Broadcom® NetXtreme® BCM57XX-Benutzerhandbuch

Letzte Aktualisierung: Februar 2015

2CS57XX-CDUM513-R

Letzte Aktualisierung: Februar 2015

2CS57XX-CDUM513-R

Inhaltsverzeichnis

Abschnitt 1: Funktionen und Leistungsmerkmale

Funktionsbeschreibung

Mit den Broadcom NetXtreme Gigabit Ethernet-Adaptern kann ein PCI Express™-kompatibles System mit einem Gigabit Ethernet-Netzwerk verbunden werden. Broadcom NetXtreme Gigabit Ethernet-Adapter verfügen über eine Technologie, mit der Daten mit einer maximalen Übertragungsrate von einem Gigabit pro Sekunde, d. h. zehnmal schneller als mit Fast Ethernet-Adaptern, übertragen werden können.

Mithilfe der Broadcom Teaming-Software können Sie Ihr Netzwerk in virtuelle LANs (VLANs) aufteilen sowie mehrere Netzwerkadapter in Teams zusammenfassen, um die Funktionen für den Netzwerk-Lastausgleich und die Fehlertoleranz zu erhalten. Ausführliche Informationen über Teaming finden Sie unter Teaming und Broadcom Gigabit Ethernet Teaming Services. Eine Beschreibung von VLANs finden Sie unter Virtuelle LANs. Unter Konfigurieren der Teaming-Funktion finden Sie Anweisungen zum Konfigurieren der Teaming-Funktion und zum Erstellen von VLANs unter Windows-Betriebssystemen.

Leistungsmerkmale

In der folgenden Liste sind die Leistungsmerkmale des Broadcom NetXtreme Gigabit Ethernet Adapters für alle unterstützten Betriebssysteme aufgeführt:

- Integrierte Quad 10/100/ 1000BASE-T- und Quad 1000Base-X/SGMII 1,25 Gbaud SerDes-Transceiver
- Energieeffizient und Ethernet™-kompatibel mit IEEE Std 802.3az-2010
- Automatisches Aushandeln nach IEEE 802.3ap Absatz 73
- Quad 10/100/1000BASE-T-Vollduplex/Halbduplex-MACs
- Quad 1000BASE-X/SGMII-Vollduplex/Halbduplex-MACs
- Automatisches MDI-Crossover
- x4-PCI-Express v2.0 bei 5 GT/s und 2,5 GT/s
- MSI- und MSI-X-Funktionen – bis zu 17 MSIX-Vektoren
- I/O-Virtualisierungsunterstützung für VMware NetQueue und Microsoft VMQ
  - 17 Empfangswarteschlangen und 16 Sendewarteschlangen
  - 17 MSI-X-Vektorunterstützung pro Warteschlangen-Interrupt zum Host
- Flexibler MSI-X-Vektor zur Übertragung und zum Empfang der Warteschlangenverknüpfung
- TLP Processing Hint (TPH) ECN an die PCI Express Base Specification v2.0
- Funktionsebene zurücksetzen
- Receive Side Scaling (RSS) mit MSI-X-Vektorunterstützung pro Warteschlange und Unterstützung für UDP-RSS Hash Type
- Transmit Side Scaling (TSS) und Multi-Tx-Warteschlange mit MSI-X-Vektorunterstützung pro Warteschlange
- Jumbo Frame-Support für Payload mit bis zu 9600 Byte
- Unterstützung für Virtual LAN (VLAN) – IEEE 802.1q VLAN-Tagging
- TCP-, IP-, UDP-Prüfsummenverschiebung
- LSO (LLarge Send Offload), TCP Segmentation Offload (TSO)
- Hardwareunterstützung für IEEE 1588- und IEEE 802.1AS-Zeitsynchronisierungsimplementierungen
- IEEE 802.3x Flow Control
- SMBus 2.0-Schnittstelle
- Statistische Daten für SNMP MIB II, Ethernet-ähnlicher MIB und Ethernet MIB (IEEE 802.3z, Absatz 30)
- ACPI-Energieverwaltungs-Compliance
- Advanced Power Management über eine Central Power Management Unit (CPMU)
- Effizienter integrierte Schaltregler-Controller
- Auf dem Chip integrierte Temperaturüberwachung
- PCI Express CLKREQ-Unterstützung
- Power Management Offload (PM Offload)
- Unterstützung für seriellen Flash und EEPROM-NVRAM, automatische Flash-Konfiguration
- ECC-Fehlererkennung und -korrektur am internen SRAM
- Unterstützung für JTAG-Boundary-Scan

Energieverwaltung

Wake-on-LAN (Magic Packet, Wake Up Frame, bestimmte Muster) wird unterstützt.

Hinweis: Die Übertragungsrate des Adapters beträgt entweder 10 Mbit/s oder 100 Mbit/s, wenn das System heruntergefahren ist und auf ein Reaktivierungssignal wartet. Sie kann jedoch erneut 1000 Mbit/s erreichen, wenn das System wieder aktiv ist, falls es an einen 1000 Mbit/s-kompatiblen Switch angeschlossen ist. Systeme, die Wake on LAN (WOL) verwenden sollen, müssen an einen Switch angeschlossen werden, der mit Raten von 1000 und 10/100 Mbit/s kompatibel ist.

Adaptive Interrupt-Frequenz

Der Adaptertreiber passt die Host-Interrupt-Frequenz je nach den Datenverkehrsbedingungen intelligent an, um den Gesamtdurchsatz der Anwendungen zu erhöhen. Bei geringem Datenverkehr generiert der Adaptertreiber für jedes empfangene Paket einen Interrupt auf dem Host und verringert so die Latenz. Bei hohem Datenverkehr generiert der Adapter einen Host-Interrupt für mehrere eingehende Back-to-Back-Pakete und trägt so zum Erhalt der CPU-Zyklen des Hosts bei.

Zwei DMA-Kanäle

Die PCIe-Schnittstelle des Broadcom NetXtreme Gigabit Ethernet Adapters verfügt über zwei unabhängige DMA-Kanäle für gleichzeitig ablaufende Lese- und Schreibvorgänge.

ASIC mit eingebettetem RISC-Prozessor

Die Kernsteuerung für den Broadcom NetXtreme Gigabit Ethernet-Adapter befindet sich in einem eng integrierten Hochleistungs-ASIC. Der ASIC umfasst einen RISC-Prozessor. Diese Funktion bietet die notwendige Flexibilität, um durch Software-Downloads neue Funktionen zur Karte hinzufügen und sie an künftige Netzwerkanforderungen anpassen zu können.

BroadcomNetXtreme-Verwaltungsfunktionen, wie z. B. DMTF, SMASH, DASH und NC-SI-Passthrough laufen auf einer High-Performance Application Processor Engine (APE) getrennt vom herkömmlichen Netzwerkprozessor.

Broadcom Advanced Control Suite

Bei der Broadcom Advanced Control Suite (BACS), einer Komponente der Broadcom Teaming-Software, handelt es sich um ein integriertes Dienstprogramm, das nützliche Informationen über jeden der auf dem System installierten Netzwerkadapter zur Verfügung stellt. Mit dem BACS-Dienstprogramm können Sie außerdem ausführliche Tests, Diagnosen und Analysen für jeden Adapter vornehmen sowie die Eigenschaftswerte für die einzelnen Adapter ändern und die Netzwerkstatistiken anzeigen. BACS wird unter Windows-Betriebssystemen zum Konfigurieren der Teaming-Funktion sowie zum Hinzufügen von VLANs verwendet. Ausführliche Informationen und Anweisungen finden Sie unter Verwenden der Broadcom Advanced Control Suite.

Unterstützte Betriebsumgebungen

Der Broadcom NetXtreme Gigabit Ethernet-Adapter wird von folgenden Betriebssystemen unterstützt:

- Microsoft® Windows® (32-Bit- und 64-Bit-Erweiterungen)
- Linux® (32-Bit- und 64-Bit-Erweiterungen)
- VMware
- Oracle Solaris

Netzwerkverbindung und Betriebsanzeige

Bei Ethernet-Anschlüssen über Kupferdraht wird der Status der Netzwerkverbindung und -betrieb wie unter Tabelle 1: "Port-LED-Anzeige des RJ-45 für Netzwerkverbindung und -betrieb" auf Seite 14 beschrieben durch die LEDs am Anschluss RJ-45 angezeigt. Broadcom Advanced Control Suite liefert darüber hinaus Informationen zum Status der Netzwerkverbindung und des Betriebs (siehe Anzeigen von Adapterinformationen).

Tabelle 1. Port-LED-Anzeige des RJ-45 für Netzwerkverbindung und -betrieb

Port-LED	*LED-Anzeige*	*Netzwerkstatus*
LINK-LED (Verbindung)	Aus	Keine Verbindung (Kabel abgetrennt)
	Leuchtet konstant	Verknüpfung
ACT-LED (Betrieb)	Aus	Kein Netzwerkbetrieb
	Blinkend	Netzwerkbetrieb

Abschnitt 2: Teaming

Hinweis: Im Abschnitt Broadcom Gigabit Ethernet Teaming Services finden Sie ausführliche Informationen zu folgenden Themen:

- Glossar zu Begriffen und Akronymen
- Teaming-Begriffe
- Softwarekomponenten
- Hardwareanforderungen
- Unterstützte Funktionen nach Teamart
- Auswählen einer Teamart
- Teaming-Verfahren
- Architektur
- Teamarten
- Vom Betriebssystem unterstützte Treiber
- Unterstützte Teaming-Raten
- Teaming und andere erweiterte Netzwerkfunktionen
- Allgemeine Netzwerkaspekte
- Anwendungsaspekte
- Behebung von Teaming-Problemen
- Häufig gestellte Fragen
- Ereignisprotokollmeldungen

Überblick

Beim Adapter-Teaming können Sie Netzwerkadapter zu einem Team zusammenfassen. Zu den Vorteilen von Teaming gehören zum Beispiel VLAN-Mitgliedschaften, Lastausgleich zwischen Adaptern und Fehlertoleranz. Diese Vorteile können so kombiniert werden, dass Sie die Lastausgleichsfunktion für die Lastausgleichsmitglieder mit einem Failover koppeln können, wobei das Team auf verschiedenen VLANs teilnimmt.

Broadcom Advanced Server Program (BASP) ist die Teaming-Software von Broadcom. Bei Windows-Betriebssystemen wird BASP über das Dienstprogramm Broadcom Advanced Control Suite (BACS) konfiguriert. Bei Linux-Betriebssystemen erfolgt das Teaming über Channel Bonding (siehe Teaming-Funktion mit Channel Bonding).

BASP unterstützt vier Arten von Lastausgleichsteams:

- Smart Load Balancing und Failover
- Link Aggregation (802.3ad)
- Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static
- SLB (Auto-Fallback deaktiviert)

Lastausgleich und Fehlertoleranz

Die Teaming-Funktion bietet einen Ausgleich der Datenverkehrslast sowie eine Fehlertoleranz (redundanter Adapterbetrieb bei Ausfall einer Netzwerkverbindung). Sind mehrere Adapter im selben System installiert, können Sie diese in bis zu 16 Teams zusammenfassen.

Jedes Team kann bis zu acht Adapter enthalten, wobei ein Adapter als Standby für die Teamarten Smart Load Balancing und Failover (SLB) oder SLB (Auto-Fallback deaktiviert) verwendet wird. Wird bei einer der Verbindungen des Adapter-Teams kein Datenverkehr festgestellt, weil ein Adapter, ein Kabel oder ein Switch ausgefallen ist, wird die Last an die verbleibenden Teammitglieder mit einer aktiven Verbindung verteilt. Falls alle Primäradapter ausfallen, wird der Datenverkehr an den Standby-Adapter weitergegeben. Die bestehenden Sitzungen bleiben erhalten, und die Situation hat keinerlei Auswirkungen auf die Benutzer.

Teamarten

In folgender Tabelle werden die für die unterstützten Betriebssysteme verfügbaren Teamarten aufgeführt:

Tabelle 2. Teamarten

Betriebssystem	Verfügbare Teamarten
Windows Server 2008 und Windows Server 2012	Smart Load Balancing und Failover Link Aggregation (802.3ad) Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static SLB (Auto-Fallback deaktiviert) **HINWEIS**: Windows Server 2012 bietet integrierten Teaming-Support, das NIC-Teaming. Es wird nicht empfohlen, dass Benutzer gleichzeitig bei mehreren Adaptern Teams über NIC-Teaming und BASP aktivieren.
Linux	Die Team-Adapter verwenden das Kernel-Modul für das Bonding sowie eine Schnittstelle für das Channel Bonding. Weitere Informationen erhalten Sie in Ihrer Linux-Dokumentation.

Smart Load Balancing™ und Failover

Smart Load Balancing™ und Failover ist das von Broadcom implementierte Verfahren zum Lastausgleich und basiert auf dem IP-Fluss. Mit dieser Funktion kann der IP-Verkehr bidirektional über mehrere Adapter (Teammitglieder) ausgeglichen werden. Bei dieser Teamart verfügen alle Adapter des Teams über separate MAC-Adressen. Diese Teamart ermöglicht die automatische Fehlererkennung und eine dynamische Ausfallsicherung durch ein anderes Teammitglied oder ein Hot Standby-Element. Dies erfolgt unabhängig vom Schicht-3-Protokoll (IP) bzw. kann in Verbindung mit vorhandenen Schicht-2- und Schicht-3-Switches verwendet werden. Für diese Teamart ist keine Switch-Konfiguration (wie Trunking oder Link Aggregation) erforderlich.

HINWEISE:

- Wenn Sie LiveLink™ beim Konfigurieren von SLB-Teams nicht aktivieren, wird empfohlen, das Spanning Tree Protocol (STP) an dem Switch oder dem Anschluss zu deaktivieren. Dadurch werden die Ausfallzeiten beim Failover auf Grund der Schleifen-Berechnung nach dem Spanning Tree-Algorithmus reduziert. Probleme dieser Art werden von LiveLink entschärft.
- Wenn die Übertragungsrate der Verbindung bei einem Teammitglied 1000 Mbit/s beträgt und bei einem anderen Teammitglied 100 Mbit/s, wird der größte Teil des Datenverkehrs von dem Teammitglied mit der 1000-Mbit/s-Verbindung bewältigt.

Link Aggregation (802.3ad)

Dieser Modus unterstützt Link Aggregation und entspricht dem IEEE-Standard 802.3ad (LACP). Mit der Konfigurationssoftware können Sie dynamisch festlegen, welche Adapter einem bestimmten Team angehören. Wenn der Verbindungspartner nicht richtig für die Verbindungskonfiguration 802.3ad konfiguriert ist, werden die Fehler erkannt und protokolliert. In diesem Modus sind alle Adapter für den Empfang von Paketen unter derselben MAC-Adresse konfiguriert. Das Lastausgleichsschema für den ausgehenden Datenverkehr wird durch den BASP-Treiber bestimmt. Das Lastausgleichsschema für ankommende Datenpakete wird dagegen durch den Verbindungspartner des Teams festgelegt. In diesem Modus muss mindestens einer der Verbindungspartner aktiv sein.

Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static

Die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static ist der Teamart Link Aggregation (802.3ad) in der Hinsicht sehr ähnlich, dass alle Adapter des Teams für den Empfang von Paketen unter derselben MAC-Adresse konfiguriert werden. Die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static) bietet jedoch keine LACP- oder Marker-Protokoll-Unterstützung. Diese Teamart unterstützt eine Vielzahl von Umgebungen, in denen die Adapterverbindungspartner zur Unterstützung eines proprietären Trunking-Verfahrens statisch konfiguriert sind. Mit dieser Teamart könnte beispielsweise OpenTrunk von Lucent oder Fast EtherChannel (FEC) von Cisco unterstützt werden. Bei dieser Teamart handelt es sich im Prinzip um eine vereinfachte Version der 802.3ad Link Aggregation. Der hier zugrunde liegende Ansatz ist wesentlich einfacher, da kein formalisiertes Link Aggregation-Steuerungsprotokoll (LACP) verwendet wird. Wie bei anderen Teamarten erfolgen die Teamerstellung und die Zuordnung der physischen Adapter zu den verschiedenen Teams statisch über die Benutzerkonfigurations-Software.

