Broadcom® NetXtreme® BCM57XX
ユーザー ガイド

最終改訂日：2015 年 2 月

2CS57XX-CDUM513-R

このマニュアルの内容は、予告なしに変更される場合があります。

最終改訂日：2015 年 2 月

2CS57XX-CDUM513-R

目次

セクション 1: 特長と機能

機能の説明

Broadcom NetXtreme Gigabit Ethernet アダプタは、PCI Express™ に準拠するシステムを Gigabit Ethernet ネットワークに接続するためのデバイスです。Broadcom NetXtreme Gigabit Ethernet アダプタには、毎秒 1 ギガビットの最大速度でデータを転送する技術が採用されています。これは、高速イーサネット アダプタの処理速度の 10 倍にあたります。

Broadcom のチーム化ソフトウェアを使用すると、ロード バランスおよびフォルト トレランス機能を実現するために、ネットワークをバーチャル LAN (VLAN) に分割したり、複数のネットワーク アダプタをチームにグループ化したりすることができます。チームに関する詳細は、チーム化および Broadcom Gigabit Ethernet のチーム化サービスを参照してください。VLAN に関しては、仮想 LAN を参照してください。Windows オペレーティング システムでチームの設定および VLAN の作成を行う方法については、「チームの設定」を参照してください。

機能

以下に、Broadcom NetXtreme Gigabit Ethernet アダプタがサポートしているオペレーティング システムでの各種機能を一覧します。

- 統合クアッド 10/100/1000BASE-T およびクアッド 1000BASE-X/SGMII 1.25 Gbaud SerDes トランシーバー
- IEEE 規格 802.3az-2010 に準拠する Energy Efficient Ethernet™
- IEEE 802.3ap 第 73 条の自動ネゴシエーション
- クアッド 10/100/1000BASE-T 全二重通信 / 半二重通信 MAC
- クアッド 1000BASE-X/SGMII 全二重通信 / 半二重通信 MAC
- 自動 MDI クロス オーバー
- x4 PCI Express v2.0 (5 GT/s または 2.5 GT/s)
- MSI および MSI-X 機能 — 最大 17 個の MSI-X ベクタ
- VMware NetQueue と Microsoft VMQ の I/O 仮想化のサポート
  - 17 個の受信キューと 16 個の転送キュー
  - ホストへのキューごとの割り込みをサポートする 17 個の MSI-X ベクタ
- 柔軟な MSI-X ベクタから転送 / 受信キューへのアソシエーション
- PCI Express Base Specification v2.0 に対する TLP Processing Hint (TPH) ECN
- 機能レベル リセット
- キューごとの MSI-X ベクタと UDP RSS ハッシュ タイプをサポートした Receive Side Scaling (RSS、受信側スケーリング)
- キューごとの MSI-X ベクタをサポートした Transmit Side Scaling (TSS、転送側スケーリング) とマルチ Tx キュー
- 最大 9600 バイトのペイロードを含むジャンボ フレームのサポート
- 仮想 LAN (VLAN) サポート — IEEE 802.1q VLAN タギング
- TCP、IP、UDP チェックサム オフロード
- Large Send Offload (LSO、大量送信オフロード)、TCP Segmentation Offload (TSO、TCP 区分化オフロード)
- IEEE 1588 および IEEE 802.1AS の時刻同期実装のハードウェア対応
- IEEE 802.3x フロー コントロール
- SMBus 2.0 インターフェイス
- SNMP MIB II、Ethernet に近い MIB、Ethernet MIB (IEEE 802.3z、第 30 条) の統計
- ACPI 電源管理への準拠
- 中央電源管理ユニット (CPMU) による高度な電源管理
- 効率的な統合スイッチング レギュレータ コントローラ
- チップ上の温度モニタ
- PCI Express CLKREQ のサポート
- 電源管理オフロード (PM Offload)
- シリアル Flash および EEPROM NVRAM のサポート (Flash の自動設定)
- 内部 SRAM での ECC エラー検出とエラー訂正
- JTAG 境界スキャンのサポート

電源の管理

Wake on LAN (Magic Packet、Wake Up Frame、特定パターン) をサポートします。

注：システム停止時、起動信号待機中のアダプタ速度接続は 10 Mbps または 100 Mbps ですが、1000 Mbps 対応のスイッチに接続した場合は、システム実行時に 1000 Mbps に戻ります。Wake on LAN の使用を試行するシステムは、1000 Mbps の動作と 10/100 Mbps の動作が可能なスイッチに接続する必要があります。

適応型割り込み周波数

トラフィックの状態に応じて、アダプタ ドライバがインテリジェントにホストの割り込み周波数を調整し、アプリケーション全体の処理量を向上します。トラフィックが少ないと、アダプタ ドライバはパケットを受信するごとにホストに割り込み、待ち時間を最短にします。トラフィックが多くなると、アダプタは 1 つのホストで複数の、連続的な着信パケットに割り込むよう命令し、ホストの CPU サイクルを維持します。

デュアル DMA チャネル

Broadcom NetXtreme Gigabit Ethernet アダプタ 上の PCIe インターフェイスは、同時読み込み・書き込み動作用に、2 種類の独立した DMA チャネルで構成されています。

埋め込み型 RISC プロセッサつき ASIC

Broadcom NetXtreme Gigabit Ethernet アダプタのコア コントロールは、強力に統合された高性能 ASIC 内に常駐しています。ASIC には RISC プロセッサが内蔵されています。この機能性により、新しい機能のカードへの追加がフレキシブルに行えるうえ、ソフトウェアのダウンロードにより今後必要とされるネットワークへの対応が可能です。

Broadcom NetXtreme の管理操作 (DMTF、SMASH、DASH、NC-SI パススルーなど) は、従来のネットワーク処理エンジンとは分離された高性能アプリケーション プロセッサ エンジン (APE) 上で実行されます。

Broadcom Advanced Control Suite

Broadcom のチーム化ソフトウェアのコンポーネントである Broadcom Advanced Control Suite (BACS) は、統合型ユーティリティであり、システムに取り付けられている各ネットワーク アダプタに関する役に立つ情報を提供します。BACS ユーティリティでは、各アダプタの詳細なテスト、診断、分析を実行できるうえ、プロパティ値の変更や各アダプタのトラフィック情報の表示も行えます。BACS は Windows OS でチームの設定および VLAN の追加に使用します。手順などについて詳しくは、「Broadcom Advanced Control Suite を使用する」をご覧ください。

サポートされるオペレーティング環境

Broadcom NetXtreme Gigabit Ethernet アダプタは、次のオペレーティング システムをサポートするソフトウェアを装備しています。

- Microsoft® Windows® (32 ビットおよび 64 ビット拡張)
- Linux® (32 ビットおよび 64 ビット拡張)
- VMware
- Oracle Solaris

ネットワーク リンクとアクティビティの状態の通知

銅線イーサネット接続の場合、ネットワーク リンクとアクティビティの状態は、13 ページの表 1 :「RJ-45 ポート LED が示すネットワーク リンクとアクティビティの状態」に示すように、RJ-45 コネクタにある LED の状態で示されます。Broadcom Advanced Control Suite も、ネットワーク リンクとアクティビティの状態についての情報を提供します (アダプタ情報の表示を参照)。

表 1:RJ-45 ポート LED が示すネットワーク リンクとアクティビティの状態

ポート LED	*LED の状態*	*ネットワークの状態*
リンク LED	OFF	リンクなし (ケーブルが外れている)
	点灯	リンク
アクティビティ LED	OFF	ネットワークのアクティビティなし
	点滅	ネットワークの活動

セクション 2: チーム化

注：次のトピックの詳細については、Broadcom Gigabit Ethernet のチーム化サービスを参照してください。

- 用語集 (用語と略語)
- チーム化の概念
- ソフトウェア コンポーネント
- ハードウェア要件
- サポートされる機能 (チーム タイプ別)
- チーム タイプの選択
- チーム化の仕組み
- アーキテクチャ
- チーム タイプ
- ドライバ サポート (オペレーティング システム別)
- サポートされるチーム化の速度
- チーム化とその他の高度なネットワーク機能
- 全般的なネットワークに関する考慮事項
- アプリケーションに関する考慮事項
- チーム化に関する問題のトラブルシューティング
- よくある質問
- イベント ログのメッセージ

概要

アダプタのチーム化では、ネットワーク アダプタをグループ化し、チームとして機能させることができます。チーム化の利点として、VLAN に対するメンバーシップ、アダプタ間のロード バランシング機能、フォルト トレランスの提供などがあります。これらの利点を組み合わせることで、チームを異なる VLAN に参加させた状態で、Load Balance メンバー向けのロード バランシング機能とフェイルオーバーの機能を連結できます。

BASP (Broadcom Advanced Server Program) は Broadcom のチーム化ソフトウェアです。Windows オペレーティング システムの場合、BASP は BACS (Broadcom Advanced Control Suite) ユーティリティで設定します。Linux オペレーティング システムの場合は、チャネル結合でチーム化を実行します (チャネル結合によるチーム化を参照)。

BASP では、以下の 4 タイプのロード バランシング チームがサポートされています。

- Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー
- リンク集約 (802.3ad)
- 通有中継 (FEC/GEC)/802.3ad-Draft Static
- スマート ロード バランス (SLB) (自動フォールバックはディスエーブル)

ロード バランシングとフォルト トレランス

チーム化を行うことで、トラフィックのロード バランシングとフォルト トレランス (ネットワーク接続に失敗した場合に、アダプタの動作を冗長化すること) が実現できます。同じシステムに複数のアダプタが取り付けられているときは、アダプタを最大 16 のチームにグループ化することができます。

各チームは最大 8 つのアダプタで構成することができ、1 つのアダプタを Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー (SLB) または SLB (自動フォールバックはディスエーブル) チーム タイプのスタンバイ アダプタとして使用します。アダプタ、ケーブル、またはスイッチの不良のために、アダプタのチーム メンバー通信でトラフィックが認識されない場合、負荷はアクティブな接続が保たれている残りのチーム メンバーに分散されます。すべてのプライマリ アダプタで障害が発生した場合、トラフィックはスタンバイ アダプタに割り当てられます。このため、既存のセッションが維持され、ユーザーへの影響はありません。

チーム タイプ

サポートされるオペレーティング システムで使用可能なチーム タイプを下の表に示します。

表 2: チーム タイプ

オペレーティング システム	使用可能なチーム タイプ
Windows Server 2008 と Windows Server 2012	Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー リンク集約 (802.3ad) 通有中継 (FEC/GEC)/802.3ad-Draft Static スマート ロード バランス (SLB) (自動フォールバックはディスエーブル) **注 :** Windows Server 2012 には、「NIC チーミング」というビルトイン チーミング サポートがあります。同じアダプタに対して、ユーザーが NIC チーミングと BASP を同時に使用してチーム化を有効にすることはお勧めできません。
Linux	結合カーネル モジュールとチャネル結合インターフェイスを使用するチーム アダプタ。詳細については、Linux の文書類を参照してください。

Smart Load Balancing™ (スマート ロード バランス) およびフェイルオーバー

Smart Load Balancing™ およびフェイルオーバーは、IP フローに基づくロード バランシングを Broadcom で実現します。この機能は、双方向で複数のアダプタ (チーム メンバー) による IP トラフィックのバランシングをサポートします。このチーム タイプでは、チーム内のすべてのアダプタは、個別の MAC アドレスを持っています。また、自動故障検出と、別のチーム メンバーまたはホット スタンバイ メンバーに対する動的フェイルオーバーが行われます。この処理は、レイヤ 3 プロトコル (IP) からは独立しており、既存のレイヤ 2 スイッチとレイヤ 3 スイッチで実行されます。このチーム タイプには、中継、リンク集約などのスイッチのコンフィギュレーションは必要ありません。

メモ：

- SLB チームの設定時に LiveLink™ をイネーブルしない場合は、スイッチまたはポートでスパニング ツリー プロトコル (STP) をディスエーブルするようにしてください。これにより、フェイルオーバーの実行時にスパニング ツリーのループが決定されるまでのダウンタイムを最低限に抑えることができます。LiveLink は、このような問題を可能な限り回避します。
- 一方のチーム メンバーが 1000 Mbit/ 秒でリンクされ、もう一方のチーム メンバーが 100 Mbit/ 秒でリンクされている場合、ほとんどのトラフィックは 1000 Mbit/ 秒のチーム メンバーによって処理されます。

リンク集約 (802.3ad)

このモードはリンク集約をサポートし、IEEE 802.3ad (LACP) 仕様に準拠しています。コンフィギュレーション ソフトウェアを使用すると、任意のチーム内でどのアダプタに分配するかを動的に設定することができます。リンクのパートナーが 802.3ad リンクに正しく設定されていない場合は、エラーが検出され記録されます。このモードでは、チーム内のすべてのアダプタが同じ MAC アドレスの受信パケットに設定されます。アウトバウンドのロードバランシング スキームは BASP ドライバにより決定されます。インバウンド パケットのロード バランシング スキームは、チームのリンク パートナーにより決定されます。このモードでは、少なくとも 1 つのリンク パートナーがアクティブ モードとされている必要があります。

通有中継 (FEC/GEC)/802.3ad-Draft Static

通有中継 (FEC/GEC)/802.3ad-Draft Static チーム タイプは、同じ MAC アドレスに対するパケットを受信するように設定する点で、リンク集約 (802.3ad) チーム タイプと非常に似ています。ただし、通有中継 (FEC/GEC)/802.3ad-Draft Static チーム タイプでは、LACP または マーカー プロトコルはサポートされません。アダプタのリンク パートナーが独自仕様のトランキング方法をサポートするよう静的に設定されている環境であれば、このチーム タイプは使用可能です。たとえば、Lucent の OpenTrunk や Cicso の FEC (Fast EtherChannel) で使用可能です。基本的に、このチーム タイプは、リンク集約 (802.3ad) チーム タイプの簡易バージョンといえます。リンク集約制御プロトコル (LACP) には複数の仕様が存在するため、この方法はとても簡易的なものです。他のチーム タイプと同様に、チームの作成、およびさまざまなチームに対する物理的なアダプタの割り当ては、ユーザー コンフィギュレーション ソフトウェアで静的に行います。

通有中継 (FEC/GEC/802.3ad-Draft Static) チーム タイプは、受発信のトラフィックのロード バランシングとフェイルオーバーをサポートしています。

スマート ロード バランス (SLB) (自動フォールバックはディスエーブル)

SLB (自動フォールバックはディスエーブル) チーム タイプは、Smart Load Balancing およびフェイルオーバー チーム タイプと同一です。ただし、スタンバイ メンバーがアクティブで、プライマリ メンバーが再びオンラインになった場合、チームはプライマリ メンバーに切り替えずに、スタンバイ メンバーをそのまま使用するところが異なります。

チームに割り当てられたプライマリ アダプタがディスエーブルされた場合、チームは自動フォールバックが発生する Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー チーム タイプとして機能します。

チーム内のプライマリ インターフェイスはすべて、トラフィックの一部の送受信などのロード バランシング動作に利用されます。スタンバイ インターフェイスは、すべてのプライマリ インターフェイスがリンク切断された場合に代用されます。

フェイルオーバーのチーム化を行うと、万がーネットワーク接続に失敗した場合に、アダプタの動作が冗長化されます (フォルト トレランス)。アダプタ、ケーブル、スイッチ ポートなどの不良によりチーム内のプライマリ アダプタの接続が切断される場合、セカンダリ チーム メンバーがアクティブになり、本来プライマリ アダプタに割り当てられていた受発信トラフィックをリダイレクトします。セッションは継続され、ユーザーに影響が及ぶことはありません。

Smart Load Balancing およびフェイルオーバー/ SLB (自動フォールバックはディスエーブル) チーム タイプの制限事項

Smart Load Balancing™ (SLB、スマート ロード バランス) は、プロトコル固有のスキームです。

表 3:Smart Load Balancing

オペレーティング システム	*フェイルオーバー/ フェイルバック ー Broadcom 全製品*	*フェイルオーバー/ フェイルバック ー 非 Broadcom 製品*
プロトコル	***IP***	***IP***
Windows Server 2008	Y	Y
Windows Server 2008 R2	Y	Y
Windows Server 2012	Y	Y
オペレーティング システム	***負荷バランス ー Broadcom 全製品***	***負荷バランス ー 非 Broadcom 製品***
プロトコル	***IP***	***IP***
Windows Server 2008	Y	Y
Windows Server 2008 R2	Y	Y
Windows Server 2012	Y	Y
Windows Server 2012 R2	Y	Y

凡例 : Y = yes
N = no
N/S = サポートなし

Smart Load Balancing チーム タイプは、スイッチ ポートを特殊な中継モードに設定しなくても、すべてのイーサネット スイッチで動作します。IP トラフィックのみ、発信・戻りの双方向でロード バランスされます。その他のプロトコル パケットは、1 つのプライマリ インターフェイスのみで送受信されます。非 IP トラフィックのフェイルオーバーは、Broadcom ネットワーク アダプタ以外ではサポートされていません。通有中継チーム タイプでは、何らかのポート中継モード (たとえば、Cisco の Gigabit EtherChannel などの各スイッチ メーカーのリンク集約モード) をサポートするイーサネット スイッチが必要になります。通有中継チーム タイプはプロトコルに依存せず、すべてのトラフィックはロード バランスが行われ、フォルト トレランスの対象になります。

注 : チームの設定時に LiveLink™ をイネーブルしない場合は、スイッチでスパニング ツリー プロトコル (STP) をディスエーブルするようにしてください。これにより、フェイルオーバーの実行時にスパニング ツリーのループが決定されるまでのダウンタイムを最低限に抑えることができます。LiveLink は、このような問題を可能な限り回避します。

LiveLink™ 機能

LiveLink™ 機能は BASP の機能の 1 つで、Smart Load Balancing™ と Failover のチーム タイプでのみ動作します。LiveLink は、スイッチで発生したネットワーク接続を検出し、リンクが有効になっているチーム メンバーのみのトラフィックをルーティングします。この機能は、チーム化ソフトウェアでも使用することができます (スマート ロード バランスおよびフェイルオーバー/ スマート ロード バランス (自動フォールバックはディスエーブル) チームの LiveLink を設定するの説明を参照)。チーム化ソフトウェアは、定期的に各チーム メンバーからリンク パケットを発行して、1 つまたは複数の特定ネットワーク アダプタのプローブ (検査) を行います。プローブ対象は、リンク パケットを受信すると応答を返します。設定された回数の試行を行った後、チーム メンバーが一定時間内に応答を検出しない場合、チーム化ソフトウェアはそのチーム メンバーとのトラフィックの送受信を中断します。その後、そのチーム メンバーがプローブ対象からの応答を検出した場合、リンクは復元され、チーム化ソフトウェアはそのチーム メンバーとのトラフィックの送受信を自動的に再開します。LiveLink は、TCP/IP でのみ動作します。

LiveLink™ 機能は、32/64 ビット Windows オペレーティング システムでサポートされています。Linux オペレーティング システムに備わっている同様の機能については、Linux の文書類のチャネル結合に関する情報を参照してください。

チーム化および Large Send Offload (大量送信オフロード)/ Checksum Offload (チェックサム オフロード) のサポート

Large Send Offload (LSO、大量送信オフロード) と Checksum Offload (チェックサム オフロード) プロパティは、すべてのメンバーが機能をサポートし、その機能用に設定されている場合にのみ、チームに対してイネーブルされます。

セクション 3:Broadcom Gigabit Ethernet のチーム化サービス

はじめに

このセクションでは、ネットワーク チーム化サービスを使用する際の技術および実装の考慮事項について説明します。このサービスは、システムに同梱されている Broadcom ソフトウェアによって提供されます。Broadcom のチーム化サービスの目的は、複数のアダプタからなるチーム全体にフォルト トレランスとリンク集約を提供することです。本書の内容は、IT プロフェッショナルが、ネットワーク フォルト トレランスとロード バランシングを必要とするシステム アプリケーションを導入しトラブルシューティングする際に役立ちます。

用語集

表 4: 用語集

項目	定義
ARP	Address Resolution Protocol：アドレス解決プロトコル
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program (中間ドライバ)
DNS	Domain Name Service：ドメイン ネーム サービス
G-ARP	Gratuitous Address Resolution Protocol：無償アドレス解決プロトコル
通有中継 (FEC/GEC)/ 802.3ad-Draft Static	スイッチ依存型のロード バランシングおよびフェイルオーバー チーム タイプで、中間ドライバが発信トラフィックを管理し、スイッチが受信トラフィックを管理します。
HSRP	Hot Standby Router Protocol：ホット スタンバイ ルーター プロトコル
ICMP	Internet Control Message Protocol：インターネット制御メッセージ プロトコル
IGMP	Internet Group Management Protocol：インターネット グループ管理プロトコル
IP	Internet Protocol：インターネット プロトコル
LACP	Link Aggregation Control Protocol：リンク集約制御プロトコル
リンク集約 (802.3ad)	LACP を使用するロード バランシングおよびフェイルオーバー チーム タイプで、中間ドライバが発信トラフィックを管理し、スイッチが受信トラフィックを管理します。
LOM	LAN on Motherboard：マザーボード内蔵 LAN
MAC	Media Access Control：メディア アクセス制御
NDIS	Network Driver Interface Specification：ネットワーク ドライバ インターフェイス仕様
NLB	Network Load Balancing：ネットワーク負荷分散 (Microsoft)
PXE	Preboot Execution Environment：プリブート実行環境

表 4: 用語集

項目	定義
RAID	redundant array of inexpensive disks：低価格ディスクの冗長アレイ
Smart Load Balance および Failover	スイッチ独立型のフェイルオーバー チーム タイプで、フェイルオーバー イベント (リンク ロスなど) が発生するまではプライマリ チーム メンバーがすべての発受信トラフィックを処理し、スタンバイ チーム メンバーはアイドルになります。中間ドライバ (BASP) が受信 / 発信トラフィックを管理します。
Smart Load Balancing (SLB)	スイッチ独立型のロード バランシングおよびフェイルオーバー チーム タイプで、中間ドライバが発信 / 受信トラフィックを管理します。
TCP	Transmission Control Protocol：伝送制御プロトコル
UDP	User Datagram Protocol：ユーザー データグラム プロトコル
WINS	Windows name service：Windows ネーム サービス
WLBS	Windows Load Balancing Service：Windows 負荷分散サービス

チーム化の概念

ネットワーク アドレス指定

チーム化の動作方法を理解するには、イーサネット ネットワークにおけるノード通信の動作方法を理解することが重要です。本書では、読者に IP およびイーサネット ネットワーク通信の基礎知識があることを前提としています。以下では、イーサネット ネットワークで使用されるネットワーク アドレス指定の概念について、高度な概要を説明します。

コンピュータ システムのようなホスト プラットフォームのイーサネット ネットワーク インターフェイスは、どれもグローバルに一意なレイヤ 2 アドレスを 1 つと、グローバルに一意なレイヤ 3 アドレスを少なくとも 1 つ必要とします。OSI モデルで定義されているように、レイヤ 2 はデータ リンク レイヤで、レイヤ 3 はネットワーク レイヤです。レイヤ 2 アドレスはハードウェアに割り当てられ、多くの場合 MAC アドレスまたは物理アドレスと呼ばれます。このアドレスは工場出荷時にあらかじめプログラムされ、ネットワーク インターフェイス カードの NVRAM、または内蔵 LAN インターフェイス用のシステム マザーボードの NVRAM に格納されます。レイヤ 3 アドレスはプロトコル アドレスまたは論理アドレスと呼ばれ、ソフトウェア スタックに割り当てられます。IP はレイヤ 3 プロトコルの 1 つです。また、レイヤ 4 (トランスポート レイヤ) では Telnet や FTP などのネットワーク上位プロトコルごとにポート番号を使用します。これらのポート番号は、アプリケーション全体のトラフィック フローを識別するのに使用されます。TCP または UDP などのレイヤ 4 プロトコルは、今日のネットワークで最も一般的に使用されています。IP アドレスと TCP ポート番号の組み合わせは、ソケットと呼ばれます。

イーサネット デバイスは、IP アドレスではなく MAC アドレスを使用して他のイーサネット デバイスと通信します。ただし、大部分のアプリケーションは、WINS や DNS などのネーミング サービスによって IP アドレスに変換されるホスト名で動作します。そのため、IP アドレスに割り当てられている MAC アドレスの識別方法が必要です。IP ネットワークの ARP (Address Resolution Protocol) はこのメカニズムを提供します。ユニキャスト アドレスは単一の MAC アドレスまたは単一の IP アドレスに対応します。ブロードキャスト アドレスは、ネットワーク上のすべてのデバイスに送信されます。

チーム化とネットワーク アドレス

アダプタのチームは単一の仮想ネットワーク インターフェイスとして機能し、チーム化されていないアダプタのネットワーク デバイスと同じように見えます。仮想ネットワーク アダプタは、単一のレイヤ 2 アドレスと 1 つまたは複数のレイヤ 3 アドレスを通知します。チーム化ドライバは、初期化の際に、チームを構成する物理アダプタのいずれかから、チーム MAC アドレスとなる MAC アドレスを 1 つ選択します。一般的にこのアドレスは、ドライバが最初に初期化するアダプタから取得されます。チームを管理しているシステムは、ARP 要求を受信すると、チーム内の物理アダプタの中から MAC アドレスを 1 つ選択して、ARP 応答のソース MAC アドレスとして使用します。Windows オペレーティング システムでは、IPCONFIG /all コマンドは個々の物理アダプタではなく仮想アダプタの IP アドレスと MAC アドレスを表示します。プロトコル IP アドレスは、個々の物理アダプタではなく仮想ネットワーク インターフェイスに割り当てられます。

スイッチ独立型のチーム化モードの場合、データ伝送時には、仮想アダプタを構成するすべての物理アダプタが、物理アダプタに割り当てられている一意の MAC アドレスを使用します。すなわち、チーム内の各物理アダプタで送信されるフレームは、一意の MAC アドレスを使用して IEEE に準拠する必要があります。ARP キャッシュ エントリが、受信フレームからではなく、ARP 要求および ARP 応答からのみ情報を得ることに注意することが重要です。

チーム タイプの説明

サポートされているチーム タイプの分類方法は 3 つあります。

- 1 つ目は、スイッチ ポートの設定がアダプタ チーム化タイプとも一致している必要があるか、に基づく方法です。
- 2 つ目は、チームでロード バランシングとフェイルオーバー、またはフェイルオーバーのみをサポートするか、というチームの機能に基づく方法です。
- 3 つ目は、Link Aggregation Control Protocol が使用されているか、いないかに基づく方法です。

表 5 はチーム タイプとそれらの分類の要約を示しています。

表 5: 利用可能なチーム タイプ

チーム タイプ	スイッチ依存型 (スイッチが特定のチーム タイプをサポートしている必要がある)	スイッチに Link Aggregation Control Protocol のサポートが必要	ロード バランシング	フェイルオーバー
Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー (ロード バランスのチーム メンバーは 2 ～ 8)			●	●
スマート ロード バランス (SLB) (自動フォールバックはディスエーブル)				●
リンク集約 (802.3ad)	●	●	●	●
通有中継 (FEC/GEC)/ 802.3ad-Draft Static	●		●	●

Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー

Smart Load Balancing™ およびフェイルオーバー チーム タイプは、ロード バランシング用に設定されている場合はロード バランシングとフェイルオーバーの両方を提供し、フォルト トレランス用に設定されている場合にはフェイルオーバーのみを提供します。このチーム タイプは、どのイーサネット スイッチでも動作し、スイッチのトランキング設定は不要です。チームは、複数の MAC アドレスおよび 1 つまたは複数の IP アドレスを通知します (セカンダリ IP アドレスを使用している場合)。チーム MAC アドレスは、[Load Balance メンバー] のリストから選択されます。システムで ARP 要求が受信されると、ソフトウェア ネットワーキング スタックは常に ARP 応答とチーム MAC アドレスを送信します。ロード バランシング プロセスを開始するには、チーム化ドライバでソース MAC アドレスをいずれかの物理アダプタと一致するように変更して、この ARP 応答を修正します。

Smart Load Balancing は、レイヤ 3/ レイヤ 4 IP アドレスと TCP/UDP ポート番号に基づいて、伝送と受信の両方のロード バランシングを有効にします。すなわち、ロード バランシングはバイトまたはフレーム レベルではなく、TCP/UDP セッション ベースで実行されます。この方法は、同じソケットの通信に属するフレームを順序正しく配信し続けるために必要です。ロード バランシングは 2 ～ 8 個のポートでサポートされます。これらのポートには、アドイン アダプタや LAN on Motherboard (LOM) デバイスの組み合わせが含まれます。伝送のロード バランシングは、発信元および宛先の IP アドレスと TCP/UDP ポート番号を使用してハッシュ テーブルを作成することにより実現されます。発信元および宛先の IP アドレスと TCP/UDP ポート番号の組み合わせが同じ場合には、通常同じハッシュ インデックスが作成されるため、チーム内の同じポートを指し示すことになります。指定されたソケットのすべてのフレームを搬送するようにポートが選択されている場合、チーム MAC アドレスではなく、物理アダプタの一意の MAC アドレスがフレームに含められます。これは、IEEE 802.3 規格に準拠するために必要です。2 つのアダプタで同じ MAC アドレスを使用して伝送した場合、スイッチで処理できない MAC アドレスの重複状態が発生します。

受信のロード バランシングは、各クライアントのユニキャスト アドレスを ARP 要求の宛先アドレスとして使用して (Directed ARP とも呼ばれる)、クライアント別に無償 ARP を送信することにより、中間ドライバで実現されます。これはクライアント ロード バランシングと見なされ、トラフィック ロード バランシングとは見なされません。中間ドライバは、SLB チーム内の物理アダプタ間で深刻なロード インバランスを検出すると、受信フレームを再分配するために G-ARP を生成します。中間ドライバ (BASP) は ARP 要求に応答しません。ソフトウェア プロトコル スタックが必要な ARP 応答を提供するだけです。受信のロード バランシングが、チーム インターフェイスでシステムに接続しているクライアントの数と相関関係にあることを、理解することが重要です。

SLB の受信のロード バランシングは、チーム内の物理ポート全体でクライアント マシンの受信トラフィックのロード バランスを行おうとします。修正された G-ARP を使用して、送信者の物理アドレスとプロトコル アドレスに含まれるチーム IP アドレスの別の MAC アドレスを通知します。この G-ARP は、対象の物理アドレスとプロトコル アドレスのそれぞれに、クライアント マシンの MAC アドレスと IP アドレスを使用するユニキャストです。これにより、対象クライアントはその ARP キャッシュを、チーム IP アドレスへの新しい MAC アドレス マップで更新します。G-ARP はブロードキャストではありません。なぜなら、すべてのクライアントが同じポートにそのトラフィックを送信することになるからです。結果として、クライアント ロード バランシングで得られる利点はなくなり、フレーム配信の順序が狂う可能性があります。この受信のロード バランシングのスキームは、すべてのクライアントとチーム化されたシステムが同じサブネットまたはブロードキャスト ドメインにある限り作用します。

クライアントとシステムが別のサブネットにあり、受信トラフィックがルーターを越えなければならない場合、システムに向かう受信トラフィックはロード バランスされません。中間ドライバで IP フローを搬送するよう選択された物理アダプタは、すべてのトラフィックを搬送します。ルーターはチーム IP アドレスにフレームを送信するときに、ARP 要求をブロードキャストします (ARP キャッシュにない場合)。サーバー ソフトウェア スタックはチーム MAC アドレスを使用して ARP 応答を生成しますが、中間ドライバがその ARP 応答を修正して特定の物理アダプタに送信し、そのセッションのフローを確立します。

これは、ARP がルータブル プロトコルではないためです。ARP には IP ヘッダがありません。そのため、ルーターまたはデフォルト ゲートウェイには送信されません。ARP はローカル サブネット プロトコルに過ぎません。さらに、G-ARP はブロードキャスト パケットではないため、ルーターはそれを処理せず、それ自身の ARP キャッシュも更新しません。

ルーターが別のネットワーク デバイス向けの ARP を処理するのは、代理 ARP が有効になっていて、ホストにデフォルト ゲートウェイがない場合のみです。このような状態は非常にまれであり、大部分のアプリケーションにはお勧めできません。

ルーターを経由する伝送トラフィックはロード バランスされます。これは、伝送のロード バランシングが発信元および宛先の IP アドレスと TCP/UDP ポート番号に基づいているためです。ルーターでは発信元と宛先の IP アドレスが変更されないため、ロード バランシングのアルゴリズムは意図したとおりに動作します。

HSRP (Hot Standby Routing Protocol) のルーターの設定では、アダプタ チーム内の受信のロード バランシングは発生しません。一般的に HSRP では、2 つのルーターが 1 つのルータとして動作して、仮想 IP アドレスと仮想 MAC アドレスを通知します。1 つの物理ルーターがアクティブ インターフェイスになっているときには、もう片方がスタンバイになり

ます。HSRP では (ホスト ノードにそれぞれ異なるデフォルト ゲートウェイを使用して) HSRP グループの複数のルーターに共有ノードをロードすることもできますが、常にチームのプライマリ MAC アドレスを示します。

通有中継

通有中継は、リンクの両端 (サーバー インターフェイスとスイッチ ポート) でポートの設定を必要とするスイッチ支援のチーム モードです。これはよく Cisco Fast EtherChannel または Gigabit EtherChannel と呼ばれます。さらに通有中継は、Extreme Networks Load Sharing および Bay Networks のような他のスイッチ OEM や、IEEE 802.3ad リンク集約の静的モードによる同様の実装をサポートします。このモードでは、プロトコル スタックが ARP 要求に応答するときに、チームは 1 つの MAC アドレスと 1 つの IP アドレスを通知します。また、チーム内の各物理アダプタは、フレーム伝送時に同じチーム MAC アドレスを使用します。これが可能になるのは、リンクの反対側の端にあるスイッチがチーム モードを認識して、チーム内のすべてのポートによる単一 MAC アドレスの使用を処理するからです。スイッチの転送先テーブルは、中継を単一の仮想ポートとして示します。

このチーム化モードでは、中間ドライバは発信トラフィックのロード バランシングとフェイルオーバーのみを制御し、受信トラフィックはスイッチのファームウェアとハードウェアで制御されます。Smart Load Balancing の場合のように、BASP 中間ドライバは IP/TCP/UDP の発信元および宛先アドレスを使用して、サーバーの伝送トラフィックのロード バランスを行います。大部分のスイッチは、発信元および宛先 MAC アドレスの XOR ハッシュを実装しています。

リンク集約 (IEEE 802.3ad LACP)

リンク集約は、Link Aggregation Control Protocol (LACP) を使用してチームを構成するポートをネゴシエートすることを除けば、通有中継と似ています。チームを使用できるようにするには、リンクの両端で LACP を有効にする必要があります。LACP がリンクの両端で利用可能になっていない場合、802.3ad はリンクの両端がリンクアップ状態であることのみを要求する手動集約を提供します。手動集約は LACP メッセージ交換を実行せずにメンバー リンクをアクティブ化するため、LACP ネゴシエート リンクと同程度に堅固で信頼できるとみなすことはできません。LACP は、どのメンバー リンクが集約可能であるかを自動的に判断して、それらを集約します。リンク集約用の物理リンクの追加と削除を制御して、フレームが失われたり複製されたりしないようにします。集約リンク メンバーの削除は、LACP 対応の集約リンクに対して、オプションとして使用可能なマーカー プロトコルで提供されます。

リンク集約グループは、中継内のすべてのポートに対して単一の MAC アドレスを通知します。集約先の MAC アドレスは、グループを構成するいずれかの MAC アドレスである可能性があります。LACP とマーカー プロトコルは、マルチキャスト宛先アドレスを使用します。

リンク集約制御機能は集約されるリンクを特定して、システムの集約機能にポートをバインドし、状況を監視して集約グループに変更が必要かどうかを判断します。リンク集約は複数のリンクの個々の能力を合わせて、高性能の仮想リンクを形成します。LACP トランク内のリンクの障害または交換で、接続性が失われることはありません。中継内の残りのリンクにトラフィックがフェイル オーバーされるだけです。

スマート ロード バランス (SLB) (自動フォールバックはディスエーブル)

このチーム タイプは、スマート ロード バランスおよびフェイルオーバー チーム タイプと同一です。ただし、スタンバイ メンバーがアクティブな状態であり、プライマリ メンバーが動作を再開した場合、チームはプライマリ メンバーに切り替えずにスタンバイ メンバーをそのまま使用するところが異なります。このチームは、ネットワーク ケーブルが外されてネットワーク アダプタに再接続されたときにのみサポートされます。アダプタがデバイス マネージャまたはホット プラグ PCI を介して取り外し / 取り付けられた場合にはサポートされません。

チームに割り当てられたプライマリ アダプタがディスエーブルされた場合、チームは自動フォールバックが発生する Smart Load Balancing (スマート ロード バランス) およびフェイルオーバー チーム タイプとして機能します。

ソフトウェア コンポーネント

Windows オペレーティング システム環境では、チーム化は NDIS 中間ドライバによって実装されます。このソフトウェア コンポーネントがミニポート ドライバ、NDIS レイヤ、およびプロトコル スタックで動作して、チーム化アーキテクチャを可能にします (図 1 を参照)。ミニポート ドライバはホスト LAN コントローラを直接制御して、送受信および割り込みの処理などの機能を有効にします。中間ドライバはミニポート ドライバとプロトコル レイヤの間に位置し、複数のミニポート ドライバ インスタンスを多重化して、NDIS レイヤに対し単一アダプタのように見える仮想アダプタを作成します。NDIS は一連のライブラリ機能を提供して、ミニポート ドライバまたは中間ドライバとプロトコル スタック間の通信を有効にします。IP アドレスなどのプロトコル アドレスは各ミニポート デバイス インスタンスに割り当てられますが、中間ドライバがインストールされている場合、プロトコル アドレスは仮想チーム アダプタに割り当てられ、チームを構成する個々のミニポート デバイスには割り当てられません。

Broadcom が提供するチーム化サポートは、協調して動作しパッケージとしてサポートされる 3 つの個別のソフトウェア コンポーネントによって実現します。1 つのコンポーネントをアップグレードする場合には、他のすべてのコンポーネントもサポートされている バージョンにアップグレードする必要があります。表 6 では、3 つのソフトウェア コンポーネントと、サポートしているオペレーティング システム用の関連ファイルについて説明します。

表 6:Broadcom チーム化ソフトウェア コンポーネント

ソフトウェア コンポーネント	Broadcom 製品の名称	Windows	Linux
ミニポート ドライバ	Broadcom Base Driver	b57nd60X.sys	tg3
中間ドライバ	BASP (Broadcom Advanced Server Program)	Basp.sys	bonding
設定ユーザー インターフェイス	Broadcom Advanced Control Suite (BACS)	BACS	BACS CLI
NDIS 6 ドライバ	Windows Vista 以降 x86 ドライバ Windows Vista 以降 x64 ドライバ	b57nd60x.sys b57nd60a.sys	10–5 以上

BACS (Broadcom Advanced Control Suite) は、32 ビットおよび 64 ビットの Windows Server オペレーティング システムで動作するよう設計されています。BACS はロード バランシングおよびフォルト トレランスのチーム化の設定と、VLAN の設定に使用されます。さらに MAC アドレス、ドライバ バージョン、および各ネットワーク アダプタのステータス情報を表示します。BACS には、ハードウェア診断、ケーブル テスト、およびネットワーク トポロジー テストなど数多くの診断ツールも含まれています。

ハードウェア要件

本書で説明されているさまざまなチーム化モードでは、クライアントをチーム化されたシステムに接続するためのネットワーク機器に、ある制限を設けています。各タイプのネットワーク インターコネクト テクノロジーがチーム化に与える影響に関してはこれ以降のセクションで説明します。

イーサネット スイッチ

イーサネット スイッチを使用すると、イーサネット ネットワークを複数のブロードキャスト ドメインに分けることができます。スイッチは、イーサネット MAC アドレスだけに基づいて、ホスト間でイーサネット パケットを転送する役割を果たします。スイッチに接続されている物理ネットワーク アダプタは、半二重または全二重モードで動作する場合があります。

通有中継と 802.3ad リンク集約をサポートするには、スイッチでこのような機能を明確にサポートしている必要があります。スイッチでこれらのプロトコルをサポートしていない場合でも、Smart Load Balancing で使用できる場合があります。

ルーター

ルーターはレイヤ 3 以上のプロトコルに基づいてネットワーク トラフィックをルーティングするよう設計されていますが、スイッチング機能を持つレイヤ 2 デバイスとして動作することもよくあります。ルーターに直接接続されるポートのチーム化は、サポートされません。

サポートされる機能 (チーム タイプ別)

表 7 は、Broadcom NIC でサポートされているチーム タイプの機能の比較を示しています。この表を使用して、アプリケーションに最適なチーム タイプを確認してください。チーム化ソフトウェアは、1 つのチームで最大 8 ポート、また 1 つのシステムで最大 16 チームをサポートします。これらのチームは、サポート対象のチーム化タイプを任意に組み合わせることができますが、各チームは別々のネットワークまたはサブネット上にある必要があります。

表 7: チーム タイプの比較

チーム タイプ	フォルト トレランス	ロード バランシング	スイッチ依存型静的中継	スイッチ非依存型動的リンク集約 (IEEE 802.3ad)
機能	スタンバイを伴う SLB[a]	SLB	通有中継	リンク集約
チームあたりのポート数 (同じブロードキャスト ドメイン)	2 ～ 8	2 ～ 8	2 ～ 8	2 ～ 8
チーム数	16	16	16	16
アダプタ フォルト トレランス	はい	はい	はい	はい
スイッチ リンク フォルト トレランス (同じブロードキャスト ドメイン)	はい	はい	スイッチ依存型	スイッチ依存型
TX ロード バランシング	いいえ	はい	はい	はい

表 7: チーム タイプの比較 (続き)

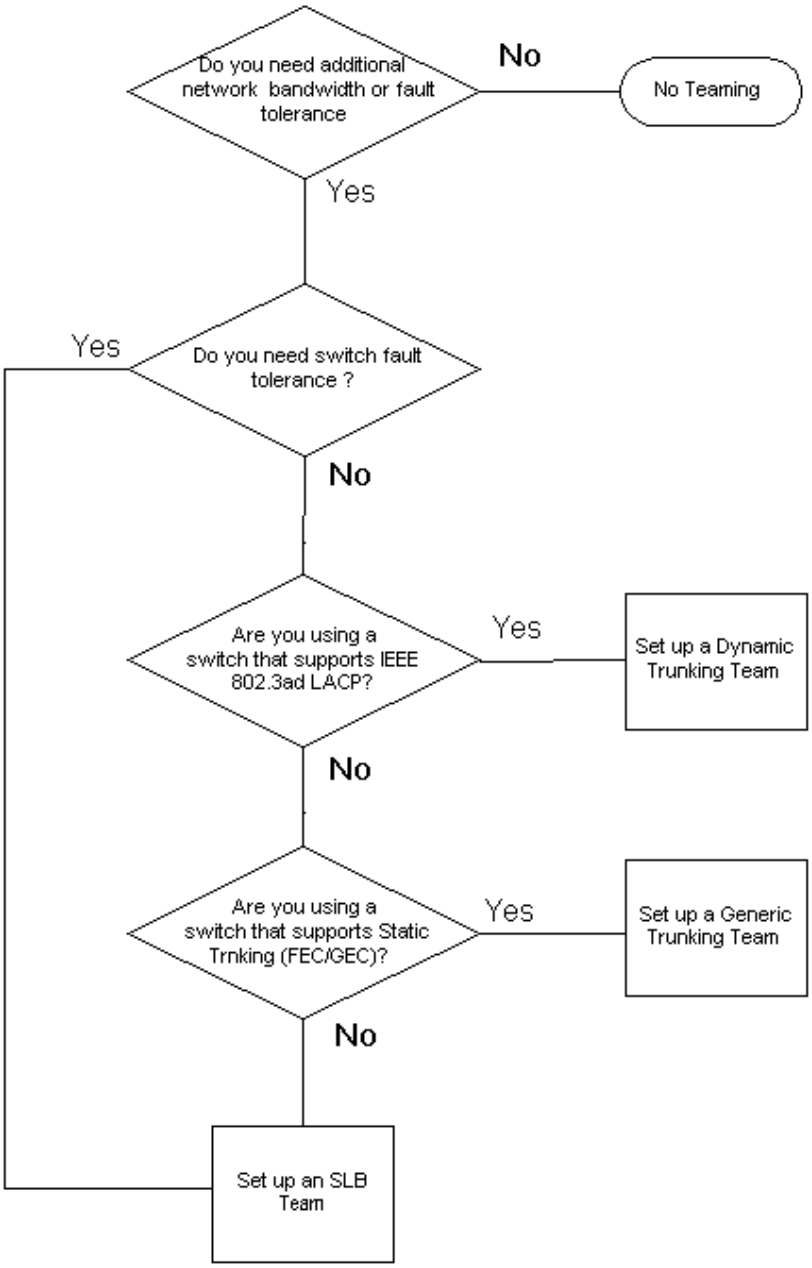
チーム タイプ	フォルト トレランス	ロード バランシング	スイッチ依存型静的中継	スイッチ非依存型動的リンク集約 (IEEE 802.3ad)
RX ロード バランシング	いいえ	はい	はい (スイッチにより実行)	はい (スイッチにより実行)
互換スイッチが必要	いいえ	いいえ	はい	はい
接続性をチェックするためのハードビート	いいえ	いいえ	いいえ	いいえ
混合メディア (異なるメディアを持つアダプタ)	はい	はい	はい (スイッチ依存型)	はい
混合速度 (共通の速度をサポートしないが異なる速度で動作できるアダプタ)	はい	はい	いいえ	いいえ
混合速度 (共通の速度をサポートするが異なる速度で動作できるアダプタ)	はい	はい	いいえ (同じ速度であることが必要)	はい
ロード バランシング TCP/IP	いいえ	はい	はい	はい
ベンダが混在するチーム作成	はい[b]	はい[b]	はい[b]	はい[b]
ロード バランシング非 IP	いいえ	はい (IPX アウトバウンド トラフィックのみ)	はい	はい
すべてのチーム メンバーに同じ MAC アドレス	いいえ	いいえ	はい	はい
すべてのチーム メンバーに同じ IP アドレス	はい	はい	はい	はい
IP アドレスによるロード バランシング	いいえ	はい	はい	はい
MAC アドレスによるロード バランシング	いいえ	はい (IP/IPX 以外に使用)	はい	はい

[a] 1 つのプライマリ メンバーと 1 つのスタンバイ メンバーがある SLB。
[b] チームには少なくとも 1 つの Broadcom アダプタが必須。

チーム タイプの選択

次のフロー チャートでは、チーム化を計画するときの意思決定フローを示します。チーム化を行う第 1 の理由は、ネットワーク帯域幅の増加とフォルト トレランスの向上が必要であることです。チーム化により、この両方の要件を満たすためのリンク集約とフォルト トレランスが提供されます。優先するチーム化は次の順序で選択する必要があります。最初の選択としてリンク集約、第 2 の選択として通有中継、さらに、管理されていないスイッチまたは最初の 2 つのオプションをサポートしないスイッチを使用する場合は第 3 の選択として SLB チーム化。スイッチのフォルト トレランスが必要な場合は、SLB が唯一の選択肢です (図 1 を参照)。

図 1: チーム タイプの選択のプロセス

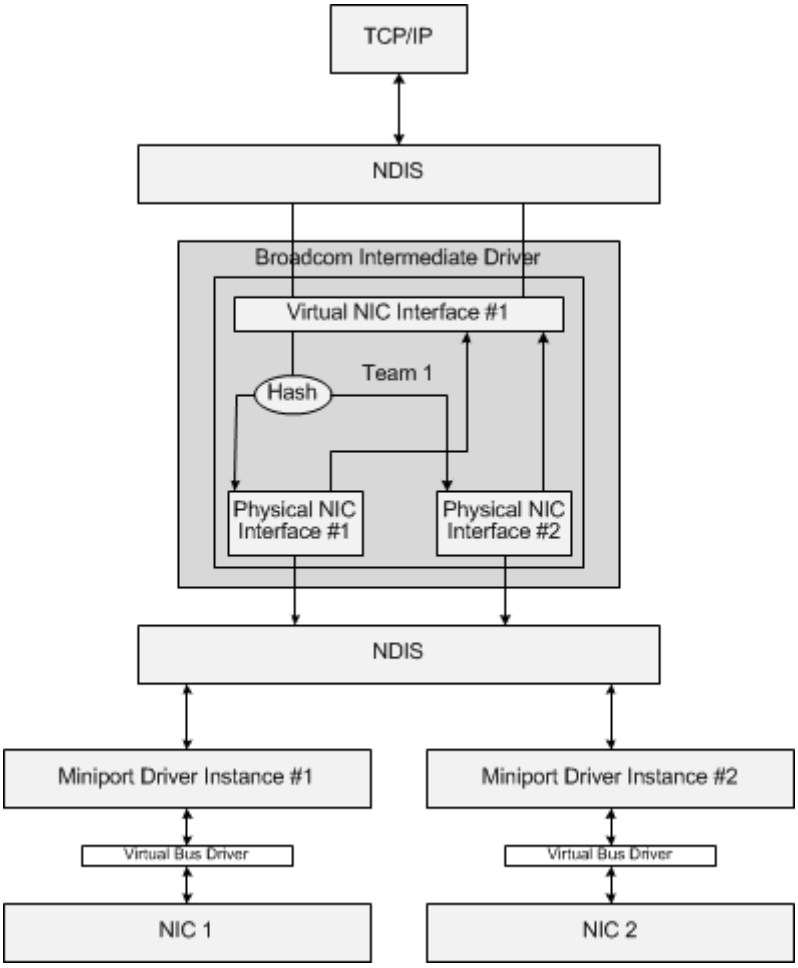


チーム化の仕組み

アーキテクチャ

Broadcom Advanced Server Program は、NDIS 中間ドライバとして実装されます (図 2 を参照)。TCP/IP などのプロトコル スタックの下で動作し、仮想アダプタとして表示されます。この仮想アダプタは、チームで最初に初期化されたポートの MAC アドレスを継承します。レイヤ 3 アドレスも、仮想アダプタに対して設定する必要があります。BASP の主要機能は、チーム化することを選択されたシステムに取り付けられている物理アダプタ間で、インバウンド トラフィック (SLB の場合) とアウトバウンド トラフィック (すべてのチーム化モードの場合) のバランスをとることです。インバウンド アルゴリズムとアウトバウンド アルゴリズムは相互に独立し、直交しています。特定のセッションに対するアウトバウンド トラフィックを特定のポートに割り当て、対応するインバウンド トラフィックを別のポートに割り当てることができます。

