwin32.sourceforge.net/packages/openssl.htm.

1. Entrez la commande suivante pour générer une clé privée :
   `openssl genrsa -des3 -out server.key 1024`
2. Vous êtes invité à entrer un mot de passe. Pensez à le mémoriser.
3. Les étapes suivantes permettent de générer une demande de signature de certificat (CSR).

   Au cours de la génération de la CSR, vous êtes invité à entrer plusieurs éléments d'information. Lorsque vous êtes invité à indiquer le Nom commun, entrez le nom d'hôte ou l'adresse IP de Windows Server.

   Entrez la commande suivante (des exemples de réponses sont présentés) :

   `openssl req -new -key server.key -out server.csr`

   Si cette commande ne fonctionne pas, essayez les solutions suivantes :

   `openssl req –new –key server.key –out server.csr –config openssl.cnf`

   Le fichier openssl.cnf doit être placé dans le même répertoire que openssl. Openssl.cnf est situé dans le dossier C:\Program Files (x86)\GnuWin32\share.

   Les informations ci-dessous sont requises :

   - Nom du pays (code à 2 lettres) [] : **US**
   - Etat ou nom de province (nom complet) [] : **Californie**
   - Nom de la localité (p. ex., ville) [] : **Irvine**
   - Nom de l'organisation (p. ex., société) [] : **Broadcom Corporation**
   - Nom de l'unité organisationnelle (p. ex., section) [] : **Ingénierie**
   - Nom commun (p. ex., votre nom) [] : Entrez le nom d'hôte ou l'adresse IP de Windows Server. Pour iPv6, saisissez le nom commun au format [xyxy:xxx: … . ::xxx], **avec les crochets [ ]**.
   - (Facultatif) Adresse e-mail [] :

   Entrez les attributs supplémentaires suivants pour recevoir votre demande de certificat :

   - Un mot de passe complexe [] :**linux1**
   - Un nom de société facultatif [] :
4. Supprimez le mot de passe de la clé.

   Entrez les commandes suivantes :

   ```
   cp server.key server.key.org
   openssl rsa -in server.key.org -out server.key
   ```

5. Générez un certificat auto-signé :

   Pour générer un certificat auto-signé actif pendant 365 jours, entrez la commande suivante :

   ```
   openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
   ```

   Le message suivant s'affiche :

   ```
   Signature ok
   subject=/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-   LAB3/
   emailAddress=
   Getting Private key
   ```

6. Entrez la commande suivante pour vérifier le certificat auto-signé généré.
   `openssl verify server.crt`

   Le message suivant s'affiche :

   ```
   server.crt:/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-
   LAB3/emailAddress=
   error 18 at 0 depth lookup:self signed certificate
   OK
   ```

   Ignorez le message d'erreur « error 18 at 0 depth lookup:self signed certificate ». Cette erreur indique qu'il s'agit d'un certificat auto-signé.

7. Convertissez le certificat du format « crt » au format « pkcs12 », comme suit :

   Pour un serveur Windows, le certificat doit avoir le format pkcs12. Entrez la commande suivante :

   ```
   openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx
   ```

   Il vous sera demandé d'entrer les éléments suivants :

   ```
   Enter Export Password:
   Verifying - Enter Export Password:
   ```

   Entrez le mot de passe et pensez à le mémoriser. Le mot de passe est nécessaire au moment de l'importation du certificat sur le serveur et le client Windows.

8. Effectuez une copie du fichier de certificat server.crt et placez-le sur le serveur où BACS sera installé, de façon à ce qu'il puisse être importé. Si vous prévoyez d'utiliser un client Windows ou Linux pour vous connecter au serveur exécutant BACS, le certificat doit également être transféré (par copier-coller) vers le système client.

   Sous Linux, le certificat doit porter l'extension « .pem ». Il n'existe pas de différence entre les extensions « .crt » et « .pem ». Aucun besoin donc d'utiliser la commande `openssl` pour convertir l'extension .crt en .pem. Vous pouvez simplement copier le fichier tel quel.

Remarque : Un certificat distinct doit être généré pour une adresse IPv4, une adresse IPv6 et un nom d'hôte.

Importer un certificat auto-signé sur le client Linux

Sur les distributions Linux, notez le répertoire suivant du certificat :

- Pour toutes les versions de SuSE, le répertoire du certificat est `/etc/ssl/certs`.
- Pour Red Hat, le répertoire du certificat peut être différent suivant chaque version. Sur certaines versions, il s'agit de `/etc/ssl/certs` ou de `/etc/pki/tls/certs`. Sur d'autres versions, identifiez le répertoire du certificat.

Copiez le fichier *hostname.pem*, créé à l'étape Générer un certificat auto-signé pour le serveur Windows/Linux :, dans le répertoire de certificats du client Linux. Par exemple, si le répertoire du certificat est `/etc/ssl/certs`, copiez *hostname.pem* dans `/etc/ssl/certs`.

1. Remplacez le répertoire par `/etc/ssl/certs`.
2. Créez une valeur de hachage en exécutant la commande suivante.
   `openssl x509 -noout -hash -in hostname.pem`

   Une valeur comme ce qui suit sera renvoyée.

   `100940db`
3. Créez un lien symbolique vers la valeur de hachage en exécutant la commande suivante :
   `ln -s hostname.pem 100940db.0`

Tester la connexion HTTPS/SSL à partir du client Linux

Utilisez la commande suivante pour vérifier si le certificat est correctement installé sous Linux :

```
# curl -v --capath /etc/ssl/certs https://Hostname or IPAddress:5986/wsman
```

En cas d'échec, cela signifie que le certificat n'est pas installé correctement et un message d'erreur s'affiche, indiquant la procédure à suivre pour y remédier.

Installation de l'application Broadcom Advanced Control Suite

Le logiciel Broadcom Advanced Control Suite (BACS) peut être installé sur un système Linux à l'aide du progiciel RPM Linux. Cette installation couvre un client d'interface de ligne de commande.

Préliminaires :

- Vérifiez que les cartes réseau Broadcom sont physiquement installées et que le pilote de périphérique approprié pour le NIC est installé sur le système à gérer avec cet utilitaire.
- Vérifiez que le fournisseur CIM est installé correctement sur le système à gérer avec cet utilitaire. Voir
- Pour gérer iSCSI sur des hôtes Linux, vérifiez que les utilitaires open-iscsi et sg sont bien installés sur l'hôte Linux.

Pour installer BACS

1. Téléchargez le progiciel RPM de la dernière application de gestion BACS.
2. Installez le progiciel RPM avec la commande suivante :
   `% rpm -i BACS-{version}.{arch}.rpm`

Pour utiliser l'interface de ligne de commande de BACS, reportez-vous au fichier BACSCLI_Readme.txt fourni avec les fichiers de version.

Pour supprimer BACS

Pour désinstaller le progiciel RPM, utilisez la commande suivante :

```
% rpm -e BACS
```

Section 11 : Logiciel pilote pour VMware

Présentation

Le pilote VMware est fourni dans le format de présentation suivant.

Tableau 19 : Présentation du pilote VMware

Format	*Pilotes*
VMware VIB	vmware-esx-drivers-net-tg3-version.x86_64.vib

Pilotes

Téléchargement, installation et mise à jour de pilotes

Pour télécharger, installer ou mettre à jour le pilote VMware ESX/ESXi pour les cartes réseau GbE NetXtreme I, consultez le site Web http://www.vmware.com/support.

Paramètres du pilote

NetQueue

Le paramètre facultatif **force_netq** peut être utilisé pour définir le nombre de files d'attente NetQueue Rx et Tx. Les périphériques BCM57XX qui prennent en charge NetQueue sont BCM5718, BCM5719, BCM5720, BCM5721 et BCM5722.

Par défaut, le pilote tente d'utiliser le nombre optimal de files d'attente NetQueue. Pour forcer explicitement le nombre de files d'attente à définir, indiquez le nombre de files d'attente NetQueue par port via la commande suivante :

```
esxcfg-module -s force_netq=x,x,x.... tg3
```

Les valeurs autorisées de x vont de -1 à 15 :

- 1–15 force le nombre de files d'attente NetQueue pour le NIC donné.
- 0 désactive NetQueue.
- –1 indique d'utiliser la valeur de pilote NetQueue par défaut.

Le nombre d'entités « x » peut monter jusqu'à 32, ce qui signifie que le nombre maximal de cartes réseau pris en charge est égal à 32.

Exemples d'usage :

```
esxcfg-module -s force_netq=-1,0,1,2 tg3]
```

- tg3 NIC 0 : Utiliser le nombre de files d'attente NetQueues par défaut.
- tg3 NIC 1 : Désactiver la fonction NetQueue.
- tg3 NIC 2 : Utiliser 1 file d'attente NetQueue.
- tg3 NIC 3 : Utiliser 2 files d'attente NetQueues.

Notez que le numéro de NIC ci-dessus ne correspond pas au numéro de vmnic. Le numéro de NIC est le numéro d'ordre de test de vmnic du système. Idéalement, le nombre de files d'attente NetQueue correspond au nombre de processeurs de la machine.

Paramètres du pilote

Plusieurs paramètres facultatifs peuvent être introduits dans la commande vmkload_mod sous la forme d'un argument de ligne de commande. Ces paramètres peuvent être également définis par le biais de la commande esxcfg-module. Reportez-vous à la man page pour de plus amples informations.

Paramètres par défaut des pilotes

Tableau 20 : Paramètres par défaut du pilote VMware

Paramètre	*Valeur par défaut*
Vitesse	Autonégociation avec toutes les vitesses annoncées
Contrôle de flux :	Autonégociation avec Rx et Tx annoncés
MTU	1 500 (plage comprise entre 46 et 9 000)
Taille de l'anneau Rx	200 (entre 0 et 511). Certaines puces sont fixées à 64.
Taille de l'anneau RX Jumbo	100 (entre 0 et 255). Certaines puces ne prennent pas en charge l'anneau Jumbo et d'autres, qui prennent en charge les trames Jumbo, n'utilisent pas l'anneau Jumbo.
Taille de l'anneau Tx	511 (entre (MAX_SKB_FRAGS+1) et 511). MAX_SKB_FRAGS varie selon les noyaux et les architectures. Sur un noyau 2.6 pour x86, MAX_SKB_FRAGS correspond à 18.
Grouper les microsecondes de RX	20 (entre 0 et 1023)
Grouper les microsecondes de RX IRQ	20 (gamme de 0 à 255)
Grouper les trames RX	5 (gamme de 0 à 1 023)
Grouper les trames RX IRQ	5 (gamme de 0 à 255)
Grouper les microsecondes de TX	72 (gamme de 0 à 1 023)
Grouper les usec de TX IRQ	20 (gamme de 0 à 255)
Grouper les trames TX	53 (gamme de 0 à 1 023)
Grouper les trames TX IRQ	5 (gamme de 0 à 255)
Grouper les usec statistiques	1000000 (env. 1 s). Certains paramètres de groupement ne sont pas utilisés ou présentent des valeurs par défaut différentes sur certaines puces.
MSI	Activés (s'ils sont pris en charge par la puce et si le test d'interruption est réussi).
WoL	Désactivé

Messages du pilote

Vous trouverez ci-dessous des exemples de messages courants qui sont susceptibles d'être consignés dans le fichier /var/log/messages. Utilisez `dmesg -n <niveau>` pour contrôler le niveau auquel les messages apparaîtront sur la console. Pour la plupart, les systèmes sont réglés par défaut sur le niveau 6. Pour visualiser l'ensemble des messages, définissez le niveau sur une valeur plus élevée.

Ouverture de session du pilote

```
tg3.c:v3.118g (Jan 4, 2012)
```

NIC détecté

```
vmnic0#: Tigon3 [partno (BCM95xxx) rev 4202 PHY (57xx) (PCI Express) 10/100/1000BaseT Ethernet
:00:xx:xx:xx:xx:xx
vmnic0#: RXcsums [1] LinkChg REG [0] MIirq [0] ASF [0] Split [0] Wirespeed [1]TSOcap [1]
vmnic0#: dma_rwctrl [76180000]
ACPI : PCI interrupt 0000:02:02.0 [A] -> GSI 26 (level,low) -> IRQ 233
```

Indication de liaison active et de vitesse

```
tg3: vmnic0: Link is up at 1000 Mbps, full duplex.
tg3: vmnic0: Flow control is on for TX and on for RX.
```

Indication de liaison inactive

```
tg3: vmnic0: Link is down.
```

Section 12 : Installation de l'application de gestion et du pilote Windows

Installation du logiciel pilote

Remarque : Ces instructions supposent que votre carte NetXtreme de Broadcom n'a pas été installée à l'usine. Si votre contrôleur a été installé à l'usine, le logiciel pilote a été installé pour vous.

Si vous démarrez Windows pour la première fois après avoir installé un périphérique matériel (par exemple, une carte NetXtreme de Broadcom) ou après avoir désinstallé le pilote de périphérique existant, votre système d'exploitation détecte automatiquement le matériel et vous invite à installer le logiciel pilote de ce périphérique.

Pour l'installation automatique, deux modes sont disponibles : un mode d'installation graphique interactive (voir Utilisation du programme d'installation) et un mode de commande de ligne silencieux (voir Installations automatiques).

Remarque :

- Avant d'installer le logiciel pilote, vérifiez que le système d'exploitation Windows a été mis à niveau, intégrant le Service Pack le plus récent.
- Vous devez avoir installé préalablement un pilote de périphérique réseau pour pouvoir utiliser la carte Gigabit Ethernet NetXtreme de Broadcom avec votre système d'exploitation Windows. Les pilotes se trouvent sur le CD-ROM d'installation.
- BACS n'est pas pris en charge pour l'option d'installation de Server Core pour Microsoft Windows Server 2008 R2.

Utilisation du programme d'installation

Outre l'installation des pilotes de périphériques Broadcom, le programme d'installation installe des applications de gestion. S'ils sont disponibles, les éléments suivants sont installés lorsque vous exécutez le programme d'installation :

- **Pilotes de périphériques Broadcom**. Installe les pilotes de périphériques Broadcom.
- **Control Suite**. Broadcom Advanced Control Suite (BACS).
- **BASP**. Installe Broadcom Advanced Server Program.
- **SNMP**. Installe le sous-agent SNMP (Simple Network Management Protocol).
- **CIM Provider**. Installe le serveur CIM (Common Information Model).
- **iSCSI Crash Dump Driver (pilote pour l'utilitaire iSCSI de vidage de la mémoire en cas de panne)**. Installe le pilote requis pour l'utilitaire iSCSI de vidage de la mémoire en cas de panne (iSCSI Crash Dump).

Remarque : Si l'installation de l'application BACS et des applications de gestion associées est facultative, l'installation des pilotes de périphériques Broadcom est requise lorsque vous utilisez le programme d'installation.

Remarque : BASP n'est pas disponible sur Windows Small Business Server (SBS) 2008.

Pour installer l'initiateur logiciel iSCSI Microsoft pour le vidage de la mémoire iSCSI

S'il est pris en charge et que vous comptez utiliser l'utilitaire Broadcom iSCSI Crash Dump, il est essentiel de suivre l'ordre d'installation :

- Lancez le programme d'installation
- Installez l'initiateur logiciel iSCSI Microsoft iSCSI en intégrant le correctif (MS KB939875)

Remarque : Si vous effectuez une mise à niveau des pilotes des périphériques à l'aide du programme d'installation, réactivez le vidage sur incident **iSCSI Crash Dump** à partir de la section Avancé de l'onglet BACS Configuration (Configuration BACS).

Suivez cette procédure après avoir exécuté le programme d'installation pour installer les pilotes des périphériques et les applications de gestion.

1. Installez l'initiateur logiciel iSCSI Microsoft (version 2.06 ou ultérieure) si celui-ci n'est pas inclus dans votre système d'exploitation. Pour déterminer quand il est nécessaire d'installer l'initiateur logiciel iSCSI Microsoft, voir Tableau 21. Pour télécharger l'initiateur logiciel iSCSI de Microsoft, rendez-vous à l'adresse http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986.
2. Installez le correctif Microsoft pour la génération d'un fichier de vidage sur incident dans le cadre du protocole iSCSI (Microsoft KB939875) à partir de l'adresse suivante : http://support.microsoft.com/kb/939875. Pour déterminer si vous devez installer le correctif Microsoft, voir Tableau 21.

Tableau 21 : Systèmes d'exploitation Windows et vidage sur incident iSCSI Crash Dump

Système d'exploitation	*Initiateur logiciel iSCSI Microsoft requis*	*Correctif Microsoft (MS KB939875) requis*
NDIS		
Windows Server 2008	Oui (inclus avec le système d'exploitation)	Non
Windows Server 2008 R2	Oui (inclus avec le système d'exploitation)	Non
Windows Server 2012	Oui (inclus avec le système d'exploitation)	Non
OIS		
Windows Server 2008	Non	Non
Windows Server 2008 R2	Non	Non
Windows Server 2012	Non	Non

Installations automatiques

Remarque :

- Toutes les commandes sont sensibles à la casse.
- Pour des instructions et des informations détaillées sur les installations automatiques, consultez le fichier Silent.txt du dossier Driver_Management_Apps_Installer.

Consultez le fichier readme.txt dans le dossier d'installation pour obtenir les instructions de ligne de commande.

Remarque : n'utilisez l'option REINSTALL que si le programme d'installation est déjà installé sur le système. Pour mettre à niveau une version antérieure du programme d'installation, utilisez la commande `setup /s /v/qn` ci-dessus.

Modification du logiciel pilote

Pour modifier le logiciel pilote

1. Dans le Panneau de configuration, cliquez sur **Ajout/Suppression de programmes**.
2. Sélectionnez **Broadcom Driver and Management Applications** (Pilote Broadcom et applications de gestion), puis cliquez sur **Modifier**.
3. Cliquez sur **Suivant** pour continuer.
4. Cliquez sur **Modifier, Ajouter ou Supprimer** pour modifier les fonctions du programme. Cette option ne permet pas d'installer les pilotes des nouvelles cartes. Pour de plus amples informations sur l'installation des pilotes de nouvelles cartes, reportez-vous à la section Réparation ou réinstallation du logiciel pilote.
5. Cliquez sur **Suivant** pour continuer.
6. Cliquez sur une icône pour modifier le mode d'installation d'une fonction.
7. Cliquez sur **Suivant**.
8. Cliquez sur **Installer**.
9. Cliquez sur **Terminer** pour fermer le programme d'installation.
10. Le programme d'installation détermine s'il est nécessaire de redémarrer le système. Suivez les instructions à l'écran.

Réparation ou réinstallation du logiciel pilote

Pour réparer ou réinstaller le logiciel pilote

1. Dans le Panneau de configuration, cliquez sur **Ajout/Suppression de programmes**.
2. Sélectionnez **Broadcom Driver and Management Applications** (Pilote Broadcom et applications de gestion), puis cliquez sur **Modifier**.
3. Cliquez sur **Suivant** pour continuer.
4. Cliquez sur **Réparer ou Réinstaller** pour réparer les erreurs ou installer des pilotes pour les nouvelles cartes.
5. Cliquez sur **Suivant** pour continuer.
6. Cliquez sur **Installer**.
7. Cliquez sur **Terminer** pour fermer le programme d'installation.
8. Le programme d'installation détermine s'il est nécessaire de redémarrer le système. Suivez les instructions à l'écran.

Suppression des pilotes de périphériques

Si vous supprimez des pilotes de périphériques, toute application de gestion installée est également supprimée.

Remarque : Windows Server 2008 et Windows Server 2008 R2 proposent la fonction Device Driver Rollback permettant de restaurer la version précédente d'un pilote. Cependant, l'architecture logicielle complexe du périphérique NetXtreme peut provoquer des problèmes si cette fonction est utilisée sur l'un des composants individuels. Par conséquent, nous vous recommandons de modifier les versions de pilotes uniquement à l'aide d'un programme d'installation de pilote.

Pour supprimer les pilotes de périphériques

1. Dans le Panneau de configuration, cliquez sur **Ajout/Suppression de programmes**.
2. Sélectionnez **Broadcom Drivers and Management Applications** (Pilote Broadcom et applications de gestion), puis cliquez sur **Supprimer**. Suivez les instructions à l'écran.
3. Réinitialisez le système pour supprimer complètement les pilotes. Si vous ne le réinitialisez pas, vous ne serez pas en mesure d'installer correctement les pilotes.

Affichage ou modification des propriétés de la carte

Pour afficher ou modifier les propriétés de la carte réseau de Broadcom

1. Dans le Panneau de configuration, cliquez sur **Broadcom Control Suite 4**.
2. Cliquez sur la section Avancé de l'onglet **Configurations**.

Définition des options de gestion de l'alimentation

Vous pouvez définir les options de gestion de l'alimentation de façon à ce que le système d'exploitation désactive le contrôleur pour économiser de l'énergie ou de façon à permettre au contrôleur de « réveiller » le système. Cependant, si le périphérique est occupé (à prendre un appel par exemple), le système d'exploitation ne l'arrête pas. Le système d'exploitation tente de désactiver tous les périphériques uniquement lorsque l'ordinateur se met en veille. Pour que la carte reste constamment active, ne cochez pas la case **Autoriser l'ordinateur à éteindre ce périphérique pour économiser l'énergie**.

Remarque : Les options de gestion d'alimentation ne sont pas disponibles sur les serveurs à lames.

Remarque :

- L'onglet Gestion de l'alimentation ne s'applique qu'aux serveurs prenant en charge la gestion de l'alimentation.
- Pour activer le Réseau local de réveil (WOL) lorsque l'ordinateur est en veille, cochez la case **Autoriser ce périphérique à sortir cet ordinateur de la mise en veille**.
- Si vous sélectionnez **N'autoriser que les stations de gestion à faire sortir l'ordinateur du mode veille**, l'ordinateur peut être sorti de son état de veille *uniquement par Magic Packet* (par paquets magiques).

Attention : Ne cochez pas la case **Autoriser l'ordinateur à éteindre ce périphérique pour économiser l'énergie** s'il s'agit d'une carte faisant partie d'une équipe.

Configuration du protocole de communication à utiliser avec BACS4

Il existe deux principaux composants d'applications de gestion BACS4 : le composant fournisseur et le logiciel du client. Un fournisseur est installé sur un serveur (ou « hôte géré ») contenant une ou plusieurs cartes réseau. Le fournisseur recueille des informations sur les cartes réseau et les rend disponibles pour la récupération depuis un ordinateur de gestion sur lequel le logiciel client est installé. Le logiciel client permet d'afficher les informations des fournisseurs et de configurer les cartes réseau. Le logiciel client BACS comprend une interface graphique et une interface de ligne de commande (CLI).

Un protocole de communication permet la communication entre le fournisseur et le logiciel client. Suivant la combinaison de systèmes d'exploitation (Linux, Windows ou les deux) installés sur les clients et les hôtes gérés dans votre réseau, vous pouvez choisir un protocole de communication approprié à utiliser. Voir « Installation de l'application de gestion pour Linux » pour lire une description des protocoles de communication disponibles pour chaque configuration réseau.

Les instructions de ce chapitre concernent uniquement les scénarios qui impliquent une communication entre des hôtes gérés Windows et des clients Windows. Dans ces scénarios, vous pouvez utiliser les protocoles de communication WMI ou WS-MAN (WinRM). Lorsque vous utilisez le programme d'installation du pilote décrit dans ce chapitre pour installer le pilote et les applications de gestion, le fournisseur WMI et WS-MAN est installé sur l'hôte géré. En outre, l'utilitaire BACS4 est installé sur le client. Les sections suivantes décrivent les étapes de configuration supplémentaires pour le protocole de communication que vous sélectionnez.

Pour des installations Linux, le pilote est installé séparément des applications de gestion. Voir pour obtenir les instructions correspondantes.

Avec WS-MAN

Pour utiliser le protocole de communication WS-MAN, suivez les instructions des sections suivantes :

- Configuration du serveur Windows pour WS-MAN
- Installation de WS-MAN sur un client Windows

Configuration du serveur Windows pour WS-MAN

Etape 1 : Installer le composant logiciel WinRM sur le serveur

WinRM 2.0 est préinstallé sur les systèmes d'exploitation suivants :

- Windows 7
- Windows 8
- Windows 8,1
- Windows Server 2008 R2
- Windows Server 2012
- Windows 2012 R2

Pour Windows XP et Windows Server 2008, installez Windows Management Framework Core, qui comprend WinRM 2.0 et Windows Powershell 2.0, à partir du lien suivant :

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11829

Etape 2 : Réaliser la configuration de base sur le serveur

Le pare-feu Windows doit être activé pour permettre le bon fonctionnement de WinRM. Pour obtenir des informations détaillées sur la configuration du pare-feu, reportez-vous à la section Etape 7 : Configuration complémentaire du serveur. Une fois le pare-feu configuré, ouvrez une invite de commande et exécutez la commande suivante pour activer la gestion à distance sur le serveur Windows :

```
winrm quickconfig
```

Vous pouvez utiliser la commande suivante pour afficher les informations de configuration pour le service :

```
winrm get winrm/config
```

Etape 3 : Réaliser la configuration d'utilisateur sur le serveur

Pour vous connecter à WinRM, le compte doit être membre du groupe d'administrateurs local sur l'ordinateur local ou distant. Le résultat de la commande `get winrm/config` sera le suivant :

```
RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
```

BA signifie BUILTIN\Administrators.

Pour ajouter un autre groupe d'utilisateurs à la liste de connexion WinRM autorisée, vous pouvez modifier le RootSDDL pour inclure le nouveau groupe d'utilisateurs. Vous aurez besoin de l'ID SSDL pour le nouveau groupe. Par exemple, la commande suivante ajoute le nouveau groupe d'utilisateurs portant l'ID SDDL S-1-5 -21-1866529496 -2433358402-1775838904-1021.

```
winrm set winrm/config/Service @{RootSDDL="O:NSG:BAD:P(A;GA;;;BA)(A;;GA;;;
S-1-5-21-1866529496-2433358402-1775838904-1021)S:P(AU;FA;GA;;
WD)(AU;SA;GWGX;;;WD)"}
```

Etape 4 : Réaliser la configuration HTTP sur le serveur

Pour utiliser l'interface graphique BACS, vous devez configurer le protocole HTTP comme suit :

Remarque : Le port HTTP par défaut est 5985 pour WinRM 2.0.

1. Cliquez sur **Démarrer** (ou appuyez sur la touche Windows) et sélectionnez **Exécuter**.
2. Saisissez **gpedit.msc** pour ouvrir l'éditeur de stratégie de groupe local.
3. Dans **Configuration de l'ordinateur**, ouvrez le dossier **Modèles d'administration**, puis le dossier **Composants Windows**.
4. Sélectionnez **Gestion à distance de Windows (WinRM)**.
5. Dans **Gestion à distance de Windows (WinRM)**, sélectionnez **Client WinRM**.
6. Dans **Client WinRM**, double-cliquez sur **Hôtes approuvés**.
7. Dans le **TrustedHostsList**, entrez les noms d'hôte des clients. Si tous les clients sont approuvés, entrez uniquement un astérisque (*).
8. Sélectionnez **Service Gestion à distance de Windows**.

9. Activez **Autoriser l'authentification de base**.
10. Activez **Autoriser le trafic non chiffré**.
11. Fermez la fenêtre **Stratégie de groupe**.
12. Dans l'invite de commande, exécutez la commande suivante pour configurer WinRM avec les paramètres par défaut :
    `winrm qc or winrm quickconfig`
13. Lorsque l'outil affiche **Effectuer ces modifications [y/n] ?**, entrez **y**.
14. Entrez l'une des commandes suivantes pour vérifier si un écouteur HTTP est créé :
    `winrm enumerate winrm/confg/listener`

    ou

    `winrm e winrm/config/Listener`
15. Entrez la commande suivante à partir de l'invite de commande pour effectuer un test localement.
    `winrm id`

Etape 5 : Réaliser la configuration HTTPS sur le serveur (pour utiliser HTTPS plutôt que HTTP)

Cette étape se décompose en deux processus distincts : la génération d'un certificat auto-signé, si celui-ci n'existe pas, et son importation sur un serveur Windows. Si aucun certificat auto-signé n'existe, vous devez en configurer un sur le serveur Windows pour activer la communication HTTPS/SSL avec l'interface graphique BACS sur le client Windows. Le client Windows doit également être configuré à l'aide du certificat auto-signé. Voir Réaliser la configuration HTTPS (si vous prévoyez d'utiliser HTTPS).