Die Teamart Allgemeines Trunking (FEC/GEC/802.3ad-Draft Static) unterstützt Load Balancing (Lastausgleich) und Failover (Ausfallsicherung) für den ankommenden und abgehenden Datenverkehr.

SLB (Auto-Fallback deaktiviert)

Die Teamart SLB (Auto-Fallback deaktiviert) ist mit der Teamart Smart Load Balancing und Failover bis auf eine Ausnahme identisch: Wenn das Standby-Mitglied aktiv ist und ein primäres Mitglied die Verbindung wiederhergestellt hat, verwendet das Team weiterhin das Standby-Mitglied, anstatt wieder auf das primäre Mitglied umzuschalten.

Wird ein primärer Adapter, der einem Team zugewiesen ist, deaktiviert, fungiert das Team als ein Team der Art "Smart Load Balancing" und "Failover", in dem Auto-Fallback auftritt.

Alle primären Schnittstellen in einem Team sind durch das Senden und Empfangen von Teilmengen des gesamten Datenverkehrs an Lastausgleichsvorgängen beteiligt. Standby-Schnittstellen übernehmen diese Funktion, wenn die Verbindungen für alle primären Schnittstellen unterbrochen werden.

Das Failover-Teaming ermöglicht bei Ausfall einer Netzwerkverbindung einen redundanten Adapterbetrieb (Fehlertoleranz). Wenn die Verbindung des Primäradapters in einem Team aufgrund eines Adapter-, Kabel- oder Switch-Port-Ausfalls unterbrochen wird, wird das sekundäre Teammitglied aktiviert und leitet sowohl den ankommenden als auch den abgehenden Datenverkehr, der ursprünglich dem Primäradapter zugewiesen wurde, weiter. Sitzungen bleiben erhalten, und die Situation hat keinerlei Auswirkungen auf die Benutzer.

Einschränkungen bei den Teamarten Smart Load Balancing und Failover/SLB (Auto-Fallback deaktiviert)

Bei **Smart Load-Balancing™ (SLB)** handelt es sich um ein Schema für ein bestimmtes Protokoll.

Tabelle 3. Smart Load Balancing

Betriebssystem	***Failover/Fallback: Nur Broadcom***	***Failover/Fallback: Herstellerunabhängig***
Protokoll	***IP***	***IP***
Windows Server 2008	J	J
Windows Server 2008 R2	J	J
Windows Server 2012	J	J
Betriebssystem	***Lastausgleich: Nur Broadcom***	***Lastausgleich: Herstellerunabhängig***
Protokoll	***IP***	***IP***
Windows Server 2008	J	J
Windows Server 2008 R2	J	J
Windows Server 2012	J	J
Windows Server 2012 R2	J	J

Legende: J = ja
N = nein
N. u. = nicht unterstützt

Die Teamart Smart Load Balancing funktioniert mit allen Ethernet-Switches, ohne dass die Switch-Ports für einen bestimmten Trunking-Modus konfiguriert werden müssen. Nur IP-Verkehr wird für sowohl für den ankommenden als auch für den abgehenden Datenverkehr dem Lastausgleich unterzogen. Andere Protokollpakete werden über eine primäre Schnittstelle gesendet und empfangen. Failover für anderen als IP-Verkehr wird nur bei Verwendung von Broadcom-Netzwerkadaptern unterstützt. Die Teamart Allgemeines Trunking erfordert, dass der Ethernet-Switch eine Form des Port-Trunking-Modus unterstützt (z. B. den Modus Gigabit EtherChannel von Cisco oder den Modus Link Aggregation anderer Hersteller von Switches). Diese Teamart ist protokollunabhängig. Sämtlicher Datenverkehr sollte fehlertolerant sein und dem Lastausgleich unterzogen werden.

Hinweis: Wenn Sie LiveLink™ beim Konfigurieren von Teams nicht aktivieren, wird empfohlen, das Spanning Tree Protocol (STP) auf dem Switch zu deaktivieren. Dadurch werden die Ausfallzeiten beim Failover auf Grund der Schleifen-Berechnung nach dem Spanning Tree-Algorithmus reduziert. Probleme dieser Art werden von LiveLink entschärft.

LiveLink™

LiveLink™ ist eine Funktion von BASP, die nur für die Teamart "Smart Load Balancing™" und "Failover" verfügbar ist. LiveLink dient dazu, die Netzwerkanbindung hinter dem Switch zu erkennen und den Datenverkehr nur durch die Teammitglieder zu leiten, die über eine Live-Verbindung verfügen. Diese Funktion steht über die Teaming-Software zur Verfügung (siehe Konfigurieren von LiveLink für ein Team aus Smart Load Balancing and Failover und SLB (Auto-Fallback deaktivieren)). Die Teaming-Software überprüft regelmäßig einen oder mehrere bestimmte Zielnetzwerkadapter (indem von jedem Teammitglied ein Verbindungspaket gesendet wird). Die zu überprüfenden Zielgeräte antworten nach Empfang des Verbindungspakets. Wenn ein Teammitglied innerhalb einer festgelegten Zeitspanne und nach einer festgelegten Anzahl erneuter Versuche keine Antwort erkennt, leitet die Teaming-Software keinen Datenverkehr mehr durch dieses Teammitglied. Wenn ein Teammitglied zu einem späteren Zeitpunkt von einem zu überprüfenden Zielgerät eine Antwort erkennt, ist dies das Anzeichen dafür, dass die Verbindung wiederhergestellt worden ist und dass die Teaming-Software automatisch wieder den Datenverkehr durch dieses Teammitglied leitet. LiveLink funktioniert nur mit TCP/IP.

LiveLink™-Funktion wird von den 32-Bit- und 64-Bit-Windows-Betriebssystemen unterstützt. Informationen zu vergleichbaren Funktionen in Linux-Betriebssystemen finden Sie unter Channel Bonding in der Linux-Dokumentation.

Unterstützung für Teaming und Large Send Offload/ Checksum Offload (Large-Send-Verschiebung/ Prüfsummenverschiebung)

Large Send Offload (LSO) und die Prüfsummenverschiebung (CO) werden nur dann für ein Team aktiviert, wenn alle Mitglieder diese Funktionen unterstützen und dafür konfiguriert wurden.

Abschnitt 3: Broadcom Gigabit Ethernet Teaming-Funktion

Einführung

In diesem Abschnitt finden Sie eine Beschreibung der Technologie und Überlegungen zur Implementierung beim Einsatz der Netzwerk-Teaming-Funktionen, die über die im Lieferumfang des Systems enthaltenen Broadcom-Software bereitgestellt werden. Das Ziel der Broadcom Teaming-Funktion ist es, Fehlertoleranz und Link Aggregation in einem Team aus zwei oder mehr Adaptern zu gewährleisten. Die Informationen in diesem Dokument sollen IT-Experten bei der Bereitstellung von Systemanwendungen unterstützen, die Netzwerkfehlertoleranz und Lastausgleich erfordern, und sie enthalten auch Hinweise für die Problembehebung.

Glossar

Tabelle 4. Glossar

Das Objekt	Definition
ARP	Address Resolution Protocol
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program (Intermediate-Treiber)
DNS	Domain Name Service
G-ARP	Gratuitous Address Resolution Protocol
Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static	Switch-abhängige Teamart für Lastausgleich und Failover, bei der der Intermediate-Treiber ausgehenden Datenverkehr und der Switch eingehenden Datenverkehr verwaltet.
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
Link Aggregation (802.3ad)	Switch-abhängige Teamart mit LACP für Lastausgleich und Failover, bei der der Intermediate-Treiber ausgehenden Datenverkehr und der Switch eingehenden Datenverkehr verwaltet.
LOM	LAN on Motherboard
MAC	Media Access Control
NDIS	Network Driver Interface Specification
NLB	Network Load Balancing (Microsoft)
PXE	Preboot Execution Environment
RAID	Redundant Array of Inexpensive Disks

Tabelle 4. Glossar

Das Objekt	Definition
"Smart Load Balance" und "Failover"	Switch-unabhängige Teamart für Failover, bei der das primäre Teammitglied sämtlichen eingehenden und ausgehenden Datenverkehr bewältigt, während das Standby-Element inaktiv ist, bis ein Failover-Ereignis (z. B. ein Verbindungsverlust) eintritt. Der Intermediate-Treiber (BASP) verwaltet eingehenden/ausgehenden Verkehr.
Smart Load Balancing (SLB)	Switch-unabhängige Teamart für Lastausgleich und Failover, bei der der Intermediate-Treiber ausgehenden/eingehenden Verkehr verwaltet.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WINS	Windows Name Service
WLBS	Windows Load Balancing Service

Teaming-Begriffe

Netzwerkadressierung

Zum besseren Verständnis der Teaming-Funktion ist es wichtig nachzuvollziehen, wie die Kommunikation zwischen Knoten in einem Ethernet-Netzwerk funktioniert. In diesem Dokument wird davon ausgegangen, dass der Leser mit den Grundlagen der Kommunikation in IP- und Ethernet-Netzwerken vertraut ist. Die folgenden Informationen geben einen allgemeinen Überblick über die Grundbegriffe der Netzwerkadressierung in einem Ethernet-Netzwerk.

Jede Ethernet-Netzwerkschnittstelle in einer Host-Plattform wie einem Computersystem benötigt eine global eindeutige Schicht-2-Adresse und mindestens eine global eindeutige Schicht-3-Adresse. Schicht 2 ist die Verbindungsebene, und Schicht 3 ist die Netzwerkebene, wie im OSI-Modell definiert. Die Schicht-2-Adresse wird der Hardware zugewiesen und häufig als MAC-Adresse oder physische Adresse bezeichnet. Diese Adresse wird werkseitig vorprogrammiert und in ein NVRAM (Non-Volatile RAM) auf einer Netzwerkkarte oder dem Mainboard des Systems für eine eingebettete LAN-Schnittstelle gespeichert. Die Schicht-3-Adressen werden als Protokolladressen oder logische Adressen bezeichnet, die dem Software-Stack zugewiesen werden. IP ist ein Beispiel für ein Schicht-3-Protokoll. Außerdem verwendet Schicht 4 (die Transportschicht) Portnummern für jedes höhere Kommunikationsprotokoll wie Telnet oder FTP. Diese Portnummern dienen zur Differenzierung des Verkehrsflusses über mehrere Anwendungen hinweg. Schicht-4-Protokolle wie TCP oder UDP werden in den heutigen Netzwerken am häufigsten verwendet. Die Kombination aus IP-Adresse und TCP-Portnummer wird als Socket bezeichnet.

Ethernet-Geräte kommunizieren mit anderen Ethernet-Geräten nicht über die IP-Adresse, sondern über die MAC-Adresse. Die meisten Anwendungen arbeiten jedoch mit einem Host-Namen, der mittels Namensauflösung, z. B. mit WINS oder DNS, in eine IP-Adresse übersetzt wird. Daher ist ein Verfahren zur Identifizierung der MAC-Adresse, die der IP-Adresse zugewiesen wurde, erforderlich. Das Address Resolution Protocol für ein IP-Netzwerk bietet ein solches Verfahren. Eine Unicast-Adresse entspricht einer einzelnen MAC- oder IP-Adresse. Eine Broadcast-Adresse wird an alle Geräte in einem Netzwerk gesendet.

Teaming und Netzwerkadressen

Ein Team von Adaptern funktioniert wie eine einzelne virtuelle Netzwerkschnittstelle und wird von anderen Netzwerkgeräten genauso betrachtet wie ein Adapter, der nicht Bestandteil eines Teams ist. Ein virtueller Netzwerkadapter kündigt eine einzelne Schicht-2- und eine oder mehrere Schicht-3-Adressen an. Wenn der Teaming-Treiber initialisiert wird, wählt er eine MAC-Adresse von einem der physischen Adapter im Team aus, die als MAC-Adresse des Teams fungieren soll. Diese Adresse stammt normalerweise vom ersten Adapter, der vom Treiber initialisiert wird. Wenn das System, das als Host für das Team fungiert, eine ARP-Anforderung empfängt, wählt es eine MAC-Adresse unter den physischen Adaptern im Team aus, die als die Quell-MAC-Adresse in der ARP-Antwort verwendet werden soll. In Windows-Betriebssystemen zeigt der Befehl **ipconfig /all** die IP- und MAC-Adresse des virtuellen Adapters, nicht die des individuellen physischen Adapters. Die Protokoll-IP-Adresse ist der virtuellen Netzwerkschnittstelle zugewiesen, nicht den individuellen physischen Adaptern.

Bei Switch-unabhängigen Teaming-Modi müssen alle physischen Adapter, die einen virtuellen Adapter bilden, die eindeutige MAC-Adresse verwenden, die ihnen bei der Datenübertragung zugewiesen wird. Das heißt, die Rahmen, die von jedem der physischen Adapter im Team gesendet werden, müssen eine eindeutige MAC-Adresse verwenden, um IEEE-kompatibel zu sein. Beachten Sie, dass ARP-Cache-Einträge nicht aus empfangenen Rahmen entnommen werden, sondern ausschließlich aus ARP-Anforderungen und ARP-Antworten.

Beschreibung der Teaming-Arten

Die unterstützten Teaming-Arten werden nach drei Verfahren klassifiziert:

- Das erste hängt von der Frage ab, ob die Konfiguration des Switch-Ports der Adapter-Teaming-Art entsprechen muss.
- Das zweite hängt von der Funktion des Teams ab, also davon, ob das Team Lastausgleich und Failover oder nur Failover unterstützt.
- Das dritte hängt davon ab, ob das Link Aggregation Control Protocol verwendet oder nicht.

Tabelle 5 zeigt eine Übersicht der Teaming-Arten und ihrer Klassifizierung.

Tabelle 5. Verfügbare Teaming-Arten

Teaming-Art	Switch-abhängig (Switch muss bestimmte Teamart unterstützen)	Unterstützung für Link Aggregation Control Protocol ist auf dem Switch erforderlich	Lastausgleich	Failover
"Smart Load Balance" und "Failover" (mit zwei bis acht Lastausgleich-Teammitgliedern)			•	•
SLB (Auto-Fallback deaktiviert)				•
Link Aggregation (802.3ad)	•	•	•	•
Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static	•		•	•

Smart Load Balancing und Failover

Die Teamart Smart Load Balancing und Failover ermöglicht bei Konfiguration für den Lastausgleich sowohl Lastausgleich als auch Ausfallsicherung, bei Konfiguration für die Fehlertoleranz dagegen nur Ausfallsicherung. Diese Teamart funktioniert mit jedem Ethernet-Switch und erfordert keine Konfiguration für Trunking auf dem Switch. Das Team kündigt mehrere MAC-Adressen und eine oder mehrere IP-Adressen an (bei Verwendung von sekundären IP-Adressen). Die MAC-Adresse des Teams wird aus der Liste der Lastausgleichsmitglieder ausgewählt. Empfängt das System eine ARP-Anforderung, sendet der Software-Netzwerkstapel stets eine ARP-Antwort mit der MAC-Adresse des Teams. Um den Lastausgleich zu starten, modifiziert der Teaming-Treiber diese ARP-Antwort, indem er die Quell-MAC-Adresse so ändert, dass sie einem der physischen Adapter entspricht.