図 2: 中間ドライバ



アウトバウンド トラフィック フロー

Broadcom 中間ドライバは、すべてのチーム化モードのアウトバウンド トラフィック フローを管理します。アウトバウンド トラフィックの場合、すべてのパケットは最初にフローに分類され、選択された物理アダプタに配分されて伝送されます。フロー分類では、既知のプロトコル フィールドに対して効率的なハッシュ計算が行われます。結果のハッシュ値を使用して、アウトバウンド フロー ハッシュ テーブルにインデックスが作成されます。選択したアウトバウンド フロー ハッシュ エントリには、このフローの伝送を行う選択済み物理アダプタのインデックスが含まれています。パケットのソース MAC アドレスは、選択した物理アダプタの MAC アドレスに変更されます。変更されたパケットは、選択した物理アダプタに渡されて伝送されます。

アウトバウンド TCP および UDP パケットは、レイヤ 3 およびレイヤ 4 ヘッダ情報を使用して分類されます。このスキームにより、HTTP や FTP などの well-known ポートを使用した一般的なインターネット プロトコル サービスの負荷分散が向上します。このため BASP は、パケットごとではなく TCP セッション単位でロード バランシングを実行します。

アウトバウンド フロー ハッシュ エントリでは、分類後に統計カウンタも更新されます。ロードバランシング エンジンは、これらのカウンタを使用して、チーム化されたポート間にフローを定期的に配分します。アウトバウンド コード パスは、アウトバウンド フロー ハッシュ テーブルへの複数の同時アクセスが許可される最善の同時性を実現するように設計されています。

TCP/IP 以外のプロトコルでは、最初の物理アダプタが常にアウトバウンド パケットに対して選択されます。例外は、インバウンドのロード バランシングを実現するために別の方法で処理される Address Resolution Protocol (ARP) です。

インバウンド トラフィック フロー (SLB のみ)

Broadcom 中間ドライバは、SLB チーム化モードのインバウンド トラフィック フローを管理します。アウトバウンドのロード バランシングとは異なり、インバウンドのロード バランシングは、ロード バランシングされたサーバーと同じサブネット内にある IP アドレスにのみ適用できます。インバウンドのロード バランシングでは、Address Resolution Protocol (RFC0826) に固有の特性を利用します。各 IP ホストは独自の ARP キャッシュを使用して、IP データグラムを Ethernet フレームにカプセル化します。BASP は ARP 応答を慎重に操作し、インバウンド IP パケットを目的の物理アダプタに送信するよう各 IP ホストに指示します。このため、インバウンドのロード バランシングはインバウンド フローの統計履歴に基づいた事前計画スキームです。クライアントからサーバーへの新規接続は、常にプライマリ物理アダプタ上で行われます (オペレーティング システム プロトコル スタックによって生成された ARP 応答は常に論理 IP アドレスをプライマリ物理アダプタの MAC アドレスに関連付けるため)。

アウトバウンドの場合と同様に、インバウンド フロー ヘッド ハッシュ テーブルがあります。このテーブル内の各エントリには、単一リンクのリストがあり、各リンク (インバウンド フロー エントリ) は同じサブネット内にある IP ホストを表します。

インバウンド IP データグラムが到着すると、IP データグラムのソース IP アドレスをハッシュすることによって適切なインバウンド フロー ヘッド エントリが検索されます。選択したエントリに格納されている 2 つの統計カウンタも更新されます。これらのカウンタは、ロード バランシング エンジンによってアウトバウンド カウンタと同じ方法で定期的に使用され、フローが物理アダプタに再割り当てされます。

インバウンド コード パスでは、インバウンド フロー ヘッド ハッシュ テーブルが同期アクセスを許可するようにも設計されています。インバウンド フロー エントリのリンク リストは、ARP パケットの処理時と定期的なロード バランシング時にのみ参照されます。インバウンド フロー エントリへのパケット単位の参照はありません。リンク リストがバインドされていない場合でも、ARP 以外の各パケットの処理のオーバーヘッドは常に一定です。ただし、インバウンドとアウトバウンド両方の ARP パケットの処理は、対応するリンク リスト内のリンク数に依存します。

インバウンド 処理パスでは、ブロードキャスト パケットが他の物理アダプタからシステムを通じてループバックすることを防ぐために、フィルタも採用されています。

プロトコル サポート

ARP および IP/TCP/UDP フローは、ロード バランシングに対応します。パケットが、ICMP や IGMP などの IP プロトコルのみの場合、特定の IP アドレスへのすべてのデータ フローが同じ物理アダプタを介して送信されます。パケットが L4 プロトコルに TCP または UDP を使用している場合は、ポート番号がハッシュ アルゴリズムに追加されるため、2 つの異なる L4 フローが 2 つの異なる物理アダプタを通じて同じ IP アドレスに送信されます。

たとえば、クライアントの IP アドレスが 10.0.0.1 であるとします。ハッシュには IP アドレスのみ使用されるため、すべての IGMP および ICMP トラフィックが同じ物理アダプタに送信されます。フローは次のようになります。

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

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

サーバーが、同じ 10.0.0.1 アドレスに TCP および UDP フローも送信する場合、これらは IGMP および ICMP と同じ物理アダプタ上にあっても、ICMP および IGMP とはまったく異なる物理アダプタ上にあってもかまいません。ストリームは次のようになります。

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

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

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

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

または、ストリームは次のようになります。

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

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

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

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

アダプタ間の実際の割り当ては、時間の経過につれて変化する場合がありますが、ハッシュでは IP アドレスのみ使用されるため、TCP/UDP ベースでないプロトコルは同じ物理アダプタを通過します。

パフォーマンス

最近のネットワーク インターフェイス カードには、特定の CPU 集中型の操作のオフローディングを行うことで CPU 利用率を軽減する多くのハードウェア機能があります (チーム化とその他の高度なネットワーク プロパティを参照)。対照的に、BASP 中間ドライバは完全なソフトウェア機能であり、プロトコル スタックから受信した各パケットを調べて、内容に対処してから特定の物理インターフェイスを通じて送信する必要があります。BASP ドライバはほぼ一定の時間で各発信パケットを処理できますが、CPU を限界まで使用している一部のアプリケーションは、チーム化されたインターフェイスで動作している場合に悪影響を受けるおそれがあります。このようなアプリケーションは、ロード バランシング機能よりも中間ドライバのフェイルオーバー機能を利用する方が適切な場合があります。または、Large Send Offload (大量送信オフロード) などの特定のハードウェア機能を提供する単一の物理アダプタで、より効率的に動作する場合があります。

ドライバ サポート (オペレーティング システム別)

前述のように、Windows Server 2008、および 2012 オペレーティング システム環境でサポートされます。

さまざまなチーム化モードの機能を次の表にまとめます。

表 8: チーム化モードの機能

機能	Windows によるサポート
Smart Load Balancing™	
ユーザー インターフェイス	BACS[a]
チーム数	16
チームごとのアダプタ数	8
動的置換	はい
動的追加	はい
動的削除	はい
リンク速度サポート	さまざまな速度
フレーム プロトコル	IP
インバウンド パケット管理	BASP
アウトバウンド パケット管理	BASP
フェイルオーバー イベント	リンク ロスまたは LiveLink イベント
フェイルオーバー時間	500 ミリ遘 未満
フォールバック時間	1.5 秒[b] (概算)
LiveLink のサポート	はい
MAC アドレス	異なる
Broadcom 以外の製品を使用したチーム化	はい
通有中継	
ユーザー インターフェイス	BACS
チーム数	16
チームごとのアダプタ数	8
動的置換	はい
動的追加	はい
動的削除	はい
リンク速度サポート	さまざまな速度
フレーム プロトコル	すべて
インバウンド パケット管理	スイッチ
アウトバウンド パケット管理	BASP
フェイルオーバー イベント	リンク ロスのみ
フェイルオーバー時間	500 ミリ秒
フォールバック時間	1.5 秒[b] (概算)
MAC アドレス	すべてのアダプタに対して同一
Broadcom 以外の製品を使用したチーム化	はい
動的中継	

表 8: チーム化モードの機能 (続き)

機能	Windows によるサポート
ユーザー インターフェイス	BACS
チーム数	16
チームごとのアダプタ数	8
動的置換	はい
動的追加	はい
動的削除	はい
リンク速度サポート	さまざまな速度
フレーム プロトコル	すべて
インバウンド パケット管理	スイッチ
アウトバウンド パケット管理	BASP
フェイルオーバー イベント	リンク ロスのみ
フェイルオーバー時間	500 ミリ遘 未満
フォールバック時間	1.5 秒 [b] (概算)
MAC アドレス	すべてのアダプタに対して同一
Broadcom 以外の製品を使用したチーム化	はい

[a] Broadcom Advanced Control Suite
[b] Port Fast または Edge Port が有効になっていることを確認してください。

サポートされるチーム化の速度

各チーム タイプにサポートされるさまざまなリンク速度を 表 9 にリストします。混合速度とは、チーム化アダプタが異なるリンク速度で稼動できることを示します。

表 9: チームのリンク速度

チーム タイプ	リンク速度	トラフィックの方向	速度サポート
SLB	10/100/1000	受信 / 発信	混合速度
FEC	100	受信 / 発信	同一速度
GEC	1000	受信 / 発信	同一速度
IEEE 802.3ad	10/100/1000	受信 / 発信	混合速度

チーム化とその他の高度なネットワーク プロパティ

チームの作成、チーム メンバーの追加や削除、またはチーム メンバーの詳細設定の変更を行う前に、各チーム メンバーが同じように構成されていることを確認してください。確認する設定として、VLAN および QoS パケット タギング、ジャンボ フレーム、および各種オフロードがあります。詳細なアダプタ プロパティとチーム化サポートを表 10 に示します。

表 10: 詳細なアダプタ プロパティとチーム化サポート

アダプタ プロパティ	チーム化仮想アダプタによるサポート
Checksum Offload（チェックサム オフロード）	はい
IEEE 802.1p QoS タギング	いいえ
Large Send Offload (大量送信オフロード)	はい [a]
ジャンボ フレーム	はい [b]
IEEE 802.1Q VLAN	はい
Wake on LAN	いいえ
Preboot Execution Environment (PXE)	はい [c]

[a] チーム上のすべてのアダプタがこの機能をサポートしている必要があります。一部のアダプタは、IPMI も有効になっている場合にこの機能をサポートしないことがあります。
[b] チーム内のすべてのアダプタによってサポートされている必要があります。
[c] クライアントとしてではなく PXE サーバーとしてのみ。

Checksum Offload（チェックサム オフロード）

Checksum Offload (チェックサム オフロード) は Broadcom ネットワーク アダプタのプロパティであり、送受信トラフィックの TCP/IP/UDP チェックサムをホスト CPU ではなくアダプタ ハードウェアで計算できるようにします。トラフィック量が多い状況では、これにより、システムはホスト CPU がチェックサムの計算を強制される場合よりも効率的に接続を処理できます。このプロパティは本質的にハードウェア プロパティであり、ソフトウェアのみの実装では利点を生かせません。Checksum Offload (チェックサム オフロード) をサポートするアダプタは、この機能をオペレーティング システムに公示するため、チェックサムをプロトコル スタックで計算する必要はありません。中間ドライバはプロトコル レイヤとミニポート ドライバの間に直接配置されるため、プロトコル レイヤはチェックサムをオフロードできません。

IEEE 802.1p QoS タギング

IEEE 802.1p 標準には、トラフィックの優先順位づけを可能にする 3 ビットのフィールド (最大 8 つの優先順位レベルをサポート) が含まれています。BASP 中間ドライバは、IEEE 802.1p QoS タギングをサポートしていません。

Large Send Offload (大量送信オフロード)

Large Send Offload (LSO、大量送信オフロード) は、Broadcom ネットワーク アダプタが提供している機能であり、TCP などの上位レベル プロトコルによって大きなデータ パケットがヘッダを付加した小さな一連のパケットに分割されるのを回避します。プロトコル スタックは最大 64 KB のデータ パケットに対して単一のヘッダのみ生成する必要があり、アダプタ ハードウェアが、(最初に提供された単一ヘッダに基づいて) 正しく並べられたヘッダを持つ適切なサイズの Ethernet フレームにデータ バッファを分割します。

ジャンボ フレーム

チーム内のすべての物理アダプタがジャンボ フレームをサポートして、チーム内のすべてのアダプタに同じサイズが設定されていれば、BASP 中間ドライバもジャンボ フレームをサポートします。

IEEE 802.1Q VLAN

IEEE 802.3ac 標準は、IEEE 802.1Q 仕様で指定されている、イーサネット ネットワーク上での Virtual Bridged Local Area Network (VLAN) タギングをサポートするフレーム形式拡張を定義しています。VLAN プロトコルでは、フレームが属する VLAN を識別するための Ethernet フレームへのタグの挿入が許可されます。現在は、4 バイトの VLAN タグが Ethernet フレームのソース MAC アドレスと長さ / タイプ フィールドの間に挿入されます。VLAN タグの最初の 2 バイトは IEEE 802.1Q タグ タイプで構成され、次の 2 バイトにはユーザー優先順位フィールドと VLAN 識別子 (VID) が含まれます。仮想 LAN (VLAN) を利用すると、ユーザーは物理 LAN を論理的なサブパーツに分割できます。定義済みの VLAN は、そのトラフィックやブロードキャストがその他の VLAN から分離されるため、それぞれが独自の分離されたネットワークとして機能します。これにより各論理グループ内の帯域幅の効率が向上します。VLAN を利用すると、管理者は適切なセキュリティおよび QoS (Quality of Service、サービス品質) ポリシーを実施することもできます。BASP では、チームまたはアダプタあたり 64 個の VLAN の作成をサポートしています。63 個がタグ付きで、1 つはタグなしです。ただし、オペレーティング システムとシステム リソースによって、実際の VLAN 数が制限されます。

VLAN サポートは、IEEE 802.1q に従って提供され、チーム化環境と単一アダプタでサポートされます。VLAN は、同種のチーム化でのみサポートされ、Broadcom 以外の製品を使用したチーム化環境ではサポートされないことに注意してください。BASP 中間ドライバは、VLAN タギングをサポートしています。1 つ以上の VLAN を中間ドライバの単一インスタンスにバインドできます。

Wake on LAN

Wake on LAN (WOL) は、イーサネット インターフェイスから特定のパケットを受信すると、システムがスリープ状態から復帰できるようにする機能です。仮想アダプタは、ソフトウェア専用デバイスとして実装されるので、Wake on LAN の実装に必要なハードウェア機能がなく、仮想アダプタではスリープ状態からシステムを始動させることができません。ただし、物理アダプタでは、アダプタがチームの一部である場合でも、このプロパティをサポートします。

Preboot Execution Environment (PXE)

Preboot Execution Environment (PXE) では、ネットワークを使用して、システムをオペレーティング システム イメージから起動できます。定義上、PXE はオペレーティング システムをロードする前に呼び出されるため、BASP 中間ドライバがチームをロードしてイネーブルする機会はありません。したがって、オペレーティング システムのロード時にチームに入れられる物理アダプタは、PXE クライアントとして使用できますが、チーム化機能のアダプタは PXE クライアントとしてサポートされません。チーム化されたアダプタは PXE クライアントとして使用できませんが、Dynamic Host Control Protocol (DHCP) と Trivial File Transfer Protocol (TFTP) を使用して PXE クライアントにオペレーティング システム イメージを提供する PXE サーバーではこのアダプタを使用できます。これらのプロトコルは両方とも IP に対応しており、すべてのチーム化モードによってサポートされます。

全般的なネットワークに関する考慮事項

複数のスイッチにまたがるチーム化

SLB のチーム化は、複数のスイッチにまたがって設定できます。ただし、スイッチ同士を接続する必要があります。通有中継とリンク集約は、複数のスイッチにまたがって動作できません。その理由は、これらの実装では、チームに含まれるすべての物理アダプタで同じイーサネット MAC アドレスを使用する必要があるためです。SLB がリンク ロスを検出できるのは、チームに含まれるポート間の接続や、直接のリンク パートナーとの接続に限られるという点に注意することが重要です。SLB には、スイッチで生じる他のハードウェア障害に対応する機能がなく、他のポートのリンク ロスを検出できません。

スイッチリンクのフォルト トレランス

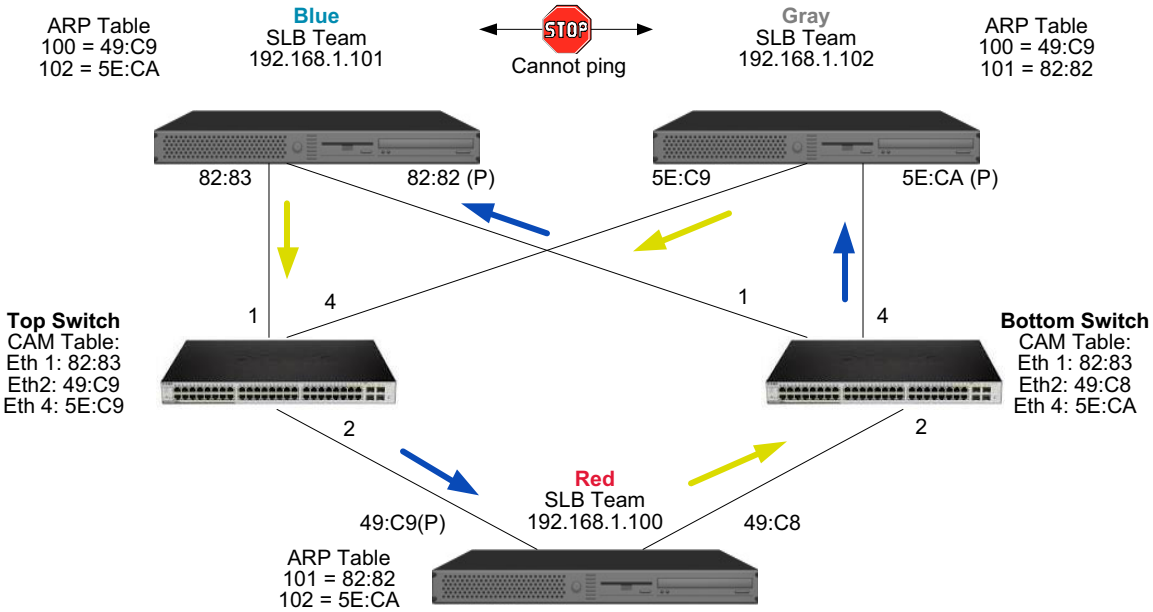
以下の図では、フォルト トレランス対応のスイッチ構成でどのように SLB チームが動作するかを説明します。SLB チームにアクティブな 2 つのメンバーがある構成で、ping リクエストと ping 応答メッセージのマッピングを説明します。すべてのサーバー (Blue、Gray、Red) は、継続的に ping の送受信を相互に行っています。図 3 は、2 つのスイッチ間に相互接続ケーブルがない構成です。図 4 では相互接続ケーブルがあります。図 5 は相互接続ケーブルがある状態でのフェイルオーバー イベントの例です。これらのシナリオでは、2 つのスイッチ間でのチーム化の動作を説明して、相互接続リンクの重要性を理解します。

この図では、ICMP エコー要求 (黄色の矢印) を送信する第 2 のチーム メンバーと、ICMP エコーの応答メッセージ (青い矢印) を受信する第 1 のチーム メンバーを示します。この図は、チーム化ソフトウェアの重要な特性を表しています。ロード バランシング アルゴリズムは、フレームの送受信時に、フレームのロード バランスを同期しません。言い換えると、特定の接続でのフレームは、チーム内の異なるインターフェイスで送信され、受信される可能性があります。これは、Broadcom がサポートするすべての タイプのチーム化で共通しています。したがって、同じチーム内のポートに接続するスイッチの間では、相互接続リンクを提供する必要があります。

相互接続していない構成では、Blue から Gray への ICMP 要求は、ポート 82:83 から Gray のポート 5E:CA に向けて送信されますが、Top Switch には、この要求を送信する方法がありません。なぜなら、この要求は、Gray の 5E:C9 ポートを通過できないからです。Gray が Blue に ping の送信を試行する場合にも、同じような問題が発生します。ICMP 要求は、5E:C9 から Blue の 82:82 に向けて送信されますが、この要求が受信されることはありません。Top Switch は、CAM テーブル内に 82:82 エントリを持っていません。なぜなら、2 つのスイッチの間に相互接続していないからです。ただし、ping は Red と Blue の間、Red と Gray の間では送受信されます。

さらにフェイルオーバー イベントによって、接続が切断される場合もあります。Top Switch のポート 4 でケーブル接続の切断が生じたと仮定します。この場合、Gray は ICMP 要求を 49:C9 に送信しますが、Bottom Switch は CAM テーブル内に 49:C9 エントリを持っていないので、フレームをこれらの全ポートに配信しても、49:C9 に接続するリンクは検出できません。

図 3: 相互接続リンクのない環境でのスイッチにまたがるチーム化



スイッチ間にリンクを設定すると、Blue と Gray の間で何の問題もなく、相互にトラフィックを送受信できます。両方のスイッチの CAM テーブルを参照して、追加されたエントリに注目してください。チームが適切に機能するには、このリンクの相互接続が重要です。したがって、2 つのスイッチを相互接続して可用性の高い接続を保証するために、リンク集約中継を使用することを強くお勧めします。

図 4: 相互接続のあるスイッチ間にまたがるチーム化

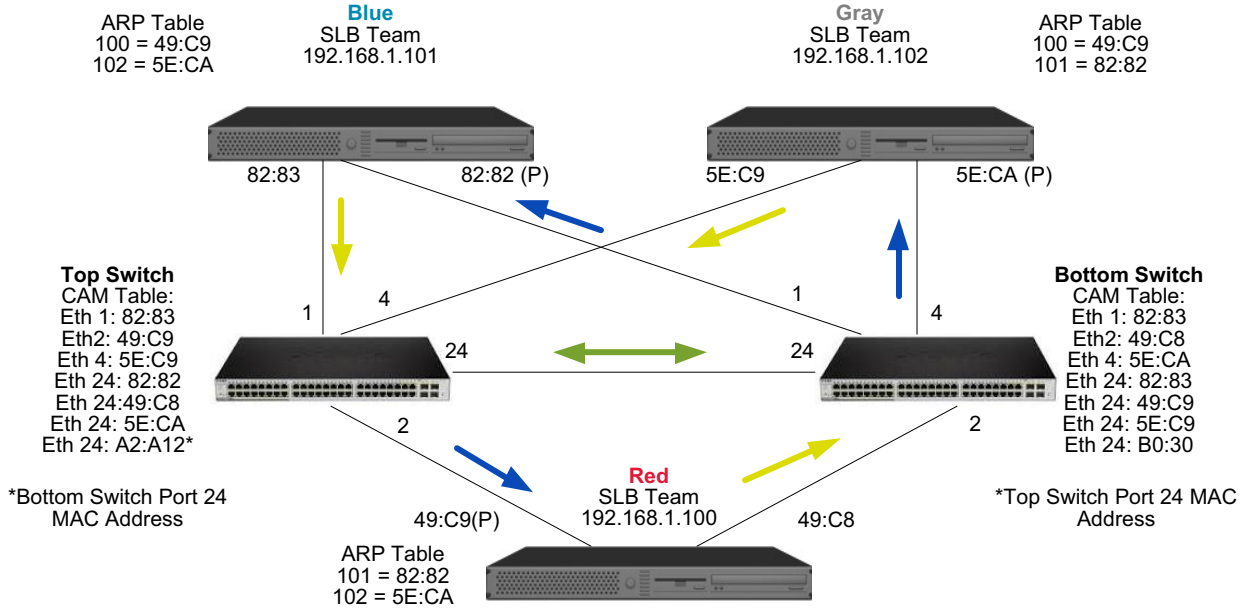
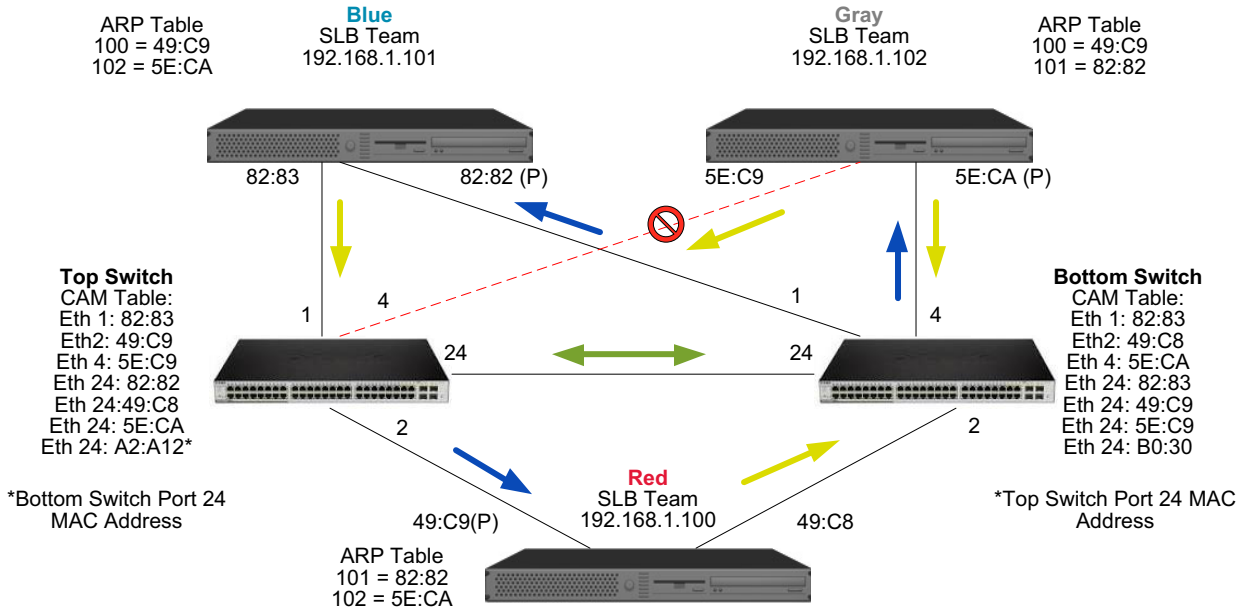


図 5 は、Top Switch のポート 4 でケーブルが外れた場合のフェイルオーバー イベントを表しています。接続が切断されずに、すべてのステーションが相互に ping を送受信できるので、これは適切なフェイルオーバーです。

図 5: フェイルオーバー イベント



スパニング ツリー アルゴリズム

- トポロジー変更通知 (TCN)
- Port Fast/Edge Port

イーサネット ネットワークの場合、2 つのブリッジ間またはスイッチ間では、アクティブなパスが 1 つだけ存在します。スイッチ間にアクティブなパスが複数存在していると、ネットワーク内にループが生じる可能性があります。ループが発生すると、一部のスイッチは、スイッチの両側でステーションを認識するようになります。この状況では、転送アルゴリズムが正常に機能できず、重複フレームが転送される可能性があります。スパニング ツリー アルゴリズムでは、拡張ネットワーク内の全スイッチにまたがるツリーを定義して、特定の冗長データ パスを強制的にスタンバイ (ブロック) 状態に切り替えることで、パスの冗長性を実現します。ネットワーク内のスイッチは、パスの識別に使用するスパニング ツリー パケットを定期的に送受信します。1 つのネットワーク セグメントが到達不能になった場合、あるいはスパニング ツリーのコストが変わった場合、スパニング ツリー アルゴリズムは、スパニング ツリー トポロジーを再設定し、スタンバイ パスをアクティブ化することでリンクを再設定します。エンド ステーション側では、スパニング ツリーの動作は見えません。したがって、これらのステーションでは、1 つの LAN セグメントに接続したのか、複数のセグメントで構成されたスイッチ LAN に接続したのかわかりません。

Spanning Tree Protocol (STP) は、ブリッジ間やスイッチ間での動作を目的としたレイヤ 2 プロトコルです。STP の仕様は、IEEE 802.1d で定義されています。STP の主な目的は、ネットワーク内に冗長パスがあるときにループに陥らないようにすることです。STP は、ネットワーク ループの検出 / ディスエーブルを行い、スイッチまたはブリッジの間にバックアップ リンクを提供します。このプロトコルを使用すると、デバイスは、ネットワーク内の 2 つのステーションの間で 1 つのパスのみを使用するように、ネットワークにある他の STP 準拠デバイスと相互操作を行うことが可能になります。

安定したネットワーク トポロジーを確立すると、すべてのブリッジはルート ブリッジから送信される hello BPDU (Bridge Protocol Data Units) を待つ状態になります。

あらかじめ定義された時間 (最大経過時間) が経過しても、ブリッジが hello BPDU を受信しない場合、ブリッジはルート ブリッジへのリンクがダウンしたと判断します。次にこのブリッジは、他のブリッジとのネゴシエーションを開始して、ネットワークを再設定して、有効なネットワーク トポロジーを再び確立します。新しいトポロジーを作成するプロセスは、最大 50 秒かかります。この間、エンドツーエンドの通信は中断されます。

エンド ステーションに接続したポートに対しては、スパニング ツリーは使用しないことをお勧めします。その理由は、定義上、エンド ステーションは、イーサネット セグメント内でループを作成しないからです。さらにチーム化したアダプタを、スパニング ツリーをイネーブルしたポートに接続すると、接続上の不測の問題が発生する可能性があります。たとえば、チーム化したアダプタが物理アダプタの 1 つでリンクを失ったと仮定します。物理アダプタが再接続された場合 (フォールバックとも呼びます)、中間ドライバはリンクが再び確立され、ポートでトラフィックの送受信が開始されたと認識します。しかし、スパニング ツリー プロトコルによってポートが一時的にブロックされると、トラフィックが失われることになります。

トポロジー変更通知 (TCN)

ブリッジ / スイッチは、特定のポートで受信したソース MAC アドレスから、MAC アドレスとポート番号の転送テーブルを作成します。このテーブルは、すべてのポートにフレームを配信するのではなく、特定のポートにフレームを転送するために利用します。テーブル エントリの最大の格納時間は、一般的に 5 分です。ホストでアクティビティが 5 分間ないと、エントリはテーブルから削除されます。エントリの格納時間を短くすると、効果がある場合もあります。たとえば、転送リンクがブロック状態になったときに、異なるリンクをブロック状態から転送状態に切り替えるときです。この変更には、最大 50 秒かかります。STP の再計算が完了すると、エンド ステーション間の通信で、新しいパスが利用可能になります。ただし、転送テーブルには依然として古いトポロジーのエントリがあるので、5 分が経過して影響を受けるポート エントリがテーブルから削除されるまで、通信が再確立されない可能性があります。そして、トラフィックはすべてのポートに配信されて、再び取得されます。このような場合は、格納時間を短くすると効果があります。これがトポロジー変更通知 (Topology Change Notice、TCN) BPDU の目的です。TCN は、影響を受けるブリッジ / スイッチからルート ブリッジ / スイッチに送信されます。ブリッジ / スイッチはトポロジーの変更 (リンクのダウンまたは転送状態へのポートの切り替え) を検出すると、すぐにルート ポートを経由して TCN をルート ブリッジに送信します。次にルート ブリッジは、トポロジーの変更を通知する BPDU をネットワーク全体に配信します。この情報を受けて、すべてのブリッジは、MAC テーブルの格納時間を 15 秒に変更します。この手順により、STP の再収束の後、スイッチはすぐに MAC アドレスを再び取得できます。

TCN BPDU は、ポートが転送状態からブロック状態に切り替わったとき、あるいはブロック状態から転送状態に切り替わったときに送信されます。TCN BPDU では、STP の再計算は開始されません。この通知は、スイッチ内の転送テーブル エントリの格納時間にのみ影響を及ぼし、ネットワーク トポロジーの変更や、ループの作成は行いません。サーバーまたはクライアントなどのエンド ノードの場合は、電源のオフ / オン時にトポロジーの変更が開始されます。

Port Fast/Edge Port

ネットワーク上で TCN の影響 (たとえば、スイッチ ポートで配信が増えるなど) を軽減するには、電源のオン / オフの頻度が高いエンド ノードに対して、接続先になるスイッチ ポートで Port Fast または Edge Port を設定する必要があります。Port Fast または Edge Port は、特定のポートに適用されるコマンドであり、以下の効果があります。

- ダウン リンクからアップ リンクまで、リンクに含まれる一連のポートは、待ち受け、情報の取得、転送という一連の手続きを行うのではなく、転送 STP モードに組み込まれます。STP は、依然としてこれらのポートで実行中です。
- スイッチは、ポートのアップ / ダウンのタイミングでは TCN を生成しません。

Microsoft NLB/WLBS とのチーム化

チーム化の SLB モードは、Microsoft の ネットワーク負荷分散 (NLB) ユニキャスト モードでは*動作しません*。マルチキャスト モードのみで動作します。NLB サービスで使用されるメカニズムでは、ロード バランシングが NLB によって管理されるため、この環境のチーム化設定はフェイルオーバー (スタンバイ NIC のある SLB) にすることをお勧めします。

アプリケーションに関する考慮事項

チーム化とクラスタリング —Microsoft クラスタ ソフトウェア

各クラスタ ノードでは、カスタマが最低 2 ネットワーク アダプタ (オンボード アダプタでも可能) を取り付けることを強くお勧めします。これらのインターフェイスは、2 つの目的に使用します。1 つのアダプタは、クラスタ内の*ハートビート*通信専用に使用されます。これは *プライベート アダプタ*と呼ばれ、通常、独立したプライベート サブネットワークに含まれます。その他のアダプタはクライアント通信に使用され、*パブリック アダプタ*と呼ばれます。

プライベートなクラスタ内通信と、パブリックな外部クライアント通信のために、それぞれの目的に合わせて複数のアダプタを使用できます。Microsoft クラスタ ソフトウェアでは、パブリック アダプタに限り、すべての Broadcom チーム化モードがサポートされます。プライベート ネットワーク アダプタのチーム化はサポートされません。Microsoft の発表によると、サーバー クラスタでは、プライベートな相互接続にチーム化を使用できません。これは、ノード間でハートビート パケットを送受信するために遅延が発生する可能性があるからです。プライベートな相互接続に冗長性を確保して、同時に優れたパフォーマンスも実現するには、チーム化をディスエーブルして、使用可能なポートでプライベートな第 2 の相互接続を確立します。この方法でも機能的には同じ効果があり、複数のノードが通信に使用できる二重の堅牢な通信パスが実現されます。

クラスタ環境でチーム化を行う場合は、同じブランドのアダプタを使用することをお勧めします。

注：Microsoft ネットワーク負荷分散は、Microsoft クラスタ ソフトウェアではサポートされません。

チーム化とネットワーク バックアップ

チーム化していない環境で、ネットワーク バックアップを実行すると、バックアップ サーバー アダプタの全体的な転送速度は、過剰なトラフィックとアダプタの大きな負荷によってすぐに影響を受けます。バックアップ サーバーの数、データ ストリーム、テープ ドライブの速度によって変わりますが、バックアップ トラフィックは、ネットワーク リンクの帯域幅の大部分を簡単に消費するので、実稼動環境のデータ処理速度やテープ バックアップのパフォーマンスに影響が出ます。ネットワーク バックアップは、通常、NetBackup、Galaxy または Backup Exec など、テープ バックアップ ソフトウェアを実行する専用のバックアップ サーバーで構成されます。バックアップ サーバーに接続するデバイスは、直接 SCSI テープ バックアップ ユニット、またはファイバ チャネルのストレージ エリア ネットワーク (SAN) で接続したテープ ライブラリです。ネットワークを通じてバックアップされるシステムは、一般的に、クライアント システムまたはリモート サーバーと呼ばれ、テープ バックアップ ソフトウェア エージェントがインストールされています。

4 つのクライアント サーバーがあるので、バックアップ サーバーは、マルチドライブ オートローダに対して、同時に 4 つのバックアップ ジョブ (クライアントごとに 1 ジョブ) を実行できます。ただし、スイッチとバックアップ サーバーの間のリンクは 1 つなので、4 ストリームのバックアップでは、アダプタとリンクがすぐにリソース不足の状態になる可能性があります。バックアップ サーバーのアダプタが 1 Gbps (125 MB/ 秒) で動作しており、各クライアントがテープ バックアップ時に 20 MB/ 秒でデータを転送できる場合、バックアップ サーバーとスイッチの間のスループットは、80 MB/ 秒 (20 MB/ 秒 x 4) になります。これは、ネットワークの帯域幅の 64 % に相当します。この数値は、ネットワークの帯域幅の中に収まっていますが、他のアプリケーションと同じリンクを共有している場合、64 % は高い割合と考えられます。

ロード バランシングおよびフェイルオーバー

バックアップ ストリームの数が増えると、全体的なスループットも増加します。ただし、各データ ストリームは、25 MB/ 秒 の 1 つのバックアップ ストリームと同じパフォーマンスを維持できない場合があります。言い換えると、バックアップ サーバーは 25 MB/ 秒 の単一クライアントのデータ ストリームには対応できますが、100 MB/ 秒 (25 MB/ 秒 x 4 ストリーム) で 4 つの同時実行バックアップ ジョブに対応することは困難です。バックアップ ストリームの数が増えると全体的なスループットが増加しますが、各バックアップ ストリームはテープ ソフトウェアまたはネットワーク スタックの制限に影響を受ける可能性があります。

クライアントのバックアップを実行するときに、テープ バックアップ サーバーでアダプタの最適なパフォーマンスを引き出し、高い信頼性でネットワークの帯域幅を使用するには、ネットワーク インフラストラクチャでロード バランシングやフォルト トレランスなど、チーム化を実装する必要があります。データ センターは、フォルト トレランス対応ソリューションの一部として、冗長スイッチ、リンク集約、およびトランキングを組み込みます。チーム化されたデバイス ドライバは、チーム化されたインターフェイスとフェイルオーバー パスをデータが流れる方法を制御しますが、この処理はテープ バックアップ アプリケーション側からは見えません。また、ネットワークを通じて、リモート システムをバックアップするときに、テープ バックアップ プロセスがこの処理の干渉を受けることもありません。図 6 では、Broadcom のチーム化環境でテープ バックアップをデモンストレーションするネットワーク トポロジーであり、Smart Load Balancing がチーム化したアダプタの間で、どのようにテープ バックアップ データの *ロード バランス*を行うかを示します。

クライアントサーバーがバックアップ サーバーへのデータ送信に使用できるパスは 4 つありますが、データ転送時にはこれらのパスの 1 つだけが指定されます。バックアップ サーバーへのデータ送信にクライアントサーバー Red が使用できるパスは以下のとおりです。

パスの例：クライアントサーバー Red は、アダプタ A、スイッチ 1、バックアップ サーバー アダプタ A を通じてデータを送信します。

指定されたパスは、以下の 2 つの要素によって決まります。

1. クライアントサーバー ARP キャッシュ。これは、バックアップ サーバーの MAC アドレスを指定します。これは、Broadcom 中間ドライバのインバウンド ロード バランシング アルゴリズムによって決定されます。
2. クライアントサーバー Red の物理アダプタ インターフェイスは、データ転送に使用されます。Broadcom 中間ドライバのアウトバウンド ロード バランシング アルゴリズムがこれを決定します (アウトバウンド トラフィック フローとインバウンド トラフィック フロー (SLB のみ) を参照)。

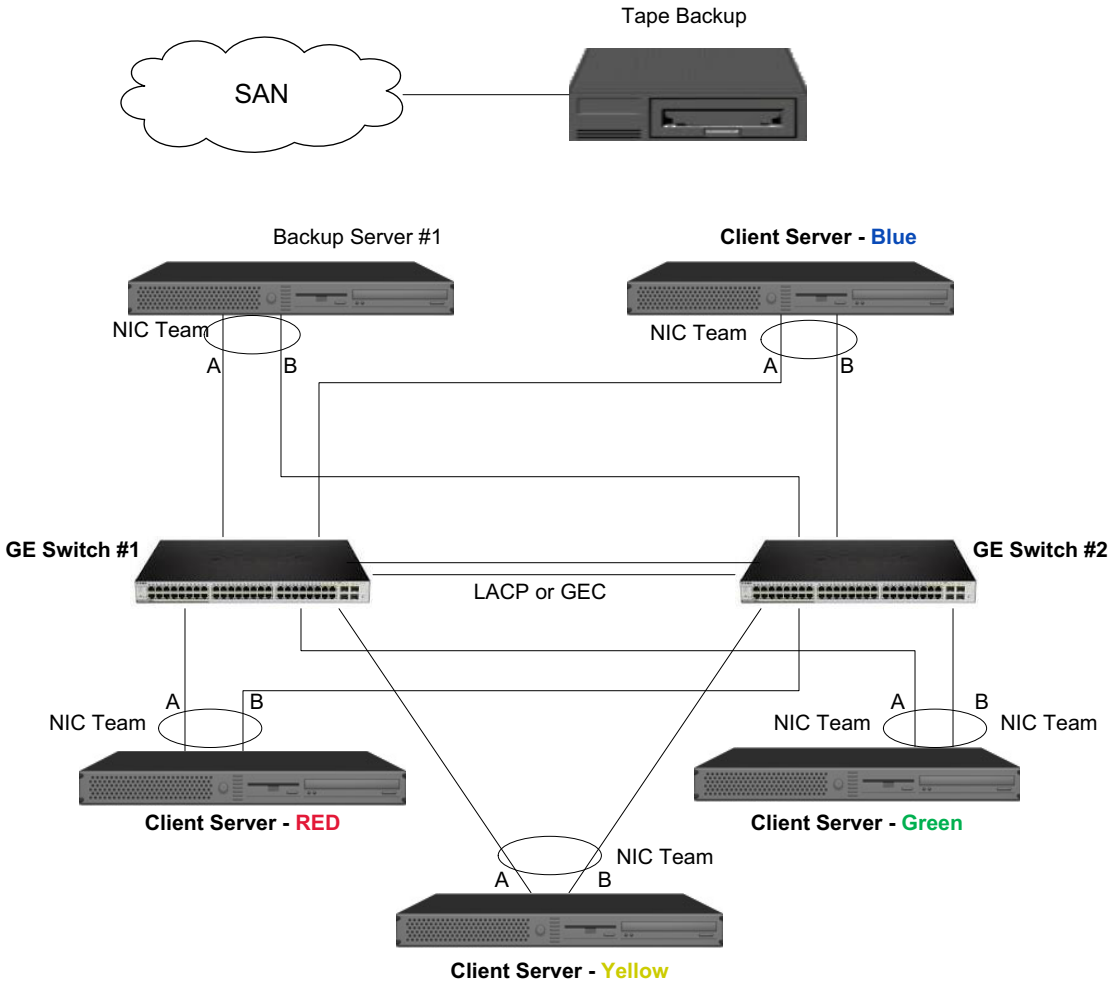
バックアップ サーバーのチーム化インターフェイスは、クライアントサーバー Red への転送に G-ARP (gratuitous address resolution protocol) を使用します。そして今後は、クライアント サーバーの ARP キャッシュがバックアップ サーバーの MAC アドレスで更新されるようになります。チーム化インターフェイス内のロード バランシング メカニズムによって、G-ARP に組み込まれる MAC アドレスが決定されます。選択された MAC アドレスは、基本的にクライアントサーバーがデータの転送先として使用するアドレスです。クライアントサーバー Red では、SLB チーム化アルゴリズムによって、2 つのアダプタ インターフェイスから、実際にデータ転送に使用するインターフェイスが決定されます。この例では、クライアントサーバー Red からのデータが、バックアップ サーバーのアダプタ A インターフェイスで受信されます。チーム化したインターフェイスにさらに負担がかかったときに SLB が機能する仕組みをデモンストレーションするため、バックアップ サーバーが第 2 のバックアップ処理を開始するシナリオを考えてみます。具体的には、クライアントサーバー Red へのバックアップに加えて、クライアントサーバー Blue に対して第 2 のバックアップを開始します。バックアップ サーバーへのデータ送信にクライアントサーバー Blue が使用するルートは、バックアップ サーバーの MAC アドレスを指定する ARP キャッシュによって決定されます。バックアップ サーバーのアダプタ A では、すでにクライアントサーバー Red のバックアップ処理で負担がかかっているため、バックアップ サーバーは、SLB アルゴリズムを呼び出します。そして、ARP キャッシュをバックアップ サーバーのアダプタ B の MAC アドレスに変更するように、クライアントサーバー Blue に (G-ARP を通じて) *通知メッセージを送信*します。クライアントサーバー Blue は、データを転送する必要があるとき、SLB アルゴリズムによって決定されたいずれかのアダプタ インターフェイスを使用します。重要な点は、クライアントサーバー Blue からのデータが、バックアップ サーバーのアダプタ A インターフェイスではなく、アダプタ B インターフェイスで受信されることです。これが重要とされる理由は、両方のバックアップ ストリームが同時に実行されており、バックアップ サーバーは、異なるクライアントからのデータ ストリームに対して *ロード バランス*を実行する必要があるからです。両方のバックアップ ストリームを実行している場合、バックアップ サーバーの各アダプタ インターフェイスは同等の負荷を担っており、ロード バランス対象のデータは、両方のアダプタ インターフェイスで均等に処理されることになります。

バックアップ サーバーが第 3、第 4 のバックアップ処理を開始した場合も、同じアルゴリズムが適用されます。バックアップ サーバーでチーム化したインターフェイスは、ユニキャスト G-ARP を転送して、バックアップ クライアントに ARP キャッシュを更新するように通知します。そして、各クライアントは、バックアップ サーバー上のターゲット MAC アドレスに至るルートで、バックアップ データを転送します。

フォルト トレランス

テープ バックアップの実行中にネットワーク リンクで障害が発生した場合、バックアップ サーバーとクライアントの間のすべてのトラフィックが停止して、バックアップ ジョブが失敗します。しかし、Broadcom SLB とスイッチ フォルト トレランスの両方に対応するように、ネットワーク トポロジーを設定した場合、リンクに障害が発生しても、滞りなくテープ バックアップを続行することができます。ネットワーク内のすべてのフェイルオーバー プロセスは、テープ バックアップ ソフトウェア アプリケーション側では見えません。ネットワーク フェイルオーバー プロセスで、バックアップ データ ストリームの送信先を決定する方法を理解するには、図 6 のトポロジーを理解してください。クライアントサーバー Red は、パス 1 を通じてバックアップ サーバーにデータを転送しますが、リンク障害はバックアップ サーバーとスイッチの間で発生します。データは、スイッチ #1 からバックアップ サーバーのアダプタ A インターフェイスへ送信できなくなったので、このデータは、スイッチ #1 からスイッチ #2 を介して、バックアップ サーバーのアダプタ B インターフェイスにリダイレクトされます。フォルト トレランス対応の動作はすべてアダプタ チームのインターフェイスとスイッチ上の中継の設定によって処理されるので、リダイレクトはバックアップ アプリケーションに認識されずに実行されます。クライアント サーバー側から見ると、元のパスを介してデータを送信しているように動作します。

図 6:2 つのスイッチにまたがる SLB チーム化によるネットワーク バックアップ



チーム化に関する問題のトラブルシューティング

仮想アダプタのチーム化インターフェイス上でプロトコル アナライザ を実行すると、送信されたフレームに示される MAC アドレスは正確でない場合があります。アナライザは、BASP で構築したフレームを表示せず、フレームを転送するインターフェイスの MAC アドレスでなく、チームの MAC アドレスを表示します。以下の手順でチームを監視することをお勧めします。

1. チームのすべてのアップリンク ポートをスイッチでミラーリングします。
2. チームが 2 つのスイッチにまたがる場合は、相互トランクもミラーリングします。
3. すべてのミラーポートを個別にサンプリングします。
4. アナライザでは、QoS と VLAN の情報をフィルタしないアダプタとドライバを使用します。

チーム化の設定のヒント

ネットワーク接続またはチーム化機能のトラブルシューティングをするときは、次の説明が指定した設定に当てはまることを確認します。

1. SLB チームに対しては、すべてのアダプタを同じリンク速度にすることをお勧めします。
2. LiveLink が有効でない場合は、Spanning Tree Protocol を無効にするか、チームに接続するスイッチ ポートの 初期フェーズ (Port Fast、Edge Port など) を迂回する STP モードを有効にします。
3. チームを直接接続するすべてのスイッチは、サポート対象であるハードウェア、ファームウェア、ソフトウェアの同じバージョンのものを使用する必要があります。
4. チーム化するには、アダプタは同じ VLAN のメンバーである必要があります。複数のチームを設定する場合は、各チームが別々のネットワーク上になければなりません。
5. [Locally Administered Address (ローカル管理アドレス)] フィールドにマルチキャストまたはブロードキャスト アドレスを入力しないでください。
6. チームのメンバーである物理アダプタには、Locally Administered Address (ローカル管理アドレス) を割り当てることができません。
7. すべての物理メンバーについて電源の管理が無効になっていることを確認します (アダプタの **[プロパティ]** の **[電源の管理]** タブで、**[電力の節約のために、コンピュータでこのデバイスの電源をオフにできるようにする]** ボックスをオフにします。「Windows ドライバとアプリケーションのインストール」の電源の管理オプションを設定するを参照してください)。
8. チームを構築する前に、チームの物理メンバーのそれぞれの静的 IP アドレスを削除します。
9. 最大のスループットを必要とするチームには LACP または GEC/FEC を使用する必要があります。このような場合は、中間ドライバがアウトバウンドのロード バランシングのみを担当し、スイッチがインバウンドのロードバランシングを行います。
10. 集約されたチーム (802.3ad/LACP および GEC/FEC) は、IEEE 802.3a、LACP、または GEC/FEC をサポートする単一のスイッチにのみ接続する必要があります。
11. ハブは半二重通信しかサポートしないため、チームをハブに接続することはお勧めできません。ハブをチームに接続するのは、トラブルシューティングを目的とする場合に限ります。LACP または GEC/FEC チームに参加しているネットワーク アダプタのデバイス ドライバをディスエーブルすると、ネットワーク接続に悪影響を与える場合があります。ネットワーク接続の切断を避けるために、デバイス ドライバをディスエーブルする前に、アダプタをスイッチか