Remarque : Le certificat auto-signé peut être créé sur n'importe quel serveur Windows. Le serveur ne nécessite pas que BACS soit installé. Le certificat auto-signé généré sur un serveur Windows doit être copié sur le disque local du client.

1. Cliquez sur **Démarrer** (ou appuyez sur la touche Windows) et sélectionnez **Exécuter**.
2. Saisissez **gpedit.msc** pour ouvrir l'éditeur de stratégie de groupe local.
3. Dans **Configuration de l'ordinateur**, ouvrez le dossier **Modèles d'administration**, puis le dossier **Composants Windows**.
4. Sélectionnez **Gestion à distance de Windows (WinRM)**.
5. Dans **Gestion à distance de Windows (WinRM)**, sélectionnez **Client WinRM**.
6. Dans **Client WinRM**, double-cliquez sur **Hôtes approuvés**.
7. Dans le **TrustedHostsList**, entrez les noms d'hôte des clients. Si tous les clients sont approuvés, entrez uniquement un astérisque (*).
8. Sélectionnez **Service Gestion à distance de Windows**.
9. Activez **Autoriser l'authentification de base**.

Générer un certificat auto-signé pour Windows Server :

OpenSSL sur Windows peut être utilisé pour générer le certificat auto-signé, comme suit :

1. Entrez la commande suivante pour générer une clé privée :
   `openssl genrsa -des3 -out server.key 1024`
2. Vous êtes invité à entrer un mot de passe. Pensez à le mémoriser.
3. Les étapes suivantes permettent de générer une demande de signature de certificat (CSR).

   Au cours de la génération de la CSR, vous êtes invité à entrer plusieurs éléments d'information. Lorsque vous êtes invité à indiquer le Nom commun, entrez le nom d'hôte ou l'adresse IP de Windows Server.

Entrez la commande suivante (des exemples de réponses sont présentés) :

```
openssl req -new -key server.key -out server.csr
```

Si cette commande ne fonctionne pas, essayez les solutions suivantes :

```
openssl req –new –key server.key –out server.csr –config openssl.cnf
```

Le fichier openssl.cnf doit être placé dans le même répertoire que openssl. Openssl.cnf est situé dans le dossier C:\Program Files (x86)\GnuWin32\share.

Les informations ci-dessous sont requises :

- Nom du pays (code à 2 lettres) [] : **US**
- Etat ou nom de province (nom complet) [] : **Californie**
- Nom de la localité (p. ex., ville) [] : **Irvine**
- Nom de l'organisation (p. ex., société) [] : **Broadcom Corporation**
- Nom de l'unité organisationnelle (p. ex., section) [] : **Ingénierie**
- Nom commun (p. ex., votre nom) [] : Entrez le nom d'hôte ou l'adresse IP de Windows Server. Pour iPv6, saisissez le nom commun au format [xyxy:xxx: ….. ::xxx], **avec les crochets [ ]**.
- (Facultatif) Adresse e-mail [] :

Entrez les attributs supplémentaires suivants pour recevoir votre demande de certificat :

- Un mot de passe complexe [] : **motdepasse1**
- Un nom de société facultatif [] :

4. Supprimez le mot de passe de la clé.

Entrez les commandes suivantes :

```
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
```

5. Générez un certificat auto-signé :

Pour générer un certificat auto-signé actif pendant 365 jours, entrez la commande suivante :

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Le message suivant s'affiche :

```
Signature ok
subject=/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-   LAB3/
emailAddress=
Getting Private key
```

6. Entrez la commande suivante pour vérifier le certificat auto-signé généré.

```
openssl verify server.crt
```

Le message suivant s'affiche :

```
server.crt:/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-
LAB3/emailAddress=
error 18 at 0 depth lookup:self signed certificate
OK
```

Ignorez le message d'erreur « error 18 at 0 depth lookup:self signed certificate ». Cette erreur indique qu'il s'agit d'un certificat auto-signé.

7. Convertissez le certificat du format crt au format pkcs12, comme suit :

Pour un serveur Windows, le certificat doit avoir le format pkcs12. Entrez la commande suivante :

```
openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx
```

Il vous sera demandé d'entrer les éléments suivants :

```
Enter Export Password:
Verifying - Enter Export Password:
```

Entrez le mot de passe et pensez à le mémoriser. Le mot de passe est nécessaire au moment de l'importation du certificat sur le serveur et le client Windows.

8. Effectuez une copie du fichier de certificat server.crt et placez-le sur le serveur où BACS sera installé, de façon à ce qu'il puisse être importé. Si vous prévoyez d'utiliser un client Windows pour vous connecter au serveur exécutant BACS, le certificat doit également être transféré (par copier-coller) vers le système client.

Remarque : Un certificat distinct doit être généré pour une adresse IPv4, une adresse IPv6 et un nom d'hôte.

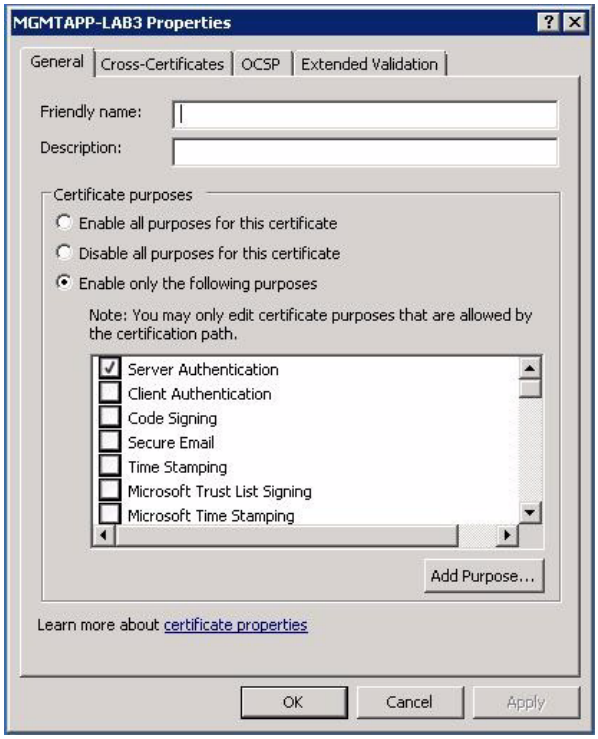
Pour installer le certificat auto-signé sur Windows Server :

Transférez le fichier *hostname*.pfx que vous avez généré sur Windows Server avant d'installer le certificat :

1. Cliquez sur **Démarrer** (ou appuyez sur la touche Windows) et sélectionnez **Exécuter**.
2. Saisissez **MMC**, puis cliquez sur **OK**.
3. Cliquez sur **Fichier** > **Ajouter/Supprimer le composant logiciel enfichable**.
4. Cliquez sur **Ajouter**.
5. Sélectionnez **Certificats** et cliquez sur **Ajouter**.
6. Sélectionnez **Compte d'ordinateur**.
7. Cliquez sur **Suivant**, puis sur **Terminer**.
8. Cliquez sur **Fermer**, puis sur **OK**.
9. Ouvrez le dossier **Certificats (ordinateur local)**, puis ouvrez le dossier **Personnel.**
10. Cliquez avec le bouton droit sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
11. Cliquez sur **Suivant** pour lancer l'assistant Importation de certificat.
12. Cliquez sur Parcourir pour sélectionner **hostname.pfx**.
13. Lorsque vous êtes invité à entrer le mot de passe de la clé privée, entrez le même mot de passe que vous avez créé dans Générer un certificat auto-signé pour Windows Server :.
14. Suivez les instructions, sélectionnez les valeurs par défaut et continuez.

    Le certificat s'affiche comme étant installé sur le côté droit de la fenêtre. Il porte le nom que vous avez indiqué lors de la création du certificat auto-signé.
15. Cliquez avec le bouton droit sur le certificat et sélectionnez **Propriétés**.

    Une boîte de dialogue s'affiche, comme suit :



16. Assurez-vous que seule l'option **Authentification du serveur** est activée, comme indiqué sur la figure.

17. Ouvrez **Autorités de certification racines de confiance**, puis **Certificats**.

18. Suivez les instructions de Etape 11. à Etape 17.

Remarque : Reportez-vous à la section Réaliser la configuration HTTPS (si vous prévoyez d'utiliser HTTPS) pour obtenir des instructions sur l'importation du certificat auto-signé sur un client.

Etape 6 : Configurer WinRM HTTPS/SSL sur le serveur

1. Créez un écouteur WinRM, comme suit :

a. Cliquez sur **Démarrer** (ou appuyez sur la touche Windows) et sélectionnez **Exécuter**.

b. Saisissez **MMC**, puis cliquez sur **OK**.

c. Sélectionnez le certificat auto-signé dans le magasin personnel.

Par exemple, si le certificat est créé avec un nom d'hôte, le nom d'hôte s'affiche.

d. Double-cliquez sur le certificat pour l'ouvrir.

e. Cliquez sur l'onglet **Détails**.

f. Faites défiler vers le bas et sélectionnez le champ **Empreinte.**

g. Sélectionnez et copiez l'empreinte dans la fenêtre **Détails**, afin de pouvoir l'insérer lors de l'étape suivante.

h. Retournez à l'invite de commande.

i. Entrez la commande suivante :

```
winrm create winrm/config/Listener?Address=*+Transport=
HTTPS @{Hostname="<HostName or IPAddress>";
CertificateThumbprint="<paste from the previous step and remove the spaces>"}
```

Remarque :

- Si le certificat a été généré à l'aide du nom d'hôte, entrez ce dernier. S'il a été généré à l'aide de l'adresse IP, entrez cette dernière. Pour une adresse IPv6, entourez l'adresse de crochets [ ].
- Si HTTPS est configuré dans votre système, l'écouteur doit être supprimé pour pouvoir créer un nouvel écouteur HTTPS. Utilisez la commande suivante :
  `winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`

j. La commande ci-dessus crée un écouteur sur le port HTTPS (5986), en utilisant toute adresse réseau du serveur, et le certificat généré SelfSSL.

k. La commande `winrm` permet de modifier ou de définir l'écouteur HTTPS, car les écouteurs WinRM peuvent être configurés sur n'importe quel port défini par l'utilisateur.

l. A partir d'une invite de commande, exécutez la commande suivante pour vérifier que le ou les auditeurs ont été configurés :
```
winrm e winrm/config/listener
```

2. Testez la connexion HTTPS/SSL sur le serveur.

a. A l'invite de commande sur le serveur, saisissez la commande suivante :
```
winrs -r:https://yourserver:5986 -u:username -p:password hostname
```

b. Si la configuration est correcte, la sortie de la commande indique le nom d'hôte du serveur.

c. Pour vérifier la configuration du service WinRM, exécutez la commande suivante :
```
winrm get winrm/config/service
```

Etape 7 : Configuration complémentaire du serveur

Si nécessaire, modifiez les règles de pare-feu comme suit :

Windows Server 2008 R2

1. A partir du menu **Outils d'administration**, ouvrez **Pare-feu Windows avec sécurité avancée**.

2. Cliquez avec le bouton droit sur **Règles de trafic entrant** et sélectionnez **Nouvelle règle**.

L'assistant de nouvelle règle s'ouvre.

3. Sélectionnez **Port**, puis cliquez sur **Suivant**.

4. Sur l'écran **Protocole et ports**, sélectionnez **TCP** et entrez le port spécifique, par exemple, 5985 pour HTTP ou 5986 pour HTTPS.

5. Cliquez sur **Suivant**.

6. Sur l'écran **Action**, sélectionnez **Autoriser la connexion** et cliquez sur **Suivant**.

7. Pour **Profil**, vous pouvez sélectionner les trois profils si votre serveur se trouve dans un groupe de travail.

8. Spécifiez un nom pour la règle et cliquez sur **Terminer**.

9. Assurez-vous que la nouvelle règle est activée (la case verte est sélectionnée).

Windows XP

1. Cliquez sur **Démarrer** > **Panneau de configuration**, puis double-cliquez sur **Pare-feu Windows**.

2. Cliquez sur l'onglet **Exceptions**.

3. Cliquez sur **Ajouter un port**.

4. Entrez un **Nom** plus explicite (par exemple, « Règle WinRM ») et le numéro de port (par exemple, 5985 pour HTTP ou 5986 pour HTTPS).

5. Cliquez sur **OK**.

Commandes WinRM utiles

Commande	*Commentaires*
`winrm quickconfig or winrm qc`	Configure WinRM avec les paramètres par défaut.
`winrm enumerate winrm/config/Listener or winrm e winrm/config/Listener`	Permet de vérifier quel écouteur de service est activé et en cours d'écoute sur quel port et adresse IP.
`winrm get winrm/config/Service`	Vérifie la configuration du service WinRM.
`winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`	Supprime un écouteur (dans ce cas, suppression d'un écouteur HTTPS).

Sites Web WinRM utiles

- http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx
- http://technet.microsoft.com/en-us/library/cc782312%28WS.10%29.aspx
- http://msdn.microsoft.com/en-us/library/aa384295%28v=vs.85%29.aspx
- Les articles suivants sur "http://support.microsoft.com :
  - « Configuring WINRM for HTTPS »
  - « Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0, and BITS 4.0) »

Installation de WS-MAN sur un client Windows

Sur Windows Client, suivez les étapes de configuration ci-dessous.

1. Réaliser la configuration HTTP (si vous prévoyez d'utiliser HTTP)
   a. Cliquez sur **Démarrer** (ou appuyez sur la touche Windows) et sélectionnez **Exécuter**.
   b. Saisissez **gpedit.msc** pour ouvrir l'éditeur de stratégie de groupe local.
   c. Dans **Configuration de l'ordinateur**, ouvrez le dossier **Modèles d'administration**, puis le dossier **Composants Windows**.
   d. Sélectionnez **Gestion à distance de Windows (WinRM)**.
   e. Dans **Gestion à distance de Windows (WinRM)**, sélectionnez **Client WinRM**.
   f. Dans **Client WinRM**, double-cliquez sur **Hôtes approuvés**.
   g. Dans **TrustedHostsList**, entrez les noms d'hôte des clients et cliquez sur **OK**. Si tous les clients sont approuvés, entrez "*" uniquement.
   h. Sélectionnez **Service Gestion à distance de Windows**.
   i. Activez **Autoriser l'authentification de base** et cliquez sur **OK**.
   j. Exécutez la commande suivante à partir de l'invite de commande pour tester la connexion :
      `winrm id -remote:<remote machine Hostname or IP Address>`
2. Réaliser la configuration HTTPS (si vous prévoyez d'utiliser HTTPS)

   Après avoir généré un certificat auto-signé, comme décrit dans la section Générer un certificat auto-signé pour Windows Server :, vous pouvez importer le certificat sur le client afin de faciliter la connexion entre le serveur et le client. Assurez-vous que toutes les opérations mentionnées dans la section Générer un certificat auto-signé pour Windows Server : sont terminées, y compris la copie de *hostname.pfx* à un endroit accessible pour le client, avant de passer aux étapes suivantes.

   a. Cliquez sur **Démarrer** (ou appuyez sur la touche Windows) et sélectionnez **Exécuter**.
   b. Saisissez **MMC**, puis cliquez sur **OK**.
   c. Cliquez sur **Fichier** et sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**.
   d. Cliquez sur **Ajouter**.

e. Sélectionnez **Certificats** et cliquez sur **Ajouter**.

f. Sélectionnez **Compte de l'ordinateur** et cliquez sur **Suivant**.

g. Cliquez sur **Terminer**.

h. Cliquez sur **Fermer**, puis sur **OK**.

i. Dans **Certificats (ordinateur local)**, cliquez avec le bouton droit sur **Autorités de certification racines de confiance**, sélectionnez **Toutes les tâches** et sélectionnez **Importer**.

j. Cliquez sur **Suivant** pour lancer l'assistant Importation de certificat.

k. Cliquez sur Parcourir pour sélectionner le fichier .pfx vous avez généré dans Générer un certificat auto-signé pour Windows Server :. Dans la liste **Fichiers par type**, sélectionnez **Echange d'informations personnelles (* .pfxas, *.p12)**, sélectionnez le fichier *hostname.pfx* et cliquez sur **Ouvrir**.

l. Entrez le mot de passe que vous avez attribué à la clé privée et cliquez sur **Suivant**.

3. Configurer HTTPS/SSL de WinRM

Vous pouvez exécuter `winrm` à partir d'un client pour récupérer des informations depuis le serveur via une connexion HTTPS WinRM. Pour tester la connexion WinRM HTTPS/SSL à partir du client, procédez comme suit :

a. Pour extraire les informations sur le système d'exploitation du serveur, entrez la commande suivante :
```
winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername -u:username
-p:password -skipCAcheck
```

b. Pour extraire les informations d'identité WinRM du serveur, entrez la commande suivante :
```
winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
```

c. Pour énumérer les services Windows sur le serveur, entrez la commande suivante :
```
winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -
skipCAcheck
```

Remarque : Il est important d'utiliser le commutateur `-skipCAcheck` dans le test de ligne de commande `winrm`, car le certificat est auto-généré et non importé sur le client. Sinon, le message d'erreur suivant s'affiche : `WSManFault.`

Avec WMI

Aucune configuration particulière n'est requise pour utiliser WMI sur Windows Client. Suivez les étapes décrites dans les sections ci-dessous pour configurer WMI sur Windows Server.

Etape 1 : Configurer la sécurité de l'espace de noms grâce au contrôle WMI

Le contrôle WMI permet de gérer la sécurité de l'espace de noms. La commande ci-dessous permet de démarrer le contrôle WMI à partir de l'invite de commande :

```
wmimgmt
```

Sur les ordinateurs Windows 9x ou Windows NT4 sur lesquels WMI est installé, utilisez cette commande :

```
wbemcntl.exe
```

Vous pouvez également accéder au contrôle WMI et à l'onglet Sécurité comme suit :

1. Cliquez avec le bouton droit sur **Poste de travail** et cliquez sur **Gérer**.
2. Double-cliquez sur **Services et applications**, puis double-cliquez sur **Contrôle WMI**.
3. Cliquez avec le bouton droit de la souris sur **Contrôle WMI** , puis cliquez sur **Propriétés**.
4. Dans Propriétés de contrôle WMI, cliquez sur l'onglet **Sécurité**.
5. Un dossier nommé Root, devancé d'un signe plus (+), devrait être visible. Développez l'arborescence de façon à localiser l'espace de noms pour lequel vous souhaitez définir des autorisations.
6. Cliquez sur **Sécurité**.

   Une liste d'utilisateurs et leurs autorisations s'affiche. Si l'utilisateur est sur la liste, modifiez les autorisations en conséquence. Si l'utilisateur n'est pas dans la liste, cliquez sur **Ajouter** et ajoutez l'utilisateur à partir de l'emplacement (machine locale, domaine, etc.) dans lequel le compte réside.

Remarque : Vous pouvez ajouter ces exportations à la fin de .bash_profile. Ce fichier se trouve dans le répertoire /root.

- Pour visualiser et définir la sécurité de l'espace de noms, l'utilisateur doit avoir les autorisations Sécurité de lecture et Sécurité de modification. Les administrateurs possèdent ces autorisations par défaut et peuvent affecter les autorisations à d'autres comptes utilisateur, le cas échéant.
- Si cet utilisateur doit accéder à l'espace de noms à distance, vous devez sélectionner l'autorisation Appel à distance autorisé.
- Par défaut, les autorisations d'utilisateur définies dans un espace de noms s'appliquent uniquement à cet espace de noms. Si vous voulez que l'utilisateur ait accès à un espace de noms et à tous les sous-espaces de noms de son arborescence, ou aux sous-espaces de noms uniquement, cliquez sur **Avancé**. Cliquez sur **Modifier** et spécifiez la portée de l'accès dans la boîte de dialogue qui s'affiche.

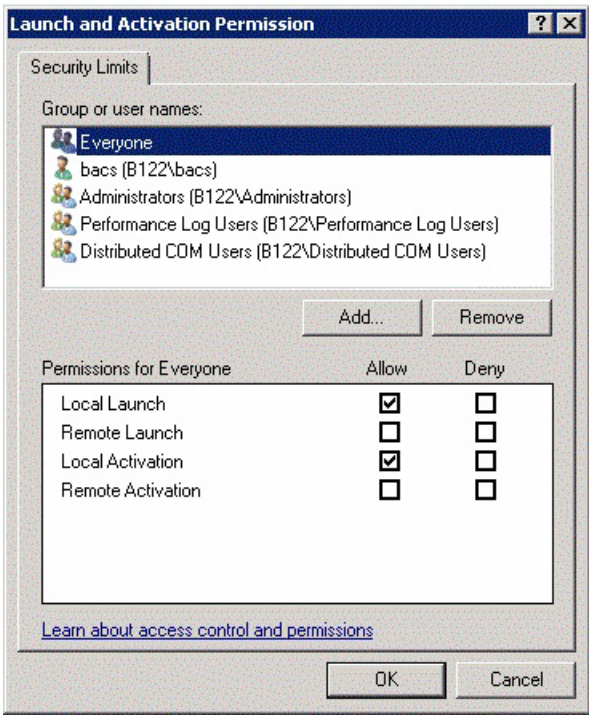
Etape 2 : Autoriser le lancement à distance DCOM et activer l'autorisation

Dans l'environnement de domaine Windows, le compte administrateur de domaine possède le niveau d'autorisation nécessaire pour accéder au composant WMI pour la gestion BACS. Aucune configuration particulière n'est donc nécessaire. Dans une grande entreprise, cependant, un utilisateur qui accède à l'hôte local ou distant grâce à l'interface graphique client BACS4 peut ne pas disposer de l'autorisation du compte administrateur de domaine. Il est nécessaire de configurer l'accès de sécurité WMI sur l'hôte distant pour permettre à l'utilisateur de se connecter en utilisant l'interface graphique client BACS4.

Cette configuration peut s'effectuer facilement grâce à la procédure suivante. Si vous ne disposez pas des autorisations suffisantes pour configurer la sécurité pour l'accès WMI, contactez votre administrateur réseau.

1. Cliquez sur **Démarrer**, puis sur **Exécuter**, saisissez **DCOMCNFG** et cliquez sur **OK**.
2. La boîte de dialogue Services de composants s'affiche.
3. Ouvrez **Services de composants**, puis **Ordinateurs**.
4. Cliquez avec le bouton droit sur **Poste de travail**, puis sur **Propriétés**.
5. Dans **Propriétés de l'ordinateur**, cliquez sur l'onglet **Sécurité COM**.
6. Dans **Autorisations d'exécution et d'activation**, cliquez sur **Modifier les limites**.
7. Procédez comme suit si votre nom ou votre groupe n'apparaît pas dans la liste **Noms d'utilisateur ou de groupes**.
   a. Dans la boîte de dialogue Autorisation d'exécution, cliquez sur **Ajouter**.
   b. Dans la boîte de dialogue Sélectionner les utilisateurs, les ordinateurs ou les groupes, ajoutez votre nom et le groupe dans la zone **Entrez les noms des objets à sélectionner**, puis cliquez sur **OK**.
   c. Dans la boîte de dialogue Autorisation d'exécution, sélectionnez votre utilisateur et votre groupe dans la liste **Noms d'utilisateur ou de groupes**.
   d. Dans la zone **Autorisations aux utilisateurs**, sélectionnez **Autoriser** pour **Exécution à distance** et **Activation à distance**, puis cliquez sur **OK**.

Figure 8 : Autorisation d'exécution et d'activation



Pour plus d'informations, reportez-vous à Securing a Remote WMI Connection sur le site Microsoft Developer Network.

Configuration spéciale pour WMI sur différents systèmes

Sous Windows Vista et Windows 7, afin de permettre à tous les utilisateurs du groupe administrateur de se connecter grâce à l'espace de noms WMI, l'utilisateur peut avoir à modifier le fichier LocalAccountTokenFilterPolicy selon le besoin.

Section 13 : Utilisation de Broadcom Advanced Control Suite 4

Présentation de l'application Broadcom Advanced Control Suite

Broadcom Advanced Control Suite (BACS) est un utilitaire intégré qui fournit des informations utiles sur toutes les cartes réseau installées sur votre système. BACS vous permet également d'effectuer des tests détaillés, des diagnostics et des analyses de toutes les cartes réseau, ainsi que de visualiser et modifier les valeurs de propriétés et les statistiques relatives au trafic de tous les objets réseau. BACS fonctionne sur les systèmes d'exploitation Windows et Linux.

Broadcom Advanced Server Program (BASP), qui s'exécute au sein de BACS, est utilisé pour la configuration d'équipes, l'équilibrage de charge, la tolérance aux pannes et les réseaux locaux virtuels (VLAN). La fonctionnalité BASP est disponible seulement pour les systèmes qui utilisent au moins une carte réseau Broadcom. BASP fonctionne uniquement sur les systèmes d'exploitation Windows.

Remarque : Certaines fonctions de l'application BACS ne s'appliquent qu'à certaines cartes. Une même instance de BACS peut être utilisée pour communiquer avec plusieurs hôtes ou types de carte. Ce document traite donc de toutes les fonctionnalités de BACS.

L'application BACS comprend une interface utilisateur graphique et une interface de ligne de commande (BACSCLI). L'interface graphique BACS et BACSCLI peuvent fonctionner sur les gammes de systèmes d'exploitation suivantes :

- Windows
- Windows Server
- Serveur Linux

Pour obtenir des informations sur les dernières versions de système d'exploitation prises en charge, reportez-vous à la documentation de la version fournie avec votre logiciel.

Initialisation de l'application Broadcom Advanced Control Suite

Cliquez sur **Broadcom Control Suite 4** dans le Panneau de configuration ou sur l'icône BACS dans la barre des tâches en bas du bureau Windows ou Windows Server.