Smart Load Balancing ermöglicht Lastausgleich beim Senden (Transmit Load Balancing, TLB) und Empfangen (Receive Load Balancing, RLB) auf Basis der Schicht-3/Schicht-4-IP-Adressen und der TCP/UDP-Portnummer. Mit anderen Worten: Der Lastausgleich erfolgt nicht auf Byte- oder Rahmenebene, sondern auf Basis der TCP/UDP-Sitzung. Durch dieses Verfahren wird die Übermittlung von Rahmen, die zur selben Socket-Konversation gehören, in der korrekten Reihenfolge

gewährleistet. Lastausgleich wird an 2 bis 8 Ports unterstützt. Dies gilt auch für Ports in einer beliebigen Kombination aus zusätzlichen Adaptern und LOM-Geräten (LAN on Motherboard). TLB wird durch Erstellen einer Hash-Tabelle mit den Quell- und Ziel-IP-Adressen sowie TCP/UDP-Portnummern herbeigeführt. Die gleiche Kombination aus Quell- und Ziel-IP-Adressen sowie TCP/UDP-Portnummern ergibt im Allgemeinen denselben Hash-Index und verweist daher auf denselben Port im Team. Bei Auswahl eines Ports für den Transport aller Rahmen eines bestimmten Sockets wird die eindeutige MAC-Adresse des physischen Adapters in den Rahmen einbezogen, nicht die MAC-Adresse des Teams. Dies ist zur Einhaltung des IEEE-Standards 802.3 erforderlich. Wenn zwei Adapter bei der Übertragung dieselbe MAC-Adresse verwenden, würde dies zu einer doppelten MAC-Adresse führen – eine Situation, die der Switch nicht bewältigen kann.

Der Lastausgleich beim Empfangen (Receive Load Balancing) erfolgt durch einen Intermediate-Treiber, der unangeforderte ARPs (G-ARPs) von Client zu Client sendet und dabei die Unicast-Adresse der einzelnen Clients als Zieladresse der ARP-Anforderung verwendet (auch als gerichtetes ARP bezeichnet). Dieser Vorgang wird nicht als Ausgleich der Datenverkehrslast (Traffic Load Balancing), sondern als Client-Lastausgleich (Client Load Balancing) betrachtet. Wenn der Intermediate-Treiber ein erhebliches Lastungleichgewicht zwischen den physischen Adaptern in einem SLB-Team erkennt, generiert er G-ARPs, um damit eingehende Rahmen umzuverteilen. Der Intermediate-Treiber (BASP) beantwortet keine ARP-Anforderungen; nur der Protokollstapel der Software liefert die erforderliche ARP-Antwort. Der Lastausgleich beim Empfangen ist eine Funktion der Anzahl der Clients, die über die Team-Schnittstelle eine Verbindung zum System herstellen.

Beim Lastausgleich beim Empfangen mit SLB wird versucht, eingehenden Datenverkehr für Client-Geräte über physische Ports im Team auszugleichen. Mit einem veränderten unangeforderten ARP wird eine andere MAC-Adresse für die IP-Adresse des Teams in der physischen und der Protokolladresse des Absenders angekündigt. Dieses G-ARP wird als Unicast mit der MAC- und IP-Adresse eines Client-Geräts in der physischen Zieladresse bzw. der Ziel-Protokolladresse gesendet. Der Ziel-Client aktualisiert daraufhin seinen ARP-Cache mit der neuen MAC-Adresse, die der IP-Adresse des Teams zugeordnet wird. G-ARPs werden nicht als Broadcasts gesendet, da sonst alle Clients ihren Datenverkehr an denselben Port senden würden. Dadurch würden die Vorteile des Client-Lastausgleichs aufgehoben, und es könnte zu einer Rahmenübermittlung in ungeordneter Reihenfolge kommen. Dieses Schema für den Lastausgleich beim Empfangen funktioniert, solange alle Clients und das Team-System sich im selben Subnetz oder derselben Broadcast-Domäne befinden.

Wenn sich die Clients und das System in verschiedenen Subnetzen befinden und eingehender Datenverkehr einen Router durchlaufen muss, wird der empfangene, für das System bestimmte Datenverkehr keinem Lastausgleich unterzogen. Der physische Adapter, der vom Intermediate-Treiber für den Transport des IP-Flusses ausgewählt wurde, befördert den gesamten Datenverkehr. Wenn der Router einen Rahmen an die IP-Adresse des Teams sendet, überträgt er eine ARP-Anforderung (falls nicht im ARP-Cache vorhanden). Der Server-Softwarestapel generiert eine ARP-Antwort mit der MAC-Adresse des Teams, diese wird jedoch vom Intermediate-Treiber modifiziert und über einen bestimmten physischen Adapter gesendet; damit wird der Fluss für diese Sitzung hergestellt.

Dies liegt daran, dass ARP kein routbares Protokoll ist. Es verfügt nicht über eine IP-Kopfzeile, und daher wird es nicht an den Router oder an das Standard-Gateway gesendet. ARP ist lediglich ein lokales Subnetzprotokoll. Da es sich bei G-ARP nicht um ein Broadcast-Paket handelt, wird es vom Router nicht verarbeitet, und der Router aktualisiert sein ARP-Cache nicht.

Der Router würde ein ARP, das für ein anderes Netzwerkgerät bestimmt ist, nur dann verarbeiten, wenn Proxy-ARP aktiviert wäre und der Host keinen Standard-Gateway hätte. Dieser Fall tritt äußerst selten ein und wird für die meisten Anwendungen nicht empfohlen.

Über einen Router gesendeter Verkehr wird ausgeglichen, da der Lastausgleich beim Senden auf der Quell- und Ziel-IP-Adresse sowie der TCP/UDP-Portnummer basiert. Da Router die Quell- und Ziel-IP-Adresse nicht verändern, funktioniert der Lastausgleichsalgorithmus wie vorgesehen.

Durch Konfigurieren von Routern für das Hot Standby Routing Protocol (HSRP) kann im Adapter-Team kein Lastausgleich beim Empfangen ausgeführt werden. Im Allgemeinen ermöglicht es HSRP, dass zwei Router als ein Router fungieren, der eine virtuelle IP- und eine virtuelle MAC-Adresse ankündigt. Ein physischer Router ist die aktive Schnittstelle, während der andere als Standby-Router dient. Obwohl durch HSRP auch die Last von Knoten (über verschiedene Standard-Gateways auf den Host-Knoten) über mehrere Router in HSRP-Gruppen aufgeteilt werden kann, verweist es stets auf die primäre MAC-Adresse des Teams.

Allgemeines Trunking

"Allgemeines Trunking" ist ein Switch-unterstützter Teaming-Modus, bei dem die Ports an beiden Enden einer Verbindung konfiguriert werden müssen: die Serverschnittstellen und die Switch-Ports. Dies wird häufig als Cisco Fast EtherChannel oder Gigabit EtherChannel bezeichnet. Allgemeines Trunking unterstützt darüber hinaus ähnliche Implementierungen durch andere Switch-OEMs wie Extreme Networks Load Sharing und Bay Networks oder IEEE 802.3ad Link Aggregation im statischen Modus. In diesem Modus kündigt das Team eine MAC-Adresse und eine IP-Adresse an, wenn der Protokollstapel auf die ARP-Anforderungen antwortet. Des Weiteren verwendet jeder physische Adapter im Team bei der Übertragung von Rahmen dieselbe Team-MAC-Adresse. Dies ist möglich, da der Switch am anderen Ende der Verbindung den Teaming-Modus kennt und die Verwendung einer einzigen MAC-Adresse durch jeden Port im Team gewährleistet. In der Weiterleitungstabelle im Switch wird der Trunk als ein einziger virtueller Port aufgeführt.

Bei diesem Teaming-Modus steuert der Intermediate-Treiber Lastausgleich und Failover nur für ausgehenden Datenverkehr, während eingehender Verkehr von der Switch-Firmware und -Hardware gesteuert wird. Wie beim Smart Load Balancing verwendet der BASP Intermediate-Treiber die IP/TCP/UDP-Quelladressen und -Zieladressen, um den vom Server gesendeten Datenverkehr auszugleichen. Die meisten Switches implementieren XOR-Hashing der Quell- und Ziel-MAC-Adresse.

Link Aggregation (IEEE 802.3ad LACP)

Link Aggregation funktioniert ähnlich wie Allgemeines Trunking, außer dass das Link Aggregation Control Protocol für das Aushandeln der Ports verwendet wird, aus denen sich das Team zusammensetzt. An beiden Enden der Verbindung muss LACP aktiviert sein, andernfalls ist das Team nicht funktionsfähig. Ist LACP nicht an beiden Enden der Verbindung verfügbar, bietet 802.3ad eine manuelle Bündelung. Hierfür ist es lediglich erforderlich, dass beide Enden verbunden sind. Da bei manueller Bündelung die Aktivierung einer Mitgliedsverbindung ohne den LACP-Austausch vollzogen wird, ist eine solche Verbindung weniger verlässlich und robust als eine durch LACP ausgehandelte Verbindung. LACP bestimmt automatisch, welche Mitgliedsverbindungen gebündelt werden können, und führt die Bündelung dann aus. Es gewährleistet das geregelte Hinzufügen und Entfernen von physischen Verbindungen für die Link Aggregation, so dass keine Rahmen verloren gehen oder dupliziert werden. Gebündelte Verbindungsmitglieder werden durch das Marker-Protokoll entfernt, das wahlweise für Verbindungen mit Aggregation Control Protocol (LACP) aktiviert werden kann.

Die Link Aggregation-Gruppe kündigt eine einzelne MAC-Adresse für alle Ports im Trunk an. Die MAC-Adresse des Aggregators kann die MAC-Adresse eines der MACs sein, aus denen die Gruppe besteht. LACP und Marker-Protokolle verwenden eine Multicast-Zieladresse.

Die Link Aggregation-Steuerungsfunktion bestimmt, welche Verbindungen gebündelt werden können, bindet dann die Ports an eine Bündelungsfunktion im System und überwacht den Zustand, um zu bestimmen, ob eine Änderung in der Aggregation-Gruppe erforderlich ist. Bei der Link Aggregation werden die Leistungen einzelner Verbindungen in einer hochleistungsfähigen virtuellen Verbindung kombiniert. Der Ausfall oder Ersatz einer Verbindung in einem LACP-Trunk hat keinen Verbindungsverlust zur Folge. Der Datenverkehr wird dank Failover einfach von den übrigen Verbindungen im Trunk übernommen.

SLB (Auto-Fallback deaktiviert)

Diese Teamart ist mit der Teamart "Smart Load Balance" und "Failover" bis auf eine Ausnahme identisch: Wenn das Standby-Element aktiv ist und ein primäres Mitglied die Verbindung wiederhergestellt hat, verwendet das Team weiterhin das Standby-Element, anstatt wieder auf das primäre Mitglied umzuschalten. Diese Teamart wird nur verwendet, wenn das Netzwerkkabel getrennt und wieder mit dem Netzwerkadapter verbunden wurde. Sie wird nicht unterstützt, wenn der Adapter mithilfe des Geräte-Managers oder über Hot-Plug PCI entfernt bzw. installiert wird.

Wird ein primärer Adapter, der einem Team zugewiesen ist, deaktiviert, fungiert das Team als ein Team der Art "Smart Load Balancing" und "Failover", in dem Auto-Fallback auftritt.

Softwarekomponenten

Teaming wird im Windows-Betriebssystem über einen NDIS Intermediate-Treiber implementiert. Diese Softwarekomponente wirkt mit dem Miniport-Treiber, der NDIS-Schicht und dem Protokollstapel zusammen und ermöglicht so die Teaming-Architektur (siehe Abbildung 1). Der Miniport-Treiber steuert den Host-LAN-Controller direkt und ermöglicht so Funktionen wie Senden, Empfangen und Unterbrechen der Verarbeitung. Der Intermediate-Treiber befindet sich zwischen Miniport-Treiber und Protokollschicht, ermöglicht das Multiplexing mehrerer Miniport-Treiberinstanzen und erstellt einen virtuellen Adapter, der von der NDIS-Schicht als einzelner Adapter wahrgenommen wird. NDIS bietet eine Reihe von Bibliotheksfunktionen und ermöglicht so die Kommunikation zwischen Miniport-Treibern oder zwischen Intermediate-Treibern und dem Protokollstapel. Jeder Miniport-Geräteinstanz wird eine Protokolladresse (z. B. eine IP-Adresse) zugewiesen. Ist jedoch ein Intermediate-Treiber installiert, wird die Protokolladresse dem virtuellen Team-Adapter zugewiesen, und nicht den individuellen Miniport-Geräten, aus denen das Team besteht.

Der von Broadcom bereitgestellte Teaming-Support wird durch drei individuelle Softwarekomponenten gewährleistet, die gemeinsam arbeiten und als Paket unterstützt werden. Wird eine Komponente aktualisiert, müssen auch alle anderen Komponenten auf die unterstützten Versionen aktualisiert werden. Tabelle 6 beschreibt die drei Softwarekomponenten und die dazugehörigen Dateien für die unterstützten Betriebssysteme.

Tabelle 6. Broadcom Teaming-Softwarekomponente

Softwarekomponente	Broadcom-Name	Windows	Linux
Miniport-Treiber	Broadcom Base Driver	b57nd60X.sys	tg3
Intermediate-Treiber	Broadcom Advanced Server Program (BASP)	Basp.sys	Bonding
Konfigurationsoberfläche	Broadcom Advanced Control Suite (BACS)	BACS	BACS-CLI
NDIS 6-Treiber	Windows Vista und höher mit X86-Treiber Windows Vista und höher mit x64-Treiber	b57nd60x.sys b57nd60a.sys	k.A.

Das BACS-Dienstprogramm (Broadcom Advanced Control Suite) ist für 32-Bit- und 64-Bit-Windows Server-Betriebssysteme ausgelegt. BACS dient zur Konfiguration von Teaming für Lastausgleich und Fehlertoleranz sowie für VLANs. Daneben werden auch die MAC-Adresse, die Treiberversion und Statusinformationen über die einzelnen Netzwerkadapter angezeigt. BACS umfasst außerdem eine Reihe von Diagnose-Tools, z. B. für Hardware-Diagnose, einen Kabeltest und einen Netzwerktopologietest.

Hardwareanforderungen

- Ethernet-Switch
- Router

Durch die verschiedenen in diesem Dokument beschriebenen Teaming-Modi gelten für die Netzwerkgeräte, die zur Verbindung von Clients mit Team-Systemen verwendet werden, gewisse Einschränkungen. Jede Art von Netzwerkverbindungstechnologie hat Auswirkungen auf das Teaming, die in den folgenden Abschnitten beschrieben werden.

Ethernet-Switch

Mit Ethernet-Switches kann ein Ethernet-Netzwerk in mehrere Broadcast-Domänen aufgeteilt werden. Der Switch ist für die Weiterleitung von Ethernet-Paketen zwischen Hosts allein auf der Grundlage von Ethernet MAC-Adressen verantwortlich. Ein physischer Netzwerkadapter, der mit einem Switch verbunden ist, kann im Halbduplex- oder Vollduplex-Modus betrieben werden.

Für die Unterstützung von Allgemeinem Trunking und 802.3ad Link Aggregation muss ein Switch speziell diese Funktion unterstützen. Sollte der Switch diese Protokolle nicht unterstützen, kann er immer noch für Smart Load Balancing verwendet werden.

Router

Ein Router dient zur Weiterleitung von Netzwerkverkehr auf der Basis von Schicht-3-Protokollen (oder höher), arbeitet jedoch häufig auch als Schicht-2-Gerät mit Switching-Funktion. Das Teaming von direkt mit einem Router verbundenen Ports wird nicht unterstützt.

Unterstützte Funktionen nach Teamart

Tabelle 7 bietet einen Vergleich der Funktionen der verschiedenen Teamarten, die von Broadcom Netzwerkkarten unterstützt werden. Anhand dieser Tabelle können Sie bestimmen, welche Teamart am besten für Ihre Anwendung geeignet ist. Die Teaming-Software unterstützt maximal acht Ports in einem Team und bis zu 16 Teams in einem System. In diesen Teams können die unterstützten Teamarten beliebig kombiniert werden, allerdings muss sich jedes Team in einem separaten Netzwerk oder Subnetz befinden.