ら物理的に取り外してください。

12. ベース (ミニポート) ドライバとチーム (中間) ドライバが同じリリース パッケージであることを確認します。
13. チーム化する前に、各物理アダプタの接続をテストします。
14. 実稼動環境に移行する前に、チームのフェイルオーバーとフォールバックの動作をテストします。
15. 非実稼動ネットワークから実稼動ネットワークに移行する場合は、フェイルオーバーとフォールバックを再度テストすることを強くお勧めします。
16. 実稼動環境に移行する前に、チームのパフォーマンスの動作をテストします。

トラブルシューティングのガイドライン

システムでアダプタのチーム化を使用している場合は、サポートへ問い合わせる前に、以下に示すネットワーク接続に関する問題のトラブルシューティングを実行してください。

1. 各アダプタのイーサネット リンク ライトが点灯しており、すべてのケーブルが接続されていることを確認します。
2. ベース ドライバと中間ドライバのリリース パッケージが同じであり、正しくロードされていることを確認します。
3. Windows の **ipconfig** コマンドを使用して、IP アドレスが有効かどうかを確認します。
4. チームに接続されたスイッチ ポートの STP が無効であることまたは Edge Port/Port Fast が有効であること、あるいは LiveLink が使用されていることを確認します。
5. アダプタとスイッチのリンク速度と二重通信方式の設定が同じであることを確認します。
6. 可能な場合は、チームを分割し、各アダプタへの接続を個別に調べて、問題が直接チーム化に関連することであるかどうかを確認します。
7. チームに接続するすべてのスイッチ ポートが同じ VLAN 上に存在することを確認します。
8. スイッチ ポートが通有中継 (FEC/GEC)/802.3ad-Draft Static チーム タイプ対応に正しく設定されていること、およびアダプタのチーム タイプに一致していることを確認します。システムが SLB チーム タイプ対応に設定されている場合は、対応するスイッチ ポートが通有中継 (FEC/GEC)/802.3ad-Draft Static チーム タイプに設定されていないことを確認します。

よくある質問

質問：	どのような状況だと、トラフィックのロード バランシングは行われないのでしょうか。チームのすべてのメンバー間で均等にロード バランシングが行われないのはなぜですか。
対応策：	大量のトラフィックが IP/TCP/UDP を使用していないか、多くのクライアントが別のネットワークに接続しています。受信のロード バランシングはトラフィック負荷に対する機能ではなく、システムに接続するクライアントの数に対して実行される機能です。

質問：	チーム内でロード バランシングが行われるネットワーク プロトコルを教えてください。
対応策：	Broadcom のチーム化ソフトウェアは IP/TCP/UDP トラフィックのみをサポートします。それ以外のトラフィックはすべてプライマリ アダプタに転送されます。

質問：	SLB でロード バランシングが行われるプロトコルと、行われないプロトコルを教えてください。
対応策：	送信と受信の両方向でロード バランシングが行われるのは、IP/TCP/UDP

質問：	100 Mbps で動作するポートと 1000 Mbps で動作するポートをチーム化できますか。
対応策：	異なるリンク速度のポートの混在は、前述のように Smart Load Balancing™ のチームと 802.3ad チームでのみサポートします。

質問：	ファイバ アダプタと銅線 Gigabit Ethernet アダプタをチーム化できますか。
対応策：	SLB では可能です。スイッチが FEC/GEC および 802.3ad に対応する場合も可能です。

質問：	アダプタのロード バランシングと Microsoft ネットワーク負荷分散 (NLB) との違いは何ですか。
対応策：	アダプタのロード バランシングはネットワーク セッション レベルで行われますが、NLB はシステム アプリケーション レベルで行われます。

質問：	チーム化されたアダプタをルーターのポートに接続できますか。
対応策：	いいえ。チーム内のポートはすべて同一のネットワーク上に存在する必要がありますが、ルーターでは定義上各ポートが個別のネットワークにあります。チーム化のすべてのモードでは、リンク パートナーがレイヤー 2 スイッチであることが必要です。

質問：	Microsoft Cluster Services でチーム化を使用できますか。
対応策：	はい。チーム化は、パブリック ネットワーク上でのみサポートされます。ハートビート リンクで使用するプライベート ネットワークではサポートされません。

質問：	PXE は仮想アダプタ (チーム) 上で動作しますか。
対応策：	PXE クライアントは、オペレーティング システムがロードされる前の環境、つまり、仮想アダプタはまだ有効になっていない状態で動作します。物理アダプタが PXE をサポートする場合は、オペレーティング システムのロード時に仮想アダプタの要素になるかどうかにかかわらず、これを PXE クライアントとして利用できます。PXE サーバーは仮想アダプタ上で動作します。

質問：	WOL は仮想アダプタ (チーム) 上で動作しますか。
対応策：	Wake-on-LAN 機能は、オペレーティング システムがロードされる前の環境で動作します。WOL は、システムが停止またはスタンバイの状態で起動するので、チームは設定されません。

質問：	ポートは最大何個までチーム化できますか。
対応策：	最大 8 個のポートをチームに割り当てることができます。

質問：	同一のシステム上で設定できるチームは最大何個ですか。
対応策：	同一のシステム上で最大 16 個のチームを設定できます。

質問：	プライマリ アダプタを元に戻して (フォールバック) から 30 ～ 50 秒間チームの接続が失われるのはなぜですか。
対応策：	Spanning Tree Protocol が、ポートをブロックから転送に移行させているためです。STP 遅延を考慮するには、チームに接続されたスイッチ ポート上で Port Fast または Edge Port を有効にするか、LiveLink を使用する必要があります。

質問：	複数のスイッチにまたがってチームを接続できますか。
対応策：	Smart Load Balancing では、システム内の個々の物理アダプタが一意の Ethernet MAC アドレスを使用するので、複数のスイッチを使用できます。リンク集約と通有中継は、すべての物理アダプタが同一の Ethernet MAC アドレスを共有するので、スイッチにまたがって動作することはできません。

質問：	中間ドライバ (BASP) をアップグレードする方法を教えてください。
対応策：	[ローカルエリア接続のプロパティ] では中間ドライバをアップグレードできません。Setup インストーラを使用してアップグレードする必要があります。

質問：	仮想アダプタ (チーム) のパフォーマンス統計を確認するにはどうすればよいですか。
対応策：	Broadcom Advanced Control Suite で、仮想アダプタの [BASP 統計] タブをクリックします。

質問：	NLB とチーム化を同時に設定できますか。
対応策：	はい。ただし、NLB がマルチキャスト モードで動作する場合に限ります (NLB は MS Cluster Services ではサポートされません)。

質問：	バックアップ システムとバックアップされるクライアント システムの両方をチーム化する必要がありますか。
対応策：	バックアップ システムは多くのデータをロードするので、常にチーム化してリンク集約とフェイルオーバーを実現する必要があります。ただし、冗長性の十分なネットワークでは、スイッチとバックアップ クライアントの両方をチーム化してフォルト トレランスとリンク集約を実現する必要があります。

質問：	バックアップ処理中に、アダプタのチーム化アルゴリズムではバイトレベルまたはセッションレベルのロード バランシングを行いますか。
対応策：	アダプタのチーム化を使用すると、データのロード バランシングはセッションレベルでのみ行われ、フレームの順序が狂うことを防ぐためにバイトレベルでは実行されません。アダプタのチーム化のロード バランシングは、EMC PowerPath などの他のストレージのロード バランシング メカニズムと同様には機能しません。

質問：	テープ バックアップ ソフトウェアまたはハードウェアには、アダプタのチーム化で動作するための特別な設定が必要ですか。
対応策：	テープ ソフトウェアにはチーム化で動作するための特別な設定は必要ありません。テープ バックアップ アプリケーション側からはチーム化は見えません。

質問：	現在使用しているドライバを確認するにはどうすればよいですか。
対応策：	すべてのオペレーティング システムにおいて、ドライバのバージョンを確認する最も確実な方法は、ドライバ ファイルを実際に探して、そのプロパティを確認することです。

質問：	SLB は、スイッチのフォルト トレランスの設定でスイッチの障害を検出できますか。
対応策：	いいえ。SLB で検出できるのは、チーム化されたポートとその直接のリンク パートナーの間で発生するリンク ロスだけです。それ以外のポートのリンク障害を検出できません。詳細は、LiveLink™ 機能を参照してください。

質問：	Windows システムでアダプタ チームの統計をリアルタイムに監視するには、どうしたらよいでしょうか。
対応策：	Broadcom Advanced Control Suite (BACS) を使用して IEEE 802.3 の一般的なカウントとカスタム カウンタを監視できます。

イベント ログのメッセージ

Windows システムのイベント ログのメッセージ

既知のベース ドライバおよび中間ドライバの Broadcom NetXtreme Gigabit Ethernet アダプタに関する Windows システムのイベント ログのステータス メッセージを次のセクションで一覧表示します。Broadcom アダプタ ドライバがロードされると、Windows はシステム イベント ビューアにステータス コードを表示します。こうしたイベント コードには、両方のドライバがロードされたかどうかに応じて (1 つはベース ドライバまたはミニポート ドライバ用、もう 1 つは中間ドライバまたはチーム化ドライバ用)、最大 2 つのクラスがあります。

ベース ドライバ (物理アダプタ / ミニポート)

表 11 に、ベース ドライバでサポートするイベント ログ メッセージを一覧表示し、メッセージの原因を説明します。また、推奨される対応策も示します。

表 11: ベース ドライバのイベント ログ メッセージ

メッセージ番号	メッセージ	原因	対応策
1	デバイス ブロックにメモリを割り当てることができませんでした。システム メモリ リソースの使用量を確認してください。	ドライバはオペレーティング システムからメモリを割り当てできません。	実行中のアプリケーションを閉じて空きメモリを増やします。
2	マップ レジスタを割り当てることができませんでした。	ドライバはオペレーティング システムからマップ レジスタを割り当てできません。	マップ レジスタを割り当てる可能性のある、他のドライバをアンロードします。
3	構成情報にアクセスできませんでした。ネットワーク ドライバを再インストールしてください。	ドライバは、アダプタ上の PCI コンフィギュレーション スペース レジスタにアクセスできません。	アドイン アダプタの場合は、アダプタをスロットに装着し直すか、アダプタを別の PCI スロットに移動するか、またはアダプタを交換します。
4	ネットワーク リンクが停止しています。ネットワーク ケーブルが正しく接続されているか確認してください。	アダプタとそのリンク パートナーとの接続が失われています。	ネットワーク ケーブルが接続されていることを確認し、ネットワーク ケーブルの種類が適切であることを調べて、リンク パートナー (スイッチまたはハブなど) が正しく機能していることを確認します。

表 11: ベース ドライバのイベント ログ メッセージ (続き)

メッセージ番号	メッセージ	原因	対応策
5	ネットワーク リンクは起動しています	アダプタがリンクを確立しています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
6	10Mb 半二重リンク用にネットワーク コントローラが構成されました。	アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
7	10Mb 全二重リンク用にネットワーク コントローラが構成されました。	アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
8	100Mb 半二重リンク用にネットワーク コントローラが構成されました。	アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
9	100Mb 全二重リンク用にネットワーク コントローラが構成されました。	アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
10	1Gb 半二重リンク用にネットワーク コントローラが構成されました。	アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
11	1Gb 全二重リンク用にネットワーク コントローラが構成されました。	アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
12	メディアはサポートされていません。	オペレーティング システムは IEEE 802.3 メディアをサポートしません。	オペレーティング システムを再起動して、ウィルス チェックを実行し、ディスク チェック (chkdsk) を実行して、オペレーティング システムを再インストールします。
13	割り込みサービスルーチンを登録できません。	デバイス ドライバは割り込みハンドラをインストールできません。	オペレーティング システムを再起動し、同一の IRQ を共有する可能性のあるその他のデバイス ドライバを削除します。
14	IO 領域をマップできません。	デバイス ドライバは、メモリにマップされた I/O をアクセス ドライバ レジスタに割り当てできません。	システムから他のアダプタを取り外し、インストールされた物理メモリ量を削減し、アダプタを交換します。
15	ドライバは正常に初期化されました。	ドライバは正常にロードされました。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
16	Ndis がミニポート ドライバをリセットしています。	NDIS レイヤは送受信パケットの問題を検出し、ドライバをリセットして問題を解決します。	Broadcom Advanced Control Suite 診断を実行し、ネットワーク ケーブルに問題がないことを確認します。

表 11: ベース ドライバのイベント ログ メッセージ (続き)

メッセージ番号	メッセージ	原因	対応策
18	不明な PHY が検出されました。既定の PHY 初期化ルーチンを使用しています。	ドライバは PHY ID を読み取れません。	アダプタを交換します。
19	このドライバはこのデバイスをサポートしません。最新のドライバに更新してください。	ドライバがインストールされたアダプタを認識しません。	このアダプタをサポートするバージョンのドライバにアップグレードします。
20	ドライバを初期化できませんでした。	ドライバの初期化中に特定できないエラーが発生しました。	ドライバを再インストールするか、新しいバージョンのドライバに更新するか、Broadcom Advanced Control Suite 診断を実行するか、あるいはアダプタを交換します。
21	Ethernet@WireSpeed は有効であり、最大リンク速度をネゴシエートできませんでした。	ケーブルまた接続に障害が発生している可能性があります。	ケーブルを再接続するか交換します。
22	このオペレーティング システムの廃止されたネットワーク コントローラ用のデバイス ドライバをインストールできません。	最新のアウトボックス ドライバは廃止されたデバイスをサポートしていません。	OS インボックス ドライバを使用するか、デバイスを最新のものと交換します。
256	連結プール用の連続した物理メモリが不足しています。	ドライバは、連結パケット バッファに対して十分な共有メモリを割り当てることができません。	システムから他のアダプタを削除 / 無効化するか、システムのメモリを増やします。

中間ドライバ (仮想アダプタ / チーム)

表 12 に、中間ドライバでサポートするイベント ログ メッセージを一覧表示し、メッセージの原因を説明します。また、推奨される対応策も示します。

表 12: 中間ドライバのイベント ログ メッセージ

システム イベント メッセージ番号	メッセージ	原因	対応策
1	Unable to register with NDIS. (NDIS に登録できません。)	ドライバを NDIS インターフェイスに登録できません。	他の NDIS ドライバをアンロードします。
2	Unable to instantiate the management interface. (管理インターフェイスをインスタンス化できません。)	ドライバはデバイス インスタンスを作成できません。	オペレーティング システムを再起動します。
3	Unable to create symbolic link for the management interface. (管理インターフェイス用のシンボリック リンクを作成できません。)	別のデバイスによって競合するデバイス名が作成されています。	*Blf* という名前を使用している、競合するデバイス ドライバをアンロードします。

表 12: 中間ドライバのイベント ログ メッセージ (続き)

システム イベント メッセージ番号	メッセージ	原因	対応策
4	Broadcom Advanced Server Program Driver has started. (Broadcom Advanced Server Program ドライバが開始しました。)	別のデバイスによって競合するデバイス名が作成されています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
5	Broadcom Advanced Server Program Driver has stopped. (Broadcom Advanced Server Program ドライバが停止しました。)	ドライバはすでに停止しています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
6	Could not allocate memory for internal data structures. (内部データ構造にメモリを割り当てることができませんでした。)	ドライバはオペレーティング システムからメモリを割り当てできません。	実行中のアプリケーションを閉じて空きメモリを増やします。
7	Could not bind to adapter. (アダプタにバインドできません。)	ドライバはチームの物理アダプタの 1 つを開けませんでした。	物理アダプタ ドライバをアンロードしてからリロードするか、更新された物理ドライバを取り付けるか、あるいは物理アダプタを交換します。
8	Successfully bind to adapter. (アダプタに正常にバインドされています。)	ドライバは物理アダプタを正常に開きました。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
9	Network adapter is disconnected. (ネットワーク アダプタは切断されています。)	物理アダプタはネットワークに接続されていません (リンクが確立されていません)。	ネットワーク ケーブルが接続されていることを確認し、ネットワーク ケーブルの種類が適切であることを調べて、リンク パートナー (スイッチまたはハブなど) が正しく機能していることを確認します。
10	Network adapter is connected. (ネットワーク アダプタは接続されています。)	物理アダプタはネットワークに接続されています (リンクが確立されています)。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
11	Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System. (Broadcom Advanced Program Features ドライバは、このバージョンのオペレーティング システムでは動作しません。)	ドライバは、インストールされているオペレーティング システムをサポートしていません。	ドライバのリリース ノートを確認し、サポートされているオペレーティング システム上にインストールするか、ドライバを更新します。
12	Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter. (ホットスタンバイ アダプタが、ロード バランシング アダプタのないチームのプライマリ アダプタとして選択されています。)	スタンバイ アダプタはアクティブになっています。	故障した物理アダプタを交換します。

表 12: 中間ドライバのイベント ログ メッセージ (続き)

システム イベント メッセージ番号	メッセージ	原因	対応策
13	Network adapter does not support Advanced Failover. (ネットワーク アダプタは Advanced Failover をサポートしません。)	物理アダプタは、Broadcom NIC Extension (NICE) をサポートしていません。	NICE をサポートするアダプタに交換します。
14	Network adapter is enabled via management interface. (ネットワーク アダプタは、管理インターフェイスを介して有効化されています。)	ドライバは、管理インターフェイスを介して物理アダプタを有効化しました。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
15	Network adapter is disabled via management interface. (ネットワーク アダプタは、管理インターフェイスを介して無効化されています。)	ドライバは、管理インターフェイスを介して物理アダプタを無効化しました。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
16	Network adapter is activated and is participating in network traffic. (ネットワーク アダプタはアクティブ化され、ネットワーク トラフィックに加わっています。)	物理アダプタはチームに追加され、アクティブにされています。	情報提供のみを目的としたメッセージです。対応策は必要ありません。
17	Network adapter is de-activated and is no longer participating in network traffic. (ネットワーク アダプタは非アクティブ化され、ネットワーク トラフィックに加わっていません。)	ドライバがインストールされたアダプタを認識しません。	情報提供のみを目的としたメッセージです。対応策は必要ありません。

セクション 4: 仮想 LAN

VLAN の概要

VLAN (仮想 LAN) を利用すると、物理 LAN を理論的なパーツに分割し、ワークグループの論理的なセグメントを作成できます。これにより各論理セグメントごとにセキュリティ ポリシーを設定することが可能になります。定義済みの VLAN は、そのトラフィックや同報通信がその他の VLAN から分離されるため、それぞれが独自の分離されたネットワークとして機能します。これにより各論理グループ内の帯域幅の効率が向上します。サーバー上の 1 つの Broadcom アダプタには最大 64 個（タグ付けされたもの 63 件、タグ付けされていないもの 1 件）までの VLAN が定義できます。定義できる数はシステム内で利用できるメモリ数により異なります。

チームには複数の VLAN を追加し、異なる VLAN ID をもつ 複数の VLAN を許可することができます。バーチャル アダプタが追加されたそれぞれの VLAN について作成されます。

VLAN は通常、独立した同報通信のドメインを作成したり、IP サブネットを分離するとき利用するものですが、サーバーには同時に 複数の VLAN を与えておくと便利です。Broadcom アダプタなら、ポート別、またはチーム別に複数の VLAN がサポートできます。このためネットワークのコンフィギュレーションがとてもフレキシブルになります。

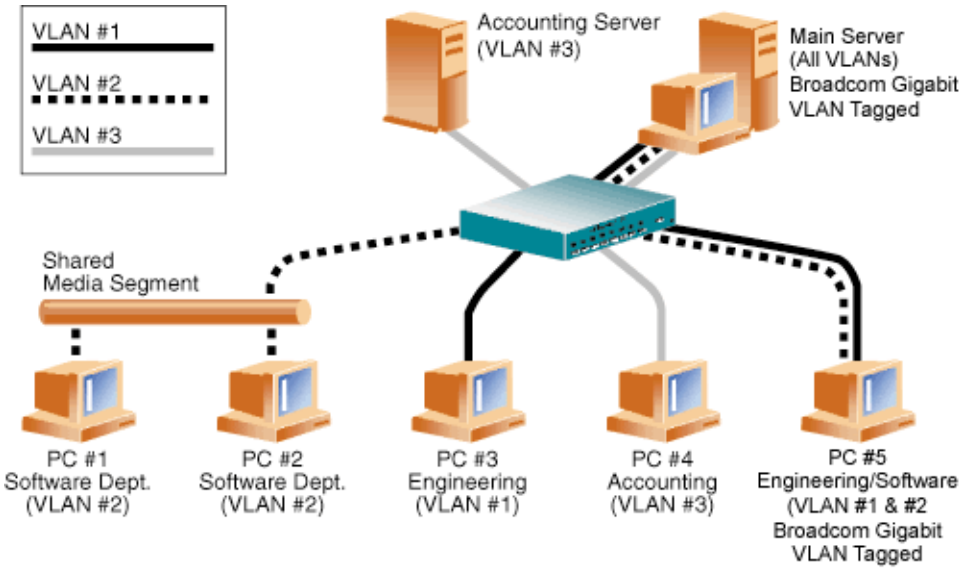


図 7: タグ付けされた複数の VLAN をサポートするサーバーの例

図 7 は、VLAN を使用するネットワークの例を示しています。このネットワーク例では、物理 LAN は 1 つのスイッチ、2 つのサーバー、5 件のクライアントで構成されています。LAN は論理的に 3 つの異なる VLAN に組織化されます。VLAN はそれぞれ異なる IP サブネットを代表します。このネットワークの機能について、表 13 で説明します。

表 13:VLAN ネットワークのトポロジー例

コンポーネント	*説明*
VLAN #1	メイン サーバー、PC #3、PC #5 で構成される IP サブネットです。このサブネットはエンジニアリング グループを表わします。
VLAN #2	メイン サーバー、共有メディア セグメント経由の PC #1、PC#2、および PC #5 を含みます。この VLAN はソフトウェア開発グループです。
VLAN #3	メイン サーバー、アカウンティング サーバー、PC #4 を含みます。この VLAN はアカウンティング グループです。
メイン サーバー	最も頻繁に使用されるサーバーで、すべての VLAN と IP サブネットからアクセスする必要があります。メイン サーバーには Broadcom アダプタがインストールされています。3 つの IP サブネットには、1 つの物理アダプタ インターフェイスでアクセスします。サーバーはスイッチ ポートの 1 つに取り付けられ、VLAN #1、#2、#3 に構成します。アダプタと接続されたスイッチ ポートのタギングは両方ともオンにします。この両デバイスのタグ付けされた VLAN の容量のために、サーバーはネットワーク内では 3 つの IP サブネットすべてで通信を行うことができますが、同報通信分離を維持しなければなりません。
アカウンティング サーバー	VLAN #3 のみで利用可能です。アカウンティング サーバーは VLAN #1 と VLAN #2 上のすべてのトラフィックから遮断されます。サーバーに接続されたスイッチ ポートのタギングはオフにします。
PC #1 および PC #2	共有メディア ハブに接続し、次にスイッチに接続します。PC #1 と PC #2 は VLAN #2 のみに属し、論理的にはメイン サーバーと PC #5 と同じ IP サブネットにあります。このセグメントに接続されたスイッチ ポートのタギングはオフにします。
PC #3	VLAN #1 と PC #3 のメンバーは、メイン サーバーと PC #5 としか通信できません。PC #3 のスイッチ ポート上ではタギングはイネーブルできません。
PC #4	VLAN #3 のメンバーである PC #4 は、サーバーとしか通信できません。PC #4 のスイッチ ポート上ではタギングはイネーブルできません。
PC #5	VLAN #1、#2 のメンバーと PC #5 には Broadcom アダプタがインストールされています。これはスイッチ ポート #10 に接続されます。両方のアダプタとスイッチ ポートは VLAN #1 と VLAN #2 用に設定され、タギングがイネーブルされます。

注：VLAN のタギングは、他のスイッチに対する中継リンクを作成するスイッチ ポート上、または Broadcom アダプタを使用しているサーバーやワークステーションといったタグ付け可能なエンド ステーション以外ではイネーブルする必要はありません。

チームに VLAN を追加する

1 つのチームあたり、64 個の VLAN がサポートできます（タグ付けされたもの 63 件、タグ付けされていないもの 1 件）。1 つのアダプタ上に複数の VLAN がある場合、アダプタが 1 つしかないサーバーでは、複数の IP サブネット上に 1 つの論理プレゼンスしか与えられません。1 つのチームに複数の VLAN がある場合は、複数の IP サブネットに 1 つの論理プレゼンスを与え、ロードバランシングとフェイルオーバーによる利点を生かすことができます。チームに VLAN を追加する手順について、Windows オペレーティング システムの場合は VLAN の追加を参照してください。

注: フェイルオーバー チームのメンバーとなっているアダプタも VLAN をサポートするよう設定することができます。サードパーティの NIC がフェイルオーバー チームのメンバーである場合、サードパーティの NIC では VLAN がサポートされないため、VLAN をチームに設定することはできません。

セクション 5: 管理方法

CIM

CIM (Common Information Model) は、DMTF (Distributed Management Task Force) により定義されている業界標準です。Microsoft は、Windows Server 2008 などの Windows プラットフォーム上に CIM を実装しています。Broadcom では、Windows Server 2008 プラットフォーム上で CIM をサポートします。

Broadcom では CIM を実装することにより、CIM クライアント アプリケーションを通じて、さまざまな情報提供クラスを実現しました。Broadcom CIM のデータ プロバイダはデータのみを提供します。このため、お好みの CIM クライアント ソフトウェアで Broadcom CIM プロバイダが公開している情報がブラウズできます。

Broadcom CIM プロバイダは BRCM_NetworkAdapter クラスと BRCM_ExtraCapacityGroup クラスにより情報を提供します。BRCM_NetworkAdapter クラスからは、Broadcom やその他のメーカーのコントローラなどを含むアダプタ群に合ったネットワーク アダプタ情報が提供されます。BRCM_ExtraCapacityGroup クラスからは、BASP (Broadcom Advanced Server Program) プログラムでのチーム設定情報が提供されます。現行の実装には、チーム情報とチームの物理ネットワーク アダプタの情報が提供されています。

Broadcom Advanced Server Program では、イベント ログによりイベントが確認できます。イベントの点検・モニタには、CIM を使用するか、Windows Server 2008 プラットフォームでは「イベント ビューアー」が利用できます。Broadcom CIM のプロバイダからは CIM の汎用イベント モデルを通じてイベントの情報が提供されます。これらのイベントは、__InstanceCreationEvent、__InstanceDeletionEvent、__InstanceModificationEvent で、CIM により定義されます。CIM では、イベントを正しく受信するために以下の例のようなクエリを使用し、クライアント アプリケーションからイベントをレジスタするためのクライアント アプリケーションが必要です。

```
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"
```

これらのイベントに関する詳細については、CIM の文書類 (http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf) をご覧ください。

SNMP

BASP サブエージェント

BASP サブエージェントの baspmgnt.dll は、Windows Server の SNMP サービス用に設計されています。BASP サブエージェントをインストールするときは、あらかじめ SNMP サービスをインストールしてください。

BASP サブエージェントを使うと、SNMP マネージャ ソフトウェアで Broadcom Advanced Server 機能の性能やコンフィギュレーションをアクティブにモニタすることができます。サブエージェントを利用すると、SNMP マネージャにアラーム トラップを使用して BASP コンポーネントの状況が変更した場合にマネージャに報告ができるようになります。

BASP サブエージェントを使用すると、コンフィギュレーションと BASP チームの統計のモニタ、チーム内の物理 NIC アダプタのモニタと、チーム化により作成された仮想 NIC アダプタのモニタが可能になります。チーム化されていない NIC アダプタはここではモニタされません。BASP コンフィギュレーション データには、チーム ID 情報、物理 / 仮想 /VLAN/ チームのアダプタ ID、物理 / 仮想 /VLAN/ チーム アダプタの記述、アダプタの MAC アドレスなどが含まれます。

統計には、物理 / 仮想 /VLAN/ チームの各種アダプタの転送・受信されたデータ パケットなどの詳細なデータが含まれます。

アラーム トラップは、物理アダプタのリンク稼動・停止や、アダプタのイベントのインストール・削除など、チーム内の物理アダプタのコンフィギュレーションへの変更に関する情報を転送します。

この情報をモニタするときは、SNMP マネジャーに Broadcom BASP MIB データベース ファイルをロードしてください。以下のファイルが、ドライバ ソース メディアに保存されています。

baspcfg.mib

baspstat.mib

basptrap.mib

BASP エクステンシブルエージェント

Broadcom NetXtreme Gigabit Ethernet Controller の拡張情報、SNMP のエクステンシブルエージェント bcmif.dll は、Windows Server の SNMP サービス用に設計されています。

エクステンシブルエージェントを使えば、SNMP マネージャ ソフトウェアで Broadcom NetXtreme アダプタのコンフィギュレーションがアクティブにモニタできるようになります。これは、標準の SNMP マネジメント ネットワーク インターフェイス情報によってすでに提供されている情報を補足するものです。

エクステンシブルエージェントからは、以下のような Broadcom NetXtreme アダプタに関する詳しい情報が提供されます。

- MAC アドレス
- バインドされた IP アドレス
- IP サブネットマスク
- 物理リンク ステータス
- アダプタの状態
- 回線速度
- 二重通信方式
- メモリ範囲

- 割り込み設定
- バス番号
- デバイス番号
- 機能番号

これらの情報をモニタするときは、SNMP マネジャーに Broadcom 拡張情報の MIB ファイルをロードし、上記のような情報のモニタを許可する必要があります。この bcmif.mib ファイルは、Broadcom NetXtreme アダプタ インストール用 CD に入っています。

モニタリング対象となるワークステーションには、Broadcom 拡張情報の SNMP エクステンシブルエージェント、bcmif.dll をインストールする必要があります。また、Windows Server 2008 の SNMP サービスもインストールし、ロードしておく必要があります。

セクション 6: ハードウェアをインストールする

注：このセクションの内容は Broadcom NetXtreme Gigabit Ethernet アダプタのアドイン NIC モデルのみに当てはまります。

取り扱い注意事項

注意事項：アダプタは、死亡事故につながる恐れのある電圧で動作するシステム内に設置されています。システムのカバーを取り外すときは、以下の注意事項に従い、怪我などのないよう、またシステム コンポーネントに損傷を与えないように注意してください。

- 両手・両手首からは、金属品や貴金属類を外してください。
- 利用する工具が、絶縁されているものであるか、または不伝導性のものであることを確認してください。
- システムの電源が切れていることを確認し、内部コンポーネントに触れる際はプラグも抜いてください。
- アダプタの取り付け・取り外しは、静電気の起きない環境で行ってください。できる限り、正しく接地されたリストストラップや帯電防止デバイス、帯電防止マットなどを利用してください。

インストール事前チェックリスト

1. サーバーで使用している BIOS が最新のものであることを確認します。
2. システムの起動後にオペレーティング システムが立ち上がる場合は、OS を正常にシャットダウンします。
3. システムのシャットダウンが終了したら、電源を切って電源コードを抜きます。
4. アダプタ カードの両角を持って、出荷用パッケージから取り出し、帯電されることのない表面に置きます。
5. アダプタに傷がないかを目視点検します。とくにカードのエッジ コネクタを確認してください。アダプタに損傷がある場合は、取り付けは行わないでください。

アダプタを取り付ける

サーバーに Broadcom NetXtreme Gigabit Ethernet アダプタ (アドイン NIC) を取り付けるときは、以下の手順に従ってください。ご使用中のサーバーによっては実行しなくてはならないタスクがあります。詳細は、サーバーに添付されている文書類をご覧ください。

1. 取り扱い注意事項とインストール事前チェックリストを確認します。アダプタをインストールする前に、システムの電源が切ってあることを確認してから、コンセントからプラグを抜きます。さらに、電気の接地手順が遵守されていることを確認してください。
2. システムのケースを開け、任意の未使用の PCI Express スロットを選択します。
3. 保護用カバー プレートを選択したスロットから取り外します。
4. アダプタのコネクタの端をシステム内のコネクタ スロットに合わせます。
5. カードの両隅に均等に力を加え、アダプタ カードがスロットにしっかりと装着されるまで押し下げます。アダプタが正しく固定されると、アダプタのポート コネクタがスロットの開口部にぴたりと合い、アダプタのフェースプレートはシステムの架台に対して平らになります。

注意事項：カード装着時は力を加えすぎないようにしてください。システムやアダプタに損傷を加える恐れがあります。カードをしっかり固定できない場合は、一度取り外し、場所決めをしなおしてからもう一度固定してください。

6. アダプタをアダプタ クリップまたはねじで固定します。
7. システムのカバーをしっかりと閉じ、帯電防止デバイスから外します。

ネットワーク ケーブルを接続する

銅

Broadcom NetXtreme Gigabit Ethernet アダプタ には、イーサネットの銅線セグメントにシステムを接続するための RJ-45 コネクタが 1 つ以上あります。

注 : Broadcom NetXtreme Gigabit Ethernet アダプタは、自動 MDIX (MDI Crossover) をサポートしています。このため、マシンを直接接続するときに、クロス オーバー ケーブルは必要ありません。また、直流の CAT5 ケーブルにより、直接接続したマシンの通信が可能になります。

1. 適切なケーブルを選択します。表 14 :「10/100/1000BASE-T ケーブルの仕様」に、10/100/1000 BASE-T ポートに接続するケーブルの要件をまとめます。

表 14:10/100/1000BASE-T ケーブルの仕様

ポート タイプ	*コネクタ*	*メディア*	*最長距離*
10BASE-T	RJ-45	CAT3、CAT4、または CAT5 UTP	100 メートル (328 フィート)
100/1000BASE-T[1]	RJ-45	CAT 5[2] の UTP	100 メートル (328 フィート)

[1]1000BASE-T の信号送信には第 5 種の平衡ケーブルのツイスト ペア (より対線) が 4 本必要です。これは ISO/IEC 11801: 1995 および EIA/TIA-568-A (1995) により規定されているもので、TIA/EIA TSB95 で定義されている手順によりテストが行われています。

[2] CAT 5 は必要最低限の要件です。CAT 5e と CAT 6 は完全にサポートされます。

2. ケーブルの片端をアダプタに接続します。
3. ケーブルのもう片端を RJ-45 イーサネット ネットワーク ポートに接続します。

注 : ケーブルの両端が正しく接続されると、アダプタのポート LED が動作します。ネットワーク リンクおよびアクティビティの状態の通知については、ページ 66 ページの表 14 :「10/100/1000BASE-T ケーブルの仕様」を参照してください。

セクション 7: ドライバ ディスクを作成する

ドライバ ディスクを作成する手順については、システムに付属の文書類を参照してください。

セクション 8:Broadcom Boot Agent ドライバ ソフトウェア

概要

Broadcom NetXtreme Gigabit Ethernet アダプタは、PXE (Preboot Execution Environment)、RPL (Remote Program Load)、iSCSI ブート、および BootP (Bootstrap Protocol) をサポートしています。MBA (Multi-Boot Agent) はソフトウェア モジュールで、これを利用するとリモート システムからのイメージでネットワーク全体のシステムを起動することができます。Broadcom MBA ドライバは PXE 2.1 仕様で構成されており、モノリシック イメージと分割バイナリ イメージの両方でリリースされます。このため、マザーボードのビルトイン ベースコードの有無に係わらず、異なる環境にあるユーザーにも柔軟に対応できます。

MBA モジュールはクライアント / システム環境で動作します。ネットワークは 1 つまたは複数のブート システムで構成され、ネットワーク全体の複数のシステムにブート イメージを提供します。Broadcom への MBA モジュールの実装は、以下の環境での動作テストが完了しています。

- **Linux® Red Hat® PXE サーバー**：Broadcom の PXE クライアントは、リモート ブート、ネットワーク リソースの使用 (NFS マウントなど)、Linux のインストールが可能です。リモート ブートの場合、Linux ユニバーサル ドライバは Broadcom Universal Network Driver Interface (UNDI) をシームレスにバインドするため、Linux リモート ブート式のクライアント環境でネットワーク インターフェイスが利用できるようになります。
- **Intel® APITEST**：Broadcom PXE ドライバは、すべての API 準拠テスト スイートをパスしています。
- **Windows Deployment Service (WS)**：Windows Server の場合、RIS は WDS で置き換えられました。WDS は Windows Server 2008 を含む Windows オペレーティング システムをインストールするために、Broadcom PXE クライアントを提供します。

クライアント環境で MBA をセットアップする

アドイン NIC の場合、次の手順に従います。LOM の場合は、お使いのコンピュータのシステムガイドを参照してください。

クライアント環境で MBA をセットアップするには、以下の手順に従います。

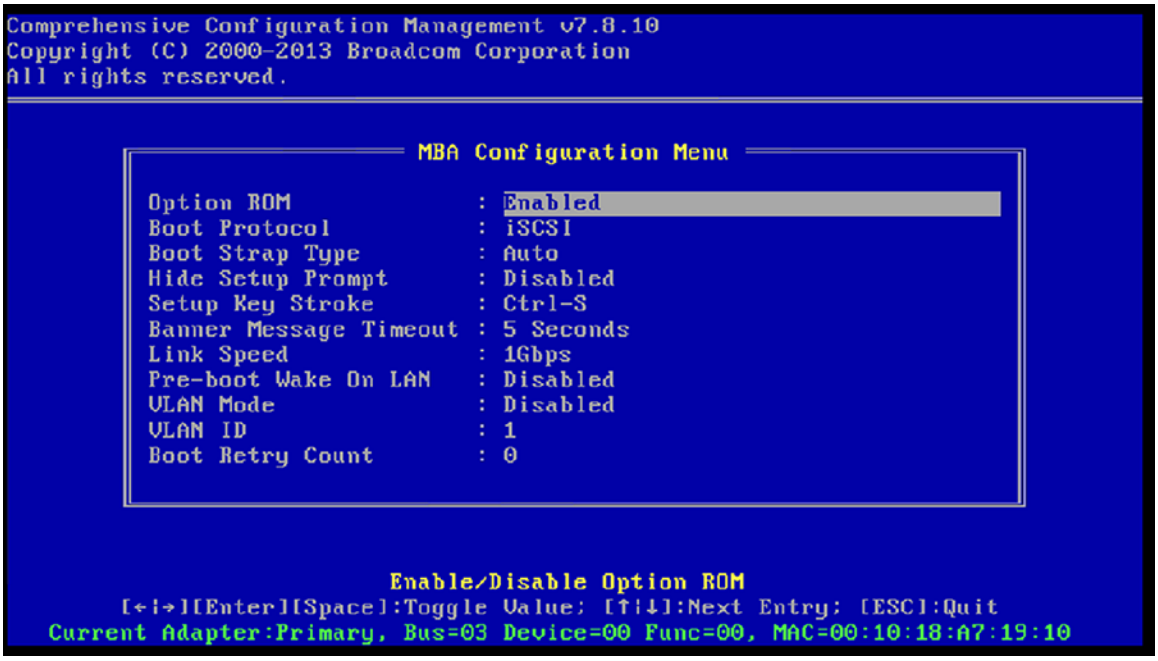
1. MBA ドライバを設定します。
2. BIOS をブート順にセットアップします。

MBA ドライバを設定する

このセクションは、Broadcom ネットワーク アダプタのアドイン NIC モデルで MBA ドライバを設定する方法を説明します。Broadcom ネットワーク アダプタの LOM モデルで MBA ドライバを設定する方法については、システムの文書類を確認してください。

CCM を使用する

1. システムを再起動します。
2. 応答を促すプロンプトが表示されたら、4 秒以内に **CTRL + S** キーを押します。アダプタのリストが表示されます。
   a. 設定するアダプタを選択し、**Enter** キーを押します。[Main/ メイン] メニューが表示されます。
   b. **[MBA Configuration/MBA 設定]** を選択します。[MBA Configuration/MBA 設定] メニューが表示されます。



3. 上向きの矢印キーまたは下向きの矢印キーを使用して、[Boot Protocol] メニュー項目に移動します。PXE (Preboot Execution Environment) 以外のブート プロトコルも利用できる場合は、右向きの矢印キーまたは左向きの矢印キーを使用して選択します。PXE 以外のブート プロトコルは、RPL (Remote Program Load) および BOOTP (Bootstrap Protocol) が利用できる場合があります。

注：特定の iSCSI ブート対応 LOM の場合、ブート プロトコルは BIOS によって設定されます。詳細については、システムの文書類を参照してください。

注：システム内に複数のアダプタがあり、設定しているアダプタがどれか分からない場合は、**CTRL + F6** キーを押すと、アダプタのポート LED が点滅し始めます。

4. 上向きの矢印キー、下向きの矢印キー、および右向きの矢印キーを使用して、必要に応じて他のメニュー項目の値に移動し、変更します。
5. **F4** キーを押して設定を保存します。
6. 終了したら、**ESC** キーを押します。

uEFI を使用する

1. システムを再起動します。
2. [System Setup/ システムセットアップ] または [Device Setting/ デバイス設定] 設定メニューに移動します。
3. MBA 設定を変更するデバイスを選択します。
4. **[MBA Configuration MenuMBA コンフィギュレーション メニュー]** を選択します。
5. Preboot Execution Environment (PXE) 以外のブート プロトコルが利用可能な場合、ドロップダウン メニューを使用して目的のブート プロトコルを選択します。他のブート プロトコルとして、iSCSI および BOOTP (Bootstrap Protocol) が利用できる場合があります。

注：iSCSI ブート対応 LOM の場合、ブート プロトコルは BIOS によって設定されます。詳細については、システムの文書類を参照してください。

6. 上向きの矢印キー、下向きの矢印キー、および右向きの矢印キーを使用して、必要に応じて他のメニュー項目の値に移動し、変更します。
7. **[Back/ 戻る]** を選択して [Main/ メイン] メニューに戻ります。
8. **[Finish/ 完了]** を選択し、保存して終了します。

BIOS をセットアップする

ネットワークから MBA でブートするときは、まず BIOS で MBA がイネーブルされているアダプタをブート可能デバイスにしてください。この手順はシステムの BIOS 実装により異なります。手順に関しては、お使いのシステムのユーザー マニュアルをご覧ください。

セクション 9:iSCSI プロトコル

iSCSI ブート

Broadcom NetXtreme Gigabit Ethernet アダプタは、ディスクレス システムでのオペレーティング システムのネットワーク ブートを可能にするために、iSCSI ブートをサポートします。iSCSI ブートにより、リモートの iSCSI ターゲット マシンから標準 IP ネットワークを介して Windows または Linux オペレーティング システムをブートできます。

Windows および Linux オペレーティング システムでは、iSCSI ブートは表 15 に示す全般パラメタを使用してブートするように設定できます。

iSCSI ブート向けにサポートされているオペレーティング システム

Broadcom NetXtreme Gigabit Ethernet アダプタは、次のオペレーティング システムで iSCSI ブートをサポートします。

- Windows Server オペレーティング システム
- Enterprise Linux ディストリビューション

iSCSI ブート セットアップ

iSCSI ブート セットアップは、次の作業から構成されます。

EBDA のメモリ制約条件のためローカルのストレージ（特に RAID）が存在している場合は、BIOS モード では iSCSI ブートがサポートされません。

- iSCSI ターゲットを設定する
- iSCSI ブート パラメタを設定する
- iSCSI ブート イメージを準備する
- ブート

iSCSI ターゲットを設定する

iSCSI ターゲットの設定は、ターゲットのベンダによって異なります。iSCSI ターゲットの設定については、ベンダが提供している文書類を参照してください。一般的な手順は次のとおりです。

1. iSCSI ターゲットを作成します。
2. 仮想ディスクを作成します。
3. ステップ 1 で作成した iSCSI ターゲットに仮想ディスクをマッピングします。
4. iSCSI イニシエータを iSCSI ターゲットに関連付けます。

5. iSCSI ターゲット名、TCP ポート番号、iSCSI 論理ユニット番号 (LUN)、イニシエータのインターネット修飾名 (IQN)、および CHAP 認証の詳細を記録します。
6. iSCSI ターゲットを設定した後で、次の情報を入手します。
   - ターゲット IQN 名
   - ターゲット IP アドレス
   - ターゲット TCP ポート番号
   - ターゲット LUN
   - イニシエータ IQN
   - CHAP ID および秘密情報

iSCSI ブート パラメタを設定する

Broadcom iSCSI ブート ソフトウェアは、静的コンフィギュレーションまたは動的コンフィギュレーション用に設定します。[General Parameters] 画面で使用できる設定オプションについては、表 15 を参照してください。

表 15 には、IPv4 と IPv6 の両方のパラメタがリストされます。IPv4 または IPv6 に固有なパラメタには注記が付いています。

注：IPv6 iSCSI ブートが使用できるかどうかは、プラットフォームとデバイスに依存します。

表 15: 構成オプション

オプション	*説明*
DHCP 経由の TCP/IP パラメタ	これは、IPv4 に固有なオプションです。iSCSI ブート ホスト ソフトウェアが DHCP を使用して IP アドレス情報を取得する (Enabled/ 有効) か、または静的 IP コンフィギュレーションを使用する (Disabled/ 無効) かを制御します。
[IP Autoconfiguration]	これは、IPv6 に固有なオプションです。DHCPv6 が存在しており、使用されている場合 (イネーブルになっている場合) に、iSCSI ブート ホスト ソフトウェアによって、ステートレスのリンク ローカル アドレスやステートフルのアドレスを設定するかどうかを制御します。Router Solicit パケットの送信は、4 秒間隔で 3 回まで試行されます。あるいは静的 IP 設定 (ディスエーブル) を使用します。
DHCP 経由の iSCSI パラメタ	iSCSI ブート ホスト ソフトウェアが iSCSI ターゲット パラメタを取得するために DHCP を使用してする (Enabled/ 有効) か、または静的コンフィギュレーションを通じて取得する (Disabled/ 無効) かを制御します。静的情報は、[iSCSI Initiator Parameters Configuration] 画面で入力します。
CHAP 認証	iSCSI ブート ホスト ソフトウェアが iSCSI ターゲットへの接続時に CHAP 認証を使用するかどうかを制御します。[CHAP Authentication] が有効な場合は、[iSCSI Initiator Parameters Configuration] 画面で [CHAP ID] と [CHAP Secret] に入力します。
DHCP ベンダ ID	DHCP 中に使用されるベンダ クラス ID フィールドを iSCSI ブート ホスト ソフトウェアがどのように解釈するかを制御します。DHCP Offer パケット内のベンダ クラス ID フィールドがこのフィールドの値と一致する場合、iSCSI ブート ホスト ソフトウェアは、DHCP オプション 43 のフィールドを参照して、必要な iSCSI ブート拡張機能を確認します。DHCP が無効な場合、この値を設定する必要はありません。

表 15: 構成オプション (続き)

オプション	*説明*
リンク アップ遅延時間	イーサネット リンクが確立された後、ネットワーク上にデータを送信する前に、iSCSI ブート ホスト ソフトウェアが待機する時間を秒単位で制御します。有効な値は 0 ～ 255 です。たとえば、スパニング ツリーなどのネットワーク プロトコルがクライアント システムへのスイッチ インターフェイスで有効になっている場合に、ユーザーはこのオプションの値を設定する必要があります。
TCP タイムスタンプを使用する	TCP タイムスタンプ オプションが有効か無効かを制御します。
第一 HDD としてターゲット	iSCSI ターゲット ドライブがシステムの最初のハード ドライブとして表示されることを指定できます。
LUN ビジー再試行回数	iSCSI ターゲット LUN がビジーな場合に、iSCSI ブート イニシエータが接続を再試行する回数を制御します。
IP バージョン	このオプションは、IPv6 に固有なオプションです。IPv4 または IPv6 プロトコルを切り替えます。プロトコルが切り替えられると、すべての IP 設定が失われます。

MBA ブート プロトコル設定

ブート プロトコルを設定するには :

1. システムを再起動します。
2. PXE バナーで、**CTRL + S** キーを押します。[MBA Configuration Menu] が表示されます (Broadcom Boot Agent を参照してください)。
3. [MBA Configuration Menu] で、**上向きの矢印キー**または**下向きの矢印キー**を使用して **[Boot Protocol]** オプションに移動します。**左向きの矢印キー**または**右向きの矢印キー**を使用して、**[Boot Protocol]** オプションを **iSCSI** に変更します。

注 : BIOS によってブート プロトコルが設定されるプラットフォームの場合、詳細についてはシステムの文書類を参照してください。

4. **[Main/ メイン] メニュー**で、**[iSCSI Boot Configuration/iSCSI ブート コンフィギュレーション]** を選択します。