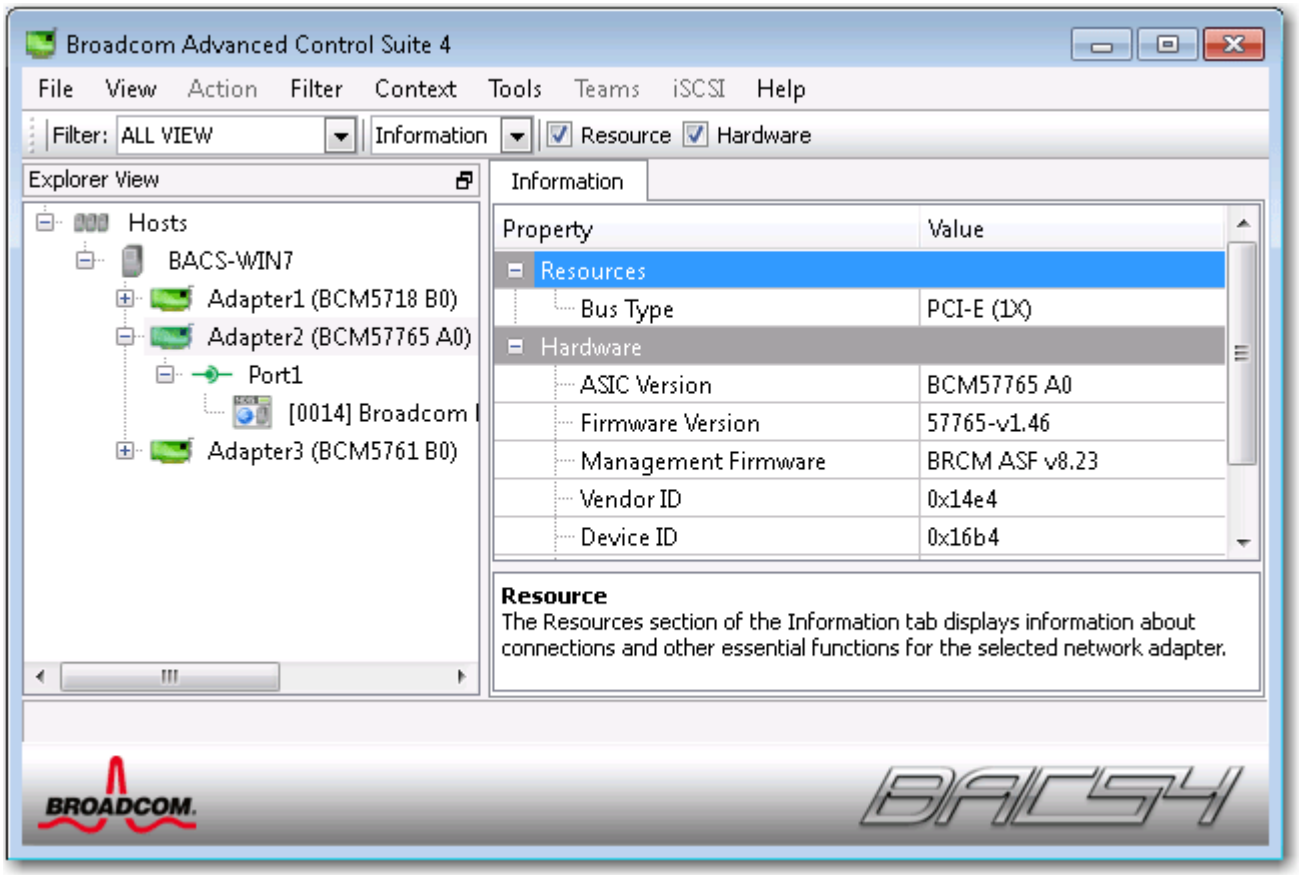
Sous les systèmes Linux, vous pouvez double-cliquer sur l'icône de bureau BACS4, ou accéder au programme BACS à partir de la barre des tâches sous **Outils système**. (Si le lancement de BACS sur un système Linux vous pose problème, reportez-vous à la rubrique associée dans Dépannage de BACS.)

Interface BACS

L'interface BACS comprend les éléments suivants :

- Panneau de la vue Explorateur
- Outil de sélection de vue contextuelle
- Panneau de l'onglet Contexte
- Barre de menus
- Panneau de description

Par défaut, le panneau de la vue Explorateur est ancré et épinglé sur la gauche de la fenêtre principale, le panneau de l'onglet Contexte sur la droite, l'outil de sélection de vue contextuelle sous la barre de menus et le panneau de description sous le panneau de l'onglet Contexte. Vous pouvez déplacer les séparateurs de panneaux pour modifier la taille des panneaux.



Panneau de la vue Explorateur

Vous pouvez ancrer et épingler le panneau de la vue Explorateur sur la gauche, la droite, le haut ou le bas de la fenêtre principale.

Le panneau de la vue Explorateur répertorie les objets pouvant être consultés, analysés, testés ou configurés dans BACS. Lorsqu'un élément est sélectionné dans le panneau de la vue Explorateur, les onglets affichant les informations et options disponibles pour cet élément s'affichent dans le panneau de l'onglet Contexte.

L'organisation de ce panneau est conçue pour présenter les objets gérables selon la même hiérarchie que les pilotes et sous-composants. Cela simplifie la gestion des divers éléments du contrôleur d'interface réseau convergente. Au niveau le plus élevé de la hiérarchie se trouve le conteneur hôte, qui répertorie tous les hôtes gérés par BACS. En dessous des hôtes, on trouve les cartes réseau installées avec les éléments gérables tels que les ports physiques et les pilotes NDIS et en dessous des cartes réseaux, les spécifications iSCSI.

Dans le panneau de la vue Explorateur, chaque icône indique l'état du périphérique en regard duquel elle est située. Une icône apparaissant comme « Normal » en regard d'un périphérique indique que ce périphérique est connecté et actif.

- **X.** Une croix (« X ») rouge apparaissant sur l'icône d'un périphérique indique que ce périphérique n'est actuellement pas connecté au réseau.
- **Icône grisée.** Si l'icône d'un périphérique est grisée, cela signifie que ce périphérique est actuellement désactivé.

Outil de sélection de vue contextuelle

L'outil de sélection de vue contextuelle se trouve sous la barre de menus et inclut les catégories de filtres et d'onglets. Vous pouvez développer et réduire les catégories s'affichant dans des onglets dans le panneau de l'onglet Contexte ou afficher une catégorie en cochant la case en regard de son nom.

Vue Filtre

Dans un environnement à hôtes multiples utilisant plusieurs C-NIC, le nombre d'éléments gérables par carte peut s'avérer important. Il devient alors difficile d'afficher, de configurer et de gérer tous ces éléments. Le filtre vous permet de sélectionner une fonction de périphérique particulière. Voici les différentes vues de filtre:

- Tous
- VUE EQUIPE
- VUE NDIS
- AFFICHER iSCSI
- VUE CIBLE iSCSI

Panneau de l'onglet Contexte

Le panneau de l'onglet Contexte affiche tous les paramètres pouvant être consultés pour l'objet sélectionné dans le panneau de la vue Explorateur. Selon le type de paramètre, les paramètres sont regroupés par onglets et catégories. Les onglets disponibles sont les suivants : Information, Configuration, Diagnostics et Statistiques. L'interface de BACS étant intuitive, seuls les paramètres applicables à l'objet sélectionné peuvent être affichés ou configurés dans le panneau de l'onglet Contexte.

Barre de menus

La barre de menus inclut les éléments suivants (les éléments de menu étant contextuels, certains éléments ne sont pas toujours disponibles) :

Menu Fichier

- Enregistrer l'équipe sous : Enregistre les configurations de l'équipe actuelle sur un fichier.
- Restaurer l'équipe : Restaure les configurations d'équipe enregistrées dans un fichier.

Menu Action

- Supprimer hôte : Supprime l'hôte sélectionné.
- Actualiser hôte : Actualise l'hôte sélectionné.

Menu Afficher

- Vue explorateur : Affiche/masque le volet Vue explorateur.
- Barre d'outils : Affiche/masque la barre d'outils.
- Barre d'état : Affiche/masque la barre d'état.
- Logo Broadcom : Affiche/masque le logo Broadcom dans BACS pour optimiser l'espace d'affichage d'informations.

Menu Outils

- Options : Permet de configurer les préférences de BACS.

Equipes (Windows uniquement)

- Créer une équipe : Crée une équipe à l'aide de l'Assistant de regroupement ou du mode Avancé.
- Gérer des équipes : Gère les équipes existantes à l'aide de l'Assistant de regroupement ou du mode Avancé.

Panneau de description

Le panneau de description fournit des informations, des instructions de configuration et des options pour le paramètre sélectionné dans le panneau de l'onglet Contexte.

Configuration des préférences dans Windows

Pour activer ou désactiver l'icône BACS dans la barre des tâches sous Windows

Sur les systèmes Windows, l'installation du programme BACS place une icône dans la zone de notification de la barre des tâches Windows. Pour activer ou désactiver cette icône, utilisez la fenêtre Options.

1. Dans le menu **Outils**, sélectionnez **Options**.
2. Activez ou désactivez l'option **Activer BACSTray** (cette option est activée par défaut).
3. Cliquez sur **OK**.

Choix du mode de regroupement sous Windows

1. Dans le menu **Outils**, sélectionnez **Options**.
2. Sélectionnez **Mode Expert** si vous ne souhaitez pas utiliser l'Assistant pour créer des équipes. Sinon, sélectionnez **Mode Assistant**.
3. Cliquez sur **OK**.

Définition de la fréquence d'actualisation de la vue Explorateur sous Windows

1. Dans le menu **Outils**, sélectionnez **Options**.
2. Sélectionnez **Auto** pour définir la fréquence d'actualisation de la vue Explorateur sur 5 secondes. Pour définir la fréquence de votre choix en secondes, sélectionnez Personnalisé.
3. Cliquez sur **OK**.

Connexion à un hôte

Vous pouvez ajouter un ou plusieurs hôtes Windows ou Linux à gérer dans BACS.

Pour ajouter un hôte local

1. Dans le menu **Action**, cliquez sur **Ajouter hôte**.
2. Pour les hôtes Windows et Linux, ne modifiez pas les paramètres par défaut. Il n'est pas nécessaire de renseigner les champs **Nom d'utilisateur** et **Mot de passe** lors de la connexion à l'hôte local.
3. Si vous souhaitez que BACS conserve les informations sur l'hôte, sélectionnez **Persistance**.
4. Cliquez sur **OK**. Vous pouvez désormais utiliser BACS pour consulter des informations sur l'hôte et le gérer.

Pour ajouter un hôte distant

1. Dans le menu **Action**, cliquez sur **Ajouter hôte**.
2. Tapez le nom ou l'adresse IP de l'hôte distant dans le champ **Hôte**.
3. Sélectionnez le protocole dans la liste **Protocole**. Les options de protocole pour Windows sont **WMI**, **WSMan** ou **Essayer tout**. Les options de protocole pour Linux sont **CimXML**, **WSMan** ou **Essayer tout**. L'option **Essayer tout** force le client de l'interface à essayer toutes les options.
4. Choisissez entre **HTTP** et **HTTPS** pour une sécurité renforcée.
5. Tapez la valeur de **numéro de port** utilisée pour configurer l'hôte si elle est différente de la valeur par défaut de **5985**.
6. Tapez le **nom d'utilisateur** et le **mot de passe**.
7. Si vous souhaitez que BACS conserve les informations sur l'hôte, sélectionnez **Persistance**. L'hôte s'affiche dans le panneau de la vue Explorateur à la réouverture de BACS. Il n'est dès lors plus nécessaire de saisir l'adresse IP ou le nom de l'hôte lors de la connexion à celui-ci. Pour des raisons de sécurité, vous devez saisir à chaque fois le **nom d'utilisateur** et le **mot de passe**.
8. Cliquez sur **OK**.

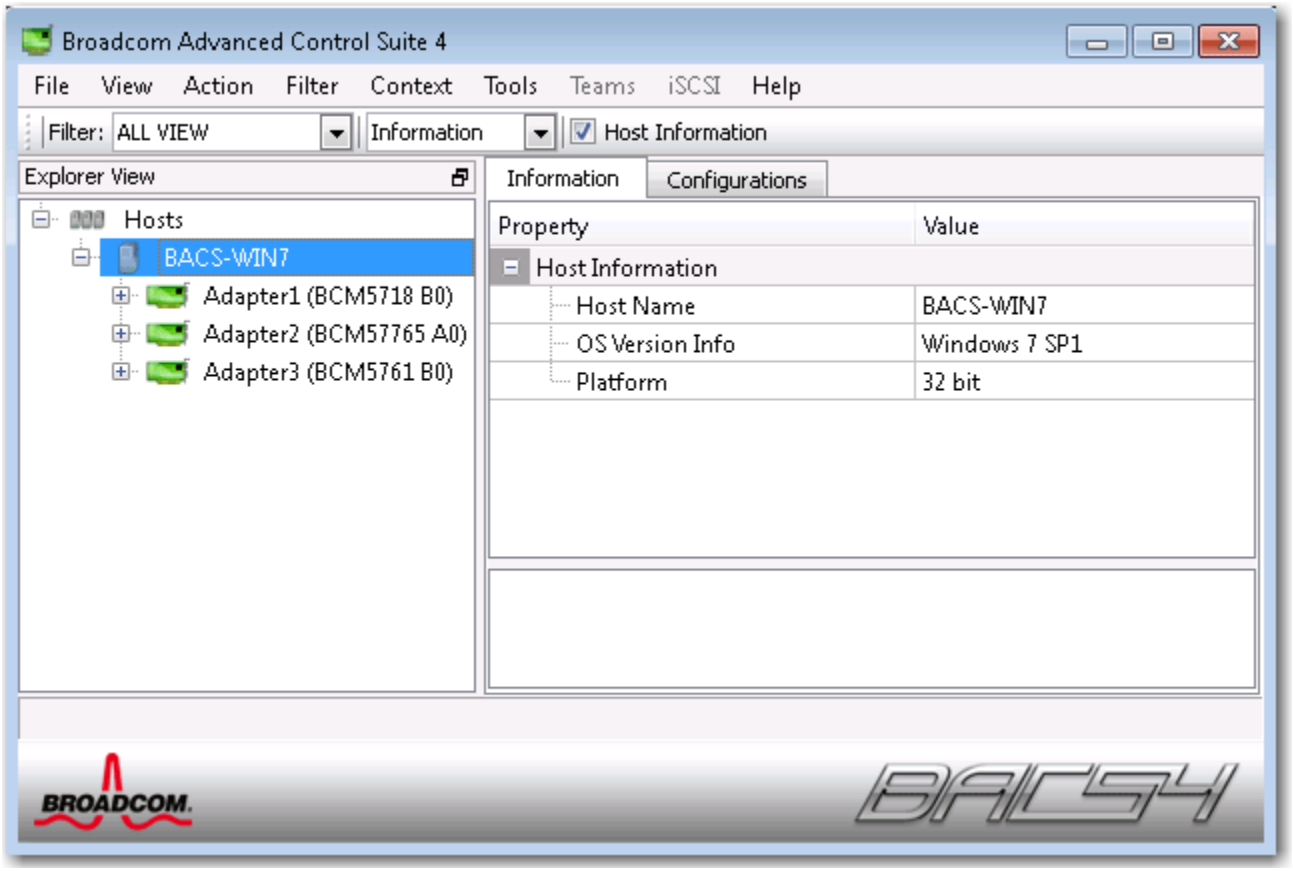
Gestion des hôtes

Au niveau des hôtes, vous pouvez consulter des informations et configurer des paramètres via les onglets suivants :

- Informations
- Configuration

Pour consulter des informations sur un hôte

Sélectionnez l'hôte dans le panneau de la **vue Explorateur**, puis sélectionnez l'onglet **Informations** pour consulter des informations sur l'hôte.



Onglet Informations : Informations sur l'hôte

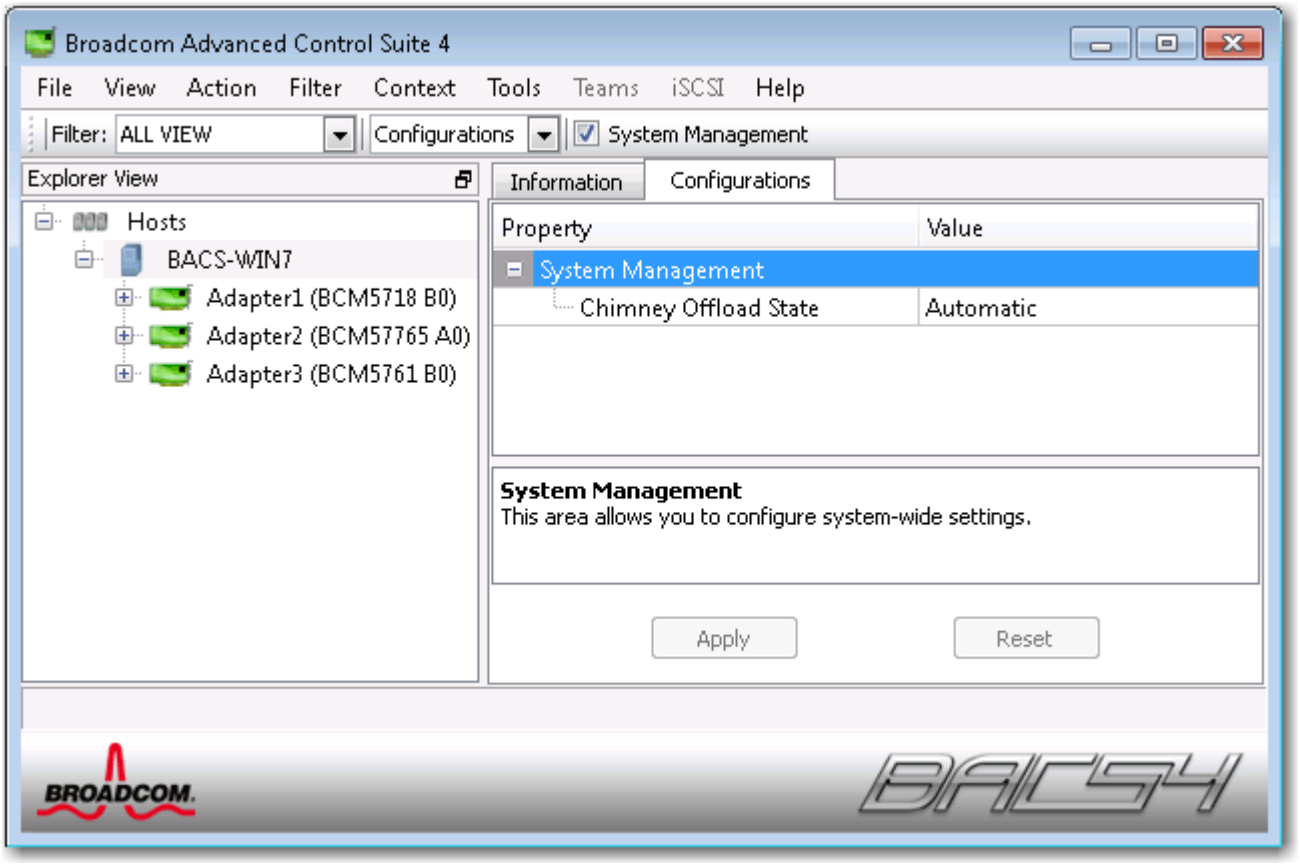
Nom d'hôte. Affiche le nom de l'hôte.

Infos sur la version de l'OS. Indique le nom et la version du système d'exploitation.

Plate-forme. Indique la plate-forme d'architecture matérielle (par exemple, 32 bits ou 64 bits)

Pour configurer un hôte

Sélectionnez l'hôte dans le panneau de la **vue Explorateur**, puis sélectionnez l'onglet **Configuration** pour configurer des paramètres applicables à l'hôte.



Gestion des cartes réseau

Les cartes réseau installées s'affichent un niveau en dessous de l'hôte dans l'arborescence du panneau de la vue Explorateur. Au niveau de la carte réseau, vous pouvez consulter des informations et configurer des paramètres via les onglets suivants :

- Informations
- Configuration

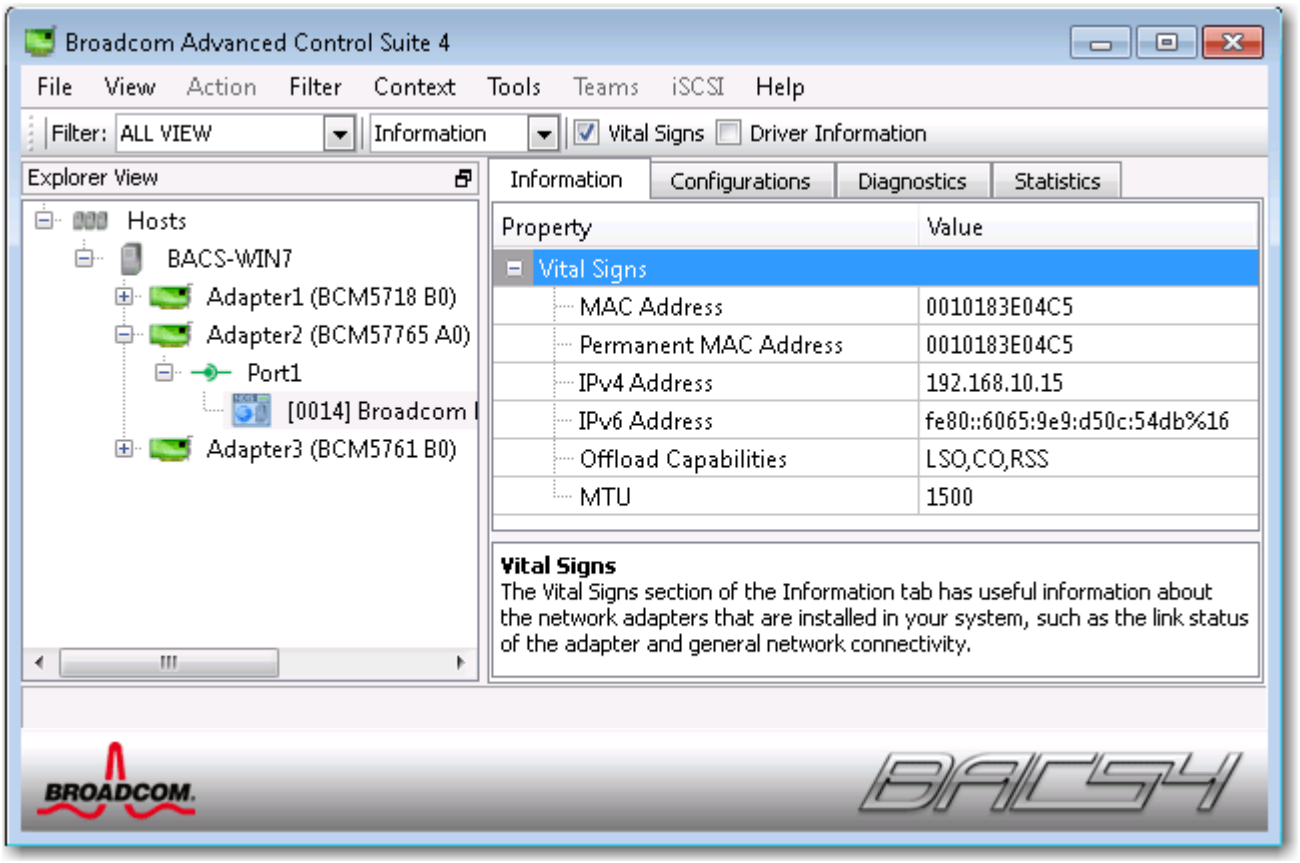
Pour consulter des informations sur une carte

La section **Signe vital** de l'onglet **Informations** présente des informations utiles sur les cartes réseau installées sur votre système, telles que leur état de liaison et la connectivité réseau générale.

Sélectionnez la carte réseau dans le panneau de la **vue Explorateur**, puis sélectionnez l'onglet **Informations** pour consulter des informations sur la carte.

Remarque :

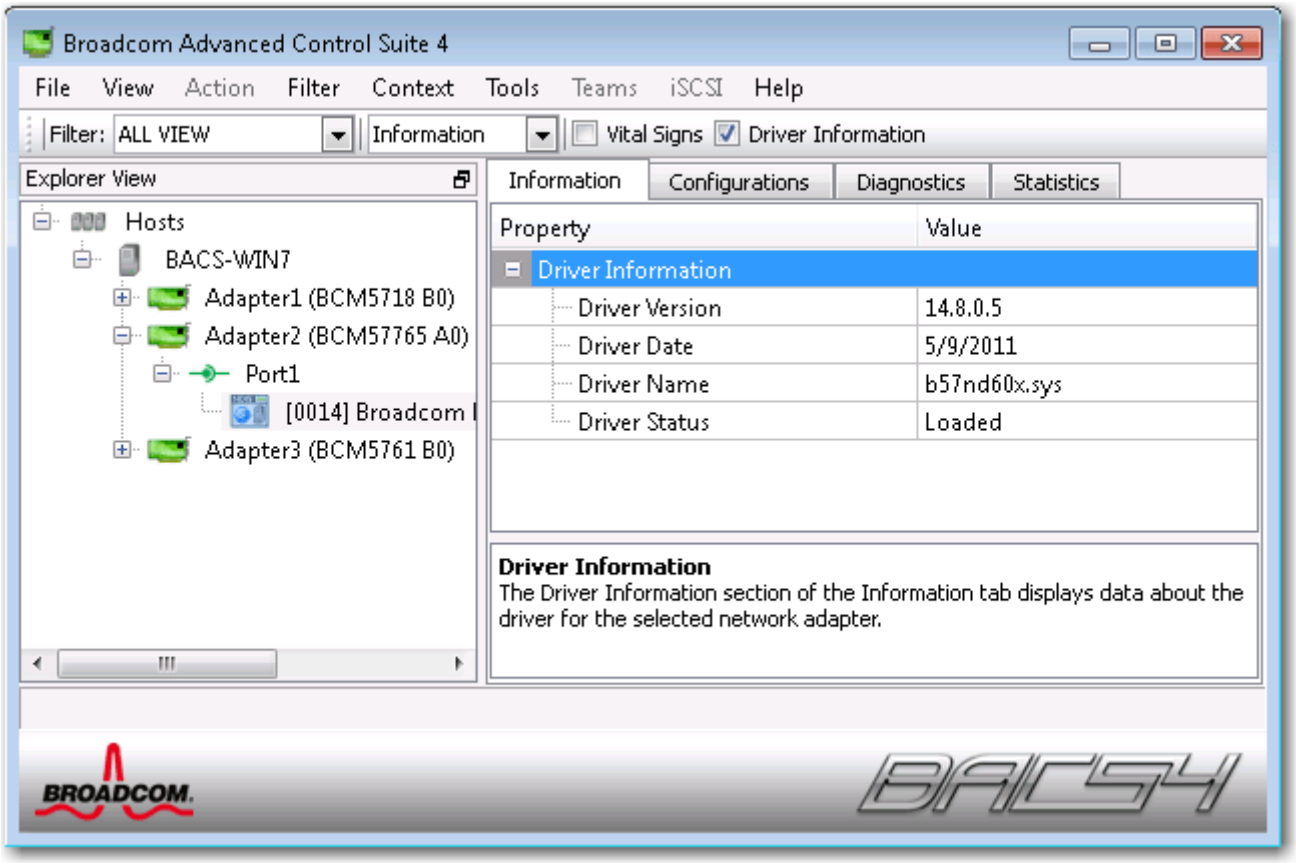
- Les informations relatives aux cartes réseau Broadcom peuvent s'avérer plus complètes que celles relatives aux cartes réseau tierces.
- Toutes les informations peuvent ne pas être disponibles pour certaines cartes réseau Broadcom.


Broadcom Advanced Control Suite 4
File View Action Filter Context Tools Teams iSCSI Help
Filter: ALL VIEW
Information
Vital Signs
Driver Information
Explorer View
Hosts
BACS-WIN7
Adapter1 (BCM5718 B0)
Adapter2 (BCM57765 A0)
Port1
[0014] Broadcom
Adapter3 (BCM5761 B0)
Information
Configurations
Diagnostics
Statistics
Property
Value
Vital Signs
MAC Address
0010183E04C5
Permanent MAC Address
0010183E04C5
IPv4 Address
192.168.10.15
IPv6 Address
fe80::6065:9e9:d50c:54db%16
Offload Capabilities
LSO,CO,RSS
MTU
1500
Vital Signs
The Vital Signs section of the Information tab has useful information about the network adapters that are installed in your system, such as the link status of the adapter and general network connectivity.
BROADCOM.
BACS4

Affichage des informations relatives aux pilotes

La section d'**informations sur les pilotes** de l'onglet **Informations** affiche des données relatives au pilote de la carte réseau sélectionnée.

Pour afficher les informations de pilote pour une carte réseau installée, cliquez sur le nom de la carte souhaitée dans le panneau de la vue Explorateur, puis cliquez sur l'onglet **Informations**.



Etat du pilote. Etat du pilote de la carte.

- **Chargé**. Mode d'exploitation normal. Le pilote de la carte a été chargé par Windows et fonctionne.
- **Non chargé**. Le pilote associé à la carte n'a pas été chargé par Windows.
- **Non disponible**. Impossible d'obtenir une valeur du pilote associé à la carte.

Nom du pilote. Nom de fichier du pilote de la carte.

Version du pilote. Version actuelle du pilote de la carte.