Tabelle 7. Vergleich der Teamarten

Teamart	Fehlertoleranz	Lastausgleich	Switch-abhängiges Static Trunking	Switch-unabhängig Dynamic Link Aggregation (IEEE 802.3ad)
Funktion	SLB mit Standby[a]	SLB	Allgemeines Trunking	Link Aggregation
Anzahl an Ports pro Team (gleiche Broadcast-Domäne)	2 bis 8	2 bis 8	2 bis 8	2 bis 8
Anzahl an Teams	16	16	16	16
Adapter-Fehlertoleranz	Ja	Ja	Ja	Ja

Tabelle 7. Vergleich der Teamarten (Forts.)

Teamart	Fehlertoleranz	Lastausgleich	Switch-abhängiges Static Trunking	Switch-unabhängig Dynamic Link Aggregation (IEEE 802.3ad)
Fehlertoleranz bei Switch-Verbindung (gleiche Broadcast-Domäne)	Ja	Ja	Switch-abhängig	Switch-abhängig
TX-Lastausgleich	Nein	Ja	Ja	Ja
RX-Lastausgleich	Nein	Ja	Ja (vom Switch ausgeführt)	Ja (vom Switch ausgeführt)
Erfordert kompatiblen Switch	Nein	Nein	Ja	Ja
Heartbeats zum Testen der Konnektivität	Nein	Nein	Nein	Nein
Gemischte Medien (Adapter mit verschiedenen Medien)	Ja	Ja	Ja (Switch-abhängig)	Ja
Verschiedene Raten (Adapter, die keine gemeinsame Übertragungsrate unterstützen, sondern bei verschiedenen Raten betrieben werden können)	Ja	Ja	Nein	Nein
Verschiedene Raten (Adapter, die eine gemeinsame Übertragungsrate unterstützen, jedoch bei verschiedenen Raten betrieben werden können)	Ja	Ja	Nein (Raten müssen identisch sein)	Ja
Lastausgleich TCP/IP	Nein	Ja	Ja	Ja
Teaming mit Geräten verschiedener Hersteller	Ja[b]	Ja[b]	Ja[b]	Ja[b]
Lastausgleich für Nicht-IP-Verkehr	Nein	Ja (nur ausgehender IPX-Verkehr)	Ja	Ja
Gleiche MAC-Adresse für alle Teammitglieder	Nein	Nein	Ja	Ja
Gleiche IP-Adresse für alle Teammitglieder	Ja	Ja	Ja	Ja
Lastausgleich nach IP-Adresse	Nein	Ja	Ja	Ja
Lastausgleich nach MAC-Adresse	Nein	Ja (verwendet für Nicht-IP-/IPX-Verkehr)	Ja	Ja

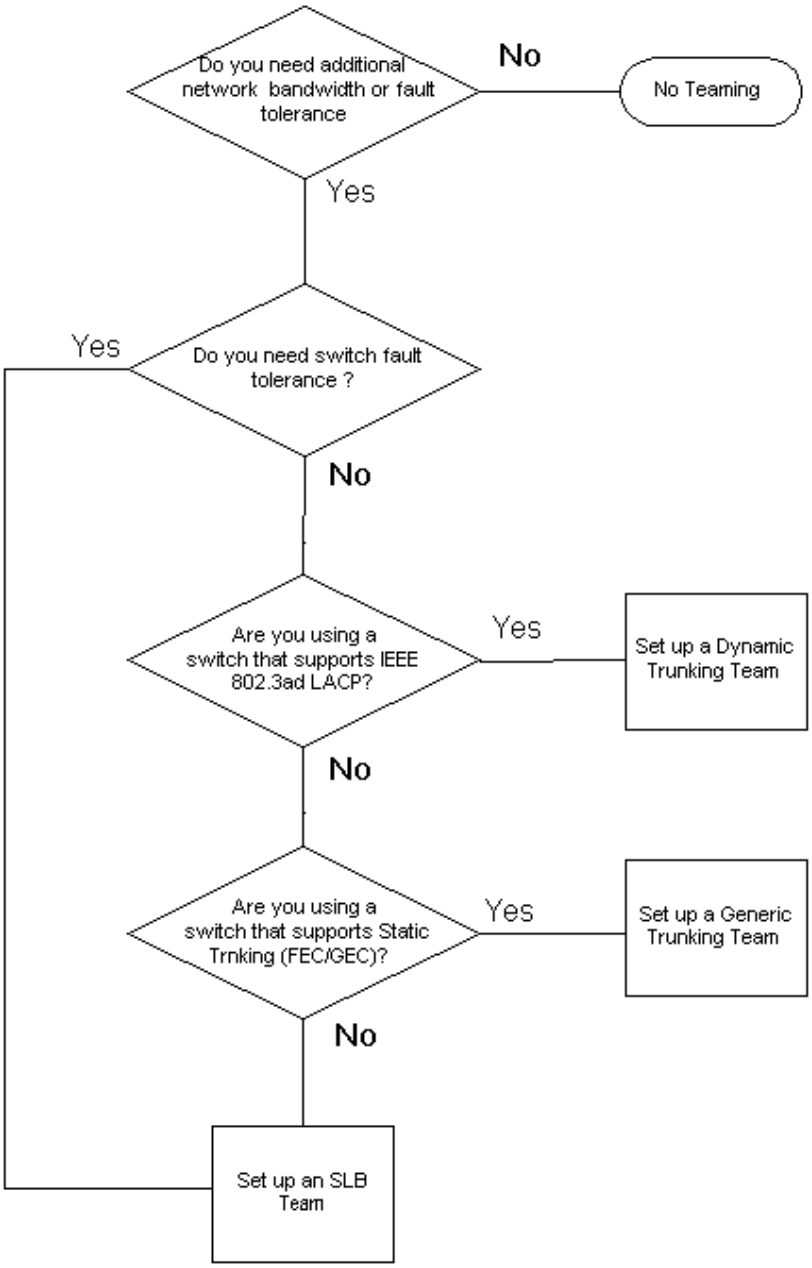
[a] SLB mit einem primären und einem Standby-Element.

[b] Erfordert mindestens einen Broadcom-Adapter im Team.

Auswählen einer Teamart

Das folgende Flussdiagramm zeigt den Entscheidungsprozess bei der Teaming-Planung. Das wichtigste Argument für Teaming ist der Bedarf an zusätzlicher Netzwerkbandbreite und Fehlertoleranz. Teaming bietet Link Aggregation und Fehlertoleranz und erfüllt damit beide Kriterien. Die Teaming-Funktion sollte vorzugsweise in der folgenden Reihenfolge ausgewählt werden: Link Aggregation als erste Wahl, Allgemeines Trunking als zweite Wahl und SLB-Teaming als dritte Wahl, wenn Switches, die die beiden ersten Optionen nicht unterstützen, oder nicht verwaltete Switches verwendet werden. Sollte Switch-Fehlertoleranz erforderlich sein, ist SLB die einzige Möglichkeit (siehe Abbildung 1).

Abbildung 1: Auswahl einer Teamart

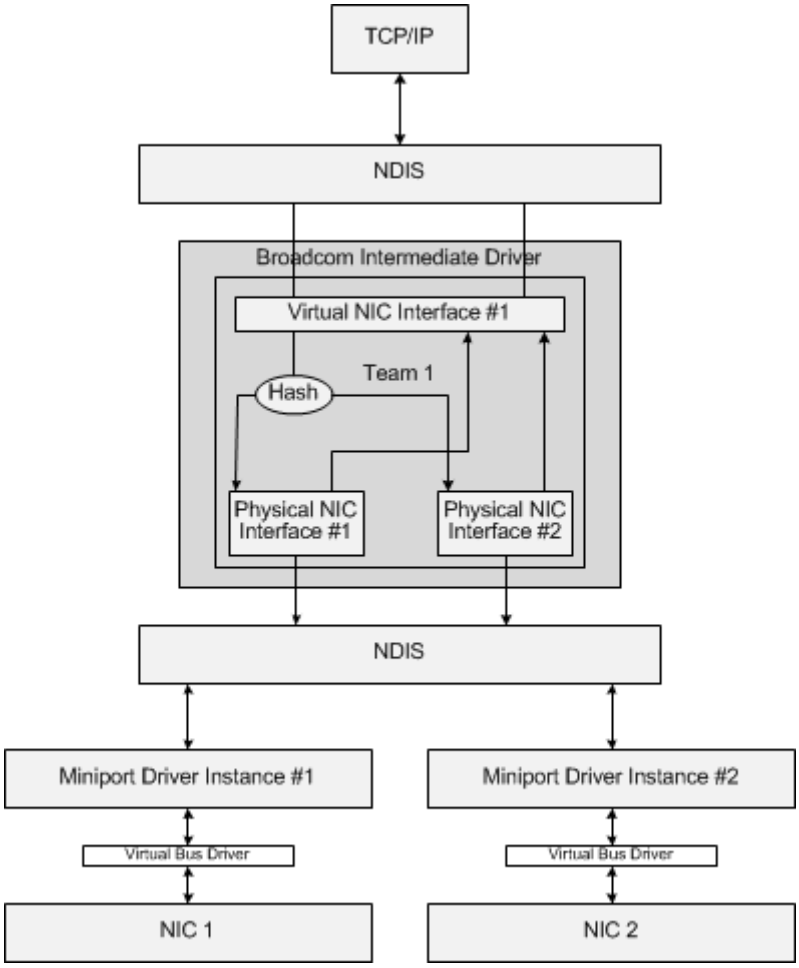


Teaming-Verfahren

Architektur

Broadcom Advanced Server Program ist als NDIS Intermediate-Treiber implementiert (siehe Abbildung 2). Es wird unterhalb von Protokollstapeln wie TCP/IP betrieben und als virtueller Adapter angezeigt. Dieser virtuelle Adapter übernimmt die MAC-Adresse des ersten im Team initialisierten Ports. Für den virtuellen Adapter muss außerdem eine Schicht-3-Adresse konfiguriert werden. Die Hauptfunktion von BASP besteht im Ausgleich des eingehenden (für SLB) und ausgehenden (für alle Teaming-Modi) Verkehrs zwischen den im System installierten physischen Adaptern, die für Teaming ausgewählt wurden. Die Algorithmen für eingehenden und ausgehenden Verkehr sind voneinander unabhängig und operieren orthogonal zueinander. Der ausgehende Verkehr und der entsprechende eingehende Verkehr für eine bestimmte Sitzung können verschiedenen Ports zugewiesen werden.

Abbildung 2: Intermediate-Treiber



Ausgehender Verkehr

Der Broadcom Intermediate-Treiber verwaltet den ausgehenden Verkehrsfluss für alle Teaming-Modi. Für den ausgehenden Verkehr wird jedes Paket zunächst einem Fluss zugeteilt und dann an die ausgewählten physischen Adapter zur Übertragung verteilt. Die Zuteilung zu einem Fluss erfolgt mittels einer effizienten Hash-Berechnung anhand bekannter Protokollfelder. Der errechnete Hash-Wert wird in den Index einer Outbound Flow Hash-Tabelle aufgenommen. Der ausgewählte Outbound Flow Hash-Eintrag enthält den Index des ausgewählten physischen Adapters, der für die Übertragung dieses Flusses verantwortlich ist. Die Quell-MAC-Adresse der Pakete wird dann in die MAC-Adresse des ausgewählten physischen Adapters geändert. Das modifizierte Paket wird anschließend an den ausgewählten physischen Adapter zur Übertragung weitergegeben.

Die ausgehenden TCP- und UDP-Pakete werden mithilfe der Kopfzeileninformationen aus Schicht 3 und Schicht 4 klassifiziert. Dieses Schema verbessert die Lastverteilung für häufig verwendete Internet-Protokoll-Dienste, die mit bekannten Ports wie HTTP und FTP arbeiten. Daher sorgt BASP für Lastausgleich auf Basis einer TCP-Sitzung, nicht auf Paket-Basis.

In den Outbound Flow Hash-Einträgen werden außerdem Statistikzähler nach der Klassifizierung aktualisiert. Das Lastausgleichsmodul verwendet diese Zähler dann, um die Datenflüsse regelmäßig über die Ports im Team zu verteilen.

Der Codepfad für den Ausgangsfluss ist so ausgelegt, dass optimale Zeitgleichheit erreicht wird, wenn gleichzeitig mehrere Zugriffe auf die Outbound Flow Hash-Tabelle zulässig sind.

Bei allen anderen Protokollen außer TCP/IP wird stets der erste physische Adapter für ausgehende Pakete ausgewählt. Eine Ausnahme bildet das Address Resolution Protocol (ARP), das anders gehandhabt wird, um Lastausgleich für eingehenden Verkehr zu erreichen.

Eingehender Verkehr (nur SLB)

Der Broadcom Intermediate-Treiber verwaltet den Fluss des eingehenden Verkehrs für den Teaming-Modus SLB. Im Gegensatz zum Lastausgleich für ausgehenden Verkehr kann Lastausgleich für eingehenden Verkehr nur auf IP-Adressen angewendet werden, die sich im selben Subnetz befinden wie der Lastausgleichsserver. Beim Lastausgleich für eingehenden Verkehr wird eine einmalige Besonderheit des Address Resolution Protocol (RFC0826) genutzt: Jeder IP-Host verwendet seinen eigenen ARP-Cache zur Einkapselung des IP-Datagramms in einen Ethernet-Rahmen. BASP manipuliert die ARP-Antwort sorgfältig, so dass jeder IP-Host angewiesen wird, das eingehende IP-Paket an den gewünschten physischen Adapter zu senden. Daher handelt es sich beim Lastausgleich für eingehenden Verkehr um ein vorausplanendes Schema, das auf dem statistischen Verlauf der eingehenden Datenflüsse basiert. Neue Verbindungen von einem Client zum System werden stets über den primären physischen Adapter hergestellt (da die vom Betriebssystem-Protokollstapel generierte ARP-Antwort die logische IP-Adresse stets der MAC-Adresse des primären physischen Adapters zuordnet).

Wie im Fall des ausgehenden Verkehrs gibt es auch hier eine Hash-Tabelle: die Inbound Flow Head Hash-Tabelle. Für jeden Eintrag in dieser Tabelle gibt es eine einfach verkettete Liste, und jede Verkettung (Inbound Flow-Einträge) stellt einen IP-Host im selben Subnetz dar.

Beim Empfang eines eingehenden IP-Datagramms wird der entsprechende Inbound Flow Head-Eintrag durch Hashing der Quell-IP-Adresse des IP-Datagramms lokalisiert. Außerdem werden zwei im ausgewählten Eintrag gespeicherte Statistikzähler aktualisiert. Diese Zähler werden vom Lastausgleichsmodul auf dieselbe Weise verwendet wie die Ausgangszähler: zur regelmäßigen Neuzuweisung der Datenflüsse an den physischen Adapter.

Die Inbound Flow Head Hash-Tabelle im Codepfad für den Eingangsfluss ist ebenfalls für gleichzeitigen Zugriff ausgelegt. Auf die Verbindungslisten der Inbound Flow-Einträge wird nur im Fall der Verarbeitung von ARP-Paketen und periodischem Lastausgleich Bezug genommen. Es gibt keinen Verweis pro Paket auf die Inbound Flow-Einträge. Obgleich die Verbindungslisten nicht beschränkt sind, ist der Overhead bei der Verarbeitung jedes Nicht-ARP-Pakets stets eine Konstante. Die Verarbeitung der ein- und ausgehenden ARP-Pakete hängt jedoch von der Anzahl der Verbindungen innerhalb der entsprechenden Verbindungsliste ab.

Im Verarbeitungspfad für eingehende Pakete werden auch Filter eingesetzt, um zu verhindern, dass Broadcast-Pakete in einer Schleife von anderen physischen Adapter durch das System zurückgeleitet werden.