注 : iSCSI ブート ファームウェアが NetXtreme ネットワーク アダプタにプログラムされていない場合は、**[iSCSI Boot Configuration/iSCSI ブート コンフィギュレーション]** を選択しても何も起こりません。

iSCSI ブート コンフィギュレーション

- 静的 iSCSI ブート コンフィギュレーション
- 動的 iSCSI ブート コンフィギュレーション

静的 iSCSI ブート コンフィギュレーション

静的コンフィギュレーションでは、iSCSI ターゲットを設定するで取得したシステムの IP アドレス、システムのイニシエータ IQN、およびターゲット パラメタのデータを入力する必要があります。設定オプションについては、表 15 を参照してください。

静的コンフィギュレーションを使用して iSCSI ブート パラメタを設定するには :

1. **[General Parameters Menu]** 画面で、次のパラメタを設定します。
   - **TCP/IP parameters via DHCP** : Disabled (IPv4 の場合)
   - **IP Autoconfiguration** : Disabled (IPv6 の場合)

- **iSCSI parameters via DHCP**：Disabled
- **CHAP Authentication**：Disabled
- **Boot to iSCSI target**：Disabled
- **DHCP Vendor ID**：BRCM ISAN
- **Link Up Delay Time**：0
- **Use TCP Timestamp**：Enabled (Dell/EMC AX100i などの一部のターゲットでは、**[Use TCP Timestamp]** を有効にする必要があります)
- **Target as First HDD**：Disabled
- **LUN Busy Retry Count**：0
- **IP Version**：IPv6 (IPv6 の場合)

2. **ESC** キーを押して **[Main]** メニューに戻ります。
3. **[Main]** メニューで、**[Initiator Parameters]** を選択します。
4. **[Initiator Parameters]** 画面で、次の項目の値を入力します。
   - IP アドレス (未指定の IPv4 および IPv6 アドレスは、それぞれ「0.0.0.0」、「::」となります **)**
   - サブネット マスク プリフィックス
   - デフォルト ゲートウェイ
   - プライマリ DNS
   - セカンダリ DNS
   - iSCSI 名 (クライアント システムで使用される iSCSI イニシエータ名に対応します)

注：よく確認したうえで IP アドレスを入力します。IP アドレスに関しては、重複や不適切なセグメント / ネットワーク割り当てを検出するためのエラーチェックは実行されません。

5. **ESC** キーを押して **[Main]** メニューに戻ります。
6. **[Main]** メニューで、**[1st Target Parameters]** を選択します。
7. **[1st Target Parameters]** 画面で、**[Connect]** を有効にして iSCSI ターゲットに接続します。iSCSI ターゲットの設定時に使用される値を使用して、次の項目の値を入力します。
   - IP アドレス
   - TCP ポート
   - ブート LUN
   - iSCSI 名
8. **ESC** キーを押して **[Main]** メニューに戻ります。
9. **ESC** キーを押して、**[Exit and Save Configuration]** を選択します。
10. **F4** キーを押して MBA 設定を保存します。

動的 iSCSI ブート コンフィギュレーション

動的コンフィギュレーションでは、システムの IP アドレスとターゲット / イニシエータ情報が DHCP サーバーによって提供されることを指定することのみが必要です (iSCSI ブートをサポートするための DHCP サーバーを設定する に記載されている IPv4 および IPv6 設定の説明を参照してください)。IPv4 の場合、イニシエータ iSCSI 名を除き、[Initiator Parameters/ イニシエータ パラメタ]、[1st Target Parameters/1 番目のターゲット パラメタ]、または [2nd Target Parameters/2 番目のターゲット パラメタ] の各画面の設定は無視されるため、クリアする必要はありません。IPv6 の場合、CHAP ID と秘密情報を除き、[Initiator Parameters]、[1st Target Parameters]、または [2nd Target Parameters] の各画面の設定は無視されるため、クリアする必要はありません。設定オプションについては、表 15 を参照してください。

メモ：

- DHCP サーバーを使用する場合、DNS サーバーのエントリが、DHCP サーバーによって提供される値で上書きされます。この状況は、ローカルに提供された値が有効であり、DHCP サーバーが DNS サーバー情報を提供しない場合に発生します。DHCP サーバーが DNS サーバー情報を提供しない場合は、プライマリとセカンダリの両方の DNS サーバー値が 0.0.0.0 に設定されます。Windows OS が引き継ぐ場合、Microsoft iSCSI イニシエータは iSCSI Initiator パラメタを取得し、適切なレジストリを静的に設定します。これにより、設定済みの値がすべて上書きされます。DHCP デーモンは Windows 環境でユーザー プロセスとして実行されるため、iSCSI Boot 環境でスタックが起動する前に、すべての TCP/IP パラメタを静的に設定する必要があります。
- DHCP オプション 17 が使用されている場合、ターゲット情報は DHCP サーバーによって提供され、イニシエータ iSCSI 名は [Initiator Parameters] 画面でプログラムされた値から取得されます。値が選択されていない場合、コントローラはデフォルトで次の名前を使用します。

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

文字列 11.22.33.44.55.66 は、コントローラの MAC アドレスに対応します。

DHCP オプション 43 (IPv4 のみ) が使用されている場合、[Initiator Parameters]、[1st Target Parameters]、または [2nd Target Parameters] の各画面の設定は無視されるため、クリアする必要はありません。

動的コンフィギュレーションを使用して iSCSI ブート パラメタを設定するには：

1. **[General Parameters Menu]** 画面で、次のパラメタを設定します。
   - **TCP/IP parameters via DHCP**：Enabled (IPv4 の場合)
   - **IP Autoconfiguration**：Enabled (IPv6 の場合)
   - **iSCSI parameters via DHCP**：Enabled
   - **CHAP Authentication**：Disabled
   - **Boot to iSCSI target**：Disabled
   - **DHCP Vendor ID：**BRCM ISAN
   - **Link Up Delay Time**：0
   - **Use TCP Timestamp**：Enabled (Dell/EMC AX100i などの一部のターゲットでは、**[Use TCP Timestamp]** を有効にする必要があります)
   - **Target as First HDD**：Disabled
   - **LUN Busy Retry Count**：0
   - **IP Version**：IPv6 (IPv6 の場合)
2. **ESC** キーを押して **[Main]** メニューに戻ります。

注：[Initiator Parameters/ イニシエータ パラメタ] および **[1st Target Parameters/1 番目のターゲット パラメタ]** 画面の情報は無視されるため、クリアする必要はありません。

3. **[Exit and Save Configuration]** を選択します。

CHAP 認証を有効化する

ターゲットで CHAP 認証が有効になっていることを確認します。

CHAP 認証の有効化

1. **[General Parameters]** 画面で、**[CHAP Authentication]** を [Enabled] に設定します。
2. **[Initiator Parameters]** 画面で、次の項目の値を入力します。
   - CHAP ID (最大 128 バイト)
   - CHAP 秘密情報 (認証が必要な場合。長さは 12 文字以上にする必要があります)
3. **ESC** キーを押して **[Main]** メニューに戻ります。
4. **[Main]** メニューで、**[1st Target Parameters]** を選択します。
5. **[1st Target Parameters]** 画面で、iSCSI ターゲットの設定時に使用される値を使用して、次の項目の値を入力します。
   - CHAP ID (双方向 CHAP の場合は任意)
   - CHAP 秘密情報 (双方向 CHAP の場合は任意。長さは 12 文字以上にする必要があります)
6. **ESC** キーを押して **[Main]** メニューに戻ります。
7. **ESC** キーを押して、**[Exit and Save Configuration]** を選択します。

iSCSI ブートをサポートするための DHCP サーバーを設定する

DHCP サーバーはオプションのコンポーネントであり、動的 iSCSI ブート コンフィギュレーション セットアップを実行する場合にのみ必要です (動的 iSCSI ブート コンフィギュレーションを参照してください)。

iSCSI ブートをサポートするように DHCP サーバーを設定する方法は、IPv4 と IPv6 で異なります。

- IPv4 の DHCP iSCSI ブート設定
- IPv6 の DHCP iSCSI ブート設定

IPv4 の DHCP iSCSI ブート設定

DHCP プロトコルには、DHCP クライアントに設定情報を提供するいくつかのオプションがあります。iSCSI ブートの場合、Broadcom アダプタは、次の DHCP コンフィギュレーションをサポートします。

- DHCP オプション 17、ルート パス
- DHCP オプション 43、ベンダ固有情報

DHCP オプション 17、ルート パス

オプション 17 は、iSCSI ターゲット情報を iSCSI クライアントに渡すために使用されます。

IETC RFC 4173 で定義されているルート パスの形式は、次のとおりです。

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

以下に、パラメタを定義します。

表 16:DHCP オプション 17 パラメタの定義

パラメタ	*定義*
"iscsi:"	リテラル文字列
<servername>	iSCSI ターゲットの IP アドレスまたは FQDN
":"	セパレータ
<protocol>	iSCSI ターゲットへのアクセスに使用される IP プロトコル。現在は TCP のみサポートされているため、プロトコルは 6 です。
<port>	プロトコルに関連付けられているポート番号。iSCSI の標準ポート番号は 3260 です。
<LUN>	iSCSI ターゲットで使用する論理ユニット番号。LUN の値は、16 進形式で表示する必要があります。ID OF 64 の LUN は、DHCP サーバーのオプション 17 のパラメタ内に 40 として設定する必要があります。
<targetname>	IQN または EUI 形式でのターゲット名 (IQN 形式と EUI 形式の詳細については、RFC 3720 を参照してください)。IQN 名は、例えば「iqn.1995-05.com.broadcom:iscsi-target」のようになります。

DHCP オプション 43、ベンダ固有情報

DHCP オプション 43 (ベンダ固有情報) は、DHCP オプション 17 より多くの設定オプションを iSCSI クライアントに提供します。この設定では、ブートに使用できる 2 つの iSCSI ターゲット IQN と共に、イニシエータ IQN を iSCSI ブートクライアントに割り当てる 3 つの追加サブオプションが提供されます。iSCSI ターゲット IQN の形式は DHCP オプション 17 と同じですが、iSCSI イニシエータ IQN は単なるイニシエータの IQN です。

注：DHCP オプション 43 は IPv4 でのみサポートされています。

以下に、サブオプションを一覧します。

表 17:DHCP オプション 43 のサブオプションの定義

サブオプション	*定義*
201	標準ルート パス形式での最初の iSCSI ターゲットの情報 "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
202	標準ルート パス形式での 2 番目の iSCSI ターゲットの情報 "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
203	iSCSI イニシエータ IQN

DHCP オプション 43 を使用するには、DHCP オプション 17 よりも多くの設定が必要ですが、より豊富な機能を備えた環境が提供され、より多くの設定オプションが提供されます。Broadcom では、動的 iSCSI ブート コンフィギュレーションを実行する場合には DHCP オプション 43 を使用することをお勧めします。

DHCP サーバーを設定する

オプション 17 またはオプション 43 をサポートするように DHCP サーバーを設定します。

注: オプション 43 を使用する場合は、オプション 60 も設定する必要があります。オプション 60 の値は、**DHCP ベンダ ID** 値と一致している必要があります。[iSCSI Boot Configuration] メニューの **[General Parameters]** に示されるように、**DHCP ベンダ ID** 値は BRCM ISAN です。

IPv6 の DHCP iSCSI ブート設定

ステートレスまたはステートフルの IP 設定や、DHCPv6 クライアントの情報など、DHCPv6 サーバーは多くのオプションを提供できます。iSCSI ブートの場合、Broadcom アダプタは、次の DHCP コンフィギュレーションをサポートします。

- DHCPv6 オプション 16、ベンダ クラス オプション
- DHCPv6 オプション 17、ベンダ固有情報

注：DHCPv6 の標準ルート パス オプションはまだ使用できません。動的 iSCSI ブートの IPv6 サポートのために、オプション 16 またはオプション 17 を使用することをお勧めします。

DHCPv6 オプション 16、ベンダ クラス オプション

DHCPv6 オプション 16 (ベンダ クラス オプション) は指定が必須であり、設定された **DHCP ベンダ ID** パラメタと一致する文字列を指定する必要があります。[iSCSI Boot Configuration] メニューの **[General Parameters]** に示されるように、**DHCP ベンダ ID** 値は BRCM ISAN です。

オプション 16 の内容は、<2 バイト長 > <DHCP ベンダ ID> の形式にする必要があります。

DHCPv6 オプション 17、ベンダ固有情報

DHCPv6 オプション 17 (ベンダ固有情報) は、より多くの設定オプションを iSCSI クライアントに提供します。この設定では、ブートに使用できる 2 つの iSCSI ターゲット IQN と共に、イニシエータ IQN を iSCSI ブート クライアントに割り当てる 3 つの追加サブオプションが提供されます。

以下に、サブオプションを一覧します。

表 18:DHCP オプション 17 のサブオプションの定義

サブオプション	*定義*
201	標準ルート パス形式での最初の iSCSI ターゲットの情報 `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	標準ルート パス形式での 2 番目の iSCSI ターゲットの情報 `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	iSCSI イニシエータ IQN

注：表 18 では、IPv6 アドレスの指定に括弧 [ ] が必要です。

オプション 17 の内容は、<2 バイト オプション番号 201|202|203> <2 バイト長 > < データ > の形式にする必要があります。

DHCP サーバーを設定する

オプション 16 およびオプション 17 をサポートするように DHCP サーバーを設定します。

注：DHCPv6 オプション 16 およびオプション 17 の形式は、RFC 3315 で完全に定義されています。

iSCSI ブート イメージを準備する

Windows Server 2008 R2 および SP2 の iSCSI ブート セットアップ

Windows Server 2008 R2 および Windows Server 2008 SP2 は iSCSI ブートをサポートします。次の手順では Windows Server 2008 R2 を取り上げていますが、手順は Windows Server 2008 R2 と SP2 で共通です。

必須の CD/ISO イメージ：

- Broadcom ドライバがインジェクトされた Windows Server 2008 R2 x64。Windows イメージ ファイルに Broadcom ドライバをインジェクト (スリップストリーム) するを参照してください。また、support.microsoft.com で Microsoft のサポート技術情報文書 KB974072 を参照してください。

メモ：

- Microsoft の手順では、NDIS のドライバのみをインジェクトします。すべてのドライバ (VBD、BXND、OIS、および NetXtreme I NDIS) をインジェクトすることをお勧めします。
- 個々の Windows NetXtreme ドライバを抽出する手順については、特定のドライバ インストーラ アプリケーションの *silent.txt* ファイルを参照してください。

必要なその他のソフトウェア：

- Bindview.exe (Windows Server 2008 R2 のみ。KB976042 を参照)

手順：

1. ブートしようとするシステム (「リモート システム」) からすべてのローカル ハード ドライブを取り外します。
2. 最新の Broadcom MBA と iSCSI ブート イメージをアダプタの NVRAM にロードします。
3. Broadcom MBA が最初のブート可能デバイス、CDROM が 2 番目のデバイスになるように、リモート システムの BIOS を設定します。
4. リモート デバイスからの接続を許可するように iSCSI ターゲットを設定します。ターゲットに、新しい OS のインストールを保持するための十分なディスク容量があることを確認します。
5. リモート システムを起動します。Preboot Execution Environment (PXE) バナーが表示されたときに、**Ctrl+S** キーを押し、PXE メニューを終了します。
6. [PXE] メニューで、**[Boot Protocol]** を **[iSCSI]** に設定します。
7. iSCSI ターゲット パラメタを入力します。
8. [General Parameters] で、**[Boot to Target]** パラメタを **[One Time Disabled/ ワンタイム ディスエーブル]** に設定します。
9. 設定を保存して、システムを再起動します。

   リモート システムは iSCSI ターゲットに接続し、DVDROM デバイスからブートします。
10. DVD へのブートを実行して、インストールを開始します。
11. インストールに関するすべての質問に対して、適切に答えます (インストールする OS を指定し、使用許諾契約の条項に同意するなど)。

    [Windows のインストール場所を選択してください。] ウィンドウが表示され、ターゲット ドライブが確認できます。これは、iSCSI ブート プロトコル経由で接続されているドライブで、リモート iSCSI ターゲットにあります。

12. **[次へ]** を選択して、Windows Server 2008 R2 のインストールに進みます。

    Windows 2008 Server R2 DVD によるインストール プロセスが開始されてから数分後に、システムが再起動されます。再起動後に Windows Server 2008 R2 インストール ルーチンが再開され、インストールが完了します。

13. もう一度システムが再起動した後、リモート システムが起動されデスクトップが正常に表示されることを確認します。

14. Windows Server 2008 R2 が起動したら、すべてのドライバをロードし、Bindview を実行します。
    a. **[All Services/ すべてのサービス]** を選択します。
    b. **[WFP Lightweight Filter/WFP ライトウェイト フィルタ]** に、AUT の **[Binding paths/ 結合パス]** が表示されるはずです。右クリックしてディセーブルにします。作業完了後に、アプリケーションを終了します。

15. OS とシステムが機能していること、およびリモート システムの IP を ping することでトラフィックを送受信できることを確認します。

Windows 2012 iSCSI ブート セットアップ

Windows Server 2012 は、iSCSI ブートとインストールをサポートしています。最新の Broadcom ドライバをインジェクトした「slipstream」(スリップストリーム) DVD を使用する必要があります。Windows イメージ ファイルに Broadcom ドライバをインジェクト (スリップストリーム) するを参照してください。また、support.microsoft.com で Microsoft のサポート技術情報文書 KB974072 を参照してください。

注 : Microsoft の手順では、NDIS のドライバのみをインジェクトします。すべてのドライバ (VBD、BXND、OIS、および NetXtreme I NDIS) をインジェクトすることをお勧めします。

次の手順で、インストール用のイメージとブートの準備をします。

1. ブートしようとするシステム (「リモート システム」) からすべてのローカル ハード ドライブを取り外します。
2. 最新の Broadcom MBA と iSCSI ブート イメージをアダプタの NVRAM にロードします。
3. Broadcom MBA が最初のブート可能デバイス、CDROM が 2 番目のデバイスになるように、リモート システムの BIOS を設定します。
4. リモート デバイスからの接続を許可するように iSCSI ターゲットを設定します。ターゲットに、新しい OS のインストールを保持するための十分なディスク容量があることを確認します。
5. リモート システムを起動します。Preboot Execution Environment (PXE) バナーが表示されたときに、**Ctrl+S** キーを押し、PXE メニューを終了します。
6. [PXE] メニューで、**[Boot Protocol]** を **[iSCSI]** に設定します。
7. iSCSI ターゲット パラメタを入力します。
8. [General Parameters] で、**[Boot to Target]** パラメタを **[One Time Disabled/ ワンタイム ディスエーブル]** に設定します。
9. 設定を保存して、システムを再起動します。

   リモート システムは iSCSI ターゲットに接続し、DVDROM デバイスからブートします。

10. DVD からのブートを実行して、インストールを開始します。
11. インストールに関するすべての質問に対して、適切に答えます (インストールする OS を指定し、使用許諾契約の条項に同意するなど)。

    [Windows のインストール場所を選択してください。] ウィンドウが表示され、ターゲット ドライブが確認できます。これは、iSCSI ブート プロトコル経由で接続されているドライブで、リモート iSCSI ターゲットにあります。

12. **[次へ]** を選択し、Windows 2012 のインストールに進みます。

    Windows 2012 DVD によるインストール プロセスが開始されてから数分後に、システムが再起動されます。再起動後に Windows 2012 インストール ルーチンが再開され、インストールが完了します。

13. もう一度システムが再起動した後、リモート システムが起動されデスクトップが正常に表示されることを確認します。

14. Windows 2012 の OS ブートが完了した後、ドライバのインストーラを実行し、Broadcom のドライバーとアプリケーションのインストールを完了することをお勧めします。

Linux iSCSI ブート セットアップ

Linux iSCSI ブートは、Red Hat Enterprise Linux 5.5 以降および SUSE Linux Enterprise Server 11 SP1 以降でサポートされます。SLES 10.x と SLES 11 は、非オフロード パスだけをサポートしています。

1. ドライバを更新する場合、最新の Broadcom Linux ドライバ CD を入手してください。
2. ネットワーク アダプタ上のターゲット オプションからのブートをディセーブルにすることにより、iSCSI ブート パラメタをターゲットへの DVD 直接インストール用に設定します。
3. 次のようにブートの順序を変更します :
   a. ネットワーク アダプタからのブート。
   b. CD/DVD ドライバからのブート。
4. システムを再起動します。
5. システムが iSCSI ターゲットに接続し、CD/DVD ドライブからブートします。
6. 対応する OS の指示に従います。
   a. RHEL 5.5 - [boot:] プロンプトで「linux dd」と入力し、ENTER キーを押します。
   b. SuSE 11.X — **[インストール]** を選択し、ブート オプションで「 **withiscsi=1 netsetup=1**」と入力します。ドライバ更新をする場合、F6 ドライバ オプションで **[はい]** を選択します。
7. ドライバ更新をする場合、指示に従って、ドライバ CD をロードします。それ以外の場合は、この手順を省略します。
8. [networking device] プロンプトで、目的のネットワーク アダプタ ポートを選択し、**[OK]** を押します。
9. [configure TCP/IP] プロンプトで、システムが IP アドレスを取得する方法を設定し、**[OK]** を押します。
10. [static IP] を選択した場合、iscsi イニシエータの IP 情報を入力する必要があります。
11. (RHEL) メディア テストの [省略] を選択します。
12. 必要に応じてインストールを続行します。この時点で、ドライブが利用可能になります。ファイルのコピーが完了したら、CD/DVD を取り出して、システムを再起動します。
13. システムが再起動したら、iSCSI ブート パラメタの [ターゲットから起動] をイネーブルにして、インストールを完了するまで続行します。

この段階で、初期インストール フェーズは終了です。残りの手順は、新しいコンポーネント更新用に新しくカスタマイズする initrd の作成に関連するものです。

14. 必要に応じて iscsi イニシエータを更新します。最初に **rpm -e** を使って、既存のイニシエータを削除する必要があります。
15. ネットワーク サービスのすべての実行レベルがオンになっていることを確認します。
    `chkconfig network on`
16. iscsi サービスの 2、3、および 5 の実行レベルがオンになっていることを確認します。
    `chkconfig -level 235 iscsi on`
17. Red Hat 6.0 の場合、Network Manager サービスが停止していて、ディセーブルになっていることを確認します。
18. 必要に応じて iscsiuio をインストールします (SuSE 10 では不要)。
19. 必要に応じて、linux-nx2 パッケージをインストールします。
20. bibt パッケージをインストールします。
21. ifcfg-eth* を削除します。
22. 再起動します。
23. SUSE 11.1 の場合、次に示す、リモート DVD のインストール ワークアラウンドに従います。

24. システムの再起動後、ログインして /opt/bcm/bibt フォルダに変更し、iscsi_setup.sh スクリプトを実行して initrd イメージを作成します。

25. initrd イメージ を /boot フォルダにコピーします。

26. grub メニューを変更して新しい initrd イメージをポイントするようにします。

27. CHAP をイネーブルにするには、iscsid.conf を変更する必要があります (Red Hat のみ)。

28. 再起動し、必要に応じて CHAP パラメタを変更します。

29. iSCSI ブート イメージへのブートを続行し、作成したイメージの 1 つ を選択します。

30. IPv6 の場合、NVRAM 設定で、イニシエータとターゲットの両方 の IP アドレスを目的の IPv6 アドレスに変更します。

SUSE 11.1 のリモート DVD インストールのワークアラウンド

1. 次の内容の boot.open-iscsi という新しいファイルを作成します。

2. 作成したファイルを /etc/init.d/ フォルダにコピーして、既存のファイルを上書きします。

新しい boot.open-iscsi ファイルの内容 :

```
#!/bin/bash
#
# /etc/init.d/iscsi
#
### BEGIN INIT INFO
# Provides:          iscsiboot
# Required-Start:
# Should-Start:      boot.multipath
# Required-Stop:
# Should-Stop:       $null
# Default-Start:     B
# Default-Stop:
# Short-Description: iSCSI initiator daemon root-fs support
# Description:       Starts the iSCSI initiator daemon if the
#                    root-filesystem is on an iSCSI device
#
### END INIT INFO

ISCSIADM=/sbin/iscsiadm
ISCSIUIO=/sbin/iscsiuio
CONFIG_FILE=/etc/iscsid.conf
DAEMON=/sbin/iscsid
ARGS="-c $CONFIG_FILE"

# Source LSB init functions
. /etc/rc.status

#
# This service is run right after booting. So all targets activated
# during mkinitrd run should not be removed when the open-iscsi
# service is stopped.
#
iscsi_load_iscsiuio()
{
    TRANSPORT=`$ISCSIADM -m session 2> /dev/null | grep "bnx2i"`
    if [ "$TRANSPORT" ] ; then
    echo -n "Launch iscsiuio "
        startproc $ISCSIUIO
```

```
    fi
}

iscsi_mark_root_nodes()
{
    $ISCSIADM -m session 2> /dev/null | while read t num i target ; do
    ip=${i%%:*}
    STARTUP=`$ISCSIADM -m node -p $ip -T $target 2> /dev/null | grep "node.conn\[0\].startup" | cut
-d' ' -f3`
    if [ "$STARTUP" -a "$STARTUP" != "onboot" ] ; then
        $ISCSIADM -m node -p $ip -T $target -o update -n node.conn[0].startup -v onboot
    fi
    done
}
# Reset status of this service
rc_reset

# We only need to start this for root on iSCSI
if ! grep -q iscsi_tcp /proc/modules ; then
    if ! grep -q bnx2i /proc/modules ; then
        rc_failed 6
        rc_exit
    fi
fi

case "$1" in
    start)
    echo -n "Starting iSCSI initiator for the root device: "
    iscsi_load_iscsiuio
    startproc $DAEMON $ARGS
    rc_status -v
    iscsi_mark_root_nodes
    ;;
    stop|restart|reload)
    rc_failed 0
    ;;
    status)
    echo -n "Checking for iSCSI initiator service: "
    if checkproc $DAEMON ; then
        rc_status -v
    else
        rc_failed 3
        rc_status -v
    fi
    ;;
    *)
    echo "Usage: $0 {start|stop|status|restart|reload}"
    exit 1
    ;;
esac
rc_exit
```

Windows イメージ ファイルに Broadcom ドライバをインジェクト (スリップストリーム) する

Windows イメージ ファイルに Broadcom ドライバをインジェクトするには、該当する Windows Server のバージョン (2008 R2、2008 SP2、2012、または 2012 R2) に適した正しい Broadcom ドライバ パッケージを取得する必要があります。パッケージには、b57nd60a という名前が付いています。

注: 個々の Windows NetXtreme ドライバを抽出する手順については、特定のドライバ インストーラ アプリケーションの *silent.txt* ファイルを参照してください。

次に、ドライバ パッケージを作動ディレクトリに配置します。たとえば、ドライバ パッケージを次のディレクトリにコピーします。

- C:\Temp\b57nd60a

最後に、これらのドライバを Windows イメージ (WIM) ファイルにインジェクトし、更新後のイメージから、該当する Windows Server のバージョンをインストールします。

詳細な手順は、以下で説明します。

注：この手順で使用するファイル名とフォルダ名は、例に過ぎません。スリップストリーム プロジェクトで、独自のファイル名とフォルダ名を指定できます。

1. Windows Server 2008 R2 および SP2 では、Windows 自動インストール キット (AIK) をインストールします。
   — または —
   Windows Server 2012 および 2012 R2 では、Windows Assessment and Deployment Kit (ADK) をインストールします。
2. 次のコマンドを使用して、一時ディレクトリを作成し、残りのすべての手順のカレント ディレクトリに設定します。
   ```
   md C:\Temp\x
   cd /d C:\Temp\x
   ```
3. 次のコマンドを使用して 2 つのサブディレクトリを作成します。
   ```
   md src
   md mnt
   ```
4. 次のコマンドを使用して元の DVD を src サブディレクトリにコピーします。
   ```
   xcopy N:\ .\src /e /c /i /f /h /k /y /q
   ```
   この例では、インストール DVD は N: ドライブである点に注意してください。
5. 管理者権限モードで Deployment and Imaging Tools コマンド プロンプトを開きます。次に、c:\Temp\x をカレント ディレクトリとして設定します。
   このコマンド プロンプト ウィンドウを、これ以降のすべての手順で使用します。
6. 次のコマンドを入力します。
   ```
   attrib -r .\src\sources\boot.wim
   attrib -r .\src\sources\install.wim
   ```
7. 次のコマンドを入力して boot.wim イメージをマウントします。
   ```
   dism /mount-wim /wimfile:.\src\sources\boot.wim /index:2 /mountdir:.\mnt
   ```
   インデックスの値として常に「2」を使用する必要があります。
8. 次のコマンドを入力して、現在マウントされているイメージに次のドライバを追加します。
   ```
   dism /image:.\mnt /add-driver /driver:C:\Temp\b57nd60a\b57nd60a.inf
   ```
9. 次のコマンドを入力して boot.wim イメージをマウント解除します。
   ```
   dism /unmount-wim /mountdir:.\mnt /commit
   ```
10. 次のコマンドを入力して、install.wim イメージ内にある目的の SKU のインデックスを確認します。
    ```
    dism /get-wiminfo /wimfile:.\src\sources\install.wim
    ```
    たとえば、Windows Server 2012 では、インデックス 2 は「Windows Server 2012 SERVERSTANDARD」と特定されます。

11. 次のコマンドを入力して install.wim イメージをマウントします。
    ```
    dism /mount-wim /wimfile:.\src\sources\install.wim /index:X /mountdir:.\mnt
    ```
    X は、手順 10 で取得したインデックスの値のプレースホルダーです。
12. 次のコマンドを入力し、現在マウントされているイメージにドライバを追加します。
    ```
    dism /image:.\mnt /add-driver /driver:C:\Temp\b57nd60a\b57nd60a.inf
    ```
13. 次のコマンドを入力して install.wim イメージをマウント解除します。
    ```
    dism /unmount-wim /mountdir:.\mnt /commit
    ```
14. 次のコマンドを入力して .iso ファイルを作成します。
    ```
    oscdimg -e -h -m -n -lslipstream -bootdata:2#p0,e,b"c:\Program Files\Windows
    AIK\Tools\PETools\amd64\boot\etfsboot.com"#pEF,e,b"c:\Program Files\Windows
    AIK\Tools\PETools\amd64\boot\efisys.bin" c:\temp\x\src c:\temp\Win20xxMOD.iso
    ```
    Platform は、インストールするオペレーティング システムのアーキテクチャ用のプレースホルダー (amd64 または x86 など) です。またファイル名の xx は、Windows Server OS バージョンのプレースホルダー (2012、2008R2、2008SP2) です。
15. DVD 書き込みアプリケーションを使用し、作成した .iso ファイルを DVD に書き込みます。
16. 手順 15 で作成した DVD を使用し、該当する Windows Server のバージョンをインストールします。

ブート

その後、システムでは iSCSI ブートの準備が完了し、オペレーティング システムが iSCSI ターゲットに存在します。最後のステップでは、実際のブートを実行します。システムは、ネットワークを介して Windows または Linux を起動し、Windows がローカル ディスク ドライブ上にあるかのように動作します。

1. サーバーを再起動します。
2. **CTRL + S** キーを押します。
3. **[Main]** メニューで、**[General Parameters]** を選択し、**[Boot to iSCSI target]** オプションを **[Enabled]** に設定します。

CHAP 認証が必要な場合は、ブートが成功したことを確認した後で、CHAP 認証を有効にします (CHAP 認証を有効化するを参照してください)。

その他の iSCSI ブートの考慮事項

システムで iSCSI ブートを設定するときに考慮する必要のある要素が他にもいくつかあります。

Windows 環境で速度と二重通信方式を変更する

NDIS パス経由のブートはサポートされません。NDIS パス経由の iSCSI ブートの場合、速度と二重通信方式は、BACS 管理ユーティリティを使用して変更できます。

Locally Administered Address (ローカル管理アドレス)

BACS の [設定] タブの [詳細設定] セクションの [Locally Administered Address/ ローカル管理アドレス] プロパティで割り当てられたユーザー定義 MAC アドレスは、iSCSI ブート対応のデバイスではサポートされません。

仮想 LAN

仮想 LAN (VLAN) タギングは、Microsoft iSCSI Software Initiator での iSCSI ブートではサポートされません。

iSCSI ブートのトラブルシューティング

次のトラブルシューティングのヒントは、iSCSI ブートに役立ちます。

トラブル：iSCSI ブートのリンク速度が 10 Mbps または 100 Mbps に設定されている場合、Broadcom iSCSI Crash Dump ユーティリティが正しく機能せずメモリ ダンプを取得できない。
ソリューション：iSCSI Crash Dump ユーティリティが動作するのは、iSCSI ブートのリンク速度が 1 Gbps または 10 Gbps に設定されている場合です。10 Mbps または 100 Mbps はサポートされていません。

トラブル：IPv6 接続を使用して Windows Server 2008 をインストールしようと、iSCSI ターゲットは、インストール ターゲットとして認識されない。
ソリューション：これはサードパーティ側の既知の問題です。Microsoft サポート技術情報文書 KB 971443 (http://support.microsoft.com/kb/971443) を参照してください。

トラブル：iSCSI コンフィギュレーション ユーティリティが実行されない。
ソリューション：iSCSI ブート ファームウェアが NVRAM にインストールされていることを確認します。

トラブル：iSCSI ブート LUN を 255 に設定すると、iSCSI ブートを実行しているときに、システムのブルー スクリーンが表示される。
ソリューション：Broadcom の iSCSI ソリューションは 0 ～ 255 の範囲で LUN をサポートしますが、Microsoft iSCSI Software Initiator は、255 の LUN をサポートしません。LUN の値は 0 ～ 254 の範囲で設定してください。

トラブル：インボックスではないハードウェア ID が存在している場合、インボックス ドライバを更新できない。
ソリューション：インストール メディア内に存在している、サポートされているドライバを使用し、カスタムのスリップストリーム DVD イメージを作成します。

iSCSI Crash Dump

Broadcom iSCSI Crash Dump ユーティリティを使用する場合は、インストール手順に従って iSCSI Crash Dump ドライバをインストールすることが重要です。詳細については、インストーラを使用する を参照してください。

セクション 10:Linux ドライバおよび管理アプリケーションのインストール

パッケージング

Linux TG3 ドライバは以下のパッケージ (ファイル名) で配布されています。

- ソース RPM (tg3-*version*.3dkms.src.rpm)
- ソース RPM (tg3-*version*.3dkms.noarch.rpm)
- 追加 (tg3_sup-*version*.tar.gz)
- 圧縮 TAR (tg3-*version*.tar.gz)

ドライバを構築するための同一ソース ファイルもこの RPM と TAR ソース パッケージに含まれています。tar ファイルには、ネットワーク インストール用のパッチ、ドライバ ディスク イメージといった付加的なユーティリティが含まれています。

TG3 ドライバ ソフトウェアをインストールする

ソース RPM パッケージをインストールする

基礎必須項目

- Linux カーネル ソース
- C コンパイラ

手順：

1. ソース RPM パッケージをインストールします。
   `rpm -ivh tg3-version.src.rpm`
2. ディレクトリを RPM のパスに変更し、カーネル のバイナリ ドライバを作成します (RPM のパスは Linux のディストリビューション版とは異なります)。
   ```
   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)
   ```

   注： ソース RPM パッケージのインストールを試行すると、次のようなメッセージが表示されることがあります。

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

   エラーの原因としては、rpm-build パッケージがインストールされていないことが考えられます。Linux インストールメディア上の rpm-build パッケージの保存場所を確認し、次のコマンドを使用してインストールします。

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

   ソース RPM のインストールを完了します。
3. 新しいビルトのパッケージをインストールします (ドライバおよび man ページ)。
   `rpm -ivh RPMS/i386/tg3-version.i386.rpm`

   ドライバがインストールされるパスは、カーネルによって異なります。

   2.6.x カーネル：

   /lib/modules/*kernel_version*/kernel/drivers/net/tg3.ko
4. ドライバをロードします。
   ```
   modprobe tg3
   ```

ネットワーク プロトコルとアドレスを設定する方法は、Linux の文書類を参照してください。

ソース TAR ファイルからドライバを構築する

1. ディレクトリ (tg3-*version*) を作成し、そのディレクトリに TAR ファイルを抽出します。
   ```
   tar xvzf tg3-version.tgz
   ```
2. カーネル実行用に、ロード可能なモジュールとして tg3.o ドライバを作成します。
   ```
   CD tg3-version
   make clean
   make; make install
   ```
3. ドライバをロードしてテストします。
   ```
   rmmod tg3
   modprobe tg3
   ```
   このコマンドが正しく実行された場合には、メッセージは返されません。

   注：インストールされているドライバの保存場所は、上の RPM の説明を参照してください。

4. ネットワーク プロトコルとアドレスを設定するときは、オペレーション システムの付属文書類を参照してください。

ネットワーク インストール

NFS、FTP、HTTP による (ネットワーク ブート ディスクまたは PXE を使用する) ネットワークのインストールでは、Linux オペレーティング システムのディストリビューションに含まれている tg3 ドライバを使用します。

TG3 ドライバをアンロード・削除する

RPM インスタレーションからドライバをアンロード・削除する

ドライバをアンロードするときは、**ifconfig** を使って、ドライバが開いたすべての *ethX* インターフェイスを閉じてから以下のように入力します。

```
rmmod tg3
```

rpm を使用してドライバをインストールした場合は、以下のコマンドを実行して削除します。

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

TAR インストレーションからドライバを削除する

TAR ファイルから make install を使ってドライバをインストールした場合、tg3.o ドライバ ファイルは手動でオペレーティング システムから削除してください。インストールされているドライバの保存場所は、ソース RPM パッケージをインストールするを参照してください。

tg3 ドライバに関係するインターフェイス コンフィギュレーションがある場合、**ifconfig ethx down**、次に **rmmod tg3** を使用して、最初にインターフェイスを閉じてください。

ドライバ メッセージ

/var/log/messages ファイルにログされるメッセージのうち、一般的なものを以下に示します。**dmesg -n*level*** を使用すると、コンソールに表示されるメッセージのレベルを指定できます。ほとんどの場合、レベル 6 がデフォルトとされています。

ドライバのサインオン

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

NIC の検出

```
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
```

フロー コントロール

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

リンクアップと速度の指定

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

リンクダウンの指定

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

チャネル結合によるチーム化

TG3 ドライバでは、結合カーネル モジュールおよびチャネル結合インターフェイスを使用して、アダプタをチーム化できます。Linux のチャンネル結合の詳細については、Linux の文書類を参照してください。

Linux 管理アプリケーションのインストール

概要

Broadcom Advanced Control Suite バージョン 4 (BACS4) は、NetXtreme I ファミリのアダプタを設定するための管理アプリケーションです。BACS4 ソフトウェアは、Windows と Linux のサーバーおよびクライアント オペレーティング システム上で動作します。

この章では、Linux システムに BACS4 管理アプリケーションをインストールする方法を説明します。Windows システムでは、Windows ドライバと、BACS4 を含む管理アプリケーションの両方をインストールするインストール プログラムが用意されています (詳細は、「Windows ドライバおよび管理アプリケーションをインストールする」を参照)。

BACS4 ユーティリティの 2 つの主要コンポーネントは、プロバイダ コンポーネントとクライアント ソフトウェアです。プロバイダは、1 つまたは複数の NIC が存在しているサーバー (または「管理ホスト」) にインストールされます。プロバイダは NIC に関する情報を収集して、クライアント ソフトウェアがインストールされている管理 PC から取得できるようにします。クライアント ソフトウェアは、プロバイダが情報を表示して NIC を設定できるようにします。BACS クライアント ソフトウェアには、グラフィカル ユーザー インターフェイス (GUI) とコマンド ライン インターフェイス (CLI) が含まれています。

通信プロトコル

通信プロトコルにより、プロバイダとクライアント ソフトウェアの間で情報を交換できます。これらは、Distributed Management Task Force (DMTF) 策定の Web-Based Enterprise Management (WBEM) と Common Information Model (CIM) 標準の独自実装、およびオープンソース実装です。ネットワーク管理者は、ネットワーク上で主に使用されている標準に基づいて、最善のオプションを選択できます。

次の表に、管理ホストとクライアントにインストールされている OS に基づいて利用可能なオプションを示します。

クライアントの使用 OS	*管理ホストの使用 OS*	*BACS が使用可能な通信プロトコル*
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)

- WMI = Windows Management Instrumentation。
- WS-MAN = Web Service-Management。WinRM は Windows ベースの実装であり、OpenPegasus は Linux 上で動作するオープンソースの実装です。
- CIM-XML = OpenPegasus の XML ベース バージョンです。

ネットワーク内に、Windows サーバーと Linux サーバーにアクセスする Windows クライアントと Linux クライアントが混在している場合、WS-MAN が適切な選択肢です。サーバーにインストールされている OS が Linux のみの場合、CIM-XML が選択肢になります。ネットワークに Windows サーバーと Windows クライアントのみが存在している場合、WMI が選択肢になります。WMI は設定が非常に簡単ですが、Windwos OS 以外ではサポートされていません。(Windows プロトコルのインストールと設定の手順は、「Windows ドライバおよび管理アプリケーションをインストールする」を参照してください)。

BACS のインストールには、管理ホストにプロバイダ コンポーネントをインストールし、管理ステーションにクライアント ソフトウェアをインストールする作業が含まれます。クライアントと管理ホストにインストールされている OS の組み合わせ、および選択した通信プロトコルに基づいて、インストール プロセスは異なります。

WS-MAN または CIM-XML を Linux サーバーにインストールする

手順 1：OpenPegasus をインストールする

Red Hat Linux OS では、2 つのインストール オプションが利用できます。

- インボックス RPM から (Red Hat のみ)
- ソースから (Red Hat および SuSE)

SUSE Linux Enterprise Server 11 (SLES11) OS では、ソース RPM を使用する必要があります。

注：インボックス RPM は、通信プロトコル WS-MAN をサポートしません。WS-MAN を使用するには、ソースから OpenPegasus をインストールする必要があります。

インボックス RPM から (Red Hat のみ)

Red Hat Linux では、Inbox OpenPegasus RPM は次の形で利用できます。`tog-pegasus-<version>.<arch>.rpm`

1. 次のコマンドを使用して tog-pegasus をインストールします。
   `rpm -ivh tog-openpegasus-<version>.<arch>.rpm`
2. 次のコマンドを使用して Pegasus を起動します。
   `/etc/init.d/tog-pegasus start`

注：SuSE Linux では、Inbox OpenPegasus RPM を利用できません。次の手順に従って、OpenPegasus をソースからインストールする必要があります。

インボックス Pegasus では、デフォルトで HTTP が有効になっていません。Inbox OpenPegasus を正常にインストールした後、それ以上の設定が必要ない場合、手順 4 : Broadcom CMPI プロバイダをインストールするの説明に従ってください。HTTP を有効にするには、HTTP を有効にするを参照してください。

ソースから (Red Hat および SuSE)

OpenPegasus のソースは、www.openpegasus.org からダウンロードできます。

注：まだインストールしていない場合、openssl および libopenssl-devel rpm をダウンロードし、インストールします。このステップはオプションであり、HTTPS を使用してクライアントを管理ホストに接続する場合のみ必須です。

環境変数を設定する

OpenPegasus をビルドするために、環境変数を次のように設定します。

環境変数	*説明*
PEGASUS_ROOT	Pegasus ソース ツリーの場所
PEGASUS_HOME	ビルドした実行ファイルやレポジトリの場所。たとえば、$PEGASUS_HOME/bin、PEGASUS_HOME/lib、$PEGAUS_HOME/repository、および $PEGASUS_HOME/mof subdirectories。
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Linux 32 ビット システムの場合：「LINUX_IX86_GNU」 Linux 64 ビット システムの場合：「LINUX_X86_64_GNU」
PEGASUS_HAS_SSL	オプション。HTTPS をサポートするには、「true」に設定します。
PEGASUS_ENABLE_PROTOCOL_WSMAN	オプション。WSMAN プロトコルをサポートするには、「true」に設定します。

追加設定

$PEGASUS_HOME 変数はシェル環境で設定する必要があり、$PEGASUS_HOME/bin は環境変数 $PATH に追加する必要があります。

例

- 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

SSL をサポートするには、次の環境変数を追加します。

- export PEGASUS_HAS_SSL=true

WS-MAN をサポートするには、次の環境変数を追加します。

- export PEGASUS_ENABLE_PROTOCOL_WSMAN=true

OpenPegasus の CIM-XML および WSMAN では、HTTP または HTTPS で同じポートを使用します。HTTP と HTTPS それぞれのデフォルトのポート番号は、5988 と 5989 です。

注：これらのエクスポートは .bash_profile の最後に追加できます。このファイルは /root ディレクトリにあります。

- PuTTY を使用してユーザーがログインする場合、これらの環境変数が設定されます。
- これらの環境変数が設定されていない各ターミナルでは、Linux システム自体で次のコマンドを実行します。
  `source /root/.bash_profile`
- ログアウトし、ログインしたときに、環境変数が設定されます。

OpenPegasus をビルドおよびインストールする

$PEGASUS_ROOT (Pegasus ソースのルート ディレクトリの場所) から、次のコマンドを実行します。

```
make clean
make
make repository
```

注：OpenPegasus をソースからビルドする場合は必ず、すべての設定はデフォルト値にリセットされます。OpenPegasus を再ビルドする場合、手順 3：サーバーで OpenPegasus を設定するの説明に従って設定をやり直す必要があります。

手順 2：サーバーで CIM サーバーを起動する

CIM サーバーを起動するには、`cimserver` コマンドを使用します。CIM サーバーを停止するには、`cimserver -s` コマンドを使用します。

OpenPegasus が正常にインストールされたかどうかを確認するには、次のコマンドを入力します。

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

注：OpenPegasus をソースからコンパイルするには、CIM サーバーを起動するときに PEGASUS_HOME を定義する必要があります。そうしないと、CIM サーバーはレポジトリを正しくロードしません。「bash_profile」ファイル内で PEGASUS_HOME を設定することを考慮してください。

手順 3：サーバーで OpenPegasus を設定する

次の表に示すように、`cimconfig` コマンドを使用して OpenPegasus を設定します。

コマンド	*説明*
`cimconfig -l`	すべての有効なプロパティ名をリストします。
`cimconfig -l -c`	すべての有効なプロパティ名とその値をリストします。
`cimconfig -g <property name>`	特定のプロパティを問い合わせます。
`cimconfig -s <property name>=<value> -p`	特定のプロパティを設定します。
`cimconfig --help`	コマンドの詳細を表示します。

`cimconfig` を実行する前に CIM サーバーを起動する必要があり、設定の変更を有効にするには CIM サーバーを再起動する必要があります。

認証を有効にする

このセクションの説明に従って、OpenPegasus の次のプロパティを設定する必要があります。そうしないと、Broadcom CIM プロバイダが正常に動作しません。BACS を起動してプロバイダに接続する前に、次の設定が行われていることを確認します。

まだ起動されていない場合、CIM サーバーを起動します。その後、次の設定を行います。

- `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`

root ユーザーがリモート接続できるようにするには、次の手順に従います。

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

権限を持ったユーザーの設定：Linux システム ユーザーは、OpenPegasus の認証に使われます。BACS 経由で接続するために、`cimuser` を使用してシステム ユーザーを OpenPegasus に追加する必要があります。

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

  例：`cimuser -a -u root -w linux1`

HTTP を有効にする

1. まだ起動していない場合、CIM サーバーを起動します。
2. 次のコマンドを使用して HTTP ポートを設定します (オプション)。
   `cimconfig -s httpPort=5988 -p`

   Inbox OpenPegasus では、このプロパティは利用できません。
3. 次のコマンドを使用して HTTP 接続を有効にします。
   `cimconfig -s enableHttpConnection=true -p`
4. 新しい設定を有効にするために、`cimserver -s` および `cimserver` の各コマンドを使用して、CIM サーバーを停止および再起動します。

HTTPS を有効にする

1. まだ起動していない場合、CIM サーバーを起動します。
2. 次のコマンドを使用して HTTPS ポートを設定します (オプション)。
   `cimconfig -s httpsPort=5989 -p`

Inbox OpenPegasus では、このプロパティは利用できません。

3. 次のコマンドを使用して HTTPS 接続を有効にします。
   `cimconfig -s enableHttpsConnection=true -p`
4. 新しい設定を有効にするために、`cimserver -s` および `cimserver` の各コマンドを使用して、CIM サーバーを停止および再起動します。

手順 4：Broadcom CMPI プロバイダをインストールする

CMPI プロバイダをインストールする前に、OpenPegasus が正しくインストールされていることを確認します。

インストール

Broadcom CMPI プロバイダをインストールするには、次のコマンドを入力します。

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

アンインストール

Broadcom CMPI プロバイダをアンインストールするには、次のコマンドを入力します。

```
% rpm -e BRCM_CMPIProvider
```

手順 5：Linux ファイアウォールを設定する (必要な場合)

ファイアウォールで適切なポートを開くには、次の手順を実行します。

Red Hat

1. **[System/ システム]** をクリックし、**[Administration/ 管理]** を選択し、**[Firewall/ ファイアーウォール]** を選択します。
2. **[Other Ports/ その他のポート]** を選択します。
3. [Port and Protocol/ ポートとプロトコル] ダイアログ ボックスで、**[User Defined/ ユーザー定義]** を選択します。
4. **[Port/Port Range (ポート / ポート範囲)]** フィールドで、ポート番号を追加します。
5. **[Protocol/ プロトコル]** フィールドで、プロトコルとして TCP または UDP などを追加します。
6. **[Apply/ 適用]** をクリックし、ファイアウォール ルールを有効にします。

例：

- CIM-XML over HTTP の場合、ポート番号は 5988、プロトコルは TCP です。
- CIM-XML over HTTPS の場合、ポート番号は 5989、プロトコルは TCP です。