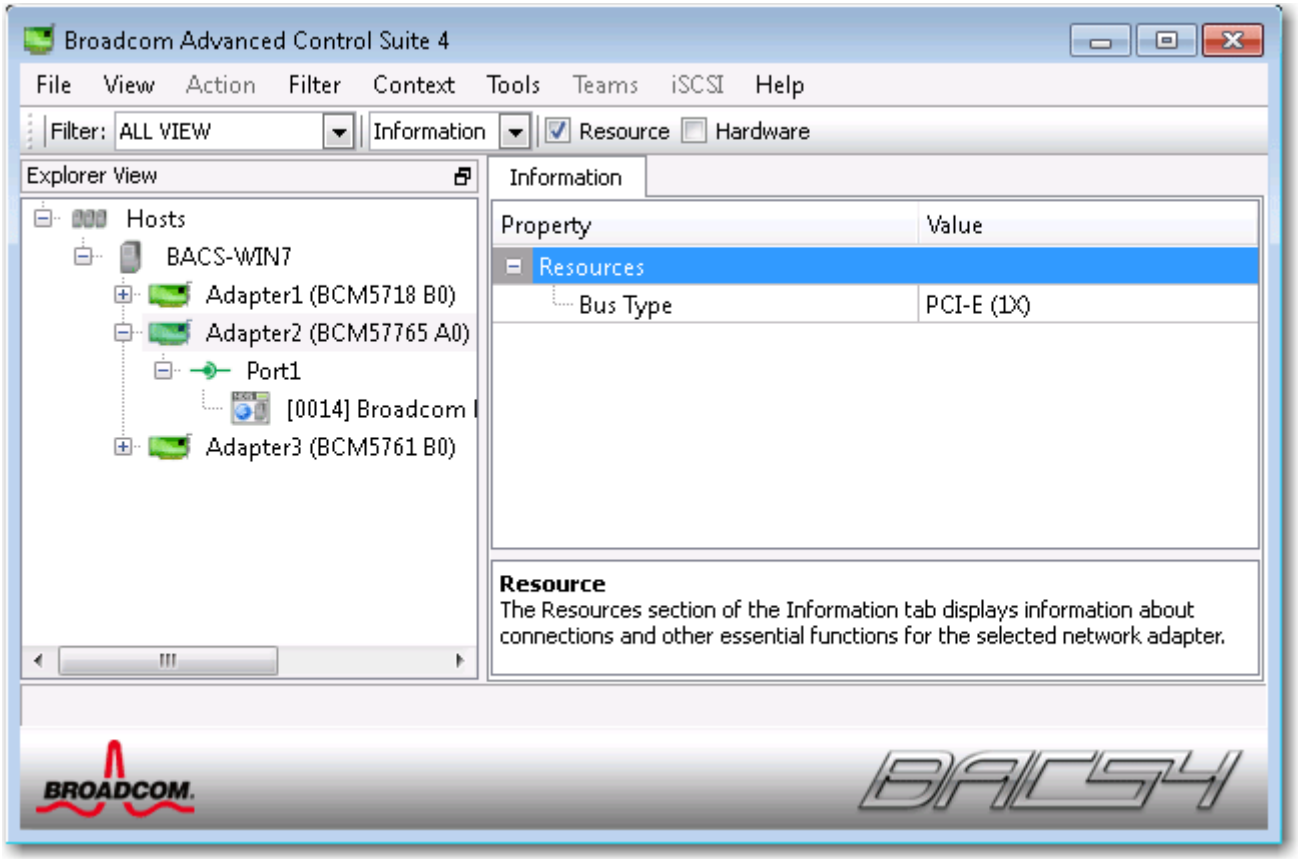
Date du pilote. Date de création du pilote de la carte.

Affichage des informations relatives aux ressources

La section **Ressources** de l'onglet **Informations** affiche des informations sur les connexions et autres fonctions essentielles de la carte réseau sélectionnée.

Pour afficher les informations de ressources pour une carte réseau installée, cliquez sur le nom de la carte souhaitée dans le panneau de la vue Explorateur, puis cliquez sur l'onglet **Informations**.

Remarque : Toutes les informations peuvent ne pas être disponibles pour certaines cartes réseau Broadcom.



Type de bus. Type d'interconnexion entrée/sortie (E/S) utilisée par la carte.

Numéro de logement. Numéro de logement où se trouve la carte sur la carte mère. Cet élément n'est pas disponible pour les cartes de type PCI Express.

Vitesse du bus (MHz). Fréquence de l'horloge du bus utilisée par la carte. Cet élément n'est pas disponible pour les cartes de type PCI Express.

Largeur de bus (bit). Nombre de bits pouvant être transférés en même temps par le bus vers et à partir de la carte. Cet élément n'est pas disponible pour les cartes de type PCI Express.

Numéro de bus. Indique le numéro du bus où la carte est installée.

Numéro de périphérique. Numéro attribué à la carte par le système d'exploitation.

Numéro de fonction. Numéro de port de la carte. Pour une carte à port unique, le numéro de fonction est 0. Pour une carte à port double, le numéro de fonction pour le premier port est zéro et le numéro de fonction pour le deuxième est 1.

Demande d'interruption. Numéro de ligne d'interruption associé à la carte. Les numéros valides sont compris entre 2 et 25.

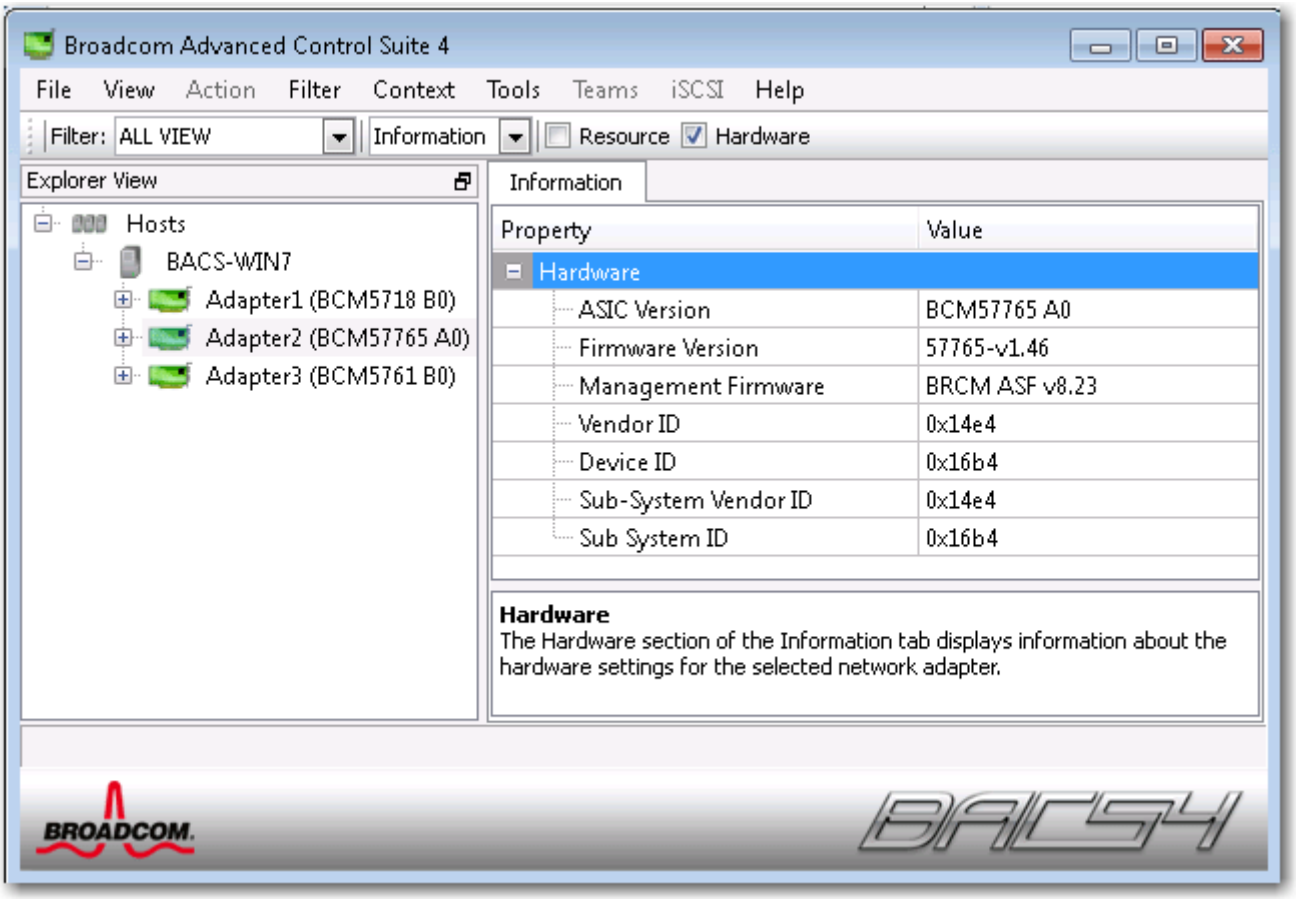
Adresse de mémoire. Adresse topographiée en mémoire attribuée à la carte. Cette valeur ne peut jamais être nulle.

Affichage des informations relatives au matériel

La section Matériel de l'onglet **Informations** affiche des données relatives aux paramètres matériels de la carte réseau sélectionnée.

Pour afficher les informations matérielles pour une carte réseau installée, cliquez sur le nom de la carte souhaitée dans le panneau de la vue Explorateur, puis cliquez sur l'onglet Informations.

Remarque : Toutes les informations peuvent ne pas être disponibles pour certaines cartes réseau Broadcom.



Version ASIC. Version de la puce de la carte Broadcom (ces informations ne sont pas disponibles pour les cartes tierces).

Version du microprogramme. Version du microprogramme de la carte Broadcom (ces informations ne sont pas disponibles pour les cartes tierces). Ces informations sont disponibles uniquement pour les cartes Broadcom NetXtreme.

ID du constructeur. L'ID du constructeur.

ID du périphérique. ID de la carte.

ID du constructeur du sous-système. L'ID du constructeur du sous-système.

ID du sous-système. ID du sous-système.

Test du réseau

L'option **Test de réseau** de l'onglet **Diagnostic** vous permet de vérifier la connectivité réseau IP. Ce test vérifie si le pilote est installé correctement et contrôle la connectivité à une passerelle ou à une autre adresse IP spécifiée appartenant au même sous-réseau. Le test de réseau envoie des paquets ICMP à des systèmes distants via TCP/IP et attend une réponse.

Remarque : L'option de test de réseau n'est pas disponible pour les cartes regroupées en équipe (voir Configuration de regroupement).

Pour exécuter le test du réseau

1. Dans le panneau de la vue Explorateur, cliquez sur le nom de la carte à tester.
2. Dans la liste de **sélection de test à exécuter**, sélectionnez **Test de réseau**. Si l'option **Test de réseau** n'est pas disponible, dans l'onglet **Contexte** situé à droite de la fenêtre, sélectionnez **Diagnostic**, puis **Test de réseau**.
3. Pour modifier l'adresse IP de destination, sélectionnez **Adresse IP de destination du ping**. Dans la fenêtre Test de réseau, entrez une adresse IP de destination, puis cliquez sur **OK**.
4. Cliquez sur **Test**.

Les résultats du test de réseau s'affichent dans le champ **Etat**.

Exécution des tests de diagnostic

L'option **Tests de diagnostic** de l'onglet **Diagnostic** vous permet de vérifier l'état des composants physiques d'une carte réseau Broadcom. Vous pouvez lancer ces tests manuellement ou laisser BACS 3 les effectuer en continu. Si ces tests sont effectués en continu, le nombre de réussites et d'échecs indiqués dans le champ **Résultat** de chaque test augmente à chaque fois qu'ils sont exécutés. Par exemple, si un test est exécuté quatre fois sans échouer, la valeur affichée dans le champ **Résultat** est de 4/0 pour ce test. Cela dit, si le test réussit trois fois et échoue une fois, la valeur affichée dans le champ **Résultat** sera 3/1.

Remarque :

- Vous devez disposer de privilèges d'administrateur pour effectuer des tests de diagnostic.
- L'exécution de ces tests entraîne une rupture temporaire de la connexion au réseau.
- Chaque test n'est pas pris en charge par toutes les cartes Broadcom.

Pour exécuter les tests de diagnostic de manière ponctuelle

1. Cliquez sur le nom de la carte à tester dans le panneau de la vue Explorateur, puis sélectionnez l'onglet Diagnostics.
2. Dans la liste **Sélectionnez un test à exécuter**, sélectionnez **Tests de diagnostic**.
3. Sélectionnez les tests de diagnostic que vous souhaitez exécuter. Cliquez sur **Tout sélectionner** pour sélectionner tous les tests ou sur **Tout effacer** pour annuler toutes les sélections de tests.
4. Sélectionnez le nombre d'exécutions des tests dans **Nombre de boucles**.
5. Cliquez sur **Exécuter test(s)**.
6. Cliquez sur **Oui** lorsque le message indiquant que la connexion réseau va subir une rupture temporaire s'affiche. Les résultats s'affichent dans le champ **Résultat** de chaque test.

Registres de contrôle. Ce test vérifie les possibilités de lecture et d'écriture des registres de la carte réseau, en écrivant diverses valeurs dans les registres et en vérifiant les résultats. Le pilote de la carte utilise ces registres pour exécuter des tâches de réseau, telles que l'envoi et la réception d'informations. Si le test échoue, le périphérique ne fonctionne peut-être pas correctement.

Registres MII. Ce test vérifie les capacités de lecture et d'écriture des registres de la couche physique (PHY). La couche physique permet de contrôler les signaux électriques du circuit et de configurer des vitesses de transmission du réseau, telles que 1 000 Mbit/s.

EEPROM. Ce test vérifie le contenu de la mémoire EEPROM en lisant une partie de celle-ci et en calculant la somme de contrôle. Le test échoue si la somme de contrôle calculée ne correspond pas à la valeur enregistrée dans la mémoire EEPROM. Une mise à niveau de l'image EEPROM ne nécessite pas de changement de code pour ce test.

Mémoire interne. Ce test vérifie que la mémoire interne de la carte fonctionne correctement. Il implique l'inscription de valeurs structurées en mémoire et la lecture des résultats en retour et échoue si une valeur erronée est renvoyée. Le périphérique ne peut pas fonctionner si sa mémoire interne ne fonctionne pas correctement.

Unités centrales sur puce. Ce test vérifie le bon fonctionnement des unités centrales internes au sein de la carte.

Interruption. Ce test vérifie que le pilote NDIS peut recevoir des interruptions de la carte.

Bouclage - MAC. Ce test vérifie que le pilote NDIS peut envoyer et recevoir des paquets de la carte.

Bouclage - PHY. Ce test vérifie que le pilote NDIS peut envoyer et recevoir des paquets de la carte.

Test LED (Test des DEL). Ce test fait clignoter 5 fois tous les voyants des ports afin d'identifier la carte.

Analyse des câbles

L'option **Analyse de câble** de l'onglet **Diagnostic** vous permet de contrôler l'état de chaque paire de fils d'une connexion par câble Ethernet de catégorie 5 au sein d'un réseau Ethernet. L'analyse évalue la qualité du câble et la compare aux caractéristiques de la norme de conformité IEEE 802.3ab.

Remarque :

- Vous devez disposer des privilèges d'administrateur pour réaliser le test d'analyse de câble.
- Une interruption temporaire de la connexion au réseau se produit au cours d'une analyse.
- Le test d'analyse de câble des cartes Broadcom NetXtreme peut être exécuté uniquement sur des connexions à vitesse de liaison Gigabit ou lorsqu'aucune connexion n'est établie.
- Cette option n'est pas disponible pour toutes les cartes réseau Broadcom.

Pour exécuter une analyse de câble

1. Connectez le câble à un port situé sur un commutateur où le port et les réglages du pilote Vitesse et duplex sont réglés sur **Auto**.
2. Dans le panneau de la vue Explorateur, cliquez sur le nom de la carte à tester.
3. Dans la liste de **sélection de test à exécuter**, sélectionnez **Analyse de câble**. Si l'option **Analyse de câble** n'est pas disponible, dans l'onglet **Vue Contexte** situé à droite de la fenêtre, sélectionnez **Diagnostic**, puis **Analyse de câble**.
4. Cliquez sur **Exécuter**.
5. Cliquez sur **Oui** lorsque le message indiquant que la connexion réseau va subir une rupture temporaire s'affiche.

Distance. Longueur de câble valide, exprimée en mètres (sauf lorsque le résultat Bruit est renvoyé).

Etat. Il s'agit du type de liaison de la paire de câbles concernée.

- **Bon**. Bon signal du câble/de la carte de circuit imprimé, mais aucune liaison Gigabit.
- **Croisé**. Broches associées ou interférence sur au moins deux signaux du câble/de la carte de circuit imprimé.
- **Ouvert**. Une broche ou les deux sont ouvertes pour une paire torsadée.
- **Court**. Deux broches de la même paire torsadée sont associées.
- **Bruit**. Présente de bruit persistant (probablement dû au 10/100 forcé).
- **Go - Lien**. La liaison Gigabit fonctionne correctement.
- **N/A**. L'algorithme n'est pas parvenu à établir une conclusion.

raccourci. Vitesse de connexion et mode duplex.

Etat. Etat suivant l'exécution du test : terminé ou en échec.

Il existe de nombreux facteurs qui peuvent affecter les résultats du test :

- **Partenaire de liaison**. Les divers fabricants de commutateurs et de concentrateurs implémentent différents PHY. Certains PHY ne sont pas conformes IEEE.
- **Qualité du câble**. Les catégories 3, 4, 5 et 6 peuvent avoir une incidence sur les résultats du test.
- **Interférences électriques**. L'environnement du test peut avoir une incidence sur les résultats.

Définition des propriétés de la carte

La section **Avancé** de l'onglet **Configurations** permet d'afficher et de modifier les propriétés disponibles de la carte sélectionnée. Les propriétés disponibles et leurs paramètres respectifs sont décrits ci-dessous.

Remarque :

- Vous devez disposer de privilèges d'administrateur pour modifier les valeurs d'une propriété.
- La liste des propriétés disponibles pour votre carte spécifique peut être différente.
- Toutes les propriétés peuvent ne pas être disponibles sur certaines cartes réseau Broadcom.

Pour définir les propriétés de la carte

1. Cliquez sur le nom de la carte dans le panneau de la vue Explorateur, puis sur l'onglet **Configurations**.
2. Dans la section **Gestion OOB**, sélectionnez la propriété que vous souhaitez définir.
3. Pour modifier la valeur d'une propriété, cliquez sur un élément dans la liste de cette propriété ou saisissez une nouvelle valeur, le cas échéant (les options de sélection sont différentes pour chaque propriété).
4. Cliquez sur **Appliquer** pour confirmer les modifications de toutes les propriétés. Cliquez sur **Redéfinir** pour restaurer les valeurs d'origine des propriétés.

802.1p QOS. Permet d'activer la *qualité de service*, une spécification IEEE (Electrical and Electronics Engineering) traitant différemment les divers types de trafic réseau afin d'assurer les niveaux nécessaires de fiabilité et les délais d'attente requis en fonction du type de trafic. Cette propriété est désactivée par défaut. Si la norme QoS n'est pas prise en charge par l'infrastructure du réseau, n'activez pas cette propriété. Dans le cas contraire, des problèmes pourraient en effet survenir.

Contrôle de flux :. Permet d'activer ou de désactiver la réception ou la transmission des trames PAUSE. Les trames PAUSE permettent à la carte de réseau et au commutateur de réguler la vitesse de transmission. L'équipement recevant la trame PAUSE s'arrête momentanément de transmettre.

- **Auto** (valeur par défaut) La réception et la transmission des trames PAUSE sont optimisées.
- **Désactiver**. La réception et la transmission des trames PAUSE sont désactivées.
- **Rx PAUSE**. La réception des trames PAUSE est activée.
- **Rx/Tx PAUSE**. La réception et la transmission des trames PAUSE sont activées.
- **Tx PAUSE**. La transmission des trames PAUSE est activée.

Vitesse et duplex. La propriété Vitesse et duplex permet d'adapter la vitesse de connexion au réseau et au mode. Notez que le mode Duplex intégral permet à l'adaptateur de transmettre et de recevoir simultanément des données du réseau.

- **10 Mb Full** (10 Mbit intégral). Règle la vitesse sur 10 Mbit/s et définit le mode sur Duplex intégral.
- **10 Mb Half** (10 Mbit semi). Règle la vitesse sur 10 Mbit/s et définit le mode sur Semi-duplex.
- **100 Mb Full** (100 Mbit intégral). Règle la vitesse sur 100 Mbit/s et définit le mode sur Duplex intégral.
- **100 Mb Half** (100 Mbit semi). Règle la vitesse sur 100 Mbit/s et définit le mode sur Semi-duplex.
- **Auto** (valeur par défaut) Règle la vitesse et le mode de façon à optimiser la connexion au réseau (recommandé).

Remarque :

- Auto correspond à l'option recommandée. Elle permet au contrôleur de détecter dynamiquement la vitesse de transmission du réseau. La carte détecte automatiquement tout changement de capacité du réseau et s'adapte à la nouvelle vitesse de transmission et au nouveau mode duplex. Auto active une vitesse de 1 Gbit/s lorsque cette vitesse est prise en charge.
- 1 Gbit intégral auto doit être relié à un partenaire de liaison pouvant également établir une connexion de 1 Gbit. La connexion étant limitée à 1 Gbit uniquement, la fonction Ethernet@Wirespeed est désactivée. Si le partenaire de liaison prend en charge les connexions à 1 Gbit uniquement, il se peut que la fonction Réseau local de réveil ne fonctionne pas. De plus, en l'absence d'un système d'exploitation, le trafic de gestion peut également être affecté.
- L'activation des paramètres 10 Mbit semi et 100 Mbit semi entraîne la connexion de la carte au réseau en mode semi-duplex. La carte risque de ne pas fonctionner si le réseau n'est pas configuré pour fonctionner dans le même mode.
- L'activation des paramètres 10 Mbit intégral et 100 Mbit intégral entraîne la connexion de la carte au réseau en mode duplex intégral. La carte risque de ne pas fonctionner si le réseau n'est pas configuré pour fonctionner dans le même mode.

Sortie de veille. Permet à la carte réseau de sortir de veille lorsqu'elle reçoit une trame de sortie de veille du réseau. Il existe deux types de trames de sortie de veille : Magic Packet (Paquet magique) et Wake Up Frame (Trame de réveil).

Cette propriété est disponible uniquement sur les cartes Broadcom NetXtreme.

- **Both (Les deux)** (valeur par défaut). Sélectionne à la fois les trames Magic Packet et les trames de réveil.
- **Magic Packet**. Sélectionne les trames Magic Packet.
- **None** (Aucune). Ne sélectionne aucune trame de sortie de veille.
- Trame de réveil. Sélectionne Wake Up Frame (Trame de réveil) et permet à la carte réseau de « réveiller » le système d'exploitation à la réception d'événements tels que ping ou ARP (Address Resolution Protocol, protocole de résolution d'adresse). Cette option fonctionne avec le mode de gestion de l'alimentation du système d'exploitation et ne fonctionne pas si le paramètre de gestion de l'alimentation n'active pas la fonction WOL.

Priorité et VLAN. Permet d'activer la hiérarchisation du trafic réseau et l'identification VLAN. L'identification VLAN survient uniquement lorsque le paramètre d'ID VLAN est configuré avec une valeur autre que 0 (zéro).

- **Priorité et VLAN activés (par défaut)**. Permet la hiérarchisation des paquets et l'identification VLAN.
- **Priorité et VLAN désactivés**. Empêche la hiérarchisation des paquets et l'identification VLAN.
- **Priorité activée**. Permet uniquement la hiérarchisation des paquets.
- **VLAN activé**. Permet uniquement l'identification VLAN.

Remarque : Si un pilote intermédiaire gère la carte réseau pour l'identification VLAN, les paramètres **Priorité et VLAN désactivés** et **Priorité activée** ne doivent pas être utilisés. Utilisez le paramètre **Priorité et VLAN activés** et définissez l'**ID VLAN** sur 0 (zéro).

ID VLAN. Active l'identification VLAN et configure l'ID VLAN lorsque la propriété **Priorité et VLAN activés** est sélectionnée comme paramètre **Priorité et VLAN**. La plage pour l'ID VLAN est comprise entre 1 et 4094 et doit correspondre à la valeur de la balise VLAN sur le commutateur connecté. Une valeur de 0 (par défaut) dans ce champ désactive l'identification VLAN.

Evaluation des risques de l'identification VLAN via le pilote miniport NDIS

Le pilote miniport NDIS 6.0 de Broadcom permet d'autoriser un système comportant une carte Broadcom à se connecter à un VLAN identifié. Contrairement à BASP, la prise en charge de la participation VLAN par le pilote NDIS 6 est exclusivement destinée à un ID VLAN unique.

De même, le pilote NDIS 6.0 permet uniquement l'identification VLAN des paquets sortants mais ne permet pas le filtrage des paquets entrants en fonction de leur ID VLAN. Il s'agit là du comportement par défaut de tous les pilotes miniport.

L'absence de filtrage de paquets selon l'appartenance VLAN peut présenter des problèmes de sécurité, mais les éléments suivants permettent de gérer les risques en fonction des limites du pilote pour un réseau IPv4 :

Un réseau configuré correctement comportant plusieurs VLAN doit conserver des segments IP distincts pour chaque VLAN. Cette mesure est nécessaire car le trafic sortant se repose sur la table d'acheminement pour savoir à travers quelle carte (virtuel ou physique) doit transiter le trafic et ne détermine pas la carte basée sur l'appartenance VLAN qui est utilisée.

La prise en charge de l'identification VLAN sur le pilote Broadcom NDIS 6.0 étant limitée au trafic en émission (Tx), il est possible que le trafic entrant (Rx) provenant d'un autre VLAN soit transmis au système d'exploitation. Toutefois, si le réseau est configuré convenablement, la segmentation IP et/ou le commutateur VLAN peut fournir un filtre supplémentaire pour limiter ce risque.

Dans le cas d'une connexion consécutive, deux ordinateurs sur le même segment IP peuvent communiquer, quelle que soit leurs configurations VLAN respectives, puisque aucun filtrage des appartenances VLAN n'est effectué. Toutefois, ce scénario présuppose qu'il y ait déjà une faille de sécurité, ce type de connexion n'étant pas habituel dans un environnement VLAN.

Si le risque ci-dessus est problématique et que le filtrage de l'appartenance d'ID VLAN est requis, il peut s'avérer nécessaire d'avoir recours à un pilote intermédiaire.

Affichage des statistiques

Les informations fournies dans l'onglet Statistiques vous permettent de consulter les statistiques relatives au trafic pour les cartes réseau Broadcom et les cartes réseau tierces. Les statistiques et les éléments analysés sont plus complets pour les cartes Broadcom.

Pour afficher les informations de statistiques pour une carte réseau installée, cliquez sur le nom de la carte souhaitée dans le panneau de la vue Explorateur, puis sur l'onglet Statistiques.

Cliquez sur **Actualiser** pour afficher les valeurs les plus récentes pour chaque statistique. Cliquez sur **Redéfinir** pour remettre toutes les valeurs à zéro.

Remarque :

- les statistiques d'équipe ne sont pas compilées pour une carte réseau Broadcom si la fonction est désactivée.
- Tous les statistiques peuvent ne pas être disponibles pour certaines cartes réseau Broadcom.

Statistiques générales

La section Statistiques générales affiche les statistiques de transmission et de réception depuis et vers la carte réseau.

Trames correctement transmises. Nombre de trames correctement transmises. Ce nombre augmente lorsque l'état de transmission indique une bonne transmission.

Trames correctement reçues. Nombre de trames correctement reçues. Cette valeur n'inclut ni les trames reçues avec des erreurs d'alignement, de longueur, de séquence de contrôle de trame (FCS), ni les trames trop longues, ni les trames perdues en raison d'erreurs internes de la sous-couche MAC. Ce nombre augmente lorsque l'état de réception indique une bonne réception (Réception OK).

Trames dirigées et transmises. Nombre de trames de données dirigées et correctement transmises.