Protokoll-Unterstützung

ARP- und IP/TCP/UDP-Datenflüsse werden einem Lastausgleich unterzogen. Handelt es sich bei dem Paket nur um ein IP-Protokoll wie ICMP oder IGMP, werden alle Daten, die an eine bestimmte IP-Adresse fließen, durch denselben physischen Adapter geleitet. Wenn das Paket TCP oder UDP für das Schicht-4-Protokoll verwendet, wird die Portnummer dem Hashing-Algorithmus hinzugefügt, sodass zwei separate Schicht-4-Flüsse durch zwei separate physische Adapter an dieselbe IP-Adresse geleitet werden können.

Beispiel: Der Client hat die IP-Adresse 10.0.0.1. Sämtlicher IGMP- und ICMP-Verkehr wird durch denselben physischen Adapter geleitet, da nur die IP-Adresse für den Hash verwendet wird. Der Fluss würde in etwa so aussehen:

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

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

Wenn der Server also einen TCP- und UDP-Fluss an dieselbe 10.0.0.1-Adresse sendet, kann hierfür derselbe physische Adapter wie bei IGMP und ICMP verwendet werden, oder es können vollkommen verschiedene physische Adapter zum Einsatz kommen. Der Fluss würde in etwa so aussehen:

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

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

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

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

Die Ströme könnten auch so aussehen:

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

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

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

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

Die eigentliche Zuweisung zwischen Adaptern kann sich im Laufe der Zeit ändern; jedes Protokoll, das nicht auf TCP/UDP basiert, wird jedoch über denselben physischen Adapter geleitet, da nur die IP-Adresse im Hash verwendet wird.

Leistung

Moderne Netzwerkkarten bieten zahlreiche Hardwarefunktionen, mit denen die CPU-Nutzung durch Entlastung bestimmter CPU-intensiver Vorgänge reduziert werden kann (siehe Teaming und andere erweiterte Netzwerkeigenschaften). Der BASP Intermediate-Treiber ist dagegen eine reine Softwarefunktion, die jedes von den Protokollstapeln empfangene Paket untersuchen und auf dessen Inhalt reagieren muss, bevor das Paket über eine bestimmte physische Schnittstelle gesendet wird. Obgleich der BASP-Treiber jedes ausgehende Paket nahezu gleich schnell verarbeiten kann, können einige Anwendungen, die bereits an die CPU gebunden sind, beeinträchtigt werden, wenn sie über eine Schnittstelle in einem Team betrieben werden. Für eine solche Anwendung ist es unter Umständen günstiger, die Failover-Funktionen des Intermediate-Treibers statt der Lastausgleichsfunktionen zu nutzen. Ebenfalls wäre es möglich, dass sie über einen einzelnen physischen Adapter mit einer bestimmten Hardwarefunktion, wie Large Send Offload (Large Send-Verschiebung), effizienter arbeitet.

Vom Betriebssystem unterstützte Treiber

Wie bereits erwähnt, wird BASP in Betriebssystemumgebungen mit Windows Server 2008 und 2012 unterstützt.

In der folgenden Tabelle werden die verschiedenen Funktionen der Teaming-Modi zusammengefasst.

Tabelle 8. Teaming-Modus-Funktionen

Leistungsmerkmale	Windows-Support
Smart Load Balancing™	
Benutzeroberfläche	BACS[a]
Anzahl an Teams	16
Anzahl an Adaptern pro Team	8
Hot-Replace	Ja
Hot-Add	Ja
Hot-Remove	Ja
Unterstützte Übertragungsrate	Verschiedene Raten
Rahmen-Protokoll	IP
Verwaltung eingehender Pakete	BASP
Verwaltung ausgehender Pakete	BASP
Failover-Ereignis	Verbindungsverlust oder LiveLink-Ereignis
Failover-Zeit	< 500 ms
Fallback-Zeit	1,5 s[b] (ca.)
LiveLink-Unterstützung	Ja
MAC-Adresse	Verschieden
Herstellerunabhängiges Teaming	Ja
Allgemeines Trunking	
Benutzeroberfläche	BACS
Anzahl an Teams	16
Anzahl an Adaptern pro Team	8
Hot-Replace	Ja
Hot-Add	Ja
Hot-Remove	Ja
Unterstützte Übertragungsrate	Verschiedene Raten
Rahmen-Protokoll	Alle
Verwaltung eingehender Pakete	Switch
Verwaltung ausgehender Pakete	BASP
Failover-Ereignis	Nur Verbindungsverlust
Failover-Zeit	500 ms
Fallback-Zeit	1,5 s[b] (ca.)
MAC-Adresse	Identisch für alle Adapter
Herstellerunabhängiges Teaming	Ja
Dynamisches Trunking	
Benutzeroberfläche	BACS

Tabelle 8. Teaming-Modus-Funktionen (Forts.)

Leistungsmerkmale	Windows-Support
Anzahl an Teams	16
Anzahl an Adaptern pro Team	8
Hot-Replace	Ja
Hot-Add	Ja
Hot-Remove	Ja
Unterstützte Übertragungsrate	Verschiedene Raten
Rahmen-Protokoll	Alle
Verwaltung eingehender Pakete	Switch
Verwaltung ausgehender Pakete	BASP
Failover-Ereignis	Nur Verbindungsverlust
Failover-Zeit	< 500 ms
Fallback-Zeit	1,5 s[b] (ca.)
MAC-Adresse	Identisch für alle Adapter
Herstellerunabhängiges Teaming	Ja

a Broadcom Advanced Control Suite
b Stellen Sie sicher, dass Port Fast oder Edge Port aktiviert ist.

Unterstützte Teaming-Raten

In Tabelle 9 werden die verschiedenen Übertragungsraten zusammengefasst, die für jede Teamart unterstützt werden. Wenn verschiedene Raten angegeben sind, können die Teaming-Adapter mit unterschiedlichen Übertragungsraten arbeiten.

Tabelle 9. Übertragungsraten beim Teaming

Teamart	*Übertragungsrate*	*Richtung des Datenverkehrs*	*Ratenunterstützung*
SLB	10/100/1000	Eingehend/ausgehend	Verschiedene Raten
FEC	100	Eingehend/ausgehend	Identische Raten
GEC	1000	Eingehend/ausgehend	Identische Raten
IEEE 802.3ad	10/100/1000	Eingehend/ausgehend	Verschiedene Raten

Teaming und andere erweiterte Netzwerkeigenschaften

Bevor Sie ein Team erstellen, Teammitglieder hinzufügen oder entfernen oder die erweiterten Einstellungen eines Teammitglieds ändern, sollten Sie sicherstellen, dass alle Teammitglieder in ähnlicher Weise konfiguriert wurden. Die Einstellungen für VLANs, QoS-Paketmarkierung, Jumbo-Rahmen und die verschiedenen Entlastungen müssen überprüft werden. Angaben zu den erweiterten Adaptereigenschaften und zur Teaming-Unterstützung finden Sie in Tabelle 10.

Tabelle 10. Erweiterte Adaptereigenschaften und Teaming-Unterstützung

Adaptereigenschaft	Unterstützung durch virtuellen Teaming-Adapter
Checksum Offload (Prüfsummenverschiebung)	Ja
IEEE 802.1p QoS-Markierung	Nein
Large Send Offload (Large Send-Verschiebung)	Ja[a]
Jumbo-Rahmen	Ja[b]
IEEE 802.1Q VLANs	Ja
Wake on LAN	Nein
Preboot Execution Environment (PXE)	Ja[c]

[a] Diese Funktion muss von allen Adaptern im Team unterstützt werden. Einige Adapter unterstützen diese Funktion u. U. nicht, wenn außerdem ASF/IPMI aktiviert ist.
[b] Muss muss von allen Adaptern im Team unterstützt werden.
[c] Nur als PXE-Server, nicht als Client.

Checksum Offload (Prüfsummenverschiebung)

Checksum Offload (Prüfsummenverschiebung) ist eine Eigenschaft der Broadcom-Netzwerkadapter, die es ermöglicht, dass die TCP/IP/UDP-Prüfsummen zum Senden und Empfangen von Datenverkehr statt von der Host-CPU von der Adapterhardware berechnet werden. Bei hohem Verkehrsaufkommen kann ein System dadurch mehr Verbindungen effizienter handhaben, als dies bei einer Prüfsummen-Berechnung durch die Host-CPU möglich wäre. Dabei handelt es sich naturgemäß um eine Hardwareeigenschaft. Bei einer reinen Softwareimplementierung ließe sich daraus kein Nutzen ziehen. Ein Adapter, der Checksum Offload unterstützt, kündigt dem Betriebssystem diese Fähigkeit an, so dass die Prüfsumme nicht im Protokollstapel berechnet werden muss. Da sich der Intermediate-Treiber direkt zwischen der Protokollschicht und dem Miniport-Treiber befindet, kann die Protokollschicht keine Prüfsummen zu verschieben.

IEEE 802.1p QoS-Markierung

Der Standard IEEE 802.1p umfasst ein 3-Bit-Feld (mit Unterstützung für maximal 8 Prioritätsebenen), das eine Priorisierung des Verkehrs ermöglicht. Der BASP Intermediate-Treiber bietet keine Unterstützung für IEEE 802.1p QoS-Markierung.

Large Send Offload (Large Send-Verschiebung)

Large Send Offload (Large Send-Verschiebung) ist eine von Broadcom-Netzwerkadaptern bereitgestellte Funktion, die verhindert, dass ein höheres Kommunikationsprotokoll wie TCP ein großes Datenpaket in eine Reihe kleinerer Pakete mit angehängten Kopfzeilen unterteilt. Der Protokollstapel muss nur eine einzige Kopfzeile für ein Datenpaket mit einer Größe von 64 KB generieren, und die Adapterhardware unterteilt den Datenpuffer in Ethernet-Rahmen von angemessener Größe mit den Kopfzeilen in korrekter Folge (basierend auf der einzelnen, ursprünglich angegebenen Kopfzeile).

Jumbo-Rahmen

Der BASP Intermediate-Treiber unterstützt Jumbo-Rahmen, vorausgesetzt, dass alle physischen Adapter im Team ebenfalls Jumbo-Rahmen unterstützen und für alle Adapter im Team dieselbe Größe eingerichtet ist.

IEEE 802.1Q VLANs

Der IEEE Standard definiert Rahmenformaterweiterungen zur Unterstützung von Virtual Bridged Local Area Network-Markierung in Ethernet-Netzwerken, wie in der IEEE 802.1Q-Spezifikation angegeben. Das VLAN-Protokoll erlaubt das Einfügen eines Tags in einen Ethernet-Rahmen zur Identifizierung des VLANs, zu dem ein Rahmen gehört. Wenn vorhanden, wird der 4 Byte lange VLAN-Tag in den Ethernet-Rahmen zwischen der Quell-MAC-Adresse und dem Feld für Länge/Typ eingefügt. Die ersten 2 Byte des VLAN-Tags bestehen aus dem IEEE 802.1Q-Tagtyp, während die letzten 2 Byte ein Feld für die Benutzerpriorität und die VLAN-ID (VID) enthalten. Virtuelle LANs (VLANs) ermöglichen es dem Benutzer, das physische LAN in logische Unterteile aufzugliedern. Jedes definierte VLAN verhält sich wie ein separates Netzwerk, dessen Datenverkehr und Broadcasts von den anderen Netzwerken getrennt sind, sodass die Bandbreiteneffizienz innerhalb der einzelnen logischen Gruppen erhöht wird. VLANs ermöglichen es dem Administrator außerdem, entsprechende Richtlinien für Sicherheit und Servicequalität (Quality of Service, QoS) festzulegen. Mit BASP können pro Team oder Adapter bis zu 64 VLANs erstellt werden: 63 markierte und 1 unmarkiertes. Die tatsächliche Anzahl möglicher VLANs wird jedoch durch das Betriebssystem und die Systemressourcen eingeschränkt. Der Standard IEEE 802.1q bietet VLAN-Unterstützung. VLANs werden sowohl in einer Teaming-Umgebung als auch an einem einzelnen Adapter unterstützt.

Beachten Sie, dass VLANs nur bei homogenem Teaming unterstützt werden, nicht aber bei herstellerunabhängigem Teaming. Der BASP Intermediate-Treiber unterstützt VLAN-Markierung. Ein oder mehrere VLANs können an eine einzelne Instanz des Intermediate-Treibers gebunden sein.

Wake on LAN

Mit Wake on LAN (WOL) kann der Ruhemodus eines Systems beendet werden, wenn ein bestimmtes Paket über die Ethernet-Schnittstelle eingeht. Da ein virtueller Adapter als reines Softwaregerät implementiert ist, fehlen ihm die Hardwarefunktionen zur Implementierung von Wake on LAN. Über einen virtuellen Adapter kann der Ruhemodus eines Systems deshalb nicht beendet werden. Die physischen Adapter hingegen unterstützen diese Eigenschaft auch dann, wenn sie Teil eines Teams sind.

Preboot Execution Environment (PXE)

Preboot Execution Environment (PXE) ermöglicht einem System das Booten mithilfe eines Betriebssystems-Image über das Netzwerk. Definitionsgemäß wird PXE aufgerufen, bevor ein Betriebssystem geladen ist, so dass der BASP Intermediate-Treiber keine Gelegenheit hat, ein Team zu laden und zu aktivieren. Infolge dessen wird Teaming als PXE-Client nicht unterstützt, obwohl ein physischer Adapter in einem Team beim Laden des Betriebssystems als PXE-Client verwendet werden kann. Ein Team-Adapter kann zwar nicht als PXE-Client verwendet werden, er kann jedoch als PXE-Server fungieren, der PXE-Clients Betriebssystem-Images bereitstellt, wobei er eine Kombination aus Dynamic Host Control Protocol (DHCP) und Trivial File Transfer Protocol (TFTP) verwendet. Beide Protokolle können über IP betrieben werden und unterstützen alle Teaming-Modi.

Allgemeine Netzwerkaspekte

Switch-übergreifendes Teaming

SLB-Teaming kann über mehrere Switches konfiguriert werden. Die Switches müssen jedoch verbunden sein. Allgemeines Trunking und Link Aggregation funktionieren nicht Switch-übergreifend, da jede dieser Implementierungen erfordert, dass alle physischen Adapter in einem Team dieselbe Ethernet MAC-Adresse haben. Beachten Sie, dass SLB nur den Verbindungsverlust zwischen den Ports im Team und ihrem unmittelbaren Verbindungspartner erkennen kann. SLB ist nicht in der Lage, auf andere Hardwarestörungen in den Switches zu reagieren oder Verbindungsverluste an anderen Ports zu erkennen.