SuSE

1. **[コンピュータ]** をクリックし、**[YaST]** を選択します。
2. 左側のペインで **[Security & Users/ セキュリティとユーザー]** を選択します。
3. 右側のペインで **[Firewall/ ファイアウォール]** をダブルクリックします。
4. 左側のペインで **[Custom Rules/ カスタムルール]** を選択します。
5. 右側のペインで **[追加]** をクリックします。
6. 次の値を入力します。
   - **[ソース ネットワーク]**：0/0 (すべて)
   - **[プロトコル]**：TCP (または適切なプロトコル)
   - **[宛先ポート]**：< *ポート番号* > または < *ポート番号の範囲* >
   - **[ソース ポート]**：空白のままにします。
7. **[Next/ 次へ]** をクリックし、**[Finish/ 完了]** をクリックしてファイアウォール ルールを有効にします。

例：

CIM-XML の場合、次の値を使用します。

- **[ソース ネットワーク]**：0/0 (すべて)
- **[プロトコル]**：TCP
- **[宛先ポート]**：5988：5989
- **[ソース ポート]**：空白のままにします。

手順 6：BACS と関連する管理アプリケーションをインストールする

Broadcom Advanced Control Suite アプリケーションをインストールするを参照してください。

Linux クライアントに WS-MAN または CIM-XML をインストールする

Linux クライアント システムで HTTP を使用するために、BACS 管理アプリケーションをインストールする以外に、特別なソフトウェア コンポーネントは必要ありません。ただし、WS-MAN をインストールする場合、BACS と組み合わせて使用するために、オプションで HTTPS プロトコルを設定することができます。

Linux クライアントで HTTPS を設定する

HTTP の代わりに HTTPS を使用する場合 (WS-MAN のみ)、次の手順に従います。

Windows/Linux サーバーの自己署名付き証明書を生成する

Linux または Windows で OpenSSL を使用し、次の手順に従って、自己署名付き証明書を生成することができます。

注：openssl は、http://gnuwin32.sourceforge.net/packages/openssl.htm からダウンロードしてインストールすることができます。

1. 次のコマンドを入力して秘密キーを生成します。
   `openssl genrsa -des3 -out server.key 1024`
2. パスフレーズの入力を要求されます。パスフレーズは忘れないようにしてください。
3. 次の手順に従って証明書の署名要求 (CSR) を生成します。

   CSR の生成中に、いくつかの情報の入力を要求されます。「共通名」の入力を要求された場合は、Windows サーバーのホスト名または IP アドレスを入力してください。

   次のコマンドを入力します (応答例も示されています)。

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

   このコマンドが動作しない場合、次のコマンドを試してください。

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

   openssl.cnf ファイルは、openssl が配置されているディレクトリと同じディレクトリに配置する必要があります。openssl.cnf は、C:\Program Files (x86)\GnuWin32\share フォルダに配置されています。

   以下の情報が要求されます。

   - 国名 (2 文字のコード) [] : **US**
   - 都道府県名 (フルネーム) [] : **California**
   - 地域名 (都市名など) [] : **Irvine**
   - 組織名 (会社など) [] : **Broadcom Corporation**
   - 組織単位名 (セクションなど) [] : **Engineering**
   - 共通名 (ユーザー名など) [] : Windows サーバーのホスト名または IP アドレスを入力します。iPv6 の場合、[xyxy:xxx:….::xxx] という形式で共通名を入力します (**括弧 [ ] を含みます**)。
   - (オプション) 電子メール アドレス [] :

   証明書要求と併せて送信される、次の追加属性を入力します。

   - チャレンジ パスワード [] : **linux1**
   - オプションの会社名 [] :
4. パスフレーズをキーから削除します。

   次のコマンドを入力します。

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

5. 署名付き証明書を生成します。

   365 日アクティブな署名付き証明書を生成するには、次のコマンドを入力します。

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

   次の出力が表示されます。

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

6. 次のコマンドを入力して、生成された署名付き証明書を検証します。
   ```
   openssl verify server.crt
   ```

   次の出力が表示されます。

   ```
   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
   ```

   エラー メッセージ「error 18 at 0 depth lookup:self signed certificate」は無視してください。このエラーは、これが署名付き証明書であることを示すものです。

7. 次のようにして、証明書の形式を 「crt」から 「pkcs12」に変換します。

   Windows サーバーの場合、証明書は pkcs12 の形式になっています。次のコマンドを入力します。

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

   次のプロンプトが表示されます。

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

   パスワードを入力します。パスワードは忘れないでください。パスワードは、証明書を Windows サーバーおよびクライアントにインポートする際に必要です。

8. 証明書をインポートできるように、証明書ファイル server.crt のコピーを作成して BACS のインストール先のサーバーに置きます。BACS を実行しているサーバーへ Windows クライアントまたは Linux クライアントから接続する場合は、証明書をクライアントのシステムにも転送する (コピーして貼り付ける) 必要があります。

   Linux では、証明書に拡張子「.pem」を付ける必要があります。拡張子「.crt」と「.pem」は同じであるため、openssl コマンドを使用して、.crt を .pem に変換する必要はありません。ファイルをそのままコピーすることができます。

注：IPv4 アドレス、IPv6 アドレス、およびホスト名に個別の証明書を作成する必要があります。

Linux クライアントに署名付き証明書をインポートする

Linux ディストリビューションで、次の証明書ディレクトリを記録します。

- SuSE のすべてのバージョンでは、証明書ディレクトリは /etc/ssl/certs です。
- Red Hat では、証明書ディレクトリはバージョンごとに異なる可能性があります。一部のバージョンでは、/etc/ssl/certs または /etc/pki/tls/certs です。他のバージョンでは、証明書ディレクトリを見つけてください。

Windows/Linux サーバーの自己署名付き証明書を生成するで作成した *hostname.pem* を、Linux クライアントの証明書ディレクトリにコピーします。たとえば、証明書ディレクトリが /etc/ssl/certs の場合、*hostname.pem* を /etc/ssl/certs にコピーします。

1. /etc/ssl/certs ディレクトリに移動します。
2. 次のコマンドを実行してハッシュ値を作成します。
   openssl x509 -noout -hash -in hostname.pem

   次のような値が返されます。

   100940db
3. 次のコマンドを実行してハッシュ値へのシンボリック リンクを作成します。
   ln -s hostname.pem 100940db.0

Linux クライアントからの HTTPS/SSL 接続をテストする

次のコマンドを使用して、Linux に証明書が正しくインストールされたかどうかをテストします。

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

このテストに失敗した場合、証明書が正しくインストールされていません。また、対応策を実行することを求めるエラーメッセージが表示されます。

Broadcom Advanced Control Suite アプリケーションをインストールする

Broadcom Advanced Control Suite (BACS) ソフトウェアは、Linux RPM パッケージを使用して Linux システムにインストールできます。

始める前に：

- このユーティリティで管理するために、Broadcom ネットワーク アダプタが物理的に取り付けられ、NIC 用の適切なデバイス ドライバがシステムにインストールされていることを確認します。
- このユーティリティで管理する CIM プロバイダがシステムに正しくインストールされていることを確認します。参照してください。
- Linux ホストで iSCSI を管理するために、open-iscsi と sg の各ユーティリティが Linux ホストにインストールされていることを確認します。

BACS をインストールするには：

1. 最新の BACS 管理アプリケーション RPM パッケージをダウンロードします。
2. 次のコマンドを使用して RPM パッケージをインストールします。
   % rpm -i BACS-{version}.{arch}.rpm

BACS の CLI を使用するには、リリース ファイルに付属の BACSCLI_Readme.txt ファイルを参照してください。

BACS を削除するには

RPM パッケージをアンインストールするには、次のコマンドを使用します。

```
% rpm -e BACS
```

セクション 11:VMware ドライバ ソフトウェア

パッケージング

VMware ドライバは以下のパッケージ形式で配布されています。

表 19:VMware ドライバのパッケージ

形式	*ドライバ*
VMware VIB	vmware-esx-drivers-net-tg3-version.x86_64.vib

ドライバ

ドライバのダウンロード、インストール、更新

NetXtreme I GbE 向けの VMware ESX/ESXi ドライバのダウンロード、インストール、更新については、http://www.vmware.com/support を参照してください。

ドライバのパラメタ

NetQueue

オプション パラメタ **force_netq** を使用して、Rx および Tx のネット キューの数を設定することができます。NetQueue をサポートする BCM57XX デバイスは、BCM5718、BCM5719、BCM5720、BCM5721、および BCM5722 です。

デフォルトで、ドライバは NetQueue の最適数を使用しようとします。キューの数を明示的に強制するには、次のコマンドを使用して、ポート当たりの NetQueues の数を設定します。

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

x には、-1 ～ 15 の値を使用することができます。

- 1 ～ 15 を指定すると、特定の NIC で NetQueue の数を強制します。
- 0 を指定すると NetQueue が無効になります。
- –1 を指定すると、NetQueue に関するドライバーのデフォルト値を使用するように指定します。

「x」エントリの数は、最大 32 個まで増やすことができます。つまり、サポートされている NIC の最大数 = 32 です。

使用例：

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

- tg3 NIC 0：NetQueues のデフォルトの数を使用します。
- tg3 NIC 1：NetQueue 機能をディセーブルします。
- tg3 NIC 2：NetQueue を 1 つ使用します。
- tg3 NIC 3：NetQueue を 2 つ使用します。

上記の NIC 番号が、vmnic<#> に対応していないことに注意してください。NIC 番号は、システムの vmnic プローブ順序番号と同じ値です。最適な方法は、NetQueue の数とマシンの CPUs の数と同じにすることです。

ドライバのパラメタ

vmkload_mod コマンドのコマンドライン引数として、いくつかのオプション パラメタを指定できます。これらのパラメタは、esxcfg-module コマンドを使っても設定できます。詳細は、man ページを参照してください。

ドライバのデフォルト

表 20:VMware ドライバ のデフォルト

パラメタ	*デフォルト値*
レート	通知されているすべての速度で自動ネゴシエーション
フロー コントロール	通知されている RX と TX で自動ネゴシエーション
MTU	1500 (範囲は 46 ～ 9000)
RX Ring Size (RX リング サイズ)	200 (範囲は 0 ～ 511) 一部のチップでは 64 に固定されています。
RX Jumbo Ring Size (RX ジャンボ リング サイズ)	100 (範囲は 0 ～ 255) すべてのチップがジャンボ リングをサポートしているわけではありません。また、ジャンボ フレームをサポートしているチップの一部はジャンボ リングを使用しません。
TX Ring Size (TX リング サイズ)	511 (範囲は (MAX_SKB_FRAGS+1) ～ 511)。MAX_SKB_FRAGS は、カーネルやアーキテクチャによって異なります。x86 の 2.6 カーネルでは、MAX_SKB_FRAGS は 18 です。
Coalesce RX Microseconds (連結 RX マイクロ秒)	20 (範囲は 0 ～ 1023)
Coalesce RX Microseconds irq (連結 RX マイクロ秒 IRQ)	20 (範囲は 0 ～ 255)
Coalesce rx frames (連結 RX フレーム)	5 (範囲は 0 ～ 1023)
Coalesce rx frames irq (連結 RX フレーム IRQ)	5 (範囲は 0 ～ 255)
Coalesce TX Microseconds (連結 TX マイクロ秒)	72 (範囲は 0 ～ 1023)
Coalesce tx users irq (連結 TX ユーザー IRQ)	20 (範囲は 0 ～ 255)
Coalesce tx frames (連結 TX フレーム)	53 (範囲は 0 ～ 1023)

表 20:VMware ドライバのデフォルト

パラメタ	*デフォルト値*
Coalesce tx frames irq (連結 TX フレーム IRQ)	5 (範囲は 0 ～ 255)
Coalesce stats usecs (連結統計マイクロ秒)	1000000 (約 1 秒)。特定のチップでは、一部の連結パラメタは使用されていないか、異なるデフォルト値を使用します。
MSI	イネーブル (チップでサポートされており、割り込みテストに合格した場合)
WoL	無効

ドライバ メッセージ

/var/log/messages ファイルにログされるメッセージのうち、とても一般的なものを以下に示します。dmesg -n <level> を使用すると、コンソールにメッセージを表示するレベルが指定できます。ほとんどの場合、レベル 6 がデフォルトとされています。すべてのメッセージを表示するには、レベルを上げます。

ドライバのサインオン

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

NIC の検出

```
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
```

リンクアップと速度の指定

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

リンクダウンの指定

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

セクション 12:Windows ドライバおよび管理アプリケーションのインストール

ドライバ ソフトウェア をインストールする

注： ここで示す手順は、Broadcom NetXtreme アダプタが工場出荷時に取り付けられていないことを前提にしています。工場出荷時にコントローラが取り付け済みだった場合は、ドライバ ソフトウェアもインストール済みです。

Broadcom NetXtreme アダプタなどのハードウェア デバイスを取り付けた後に初めて Windows を起動する場合、あるいは既存のデバイス ドライバを削除した場合、オペレーティング システムによって自動的にハードウェアが検出され、このデバイスのドライバ ソフトウェアをインストールするようプロンプトが表示されます。

視覚的な対話型インストール モード (インストーラを使用するを参照) と、無人インストール (サイレント インストールを使用するを参照) 用コマンド ライン サイレント モードの両方を使用できます。

メモ：

- ドライバ ソフトウェアをインストールする前に、Windows オペレーティング システムが最新サービス パックにより最新バージョンに更新されていることを確認してください。
- Broadcom NetXtreme Gigabit Ethernet アダプタを Windows システムで使用するときは、あらかじめネットワーク デバイス ドライバをインストールしておかなければなりません。ドライバは、インストール CD-ROM に保存されています。
- BACS は、Microsoft Windows Server 2008 R2 用の Server Core インストール オプションでサポートされません。

インストーラを使用する

インストーラでは、Broadcom デバイス ドライバに加えて、管理アプリケーションがインストールされます。インストーラの実行時には、以下がインストールされます。

- **Broadcom Device Drivers**：Broadcom デバイス ドライバをインストールします。
- **Control Suite**：Broadcom Advanced Control Suite (BACS)。
- **BASP**：Broadcom Advanced Server Program をインストールします。
- **SNMP**：Simple Network Management Protocol サブエージェントをインストールします。
- **CIM Provider**：Common Information Model プロバイダをインストールします。
- **iSCSI Crash Dump ドライバ**。iSCSI Crash Dump ユーティリティに必要なドライバをインストールします。

注: BACS ソフトウェアおよび関連する管理アプリケーションのインストールはオプションですが、インストーラを使用する場合、Broadcom デバイス ドライバはインストールする必要があります。

注： BASP は、Windows Small Business Server (SBS) 2008 では使用できません。

iSCSI Crash Dump 用の Microsoft iSCSI Software Initiator をインストールするには

Broadcom iSCSI Crash Dump ユーティリティがサポートされている場合に、ユーティリティを使用するときは、インストール手順に従うことが重要です。

- インストーラを実行する
- Microsoft iSCSI Software Initiator とパッチをインストールする (MS KB939875)

注: インストーラからデバイス ドライバのアップグレードを実行している場合、BACS の [設定] タブの [詳細設定] セクションで **[iSCSI Crash Dump/iSCSI クラッシュ ダンプ]** を再度イネーブルします。

インストーラを実行してデバイス ドライバと管理アプリケーションをインストールした後で、この手順を実行します。

1. OS に含まれていない場合、Microsoft iSCSI Software Initiator (バージョン 2.06 以降) をインストールします。Microsoft iSCSI Software Initiator のインストールが必要であるかどうかを確認するには、表 21 を参照してください。Microsoft から iSCSI Software Initiator をダウンロードするには、http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986 にアクセスします。
2. http://support.microsoft.com/kb/939875 から iSCSI Crash Dump ファイル生成 (Microsoft KB939875) 用の Microsoft パッチを入手してインストールします。Microsoft パッチのインストールが必要であるかどうかを確認するには、表 21 を参照してください。

表 21:Windows オペレーティング システムと iSCSI クラッシュ ダンプ

オペレーティング システム	*MS iSCSI Software Initiator が必要*	*Microsoft パッチ (MS KB939875) が必要*
NDIS		
Windows Server 2008	はい (OS に搭載)	いいえ
Windows Server 2008 R2	はい (OS に搭載)	いいえ
Windows Server 2012	はい (OS に搭載)	いいえ
OIS		
Windows Server 2008	いいえ	いいえ
Windows Server 2008 R2	いいえ	いいえ
Windows Server 2012	いいえ	いいえ

サイレント インストールを使用する

メモ:

- コマンドはすべて、大文字と小文字が区別されます。
- 無人インストールの詳細については、Driver_Management_Apps_Installer フォルダの Silent.txt ファイルを参照してください。

コマンド ラインの説明については、インストール フォルダ内の readme.txt ファイルを参照してください。

注: REINSTALL スイッチは、同じインストーラがシステムにすでにインストールされている場合にのみ使用します。以前のバージョンのインストーラをアップグレードする場合は、前述した `setup /s /v/qn` を使用します。

ドライバ ソフトウェアの変更

ドライバ ソフトウェアを変更するには：

1. [コントロール パネル] で、**[プログラムの追加と削除]** をダブルクリックします。
2. **[Broadcom Drivers and Management Applications/Broadcom ドライバおよび管理アプリケーション]** をクリックし、**[変更]** をクリックします。
3. **[次へ]** をクリックして次に進みます。
4. プログラムの機能を変更するには、**[Modify/ 変更]**、**[追加]**、**または [削除]** をクリックします。このオプションでは、新しいアダプタにドライバはインストールされません。新しいアダプタにドライバをインストールする方法については、ドライバ ソフトウェアの修復または再インストールを参照してください。
5. **[次へ]** をクリックして次に進みます。
6. アイコンをクリックして、機能をインストールする方法を変更します。
7. **[次へ]** をクリックします。
8. **[インストール]** をクリックします。
9. **[完了]** をクリックしてインストーラを閉じます。
10. システムの再起動が必要かどうかインストーラが判断します。画面に表示されるプロンプトに従います。

ドライバ ソフトウェアの修復または再インストール

ドライバ ソフトウェアを修復または再インストールするには :

1. [コントロール パネル] で、**[プログラムの追加と削除]** をダブルクリックします。
2. **[Broadcom Drivers and Management Applications/Broadcom ドライバおよび管理アプリケーション]** をクリックし、**[変更]** をクリックします。
3. **[次へ]** をクリックして次に進みます。
4. エラーの修復、または新しいアダプタへのドライバのインストールには、**[Repair/ 修復] または [Reinstall/ 再インストール]** をクリックします。
5. **[次へ]** をクリックして次に進みます。
6. **[インストール]** をクリックします。
7. **[完了]** をクリックしてインストーラを閉じます。
8. システムの再起動が必要かどうかインストーラが判断します。画面に表示されるプロンプトに従います。

デバイス ドライバの削除

デバイス ドライバを削除すると、インストールされている管理アプリケーションもすべて削除されます。

注 : 現在のデバイス ドライバを以前にインストールされていたドライバで置き換えるために、Windows Server 2008 および Windows Server 2008 R2 には、デバイス ドライバ ロールバック機能が備わっています。ただし、個々のコンポーネントでロールバック機能を使用する場合、NetXtreme デバイスの複雑なソフトウェア アーキテクチャにより問題が発生する場合があります。したがって、ドライバ バージョンを変更するのは、ドライバ インストーラを使用して行うことをお勧めします。

デバイス ドライバを削除するには :

1. [コントロール パネル] で、**[プログラムの追加と削除]** をダブルクリックします。
2. **[Broadcom Drivers and Management Applications/Broadcom ドライバおよび管理アプリケーション]** をクリックし、**[削除]** をクリックします。画面に表示されるプロンプトに従います。
3. コンピュータを再起動すると、ドライバの削除が完了します。コンピュータの再起動に失敗すると、ドライバは正常にインストールできません。

アダプタのプロパティを表示または変更する

Broadcom ネットワーク アダプタのプロパティを表示または変更するには：

1. [コントロール パネル] で、**[Broadcom Control Suite 4]** をクリックします。
2. **[設定]** タブの [詳細設定] タブをクリックします。

電源の管理オプションを設定する

[電源の管理] オプションを設定すると、節電のために、オペレーティング システムがコントローラの電源をオフにできるようになります。また、コントローラは、節電モードからコンピュータを起動できます。ただし、デバイスが作動中でビジーの場合 (呼び出しに対応している場合など) は、オペレーティング システムがそのデバイスをシャットダウンすることはありません。オペレーティング システムが、各デバイスのシャットダウンを試行するのは、コンピュータが休止状態に移行しようとするときだけです。コントローラを常時オンにしておく場合は、[**電力の節約のために、コンピュータでこのデバイスの電源をオフにできるようにする**] チェック ボックスを選択しないでください。

注：[電源の管理] オプションは、ブレード サーバーでは使用できません。

メモ：

- [電源の管理] タブは、電源の管理をサポートしているサーバーに対してのみ利用できます。
- コンピュータがスタンバイ モードのときに WOL (Wake on LAN、LAN の始動) をイネーブルするには、必ず **[このデバイスで、コンピュータのスタンバイ状態を元に戻すことができるようにする]** ボックスをクリックしてください。
- **[管理ステーションでのみ、コンピュータのスタンバイ状態を解除できるようにする]** を選択すると、コンピュータをスタンバイ状態から元に戻せるのは、*Magic Packet だけ*になります。

注意事項：チームのメンバーであるアダプタに **[電力の節約のために、コンピュータでこのデバイスの電源をオフにできるようにする]** は選択しないでください。

BACS4 と併せて使用する通信プロトコルを設定する

BACS4 管理アプリケーションの 2 つの主要コンポーネントは、プロバイダ コンポーネントとクライアント ソフトウェアです。プロバイダは、1 つまたは複数の NIC が存在しているサーバー (または「管理ホスト」) にインストールされます。プロバイダは NIC に関する情報を収集して、クライアント ソフトウェアがインストールされている管理 PC から取得できるようにします。クライアント ソフトウェアは、プロバイダが情報を表示して NIC を設定できるようにします。BACS クライアント ソフトウェアには、グラフィカル ユーザー インターフェイス (GUI) とコマンド ライン インターフェイス (CLI) が含まれています。

通信プロトコルにより、プロバイダとクライアント ソフトウェア間に通信が確立されます。ネットワーク内にあるクライアントと仮ホスト上のオペレーティング システム (Linux、Windows、または両方) の組み合わせによって、使用する適切な通信プロトコルを選択できます。各ネットワーク設定で利用可能な通信プロトコルの説明は、『Linux 管理アプリケーションのインストール』を参照してください。

この章の手順は、Windows 管理ホストが Windows クライアントと通信するシナリオのみに適用されます。これらのシナリオでは、WMI または WS-MAN (WinRM) どちらかの通信プロトコルを使用できます。本章で説明しているドライバ インストーラを使用してドライバと管理アプリケーションの両方をインストールすると、WMI と WS-MAN の両方のプロバイダが管理ホストにインストールされます。また、BACS4 ユーティリティもクライアントにインストールされます。これ以降のセクションでは、選択した通信プロトコルの詳細な設定手順について説明します。

Linux インストールでは、ドライバは管理アプリケーションとは別にインストールされます。関連する説明は、を参照してください。

WS-MAN を使用する

WS-MAN 通信プロトコルを使用するには、次のセクションの手順に従います。

- WS-MAN を使用する Windows サーバーの設定
- Windows クライアントへの WS-MAN のインストール

WS-MAN を使用する Windows サーバーの設定

手順 1：WinRM ソフトウェア コンポーネントをサーバーにインストールする

WinRM 2.0 は、次のオペレーティング システムにプリインストールされています。

- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows 2012 R2

Windows Server 2008 の場合、WinRM 2.0 と Windows Powershell 2.0 を含んでいる Windows Management Framework Core を、次のリンクからインストールします。

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

手順 2：サーバーの基本設定を行う

WinRM が正しく機能するためには、Windows ファイアウォールを有効にする必要があります。ファイアウォールの設定の詳細については、「手順 7：追加のサーバー設定」を参照してください。ファイアウォールを設定したら、コマンド プロンプトを開き、次のコマンドを実行して Windows サーバーのリモート管理を有効にします。

```
winrm quickconfig
```

次のコマンドを使用して、サービスの設定情報を表示することができます。

```
winrm get winrm/config
```

手順 3：サーバーのユーザー設定を行う

WinRM に接続するには、アカウントをローカル コンピュータまたはリモート コンピュータのローカル管理者グループのメンバーにする必要があります。`get winrm/config` コマンドの出力は次のようになります。

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

BA は BUILTIN\Administrators を意味します。

別のユーザー グループを WinRM で許可された接続リストに追加するには、RootSDD を変更して新しいユーザー グループを含めます。新しいグループの SDDL ID が必要です。たとえば、次のコマンドは、S-1-5-21-1866529496-2433358402-1775838904-1021 という SDDL ID で新しいユーザー グループを追加します。

```
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)"}
```

手順 4：サーバーの HTTP 設定を行う

BACS GUI を使用するには、以下の方法で HTTP プロトコルを設定する必要があります。

注：WinRM 2.0 のデフォルトの HTTP ポートは 5985 です。

1. **[スタート]** をクリックして (または Windows ロゴ キーを押して)、**[ファイル名を指定して実行]** を選択します。
2. 「**gpedit.msc**」と入力して、ローカルのグループ ポリシー エディタを開きます。
3. **[コンピュータの構成]** で、**[管理用テンプレート]** フォルダを開き、続いて **[Windows コンポーネント]** フォルダを開きます。
4. **[Windows リモート管理 (WinRM)]** を選択します。
5. **[Windows リモート管理 (WinRM)]** で、**[WinRm クライアント]** を選択します。
6. **[WinRM クライアント]** で、**[信頼されたホスト]** をダブルクリックします。
7. **[TrustedHostsList]** に、クライアントのホスト名を入力します。すべてのクライアントが信頼される場合は、アスタリスク (*) だけを入力します。
8. **[WinRM サービス]** を選択します。
9. **[基本認証を許可する]** を有効にします。

10. **[暗号化されていないトラフィックを許可する]** を有効にします。
11. **[グループ ポリシー]** ウィンドウを閉じます。
12. コマンド プロンプトから次のコマンドを実行して、WinRM をデフォルトの設定で設定します。
    `winrm qc or winrm quickconfig`
13. 「**Make these changes[y/n]?**」と表示されたら、「**y**」を入力します。
14. 次のどちらか 1 つのコマンドを入力して、HTTP リスナーが作成されているかどうかを確認します。
    `winrm enumerate winrm/confg/listener`

    または

    `winrm e winrm/config/Listener`
15. コマンド プロンプトで次のコマンドを入力して、ローカル テストを実行します。
    `winrm id`

手順 5：サーバーの HTTPS 設定を行う (HTTP ではなく HTTPS を使用する)

この手順には、自己署名付き証明書を生成するプロセス (証明書が存在しない場合) と、証明書を Windows サーバーにインポートするプロセスの 2 つのプロセスがあります。自己署名付き証明書がない場合は、Windows サーバー上でこの証明書を設定して、Windows クライアントの BACS GUI との間で HTTPS/SSL 通信を有効にする必要があります。Windows クライアントも自己署名付き証明書を使用して設定する必要があります。HTTPS 設定を行う (HTTPS を使用する場合) を参照してください。

注：自己署名付き証明書は任意の Windows サーバーに生成できます。サーバーに BACS がインストールされている必要はありません。Windows サーバーに生成された自己署名付き証明書は、クライアントのローカル ドライブにコピーされます。

1. **[スタート]** をクリックして (または Windows ロゴ キーを押して)、**[ファイル名を指定して実行]** を選択します。
2. 「**gpedit.msc**」と入力して、ローカルのグループ ポリシー エディタを開きます。
3. **[コンピュータの構成]** で、**[管理用テンプレート]** フォルダを開き、続いて **[Windows コンポーネント]** フォルダを開きます。
4. **[Windows リモート管理 (WinRM)]** を選択します。
5. **[Windows リモート管理 (WinRM)]** で、**[WinRm クライアント]** を選択します。
6. **[WinRM クライアント]** で、**[信頼されたホスト]** をダブルクリックします。
7. **[TrustedHostsList]** に、クライアントのホスト名を入力します。すべてのクライアントが信頼される場合は、アスタリスク (*) だけを入力します。
8. **[WinRM サービス]** を選択します。
9. **[基本認証を許可する]** を有効にします。

Windows サーバーの自己署名付き証明書を生成するには：

Windows で OpenSSL を使用し、次の手順に従って、自己署名付き証明書を生成することができます。

1. 次のコマンドを入力して秘密キーを生成します。
   `openssl genrsa -des3 -out server.key 1024`
2. パスフレーズの入力を要求されます。パスフレーズは忘れないようにしてください。
3. 次の手順に従って証明書の署名要求 (CSR) を生成します。

   CSR の生成中に、いくつかの情報の入力を要求されます。「共通名」の入力を要求された場合は、Windows サーバーのホスト名または IP アドレスを入力してください。

   次のコマンドを入力します (応答例も示されています)。

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

このコマンドが動作しない場合、次のコマンドを試してください。

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

openssl.cnf ファイルは、openssl が配置されているディレクトリと同じディレクトリに配置する必要があります。openssl.cnf は、C:\Program Files (x86)\GnuWin32\share フォルダに配置されています。

以下の情報が要求されます。

- 国名 (2 文字のコード) [] : **US**
- 都道府県名 (フルネーム) [] : **California**
- 地域名 (都市名など) [] : **Irvine**
- 組織名 (会社など) [] : **Broadcom Corporation**
- 組織単位名 (セクションなど) [] : **Engineering**
- 共通名 （ ユーザー名など ） [] : Windows サーバーのホスト名または IP アドレスを入力します。iPv6 の場合、[xyxy:xxx:….::xxx] という形式で共通名を入力します (**括弧 [ ] を含みます**)。
- (オプション) 電子メール アドレス [] :

証明書要求と併せて送信される、次の追加属性を入力します。

- チャレンジ パスワード [] : **password1**
- オプションの会社名 [] :

4. パスフレーズをキーから削除します。

次のコマンドを入力します。

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

5. 署名付き証明書を生成します。

365 日アクティブな署名付き証明書を生成するには、次のコマンドを入力します。

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

次の出力が表示されます。

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

6. 次のコマンドを入力して、生成された署名付き証明書を検証します。

```
openssl verify server.crt
```

次の出力が表示されます。

```
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
```

エラー メッセージ「error 18 at 0 depth lookup:self signed certificate」は無視してください。このエラーは、これが署名付き証明書であることを示すものです。

7. 次のようにして、証明書の形式を 「crt」から 「pkcs12」に変換します。

Windows サーバーの場合、証明書は pkcs12 の形式になっています。次のコマンドを入力します。

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

次のプロンプトが表示されます。

```
Enter Export Password:
```

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

パスワードを入力します。パスワードは忘れないでください。パスワードは、証明書を Windows サーバーおよびクライアントにインポートする際に必要です。

8. 証明書をインポートできるように、証明書ファイル server.crt のコピーを作成して BACS のインストール先のサーバーに置きます。BACS を実行しているサーバーへ Windows クライアントから接続する場合は、証明書をクライアントのシステムにも転送する (コピーして貼り付ける) 必要があります。

注：IPv4 アドレス、IPv6 アドレス、およびホスト名に個別の証明書を作成する必要があります。

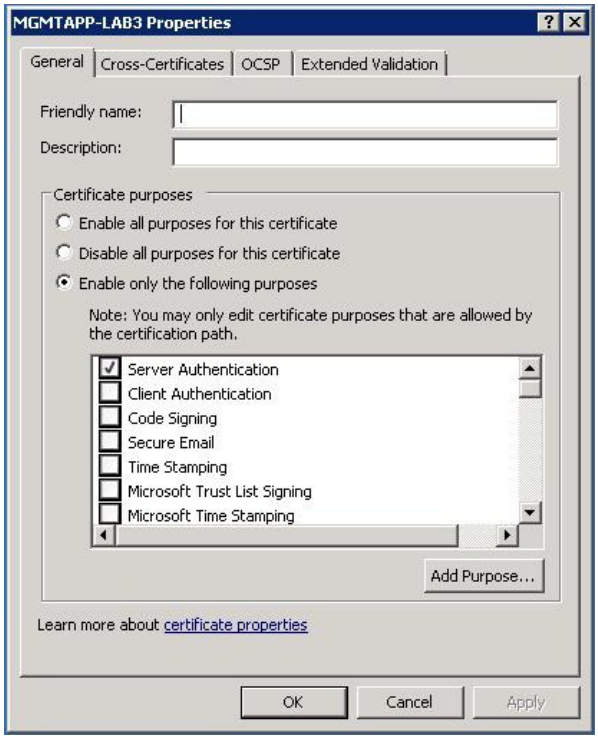
自己署名付き証明書を Windows サーバーにインストールするには :

生成したファイル *hostname*.pfx を Windows サーバーに転送してから、証明書をインストールします。

1. **[スタート]** をクリックして (または Windows ロゴ キーを押して)、**[ファイル名を指定して実行]** を選択します。
2. **「MMC」**と入力し、**[OK]** をクリックします。
3. **[ファイル]** > **[スナップインの追加と削除]** をクリックします。
4. **[追加]** をクリックします。
5. **[証明書]** を選択し、**[追加]** をクリックします。
6. **[コンピュータ アカウント]** を選択します。
7. **[次へ]** をクリックして、**[完了]** をクリックします。
8. **[閉じる]** をクリックして、**[OK]** をクリックします。
9. **[証明書 (ローカル コンピュータ)]** フォルダを開き、**[個人用]** フォルダを開きます。
10. **[証明書]** を右クリックし、**[All Tasks/ すべてのタスク]** を選択して、**[インポート]** をクリックします。
11. **[次へ]** をクリックして、証明書のインポート ウィザードを開始します。
12. **hostname.pfx** を指定して選択します。
13. 秘密キーのパスワードを要求された場合は、「Windows サーバーの自己署名付き証明書を生成するには : 」で作成したパスワードを入力します。
14. 画面の指示に従い、デフォルトの設定を選択して続行します。

    ウィンドウの右側に証明書がインストール済みとして表示されます。名前は、自己署名付き証明書の作成時に指定した名前になります。
15. 証明書を右クリックして **[プロパティ]** を選択します。

    次のようなダイアログ ボックスが表示されます。



16. 図のように **[サーバー認証]** だけが有効になっていることを確認します。

17. **[信頼されたルート証明機関]** を開き、**[証明書]** を開きます。

18.「ステップ 11.」から「ステップ 17.」の手順に従います。

注：自己署名付き証明書をクライアントにインポートする手順については、「HTTPS 設定を行う (HTTPS を使用する場合)」を参照してください。

手順 6：サーバーの WinRM HTTPS/SSL を設定する

1. 次のようにして WinRM リスナーを作成します。

a. **[スタート]** をクリックして (または Windows ロゴ キーを押して)、**[ファイル名を指定して実行]** を選択します。

b.「**MMC**」と入力し、**[OK]** をクリックします。

c. 自己署名付き証明書を個人用ストアから選択します。

たとえば、ホスト名を指定して証明書を作成した場合、ホスト名が表示されます。

d. 証明書をダブルクリックして開きます。

e. **[詳細]** タブをクリックします。

f. スクロール ダウンして **[捺印]** フィールドを選択します。

g. **[詳細]** ウィンドウで捺印を選択してコピーします。これで次の手順で捺印を挿入できます。

h. コマンド プロンプトに戻ります。

i. 次のコマンドを入力します。

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

メモ：

- ホスト名を指定して証明書を作成した場合は、ホスト名を入力します。IP アドレスを指定して生成した場合は、その IP アドレスを入力します。IPv6 アドレスの場合、括弧 [ ] を使用してアドレスを囲みます。
- システムで HTTPS で設定されている場合、リスナーを削除してから、新しい HTTPS リスナーを作成する必要があります。次のコマンドを使用します。
  `winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`

j. 上記のコマンドは、サーバーの任意またはすべてのネットワーク アドレス、および my SelfSSL で生成された証明書を使用して、HTTPS ポート (5986) にリスナーを作成します。

k. WinRM リスナーは任意のユーザー定義ポート上に設定できるため、`winrm` コマンドを使用して HTTPS リスナーを変更または設定することができます。

l. コマンド プロンプトで次のコマンドを実行して、リスナーが設定されていることを検証します。
```
winrm e winrm/config/listener
```

2. サーバーの HTTPS/SSL 接続をテストします。

a. サーバーのコマンド プロンプトで、次のコマンドを入力します。
```
winrs -r:https://yourserver:5986 -u:username -p:password hostname
```

b. セットアップが正しければ、コマンドの出力にサーバーのホスト名が表示されます。

c. WinRM のサービス構成を確認するには、次のコマンドを実行します。
```
winrm get winrm/config/service
```

手順 7：追加のサーバー設定

必要に応じて、ファイアウォールの規則を次のように変更します。

Windows Server 2008 R2

1. **[管理ツール]** メニューから、**[セキュリティが強化された Windows ファイアウォール]** を開きます。
2. **[受信の規則]** を右クリックし、**[新しい規則]** を選択します。
   新しい規則ウィザードが開きます。
3. **[ポート]** を選択して **[次へ]** をクリックします。
4. **[プロトコルおよびポート]** 画面で、**[TCP]** を選択し、特定のポートを入力します。たとえば、HTTP の場合は 5985、HTTPS の場合は 5986 を入力します。
5. **[次へ]** をクリックします。
6. **[アクション]** 画面で、**[接続を許可する]** を選択して **[次へ]** をクリックします。
7. **[プロファイル]** には、サーバーがワークグループに属していれば、3 つすべてのプロファイルを選択できます。
8. 規則の名前を指定し、**[完了]** をクリックします。
9. 新しい規則が有効になっていること (緑のチェック ボックスがオンになっていること) を確認します。

Windows XP

1. **[スタート]** > **[コントロール パネル]** をクリックし、**[Windows ファイアウォール]** をダブルクリックします。
2. **[例外]** タブをクリックします。
3. **[ポートの追加]** をクリックします。
4. わかりやすい**名前** (たとえば “WinRM 規則 ”) とポート番号 (HTTP の場合は 5985、HTTPS の場合は 5986) を入力します。
5. **[OK]** をクリックします。

便利な WinRM コマンド

コマンド	*説明*
`winrm quickconfig or winrm qc`	デフォルトの設定で WinRM を設定します。
`winrm enumerate winrm/config/Listener or winrm e winrm/config/Listener`	有効になっているサービス リスナーとリスニングの対象のポートおよび IP アドレスを確認します。
`winrm get winrm/config/Service`	WinRM のサービス構成を確認します。
`winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`	リスナーを削除します (この場合は HTTPS リスナーを削除)。

WinRM に関する役立つ Web サイト

- 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
- http://support.microsoft.com の次の記事 :
  - “Configuring WINRM for HTTPS” (英語)
  - “Windows Management Framework (Windows PowerShell 2.0、WinRM 2.0、および BITS 4.0)”

Windows クライアントへの WS-MAN のインストール

Windows クライアントで、次の設定手順を実行します。

1. HTTP 設定を行う (HTTP を使用する場合)
   a. **[スタート]** をクリックして (または Windows ロゴ キーを押して)、**[ファイル名を指定して実行]** を選択します。
   b. 「**gpedit.msc**」と入力して、ローカルのグループ ポリシー エディタを開きます。
   c. **[コンピュータの構成]** で、**[管理用テンプレート]** フォルダを開き、続いて **[Windows コンポーネント]** フォルダを開きます。
   d. **[Windows リモート管理 (WinRM)]** を選択します。
   e. **[Windows リモート管理 (WinRM)]** で、**[WinRm クライアント]** を選択します。
   f. **[WinRM クライアント]** で、**[信頼されたホスト]** をダブルクリックします。
   g. **[TrustedHostsList]** に、クライアントのホスト名を入力して **[OK]** をクリックします。すべてのクライアントが信頼される場合は、「*」だけを入力します。
   h. **[WinRM サービス]** を選択します。
   i. **[基本認証を許可する]** を有効にして **[OK]** をクリックします。
   j. コマンド プロンプトで次のコマンドを実行して、接続をテストします。
      `winrm id -remote:<remote machine Hostname or IP Address>`
2. HTTPS 設定を行う (HTTPS を使用する場合)

   「Windows サーバーの自己署名付き証明書を生成するには :」の説明に従って自己署名付き証明書を生成したら、証明書をクライアントにインポートしてサーバーとクライアント間をスムーズに接続することができます。セクション「Windows サーバーの自己署名付き証明書を生成するには :」で説明している手順 (クライアントがアクセスできる場所への *hostname.pfx* のコピーも含む) をすべて実行してから、次の手順に進んでください。

   a. **[スタート]** をクリックして (または Windows ロゴ キーを押して)、**[ファイル名を指定して実行]** を選択します。
   b. 「**MMC**」と入力し、**[OK]** をクリックします。
   c. **[ファイル]** をクリックして、**[スナップインの追加と削除]** を選択します。
   d. **[追加]** をクリックします。
   e. **[証明書]** を選択し、**[追加]** をクリックします。

f. **[コンピュータ アカウント]** を選択して **[次へ]** をクリックします。
g. [**完了**] をクリックします。
h. **[閉じる]** をクリックして、**[OK]** をクリックします。
i. **[証明書 (ローカル コンピュータ)]** で、**[信頼されたルート証明機関]** を右クリックして、**[All Tasks/ すべてのタスク]** を選択し、**[インポート]** を選択します。
j. **[次へ]** をクリックして、証明書のインポート ウィザードを開始します。
k. 「Windows サーバーの自己署名付き証明書を生成するには:」で生成した .pfx ファイルを指定して選択します。**[ファイルの種類]** の一覧の選択内容を **[Personal Information Exchange (*.pfxas, *.p12)]** に変更し、*hostname.pfx* ファイルを選択して **[開く]** をクリックします。
l. 秘密キーに割り当てたパスワードを入力して **[次へ]** をクリックします。

3. WinRM HTTPS/SSL を設定する

クライアントから `winrm` を実行し、WinRM THHPS 接続を使用してサーバーから情報を取得することができます。WinRM HTTPS/SSL 接続をクライアントからテストするには、次の手順に従います。

a. サーバーのオペレーティング システムの情報を取得するには、次のコマンドを入力します。
```
winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername -u:username
-p:password -skipCAcheck
```
b. サーバーの WinRM ID 情報を取得するには、次のコマンドを入力します。
```
winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
```
c. サーバーの Windows サービスの一覧を作成するには、次のコマンドを入力します。
```
winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -
skipCAcheck
```

注 : 証明書は自動生成されますがクライアントにはインポートされないため、`winrm` コマンド ライン テストで `-skipCAcheck` スイッチを使用することが重要です。そうしないと、`WSManFault` というエラー メッセージが表示されます。

WMI を使用する

WMI を Windows クライアント上で使用する場合、特別な設定は不要です。WMI を Windows サーバー上で設定するには、次のセクションの手順を実行します。

手順 1：WMI コントロールを使用して名前空間のセキュリティを設定する

WMI コントロールを使用して名前空間のセキュリティを管理できます。WMI コントロールは、次のコマンドを使用してコマンド プロンプトから開始できます。

```
wmimgmt
```

WMI がインストールされている Windows 9x または Windows NT4 のコンピュータでは、代わりに次のコマンドを使用します。

```
wbemcntl.exe
```

あるいは、次のようにして WMI コントロールとその [セキュリティ] タブにアクセスすることもできます。

1. **[マイ コンピュータ]** を右クリックして **[管理]** をクリックします。
2. **[サービスとアプリケーション]** をダブルクリックして、**[WMI コントロール]** をダブルクリックします。
3. **[WMI コントロール]** を右クリックして、**[プロパティ]** をクリックします。
4. [WMI コントロールのプロパティ] で、**[セキュリティ]** タブをクリックします。
5. 横にプラス記号 (+) の付いた Root という名前のフォルダが表示されます。必要に応じてこのツリーを展開し、アクセス許可を設定する名前空間を探します。
6. **[セキュリティ]** をクリックします。

   ユーザーとユーザーのアクセス許可の一覧が表示されます。ユーザーが一覧に表示されている場合は、アクセス許可を適宜に変更します。ユーザーが一覧に表示されていない場合は、**[追加]** をクリックし、アカウントのある場所 (ローカル マシンやドメインなど) からユーザーを追加します。

注： これらのエクスポートは .bash_profile の最後に追加できます。このファイルは /root ディレクトリにあります。

- 名前空間のセキュリティを表示して設定するためには、セキュリティの読み取りおよびセキュリティの編集のアクセス許可がユーザーに必要です。管理者はこれらのアクセス許可をデフォルトで持っているため、必要に応じて権限を他のユーザー アカウントに割り当てることができます。
- ユーザーが名前空間にリモートからアクセスできるようにするには、リモートの有効化のアクセス許可を選択する必要があります。
- デフォルトでは、名前空間に対して設定されたユーザーのアクセス許可が適用されるのは、該当する名前空間に限られます。名前空間とその下のツリーのすべてのサブ名前空間へのアクセス権、またはサブ名前空間内のみのアクセス権をユーザーに付与するには、**[詳細設定]** をクリックします。**[編集]** をクリックし、表示されるダイアログ ボックスにアクセスの範囲を指定します。

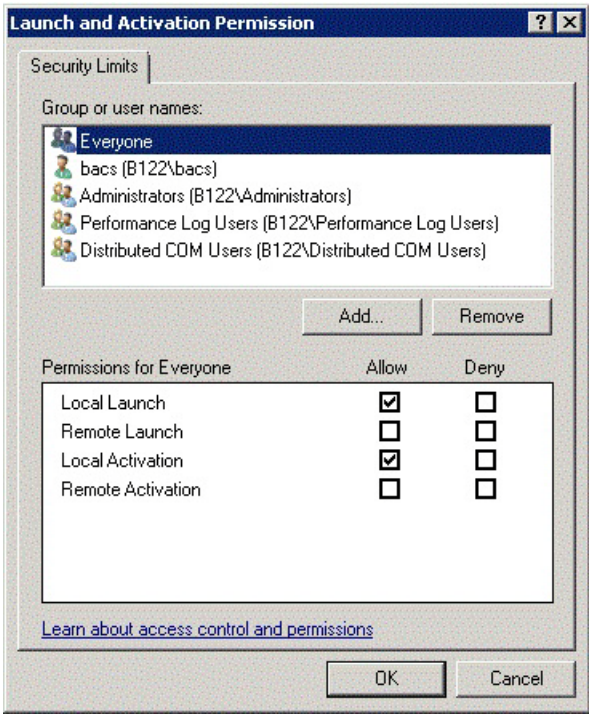
手順 2：DCOM のリモートからの起動およびアクティブ化のアクセス許可を付与する

Windows ドメイン環境では、ドメイン管理者は BACS 管理用 WMI コンポーネントにアクセスするのに必要な特権レベルを持っているため、特別な設定は不要です。ただし大企業においては、BACS4 クライアント GUI を使用してローカルまたはリモートのホストにアクセスするユーザーが必ずしもドメイン管理者のアカウント権限を有しているとは限りません。そのため、ユーザーが BACS4 クライアント GUI を使用してリモート ホストにアクセスできるように、WMI のセキュリティ アクセス権をリモート ホスト上で設定する必要があります。

この設定は、次の手順に従って簡単に実行できます。WMI のセキュリティ アクセスを設定するための十分な権限がない場合は、ネットワーク管理者に問い合わせてください。

1. **[スタート]**、**[ファイル名を指定して実行]** をクリックし、「**DCOMCNFG**」と入力して **[OK]** をクリックします。
2. [コンポーネント サービス] ダイアログ ボックスが表示されます。
3. **[コンポーネント サービス]** を開き、**[コンピュータ]** を開きます。
4. **[マイ コンピュータ]** を右クリックして **[プロパティ]** をクリックします。
5. **[My Computer Properties/ コンピュータのプロパティ]** で、**[COM Security/COM セキュリティ]** タブをクリックします。
6. **[起動とアクティブ化のアクセス許可]** で、**[制限の編集]** をクリックします。
7. 自分の名前またはグループが **[グループまたはユーザー名]** の一覧に表示されない場合は、次の手順を実行します。
   a. [Launch Permission/ 起動のアクセス許可] ダイアログ ボックスで、**[追加]** をクリックします。
   b. [ユーザー、コンピュータ、またはグループの選択] ダイアログ ボックスで、**[選択するオブジェクト名を入力してください]** ボックスに自分の名前とグループを追加して、**[OK]** をクリックします。
   c. [Launch Permission/ 起動のアクセス許可] ダイアログ ボックスで、**[グループまたはユーザー名]** の一覧から自分のユーザー名とグループを選択します。
   d. **[Permissions for User/ ユーザーのアクセス許可]** の領域で、**[リモートからの起動]** と **[リモートからのアクティブ化]** に **[許可]** を選択して、**[OK]** をクリックします。

図 8: 起動とアクティブ化のアクセス許可



詳細については、マイクロソフトの開発者向け情報サイト (MSDN) の「Securing a Remote WMI Connection 」(英語) を参照してください。

異なるシステムにおける WMI の特別な設定

Windows Vista および Windows 7 では、管理者グループのすべてのユーザーに WMI 名前空間を使用して接続させるためには、必要に応じて LocalAccountTokenFilterPolicy を変更する必要があります。

セクション 13:Broadcom Advanced Control Suite 4 を使用する

Broadcom Advanced Control Suite の概要

Broadcom Advanced Control Suite (BACS) は、統合型ユーティリティであり、システムにインストールされている各ネットワーク アダプタに関する役に立つ情報を提供します。BACS では、各アダプタの詳細なテスト、診断、分析を実行できるうえ、プロパティ値の表示と変更やネットワーク オブジェクトのトラフィック情報も表示できます。BACS は Windows OS 上および Linux OS 上で動作します。