Trames de multidiffusion transmises. Nombre de trames correctement transmises, (dont l'état indique une transmission correcte), vers une adresse d'équipe de destination autre que de diffusion.

Trames de diffusion transmises. Nombre de trames correctement transmises vers l'adresse de diffusion (dont l'état indique une transmission correcte). Les trames transmises vers des adresses multicast ne sont pas des trames de diffusion et sont exclues.

Trames dirigées reçues. Nombre de trames de données dirigées et correctement reçues.

Trames de multidiffusion reçues. Nombre de trames reçues et dirigées vers une adresse active d'équipe de non-diffusion. Cette valeur n'inclut ni les trames reçues avec des erreurs d'alignement, de longueur, de séquence de contrôle de trame (FCS), ni les trames trop longues, ni les trames perdues en raison d'erreurs internes de la sous-couche MAC. Cette valeur augmente comme l'indique l'état de réception.

Trames de diffusion reçues. Nombre de trames reçues et dirigées vers une adresse d'équipe de diffusion. Cette valeur n'inclut ni les trames reçues avec des erreurs d'alignement, de longueur, de séquence de contrôle de trame (FCS), ni les trames trop longues, ni les trames perdues en raison d'erreurs internes de la sous-couche MAC. Cette valeur augmente comme l'indique l'état de réception.

Réception de trames avec erreur CRC. Nombre de trames reçues avec des erreurs CRC.

Configuration de regroupement

La fonction de regroupement permet de regrouper n'importe quelles cartes réseau disponibles pour qu'elles fonctionnent de manière groupée. Le regroupement est une méthode de création d'une carte réseau virtuelle (équipe de plusieurs cartes fonctionnant comme une seule et même carte). Cette méthode présente l'avantage de permettre l'équilibrage de volume et la compensation. Le regroupement est effectué via le logiciel Broadcom Advanced Server Program (BASP). Pour une description détaillée des technologies et des informations sur l'implémentation du logiciel de regroupement, reportez-vous à la section « Broadcom Gigabit Ethernet Teaming Services » du Guide d'utilisation de votre carte réseau Broadcom.

Le regroupement peut être effectué de l'une des manières suivantes :

- Utilisation de l'Assistant de regroupement Broadcom
- Utilisation du mode Expert

Remarque :

- Pour en savoir plus sur les protocoles de regroupement, consultez la rubrique « Regroupement » du Guide d'utilisation de carte de réseau Broadcom.
- Si vous n'activez pas LiveLink™ lors de la configuration d'équipes, il est recommandé de désactiver le protocole STP au niveau du commutateur. Ceci permet de minimiser le temps d'interruption nécessaire à la détermination de la boucle de l'arbre maximal lors d'une reprise. LiveLink réduit ce genre de problèmes.
- BASP est disponible uniquement si le système est doté d'une ou plusieurs cartes de réseau Broadcom.
- Les propriétés Large Send Offload (Déchargement important à l'émission) et Checksum Offload (Déchargement de la somme de contrôle) sont uniquement activées pour une équipe lorsque tous ses membres prennent en charge la fonctionnalité et sont configurés en conséquence.
- Vous devez disposer de privilèges d'administrateur pour créer ou modifier une équipe.
- Dans un environnement d'équipe dans lequel les éléments sont connectés à différentes vitesses, l'algorithme d'équilibrage de charge favorise les éléments connectés avec une liaison Gigabit Ethernet par rapport à ceux connectés avec des liaisons de vitesse plus faibles (100 Mbit/s ou 10 Mbit/s) jusqu'à ce qu'un seuil soit atteint. Il s'agit d'un comportement normal.
- Le réseau local de réveil est une fonction permettant à un système de sortir de veille à l'arrivée d'un paquet spécifique sur l'interface Ethernet. Dans la mesure où les cartes virtuelles sont implémentées en tant que périphérique logiciel, elles ne disposent pas des fonctions matérielles permettant de mettre WOL en œuvre. Il est donc impossible de sortir le système d'un état de veille en utilisant la carte virtuelle. Les cartes physiques, en revanche, prennent en charge cette propriété, même lorsque la carte fait partie d'une équipe.

Types d'équipe

Vous pouvez créer quatre types d'équipe d'équilibrage de charge :

- Smart Load Balance and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/Projet 802.3ad en mode statique
- SLB (désactivation de la reprise automatique) – La fonction de désactivation de la reprise automatique est configurée pour les types d'équipe Smart Load Balance and Failover dans l'Assistant de regroupement.

Pour obtenir une description de ces types, reportez-vous à la section Equilibrage de charge et tolérance de panne dans le *guide de l'utilisateur NetXtreme® BCM57XX de Broadcom®*.

Utilisation de l'Assistant de regroupement Broadcom

L'Assistant de regroupement Broadcom permet de créer une équipe, de configurer une équipe déjà existante ou de créer un VLAN.

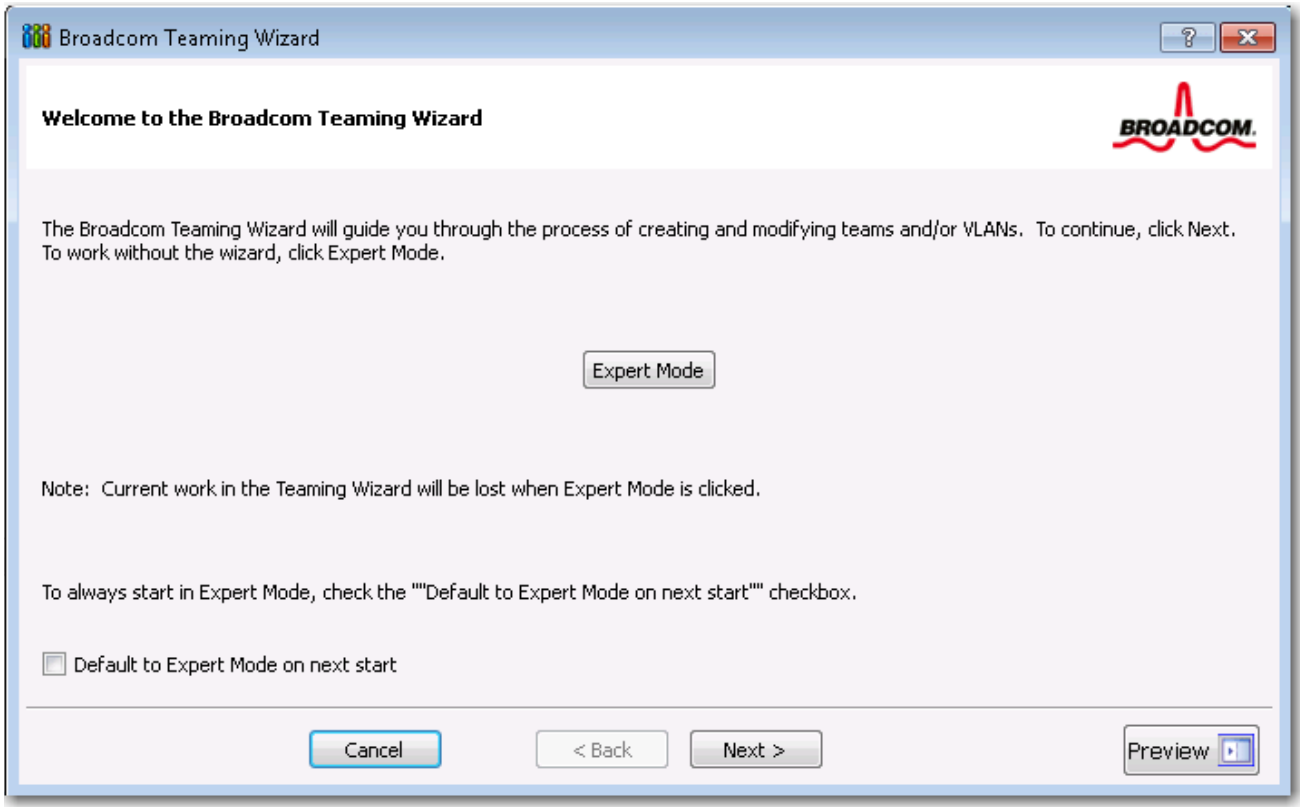
1. Créer ou modifier une équipe :

   Pour créer une nouvelle équipe, sélectionnez **Créer une équipe** dans le menu **Equipe** ou bien cliquez avec le bouton droit de la souris sur l'un des périphériques répertoriés dans la section des« cartes non attribuées », puis sélectionnez **Créer une équipe**. Si aucun périphérique n'est répertorié dans la section des « cartes non attribuées », cette option n'est pas disponible étant donné que toutes les cartes sont déjà attribuées à des équipes.

   Pour configurer une équipe existante, cliquez avec le bouton droit de la souris sur l'une des équipes dans la liste, puis sélectionnez **Modifier l'équipe**. Cette option est disponible uniquement si une équipe a déjà été créée et qu'elle est répertoriée dans le volet Gestion des équipes.

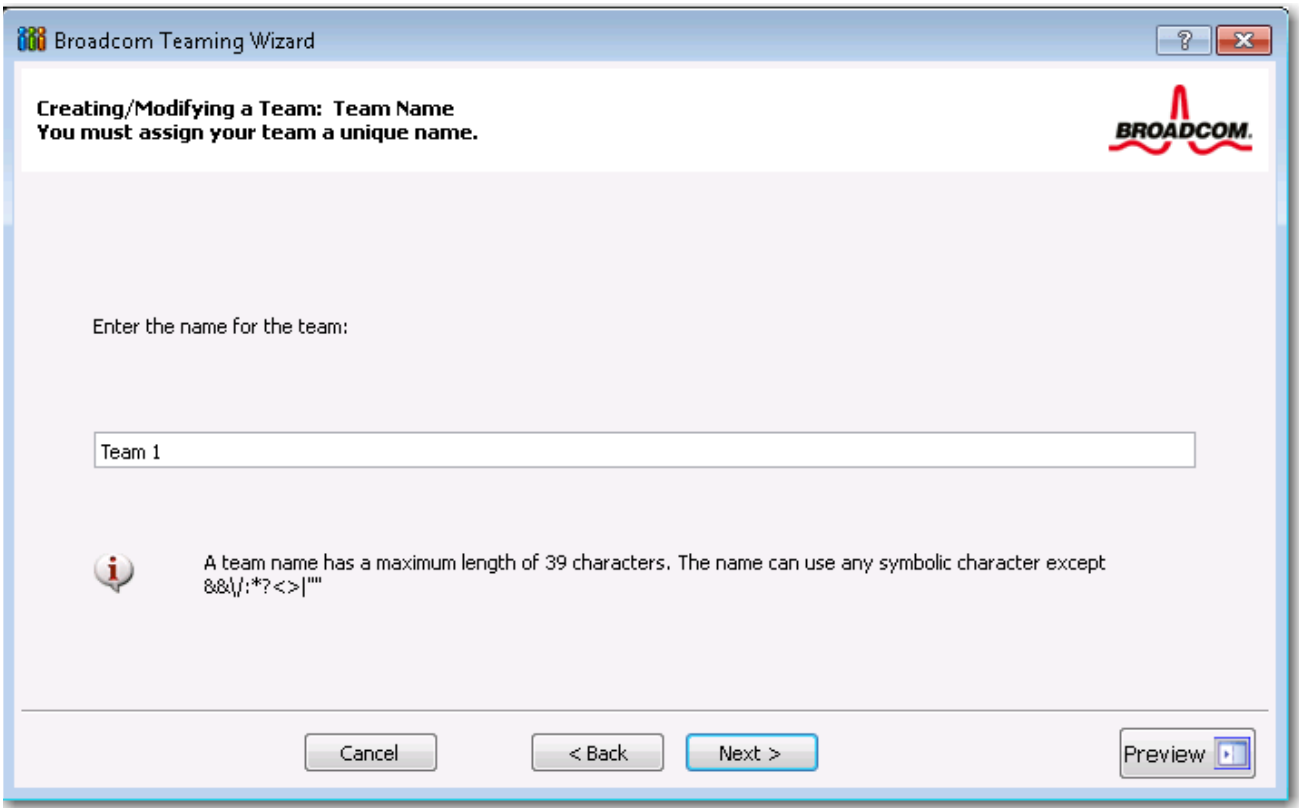
Remarque : Si vous ne souhaitez pas utiliser l'assistant pour le moment, cliquez sur **Mode Expert**. Pour toujours utiliser le mode Expert pendant la création d'une équipe, activez l'option **Passer par défaut en Mode Expert au prochain démarrage**. Voir Utilisation du mode Expert.

2. Pour poursuivre en utilisant l'assistant, cliquez sur **Suivant**.

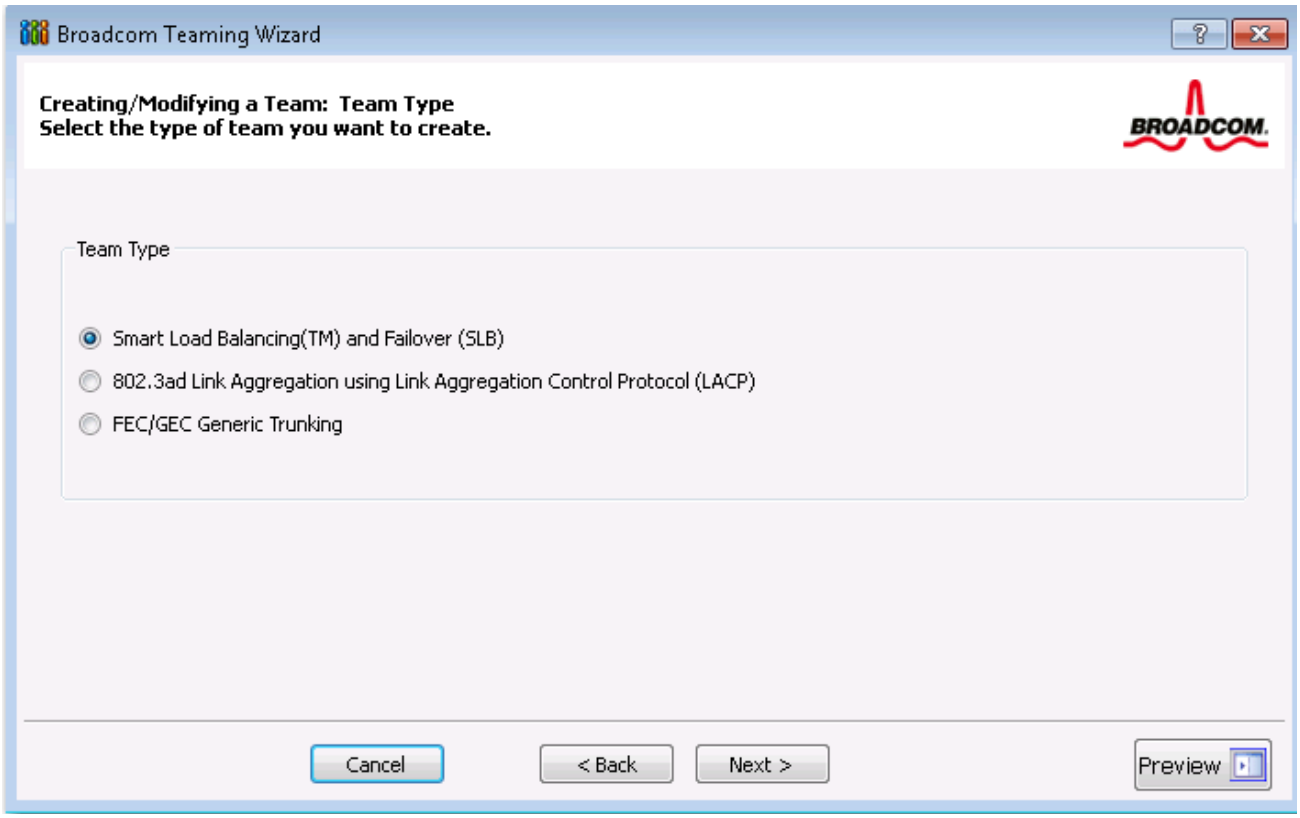


3. Saisissez le nom de l'équipe, puis cliquez sur **Suivant**. Pour passer en revue ou modifier vos paramètres, cliquez sur **Précédent**. Cliquez sur **Annuler** pour annuler vos paramètres et quitter l'assistant.

Remarque : le nom de l'équipe ne peut ni dépasser 39 caractères, ni commencer par un espace, ni contenir les caractères suivants : & \ / : * ? < > |



4. Sélectionnez le type d'équipe que vous souhaitez créer. Si l'équipe est du type SLB, cliquez sur **Suivant**. Si l'équipe n'est pas du type SLB, une boîte de dialogue s'affiche. Vérifiez que le commutateur réseau connecté aux éléments de l'équipe est correctement configuré pour le type d'équipe, cliquez sur **OK**, puis continuez.

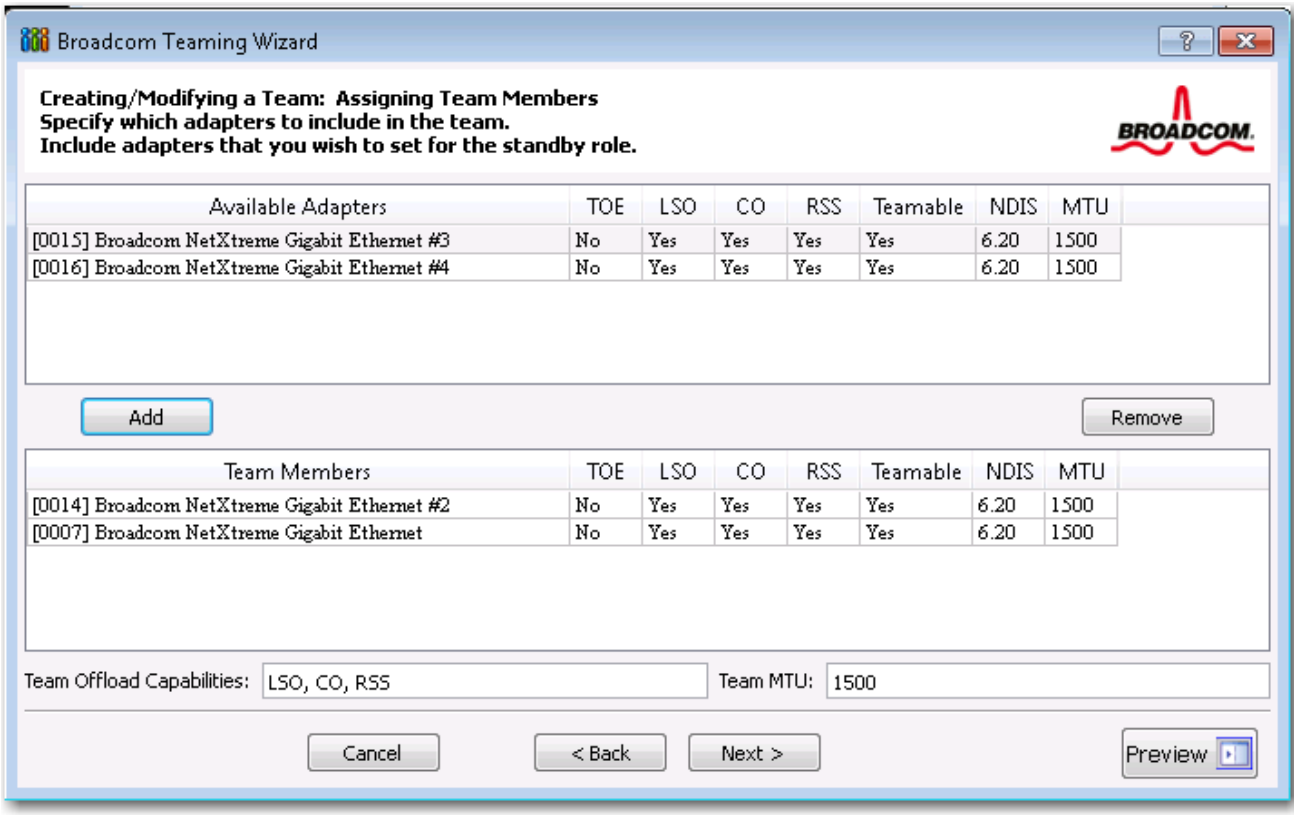


5. Dans la liste **Cartes disponibles**, cliquez sur la carte que vous voulez ajouter à l'équipe, puis cliquez sur **Ajouter**. Supprimez les éléments de l'équipe depuis la liste **Eléments de l'équipe** en cliquant sur la carte, puis sur **Supprimer**. Cliquez sur **Suivant**.

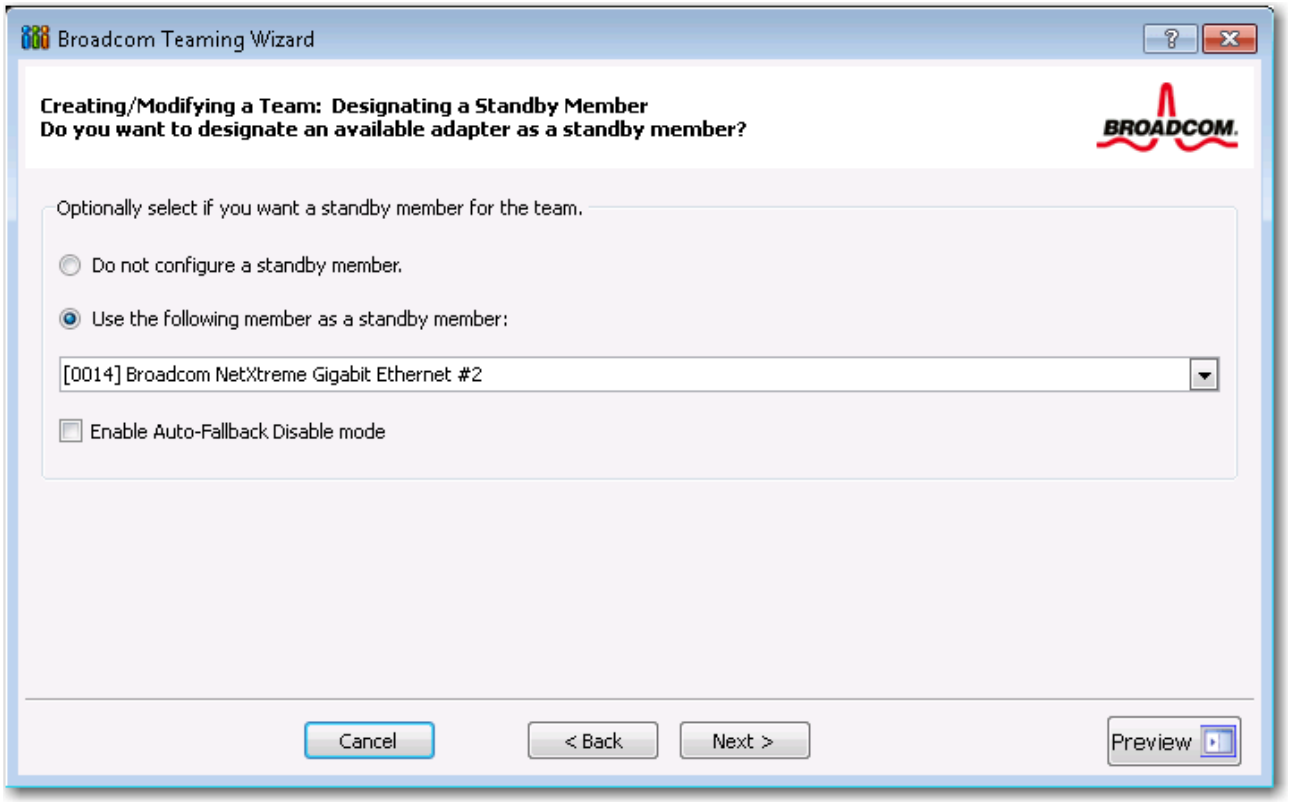
Remarque : Au moins une carte réseau Broadcom doit être affectée à l'équipe.

Les colonnes Large Send Offload (LSO, Déchargement important à l'émission) et Checksum Offload (CO, Déchargement de la somme de contrôle) indiquent si les propriétés correspondantes sont prises en charge pour la carte. Les propriétés LSO et CO sont uniquement activées pour une équipe lorsque tous ses membres prennent en charge la fonctionnalité et sont configurés en conséquence. Si tel est le cas, les capacités de déchargement de l'équipe apparaissent en bas de l'écran.

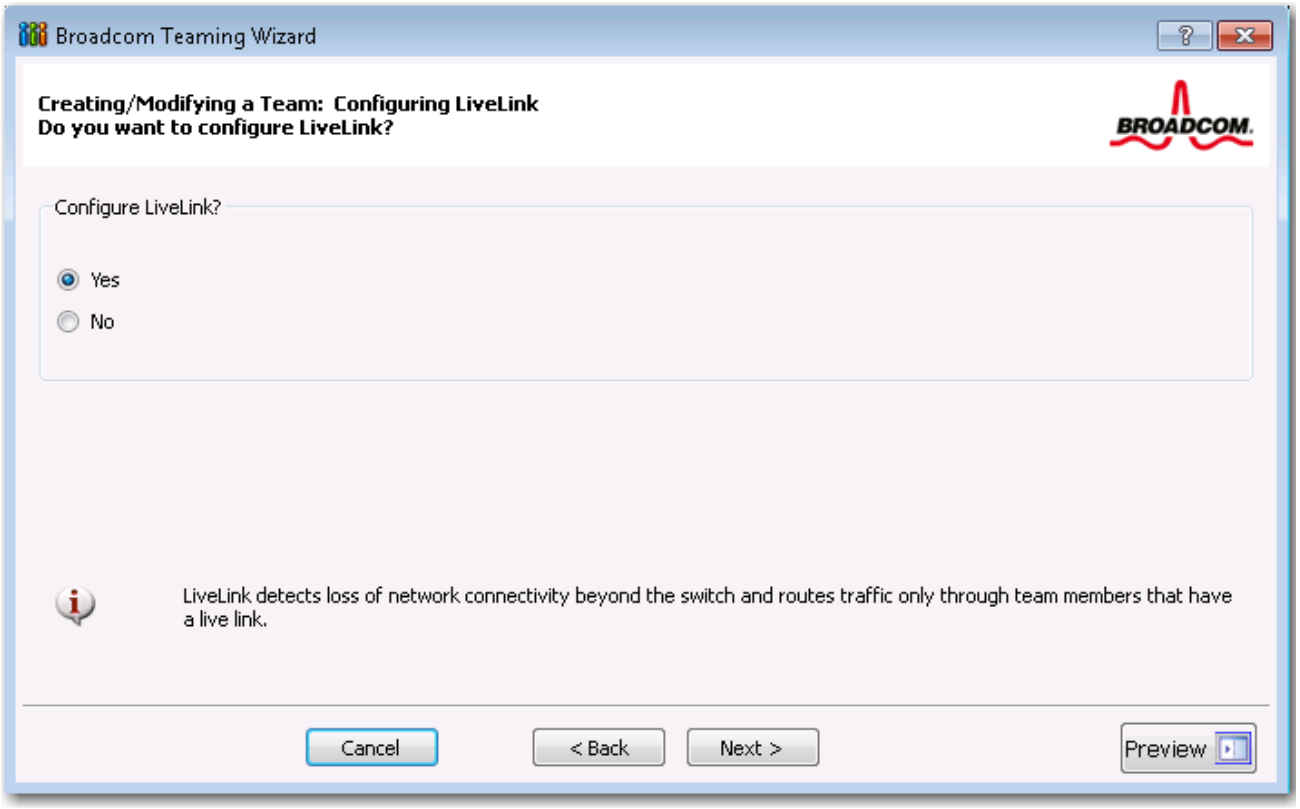
Remarque : l'ajout d'une carte réseau dans une équipe où le pilote est désactivé peut influer de façon négative sur les capacités de déchargement de l'équipe. Cela peut avoir un impact sur les performances de l'équipe. Il est donc recommandé que seules les cartes réseau compatibles avec le pilote soient ajoutées comme membres d'une équipe.