Fehlertoleranz bei Switch-Verbindung

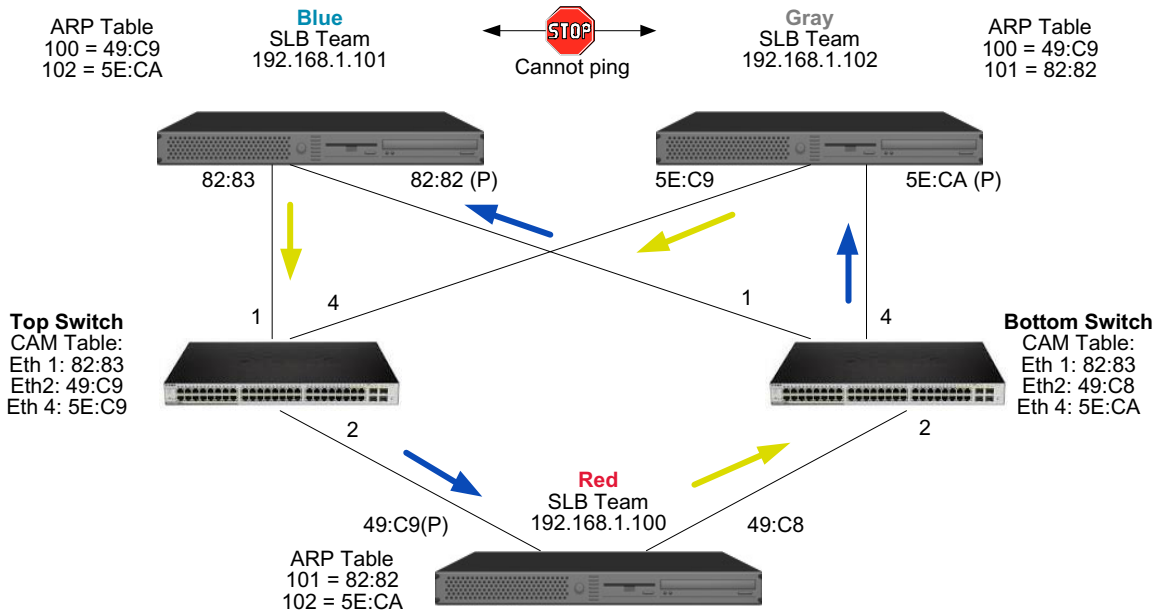
Die unten stehenden Diagramme demonstrieren den Betrieb eines SLB-Teams in einer Konfiguration mit Switch-Fehlertoleranz. Gezeigt wird die Zuordnung der Ping-Anforderung und der Ping-Antwort in einem SLB-Team mit zwei aktiven Mitgliedern. Alle Server (Blue, Gray und Red) senden sich gegenseitig einen Dauerping. Abbildung 3 zeigt eine Konfiguration ohne Verbindungskabel zwischen den beiden Switches. In Abbildung 4 ist das Verbindungskabel vorhanden, und Abbildung 5 zeigt ein Beispiel für ein Failover-Ereignis, ebenfalls mit Verbindungskabel. Diese Beispiele veranschaulichen das Prinzip des Switch-übergreifenden Teamings und die Bedeutung des Verbindungskabels.

Die Diagramme zeigen, wie das sekundäre Teammitglied die ICMP-Echoanfrage sendet (gelbe Pfeile), während das primäre Teammitglied die entsprechende ICMP-Echoantwort empfängt (blaue Pfeile). Hierdurch wird eine Haupteigenschaft der Teaming-Software veranschaulicht. Durch die Lastausgleichsalgorithmen wird die Art des Lastausgleichs von Rahmen beim Senden oder Empfangen nicht synchronisiert. Mit anderen Worten: Rahmen für eine bestimmte Konversation können an verschiedene Schnittstellen im Team gesendet und dort empfangen werden. Dies gilt für alle von Broadcom unterstützten Teaming-Arten. Daher muss eine Verbindung zwischen den Switches bestehen, die mit Ports im selben Team verbunden sind.

In der Konfiguration ohne das Verbindungskabel wird eine ICMP-Anforderung von Blue an Gray von Port 82:83 abgeschickt, die für den Gray-Port 5E:CA bestimmt ist. Der Top Switch hat jedoch keine Möglichkeit zum Senden, da er den Gray-Port 5E:C9 nicht benutzen kann. Eine ähnliche Situation tritt ein, wenn Gray versucht, einen Ping an Blue zu senden. Eine ICMP-Anforderung, bestimmt für Blue 82:82, wird von 5E:C9 gesendet, erreicht ihr Ziel jedoch nicht. Dem Top Switch fehlt der Eintrag für 82:82 in der CAM-Tabelle, da es keine Verbindung zwischen den beiden Switches gibt. Zwischen Red und Blue und zwischen Red und Gray können die Pings jedoch fließen.

Ein Failover-Ereignis würde außerdem zu weiterem Konnektivitätsverlust führen. Angenommen, an Port 4 am Top Switch würde das Kabel entfernt. In diesem Fall würde Gray die ICMP-Anforderung an Red 49:C9 senden. Da allerdings der Bottom Switch keinen Eintrag für 49:C9 in seiner CAM-Tabelle vorfindet, wird der Frame an alle Ports gesendet, dieser kann 49:C9 jedoch nicht erreichen.

Abbildung 3: Switch-übergreifendes Teaming ohne Verbindung zwischen den Switches



Werden die Switches miteinander gekoppelt, kann der Verkehr von Blue nach Gray und umgekehrt problemlos fließen. Beachten Sie die zusätzlichen Einträge in der CAM-Tabelle für beide Switches. Die Verbindung ist entscheidend für den korrekten Betrieb des Teams. Daher wird die Einrichtung eines Link Aggregation-Trunks zur Koppelung der beiden Switches dringend empfohlen, damit eine hohe Verfügbarkeit der Verbindung gewährleistet werden kann.

Abbildung 4: Switch-übergreifendes Teaming mit Schnittstelle

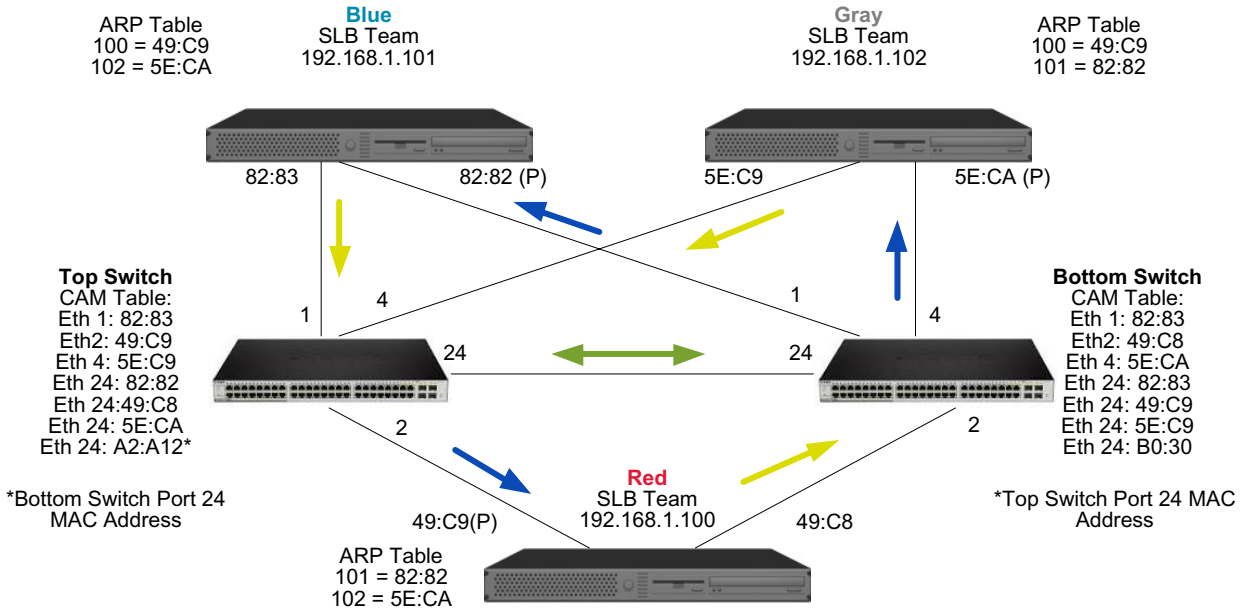
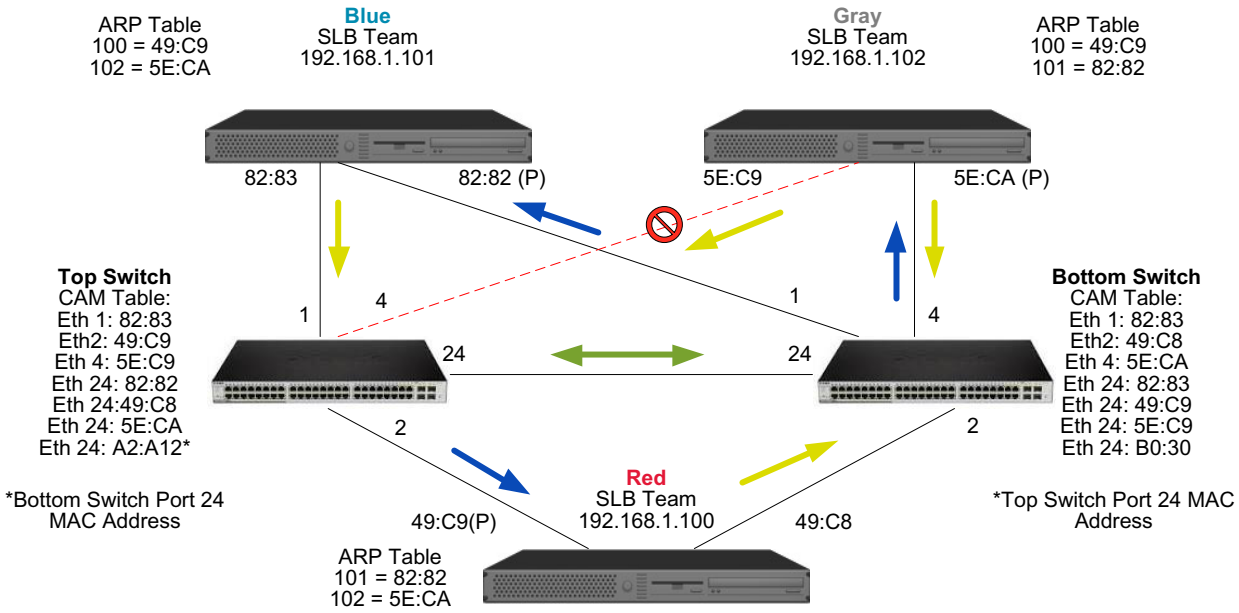


Abbildung 5 zeigt ein Failover-Ereignis, bei dem das Kabel an Port 4 des Top Switches herausgezogen wurde. Die Failover-Funktion wird erfolgreich ausgeführt, und alle Stationen senden sich gegenseitig Pings, ohne dass es zu Verbindungsverlusten kommt.

Abbildung 5: Failover-Ereignis



Spanning Tree-Algorithmus

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

In Ethernet-Netzwerken existiert u. U. nur ein aktiver Pfad zwischen zwei Bridges oder Switches. Bei mehreren aktiven Pfaden zwischen Switches kann es zu Schleifen im Netzwerk kommen. Wenn Schleifen auftreten, erkennen einige Switches Stationen auf beiden Seiten des Switches. Dies führt zu einer Störung im Forwarding-Algorithmus, so dass doppelte Rahmen weitergeleitet werden. Spanning Tree-Algorithmen ermöglichen Pfadredundanz, indem sie einen Tree definieren, der alle Switches in einem erweiterten Netzwerk umfasst, und dann bestimmte redundante Datenpfade in einen Standby-Status (blockiert) zwingen. In regelmäßigen Abständen senden und empfangen die Switches im Netzwerk Spanning Tree-Pakete, die sie zur Identifizierung des Pfades verwenden. Falls ein Netzwerksegment nicht mehr erreicht werden kann oder wenn sich der Spanning Tree-Zeitaufwand ändert, konfiguriert der Spanning Tree-Algorithmus die Spanning Tree-Topologie neu und stellt die Verbindung wieder her, indem er den Standby-Pfad aktiviert. Der Spanning Tree-Betrieb ist für Endstationen transparent, die nicht erkennen, ob sie mit einem einzelnen LAN-Segment oder einem Switched-LAN aus mehreren Segmenten verbunden sind.

Spanning Tree Protocol (STP) ist ein Schicht-2-Protokoll, das für Bridges und Switches ausgelegt ist. Die Spezifikation für STP ist im Standard IEEE 802.1d definiert. Die Hauptaufgabe von STP besteht darin, sicherzustellen, dass es nicht zu einer Schleifensituation kommt, wenn redundante Pfade im Netzwerk vorhanden sind. STP erkennt/deaktiviert Netzwerkschleifen und bietet Backup-Verbindungen zwischen Switches oder Bridges. Es ermöglicht dem Gerät, mit anderen STP-kompatiblen Geräten im Netzwerk zu interagieren, und stellt damit sicher, dass nur ein Pfad zwischen jeweils zwei Stationen im Netzwerk existiert.

Nachdem eine stabile Netzwerktopologie eingerichtet wurde, empfangen alle Bridges BPDU-Nachrichten (Bridge Protocol Data Units), die von der Root-Bridge übertragen werden. Empfängt eine Bridge nach einem vordefinierten Intervall (Max Age) keine BPDU-Nachricht, nimmt die Bridge an, dass die Verbindung zur Root-Bridge unterbrochen wurde. Diese Bridge beginnt dann Verhandlungen mit anderen Bridges zur Neukonfiguration des Netzwerks, um wieder eine gültige Netzwerktopologie herzustellen. Der Vorgang zum Erstellen einer neuen Topologie kann bis zu 50 Sekunden in Anspruch nehmen. In dieser Zeit ist die End-to-End-Kommunikation unterbrochen.

Für Ports, die mit Endstationen verbunden sind, wird die Verwendung von Spanning Tree nicht empfohlen, da eine Endstation definitionsgemäß keine Schleife in einem Ethernet-Segment erstellt. Wenn ein Team-Adapter mit einem Port verbunden und der Spanning Tree aktiviert ist, kann es außerdem zu unerwarteten Konnektivitätsproblemen kommen. Angenommen, bei einem Adapter im Team ist ein Verbindungsverlust an einem der physischen Adapter aufgetreten. Würde die Verbindung des physischen Adapters wiederhergestellt (auch als Fallback bezeichnet), würde der Intermediate-Treiber erkennen, dass die Verbindung wieder aufgebaut wurde und beginnen, Datenverkehr durch den Port zu leiten. Der Datenverkehr würde verloren gehen, wenn der Port vorübergehend durch das Spanning Tree Protocol blockiert würde.

Topology Change Notice (TCN)

Eine Bridge/ein Switch erstellt eine Forwarding-Tabelle mit MAC-Adressen und Portnummern, indem er/sie die Quell-MAC-Adresse lernt, die an einem bestimmten Port empfangen wurde. Die Tabelle wird verwendet, um Rahmen an einen bestimmten Port weiterzuleiten, anstatt den Rahmen an alle Ports zu senden. Die maximale Verfallszeit der Einträge beträgt normalerweise 5 Minuten. Erst wenn ein Host 5 Minuten lang nicht gesendet hat, wird der Eintrag aus der Tabelle entfernt. In manchen Situationen ist es von Vorteil, die Verfallszeit zu reduzieren. Ein Beispiel: Eine Verbindung wechselt aus dem Weiterleitungszustand in den blockierten Zustand, und eine andere Verbindung wechselt aus dem blockierten Zustand in den Weiterleitungszustand. Dieser Wechsel könnte bis zu 50 Sekunden dauern. Am Ende der STP-Neuberechnung stünde ein neuer Pfad für die Kommunikation zwischen Endstationen zur Verfügung. Da jedoch die Forwarding-Tabelle noch immer Einträge auf Basis der alten Topologie enthalten würde, könnte die Kommunikation möglicherweise erst nach 5 Minuten wiederhergestellt werden, wenn die betroffenen Port-Einträge aus der Tabelle entfernt sind. Der Datenverkehr würde dann an alle Ports gesendet und neu gelernt werden. In diesem Fall wäre eine Reduzierung der Verfallszeit von Vorteil. Dies ist der Zweck einer speziellen BPDU namens TCN (Topology Change Notice). Eine TCN wird von der betroffenen Bridge/vom Switch an die Root-Bridge/den Root-Switch gesendet. Sobald eine Bridge/ein Switch eine Änderung der Topologie erkennt (wenn eine Verbindung verloren geht oder ein Port in den weiterleitenden Zustand wechselt), wird über den Root-Port eine TCN an die Root-Bridge gesendet. Die Root-Bridge kündigt dann dem gesamten Netzwerk eine BPDU mit einer TCN an. Dadurch reduziert jede Bridge die Verfallszeit der MAC-Tabelle für einen bestimmten Zeitraum auf 15 Sekunden reduziert. Dadurch kann der Switch die MAC-Adressen neu lernen, sobald STP erneut konvergiert.