Broadcom Advanced Server Program (BASP) は Broadcom Advanced Control Suite 内で実行され、ロード バランシング、フォルト トレランス、VLAN (Virtual Local Area Network) のチームの設定に使用します。BASP の機能は、Broadcom ネットワーク アダプタを少なくとも 1 つ装備しているシステムでのみ使用可能です。BASP は Windows OS 上でのみ動作します。

注：BACS の一部の機能は、特定のアダプタにのみ該当します。BACS の単一インスタンスを使用して複数のホストおよびアダプタ タイプと通信することができるので、このドキュメントではすべての BACS 機能について説明します。

BACS アプリケーションには、グラフィック ユーザー インターフェイスとコマンド ライン インターフェイス (BACSCLI) があります。BACS GUI と BACS CLI は、次のオペレーティング システム ファミリで使用できます。

- Windows
- Windows Server
- Linux Server

サポート対象 OS の最新のバージョンについては、ご使用のソフトウェア ディストリビューションに提供されているリリースに関する文書類を参照してください。

Broadcom Advanced Control Suite を起動する

[コントロール パネル] で **[Broadcom Control Suite 4]** をクリックするか、Windows または Windows Server デスクトップの一番下にあるタスクバーで BACS アイコンをクリックします。

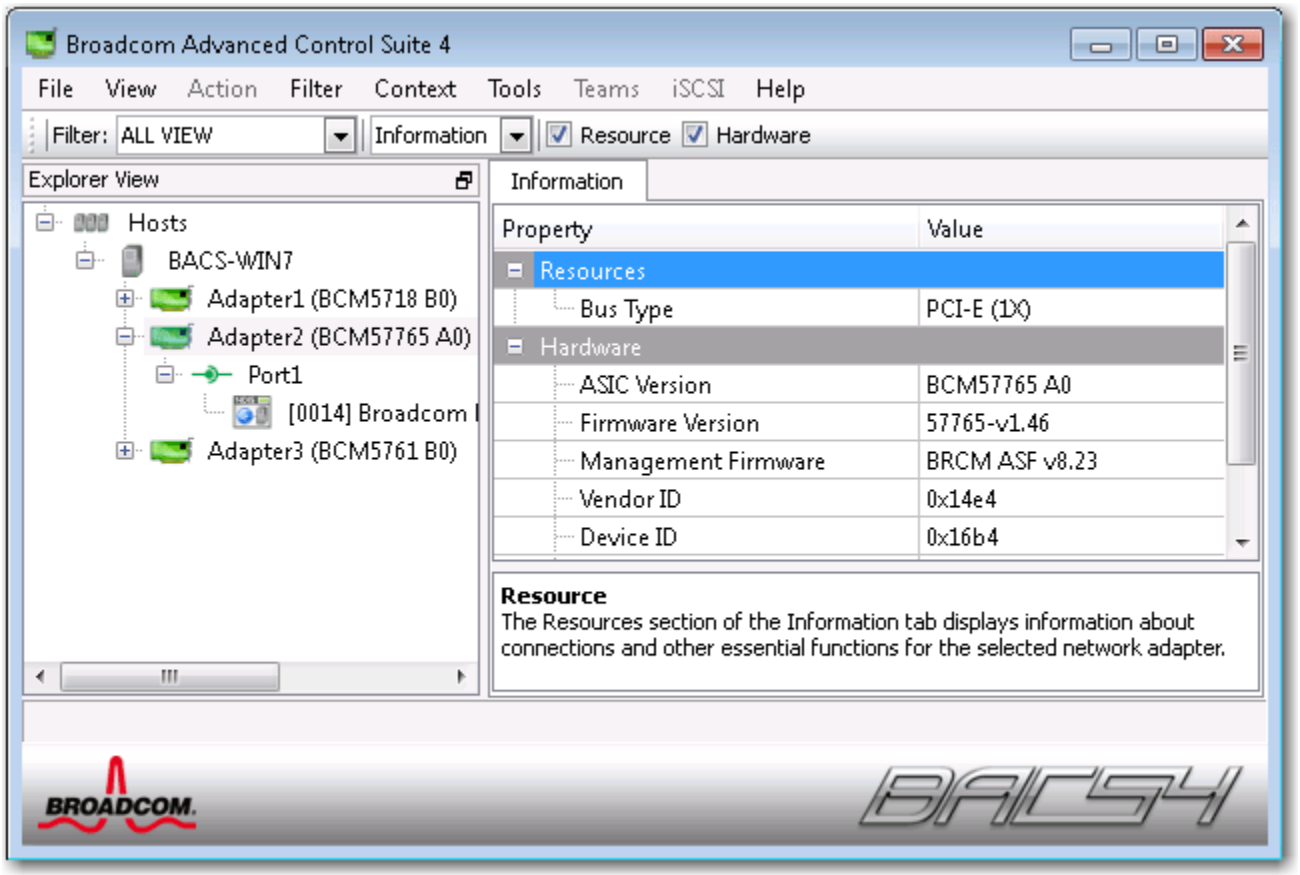
Linux システムでは、BACS4 デスクトップ アイコンをダブルクリックするか、**[System Tools]** の下にあるタスク バーから BACS プログラムにアクセスすることができます。(Linux システムでの BACS の起動に問題がある場合、BACS のトラブルシューティングにある関連トピックを参照してください。)

BACS インターフェイス

BACS インターフェイスは、次の各領域で構成されています。

- [エクスプローラ ビュー] ペイン
- コンテキスト ビュー セレクタ
- [コンテキスト ビュー] ペイン
- メニュー バー
- [説明] ペイン

デフォルトでは、[エクスプローラ ビュー] ペインはメイン ウィンドウの左側のドックに配置され、[コンテキスト ビュー] ペインは右側に配置されています。[コンテキスト ビュー] セレクタはメニュー バーの下にあり、[説明] ペインは [コンテキスト ビュー] ペインの下にあります。ペインのサイズを変更するには、2 つのペインの間にある分割線をドラッグします。



[エクスプローラ ビュー] ペイン

[エクスプローラ ビュー] ペインは、メイン ウィンドウの左側、右側、上側、下側のドックに配置することができます。

[エクスプローラ ビュー] ペインには、BACS で表示、分析、テスト、または設定できるオブジェクトが一覧表示されます。[エクスプローラ ビュー] ペインで項目を選択すると、その項目で使用できる情報やオプションが [コンテキスト ビュー] ペインのタブに表示されます。

このパネルの構成は、管理可能なオブジェクトをドライバやそのサブコンポーネントと同じ階層形式で表示するように設計されています。このパネルにより、コンバージド ネットワーク インターフェイス コントローラのさまざまな要素を管理しやすくなっています。階層の最上位は [ホスト] コンテナであり、BACS で管理されるすべてのホストが一覧表示されます。ホストの下には、インストール済みのネットワーク アダプタが表示され、アダプタの下には、物理ポート、NDIS、iSCSI など、管理可能な要素が表示されます。

[エクスプローラ ビュー] ペインの各デバイスの隣に表示されるアイコンは、ステータスを示します。デバイス名の隣のアイコンが通常どおりに表示されている場合は、デバイスが接続され、機能していることを示します。

- **X の場合**：デバイスのアイコンに赤い「X」が表示されている場合は、デバイスが現在ネットワークに接続されていないことを示します。
- **グレーの場合**： デバイスのアイコンがグレーで表示されている場合は、デバイスが現在無効になっていることを示します。

コンテキスト ビュー セレクタ

[コンテキスト ビュー] セレクタは、メニュー バーの下に表示され、フィルタやタブ カテゴリが含まれます。[コンテキスト ビュー] ペインでは、タブに表示されるカテゴリを展開したり折りたむことができますが、カテゴリ名の横にあるボックスをオンにして、カテゴリを表示することも可能です。

[フィルタ] ビュー

複数の C-NIC を使用した複数のホスト環境では、アダプタごとに管理可能な要素が多く存在している可能性があります。この場合、すべての要素の表示、設定、および管理は困難になり、手間がかかる可能性があります。特定のデバイスの機能を選択するには、フィルタを使用します。次のようなフィルタ ビューがあります。

- すべて
- チーム ビュー
- NDIS ビュー
- iSCSI ビュー
- iSCSI ターゲット ビュー

[コンテキスト ビュー] ペイン

[コンテキスト ビュー] ペインには、[エクスプローラ ビュー] ペインで選択したオブジェクトに関連するすべての表示可能なパラメタが表示されます。パラメタは、パラメタの種類に応じてタブとカテゴリでグループ化されます。利用可能なタブは、[情報]、[設定]、[診断]、および [統計] です。BACS のインターフェイスはコンテキストに対応するため、[コンテキスト ビュー] ペインには、選択したオブジェクトに適用されるパラメタのみが表示され、調整することができます。

メニュー バー

メニュー バーには次の項目が表示されますが、メニュー項目はコンテキストに基づくため、常にすべての項目が表示されるとは限りません。

[ファイル] メニュー

- [チームに名前を付けて保存] : 現在のチーム設定をファイルに保存します。
- [チームの復元] : 保存済みのチーム設定をファイルから復元します。

[アクション] メニュー

- [ホストの削除] : 選択したホストを削除します。
- [ホストの情報を最新に更新] : 選択したホストの情報を最新に更新します。

[表示] メニュー

- [エクスプローラ ビュー] : [エクスプローラ ビュー] ペインの表示 / 非表示を切り替えます。
- [ツール バー] : ツール バーの表示 / 非表示を切り替えます。
- [ステータス バー] : ステータス バーの表示 / 非表示を切り替えます。
- [Broadcom ロゴ] : 表示領域を最大にするために、BACS で Broadcom ロゴの表示 / 非表示を切り替えます。

[ツール] メニュー

- [オプション] : BACS の設定に使用します。

[Teams/ チーム化] (Windows のみ)

- [Create Teams/ チームを作成] : [チーム化ウィザード] または [詳細設定] モードで新しいチームを作成します。
- [チームの管理] : [チーム化ウィザード] または [詳細設定] モードで既存のチームを管理します。

[説明] ペイン

[説明] ペインでは、[コンテキスト ビュー] ペインで選択したパラメタの情報、設定手順、およびオプションが表示されます。

Windows での環境設定の指定

Windows で BACS トレイ アイコンを有効 / 無効にするには :

Windows システムで BACS のプログラムがインストールされると、Windows のタスクバーにアイコンが表示されます。このアイコンは [オプション] ウィンドウを使用してオン / オフできます。

1. **[ツール]** メニューの **[オプション]** を選択します。
2. **[BACSTray の有効化]** をオン / オフにします (このオプションはデフォルトでオンになっています)。
3. **[OK]** をクリックします。

Windows でのチーム化モードの設定

1. **[ツール]** メニューの **[オプション]** を選択します。
2. チームの作成時にチーム化ウィザードを使用する必要がない場合は、**[エキスパート モード]** を選択します。それ以外の場合、**[ウィザード モード]** を選択します。
3. **[OK]** をクリックします。

Windows でのエクスプローラ ビューの更新間隔の設定

1. **[ツール]** メニューの **[オプション]** を選択します。
2. **[自動]** を選択すると、エクスプローラ ビューの更新間隔は 5 秒に設定されます。それ以外の場合、[カスタム] を選択して、更新間隔を秒数で指定します。
3. **[OK]** をクリックします。

ホストへの接続

BACS では、管理する Windows ホストまたは Linux ホストを 1 つまたは複数追加できます。

ローカル ホストを追加するには、以下を実行してください。

1. **[アクション]** メニューから **[ホストの追加]** をクリックします。
2. Windows ホストと Linux ホストのどちらでも、デフォルトの設定は変更しないでください。ローカル ホストに接続する場合、**ユーザー名**と**パスワード**は不要です。
3. BACS でそのホストの情報を保存する場合は、**[持続]** を選択します。
4. **[OK]** をクリックします。現在、情報の表示とホストの管理のために、BACS を使用することができます。

リモート ホストを追加するには、以下を実行してください。

1. **[Action / アクション]** メニューから **[ホストの追加]** をクリックします。
2. リモート ホスト名または IP アドレスを **[ホスト]** ボックスに入力します。
3. **[プロトコル]** リストから、プロトコルを選択します。Windows のプロトコル オプションは、**[WMI]**、**[WSMan]**、または **[すべて試す]** です。Linux のプロトコル オプションは、**[CimXML]**、**[WSMan]**、または **[すべて試す]** です。**[すべて試す]** オプションを選択すると、GUI クライアントでは、すべてのオプションが強制的に試行されます。
4. **[HTTP]** スキームを選択します。また、強力なセキュリティが必要な場合は、**[HTTPS]** スキームを選択します。
5. ポート番号の値がデフォルトの **5985** と異なる場合は、ホストの設定に使用する値を **[ポート番号]** に入力します。
6. **ユーザー名**と**パスワード**を入力します。
7. BACS でそのホストの情報を保存する場合は、**[持続]** を選択します。BACS を再び開くと、エクスプローラ ペインにはホストが必ず表示されます。ホストに接続するときは、ホスト IP アドレスまたはホスト名を入力する必要はありません。セキュリティ上の理由により、**ユーザー名**と**パスワード**は毎回入力する必要があります。
8. **[OK]** をクリックします。

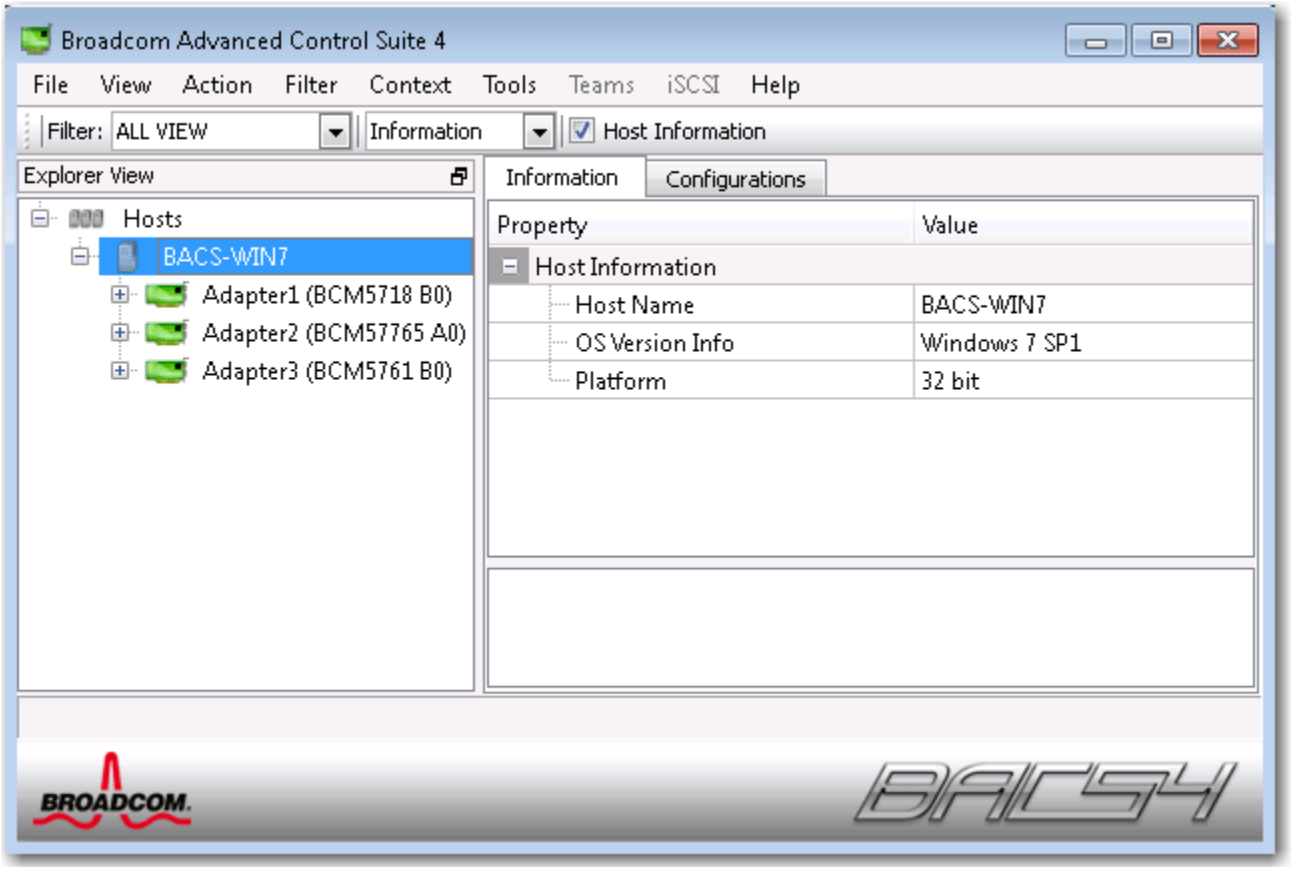
ホストの管理

ホスト レベルでは、ホスト情報を表示して、次のタブでパラメタを設定できます。

- 情報
- 構成

ホスト情報を表示するには、以下を実行してください。

[エクスプローラ ビュー] ペインでホストを選択し、**[情報]** タブを選択してホストレベルの情報を表示します。



[情報] タブ : [ホスト情報]

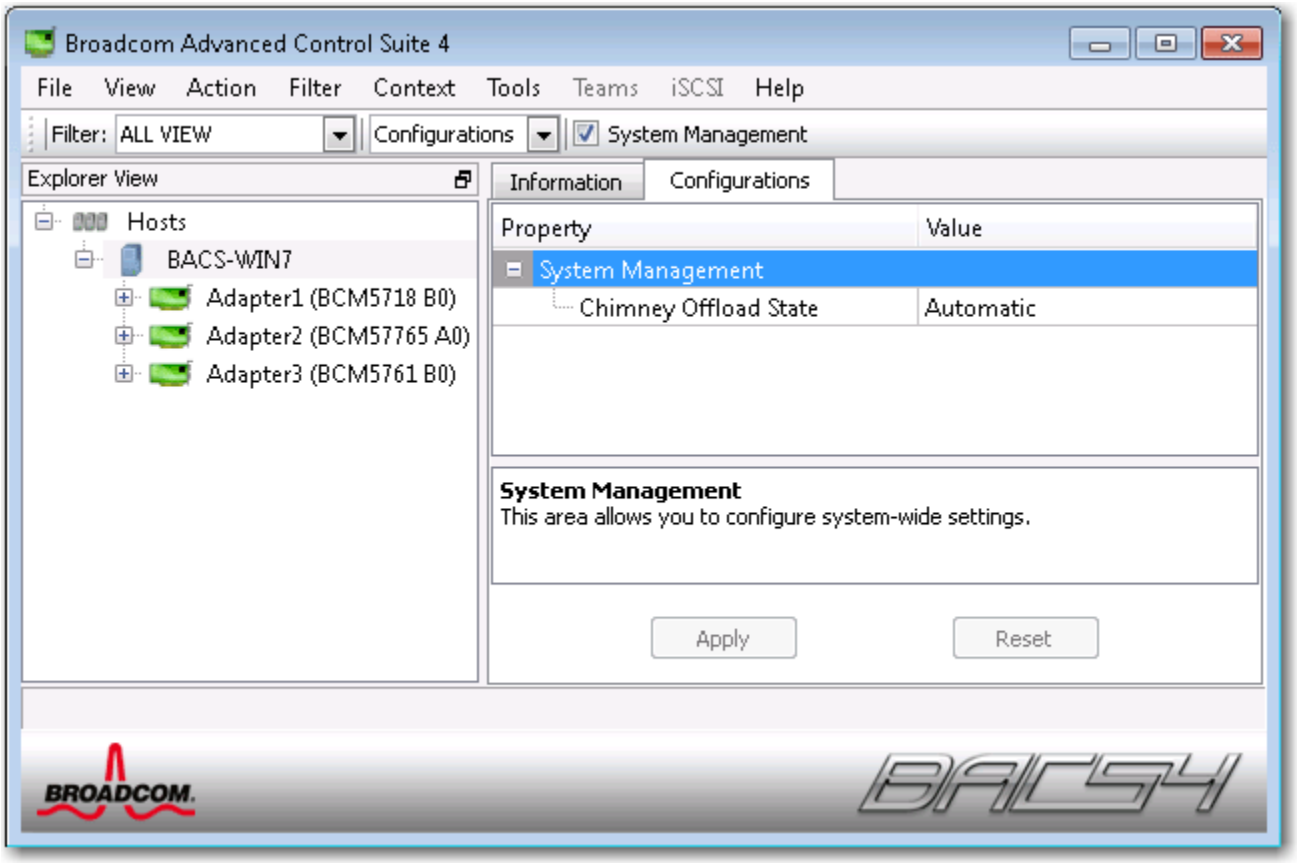
ホスト名 . ホスト名を表示します。

OS バージョン情報 . バージョンを含めて、オペレーティング システムを表示します。

プラットフォーム . ハードウェアのアーキテクチャ プラットフォーム (たとえば、32 ビットまたは 64 ビット) を表示します

ホストを設定するには、以下を実行してください。

[エクスプローラ ビュー] ペインでホストを選択し、**[設定]** タブを選択してホストレベルのパラメタを設定します。



ネットワーク アダプタの管理

[エクスプローラ ビュー] ペインの階層形式のツリーで、取り付けられたネットワーク アダプタが、ホストの 1 階層下のレベルに表示されます。アダプタ レベルでは、情報を表示して、次のタブでパラメタを設定できます。

- 情報
- 構成

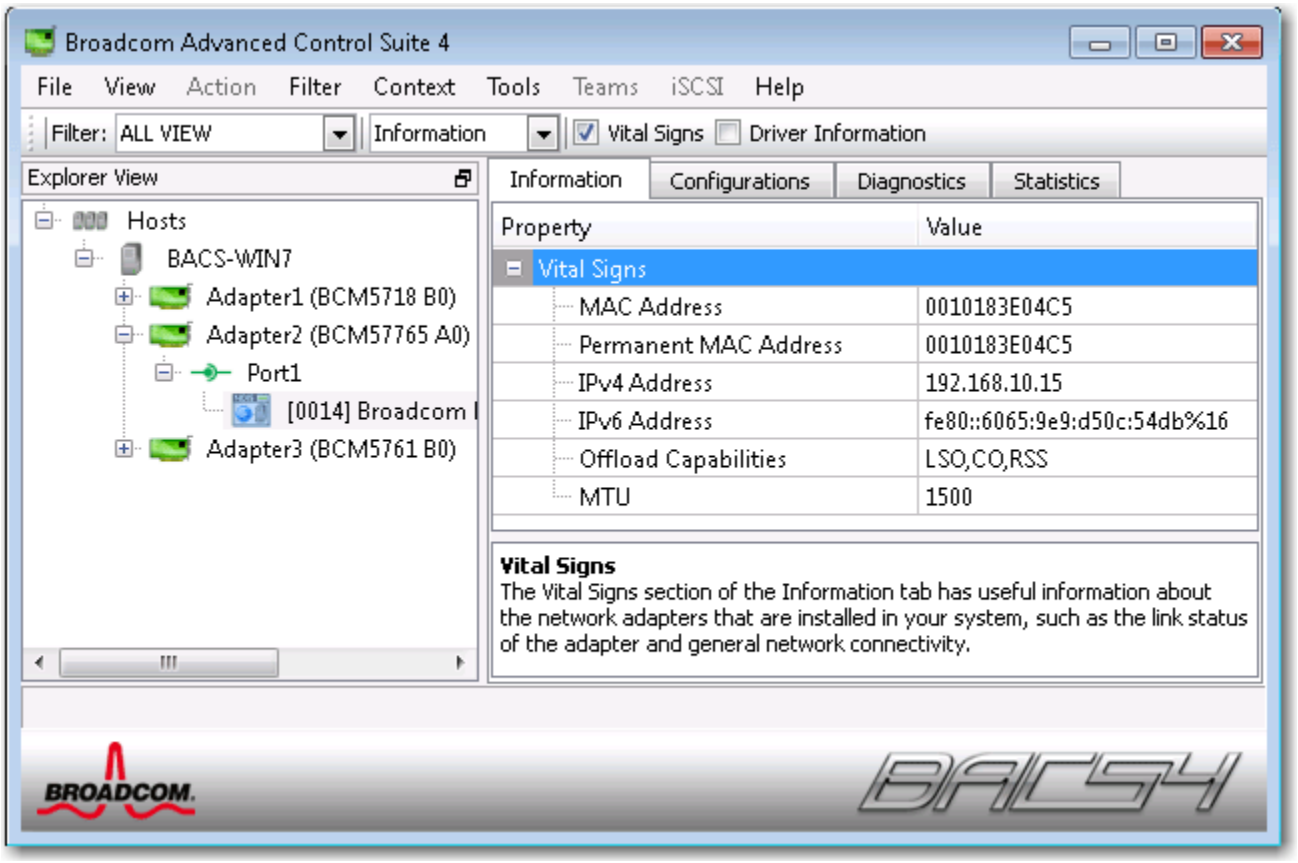
アダプタ情報の表示

[情報] タブの **[バイタル サイン]** セクションには、アダプタのリンク ステータスやネットワークの全体的な接続性など、システムにインストールされているネットワーク アダプタに関する役立つ情報が表示されます。

[エクスプローラ ビュー] ペインでネットワーク アダプタを選択し、**[情報]** タブを選択してアダプタ レベルの情報を表示します。

メモ：

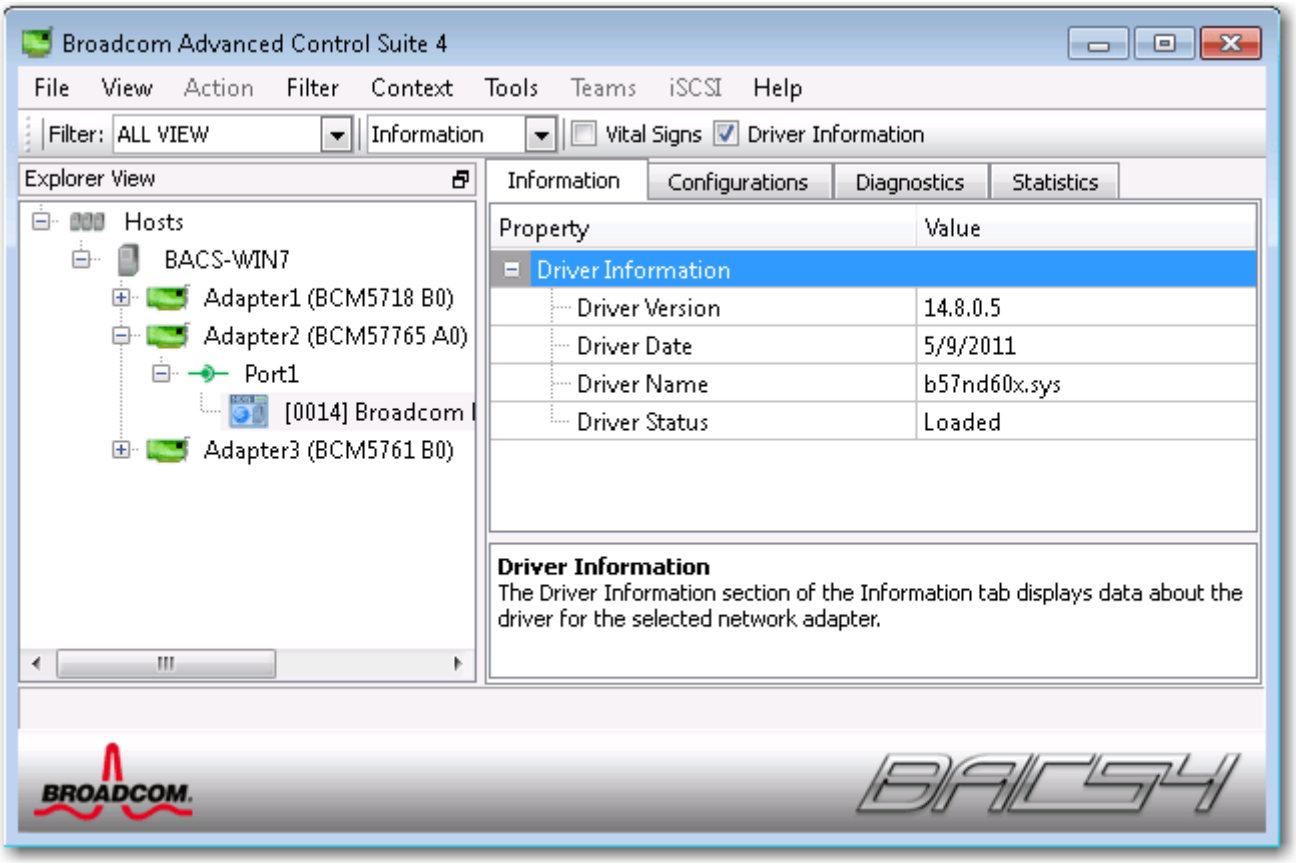
- Broadcom ネットワーク アダプタに関する情報は、他社のネットワーク アダプタの情報よりも広範囲にわたっていることがあります。
- Broadcom ネットワーク アダプタによっては、利用できない情報もあります。


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

ドライバ情報を表示する

[情報] タブの **[ドライバ情報]** セクションには、選択したネットワーク アダプタのドライバに関するデータが表示されます。

インストールされているネットワーク アダプタのドライバ情報を表示するには、[エクスプローラ ビュー] ペインに一覧表示されているアダプタの名前をクリックし、**[情報]** タブをクリックします。



ドライバ ステータス . アダプタ ドライバのステータスです。

- **ロード済み**：通常動作モードです。アダプタ ドライバはロードされ、動作しています。
- **ロード未完了**：アダプタに関連付けられているドライバは、Windows によってロードされていません。
- **利用不可**：アダプタに関連付けられているドライバから取得可能な値はありません。

ドライバ名 . アダプタ ドライバのファイル名です。

ドライバ バージョン . アダプタ ドライバの現在のバージョンです。

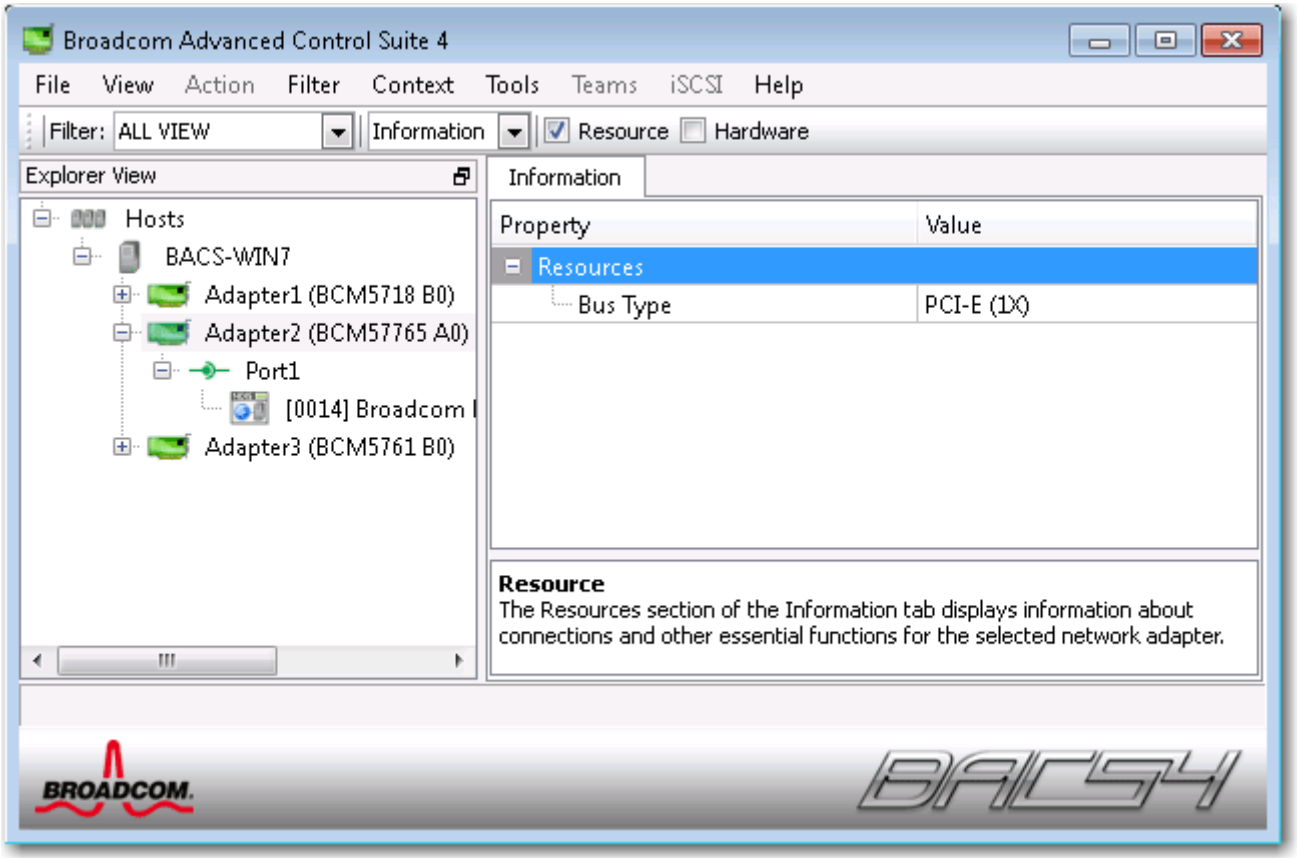
ドライバ更新日付 . アダプタ ドライバの作成日です。

リソース情報を表示する

[情報] タブの **[リソース]** セクションには、選択したネットワーク アダプタの接続やその他の必須機能に関する情報が表示されます。

インストールされているネットワーク アダプタのリソースを表示するには、[エクスプローラ ビュー] ペインに一覧表示されているアダプタの名前をクリックし、**[情報]** タブをクリックします。

注：Broadcom ネットワーク アダプタによっては、利用できない情報もあります。



バス タイプ . アダプタが使用する入力 / 出力 (I/O) インターコネクトのタイプです

スロット番号 . アダプタが使用するシステム ボード上のスロット番号です。PCI Express タイプのアダプタの場合、この項目は表示されません。

バス速度 (MHz). アダプタが使用するバス クロック シグナルの周波数です。PCI Express タイプのアダプタの場合、この項目は表示されません。

バス幅 (ビット). バスがアダプタとの間で一度に転送できるビット数です。PCI Express タイプのアダプタの場合、この項目は表示されません。

バス番号 . アダプタをインストールされたバスの番号を示します。

デバイス番号 . オペレーティング システムによってアダプタに割り当てられた番号です

機能番号 . アダプタのポート番号です。シングルポートのアダプタの場合、機能番号は 0 になります。2 ポートのアダプタの場合、最初のポートの機能番号は 0 に、2 つ目のポートの機能番号は 1 になります。

割り込み要求 . アダプタに関連付けられている割り込み線番号です。有効値の範囲は 2 ～ 25 です。

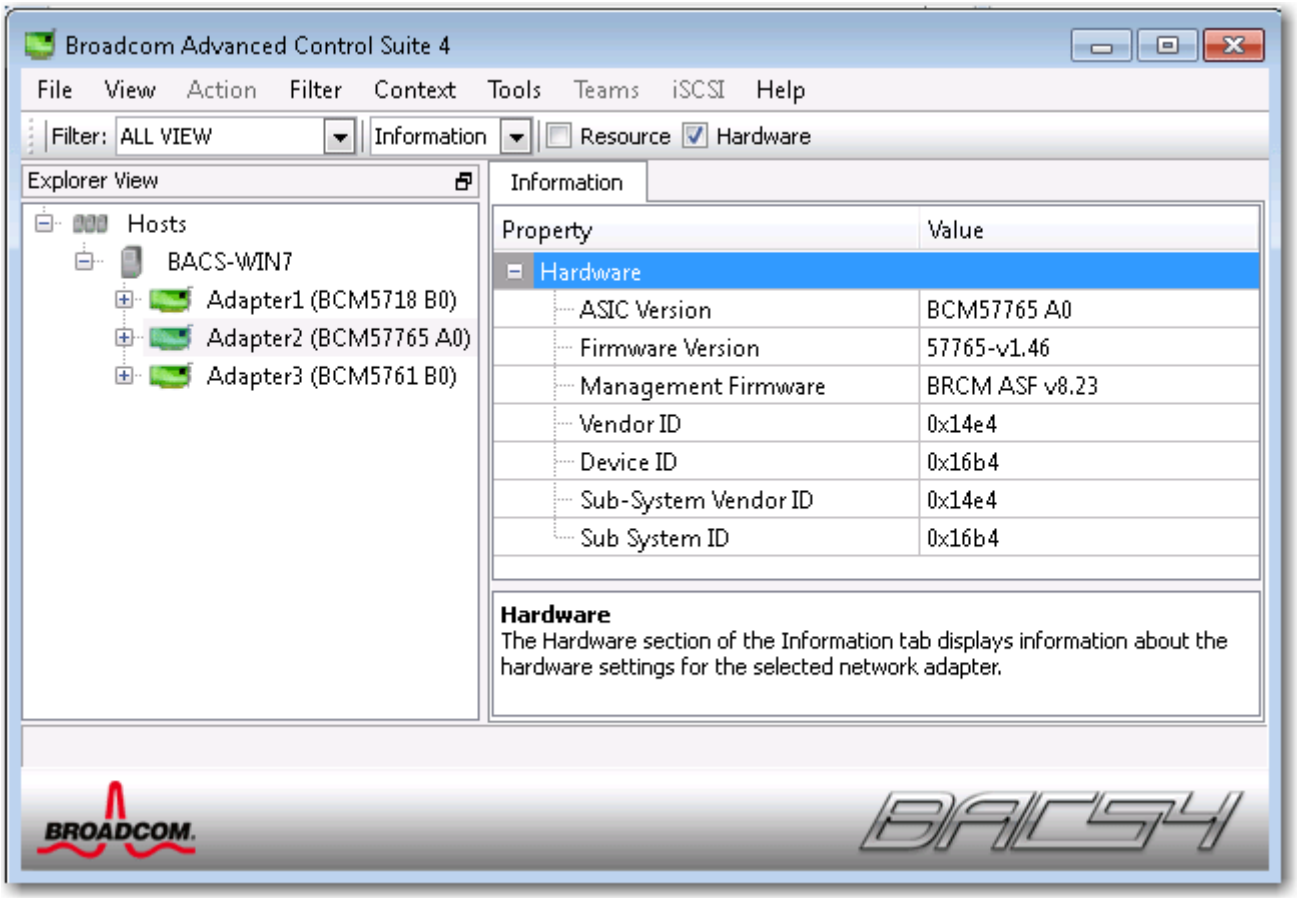
メモリ アドレス . アダプタに割り当てられている、メモリにマップされたアドレスです。この値が 0 になることはありません。

ハードウェア情報を表示する

[情報] タブの [ハードウェア] セクションには、選択したネットワーク アダプタのハードウェア設定に関する情報が表示されます。

インストールされているネットワーク アダプタのハードウェアを表示するには、[エクスプローラ ビュー] ペインに一覧表示されているアダプタの名前をクリックし、[情報] タブをクリックします。

注：Broadcom ネットワーク アダプタによっては、利用できない情報もあります。



ASIC バージョン . Broadcom アダプタのチップ バージョンです (他社製アダプタの場合には、この情報は表示されません)。

ファームウェア バージョン . Broadcom アダプタのファームウェア バージョンです (他社製アダプタの場合には、この情報は表示されません)。この情報が利用できるのは、Broadcom NetXtreme アダプタだけです。

ベンダ ID. ベンダ ID です。

デバイス ID. アダプタ ID です。

サブシステムベンダ ID. サブシステム ベンダ ID です。

サブシステム ID. サブシステム ID です。

ネットワークをテストする

[診断] タブの **[ネットワーク テスト]** オプションで、IP ネットワークの接続性を確認できます。このテストは、ドライバが正しくインストールされているかどうかを確認し、また、同一サブネット上で他に指定されている IP アドレスやゲートウェイへの接続性を検証します。ネットワーク テストでは、TCP/IP を使用して ICMP パケットをリモート システムに送信し、応答を待ちます。

注 : ネットワーク テスト オプションは、チームにグループ化されているアダプタでは使用できません (チームの設定を参照してください)。

ネットワーク テストを実行するには :

1. [エクスプローラ ビュー] ペインで、テストするアダプタの名前をクリックします。
2. **[実行するテストを選択]** リストから **[ネットワーク テスト]** を選択します。**[ネットワーク テスト]** オプションを使用できない場合は、ウィンドウの右側にある **[コンテキスト ビュー]** タブから **[診断]** を選択し、**[ネットワーク テスト]** を選択します。
3. 宛先の IP アドレスを変更するには、**[ping する IP アドレス]** を選択します。[ネットワーク テスト] ウィンドウで、宛先の IP アドレスを入力して **[OK]** をクリックします。
4. **[テスト]** をクリックします。

ネットワーク テストの結果が **[ステータス]** フィールドに表示されます。

診断テストを実行する

[診断] タブの **[診断テスト]** オプションで、Broadcom ネットワーク アダプタの物理コンポーネントの状態を確認できます。手動でテストを開始することも、BACS 3 でテストを継続的に実行することもできます。テストを継続的に実行する場合は、テストが実行されるたびにそのテストの **[結果]** フィールドにパスおよび失敗の数が加算されます。たとえば、テストが 4 回実行され、失敗がなかった場合、**[結果]** フィールドの値は 4/0 となります。これに対し、パスが 3 回で失敗が 1 回あった場合は 3/1 となります。

メモ：

- 診断テストを実行するには、管理者特権が必要です。
- これらのテストの実行中には、ネットワーク接続が一時的に失われます。
- 各テストをサポートしていない Broadcom アダプタもあります。

診断テストを 1 回実行するには：

1. [エクスプローラ ビュー] ペインでテストするアダプタの名前をクリックし、[診断] タブを選択します。
2. **[実行するテストを選択]** リストから **[診断テスト]** を選択します。
3. 実行する診断テストを選択します。すべてのテストを選択する場合は **[すべて選択]**、テストの選択をすべて解除する場合は **[すべてクリア]** を選択します。
4. **[ループ数]** から、テストを実行する回数を選択します。
5. **[テストの実行]** をクリックします。
6. ネットワーク接続が一時的に中断されることを警告するエラー メッセージ ウィンドウで、**[はい]** をクリックします。結果が、各テストの **[結果]** フィールドに表示されます。

制御レジスタテスト . このテストはネットワーク アダプタ レジスタの読み書き能力を検証するもので、レジスタに対してさまざまな値を書き込み、その結果を検証します。アダプタ ドライバはネットワーク コントローラ レジスタを使用し、データ送受信などのネットワーク機能を実行します。テストに失敗した場合は、アダプタが正しく動作していない可能性があります。

MII レジスタ . このテストは、物理層 (PHY) のレジスタの読み書き能力を検証します。物理層は、ワイヤ上の電気信号を制御するため、および、ネットワーク速度を設定 (1,000 Mbit/ 秒など) するために利用されています。

EEPROM. このテストは、EEPROM (Electrically Erasable Programmable Read-only Memory) の一部を読み出し、チェックサムをコンピュータ計算して EEPROM のコンテンツを検証します。コンピュータ計算したチェックサムが EEPROM 内に保存されているチェックサムと異なる場合、テストは失敗となります。EEPROM イメージのアップグレードでは、このテストのコードを変更する必要はありません。

内部メモリ . このテストでは、アダプタの内部メモリが正しく機能しているかを確認します。テスト時は、パターン化された値をメモリに書き込み、その結果を読み出します。誤った値が読み戻されると、テストは失敗となります。内部メモリが正しく機能していないと、アダプタは機能しません。

チップ上 CPU. このテストでは、アダプタ内の内部 CPU の動作を検証します。

キャンセル . このテストでは、NDIS (Network Device Driver Interface Specification) ドライバがアダプタからの割り込みを受信できるかどうかを検証します。

ループバック - MAC. このテストでは、NDIS ドライバとアダプタ間でパケットの送受信ができるかどうかを検証します。

ループバック - PHY. このテストでは、NDIS ドライバとアダプタ間でパケットの送受信ができるかどうかを検証します。

LED テスト . このテストでは、特定のアダプタを識別するために、すべてのポート LED を 5 回点滅させます。

ケーブルを分析する

[診断] タブの **[ケーブル分析]** オプションでは、イーサネット ネットワーク内にあるイーサネット カテゴリ 5 ケーブル接続の各ワイヤの組み合わせの状態をモニタできます。この分析により、ケーブルの品質が測定され、IEEE 802.3ab 仕様に準拠しているかどうかが比較されます。

メモ：

- ケーブル分析テストを実行するには、管理者特権が必要です。
- 分析中には、ネットワーク接続が一時的に失われます。
- Broadcom NetXtreme アダプタの場合、ケーブル分析テストを実行できるのは、ギガビット リンクの速度接続のみで、かつ接続がないときだけです。
- 一部の Broadcom ネットワーク アダプタでは、このオプションを利用できません。

ケーブル分析を実行するには：

1. ポートが **Auto** に設定されていて、Speed & Duplex (速度と二重通信方式) ドライバ設定も **Auto** であるスイッチのポートにケーブルを接続します。
2. [エクスプローラ ビュー] ペインで、テストするアダプタの名前をクリックします。
3. **[実行するテストを選択]** リストから **[ケーブル分析]** を選択します。**[ケーブル分析]** オプションを使用できない場合は、ウィンドウの右側にある **[コンテキスト ビュー]** タブから **[診断]** を選択し、**[ケーブル分析]** を選択します。
4. **[実行]** をクリックします。
5. ネットワーク接続が一時的に中断されることを警告するエラー メッセージ ウィンドウで、**[はい]** をクリックします。

距離 . 有効なケーブルの長さ (メートル) です (結果として [ノイズ] が返される場合は異なります)。

ステータス . このケーブル ペアのリンク タイプが表示されます。

- **良好**：ケーブル /PCB の信号パスは良好ですが、ギガビット リンクは確立されていません。
- **クロス**：ピンがショートであるか、2 つ以上のケーブル /PCB の信号パスでクロストークが生じています。
- **オープン**：より線対に対して、ピンのどちらか一方または両方がオープンです。
- **ショート**：同一のより線対に接続されている 2 つのピンが同時にショートしました。
- **ノイズ**：常にノイズが発生しています (強制 10/100 が原因として考えられます)。
- **GB リンク**：ギガビット リンクが稼働中です。
- **該当なし**：アルゴリズムが結論に達することができませんでした。

リンク . リンク接続の速度と二重通信方式です。

ステータス . テストが実行された後のステータスです。完了か失敗になります。

テスト結果に影響を与える可能性があるいくつかの要素があります。

- **リンク パートナー**：さまざまなスイッチやハブ メーカーが、それぞれ異なる PHY を実装しています。一部の PHY は IEEE に準拠していません。
- **ケーブル品質**：カテゴリ 3、4、5 および 6 はテスト結果に影響を与える場合があります。
- **電気干渉**：テスト環境がテスト結果に影響を与える場合があります。

アダプタ プロパティを設定する

[設定] タブの **[詳細設定]** では、選択したアダプタの利用可能なプロパティの値を表示および変更できます。利用できる可能性のあるプロパティとその設定について以下で説明します。

メモ：

- プロパティの値を変更するには、管理者特権が必要です。
- ご使用のアダプタの利用可能なプロパティのリストは異なる場合があります。
- Broadcom ネットワーク アダプタによっては、利用できないプロパティもあります。

アダプタ プロパティを設定するには：

1. [エクスプローラ ビュー] ペインでアダプタの名前をクリックし、**[設定]** タブをクリックします。
2. **[詳細設定]** セクションから、設定するプロパティを選択します。
3. プロパティの値を変更するには、必要に応じてプロパティ リストから項目をクリックするか、新しい値を入力します (選択オプションはプロパティごとに異なります)。
4. **[適用]** をクリックして、すべてのプロパティに対する変更を確定します。プロパティを元の値に戻す場合は、**[リセット]** をクリックします。

802.1p QOS. *QOS* (Quality of Service、サービス品質) をイネーブルします。これは IEEE (Institute of Electrical and Electronics Engineering、米電気電子学会) の仕様であり、必要な品質レベル、信頼性、待ち時間を実現するために、トラフィックのタイプに応じて、さまざまなタイプのネットワーク トラフィックを異なる方式で制御するものです。このプロパティは、デフォルトでディスエーブルに設定されています。ネットワーク環境が QoS をサポートしている場合を除いて、QoS はイネーブルしないでください。イネーブルすると、問題が発生する可能性があります。

フロー コントロール . PAUSE フレームの受信・転送のイネーブルとディスエーブルを切り替えます。PAUSE フレームは、ネットワーク アダプタとスイッチで速度をコントロールできるようにします。PAUSE フレームを受信している側は、一時的に受信を停止します。

- **Auto (自動)** (デフォルト) : PAUSE フレームの受信と転送が最適化されます。
- **Disable (ディスエーブル)** : PAUSE フレームの受信と転送がディスエーブルされます。
- **Rx PAUSE** : PAUSE フレームの受信がイネーブルされます。
- **Rx/Tx PAUSE** : PAUSE フレームの受信と転送がイネーブルされます。
- **Tx PAUSE** : PAUSE フレーム転送がイネーブルされます。

Speed & Duplex (速度と二重通信方式). Speed & Duplex (速度と二重通信方式) のプロパティでは、ネットワークへの接続速度や通信方式を設定します。全二重通信方式モードにすると、アダプタでのネットワーク データ受信・転送が同時にできるようになります。

- **10 Mb Full (10 Mb 全二重)** : 速度を 10Mbit/ 秒に、通信方式を全二重に設定します
- **10 Mb Half (10 Mb 半二重)** : 速度を 10Mbit/ 秒に、通信方式を半二重に設定します
- **100 Mb Full (10 Mb 全二重)** : 速度を 100Mbit/ 秒に、通信方式を全二重に設定します
- **100 Mb Half (10 Mb 半二重)** : 速度を 100Mbit/ 秒に、通信方式を半二重に設定します
- **Auto (自動)** (デフォルト) : 速度と通信方式をネットワークに最適な接続に設定します (推奨)。