6. Pour désigner l'une des cartes en tant qu'élément auxiliaire (facultatif), activez l'option **Utiliser l'élément d'équilibrage suivant**, puis désignez cet élément auxiliaire en sélectionnant la carte souhaitée dans la liste.
7. Le mode de désactivation de la reprise automatique permet à l'équipe de continuer à utiliser l'élément d'équilibrage au lieu de rebasculer sur l'élément principal si celui-ci revient en ligne. Pour activer cette fonction, activez l'option **Activer le mode de désactivation de la reprise automatique**. Cliquez sur **Suivant**.



8. Si vous souhaitez configurer LiveLink, cliquez sur **Oui** (dans le cas contraire, cliquez sur **Non**), puis sur **Suivant**.



9. Sélectionnez l'intervalle de test (nombre de secondes entre chaque retransmission d'un paquet de liaison à la cible de test) et le nombre maximal de tentatives de test (nombre de réponses manquées consécutives de la cible de test avant qu'une reprise ne soit déclenchée) souhaités.

10. Réglez l'ID de VLAN de test pour permettre la connectivité avec les cibles de test se trouvant sur un réseau local virtuel identifié. Le nombre défini doit correspondre à l'ID de VLAN des cibles de test, ainsi qu'au(x) port(s) situé(s) sur le commutateur auquel l'équipe est connectée.

Remarque : chaque équipe pouvant utiliser LiveLink peut seulement communiquer avec les cibles de test sur un VLAN unique. De plus, l'ID VLAN 0 correspond à un réseau non identifié. Si l'ID de VLAN de test est défini sur une valeur autre que 0, un VLAN doit être créé à l'aide d'une balise VLAN (valeur d'identification du réseau local virtuel) identique (voir Etape 16.).

11. Sélectionnez la cible de test située en haut de la liste, cliquez sur **Modifier l'adresse IP cible**, saisissez l'adresse IP de la cible dans la zone **Adresse IP** pour une ou l'ensemble des cibles de test, puis cliquez sur **OK**. Cliquez sur **Suivant**.

Remarque : Seule la première cible de test est nécessaire. Vous pouvez indiquer jusqu'à trois cibles de test supplémentaires à des fins de sauvegarde en attribuant des adresses IP supplémentaires aux autres cibles de test.

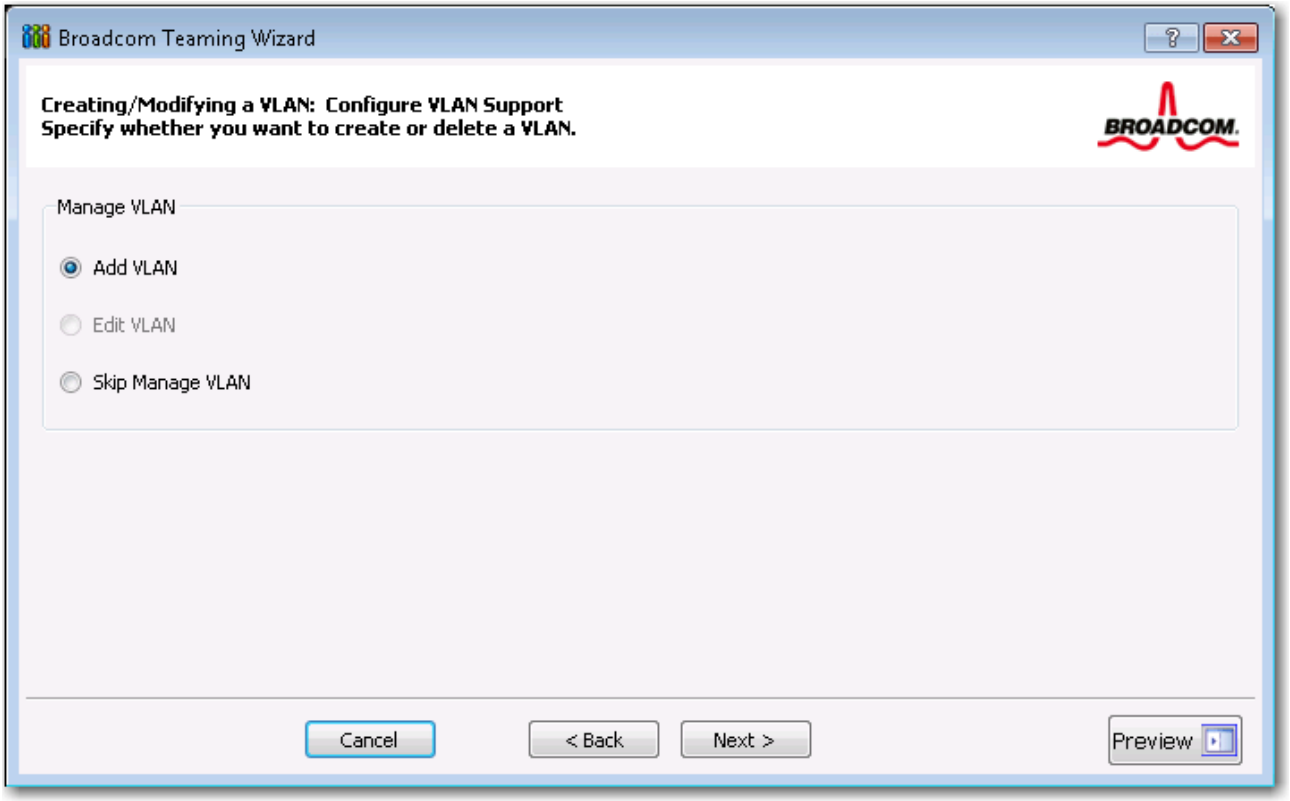
12. Sélectionnez un élément de l'équipe dans la liste, cliquez sur **Modifier l'adresse IP de membre**, puis saisissez l'adresse IP de cet élément dans la zone Adresse IP. Répétez cette opération pour tous les éléments de l'équipe répertoriés, puis cliquez sur **OK**. Cliquez sur **Suivant**.

Remarque : Toutes les adresses IP des éléments doivent se trouver sur le même sous-réseau que les cibles de test.

13. Cliquez sur **Ajouter un VLAN** si vous souhaitez créer un réseau local virtuel pour l'équipe ou sur **Modifier un VLAN** si vous souhaitez modifier les paramètres d'un un réseau local virtuel existant, puis cliquez sur **Suivant**. Si vous ne souhaitez ni créer, ni modifier un réseau local virtuel, cliquez sur **Ignorer la gestion de VLAN**, puis sur **Suivant** et passez à la dernière étape de l'assistant (voir Etape 18. de cette procédure).

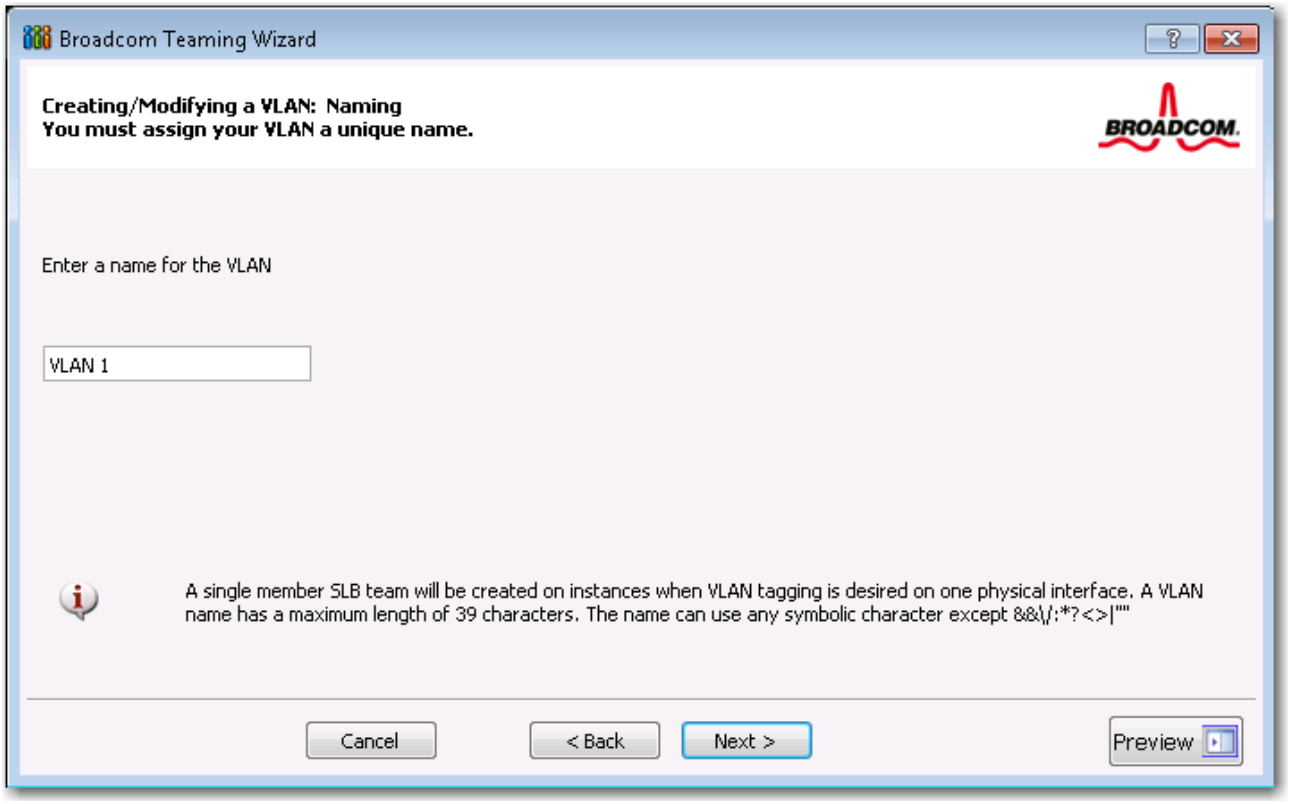
Les réseaux locaux virtuels vous permettent d'ajouter plusieurs cartes virtuelles qui se trouvent sur différents sous-réseaux. L'avantage est que votre système peut disposer d'une seule carte réseau qui peut appartenir à plusieurs sous-réseaux.

Remarque : Les réseaux locaux virtuels ne peuvent être créés que lorsque tous les éléments de l'équipe sont des cartes Broadcom.

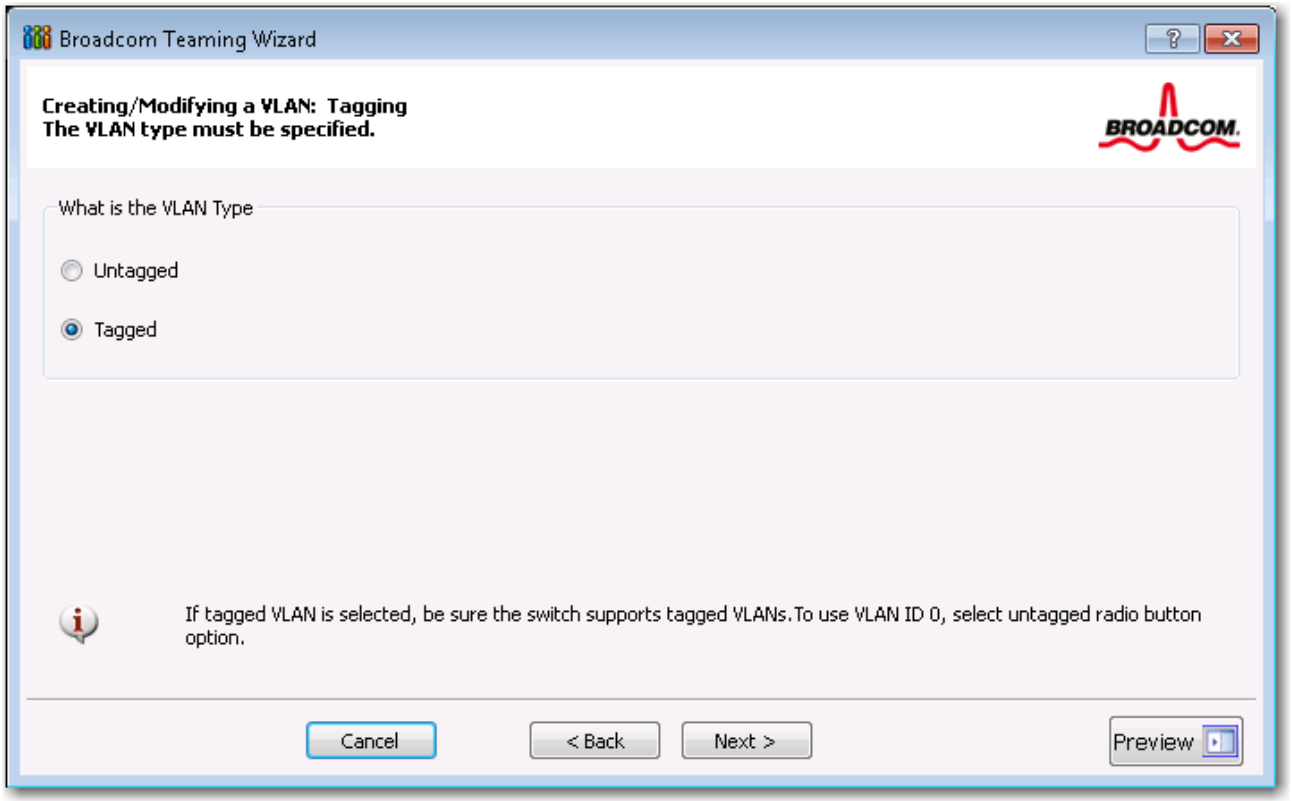


14. Saisissez le nom du réseau local virtuel, puis cliquez sur **Suivant**.

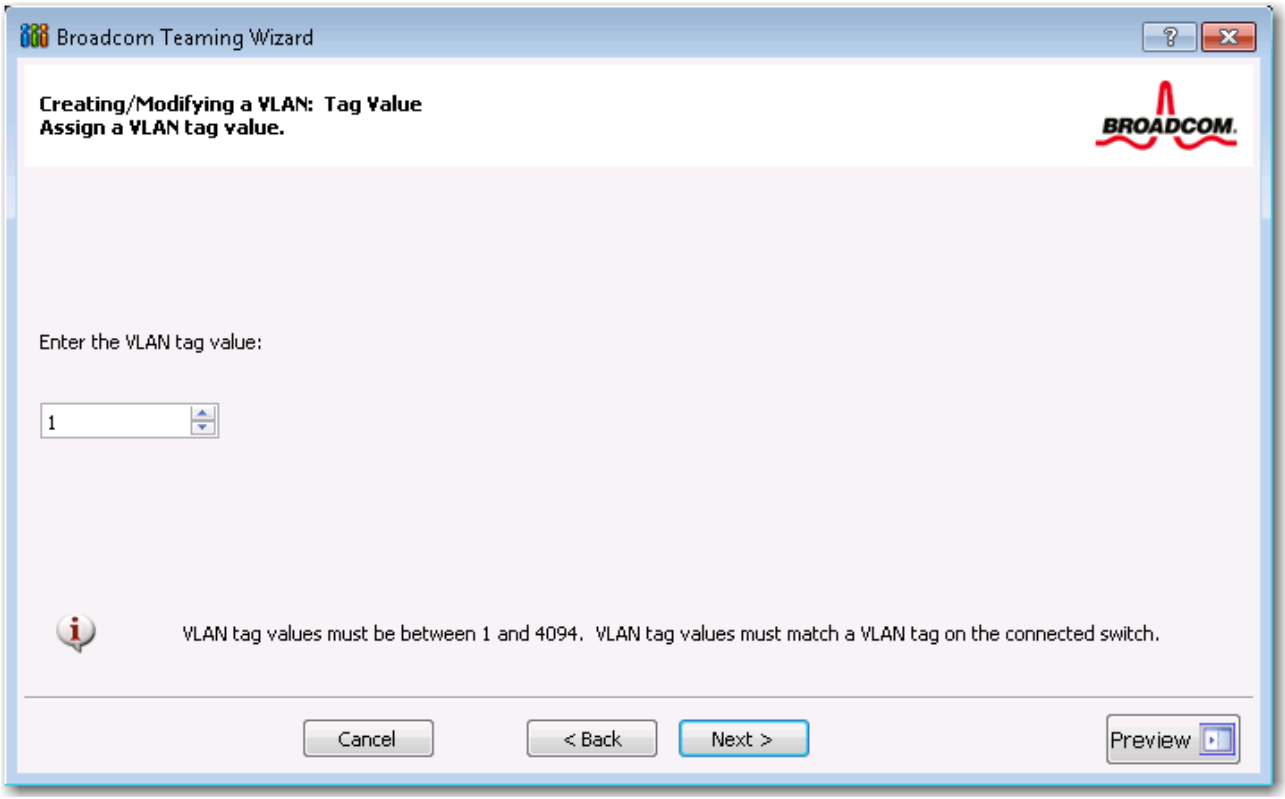
Remarque : le nom de l'équipe ne peut ni dépasser 39 caractères, ni commencer par un espace, ni contenir les caractères suivants : & \ / : * ? < > |



15. Pour identifier le réseau local virtuel (VLAN), sélectionnez **Identifié**, puis cliquez sur **Suivant**. Si vous ne souhaitez pas l'identifier, cliquez sur **Non identifié**, puis **Suivant** et passez à l'étape d'ajout de réseaux locaux virtuels supplémentaires de l'assistant (voir Etape 17. de cette procédure).



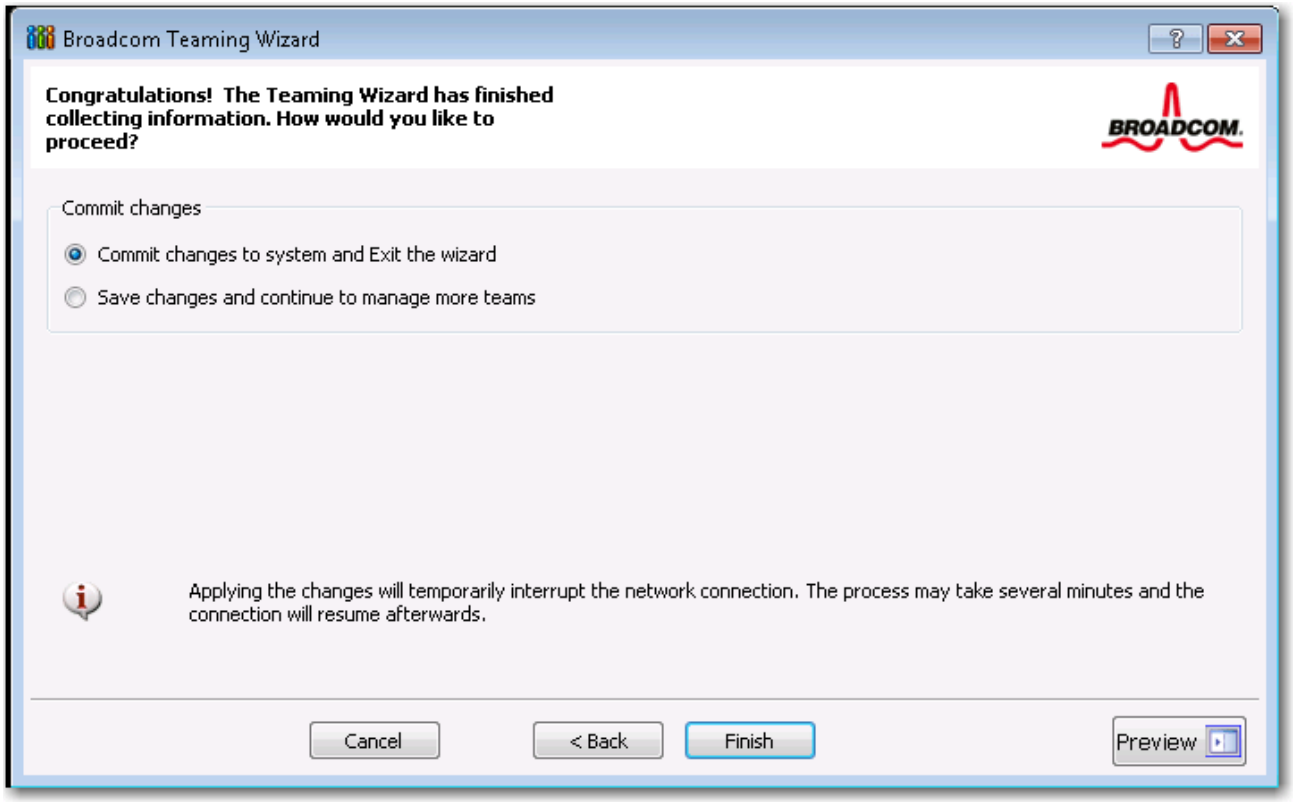
16. Saisissez la valeur d'identification du réseau local virtuel (balise VLAN), puis cliquez sur **Suivant**. Cette valeur doit être comprise entre 1 et 4094.



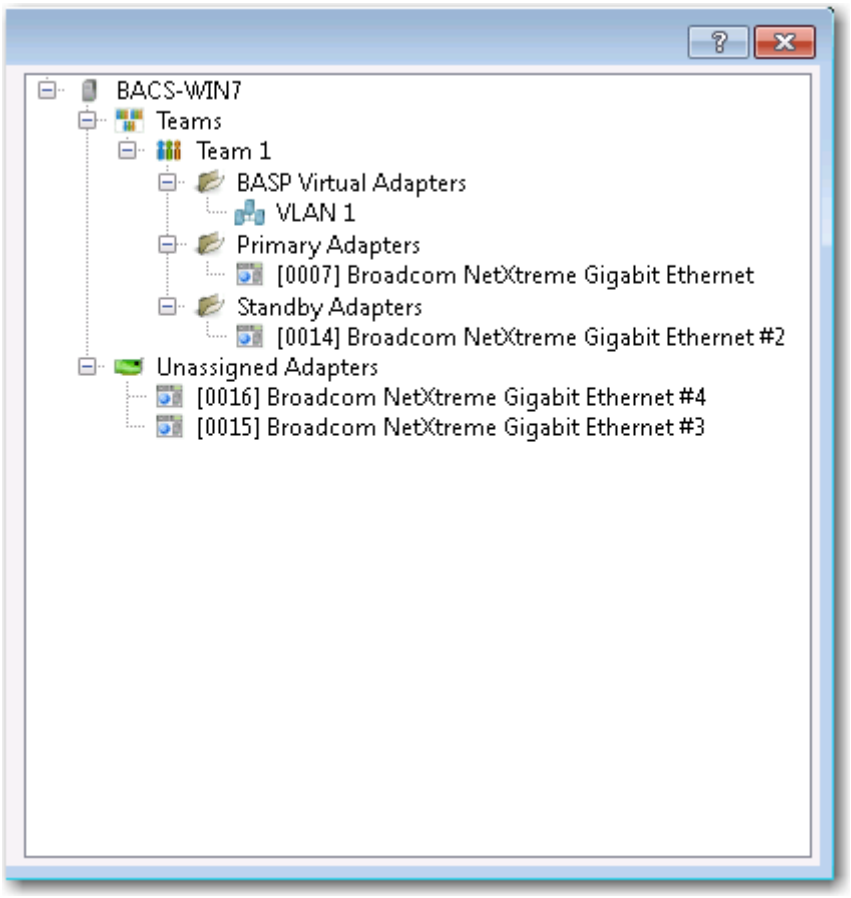
17. Cliquez sur **Oui** pour ajouter ou gérer un autre réseau local virtuel, puis cliquez sur **Suivant**. Répétez l'opération jusqu'à ce que vous ne souhaitiez plus ajouter ou gérer d'autres réseaux locaux supplémentaires.

Remarque : Vous pouvez définir jusqu'à 64 réseaux locaux virtuels par équipe (63 identifiés et 1 non identifié). L'ajout de réseaux locaux virtuels peut ralentir la réactivité de l'interface Windows en raison de l'utilisation de la mémoire et de l'unité centrale pour chaque réseau local virtuel. L'incidence de l'ajout de réseaux locaux sur les performances de Windows varie selon le système d'exploitation.

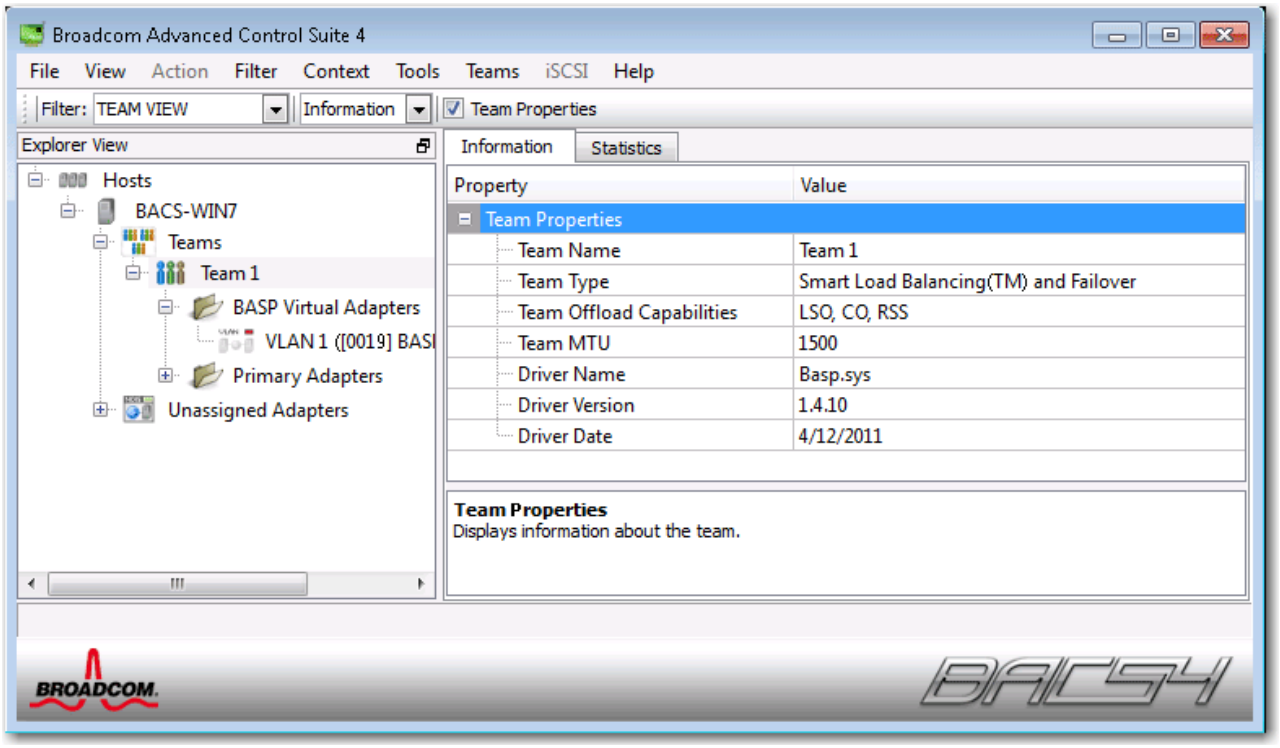
18. Pour appliquer et valider les modifications apportées à l'équipe, sélectionnez /**Valider les modifications apportées au système et quitter l'assistant**. Pour appliquer vos modifications et continuer à utiliser l'assistant, sélectionnez **Enregistrer les modifications et continuer à gérer d'autres équipes**. Cliquez sur Terminer.



Remarque : A tout moment du processus de l'Assistant de regroupement Broadcom, vous pouvez cliquer sur **Aperçu** pour obtenir une représentation visuelle des conséquences de vos modifications sur l'équipe avant de valider ces dernières.



19. Dans le volet Gestion des équipes, cliquez sur le nom de l'équipe concernée pour en afficher les propriétés dans l'onglet **Informations** et les données de transmission et de réception dans l'onglet **Statistiques**.