TCN BPDUs werden gesendet, wenn ein Port aus dem weiterleitenden Zustand in den blockierten Zustand wechselt oder umgekehrt. Eine TCN BPDU initiiert keine STP-Neuberechnung. Sie beeinflusst lediglich die Verfallszeit der Einträge der Forwarding-Tabelle im Switch. Sie führt keine Änderung der Topologie herbei und erstellt keine Schleifen. Endknoten wie Server oder Clients lösen eine Topologieänderung aus, wenn sie aus- und wieder eingeschaltet werden.

Port Fast/Edge Port

Um die Auswirkungen von TCNs auf das Netzwerk (z. B. eine verstärkte Überflutung der Switch-Ports) zu reduzieren, sollten Endknoten, die häufig ein- bzw. ausgeschaltet werden, auf dem Switch-Port, an den sie angeschlossen sind, die Port Fast- oder Edge Port-Einstellung verwenden. Port Fast oder Edge Port ist ein Befehl, der auf bestimmte Ports angewendet wird und die folgenden Auswirkungen hat:

- Ports, deren Verbindung aus dem inaktiven in den aktiven Zustand wechselt, werden in den weiterleitenden STP-Modus versetzt, anstatt aus dem wartenden Zustand in den lernenden und dann in den weiterleitenden Zustand überzugehen. STP wird auf diesen Ports weiterhin ausgeführt.
- Der Switch generiert keine Benachrichtigung über eine Topologieänderung, wenn der Port aktiv oder wieder inaktiv wird.

Teaming mit Microsoft NLB/WLBS

Der Teaming-Modus SLB funktioniert nicht im Microsoft NLB-Unicast-Modus, sondern nur im Multicast-Modus. Aufgrund des vom NLB-Dienst verwendeten Verfahrens sollte in dieser Umgebung die Teaming-Konfiguration Failover eingesetzt werden (SLB mit einer Standby-Netzwerkkarte), da der Lastausgleich von NLB verwaltet wird.

Anwendungsaspekte

Teaming- und Clustering–Microsoft Cluster-Software

Es wird dringend empfohlen, in jedem Clusterknoten mindestens zwei Netzwerkadapter zu installieren (die Verwendung von On-Board-Adaptern ist möglich). Diese Schnittstellen dienen einem doppelten Zweck. Ein Adapter wird ausschließlich für die Intracluster-*Heartbeat*-Kommunikation verwendet. Dieser wird als *privater Adapter* bezeichnet und befindet sich normalerweise in einem separaten privaten Subnetzwerk. Der andere Adapter wird zur Client-Kommunikation verwendet und als *öffentlicher Adapter* bezeichnet.

Es können mehrere Adapter für jeden dieser Zwecke eingesetzt werden: private Intracluster-Kommunikation und öffentliche Kommunikation mit externen Clients. Microsoft Cluster-Software unterstützt alle Broadcom-Teaming-Modi ausschließlich für den öffentlichen Adapter. Teaming für private Netzwerkadapter wird nicht unterstützt. Nach Angaben von Microsoft wird Teaming an der privaten Schnittstelle eines Serverclusters deshalb nicht unterstützt, weil es beim Senden und Empfangen von Heartbeat-Paketen zwischen den Knoten zu Verzögerungen kommen könnte. Wenn Redundanz für die private Verbindung gewünscht wird, sollten Sie Teaming deaktivieren und mit den verfügbaren Ports eine zweite private Verbindung bilden. Damit erzielen Sie dasselbe Ergebnis und erhalten zwei robuste Kommunikationspfade, über die die Knoten kommunizieren können.

Beim Teaming in einer Clusterumgebung wird empfohlen, Adapter derselben Marke zu verwenden.

Hinweis: Microsoft Cluster-Software bietet keine Unterstützung für Microsoft Network Load Balancing.

Teaming und Netzwerkbackup

Bei der Ausführung von Netzwerkbackups in einer Umgebung ohne Teams kann der Gesamtdurchsatz an einem Adapter auf einem Backupserver aufgrund des übermäßigen Datenverkehrs und der Adapterüberlastung leicht beeinträchtigt werden. Je nach Anzahl der Backupserver und Datenströme und in Abhängigkeit von der Bandlaufwerksgeschwindigkeit kann der Backupverkehr unter Umständen einen hohen Prozentsatz der Bandbreite der Netzverbindung beanspruchen und so die Produktionsdaten und die Backupleistung des Bands beeinflussen. Netzwerkbackups umfassen in der Regel einen speziellen Backupserver, der mit Bandbackup-Software wie NetBackup, Galaxy oder Backup Exec arbeitet. Der Backupserver ist entweder direkt mit einer SCSI-Bandeinheit verbunden, oder es ist eine Bandbibliothek über ein Fibre-Channel-SAN (Storage Area Network) angeschlossen. Über das Netzwerk gesicherte Systeme werden in der Regel als Client- oder Remote-Server bezeichnet. Normalerweise ist für solche Systeme ein Bandbackup-Softwareagent installiert.

Da es vier Client-Server gibt, kann der Backupserver simultan vier Backupjobs (einen pro Client) an einen Autoloader mit mehreren Laufwerken streamen. Da jedoch nur eine Verbindung zwischen dem Switch und dem Backupserver besteht, können Adapter und Verbindung bei einem Backup mit vier Datenströmen schnell ausgelastet werden. Wenn der Adapter auf dem Backupserver mit 1 GBit/s (125 MB/s) betrieben wird und jeder Client während des Bandbackups Daten mit 20 MB/s streamen kann, beträgt der Durchsatz zwischen Backupserver und Switch 80 MB/s (20 MB/s x 4), was 64 % der Netzbandbreite entspricht. Dieser Wert liegt zwar innerhalb des Bandbreitenbereichs des Netzwerks; 64 % stellen jedoch einen hohen Prozentsatz dar, wenn dieselbe Verbindung auch von anderen Anwendungen genutzt wird.

Lastausgleich und Failover

Mit zunehmender Zahl der Backup-Streams erhöht sich der Durchsatz insgesamt. Es ist jedoch möglich, dass nicht jeder Datenstrom in der Lage ist, dieselbe Leistung wie ein einzelner Backup-Stream mit 25 MB/s aufrecht zu erhalten. Mit anderen Worten: Obwohl ein Backupserver Daten von einem einzelnen Client mit 25 MB/s streamen kann, ist nicht damit zu rechnen, dass vier simultan ausgeführte Backupjobs Daten mit 100 MB/s (25 MB/s x 4 Streams) streamen. Obgleich sich der Gesamtdurchsatz mit der Anzahl der Backup-Streams erhöht, können sich mit der Bandsoftware oder dem Netzwerkstapel verbundene Einschränkungen auf die einzelnen Backup-Streams auswirken.

Damit ein Bandbackup-Server beim Backup von Clients verlässlich von Adapterleistung und Netzwerkbandbreite Gebrauch macht, muss eine Netzwerkinfrastruktur Teaming-Funktionen wie Lastausgleich und Fehlertoleranz implementieren. Datenzentren beinhalten redundante Switches, Link Aggregation und Trunking im Rahmen ihrer fehlertoleranten Lösung. Obwohl Teaming-Gerätetreiber die Art des Datenflusses durch Team-Schnittstellen und Failover-Pfade manipulieren, ist dieser Vorgang für Bandbackup-Anwendungen transparent und führt nicht zur Unterbrechung der Bandbackup-Prozesse, wenn Remote-Systeme über das Netzwerk gesichert werden. Abbildung 6 zeigt eine Netzwerktopologie, die Bandbackup in einer Broadcom-Teamumgebung veranschaulicht und verdeutlicht, wie durch Smart Load Balancing Bandbackup-Daten über Team-Adapter einem *Lastausgleich* unterzogen werden können.

Es gibt vier Pfade, die der Client-Server zum Senden von Daten an den Backupserver verwenden kann; während des Datentransfers wird jedoch nur einer dieser Pfade zugewiesen. Einer der möglichen Pfade, die der Client-Server Red zum Senden von Daten an den Backupserver nutzen kann, ist Folgender:

Beispielpfad: Client-Server Red sendet Daten über Adapter A, Switch 1 und Backupserver-Adapter A.

Der zugewiesene Pfad wird von zwei Faktoren bestimmt:

1. ARP-Cache des Client-Servers; verweist auf die MAC-Adresse des Backupservers. Dies wird bestimmt durch den Lastausgleichalgorithmus für eingehenden Verkehr des Broadcom Intermediate-Treibers.

2. Die physische Adapterschnittstelle am Client-Server Red wird zur Übertragung der Daten verwendet. Dies wird durch den Lastausgleichalgorithmus für ausgehenden Verkehr des Broadcom Intermediate-Treibers bestimmt (siehe Ausgehender Verkehr und Eingehender Verkehr (nur SLB)).

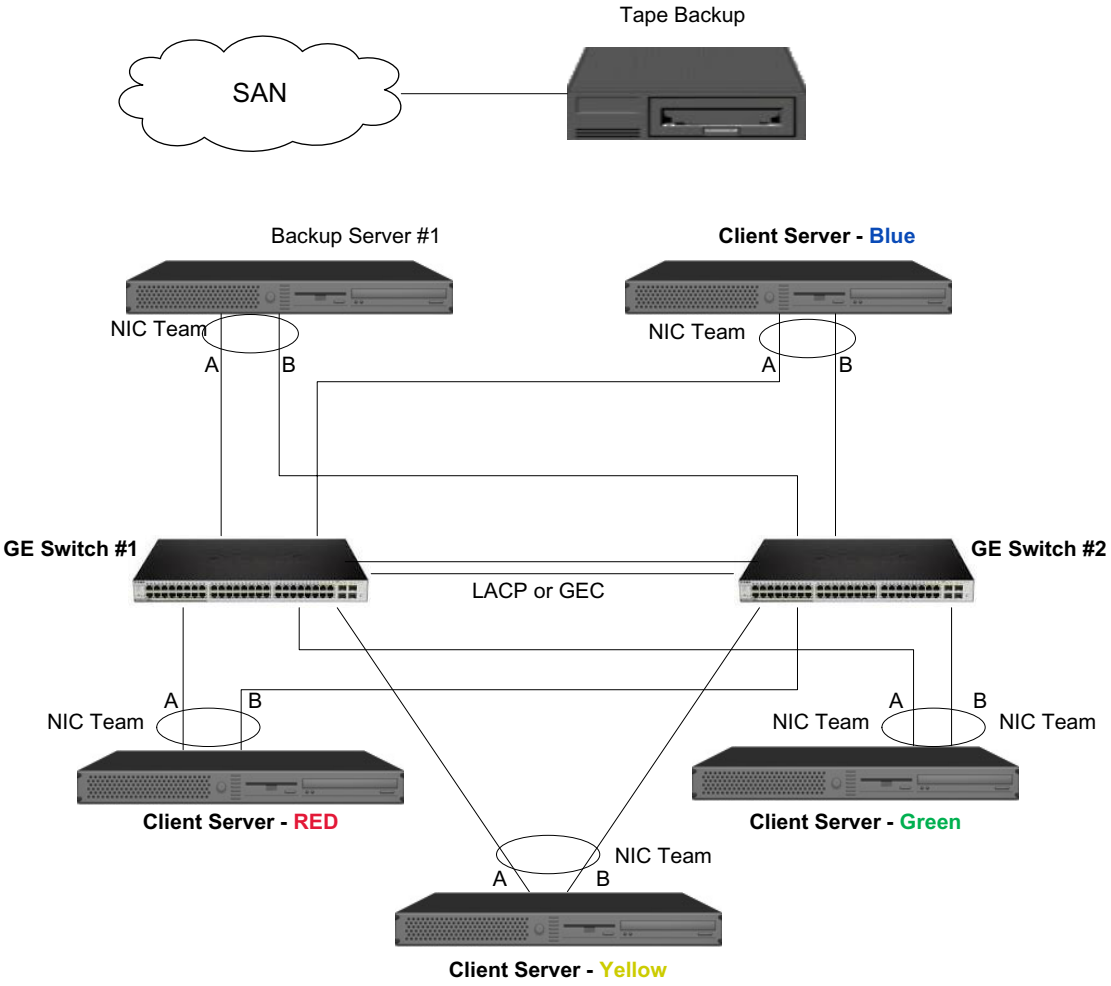
Die Team-Schnittstelle auf dem Backupserver sendet ein unangefordertes G-ARP (Gratuitous Address Resolution Protocol) an den Client-Server Red, was wiederum dazu führt, dass der ARP-Cache des Client-Servers mit der MAC-Adresse des Backupservers aktualisiert wird. Das Lastausgleichverfahren in der Team-Schnittstelle bestimmt die MAC-Adresse, die im G-ARP eingebettet ist. Die ausgewählte MAC-Adresse ist im Wesentlichen das Ziel für den Datentransfer vom Client-Server. Im Client-Server Red bestimmt der SLB-Teaming-Algorithmus, welche der beiden Adapterschnittstellen zur Datenübertragung verwendet wird. In diesem Beispiel werden Daten vom Client-Server Red an der Adapterschnittstelle A des Backupservers empfangen. Zur Veranschaulichung der SLB-Mechanismen bei Einwirkung einer zusätzlichen Datenlast an der Team-Schnittstelle stellen Sie sich ein Szenario vor, in dem der Backupserver einen zweiten Backupvorgang initiiert: einen zum Client-Server Red und einen zum Client-Server Blue. Die Route, die der Client-Server Blue zum Senden von Daten an den Backupserver verwendet, hängt von seinem ARP-Cache ab, der auf die MAC-Adresse des Backupservers verweist. Da der Adapter A des Backup-Servers bereits durch den Backupvorgang mit dem Client-Server Red belastet ist, ruft der Backup-Server seinen SLB-Algorithmus auf, um den Client-Server Blue darüber zu *informieren* (durch ein G-ARP), seinen ARP-Cache mit der MAC-Adresse von Adapter B des Backup-Servers zu aktualisieren. Wenn der Client-Server Blue Daten übertragen muss, verwendet er eine der Adapterschnittstellen, die durch seinen eigenen SLB-Algorithmus bestimmt wird. Wichtig ist, dass die Daten vom Client-Server Blue von der Adapterschnittstelle B des Backupservers und nicht von der Adapterschnittstelle A empfangen werden. Dies ist deshalb von Bedeutung, da der Backupserver Datenströme von verschiedenen Clients einem *Lastausgleich* unterziehen muss, wenn beide Backup-Streams simultan laufen. Sind beide Backup-Streams aktiv, verarbeitet jede Adapterschnittstelle auf dem Backupserver die gleiche Last, sodass Daten über beide Adapterschnittstellen ausgeglichen werden.

Derselbe Algorithmus wird angewendet, wenn ein dritter und vierter Backupvorgang vom Backupserver eingeleitet wird. Die Team-Schnittstelle auf dem Backupserver sendet ein Unicast-G-ARP an Backup-Clients, um sie zur Aktualisierung ihres ARP-Cache zu veranlassen. Jeder Client überträgt dann Backupdaten entlang einer Route an die MAC-Adresse auf dem Backupserver.

Fehlertoleranz

Wenn eine Netzverbindung während des Bandbackups ausfällt, wird der gesamte Verkehr zwischen Backupserver und Client gestoppt und die Backupjobs schlagen fehl. Wurde jedoch die Netzwerktopologie sowohl für Broadcom-SLB als auch für die Switch-Fehlertoleranz konfiguriert, können die Bandbackup-Vorgänge während des Verbindungsausfalls ohne Unterbrechung fortgesetzt werden. Alle Failover-Vorgänge innerhalb des Netzwerks sind für Bandbackup-Softwareanwendungen transparent. Informationen dazu, wie Backup-Datenströme beim Netzwerk-Failover gelenkt werden, gibt die Topologie in Abbildung 6. Der Client-Server Red überträgt über Pfad 1 Daten an den Backupserver, zwischen dem Backupserver und dem Switch kommt es jedoch zu einem Verbindungsausfall. Da die Daten nicht länger von Switch 1 an die Adapterschnittstelle A auf dem Backupserver gesendet werden können, werden sie von Switch 1 über Switch 2 an die Adapterschnittstelle B auf dem Backupserver umgeleitet. Dies geschieht ohne Wissen der Backupanwendung, da alle fehlertoleranten Vorgänge von der Adapterteam-Schnittstelle und den Trunk-Einstellungen der Switches bewältigt werden. Aus der Perspektive des Client-Servers läuft der Betrieb genauso, als würden Daten über den Originalpfad gesendet.