メモ：

- [Auto/ 自動] に設定しておくことをお勧めします。この設定にしておくと、ネットワーク アダプタが動的にネットワークの回線速度を検出できるようになります。ネットワークの容量が変化するたびに、自動検出により新しい回線速度と二重通信方式にネットワーク アダプタが調整されます。1 Gbit/ 秒の転送速度がサポートされている場合、[Auto/ 自動] を選択するとこの速度がイネーブルされます。
- [1 Gb Full Auto/1 Gb 全自動] は 1 Gb 接続が可能なリンク パートナーに接続する必要があります。接続は 1 Gb 接続のみに限られているため、Ethernet@Wirespeed 機能はディスエーブルされます。リンク パートナーが 1 Gb 接続のみをサポートしている場合、Wake on LAN 機能は動作しない可能性があります。さらに、オペレーティング システムがない場合、管理トラフィックも影響を受けることがあります。
- [10 Mb Half/10 Mb 半二重] や [100 Mb Half/100 Mb 半二重] を選択すると、ネットワーク アダプタのネットワークへの接続が半二重モードに強制されます。ただし、ネットワークで半二重通信モード動作が設定されていない場合は、ネットワーク アダプタが機能しない場合もあります。
- [10 Mb Full/10 Mb 全二重] や [100 Mb Full/100 Mb 全二重] を選択すると、ネットワーク アダプタのネットワークへの接続が全二重モードに強制されます。ただし、ネットワークが同じモードで動作するよう設定されていない場合、ネットワーク アダプタが機能しない場合もあります。

Wake Up Capabilities（節電モードからの起動能力）ネットワーク起動フレームの受信時に、低電力モードからネットワーク アダプタを起動できます。起動フレームには、Magic Packet と Wake Up Frame (起動フレーム) の 2 種類が選択できます。

このプロパティが利用できるのは、Broadcom NetXtreme アダプタだけです。

- **Both (両方)** (デフォルト) : 起動フレームとして、Magic Packet と Wake Up Frame (起動フレーム) の両方を選択します。
- **Magic Packet** : 起動フレームとして Magic Packet を選択します。
- **None (なし)** : 起動フレームは選択されません。
- **[起動フレーム]** - 起動フレームとして Wake Up Frame (起動フレーム) を選択し、ping や ARP (Address Resolution Protocol) の受信などのイベント発生時にネットワーク アダプタによりシステムが起動できるようにします。このオプションはオペレーティング システムの節電モードと連動しており、節電設定が WOL をイネーブルしていない場合は動作しません。

Priority および VLAN. ネットワーク トラフィックの優先度および VLAN タギングの両方を有効にできます。VLAN タギングは、VLAN ID 設定が 0 (ゼロ) 以外の値に設定されている場合にのみ行われます。

- **Priority および VLAN が有効 (デフォルト)** : パケットの優先度および VLAN タギングを利用できます。
- **Priority および VLAN が無効** : パケットの優先度および VLAN タギングは利用できません。
- **Priority が有効** : パケットの優先度のみを利用できます。
- **VLAN が有効** : VLAN タギングのみを利用できます。

注: 中間ドライバが VLAN タギング用にネットワーク アダプタを管理している場合、**[Priority および VLAN が無効]** および **[Priority が有効]** 設定を使用しないでください。**[Priority および VLAN が有効]** 設定を使用して、**VLAN ID** を 0 (ゼロ) に変更します。

VLAN ID. [Priority および VLAN] の設定として **[Priority および VLAN が有効]** が選択されている場合に、VLAN タギングをイネーブルし、VLAN ID を設定します。VLAN ID の範囲は 1 ～ 4094 で、接続されたスイッチの VLAN タグ値と一致していなければなりません。このフィールドの値を 0 (デフォルト) にすると、VLAN タギングが無効になります。

NDIS ミニポート ドライバを使用した VLAN タギングのリスク評価

Broadcom の NDIS 6.0 ミニポート ドライバを使用すると、Broadcom アダプタを含むシステムがタグ付けされた VLAN に接続できるようになります。しかし、NDIS 6 ドライバの VLAN のサポートは、BASP とは異なり、1 つの VLAN ID のみに対応しています。

また NDIS 6.0 ドライバは、BASP とは異なり、発信パケットの VLAN タギングのみを提供しており、VLAN ID メンバーシップに基づく受信パケットのフィルタリングは提供していません。これはすべてのミニポート ドライバでデフォルトの動作となっています。VLAN メンバーシップに基づくフィルタリングパケットが存在しないとセキュリティ上の問題が発生する場合がありますが、次の方法により、このドライバ制限に基づく IPv4 ネットワーク用のリスク評価を行うことができます。

複数の VLAN を持つ、適切に設定されたネットワークは、各 VLAN に別個の IP セグメントを維持する必要があります。これが必要となる理由は、発信トラフィックが、どのアダプタ (仮想または物理) にトラフィックを流すかを特定する上でルーティング テーブルに依存しており、VLAN メンバーシップに基づいてアダプタを特定しているわけではないからです。

Broadcom の NDIS 6.0 ドライバにおける VLAN タギングのサポートは、伝送トラフィック (Tx) のみに制限されており、異なる VLAN からの受信トラフィック (Rx) がオペレーティング システムにまで流れてしまう危険性があります。しかし、上記のような適切に設定されたネットワークを前提とする場合には、IP 区分化やスイッチ VLAN 設定は、リスクを制限するために追加のフィルタを使用できる場合があります。

連続的な接続シナリオでは、VLAN メンバーシップのフィルタリングが発生しないため、同一の IP セグメントに存在する 2 台のコンピュータは、VLAN 設定にかかわらず通信できます。しかし、VLAN 環境ではこの接続タイプは一般的なものではないため、このシナリオでは、セキュリティ違反がすでに発生しているという仮定になっています。

上記のリスクが回避すべきものであり、VLAN ID メンバーシップのフィルタリングが必要な場合には、中間ドライバを通じたサポートが必要になります。

統計を表示する

[統計] タブに表示される情報で、Broadcom ネットワーク アダプタと他社製ネットワーク アダプタの両方のトラフィック統計を確認できます。統計情報と統計の対象は、Broadcom アダプタの方が広範囲にわたります。

インストールされているネットワーク アダプタの統計情報を表示するには、[エクスプローラ ビュー] ペインに一覧表示されているアダプタの名前をクリックし、[統計] タブをクリックします。

[更新] をクリックすると、各統計の最新値が表示されます。**[リセット]** をクリックすると、すべての値がゼロになります。

メモ：

- Broadcom ネットワーク アダプタの場合でも、ディスエーブルされると、チームの統計は集計されません。
- Broadcom ネットワーク アダプタによっては、利用できない統計もあります。

全般

[全般] には、アダプタとの間で転送および受信された統計が表示されます。

フレーム Tx. OK. 無事転送されたフレーム数のカウントです。このカウンタは、転送ステータスが Transmit OK (転送 OK) とレポートされるとインクリメントします。

フレーム Rx. OK. 無事受信されたフレーム数のカウントです。これには、長すぎるフレーム、フレーム チェック シーケンス (FCS)、長さ、またはアラインメントのエラーを受信したフレームも、内部 MAC サブレイヤ エラーのため損失したフレームも含まれません。このカウンタは、受信ステータスが Receive OK (受信 OK) とレポートされるとインクリメントします。

伝送フレーム Tx. 無事転送された伝送データ フレーム数のカウントです

マルチキャスト フレーム Tx. 同報通信アドレス以外のグループ宛先アドレスに無事転送されたフレーム数のカウントです (ステータス値は Transmit OK)。

同報通信フレーム Tx. 同報通信アドレスに無事転送されたフレーム数のカウントです (転送ステータスは Transmit OK)。マルチキャスト アドレスへ転送されたフレームは同報通信フレームにはならないため、除外されます。

伝送フレーム Rx. 無事受信されたフレーム数のカウントです。

マルチキャスト フレーム Rx. 無事受信され、アクティブの非同報通信グループ アドレスに伝送されたフレーム数のカウントです。これには、長すぎるフレーム、FCS、長さ、またはアラインメントのエラーを受信したフレームも、内部 MAC サブレイヤ エラーによって損失したフレームも含まれません。このカウンタは Receive OK ステータスが示されるとインクリメントします。

同報通信フレーム Rx. 無事受信され、同報通信グループ アドレスに伝送されたフレーム数のカウントです。これには、長すぎるフレーム、FCS、長さ、またはアラインメントのエラーを受信したフレームも、内部 MAC サブレイヤ エラーによって損失したフレームも含まれません。このカウンタは Receive OK ステータスが示されるとインクリメントします。

フレーム Rx の CRC エラー . CRC エラーで受信されたフレーム数です。

チームの設定

チーム化機能を使用すると、ネットワーク アダプタをグループ化し、チームとして機能させることができます。チーム化は、バーチャル NIC (1 つのアダプタとして機能する複数のアダプタのグループ) を作成する方法の 1 つです。この方法の利点は、ロード バランシングとフェイルオーバーが可能になることです。チーム化は Broadcom Advanced Server Program ソフトウェア を使用して実行します。チーム化ソフトウェアの技術および実装の考慮事項に関する総合的な説明については、Broadcom ネットワーク アダプタ ユーザーガイドの「Broadcom Gigabit Ethernet のチーム化サービス」のセクションを参照してください。

チーム化は、以下の方法のいずれかで実行できます。

- Broadcom チーム化ウィザードを使用する
- エキスパート モードを使用する

メモ：

- チーム化のプロトコルの詳細については、Broadcom ネットワーク アダプタ ユーザーガイドの「チーム化」を参照してください。
- チームの設定時に LiveLink™ をイネーブルしない場合は、スイッチでスパニング ツリー プロトコル (STP) をディスエーブルするようにしてください。これにより、フェイルオーバーの実行時にスパニング ツリーのループが決定されるまでのダウンタイムを最低限に抑えることができます。LiveLink は、このような問題を可能な限り回避します。
- BASP は、Broadcom ネットワーク アダプタがシステムに 1 つまたは複数取り付けられている場合にのみ使用可能です。
- Large Send Offload (LSO、大量送信オフロード) プロパティと Checksum Offload (チェックサム オフロード) プロパティは、すべてのメンバーが機能をサポートし、その機能用に設定されている場合にのみ、チームに対してイネーブルされます。
- チームを作成、変更するには、管理者特権が必要です。
- チーム メンバーがそれぞれ異なる速度で接続している環境でのロード バランス アルゴリズムでは、ギガビット イーサネット リンクで接続しているメンバーのほうが、しきい値に達するまで低速リンク (100 Mbps または 10 Mbps) で接続しているメンバーよりも有利です。これは通常の動作です。
- Wake on LAN (WOL) は、イーサネット インターフェイスから特定のパケットを受信すると、システムがスリープ状態から復帰できるようにする機能です。仮想アダプタは、ソフトウェア専用デバイスとして実装されるので、WOL の実装に必要なハードウェア機能がなく、仮想アダプタではスリープ状態からシステムを始動させることができません。ただし、物理アダプタでは、アダプタがチームの一部である場合でも、このプロパティをサポートします。

チーム タイプ

以下の 4 種類の Load Balance チームを作成できます。

- Smart Load Balance および Failover
- リンク集約 (802.3ad)
- 通有中継 (FEC/GEC)/802.3ad-Draft Static
- スマート ロード バランス (SLB) (自動フォールバックはディスエーブル) — 自動フォールバックはディスエーブル機能は、チーム化ウィザードで、スマート ロード バランスおよびフェイルオーバー タイプのチームに対して設定されます。

これらのタイプについては、*Broadcom® NetXtreme® BCM57XX ユーザー ガイド*の「ロード バランシングとフォルト トレランス」を参照してください。

Broadcom チーム化ウィザードを使用する

Broadcom チーム化ウィザードを使用して、チームの作成、既存のチーム (チームがすでに作成されている場合) の設定、または VLAN の作成を行うことができます。

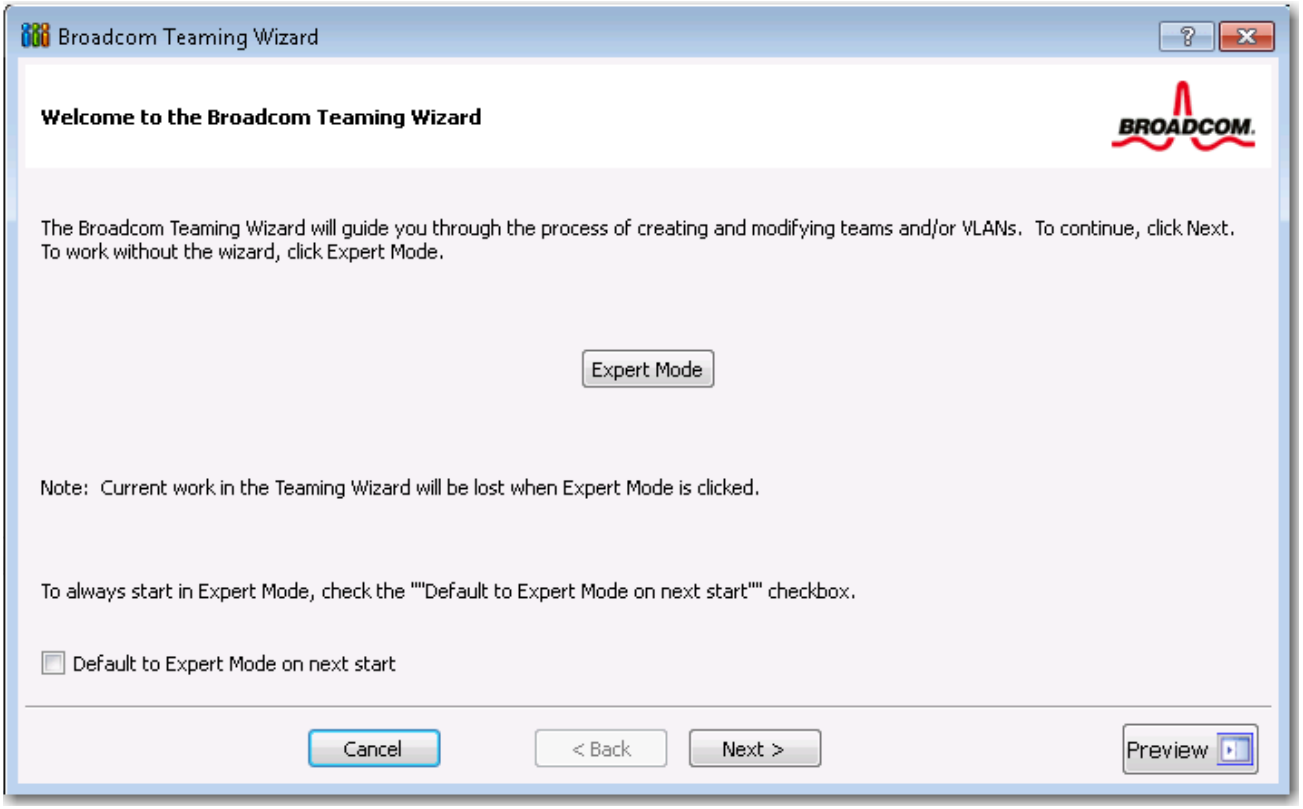
1. チームを作成または編集します。

   新しいチームを作成するには、**[チーム]** メニューから **[チームの作成]** を選択するか、[割り当てられていないアダプタ] セクションでデバイスのいずれかを右クリックして **[チームの作成]** を選択します。[割り当てられていないアダプタ] セクションにデバイスが表示されていない場合、このオプションは使用できません。すべてのアダプタがすでにチームに割り当てられています。

   既存のチームを設定するには、リスト内のいずれかのチームを右クリックして、**[チームの編集]** を選択します。このオプションは、チームがすでに作成されていて [チームの管理] ペインに表示されている場合のみ使用できます。

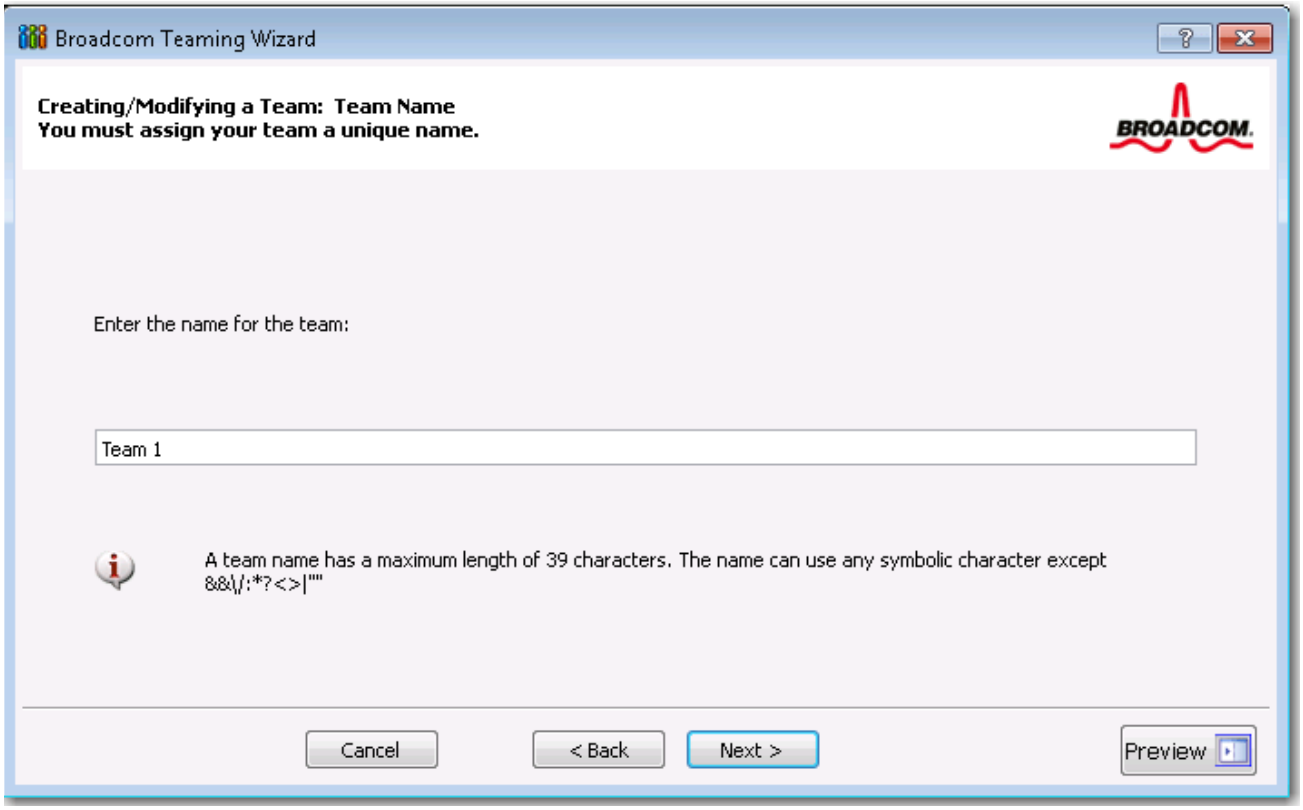
注：ウィザードを使用しない場合は、**[エキスパート モード]** をクリックします。常にエキスパート モードを使用してチームを作成する場合は、**[次回起動時にエキスパート モードをデフォルトにする]** チェック ボックスをオンにします。エキスパート モードを使用するを参照してください。

2. ウィザードを使用して続行するには、**[次へ]** をクリックします。

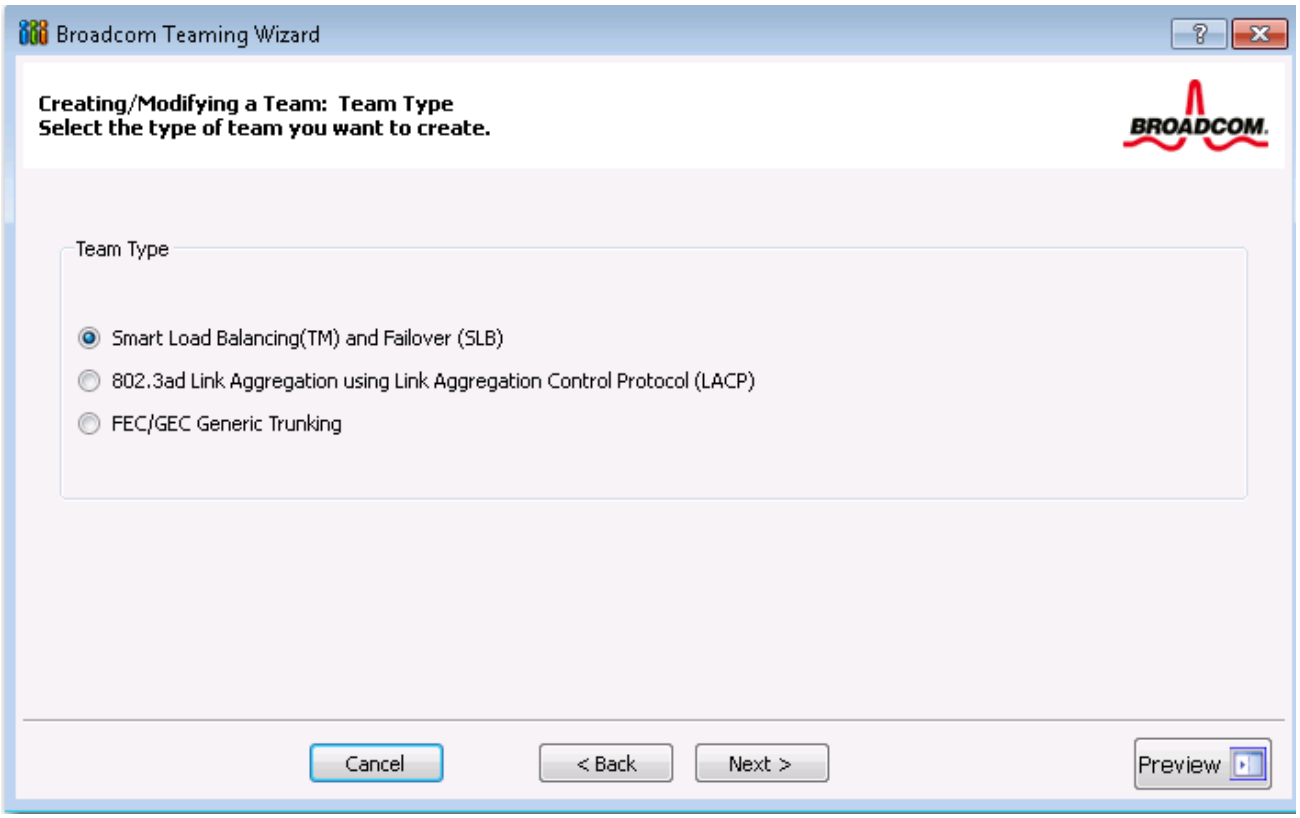


3. チーム名を入力し、**[次へ]** をクリックします。設定を確認または変更する場合は、**[戻る]** をクリックします。設定を破棄してウィザードを終了するには、**[キャンセル]** をクリックします。

注：チーム名は最大 39 文字で、スペースで開始することはできず、以下の文字は使用できません：
& \ / : * ? < > |



4. 作成するチームのタイプを選択します。チーム タイプが SLB タイプのチームの場合、**[次へ]** をクリックします。チーム タイプが SLB タイプのチームではない場合、ダイアログ ボックスが表示されます。チーム メンバーに接続されたネットワーク スイッチが、チーム タイプに対して適切に設定されていることを確認し、**[OK]** をクリックして続行します。

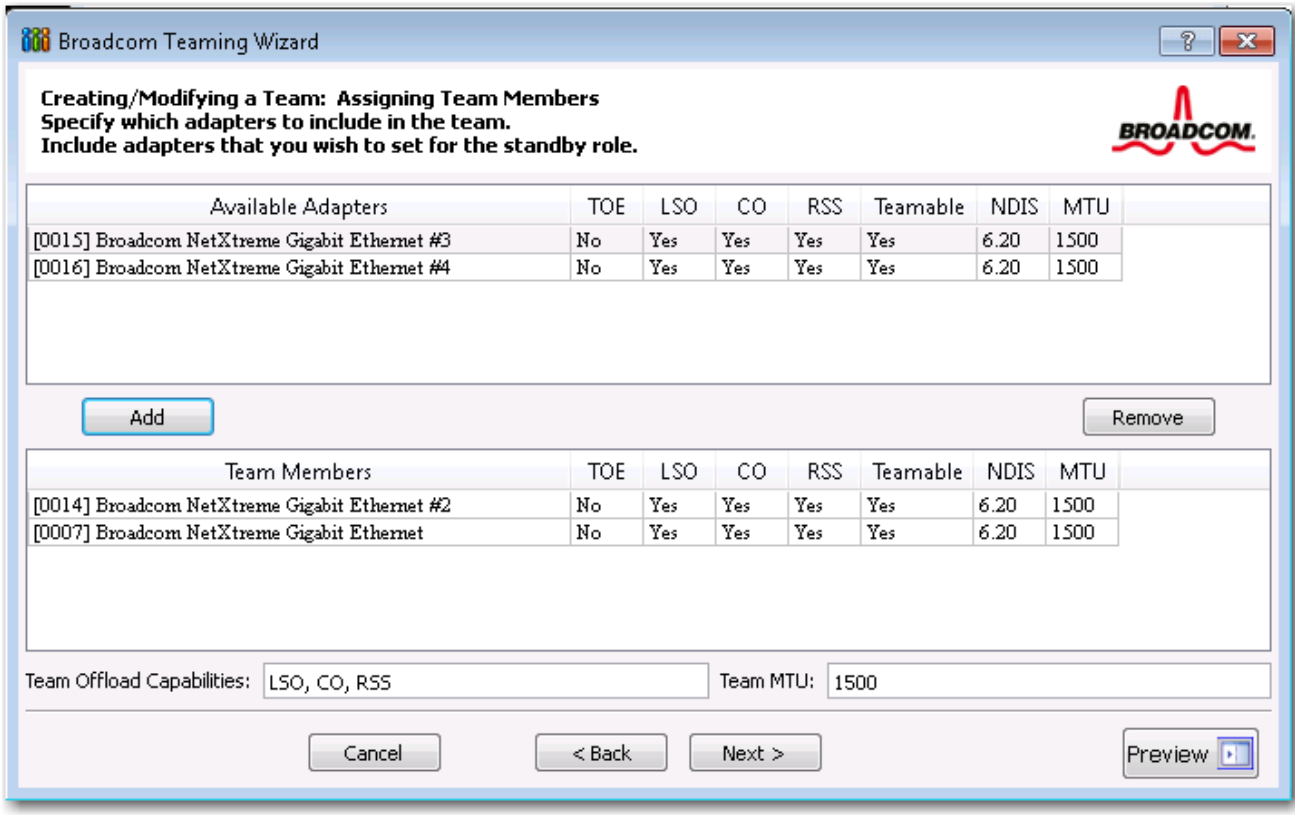


5. **[利用可能なアダプタ]** リストで、チームに追加するアダプタをクリックし、**[追加]** をクリックします。チーム メンバーを **[チーム メンバー]** リストから削除する場合は、アダプタをクリックして **[削除]** をクリックします。**[次へ]** をクリックします。

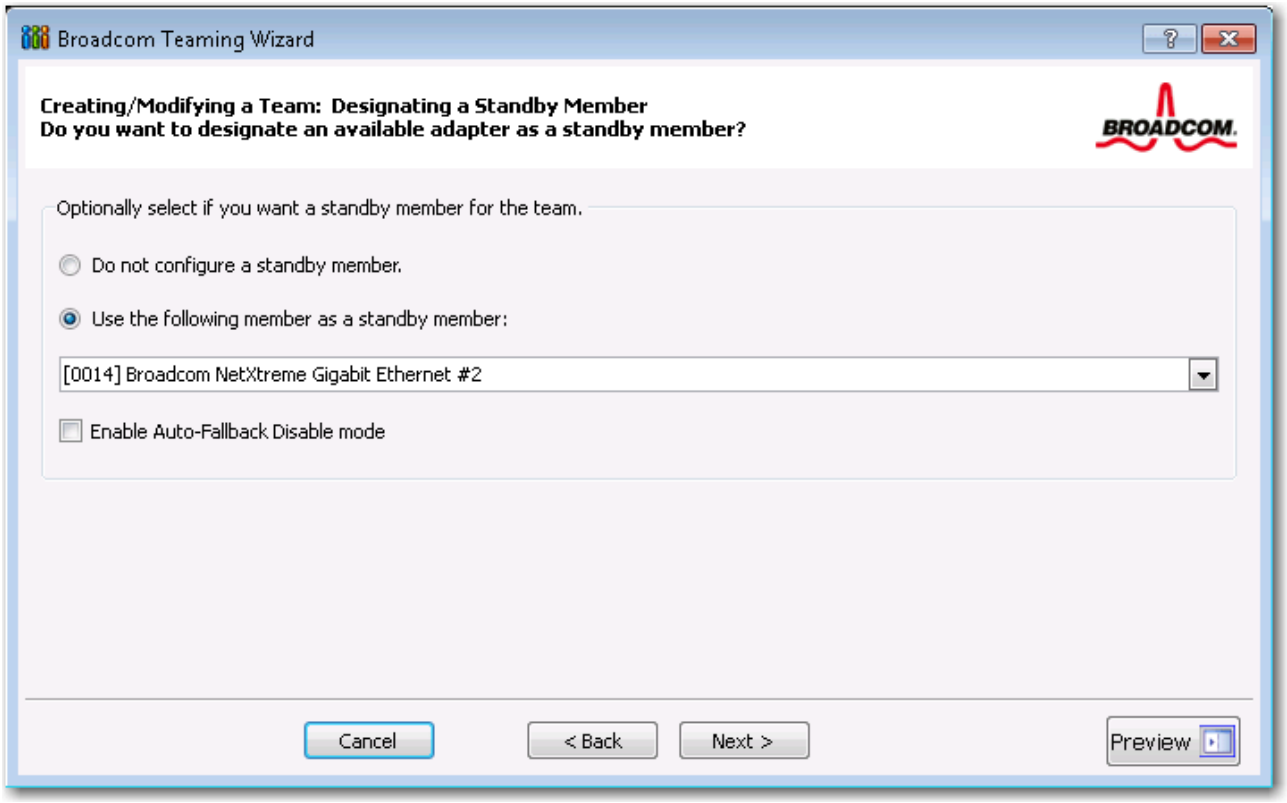
注：少なくとも 1 つの Broadcom ネットワーク アダプタをチームに割り当てる必要があります。

Large Send Offload (LSO、大量送信オフロード) コラムおよび Checksum Offload (CO、チェックサム オフロード) コラムは、アダプタに対して LSO および CO のプロパティがサポートされているかを示します。LSO プロパティおよび CO プロパティは、すべてのメンバーが機能をサポートし、その機能用に設定されている場合にのみ、チームに対してイネーブルされます。この場合、スクリーンの下部にチーム オフロード機能が表示されます。

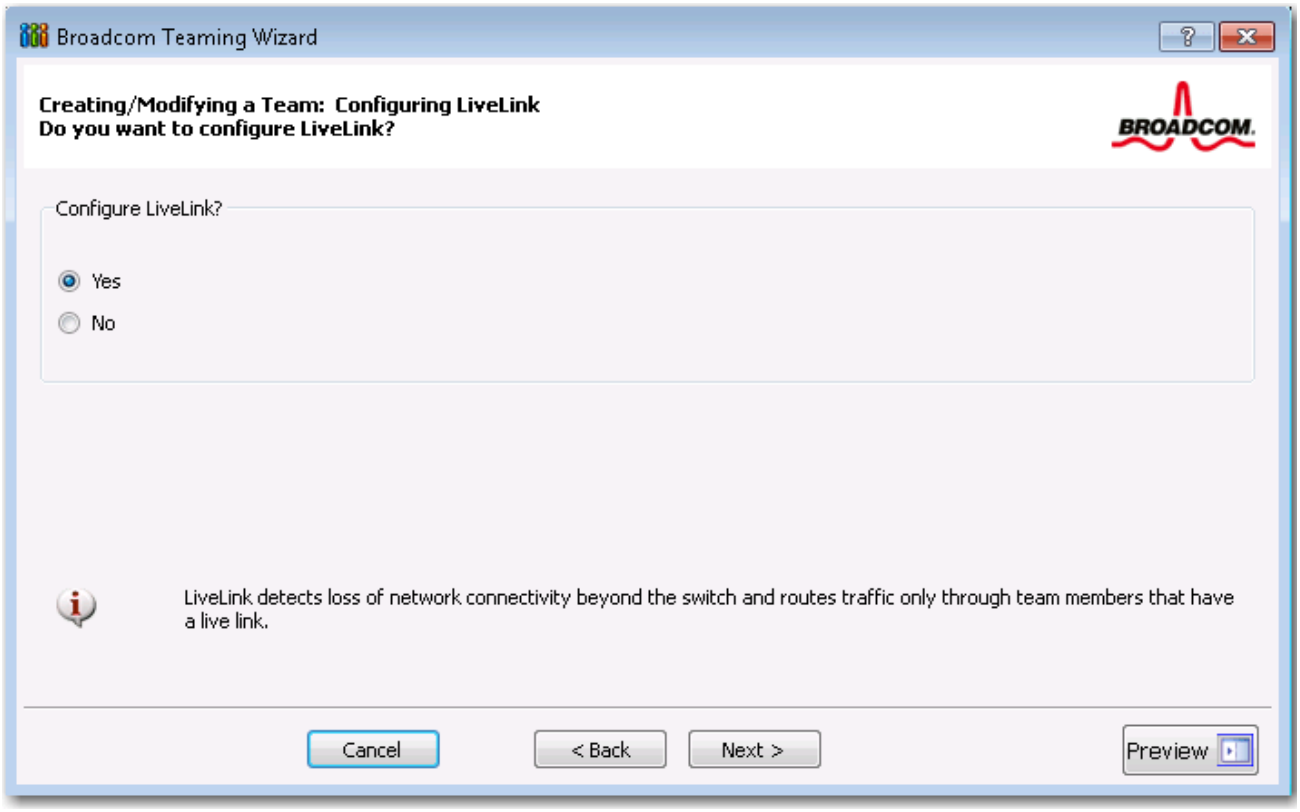
注：ドライバが無効になっているチームにネットワーク アダプタを追加すると、チームのオフロード機能に悪影響を与える可能性があります。これはチームのパフォーマンスに影響を与える場合もあります。そのため、ドライバが対応しているネットワーク アダプタのみを、メンバーとしてチームに追加することをお勧めします。



6. アダプタの 1 つをスタンバイ メンバーとして指定する場合 (オプション) は、**[以下のメンバーはスタンバイ メンバーとして使用します。]** を選択し、アダプタのリストからスタンバイ メンバーを選択します。
7. 自動フォールバックはディスエーブル モード機能によって、プライマリ メンバーが再びオンラインになったときに、チームはプライマリ メンバーに切り替えずにスタンバイ メンバーをそのまま使用できます。この機能をイネーブルにするには、**[自動フォールバックはディスエーブル モードをイネーブルする]** を選択します。**[次へ]** をクリックします。



8. LiveLink を設定する場合は **[はい]**、それ以外の場合は **[いいえ]** を選択して、**[次へ]** を選択します。



9. プローブのインターバル (プローブ対象に対するリンク パケットの各再転送間隔の秒数) およびプローブの最大再送回数 (フェイルオーバーが発生する前にプローブ対象からの応答を連続して受信しない回数) を選択します。

10. タグ付きの VLAN に含まれるプローブ対象との接続が許可されるよう、[プローブ VLAN ID] を設定します。番号の組み合わせは、プローブ対象の VLAN ID、およびチームを接続するスイッチのポートと一致している必要があります。

注：LiveLink がイネーブルされた各チームは、1 つの VLAN のプローブ対象とのみ通信できます。また、VLAN ID 0 とは、タグなしネットワークを意味します。[プローブ VLAN ID] に 0 以外の数値が設定されている場合は、同一の VLAN タグ値を使用して VLAN を作成するを参照してください。ステップ 16. 必要があります (を参照してください)。

11. リストの最上部にあるプローブ対象をクリックし、**[対象 IP アドレスの編集]** をクリックして、**[IP アドレス]** ボックスに、1 つまたはすべてのプローブ対象の対象 IP アドレスを入力し、**[OK]** をクリックします。**[次へ]** をクリックします。

注：1 つ目のプローブ対象のみが必須です。他のプローブ対象に IP アドレスを割り当てることで、プローブ対象を最大 3 個までバックアップとして追加することができます。

12. リストされているチーム メンバーを選択し、**[メンバー IP アドレスの編集]** をクリックして、[IP アドレス] ボックスにメンバー IP アドレスを入力します。リストされているチーム メンバーすべてに対してこのステップを繰り返し、**[OK]** をクリックします。**[次へ]** をクリックします。

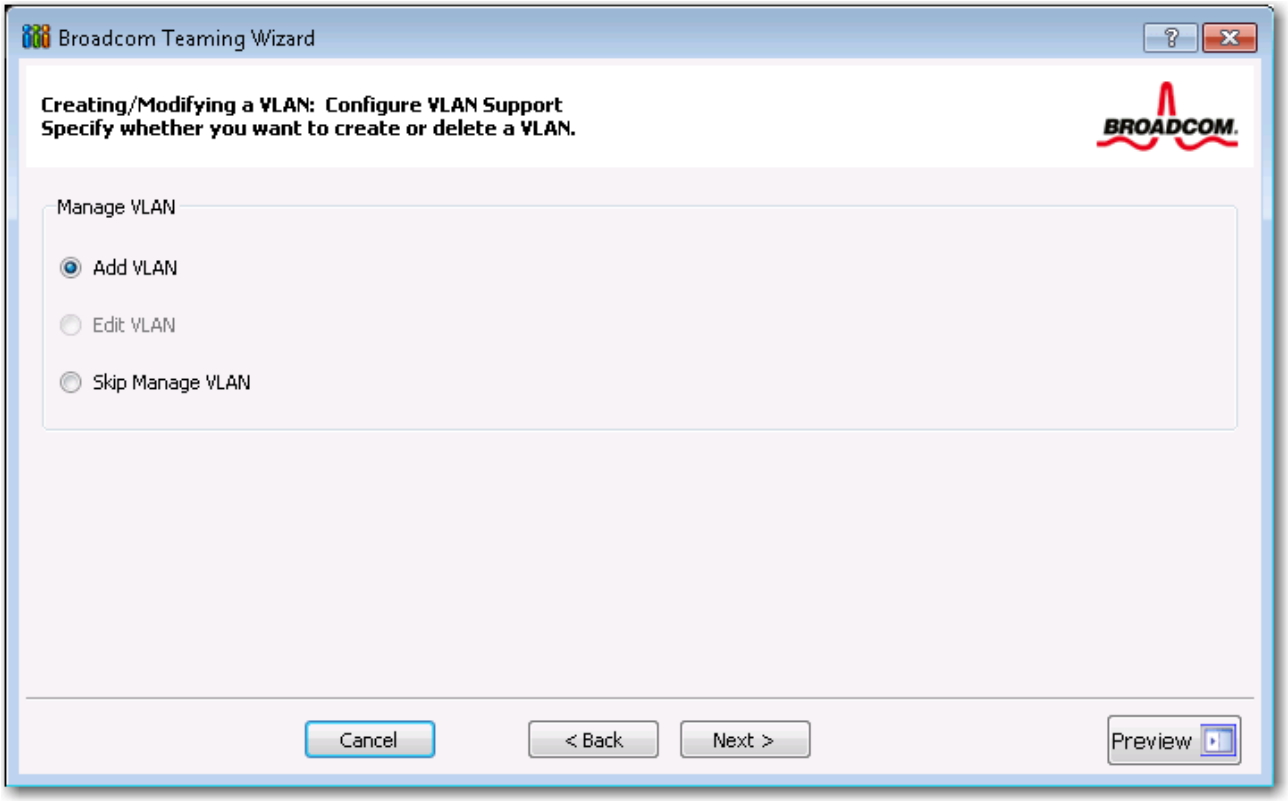
注：すべてのメンバー IP アドレスは、プローブ対象と同一のサブネットにある必要があります。

13. チームに VLAN を作成する場合は **[VLAN の追加]**、既存の VLAN の設定を変更する場合は **[VLAN の編集]** を選択して、**[次へ]** を選択します。VLAN を作成または編集しない場合は、**[VLAN の管理をスキップ]** を選択して、**[次へ]** をクリックし、[完了] スクリーンからウィザードを続行します (この手順のステップ 18. を参照してください)。

VLAN により、異なるサブネット上にある複数の仮想アダプタを追加できます。複数のサブネットに所属することが可

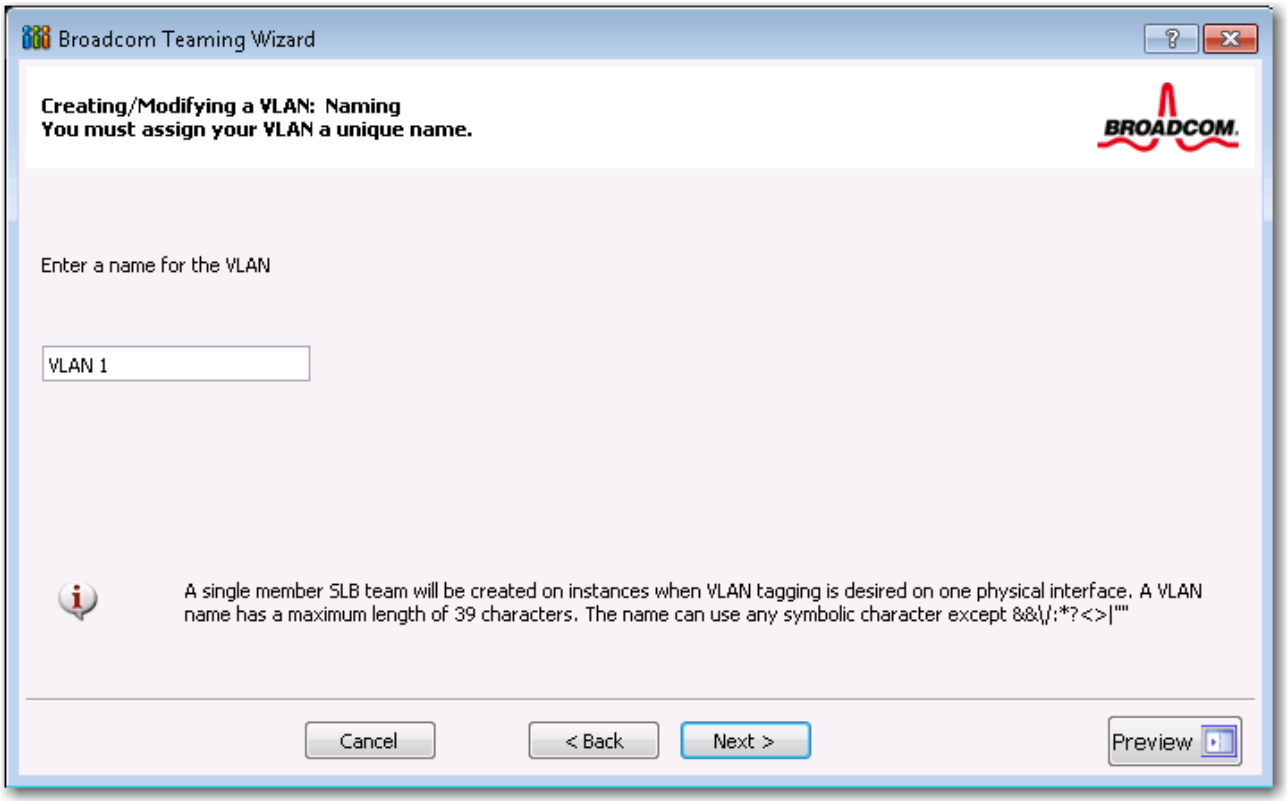
能な 1 つのネットワーク アダプタを、利用中のシステムに装備できるようになります。

注：ただし、すべてのチーム メンバーが Broadcom アダプタでないと VLAN は作成できません。

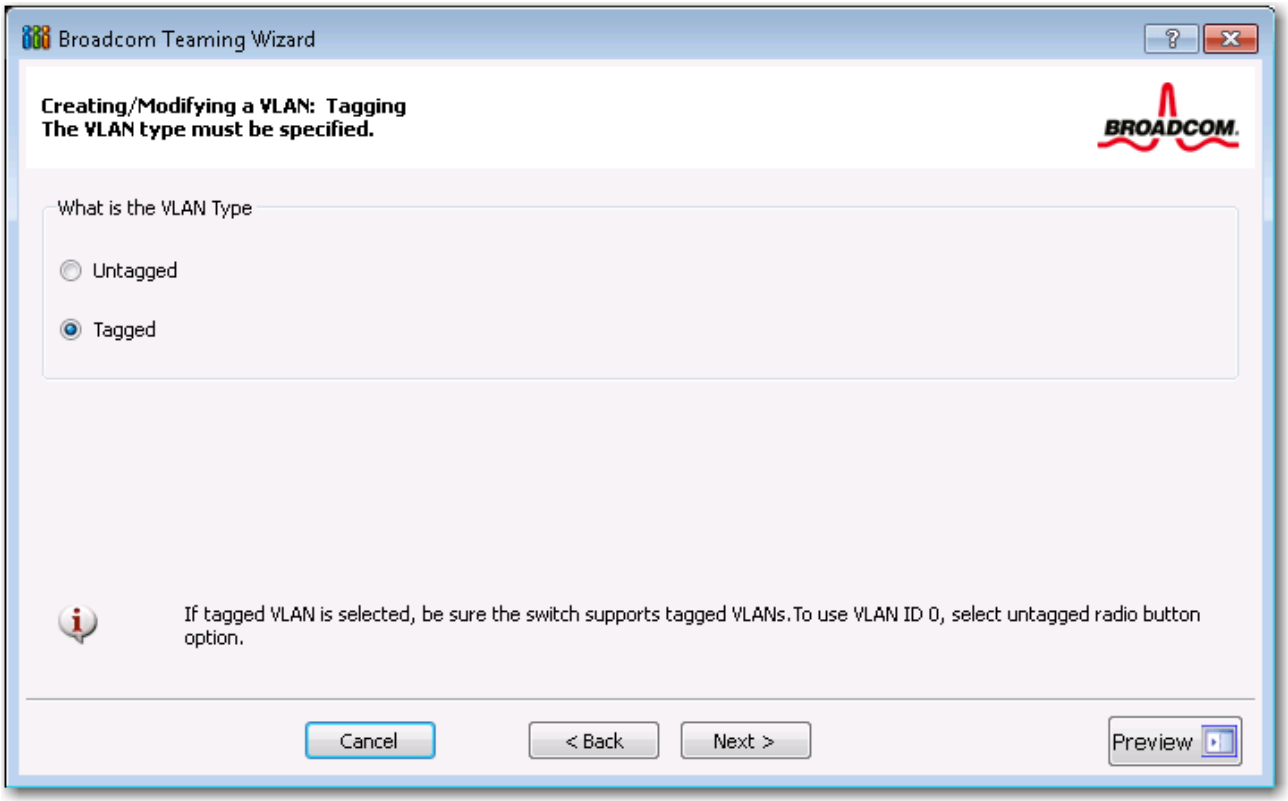


14. VLAN 名を入力し、**[次へ]** をクリックします。

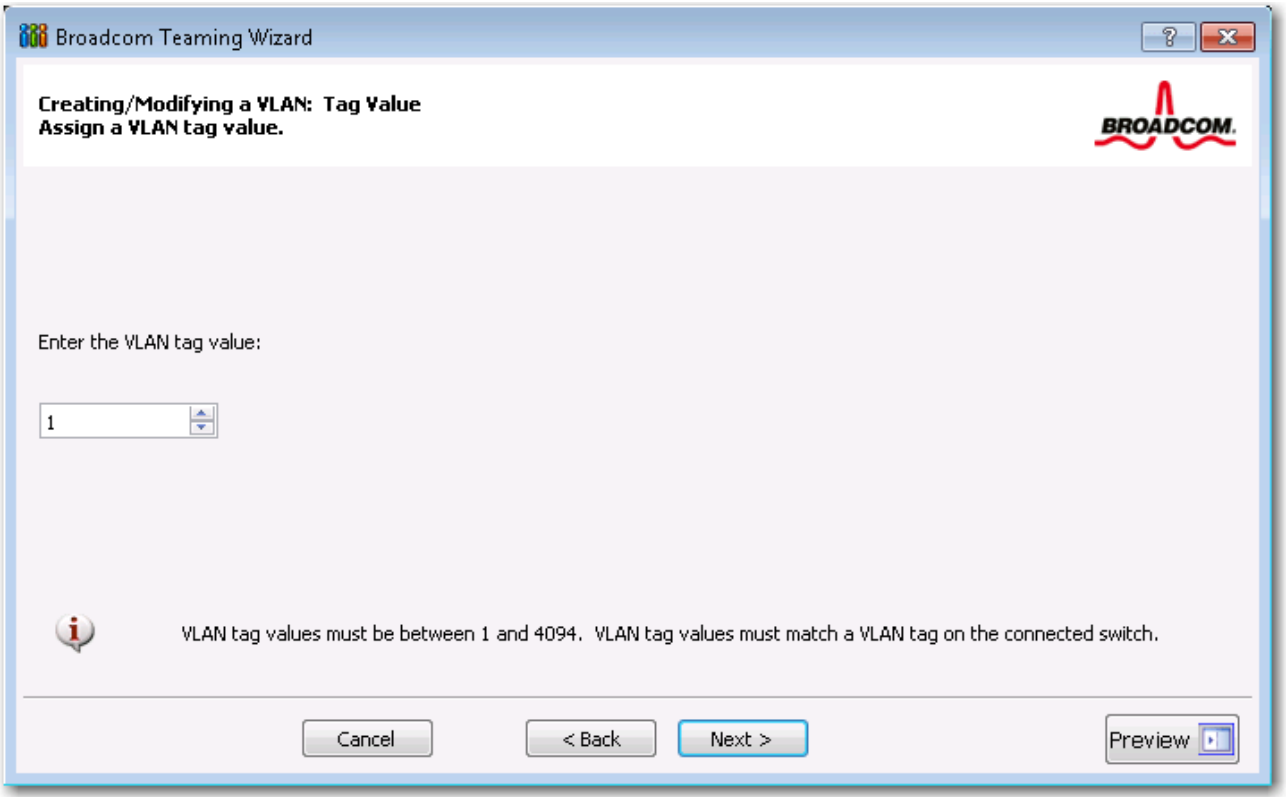
注：チーム名は最大 39 文字で、スペースで開始することはできず、以下の文字は使用できません：
& \ / : * ? < > |