Utilisation du mode Expert

Vous pouvez également utiliser le mode Expert pour créer une équipe, modifier une équipe, ajouter un réseau local virtuel (VLAN) et configurer LiveLink pour une équipe de type Smart Load Balancing and Failover (Equilibrage de charge intelligent et reprise) ou SLB (désactivation de la reprise automatique). Pour créer une équipe à l'aide de l'assistant, voir Utilisation de l'Assistant de regroupement Broadcom.

Pour définir le mode de regroupement par défaut, sélectionnez **Options** dans le menu **Outils**, puis **Mode Expert** ou **Mode Assistant** (le paramètre par défaut est Mode Assistant).

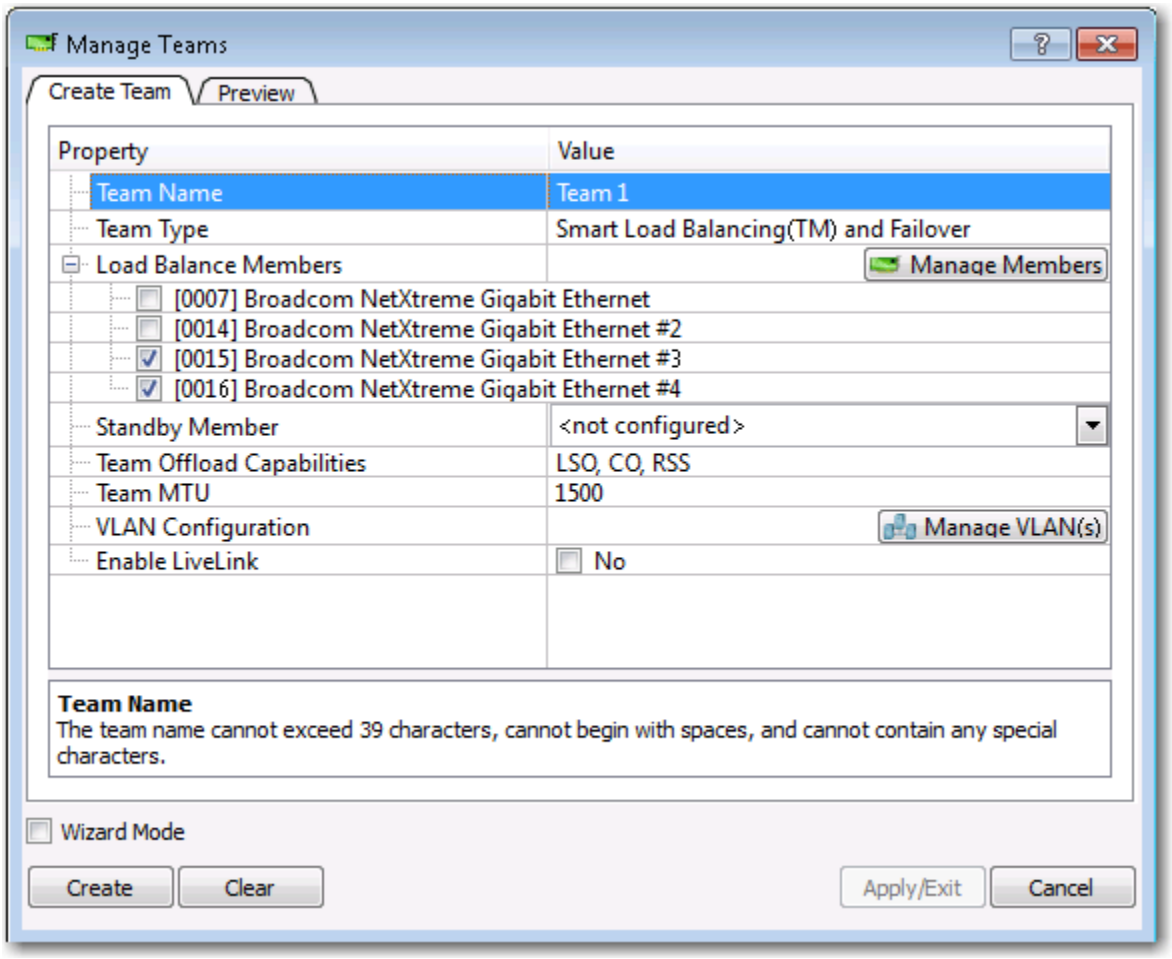
Création d'une équipe

Remarque : Il n'est pas recommandé d'activer le protocole DHCP pour les éléments d'une équipe de type SLB.

1. Sélectionnez **Créer une équipe** dans le menu **Equipe** ou bien cliquez avec le bouton droit de la souris sur l'un des périphériques répertoriés dans la section « Cartes non attribuées », puis sélectionnez **Créer une équipe**. Si aucun périphérique n'est répertorié dans la section des « cartes non attribuées », cette option n'est pas disponible étant donné que toutes les cartes sont déjà attribuées à des équipes.
2. Cliquez sur **Mode Expert**.

Remarque : Pour toujours utiliser le mode Expert pour créer une équipe, activez la case à cocher **Passer par défaut en Mode Expert au prochain démarrage**.

3. Cliquez sur l'onglet **Créer une équipe**.



Remarque : L'onglet **Créer une équipe** s'affiche uniquement si des cartes sont disponibles pour le regroupement.

4. Cliquez sur le champ **Nom de l'équipe** pour saisir un nom d'équipe.
5. Cliquez sur le champ **Type d'équipe** pour sélectionner un type d'équipe.
6. Affectez la ou les cartes souhaitées à l'équipe en les sélectionnant dans la liste **Equilibrage de volume des éléments**. Au moins une carte doit être sélectionnée dans la liste **Equilibrage de volume des éléments**.
7. Vous pouvez désigner toute autre carte disponible comme élément auxiliaire en la sélectionnant dans la liste **Elément auxiliaire**.

Remarque : Au moins une carte réseau Broadcom doit être affectée à l'équipe.

Les paramètres LSO (Large Send Offload, Déchargement important à l'émission), CO (Checksum Offload, Déchargement de la somme de contrôle) et RSS indiquent si les propriétés LSO, CO et/ou RSS sont prises en charge

pour l'équipe. Les propriétés LSO, CO et RSS sont activées pour une équipe uniquement lorsque tous ses membres prennent en charge la fonctionnalité et sont configurés en conséquence.

Remarque : l'ajout d'une carte réseau dans une équipe où le pilote est désactivé peut influer de façon négative sur les capacités de déchargement de l'équipe. Cela peut avoir un impact sur les performances de l'équipe. Il est donc recommandé que seules les cartes réseau compatibles avec le pilote soient ajoutées comme membres d'une équipe.

8. Tapez une valeur pour **Equipe MTU**.
9. Pour enregistrer les informations sur l'équipe, cliquez sur **Créer**.
10. Pour définir des équipes supplémentaires, répétez les étapes 4. à 9.. Une fois les équipes définies, elles sont sélectionnables dans la liste, mais elles ne sont pas encore créées pour autant. Pour visualiser la structure de l'équipe avant d'appliquer les modifications, cliquez sur l'onglet **Aperçu**.
11. Pour créer toutes les équipes que vous avez définies et quitter la fenêtre Gérer les équipes, cliquez sur **Appliquer/ Quitter**.
12. Cliquez sur **Oui** lorsque le message indiquant que la connexion au réseau va subir une rupture temporaire s'affiche.

Remarque :

- le nom de l'équipe ne peut ni dépasser 39 caractères, ni commencer par un espace, ni contenir les caractères suivants : & \ / : * ? < > |
- Les noms d'équipes doivent être uniques. Si vous tentez d'utiliser un nom d'équipe plus d'une fois, un message d'erreur s'affiche, indiquant que le nom saisi existe déjà.
- Une équipe peut comprendre huit éléments au maximum.
- Une fois la configuration de l'équipe réalisée correctement, un pilote de carte d'équipe virtuel est créé pour chaque équipe configurée.
- Si vous désactivez une équipe virtuelle et que vous souhaitez ensuite la réactiver, vous devez d'abord désactiver et réactiver tous les éléments de l'équipe avant de réactiver l'équipe virtuelle.
- Lorsque vous créez des équipes Generic Trunking et Link Aggregation, vous ne pouvez pas désigner d'élément auxiliaire. Les éléments auxiliaires fonctionnent uniquement avec les types d'équipe Smart Load Balancing and Failover (Equilibrage de charge intelligent et reprise) et SLB (désactivation de la reprise automatique).
- Pour une équipe SLB (désactivation de la reprise automatique), lorsque vous souhaitez restaurer le trafic des éléments auxiliaires vers les éléments d'équilibrage de charge, cliquez sur le bouton Reprise dans l'onglet Propriétés de l'équipe.
- Lorsque vous configurez une équipe SLB, il est recommandé de connecter les éléments de l'équipe à un commutateur, bien que leur connexion à un concentrateur soit prise en charge à des fins de vérification.
- Les cartes réseau tierces ne sont pas toutes prises en charge ou homologuées pour le regroupement.

13. Configurez l'adresse IP de l'équipe.
    a. Dans le **Panneau de configuration**, cliquez deux fois sur **Network Connections (Connexions réseau)**.
    b. Cliquez avec le bouton droit de la souris sur le nom de l'équipe que vous souhaitez configurer, puis cliquez sur **Propriétés**.
    c. Dans l'onglet **Général**, cliquez sur **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.
    d. Configurez l'adresse IP et les autres propriétés TCP/IP requises concernant l'équipe, puis cliquez sur **OK**.

Modification d'une équipe

Après avoir créé une équipe, vous pouvez la modifier selon les manières suivantes :

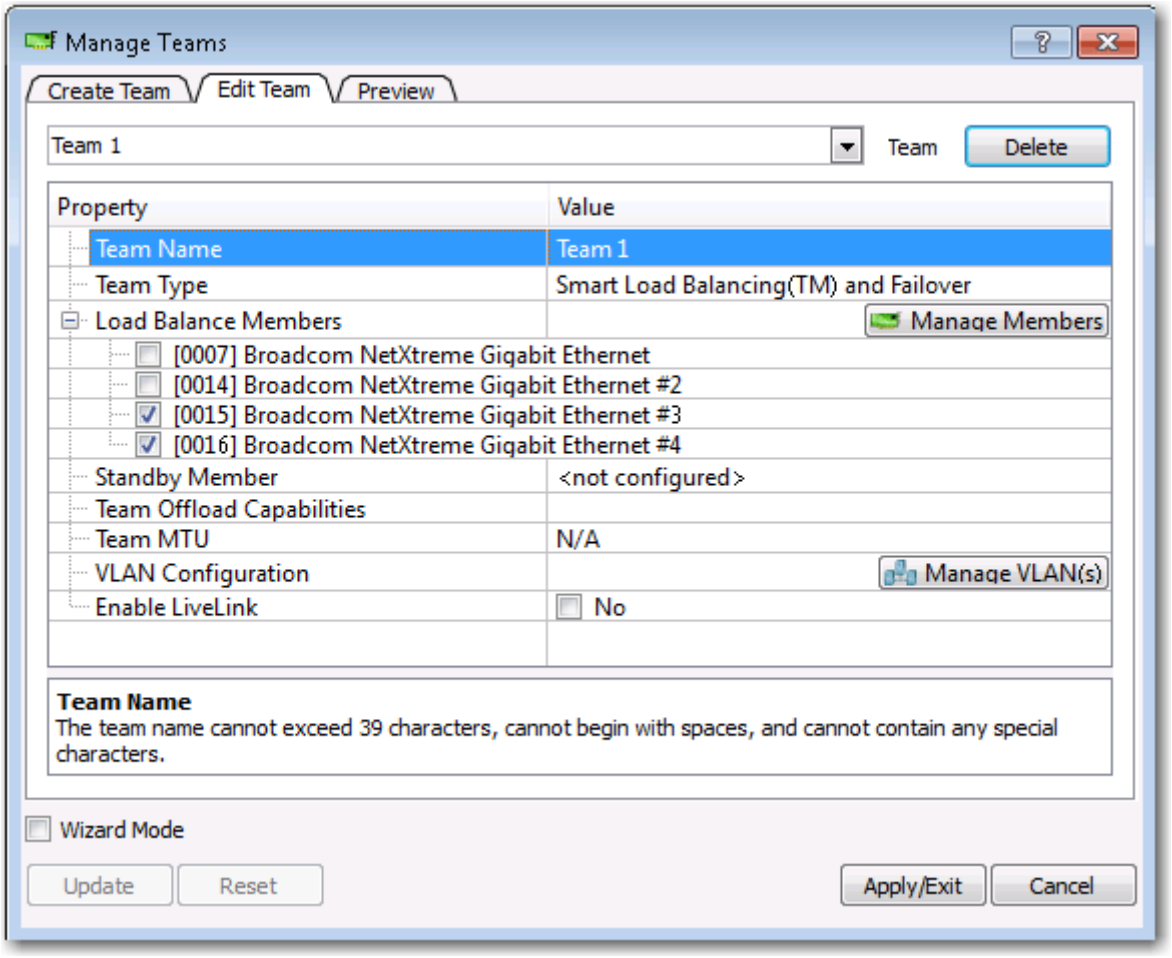
- En modifiant le type d'équipe
- En modifiant les éléments attribués à l'équipe
- En ajoutant un réseau local virtuel
- En modifiant un réseau local virtuel (à l'aide du mode Expert)
- En supprimant une équipe ou un réseau local virtuel (à l'aide du mode Expert)

Pour modifier une équipe

1. Dans le menu **Equipe**, cliquez sur **Modifier l'équipe** ou bien cliquez avec le bouton droit de la souris sur l'une des équipes répertoriées et sélectionnez **Modifier l'équipe**. Cette option est disponible uniquement si une équipe a déjà été créée et qu'elle est répertoriée dans le volet Gestion des équipes.
2. L'écran de bienvenue de l'assistant apparaît. Cliquez sur **Suivant** pour continuer à modifier une équipe à l'aide de l'assistant ou sur **Mode Expert** pour passer en mode Expert.

Remarque : L'onglet **Modifier l'équipe** dans le mode Expert est affiché uniquement si des équipes sont configurées sur le système.

3. Cliquez sur l'onglet **Modifier l'équipe**.



4. Apportez les modifications souhaitées, puis cliquez sur **Mettre à jour**. Les modifications n'ont pas encore été prises en compte ; cliquez sur l'onglet **Aperçu** pour visualiser la structure mise à jour de l'équipe avant d'appliquer les modifications.
5. Pour appliquer les mises à jour et quitter la fenêtre Gérer les équipes, cliquez sur **Appliquer/Quitter**.
6. Cliquez sur **Oui** lorsque le message indiquant que la connexion au réseau va subir une rupture temporaire s'affiche.

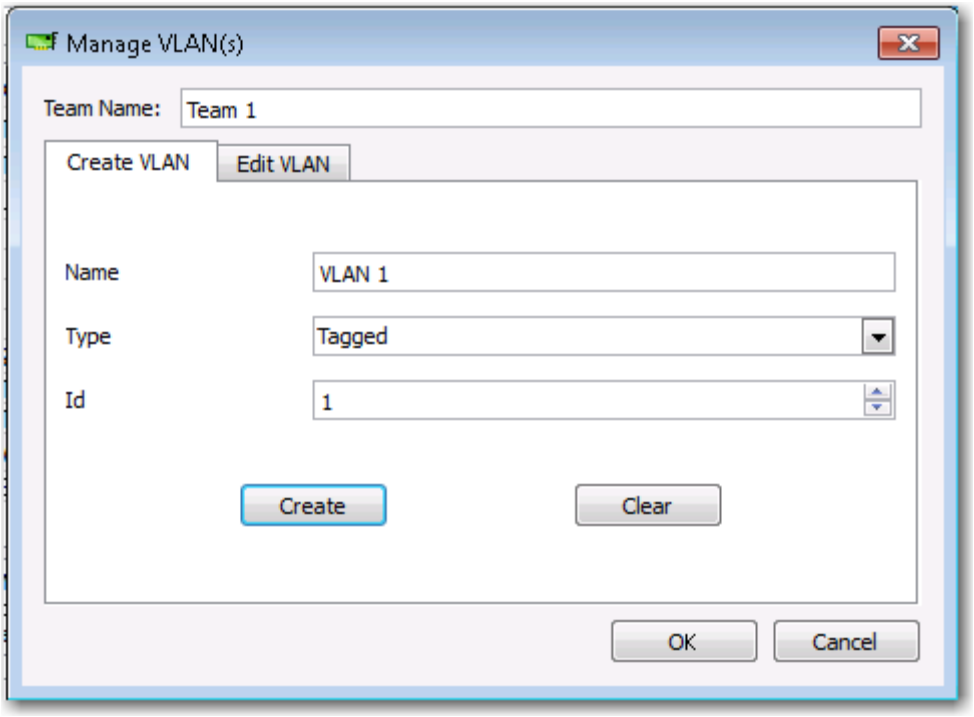
Ajout d'un réseau local virtuel

Vous pouvez ajouter des réseaux locaux virtuels (VLAN) à une équipe. Cela vous permet d'ajouter plusieurs cartes virtuelles qui se trouvent sur différents sous-réseaux. L'avantage est que votre système peut disposer d'une seule carte réseau qui peut appartenir à plusieurs sous-réseaux. Avec un réseau local virtuel, vous pouvez associer la fonction d'équilibrage de charge pour les éléments d'équilibrage de charge et vous pouvez utiliser une carte de reprise.

Vous pouvez définir jusqu'à 64 réseaux locaux virtuels par équipe (63 identifiés et 1 non identifié). Les réseaux locaux virtuels ne peuvent être créés que lorsque tous les éléments de l'équipe sont des cartes Broadcom. Si vous tentez de créer un réseau local virtuel avec une carte d'un autre fabricant, un message d'erreur s'affiche.

Pour configurer une équipe avec un réseau local virtuel

1. Dans le menu **Equipes**, sélectionnez **Ajouter un VLAN**.
2. L'écran de bienvenue apparaît.
3. Cliquez sur **Mode Expert**.
4. Dans l'onglet **Créer une équipe** de la fenêtre **Gérer les équipes**, cliquez sur **Gérer le(s) VLAN**.
5. Saisissez le nom du réseau local virtuel, puis sélectionnez son type et son ID.
6. Pour enregistrer les informations sur le réseau local virtuel, cliquez sur **Créer**. Une fois les réseaux locaux virtuels définis, ils sont sélectionnables dans la liste Nom de l'équipe, mais ils ne sont pas encore créés pour autant.
7. Poursuivez cette procédure jusqu'à ce que tous les réseaux locaux virtuels soient définis, puis cliquez sur **OK** pour les créer.



8. Cliquez sur **Oui** lorsque le message indiquant que la connexion au réseau va subir une rupture temporaire s'affiche.

Remarque : Pour une utilisation optimale de la carte, votre système doit disposer de 64 Mo de mémoire système pour chacun des huit réseaux locaux virtuels créés par carte.

Affichage des propriétés et des statistiques du réseau local virtuel (VLAN) et exécution de tests de VLAN

Pour afficher les propriétés et les statistiques du réseau local virtuel (VLAN) et exécuter des tests de VLAN

1. Sélectionnez l'un des réseaux locaux virtuels (VLAN) répertoriés.
2. Pour afficher les propriétés de la carte de réseau local virtuel, cliquez sur l'onglet **Informations**.
3. Pour afficher les statistiques de la carte de réseau local virtuel, cliquez sur l'onglet **Statistiques**.
4. Pour exécuter un test de réseau sur la carte de réseau local virtuel, cliquez sur l'onglet **Diagnostic**.

Suppression d'un réseau local virtuel

La procédure ci-dessous s'applique lorsque vous êtes en mode Expert.

Pour supprimer un réseau local virtuel

1. Sélectionnez le réseau local virtuel (VLAN) à supprimer.
2. Dans le menu **Equipes**, sélectionnez **Supprimer VLAN**.
3. Cliquez sur **Appliquer**.
4. Cliquez sur **Oui** lorsque le message indiquant que la connexion au réseau va subir une rupture temporaire s'affiche.

Remarque : Si vous supprimez une équipe, les réseaux locaux virtuels configurés pour cette équipe sont également supprimés.

Configuration de LiveLink pour une équipe de type Smart Load Balancing and Failover (Equilibrage de charge intelligent et reprise) ou SLB (désactivation de la reprise automatique)

LiveLink est une fonctionnalité de BASP disponible pour les équipes de type Smart Load Balancing (SLB) et SLB (désactivation de la reprise automatique). L'objectif de LiveLink est de détecter les pertes de liaison situées après le commutateur et d'acheminer le trafic uniquement via les éléments de l'équipe dont la liaison fonctionne.

Lisez les remarques suivantes avant d'entreprendre la configuration de LiveLink.

Remarque :

- Avant de commencer la configuration de LiveLink™, prenez connaissance de la description de LiveLink. Vérifiez également que chaque cible de test que vous comptez spécifier est disponible et fonctionne. Si, pour une raison quelconque, l'adresse IP de la cible de test est modifiée, vous devez reconfigurer LiveLink. Si, pour une raison quelconque, l'adresse MAC de la cible de test est modifiée, vous devez relancer l'équipe (consultez la rubrique « Dépannage »).
- Une cible de test doit se trouver sur le même sous-réseau que l'équipe, posséder une adresse IP en mode statique valide (ni de diffusion, de multidiffusion ou de monodiffusion) et disposer d'une haute disponibilité (en continu).
- Pour vérifier la connectivité du réseau à la cible de test, utilisez la commande ping sur la cible de test depuis l'équipe.
- Vous pouvez indiquer jusqu'à quatre cibles de test.
- L'adresse IP attribuée à une cible de test ou à un élément d'équipe ne peut pas avoir zéro comme premier ou dernier octet.

Pour configurer LiveLink

1. Dans le menu **Equipes**, sélectionnez **Modifier l'équipe**.
2. Cliquez sur Mode Expert (pour configurer LiveLink à l'aide de l'Assistant de regroupement, voir Utilisation de l'Assistant de regroupement Broadcom).
3. Dans la fenêtre Gérer des membres, cliquez sur l'onglet **Modifier l'équipe**.
4. Sélectionnez **Activer LiveLink**. Les options de configuration de LiveLink s'affichent juste en-dessous.
5. Il est recommandé d'accepter les valeurs par défaut pour les champs **Intervalle de test** (le nombre de secondes entre chaque retransmission d'un paquet de liaison à la cible de test) et **Nombre maximum de nouvelles tentatives de test** (le nombre de réponses manquées consécutives de la cible de test avant qu'une reprise ne soit déclenchée). Pour indiquer d'autres valeurs, cliquez sur l'intervalle de test souhaité dans la liste **Intervalle de test (en secondes)**, puis sur le nombre maximum de tentatives de test dans la liste **Nombre maximum de nouvelles tentatives de test**.
6. Réglez l'**ID de VLAN de test** de sorte qu'il corresponde au réseau local virtuel sur lequel se trouve(nt) la/les cible(s) de test. Ainsi, la valeur d'identification du réseau local virtuel appropriée sera appliquée au paquet de liaison en fonction de la configuration partagée du/des port(s) de commutateur relié(s).

Remarque : chaque équipe pouvant utiliser LiveLink peut seulement communiquer avec les cibles de test sur un VLAN unique. De plus, l'ID VLAN 0 correspond à un réseau non identifié.

7. Sélectionnez **Cible de test 1** et saisissez l'adresse IP cible de l'une ou de toutes les cibles de test.

Remarque : Seule la première cible de test est nécessaire. Vous pouvez indiquer jusqu'à 3 cibles de test supplémentaires à des fins de sauvegarde en attribuant des adresses IP supplémentaires aux autres cibles de test.

8. Sélectionnez l'un des éléments de l'équipe répertoriés et saisissez son adresse IP.

Remarque : Toutes les adresses IP des éléments doivent se trouver sur le même sous-réseau que les cibles de test.

9. Cliquez sur **Mettre à jour**. Répétez ces étapes pour chacun des éléments de l'équipe répertoriés.
10. Cliquez sur **Appliquer/Quitter**.

Enregistrement et restauration d'une configuration

Pour enregistrer une configuration

1. Dans le menu **Fichier**, sélectionnez **Enregistrer l'équipe sous**.
2. Saisissez *le chemin et le nom du nouveau fichier de configuration* et cliquez sur **Enregistrer** (le fichier portera l'extension .bcg).

   Le fichier de configuration est un fichier de texte qui peut être visualisé à l'aide d'un éditeur de texte. Ce fichier contient des informations de configuration à la fois sur la carte et sur l'équipe.

Pour restaurer une configuration

1. Dans le menu **Fichier**, sélectionnez sur **Restaurer l'équipe**.
2. Cliquez sur le nom du fichier à restaurer, puis cliquez sur **Ouvrir**.

Remarque : le cas échéant, recherchez le dossier où se trouve le fichier.

3. Cliquez sur **Appliquer**.
4. Cliquez sur **Oui** lorsque le message indiquant que la connexion au réseau va subir une rupture temporaire s'affiche.
5. Si une configuration est déjà chargée, un message vous demandant si vous souhaitez enregistrer la configuration en cours s'affiche. Cliquez sur **Oui** pour enregistrer la configuration en cours. Sinon, les données de configuration en cours de chargement seront perdues.

Remarque : Si l'équipe est configurée avec de nombreux VLAN et une adresse IP statique, sa restauration peut prendre un temps important.

Affichage des statistiques BASP

La section Statistiques affiche des informations sur les performances des cartes réseau présentes dans une équipe.

Pour afficher les statistiques BASP pour une carte élément de l'équipe ou pour l'intégralité de l'équipe, cliquez sur le nom de cet élément ou de cette équipe dans la liste du volet Gestion des équipes, puis cliquez sur l'onglet **Statistiques**.

Cliquez sur **Actualiser** pour afficher les valeurs les plus récentes pour chaque statistique. Cliquez sur **Redéfinir** pour remettre toutes les valeurs à zéro.

Tx. Paquet. Il s'agit du nombre de paquets transmis.

Tx. Paquet supprimé. Il s'agit du nombre de paquets supprimés.

Tx. Paquet en file d'attente. Il s'agit du nombre de paquets mis en file d'attente.

Rx. Paquet. Il s'agit du nombre de paquets reçus.

Rx. Paquet supprimé. Il s'agit du nombre de paquets supprimés.

Nouvelles tentatives de test. Il s'agit du nombre de réponses manquées consécutives de la cible de test avant qu'une reprise ne soit déclenchée.

Configuration à l'aide de l'utilitaire d'interface de ligne de commande

Outre BACS, vous pouvez également configurer des cartes réseau Broadcom à l'aide de BACSCLI, un utilitaire Broadcom permettant d'afficher des informations et de configurer des cartes réseau à partir d'une console, en mode d'interface de ligne de commande (CLI) non-interactif ou en mode interactif. Tout comme BACS, BACSCLI fournit des informations sur chaque carte réseau et permet d'effectuer des tests détaillés, d'exécuter des diagnostics, d'afficher des statistiques et de modifier les valeurs des propriétés. BACSCLI permet également de regrouper des cartes réseau pour l'équilibrage de charge et la compensation.

Pour obtenir une liste complète des commandes disponibles ainsi que des exemples, reportez-vous au fichier texte Lisez-moi relatif à BACSCLI disponible sur le CD fourni par Dell.

Sur un système doté de cartes réseau Broadcom NetXtreme I et NetXtreme II, BACSCLI est installé lorsque l'installation de BACS est effectuée à l'aide du programme d'installation.

Dépannage de BACS

Problème : Quand je tente d'ouvrir BACS sous un système Linux, le message d'erreur suivant apparaît :

> « Une autre instance du client BACS semble être en cours d'exécution sur ce système. Une seule instance du client BACS peut être exécutée à la fois. Si vous êtes sûr qu'aucun autre client BACS n'est en cours d'exécution, une instance précédente a peut-être été interrompue de manière inattendue. »

Solution : Ce message apparaît si vous tentez d'exécuter une deuxième instance de BACS. Si vous recevez ce message et si vous êtes sûr qu'aucune autre instance de BACS n'est en cours d'exécution, une instance précédente de BACS peut avoir été interrompue de manière inattendue. Pour effacer cette instance, supprimez le fichier « dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0} ».