15. VLAN にタグを付けるには、**[タグ付き]**、**[次へ]** の順に選択します。タグを付けない場合は、**[タグなし]**、**[次へ]** の順にクリックし、ウィザードを続行してその他の VLAN を追加します (この手順のステップ 17. を参照)。



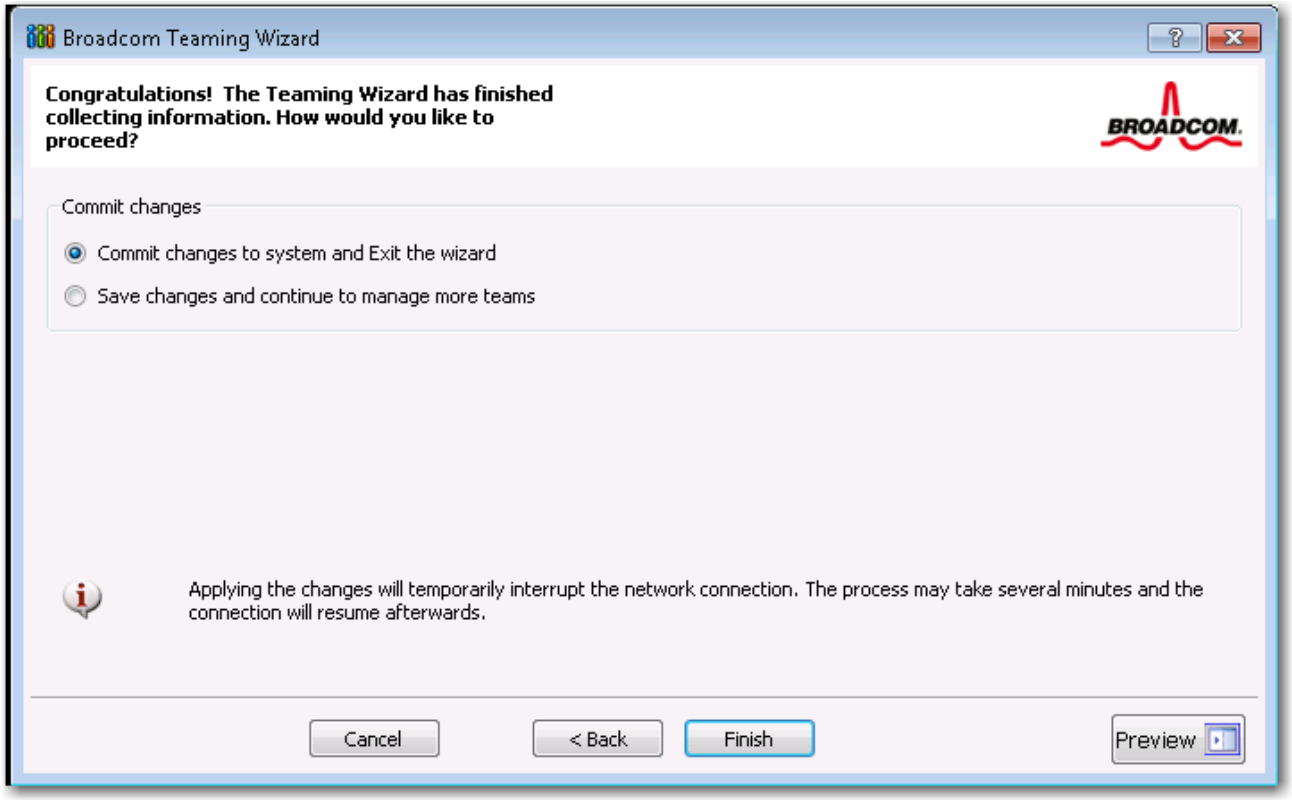
16. VLAN タグ値を入力して、**[次へ]** をクリックします。数値は、1 ～ 4094 である必要があります。



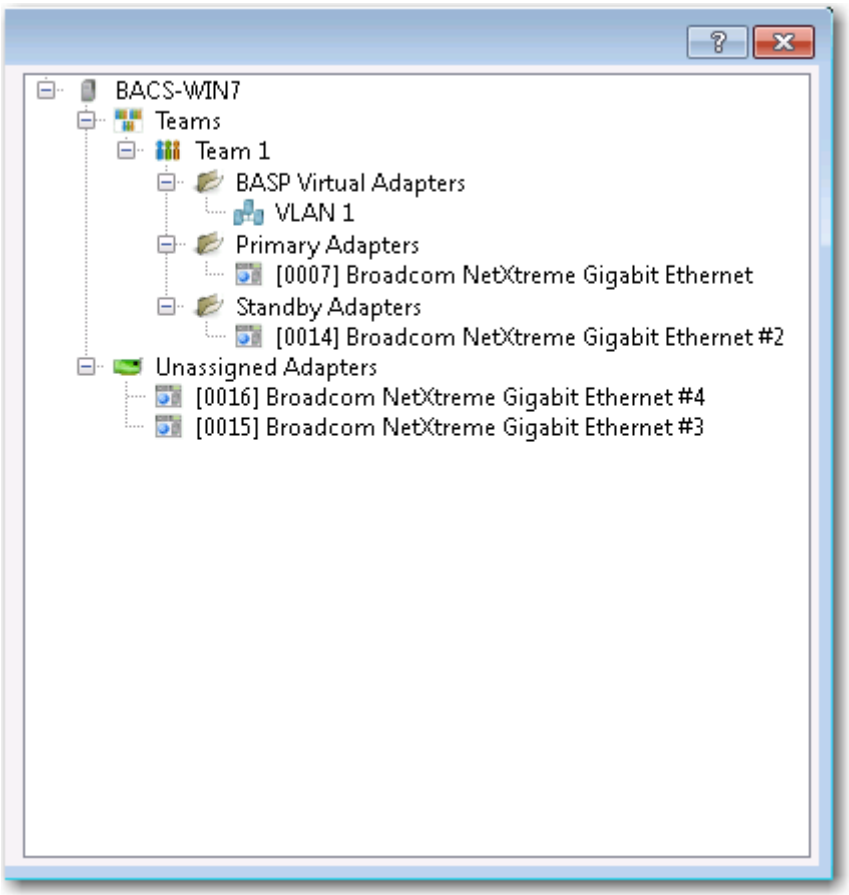
17. **[はい]** を選択して別の VLAN を追加または管理し、**[次へ]** をクリックします。必要な VLAN の追加または管理が完了するまで繰り返します。

注 : 1 つのチームには、64 件まで VLAN を定義することができます (タグ付けされた VLAN 63 件、タグ付けされていない VLAN 1 件)。複数の VLAN を追加すると、各 VLAN のメモリおよびプロセッサ時間の使用によって、Windows インターフェイスの応答時間が遅くなる場合があります。Windows のパフォーマンスが影響を受ける程度は、システムの設定によって異なります。

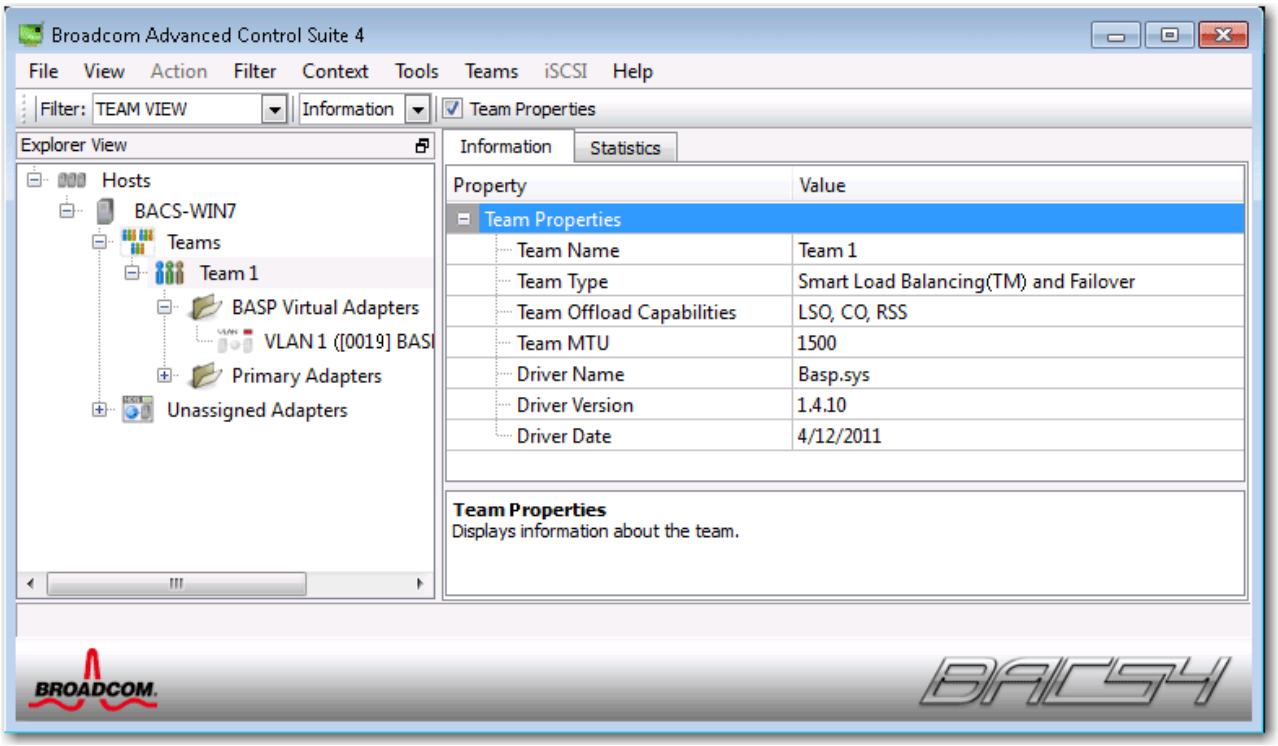
18. 変更内容をチームに適用して確定するには、**[変更をシステムに適用してウィザードを終了する]** を選択します。変更内容を適用した後もウィザードを引き続き使用するには、**[変更を保存して、引き続き他のチームを管理する]** を選択します。[完了] をクリックします。



注: Broadcom チーム化ウィザードのどの段階でも、**[プレビュー]** をクリックすれば、変更を確定する前にチームの状態を視覚的に確認できます。



19. [チームの管理] ペインでチーム名をクリックすると、チームのプロパティが **[情報]** タブに、転送および受信のデータが **[統計]** タブに表示されます。



エキスパート モードを使用する

チームの作成、チームの変更、VLAN の追加と、スマート ロード バランスおよびフェイルオーバー、スマート ロード バランス (自動フォールバックはディスエーブル) の各チームの LiveLink の設定を行うには、エキスパート モードを使用してください。ウィザードを使用してチームを作成するには、Broadcom チーム化ウィザードを使用するを参照してください。

デフォルトのチーム化モードを設定するには、**[ツール]** メニューから **[オプション]** を選択し、**[エキスパート モード]** または **[ウィザード モード]** を選択します (デフォルトはウィザード モードです)。

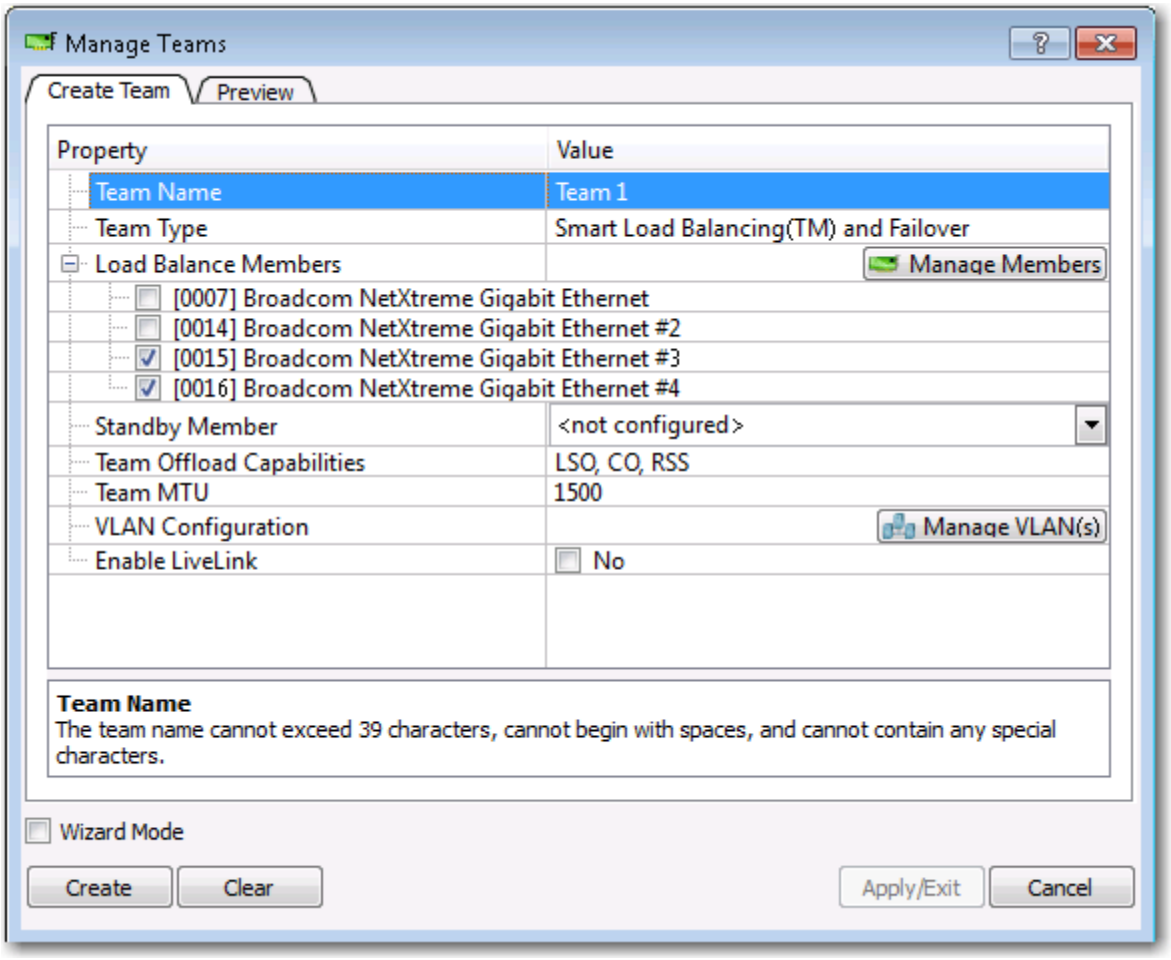
チームの作成

注：SLB (スマート ロード バランス) チームのメンバーには、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) をイネーブルすることはお勧めしません。

1. **[チーム]** メニューから **[チームの作成]** を選択するか、[割り当てられていないアダプタ] セクションでデバイスのいずれかを右クリックして **[チームの作成]** を選択します。[割り当てられていないアダプタ] セクションにデバイスが表示されていない場合、このオプションは使用できません。すべてのアダプタがすでにチームに割り当てられています。
2. **[エキスパート モード]** をクリックします。

注: 常にエキスパート モードを使用してチームを作成する場合は、**[次回起動時にエキスパート モードをデフォルトにする]** チェック ボックスをオンにします。

3. **[チームの作成]** タブをクリックします。



注：[チームの作成] タブが表示されるのは、チーム化可能なアダプタがある場合のみです。

4. **[チーム名]** フィールドをクリックして、チーム名を入力します。
5. **[チーム タイプ]** フィールドをクリックして、チーム タイプを選択します。
6. **[Load Balance メンバー]** リストからアダプタを選択して、利用可能な 1 つまたは複数のアダプタをチームに割り当てます。**[Load Balance メンバー]** リストでは、少なくとも 1 つのアダプタを選択してください。
7. その他の利用可能なアダプタを **[スタンバイ メンバー]** リストから選択して、スタンバイ メンバーになるように割り当てることができます。

注：少なくとも 1 つの Broadcom ネットワーク アダプタをチームに割り当てる必要があります。

[Large Send Offload/ 大量送信オフロード](LSO)、[Checksum Offload/ チェックサム オフロード](CO)、および [RSS] は、LSO、CO、および RSS のプロパティが、チームに対してサポートされていることを示します。LSO、CO、および RSS のプロパティは、すべてのメンバーが機能をサポートし、その機能用に設定されている場合にのみ、チームに対してイネーブルされます。

注：ドライバが無効になっているチームにネットワーク アダプタを追加すると、チームのオフロード機能に悪影響を与える可能性があります。これはチームのパフォーマンスに影響を与える場合もあります。そのため、ドライバが対応しているネットワーク アダプタのみを、メンバーとしてチームに追加することをお勧めします。

8. **[チーム MTU]** に値を入力します。
9. **[作成]** をクリックしてチーム情報を保存します。
10. 手順 4. から 9. を繰り返して、追加のチームを定義します。チームが定義されると、そのチームがチーム リストから選択できるようになりますが、まだ作成はされていません。**[プレビュー]** タブをクリックして、チーム構造を確認してから変更を適用します。
11. **[適用]/[終了]** をクリックして、定義したすべてのチームを作成し、[チームの管理] ウィンドウを閉じます。
12. ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、**[はい]** をクリックします。

メモ：

- チーム名は最大 39 文字で、スペースで開始することはできず、以下の文字は使用できません：
  & \ / : * ? < > |
- チーム名は一意の名前にする必要があります。すでに使用しているチーム名を再度指定しようとすると、名前がすでに存在していることを示すエラー メッセージが表示されます。
- 1 チームの最大メンバー数は 8 件です。
- チームの設定が正しく実行されると、設定が済んだそれぞれのチームに仮想チーム アダプタ ドライバが 1 つずつ作成されます。
- いったんディスエーブルにした仮想チームを再度イネーブルにする場合は、すべてのチーム メンバーをいったんディスエーブルにし再度イネーブルにしてから、仮想チームをイネーブルします。
- 通有中継チームとリンク集約チームを作成した場合は、スタンバイ メンバーを指定することはできません。スタンバイ メンバーは、スマート ロード バランスおよびフェイルオーバー チームかスマート ロード バランス (自動フォールバックはディスエーブル) チームでのみ動作します。
- スマート ロード バランス (自動フォールバックはディスエーブル) チームについては、スタンバイ メンバーから Load Balance メンバーへのトラフィックを復元する場合、[チームプロパティ] タブの [フォールバック] ボタンをクリックします。
- SLB チームを設定するとき、チーム メンバーのハブへの接続がテストのためにサポートされていますが、チーム メンバーをスイッチへ接続することをお勧めします。
- 他社製のネットワーク アダプタについては、チーム化をサポートしていなかったり完全認定していないものもあります。

13. チーム IP アドレスを設定します。
    a. **[コントロール パネル]** で、**[ネットワーク接続]** をダブルクリックします。
    b. 設定するチームの名前を右クリックし **[プロパティ]** をクリックします。
    c. **[全般]** タブで、**[インターネット プロトコル (TCP/IP)]** をクリックし、**[プロパティ]** をクリックします。
    d. そのチームについて、IP アドレスや他に必要な TCP/IP コンフィギュレーションを設定し、終了したら **[OK]** ボタンをクリックします。

チームの変更

チームを作成したら、以下の方法でチームを変更することができます。

- チーム タイプの変更
- チームに割り当てられたメンバーの変更
- VLAN の追加

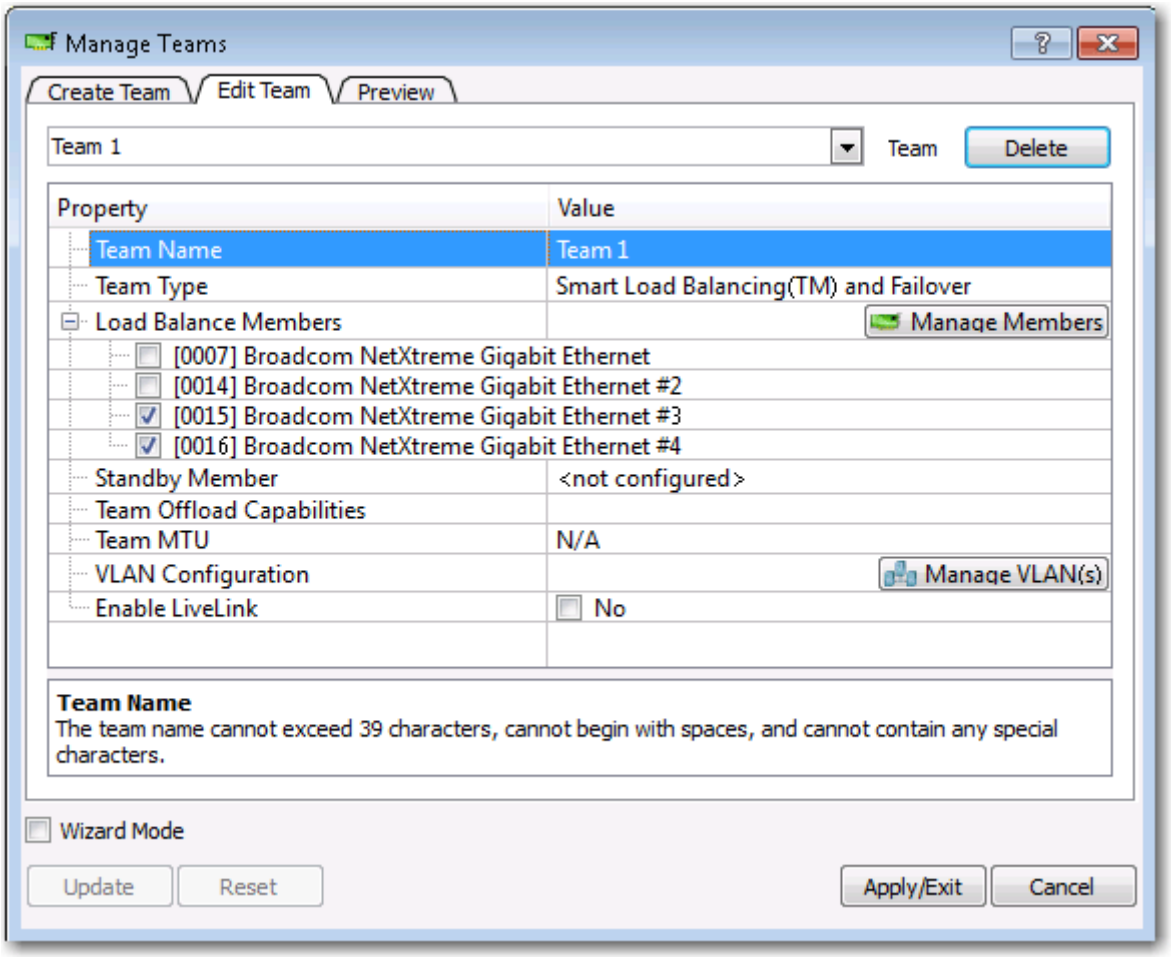
- VLAN の変更 (エキスパート モードを使用)
- チームまたは VLAN の削除 (エキスパート モードを使用)

チームを変更するには :

1. **[チーム]** メニューから **[チームの編集]** をクリックするか、リストでチームのいずれかを右クリックして **[チームの編集]** を選択します。このオプションは、チームがすでに作成されていて [チームの管理] ペインに表示されている場合のみ使用できます。
2. ウィザードの初期画面が表示されます。**[次へ]** をクリックしてウィザードを使用してチームの変更を続行するか、**[エキスパート モード]** をクリックしてエキスパート モードで操作します。

注 : エキスパート モードで **[チームの編集]** タブが表示されるのは、システム上に設定済みのチームがある場合のみです。

3. **[チームの編集]** タブをクリックします。



4. 必要な変更を行ったら、**[更新]** をクリックします。変更内容はまだ適用されていません。**[プレビュー]** タブをクリックして、更新したチーム構造を確認してから変更を適用します。
5. **[適用]/[終了]** をクリックして更新を適用し、[チームの管理] ウィンドウを閉じます。
6. ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、**[はい]** をクリックします。

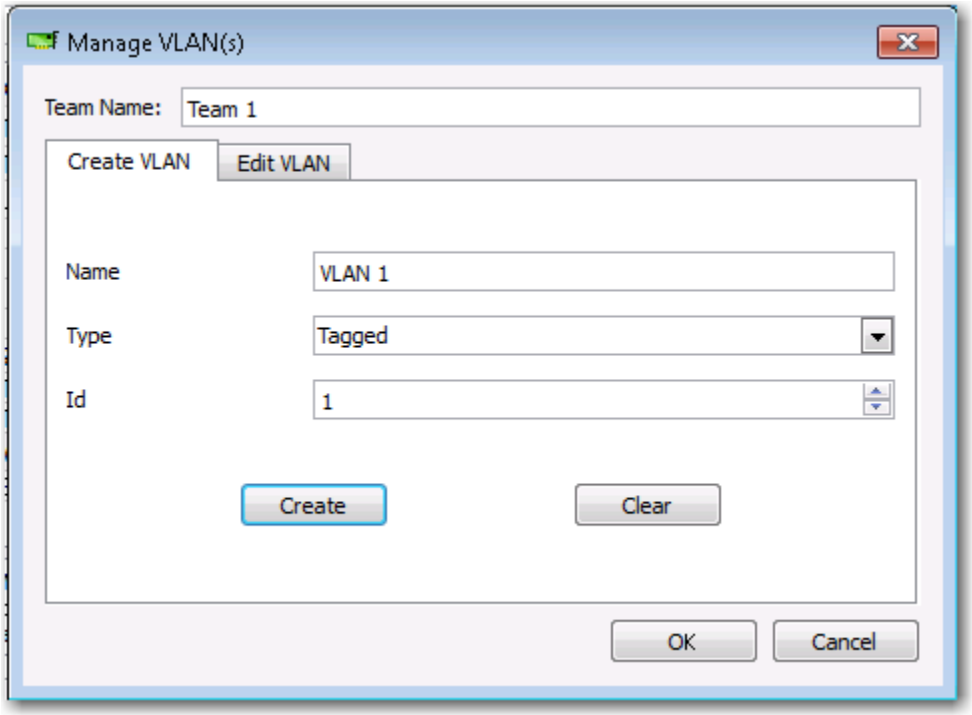
VLAN の追加

チームに複数の仮想 LAN (VLAN) を追加できます。これにより、異なるサブネット上にある複数の仮想アダプタを追加できます。複数のサブネットに所属することが可能な 1 つのネットワーク アダプタを、利用中のシステムに装備できるようになります。VLAN を利用すると、Load Balance メンバーのロード バランシング機能が連結でき、フェイルオーバー アダプタも採用できるようになります。

1 つのチームには、64 件まで VLAN を定義することができます (タグ付けされた VLAN 63 件、タグ付けされていない VLAN 1 件)。ただし、すべてのチーム メンバーが Broadcom アダプタでないと VLAN は作成できません。Broadcom 以外のアダプタで VLAN を作成しようとすると、エラーメッセージが表示されます。

VLAN 環境でチームを設定するには :

1. **[チーム]** メニューから **[VLAN の追加]** を選択します。
2. 初期画面が表示されます。
3. **[エキスパート モード]** をクリックします。
4. **[チームの管理]** ウィンドウの **[チームの作成]** タブで **[VLAN の管理]** をクリックします。
5. VLAN 名を入力してから、タイプと ID を選択します。
6. **[作成]** をクリックして VLAN 情報を保存します。VLAN が定義されると、その VLAN はチーム名リストから選択できるようになりますが、まだ作成はされていません。
7. この手順を繰り返してすべての VLAN を定義し、定義し終わったら **[OK]** をクリックして作成します。



8. ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、**[はい]** をクリックします。

注 : アダプタ性能を最適な状態に保つためには、アダプタごとに作成される 8 つの VLAN それぞれに、64 MB のシステム メモリが必要です。

VLAN プロパティと統計を表示し VLAN テストを実行するには

VLAN プロパティと統計を表示し、VLAN テストを実行するには：

1. 一覧表示されている VLAN のいずれかを選択します。
2. VLAN アダプタのプロパティを表示するには、**[情報]** タブをクリックします。
3. VLAN アダプタの統計を表示するには、**[統計]** タブをクリックします。
4. VLAN アダプタでネットワーク テストを実行するには、**[診断]** タブをクリックします。

VLAN の削除

エキスパート モードの場合は、以下の手順が適用されます。

VLAN を削除するには：

1. 削除する VLAN を選択します。
2. **[チーム]** メニューから **[VLAN の削除]** を選択します。
3. **[適用]** をクリックします。
4. ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、**[はい]** をクリックします。

注：チームを削除すると、そのチームに設定されている VLAN もすべて削除されます。

スマート ロード バランスおよびフェイルオーバー / スマート ロード バランス (自動フォールバックはディスエーブル) チームの LiveLink を設定する

LiveLink は BASP の機能であり、チーム タイプがスマート ロード バランス (SLB) および スマート ロード バランス (自動フォールバックはディスエーブル) の場合に使用できます。LiveLink は、スイッチで発生したリンク ロスを検出し、リンクが有効になっているチーム メンバーのみのトラフィックをルーティングします。

LiveLink を設定する前に、以下の事項をお読みください。

メモ：

- LiveLink™ を設定する前に、「LiveLink」の説明をお読みください。また、指定するプローブの各対象が利用可能かつ動作していることも確認してください。プローブ対象となる IP アドレスが何らかの理由で変更された場合、LiveLink を再設定する必要があります。何らかの理由でプローブ対象の MAC アドレスが変わった場合、チームを再起動する必要があります (「トラブルシューティング」を参照)。
- プローブ対象は、チームと同じサブネット上にあり、有効 (同報通信、マルチキャスト、ユニキャストではない) で静的な IP アドレスを割り当てられ、どのような場合でも使用できる (常時オンの状態) 必要があります。
- プローブ対象にネットワークが接続されていることを確認するために、チームから ping コマンドを使いプローブの対象を調べます。
- 最大 4 個のプローブ対象を指定することができます。
- プローブ対象またはチーム メンバーに割り当てられる IP アドレスでは、最初または最後の 8 ビットにゼロを指定できません。

LiveLink を設定するには：

1. **[チーム]** ニューから **[チームの編集]** を選択します。
2. [エキスパート モード] をクリックします (チーム化ウィザードで LiveLink を設定する方法については、Broadcom チーム化ウィザードを使用するを参照してください)。
3. [メンバーの管理] ウィンドウでの **[チームの編集]** タブをクリックします。
4. **[ライブリンクをイネーブルする]** を選択します。[ライブリンク設定] のオプションが下部に表示されます。
5. **[プローブ インターバル]** (プローブ対象に対するリンク パケットの各再転送間隔の秒数) および **[プローブ最大再送回数]** (フェイルオーバーが発生する前にプローブ対象からの応答を連続して受信しない回数) のデフォルト値をそのまま利用することをお勧めします。異なる値を指定するには、**[プローブ インターバル (秒)]** リストからプローブのインターバル、**[プローブ最大再送回数]** リストからプローブの最大再送回数をそれぞれ選択します。
6. プローブ対象が存在する VLAN に対応するよう **[プローブ VLAN ID]** を設定します。これにより、接続されているスイッチ ポートの共有構成に基づいて適切な VLAN タグがリンク パケットに適用されます。

注：LiveLink がイネーブルされた各チームは、1 つの VLAN のプローブ対象とのみ通信できます。また、VLAN ID 0 とは、タグなしネットワークを意味します。

7. **[対象 1 のプローブ]** を選択し、1 つまたはすべてのプローブ対象の対象 IP アドレスを選択します。

注：1 つ目のプローブ対象のみが必須です。他のプローブ対象に IP アドレスを割り当てることで、プローブ対象を最大 3 個までバックアップとして追加することができます。

8. 一覧表示されているチーム メンバーのいずれかを選択し、メンバー IP アドレスを入力します。

注：すべてのメンバー IP アドレスは、プローブ対象と同一のサブネットにある必要があります。

9. **[更新]** をクリックします。これらの手順を繰り返し、リストにある他のチーム メンバーの設定を行います。

10. [適用]/[終了] をクリックします。

設定の保存と復元

設定を保存するには :

1. **[ファイル]** メニューの **[チームに名前を付けて保存]** を選択します。
2. *新しい設定ファイルのパスと名前*を入力し、**[保存]** をクリックします (ファイル名には .bcg 拡張子が付加されます)。

   この設定ファイルはテキスト ファイルです。このため、どんなテキスト エディタでも表示できます。このファイルには、アダプタとチーム設定に関する情報が格納されます。

設定を復元するには :

1. **[ファイル]** メニューの **[チームの復元]** を選択します。
2. 復元するファイルの名前をクリックし、**[開く]** をクリックします。

注 : 必要に応じて、ファイルが保存されているフォルダに移動してください。

3. **[適用]** をクリックします。
4. ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、**[はい]** をクリックします。
5. 設定がすでにロードされている場合は、現在の設定を保存するかどうかを確認するメッセージが表示されます。現在の設定を保存するには、**[はい]** をクリックします。保存しないと、現在ロードされている設定データは失われます。

注 : チームが多くの VLAN や静的 IP アドレスと関連付けて設定されている場合、チームの復元には、非常に長い時間がかかる可能性があります。

BASP 統計を表示する

[統計] セクションには、チームのネットワーク アダプタに関するパフォーマンス情報が表示されます。

チーム メンバー アダプタのいずれか、またはチーム全体の BASP 統計情報を表示するには、[チームの管理] ペインに一覧表示されているアダプタまたはチームの名前をクリックして、**[統計]** タブをクリックします。

[更新] をクリックすると、各統計の最新値が表示されます。**[リセット]** をクリックすると、すべての値がゼロになります。

Tx. パケット . 転送されたパケットの数です。

Tx. 廃棄パケット . 廃棄されたパケットの数です。

Tx. キューに入れられたパケット . キューに入れられたパケットの数です。

Rx. パケット . 受信したパケットの数です。

Rx. 廃棄パケット . 廃棄されたパケットの数です。

再送プローブ . フェイルオーバーが発生する前にプローブ対象からの応答を連続して受信しない回数です。

コマンド ライン インターフェイス ユーティリティで設定する

Broadcom ネットワーク アダプタを設定する場合、BACS の代わりに BACSCLI を使用することができます。これは、ネットワーク アダプタの情報表示と設定に利用できる Broadcom ユーティリティであり、コンソールを使用して、対話形式ではないコマンド ライン インターフェース (CLI) モードまたは対話形式のモードを利用できます。BACS と同様に、BACSCLI では、各ネットワーク アダプタの情報が表示され、詳細なテストや診断の実行、統計情報の表示、プロパティ値の変更が可能です。また BACSCLI では、ロード バランシングとフェイルオーバーのために、ネットワーク アダプタをチーム化することができます。

使用可能なコマンドとサンプルの完全なリストについては、Dell により提供された CD に保存されている BACSCLI の ReadMe テキスト ファイルを参照してください。

Broadcom NetXtreme I および NetXtreme II ネットワーク アダプタを搭載したシステムでは、インストーラで BACS がインストールされるときに BACSCLI もインストールされます。

BACS のトラブルシューティング

トラブル：Linux システム上で BACS を開こうとしたときに、次のエラー メッセージが表示されます。

> 「Another instance of the BACS client appears to be running on this system. (このシステム上で、BACS クライアントの別のインスタンスが実行されているようです。) Only one instance of the BACS client can be running at a time. (一度に実行できる BACS クライアントのインスタンスは 1 つのみです。) If you are sure that no other BACS client is running, then a previous instance may have quit unexpectedly. (他の BACS クライアントが動作していないと考えられる場合、以前のインスタンスが予期せずに終了された可能性があります。)」

ソリューション：BACS の 2 番目のインスタンスを実行しようとしたときに、このメッセージが表示されます。このメッセージが表示されたときに、BACS の他のインスタンスが現在実行されていないことが確実な場合、BACS の以前のインスタンスが予期せずに終了した可能性があります。そのようなインスタンスをクリアするには、次のファイルを削除します。"/dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0}"。

セクション 14: 仕様

10/100/1000BASE-T ケーブルの仕様

表 22:10/100/1000BASE-T ケーブルの仕様

ポート タイプ	コネクタ	メディア	最長距離
10BASE-T	RJ-45	CAT3、CAT4、または CAT5 の非シールドより対線 (UTP)	100 メートル (328 フィート)
100/1000BASE-T[1]	RJ-45	CAT 5[2] の UTP	100 メートル (328 フィート)

[1]1000BASE-T の信号送信には、ISO/IEC 11801：1995 および ANSI/EIA/TIA-568-A (1995) で規定されている、CAT5 の平衡ケーブル配線のツイストペア (より対線) が 4 本必要です。また、TIA/EIA TSB95 で定義されているテスト手順を利用した付加的な性能テストも必要となります。

[2] CAT 5 は必要最低限の要件です。CAT 5e と CAT 6 は完全にサポートされます。

性能の仕様

表 23: 性能の仕様

機能	仕様
PCI Express™ タイプ コントローラ (BCM57XX コントローラ)	
PCI Express インターフェイス	x1、x2、x4 リンク幅
PCI Express 合計帯域幅 (転送および受信)	2.5 Gbps または 5.0 Gbps
10/100/1000BASE-T	10/100/1000 Mbps (完全二重通信方式)

セクション 15: 法規制情報

FCC クラス B 通告

Broadcom NetXtreme Gigabit Ethernet Controller
BCM95721A211
BCM95722A2202

当機器は、FCC (米連邦通信委員会) 標準の第 15 部に準拠しており、その動作は以下の 2 つの条件に準じています。1) 当装置は有害な干渉を起こさない。2) 当機器は、予期せぬ動作をもたらす可能性のある干渉も含む、あらゆる干渉を許容できる。

当機器は、FCC 標準の第 15 部によるクラス B デジタル デバイスの制限に準じるものであることが試験により明らかになっています。この制限は、住宅地環境での有害な受信干渉に対して適正な保護を与えることを目的に設定されています。当機器は、無線周波数エネルギーを生成、利用するとともに、無線周波数エネルギーを放射するため、取扱説明書に従わずに設置が行われた場合には、無線通信に有害な干渉を引き起こす恐れがあります。ただし、特定の設置状況で干渉が発生しないことは保証できません。有害な干渉が機器から発生しているかどうかは、電源を入れたり切ったりすることで確認できます。当機器が無線 (ラジオ) またはテレビの受信に有害な干渉をもたらしている場合は、以下のいずれかの解決方法をお試しください。

- 受信アンテナの向きを変えたり、設置場所を移動する。
- 当機器と受信機器との距離を広げる。
- 受信機器が接続されている回路とは異なる回路の出力に接続する。
- 販売代理店か、無線、ラジオ、テレビに詳しい技術者に相談する。

当機器に対し、機械的または電気的な改良は加えないでください。

注：Broadcom 社の許可なくアダプタの改造または修理を行うと、機器を使用する権利が無効となる場合があります。

Broadcom Corporation
190 Mathilda Place
Sunnyvale, California 94086 USA

VCCI クラス B 通告

当機器は、VCCI (Voluntary Control Council for Information Technology Equipment、情報処理装置等電波障害自主規制協議会) の基準に基づくクラス B の条件を満たしています。家庭環境で、無線 (ラジオ) やテレビの受信機の近くで当機器を使用すると、無線干渉を起こす場合があります。当機器は取扱説明書に従って、設置・利用してください。

⚠ **注意事項** : 周波数が 59 ～ 66 MHz の伝導無線周波数エネルギーが存在する場合には、当機器に障害が発生する可能性がありますが、RF のエネルギー発生源が取り除かれると通常動作に戻ります。

VCCI クラス B 通告 (日本)

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。

CE の通告

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.
PORTUGUÊS 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.

カナダの法規制に関する情報 (カナダのみ)

カナダ産業省、クラス B

当クラス B デジタル機器は Canadian ICES-003 に準拠しています。

通告：カナダ産業省の規制により、Broadcom による明確な承認を得ずに変造や改造を加えた場合には、当機器の利用権限が無効になります。

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.

MIC の通告 (韓国のみ)

B クラス デバイス

Broadcom NetXtreme Gigabit Ethernet Controller
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

当機器は、非事業用として承認を受けているものであり、住宅地域などのあらゆる環境でご利用いただけます。

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。

セクション 16: トラブルシューティング

ハードウェアの診断

アダプタ ハードウェアをテストするためのループバック診断テストが利用できます。ループバック診断テストでは、パケット情報が物理リンクに転送されるため、アダプタ内部・外部の診断が可能になります。Windows 環境の場合は診断テストを実行するを参照してください)。

BACS 診断テストの失敗

BACS の 診断テストを実行するタブで診断テストを実行していて、次のテストのいずれかが失敗した場合、システムに取り付けた NIC または LOM にハードウェアの問題がある可能性があります。

- 制御レジスタテスト
- MII レジスタ
- EEPROM
- 内部メモリ
- チップ上 CPU
- キャンセル
- ループバック - MAC
- ループバック - PHY
- LED テスト

ここでは、失敗の解決に役立つトラブルシューティングの手順を説明します。

1. 失敗したデバイスを取り外し、スロットに再度取り付けて、カードがスロット全体にわたってしっかりと固定されていることを確認します。
2. テストを再実行します。
3. テストが再度失敗する場合は、同じモデルの別のカードに交換してテストを実行します。正常なカードでテストにパスした場合は、テストに失敗したデバイスについて、ハードウェア ベンダーにお問い合わせください。
4. マシンの電源を切り、マシンから AC 電源を取り外してシステムを再起動します。

5. 診断ソフトウェアを削除して、再インストールします。
6. ハードウェア ベンダーに問い合わせてください。

BACS ネットワーク テストの失敗

通常、BACS ネットワークをテストするが失敗するのは、ネットワークまたは IP アドレスの設定に問題があります。ここでは、ネットワークのトラブルシューティングを行う場合の一般的な手順を説明します。

1. ケーブルが接続されており、適切なリンクが確立されていることを確認します。
2. ドライバがロードされ、イネーブルになっていることを確認します。
3. NIC/LOM に接続されているケーブルを交換します。
4. 「ipconfig」コマンドを使用するか、または OS IP 割り当てツールを確認して、IP アドレスが正しく割り当てられていることを確認します。
5. アダプタが接続されているネットワークに対して、IP アドレスが正しいことを確認します。

トラブルシューティングのチェックリスト

⚠ **注意事項**：システムのカバーを開ける前に、取り扱い注意事項をお読みください。

以下のチェックリストで、Broadcom NetXtreme Gigabit Ethernet アダプタの取り付け・実行時のトラブルを解消するための推奨アクションを確認してください。

- ケーブルと接続をすべて点検します。ネットワーク アダプタのケーブル接続やスイッチが正しく接続されていることを確認します。ケーブル長や定格がネットワーク ケーブルを接続するにリストされている要件に準じているかどうかを確認します。
- ハードウェアを取り付けるの内容を再確認し、アダプタの取り付けを点検します。アダプタがスロットに正しく固定されているかどうか確認します。ボードの構成部品や PCI エッジ コネクタなどに、すぐ目に付く損傷がないかなど、ハードウェアを確認します。
- コンフィギュレーション設定値を点検し、別のデバイスと競合している場合はそれを変更します。
- システムで使用している BIOS が最新のものであることを確認します。
- アダプタを別のスロットに挿入してみます。移動先でアダプタが動作する場合は、元のスロットに瑕疵があることが考えられます。
- 不良のあるアダプタを、正しい動作が確認されているアダプタと交換します。交換したアダプタがそのスロット内で動作すれば、元のアダプタに瑕疵があると考えられます。
- 機能の異なるシステムにそのアダプタを取り付け、もう一度テストを実行します。この新しいシステム内でアダプタがテストに合格した場合は、元のシステムに瑕疵がある場合があります。
- システムから他のアダプタをすべて取り外し、もう一度テストを実行します。アダプタがテストに合格した場合は、別のアダプタが競合を起こしていたことが考えられます。

ネットワーク リンクとアクティビティの状態を確認する

ポート LED が示すネットワーク リンクとアクティビティの状態を確認するには、ネットワークの接続性をテストするまたはアダプタ情報の表示を参照してください。

正しいドライバがロードされているかどうかを点検する

Windows

アダプタ、リンク ステータス、ネットワークの接続性などの参考となる情報を確認するには、アダプタ情報の表示を参照してください。

Linux

TG3 Linux ドライバが正しくロードされているかどうかを確認するときは、以下を実行します。

```
lsmod | grep tg3
```

ドライバがロードされていれば、以下のような結果が表示されます。*size* はドライバのサイズ (単位 : バイト) で、*n* は設定されているアダプタの個数です。

表 24:Linux ドライバ

モジュール	*size*	*利用元*
TG3	*size*	*n*

ケーブル長のテストを実行する

Windows 環境では、ケーブル長のテストを実行できます。ケーブル長のテストの実行については、ケーブルを分析するを参照してください。

ネットワークの接続性をテストする

注：リンク速度を強制したときは、アダプタとスイッチの両方が同じ速度に強制されているか、または、両側が自動ネゴシエーションに設定されていることを確認してください。

Windows

ping コマンドを使い、ネットワーク接続が動作しているかどうかを確認します。

注：ネットワークの接続性は、Broadcom Advanced Control Suite 2 のネットワークをテストする機能でもテストできます。

1. ドライバがロードされ、イネーブルになっていることを確認します。
2. ケーブルが接続されており、適切なリンクが確立されていることを確認します。
3. **[スタート]**、**[ファイル名を指定して実行]** の順にクリックします。
4. **[名前]** ボックスに **cmd** と入力し、**[OK]** をクリックします。
5. **ipconfig /all** と入力して、テストするネットワーク接続を表示します。
6. アダプタが接続されているネットワークに対して、IP アドレスが正しいことを確認します。
7. **ping IP address** と入力し、ENTER キーを押します。

表示される ping 統計は、ネットワーク接続が動作しているかどうかを示します。

Linux

イーサネット インターフェイスが立ち上がっているかどうかを確認するときは、**ifconfig** を実行し、イーサネット インターフェイスのステータスをチェックします。**netstat -i** を実行することで、イーサネット インターフェイス上の統計情報を確認することができます。**ifconfig** および **netstat** については、Linux ドライバ ソフトウェアをご覧ください。

ネットワーク上で IP ホストをピングして、接続が確立されるかどうかを確認します。

コマンド ラインに **ping IP address** と入力し、ENTER キーを押します。

表示される ping 統計は、ネットワーク接続が動作しているかどうかを示します。

Broadcom ブート エージェント

トラブル：PXE を使って DHCP からネットワークの設定値が入手できない。
ソリューション：正しく操作するためには、スパニング ツリー プロトコル (STP) がディスエーブルされているか、または PXE クライアントが接続されているポートで portfast モード (Cisco) がイネーブルされているかを確認してください。たとえば、スパンツリーの portfast には 4/12 をイネーブルするよう設定します。

BASP (Broadcom Advanced Server Program)

トラブル：チームの一部だった NIC を物理的に削除して再起動すると、チームは期待どおりに動作しなくなった。
ソリューション：システムからチーム化した NIC を物理的に削除するには、最初にチームから NIC を削除する必要があります。シャットダウンする前にこれを実行しておかないと、その後の再起動でチームが分割される可能性があります。これが原因で、チームが予期しない動作をすることがあります。

トラブル：INETCFG を使ってチームを変更した場合、変更が反映されない。
ソリューション：INETCFG でチームを変更した場合、変更を反映させるために、再度初期化してから再起動が必要な場合があります。

イーサネット経由のカーネル デバッグ

トラブル：Windows 8.0 または Windows Server 2012 システムで、イーサネット ネットワーク経由のカーネル デバッグを実行しようとすると、システムが起動されません。Windows 8.0 または Windows Server 2012 OS が UEFI モード向けに設定されているシステムでは、このトラブルが一部のアダプタで発生する可能性があります。UEFI プリブート環境では、ファームウェアのエラーが画面に表示され、マスク不可能割り込みの例外が発生したことが通知されることがあります。

ソリューション：Microsoft サポート技術情報文書 2920163「Non Maskable Interrupt error during boot on a system which has been configured for kernel debugging over Ethernet/ イーサネット経由でカーネル デバッグを実行するように設定されたシステムでは、起動時にマスク不可能割り込みエラーが発生する」を参照してください。

その他

トラブル：Large Send Offload (LSO、大量送信オフロード) と Checksum Offload (チェックサム オフロード) がチームで機能しない。
ソリューション：チームのアダプタのうちいずれか 1 つでも LSO をサポートしていない場合は、LSO はそのチームでは機能しません。LSO をサポートしないアダプタをチームから取り除き、LSO をサポートするアダプタと交換してください。Checksum Offload (チェックサム オフロード) の場合も同様です。