Section 14 : Caractéristique

Caractéristiques du câble 10/100/1000BASE-T

Tableau 22 : Caractéristiques du câble 10/100/1000BASE-T

Type de port	Connecteur	Type de câble	Longueur maximum
10BASE-T	RJ-45	Paires torsadées non blindées (UTP) de catégorie 3, 4 ou 5	100 m
100/1000BASE-T[1]	RJ-45	Catégorie 5[2] UTP	100 m

[1]Conformément aux normes ISO/IEC 11801:1995 et ANSI/EIA/TIA-568-A (1995), le support 1000BASE-T requiert quatre paires de câbles torsadés de catégorie 5, dont les performances supplémentaires ont été testées selon les procédures d'essai définies dans TIA/EIA TSB95.

[2]CAT 5 est la configuration minimale requise. Les configurations CAT 5e et CAT 6 sont entièrement prises en charge.

Caractéristiques de fonctionnement

Tableau 23 : Caractéristiques de fonctionnement

Fonctionnalité	Caractéristique
Contrôleurs de type PCI Express™ (contrôleurs BCM57XX)	
Interface PCI Express	Largeur de liaison x1, x2, x4
Bande passante agrégée PCI Express (Transmission et réception)	2,5 Gbit/s ou 5,0 Gbit/s
10/100/1000BASE-T	10/100/1000 Mbit/s (en duplex)

Section 15 : Réglementation

Avis FCC - Classe B

Contrôleur Gigabit Ethernet Broadcom NetXtreme II
BCM95721A211
BCM95722A2202

Cet appareil est conforme à la section 15 des règlements FCC. Son fonctionnement est soumis aux deux conditions suivantes : 1) cet appareil ne doit pas causer d'interférence entraînant des nuisances et 2) cet équipement doit accepter toute interférence qu'il est susceptible de recevoir, y compris les interférences pouvant entraîner un fonctionnement indésirable.

L'équipement a été testé et déclaré conforme aux limites des dispositifs numériques de la Classe B définies par l'alinéa 15 du règlement de la FCC. These limits are designed to provide reasonable protection against harmful interference in a residential installation. Cet équipement génère, utilise et peut émettre des fréquences radioélectriques et peut, s'il n'est pas installé et utilisé conformément au manuel d'instructions du fabricant, provoquer des interférences avec les communications radio. Nous ne pouvons cependant pas garantir qu'aucune interférence ne se produira dans le cadre d'une installation particulière. Si cet équipement cause des interférences nuisibles à la réception de la radio ou de la télévision, ce qui peut être déterminé en éteignant et rallumant l'équipement, nous vous conseillons d'essayer de corriger ces interférences en prenant les mesures suivantes :

- Réorientez l'antenne de réception.
- Augmentez la distance séparant l'équipement et le récepteur.
- Connectez l'équipement à une prise sur un circuit différent de celui auquel le récepteur est raccordé.
- Consultez le représentant ou un technicien de radio/télévision qui pourra vous conseiller.

Ne modifiez aucune partie mécanique ou électrique de l'équipement.

Remarque : Si vous changez ou modifiez la carte sans avoir obtenu la permission de Broadcom, vous risquez d’invalider vos droits d’utilisation de l'équipement.

Broadcom Corporation
190 Mathilda Place
Sunnyvale, California 94086 USA

Avis VCCI - Classe B

L'équipement est un produit de classe B selon la norme en matière d'interférences du VCCI (Voluntary Control Council for Interference). S'il est utilisé près d'un poste de radio ou de télévision dans un environnement domestique, il risque de provoquer des interférences radioélectriques. Il convient d'installer et d'utiliser l'équipement conformément aux instructions du manuel du fabricant.

Attention : Les performances de cet équipement risquent de se dégrader en présence de fréquences radioélectriques comprises entre 59 et 66 MHz, provoquant des interférences par conduction. L'équipement reprendra son fonctionnement normal dès la suppression de la source de fréquences radioélectriques.

Avis VCCI - Classe B (Japon)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Réglementation de la CE

БЪЛГАРСКИ Bulgarian	Този продукт отговаря на 2006/95/EC (Нисковолтова директива), 2004/108/EC (Директива за електромагнитна съвместимост) и измененията на Европейския съюз. **Европейски съюз, Клас B** Това устройство на Broadcom е класифицирано за използване в типичната за Клас B жилищна среда. Изготвена е “Декларация за съответствие” според горепосочените директиви и стандарти, която се съхранява в Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ČESKÝ Czech	Bylo ustanoveno, že tento produkt splňuje směrnici 2006/95/EC (nízkonapěťová směrnice), směrnici 2004/108/EC (směrnice EMC) a dodatky Evropské unie. **Evropská unie, třída B** Toto zařízení společnosti Broadcom je klasifikováno pro použití v obvyklém prostředí domácnosti (třída B). „Prohlášení o shodě“ v souladu s výše uvedenými směrnicemi a normami bylo zpracováno a je uloženo v archivu společnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Danish	Dette produkt er fundet i overensstemmelse med 2006/95/EC (Lavvoltsdirektivet), 2004/108/EC (EMC-direktivet) og den Europæiske Unions ændringer. **Den Europæiske Union, Klasse B** Denne Broadcom-enhed er klassificeret til anvendelse i et typisk Klasse B-hjemligt miljø. En "Overensstemmelseserklæring", som er i henhold til foregående direktiver og standarder, er udført og arkiveret hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
NEDERLANDS Dutch	Dit product is in overeenstemming bevonden met 2006/95/EC (Laagspanningsrichtlijn), 2004/108/EC (EMC-richtlijn) en amendementen van de Europese Unie. **Europese Unie/Klasse B** Dit Broadcom-apparaat is geclassificeerd voor gebruik in een typische klasse B woonomgeving. Een “Verklaring van conformiteit” in overeenstemming met de voorgenoemde richtlijnen en standaarden is beschikbaar bij Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
English	This product has been determined to be in compliance with 2006/95/EC (Low Voltage Directive), 2004/108/EC (EMC Directive), and amendments of the European Union. **European Union, Class B** This Broadcom device is classified for use in a typical Class B domestic environment. A “Declaration of Conformity” in accordance with the preceding directives and standards has been made and is on file at Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
EESTLANE Estonian	Antud toode vastab direktiividele 2006/95/EU (Madalpinge direktiiv), 2004/108/EU (EMC direktiiv) ja ELi parandustele. **Euroopa Liit, Klass B** Antud Broadcom toode on klassifitseeritud kasutamiseks tüüpilises B-klassi koduses keskkonnas. Vastavalt ülaltoodud direktiividele ja standarditele on koostatud „Vastavusdeklaratsioon”, mis on arvel ettevõttes Broadcom Corporation, 190 MathildaPlace, Sunnyvale, California 94086, USA.
Finnish	Tämä tuote täyttää Euroopan unionin direktiivin 2006/95/EY (pienjännitedirektiivi) ja direktiivin 2004/108/EY (sähkömagneettisesta yhteensopivuudesta annettu direktiivi), sellaisina kuin ne ovat muutettuina, vaatimukset. **Euroopan unioni, luokka B** Tämä Broadcom-laite on luokiteltu käytettäväksi tyypillisessä luokan B kotiympäristössä. Yllä mainittujen direktiivien ja standardien mukainen vaatimustenmukaisuusvakuutus on tehty, ja sitä säilyttää Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
FRANÇAIS French	Ce produit a été déclaré conforme aux directives 2006/95/EC (Directive sur la faible tension), 2004/108/EC (Directive EMC) et aux amendements de l'Union européenne. **Union européenne, classe B** Cet appareil Broadcom est classé pour une utilisation dans un environnement résidentiel classique (classe B). Une « Déclaration de Conformité » relative aux normes et directives précédentes a été rédigée et est enregistrée auprès de Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.

DEUTSCH German	Es ist befunden worden, dass dieses Produkt in Ubereinstimmung mit 2006/95/EC (Niederspannungs-Richtlinie), 2004/108/EC (EMV-Richtlinie) und Ergänzungen der Europäischen Union steht. **Europäische Union, Klasse B** Dieses Gerät von Broadcom ist für die Verwendung in einer typisch häuslichen Umgebung der Klasse B vorgesehen. Eine Konformitätserklärung in Ubereinstimmung mit den oben angeführten Normen ist abgegeben worden und kann bei Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ΕΛΛΗΝΙΚΟΣ Greek	Το προϊόν αυτό συμμορφώνεται με τις οδηγίες 2006/95/ΕΕ (Οδηγία περί χαμηλής τάσης), 2004/108/ΕΕ (Οδηγία περί ηλεκτρομαγνητικής συμβατότητας), και τροποποιήσεις τους από την Ευρωπαϊκή Ένωση. **Ευρωπαϊκή Ένωση, Κατηγορία Β** Αυτή η συσκευή Broadcom είναι κατάλληλη για χρήση σε ένα σύνηθες οικιακό περιβάλλον κατηγορίας Β. Μία «Δήλωση Συμμόρφωσης» σύμφωνα με τις προηγούμενες οδηγίες και πρότυπα υπάρχει και είναι αρχειοθετημένη στο Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
MAGYAR Hungarian	A termék megfelel a 2006/95/EGK (alacsony feszültségű eszközökre vonatkozó irányelv), a 2004/108/EGK (EMC irányelv) és az Európai Unió ajánlásainak. **Európai Unió, „B" osztály** Ez a Broadcom eszköz „B" osztályú besorolást kapott, tipikus lakossági környezetben való használatra alkalmas. Az előbbiekben ismertetett irányelvek és szabványok szellemében „Megfelelőségi nyilatkozat" készült, amely az irországi Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
PORTUGUÉS Iberian Portuguese	Este produto está em conformidade com 2006/95/EC (Directiva de baixa tensão), com 2004/108/EC (Directiva de compatibilidade electromagnética) e com as alterações da União Europeia. **União Europeia, Classe B** Este dispositivo Broadcom está classificado para utilização num ambiente doméstico típico Classe B. Foi elaborada uma "declaração de conformidade" de acordo com as normas e directivas anteriores, encontrando-se arquivada na Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ITALIANO Italian	Il presente prodotto è stato determinato essere conforme alla 2006/95/CE (Direttiva Bassa Tensione), alla 2004/108/CE (Direttiva CEM) e a rettifiche da parte dell'Unione Europea. **Unione Europea, Classe B** Il presente dispositivo Broadcom è classificato per l'uso nel tipico ambiente domestico di Classe B. Una "Dichiarazione di conformità" secondo gli standard e le direttive precedenti è stata emessa e registrata presso Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
LATVISKS Latvian	Sis izstrādājums atbilst direktīvām 2006/95/EK (Direktīva par zemsprieguma iekārtām), 2004/108/EK (Direktīva par elektromagnētisko saderību) un to labojumiem Eiropas Savienības ietvaros. **Eiropas Savienība, klase B** Šī firmas Broadcom ražotā ierīce ir atzīta par derīgu darbam B klasei atbilstošos mājas apstākļos. "Atbilstības deklarācija", kas ir saskaņā ar iepriekšminētajām direktīvām un standartiem, ir sastādīta un tiek glabāta firmā Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Lithuanian	Buvo nustatyta, kad šis produktas atitinka direktyvą 73/23/EEB (žemos įtampos direktyvą), 89/336/EEB (elektromagnetinio suderinamumo direktyvą) ir Europos Sąjungos pataisas. **Europos Sąjunga, B klasė** Šis „Broadcom" prietaisas yra klasifikuotas naudoti įprastose B klasės gyvenamosiose aplinkose. Atitikties deklaracija pagal visas galiojančias direktyvas ir standartus yra sudaryta ir saugoma įrašyta faile Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.

Maltese	Gie stabbilit li dan il-prodott hu konformi ma' 2006/95/KE (Direttiva dwar il-Vultaġġ Baxx), 2004/108/KE (Direttiva EMC), u emendi ta' l-Unjoni Ewropea. **Unjoni Ewropea, Klassi B** Dan it-tagħmir Broadcom hu kklassifikat għall-użu f'ambjent residenzjali tipiku ta' Klassi B. Saret "Dikjarazzjoni ta' Konformità" b'konformità mad-direttivi u ma' l-istandards imsemmijin qabel, u din tinsab iffajljata għand Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
POLSKI Polish	Niniejszy produkt został określony jako zgodny z dyrektywą niskonapięciową 2006/95/WE i dyrektywą zgodności elektromagnetycznej 2004/108/WE oraz poprawkami do nich. **Unia Europejska, klasa B** Niniejsze urządzenie firmy Broadcom zostało zakwalifikowane do klasy B, do użytku w typowych środowiskach domowych. Zgodnie ze stosownymi dyrektywami i normami została sporządzona „Deklaracja zgodności", która jest dostępna w aktach firmy Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ROMÂN Romanian	S-a stabilit că acest produs respectă cerinţele Directivei 2006/95/CE privind echipamentele de joasă tensiune, ale Directivei 2004/108/CE (Directiva EMC) privind compatibilitatea electromagnetică şi ale amendamentelor Uniunii Europene. **Uniunea Europeană, Clasa B** Acest echipament Broadcom este clasificat pentru utilizare într-un mediu casnic tipic de Clasă B. Conform directivelor şi standardelor de mai sus, a fost emisă o „Declaraţie de Conformitate", arhivată la sediul Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
SLOVENSKÝ Slovakian	Tento výrobok vyhovuje požiadavkám smernice 2006/95/EC (smernica o nízkom napätí), 2004/108/EC (smernica o elektromagnetickej kompatibilite) a neskorším zmenám a doplnkom Európskej. **Európska únia, Trieda B** Toto zariadenie Broadcom triedy B je určené pre domáce prostredie. „Vyhlásenie o zhode" vydané v súlade s predchádzajúcimi smernicami a štandardmi sa nachádza v spoločnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Slovenian	Ta izdelek je v skladu z 2006/95/ES (Direktiva o nizki napetosti), 2004/108/ES (Direktiva o elektromagnetni združljivosti) in dopolnili Evropske unije. **Evropska unija, razred B** Ta Broadcomova naprava je razvrščena za uporabo v značilnem bivalnem okolju razreda B. «Izjava o skladnosti» je bila sprejeta v skladu s predhodnimi direktivami in standardi in je shranjena na naslovu Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ESPAÑOL Spanish	Este producto se ha fabricado de conformidad con la Directiva para bajo voltaje 2006/95/EC (Low Voltage Directive), la Directiva para compatibilidad electromagnética 2004/108/EC (EMC Directive) y las enmiendas de la Unión Europea. **Unión Europea, Clase B** Este dispositivo Broadcom está clasificado para ser utilizado en un entorno doméstico convencional de Clase B. Se ha realizado una "Declaración de conformidad" de acuerdo con las directivas y estándares anteriores y está archivada en Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
SVENSK Swedish	Denna produkt överensstämmer med EU-direktivet 2006/95/EC (lågspänningsdirektivet), 2004/108/EC (EMC direktivet), och andra ändringar enligt den Europeiska unionen. **Europeiska unionen, klass B** Den här Broadcom-enheten är klassificerad för användning i vanlig klass B-bostadsmiljö. En "Försäkran om överensstämmelse" i enlighet med de föregående direktiven och standarderna har framställts och finns registrerad hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
TÜRK Turkish	Bu ürünün 2006/95/EC (Düşük Voltaj Direktifi), 2004/108/EC (EMC Direktifi), ve Avrupa Birliği'nin ilavelerine uygun olduğu belirlenmiştir. **Avrupa Birliği, B Sınıfı** Bu Broadcom cihazı,tipik bir B sınıfı, ev içi ortamda kullanılmak üzere sınıflandırılmıştır. Yukarıda belirtilen direktifler ve standarlara uygun olarak, bir "Uygunluk Beyanı" hazırlanmıştır, ve Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.

Réglementation canadienne (Canada uniquement)

Industry Canada, Class B

This Class B digital apparatus complies with Canadian ICES-003.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by Broadcom could void your authority to operate this equipment.

Industry Canada, classe B

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Avis : Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par Broadcom y sont apportés.

Avis MIC (République de Corée uniquement)

Dispositif de CLASSE B

Contrôleur Gigabit Ethernet Broadcom NetXtreme II
BCM95721A211
BCM95722A2202

기종별	사용자안내문
B급 기기 (가정용)	이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다.

1. 기기의 명칭(모델명) : BCM95721A211
2. 인증번호 : E-G021-04-2613(B)
3. 인증받은 자의 상호 : Broadcom
4. 제조년월일: 5/12/2004
5. 제조자/제조국가 : Foxconn/China

1. 기기의 명칭(모델명) : BCM95722A2202G
2. 인증번호 : BCM-BCM95722A2202G (B)
3. 인증받은 자의 상호 : BROADCOM
4. 제조년월일: 04/30/2007
5. 제조자/제조국가 : Foxconn/China

Veuillez noter que ce dispositif a été approuvé pour un usage non commercial et peut fonctionner en tous lieux, y compris les zones résidentielles.

BSMI

BSMI通告（僅限於台灣）

大多數的 Dell 電腦系統被 BSMI（經濟部標準檢驗局）劃分爲乙類數位裝置。但是，使用某些選件會使有些組態的等級變成甲類。若要確定您的電腦系統適用等級，請檢查所有位於電腦底部或背面板、擴充卡安裝托架，以及擴充卡上的 BSMI 註冊標籤。如果其中有一甲類標籤，即表示您的系統爲甲類數位裝置。如果只有 BSMI 的檢磁號碼標籤，則表示您的系統爲乙類數位裝置。

一旦確定了系統的 BSMI 等級，請閱讀相關的 BSMI 通告。請注意，BSMI通告規定凡是未經 Dell Inc. 明確批准的擅自變更或修改，將導致您失去此設備的使用權。

此裝置符合 BSMI（經濟部標準檢驗局）的規定，使用時須符合以下兩項條件：

- 此裝置不會產生有害干擾。
- 此裝置必須能接受所接收到的干擾，包括可能導致無法正常作業的干擾。

乙類

此設備經測試證明符合 BSMI（經濟部標準檢驗局）之乙類數位裝置的限制規定。這些限制的目的是爲了在住宅區安裝時，能防止有害的干擾，提供合理的保護。此設備會產生、使用並散發射頻能量；如果未遵照製造廠商的指導手冊來安裝和使用，可能會干擾無線電通訊。但是，這並不保證在個別的安裝中不會產生干擾。您可以透過關閉和開啓此設備來判斷它是否會對廣播和電視收訊造成干擾；如果確實如此，我們建議您嘗試以下列一種或多種方法來排除干擾：

- 重新調整天線的接收方向或重新放置接收天線。
- 增加設備與接收器的距離。
- 將設備連接至不同的插座，使設備與接收器連接在不同的電路上。
- 請向經銷商或有經驗的無線電／電視技術人員查詢，以獲得幫助。

Section 16 : Procédures de dépannage

Diagnostic du matériel

Vous pouvez effectuer des tests de diagnostic de bouclage pour tester la carte physique. Ces tests permettent d'accéder à l'interface de diagnostic interne/externe de la carte, à laquelle des données en paquets sont transmises par le biais de la liaison physique. dans un environnement Windows, voir Exécution des tests de diagnostic).

Echecs des tests de diagnostic BACS

Si l'un des tests suivants échoue lors de l'exécution des tests de diagnostic depuis l'onglet Exécution des tests de diagnostic de BACS, cela signifie que la carte NIC ou LOM installée sur le système peut présenter un problème matériel.

- Registres de contrôle
- Registres MII
- EEPROM
- Mémoire interne
- Unités centrales sur puce
- Interruption
- Bouclage - MAC
- Bouclage - PHY
- Test LED (Test des DEL)

Vous trouverez ci-dessous des procédures de dépannage pouvant vous aider à corriger cet échec.

1. Retirez le périphérique défectueux puis réinstallez-le dans son logement, en vous assurant que la carte y est bien positionnée de l'avant vers l'arrière.
2. Exécutez à nouveau les tests.
3. Si la carte échoue de nouveau, remplacez-la par une autre carte de même modèle et exécutez le test. Si le test réussit avec la carte qui fonctionne, contactez le fournisseur de votre matériel pour toute assistance concernant le périphérique défectueux.
4. Mettez l'ordinateur hors tension, débranchez-le, puis réinitialisez le système.

5. Supprimez puis réinstallez le logiciel de diagnostic.
6. Contactez le fournisseur de votre matériel.

Echecs du test réseau BACS

En général, les échecs Test du réseau BACS sont dus à des problèmes de configuration sur le réseau ou au niveau des adresses IP. Vous trouverez ci-dessous les étapes courantes à suivre lors du dépannage du réseau.

1. Vérifiez que le câble est connecté et que la liaison est correcte.
2. Vérifiez que les pilotes sont chargés et activés.
3. Remplacez le câble connecté à la carte NIC/LOM.
4. Vérifiez que l'adresse IP est attribuée correctement en utilisant la commande « ipconfig » ou à l'aide de l'outil d'affectation IP du système d'exploitation.
5. Vérifiez que l'adresse IP du réseau auquel est connectée la carte est correcte.

Liste de vérification pour le dépannage

Attention : avant d'ouvrir le boîtier de votre système, prenez connaissance des Mesures de sécurité.

La liste de vérification suivante recense les mesures à prendre pour résoudre les problèmes survenant lors de l'installation de la carte Gigabit Ethernet NetXtreme de Broadcom ou de son exécution dans votre système.

- Examinez tous les câbles et les connexions. Vérifiez que les câbles connectés à la carte réseau et le commutateur sont fixés correctement. Assurez-vous que la longueur du câble et ses caractéristiques nominales sont conformes aux normes répertoriées dans Connexion des câbles réseau.
- Vérifiez l'installation de la carte en vous référant à Installation du matériel. Assurez-vous que la carte est correctement positionnée dans le logement. Vérifiez que le matériel ne présente pas de problèmes, tels que la détérioration évidente de composants de carte ou du connecteur de bord PCI.
- Vérifiez les paramètres de configuration et modifiez-les en cas de conflit avec un autre périphérique.
- Vérifiez si votre système utilise le BIOS le plus récent.
- Essayez d'insérer la carte dans un autre logement. Si cette nouvelle position assure son fonctionnement, il se peut que le logement d'origine de votre système soit défectueux.
- Remplacez la carte défectueuse par une carte en bon état de fonctionnement. Si la deuxième carte fonctionne dans le logement où la première ne marchait pas, cette première carte est probablement défectueuse.
- Installez la carte dans un autre système qui fonctionne et réexécutez les tests. Si la carte a subi les tests avec succès dans le nouveau système, il se peut que le système d'origine soit défectueux.
- Retirez toutes les autres cartes du système et réexécutez les tests. Si la carte subit les tests avec succès, il se peut que les autres cartes causent le conflit.

Vérification de la liaison et de l'activité réseau

Voir Vérification de la connectivité du réseau et Pour consulter des informations sur une carte pour contrôler l'état de la liaison au réseau et de l'activité indiqué par les voyants de port.

Vérification du chargement des pilotes en cours

Windows

Voir Pour consulter des informations sur une carte pour obtenir des informations utiles sur la carte, l'état de la liaison et la connectivité du réseau.

Linux

Pour vérifier si le pilote Linux TG3 est chargé correctement, exécutez :

```
lsmod | grep tg3
```

Si le pilote est chargé, une ligne similaire à celle figurant ci-dessous apparaît, où *taille* correspond à la taille du pilote en octets et *n* correspond au nombre de cartes configurées.

Tableau 24 : Pilote Linux

Module	***size***	***Utilisateur***
TG3	*size*	*n*

Exécution d'un test de longueur de câble

Sous Windows, vous pouvez effectuer un test de longueur de câble. Voir Analyse des câbles pour obtenir des informations sur l'exécution d'un test de longueur de câble.

Vérification de la connectivité du réseau

Remarque : Lorsque vous utilisez des vitesses de liaison forcées, assurez-vous que la carte et le commutateur sont forcés à la même vitesse ou qu'ils sont tous les deux configurés pour la négociation automatique.

Windows

Utilisez la commande ping pour déterminer si la connectivité du réseau fonctionne.

Remarque : la connectivité du réseau peut également être testée à l'aide de la fonction Test du réseau de l'application Broadcom Advanced Control Suite 2.

1. Vérifiez que les pilotes sont chargés et activés.
2. Vérifiez que le câble est connecté et que la liaison est correcte.
3. Cliquez sur **Démarrer**, puis sur **Exécuter**.
4. Saisissez **cmd** dans la fenêtre **Ouvrir**, puis cliquez sur **OK**.
5. Saisissez **ipconfig /all** pour afficher la connectivité du réseau à tester.
6. Vérifiez que l'adresse IP du réseau auquel est connectée la carte est correcte.
7. Saisissez **ping Adresse IP**, puis appuyez sur ENTREE.

Les statistiques ping s'affichent et indiquent si la connectivité du réseau fonctionne.

Linux

Pour vérifier si l'interface Ethernet fonctionne, exécutez **ifconfig**. **netstat -i** peut être utilisé pour obtenir des statistiques sur l'interface Ethernet. Reportez-vous à la section Logiciel pilote pour Linux pour plus d'informations sur **ifconfig** et **netstat**.

Vérifiez si la connexion a été établie avec un hôte IP sur le réseau à l'aide de la commande ping :

Sur la ligne de commande, saisissez **ping Adresse IP**, puis appuyez sur ENTREE.

Les statistiques ping s'affichent et indiquent si la connectivité du réseau fonctionne.

Boot Agent de Broadcom

Problème : Impossible d'obtenir les paramètres réseau via DHCP en utilisant PXE.
Solution : Pour un fonctionnement correct, vérifiez que le protocole STP (Spanning Tree Protocol) est désactivé ou que le mode portfast (pour Cisco) est activé sur le port auquel le client PXE est connecté. Par exemple, activez spantree portfast 4/12.

Broadcom Advanced Server Program (BASP)

Problème : Après le retrait physique d'un NIC appartenant à une équipe, puis un redémarrage, l'équipe ne se comporte pas comme prévu.
Solution : Pour retirer physiquement du système un NIC appartenant à une équipe, vous devez d'abord le supprimer de l'équipe. Si vous ne procédez pas à cette opération avant d'arrêter le système, l'équipe risque de se décomposer au prochain redémarrage et de présenter par la suite un comportement inattendu.

Problème : Les modifications de regroupement que j'avais apportées à l'aide de INETCFG n'ont pas été appliquées.
Solution : Lorsque vous modifiez une équipe à l'aide de INETCFG, il est possible que vous deviez redémarrer après la réinitialisation pour que les modifications soient prises en compte.

Débogage du noyau via Ethernet

Problème : Lorsque vous tentez d'effectuer le débogage du noyau via un réseau Ethernet sur un système Windows 8.0 ou Windows Server 2012, le système ne démarre pas. Ce problème peut survenir avec certaines cartes sur des systèmes sur lesquels le système d'exploitation Windows 8.0 ou Windows Server 2012 est configuré pour le mode UEFI. Une erreur du micrologiciel peut s'afficher à l'écran, indiquant qu'une exception Interruption non masquable est survenue dans l'environnement de prédémarrage UEFI.

Solution : Reportez-vous à la rubrique 2920163 de la base de connaissances Microsoft, « Erreur d'interruption non masquable lors du démarrage sur un système configuré pour un débogage du noyau via Ethernet ».

Divers

Problème : Les propriétés Large Send Offload (Déchargement important à l'émission) et Checksum Offload (Déchargement de la somme de contrôle) ne fonctionnent pas sur mon équipe.
Solution : Si une des cartes de l'équipe ne prend pas en charge la propriété Large Send Offload (Déchargement important à l'émission), celle-ci ne peut pas fonctionner pour l'équipe. Retirez de l'équipe la carte qui ne prend pas en charge Large Send Offload (Déchargement important à l'émission) ou remplacez-la par une qui le fait. La solution est la même pour Checksum Offload (Déchargement de la somme de contrôle).