Abbildung 6: Netzwerkbackup mit SLB-Teaming über zwei Switches



Behebung von Teaming-Problemen

Bei Ausführung eines Protokollanalysators über einer Team-Schnittstelle eines virtuellen Adapters ist die in den gesendeten Rahmen angezeigte MAC-Adresse möglicherweise falsch. Der Analysator zeigt die Rahmen nicht so an, wie sie von BASP konstruiert wurden; anstelle der MAC-Adresse der Schnittstelle, die den Rahmen überträgt, wird die MAC-Adresse des Teams angezeigt. Folgendes Verfahren wird zur Überwachung eines Teams empfohlen:

1. Spiegeln Sie alle Uplink-Ports des Teams am Switch.
2. Umfasst das Team zwei Switches, spiegeln Sie auch den Trunk, über den die Switches gekoppelt sind.
3. Prüfen Sie alle Spiegel-Ports unabhängig voneinander.
4. Verwenden Sie am Analysator einen Adapter und einen Treiber, der QoS- und VLAN-Daten nicht filtert.

Tipps zur Teaming-Konfiguration

Vergewissern Sie sich bei der Behebung von Problemen mit der Netzwerkanbindung oder mit Teaming-Funktionen, dass die folgenden Angaben auf Ihre Konfiguration zutreffen.

1. Für ein SLB Team sollen alle Adapter die gleiche Übertragungsrate aufweisen.
2. Wenn LiveLink nicht aktiviert ist, deaktivieren Sie das Spanning Tree Protocol, oder aktivieren Sie einen STP-Modus, der die Initialphasen für die mit einem Team verbundenen Switch-Ports umgeht (z. B. Port Fast, Edge Port).
3. Alle Switches, mit denen das Team direkt verbunden ist, müssen dieselbe Hardware-, Firmware- und Softwareversion haben. Andernfalls ist keine Unterstützung gewährleistet.
4. Adapter, die ein Team bilden sollen, müssen demselben VLAN angehören. Falls mehrere Teams konfiguriert werden, sollte sich jedes Team in einem separaten Netzwerk befinden.
5. Geben Sie keine Multicast- oder Broadcast-Adresse in das Feld **Lokal verwaltete Adresse** ein.
6. Weisen Sie eine "Locally Administered Address" (Lokal verwaltete Adresse) niemals einem physischen Adapter zu, der dem Team angehört.
7. Überprüfen Sie, ob die Energieverwaltung für alle physischen Mitglieder aller Teams deaktiviert wurde (das Kontrollkästchen **Computer kann Gerät ausschalten, um Energie zu sparen** auf der Registerkarte **Energieverwaltung** unter **Eigenschaften** für den Adapter sollte deaktiviert sein; siehe Einstellen der Optionen zur Energieverwaltung in "nstallation der Windows-Treiber und Anwendung").
8. Löschen Sie alle statischen IP-Adressen in den einzelnen physischen Teammitgliedern, bevor das Team erstellt wird.
9. Ein Team, für das maximaler Durchsatz erforderlich ist, sollte LACP oder GEC\FEC verwenden. In diesen Fällen ist der Intermediate-Treiber nur verantwortlich für den Lastausgleich für ausgehenden Datenverkehr, während der Switch für den Lastausgleich für eingehenden Datenverkehr zuständig ist.
10. Gebündelte Teams (802.3ad \ LACP und GEC\FEC) müssen an nur einen Switch angeschlossen werden, der IEEE 802.3a, LACP oder GEC/FEC unterstützt.
11. Es wird nicht empfohlen, ein Team an einen Hub anzuschließen, da ein Hub nur den Halbduplex-Modus unterstützt. Hubs sollten nur zum Zweck der Problembehebung mit einem Team verbunden werden. Deaktivieren des Gerätetreibers eines Netzwerkadapters, der an einem LACP- oder GEC/FEC-Team teilnimmt, kann sich ungünstig auf die Netzwerkanbindung auswirken. Broadcom empfiehlt, dass der Adapter erst physisch vom Switch getrennt wird, bevor der Gerätetreiber deaktiviert wird, um einen Verlust der Netzwerkverbindung zu vermeiden.

12. Überprüfen Sie, ob die Basistreiber (Miniport) und Teamtreiber (Intermediate) demselben Versionspaket entstammen.
13. Testen Sie die Konnektivität für jeden physischen Adapter vor dem Teaming.
14. Testen Sie das Failover- und Fallback-Verhalten des Teams, bevor Sie es in einer Produktionsumgebung einsetzen.
15. Beim Übergang von einem Nicht-Produktionsnetzwerk zu einem Produktionsnetzwerk wird dringend empfohlen, erneut Failover- und Fallback-Tests durchzuführen.
16. Testen Sie das Leistungsverhalten des Teams, bevor Sie es in einer Produktionsumgebung einsetzen.

Richtlinien für die Problembehebung

Bevor Sie sich an den Support wenden, stellen Sie sicher, dass Sie die folgenden Schritte zur Behebung von Problemen mit der Netzwerkanbindung ausgeführt haben, wenn auf dem Server Adapter-Teaming verwendet wird.

1. Stellen Sie sicher, dass das Ethernet-Verbindungssignal für alle Adapter leuchtet und dass alle Kabel angeschlossen sind.
2. Überprüfen Sie, ob die passenden Basis- und Intermediate-Treiber demselben Versionspaket angehören und ordnungsgemäß geladen sind.
3. Überprüfen Sie mit dem Windows-Befehl **ipconfig**, ob eine gültige IP-Adresse vorhanden ist.
4. Überprüfen Sie, ob an den Switch-Ports, die mit dem Team verbunden sind, STP deaktiviert oder Edge Port/Port Fast aktiviert ist oder ob LiveLink verwendet wird.
5. Überprüfen Sie, ob die Konfiguration von Adaptern und Switch für die Übertragungsrate und Duplex übereinstimmt.
6. Wenn möglich, lösen Sie das Team auf, und überprüfen Sie die Konnektivität für alle Adapter unabhängig voneinander, um festzustellen, ob das Problem in direktem Zusammenhang mit dem Teaming steht.
7. Überprüfen Sie, ob alle mit dem Team verbundenen Switch-Ports sich im selben VLAN befinden.
8. Überprüfen Sie, ob die Switch-Ports korrekt für die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static konfiguriert sind und ob dies der Teamart des Adapters entspricht. Wenn das System für ein Team der Art SLB konfiguriert ist, stellen Sie sicher, dass die entsprechenden Switch-Ports nicht für die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static konfiguriert wurden.

Häufig gestellte Fragen

Frage:	Unter welchen Bedingungen wird der Datenverkehr keinem Lastausgleich unterzogen? Warum wird nicht sämtlicher Datenverkehr gleichmäßig über die Teammitglieder verteilt?
Antwort:	Der größte Teil des Datenverkehrs verwendet nicht IP/TCP/UDP, oder der Großteil der Clients befindet sich in einem anderen Netzwerk. Receive Load Balancing (RLB) ist keine Funktion der Datenverkehrslast, sondern eine Funktion der Anzahl der Clients, die mit dem System verbunden sind.

Frage:	Welche Netzwerkprotokolle werden in einem Team ausgeglichen?
Antwort:	Die Teaming-Software von Broadcom unterstützt nur IP/TCP/UDP-Verkehr. Der übrige Datenverkehr wird an den Primäradapter weitergeleitet.

Frage:	Welche Protokolle werden mit SLB ausgeglichen und welche nicht?
Antwort:	Nur für IP/TCP/UDP-Protokolle erfolgt ein Lastausgleich in beide Richtungen, also beim Senden und beim Empfangen.

Frage:	Kann ich einen Port mit 100 Mbit/s und einen Port mit 1000 Mbit/s in einem Team zusammenfassen?
Antwort:	Das Mischen von Übertragungsraten innerhalb eines Teams wird nur für Teams der Art Smart Load Balancing™ und 802.3ad-Teams unterstützt, wie an früherer Stelle beschrieben.

Frage:	Kann ich ein Team aus einem Fiber-Adapter und einem Gigabit Ethernet-Kupferadapter bilden?
Antwort:	In der Teamart SLB ist dies möglich. Es ist auch möglich, wenn der Switch dies für FEC/GEC und 802.3ad unterstützt.

Frage:	Worin besteht der Unterschied zwischen dem Lastausgleich über Adapter und Network Load Balancing (NLB) von Microsoft?
Antwort:	Der Lastausgleich über Adapter findet auf der Ebene der Netzwerksitzung statt, während NLB auf der Ebene der Systemanwendung ausgeführt wird.

Frage:	Kann ich die Team-Adapter an Ports in einem Router anschließen?
Antwort:	Nein. Alle Ports in einem Team müssen sich im selben Netzwerk befinden; in einem Router bildet jedoch jeder Port per Definition ein separates Netzwerk. In allen Teaming-Modi muss der Verbindungspartner ein Schicht-2-Switch sein.

Frage:	Kann ich Teaming mit Microsoft Cluster Services einsetzen?
Antwort:	Ja. Teaming wird nur im öffentlichen Netzwerk unterstützt, nicht im privaten Netzwerk, das für die Heartbeat-Verbindung verwendet wird.

Frage:	Funktioniert PXE über einen virtuellen Adapter (Team)?
Antwort:	Ein PXE-Client operiert in einer Umgebung vor dem Laden des Betriebssystems; daher wurden noch keine virtuellen Adapter aktiviert. Wenn der physische Adapter PXE unterstützt, kann er als PXE-Client verwendet werden, unabhängig davon, ob er Teil eines virtuellen Adapters ist, wenn das Betriebssystem geladen wird. PXE-Server können über einen virtuellen Adapter betrieben werden.

Frage:	Funktioniert WOL über einen virtuellen Adapter (Team)?
Antwort:	Die Wake On LAN-Funktion wird in einer Umgebung vor dem Laden des Betriebssystems wirksam. WOL tritt auf, wenn das System ausgeschaltet ist oder sich im Standby-Modus befindet, es ist also kein Team konfiguriert.

Frage:	Wie viele Ports können maximal in einem Team zusammengefasst werden?
Antwort:	Einem Team können bis zu 8 Ports zugewiesen werden.

Frage:	Wie viele Teams können maximal im selben System konfiguriert werden?
Antwort:	In einem System können bis zu 16 Teams konfiguriert werden.

Frage:	Warum geht bei meinem Team in den ersten 30 bis 50 Sekunden nach der Wiederherstellung des primären Adapters (Fallback) die Konnektivität verloren?
Antwort:	Dies liegt daran, dass der Port vom Spanning Tree Protocol vom blockierten Zustand in den weiterleitenden Zustand versetzt wird. Sie müssen auf den Switch-Ports, die mit dem Team verbunden sind, Port Fast oder Edge Port aktivieren oder LiveLink verwenden, um die STP-Verzögerung zu berücksichtigen.

Frage:	Kann ich ein Team über mehrere Switches hinweg verbinden?
Antwort:	Smart Load Balancing eignet sich für den Einsatz mit mehreren Switches, da jeder physische Adapter im System eine eindeutige Ethernet MAC-Adresse verwendet. Link Aggregation und Allgemeines Trunking können nicht über mehrere Switches eingerichtet werden, da hier alle physischen Adapter dieselbe Ethernet MAC-Adresse haben müssen.

Frage:	Wie kann ich den Intermediate-Treiber (BASP) aktualisieren?
Antwort:	Der Intermediate-Treiber kann nicht unter Local Area Connection Properties (LAN-Verbindungseigenschaften) aktualisiert werden. Die Aktualisierung muss über das Setup-Installationsprogramm erfolgen.

Frage:	Wie kann ich die Leistungsstatistik eines virtuellen Adapters (Team) feststellen?
Antwort:	Klicken Sie in Broadcom Advanced Control Suite auf die Registerkarte BASP Statistics (BASP-Statistik) für den virtuellen Adapter.

Frage:	Kann ich NLB und Teaming gleichzeitig konfigurieren?
Antwort:	Ja, allerdings nur, wenn NLB in einem Multicast-Modus ausgeführt wird (NLB wird von MS Cluster Services nicht unterstützt).

Frage:	Sollten das Backupsystem und die Client-Systeme, die gesichert werden, im Team konfiguriert werden?
Antwort:	Da die Datenlast für das Backupsystem am höchsten ist, sollte es für Link Aggregation und Failover stets im Team konfiguriert werden. Ein vollständig redundantes Netzwerk erfordert jedoch Teaming sowohl für Switches als auch Backup-Clients für Fehlertoleranz und Link Aggregation.

Frage:	Führt der Adapter-Teaming-Algorithmus bei Backupvorgängen den Lastausgleich für Daten auf Byte-Ebene oder auf Sitzungsebene durch?
Antwort:	Bei Verwendung von Adapter-Teaming wird die Datenlast nur auf Sitzungsebene und nicht auf Byte-Ebene ausgeglichen, damit Rahmen in ungeordneter Reihenfolge vermieden werden. Lastausgleich bei Adapter-Teaming funktioniert nicht in derselben Weise wie andere Lastausgleichsverfahren (z. B. EMC PowerPath).

Frage:	Ist für die Bandbackup-Software oder -Hardware eine besondere Konfiguration erforderlich, damit sie mit Adapter-Teaming funktioniert?
Antwort:	Es ist keine besondere Konfiguration der Bandbackup-Software erforderlich, damit sie mit Teaming funktioniert. Teaming ist für Bandbackup-Anwendungen transparent.

Frage:	Woher weiß ich, welchen Treiber ich derzeit verwende?
Antwort:	Die exakte Methode zum Überprüfen der Treiberversion ist in allen Betriebssystemen identisch: Suchen Sie die eigentliche Treiberdatei, und überprüfen Sie die Eigenschaften.

Frage:	Kann SLB einen Switch-Ausfall in einer Konfiguration mit Switch-Fehlertoleranz erkennen?
Antwort:	Nein. SLB kann nur den Verbindungsverlust zwischen dem Team-Port und seinem unmittelbaren Verbindungspartner erkennen. Verbindungsausfälle an anderen Ports kann SLB nicht erkennen. Weitere Informationen finden Sie unter LiveLink™.

Frage:	Wo kann ich Echtzeitstatistiken für ein Adapter-Team in einem Windows-System überwachen?
Antwort:	Verwenden Sie Broadcom Advanced Control Suite (BACS) zur Überwachung allgemeiner, IEEE 802.3- und benutzerdefinierter Leistungsindikatoren.

Ereignisprotokollmeldungen

Ereignisprotokollmeldungen unter Windows

Im folgenden Abschnitt werden die bekannten Ereignisprotokoll-Statusmeldungen für Basis- und Intermediate-Treiber in Windows-Systemen für Broadcom NetXtreme Gigabit Ethernet-Adapter aufgeführt. Beim Laden eines Broadcom-Adaptertreibers zeigt Windows einen Statuscode in der Ereignisanzeige des Systems an. Für diese Ereigniscodes kann es bis zu zwei Klassen von Einträgen geben, je nachdem, ob beide Treiber geladen werden (ein Satz für den Basis- oder Miniport-Treiber und ein Satz für den Intermediate- oder Teaming-Treiber).

Basistreiber (Physischer Adapter/Miniport)

Tabelle 11 listet die Ereignisprotokollmeldungen auf, die vom Basistreiber unterstützt werden, erläutert die Ursache der jeweiligen Meldung und informiert über die empfohlenen Maßnahmen.

Tabelle 11. Ereignisprotokollmeldungen für Basistreiber

Benachrichtigung Nummer	Benachrichtigung	Ursache	Korrekturmaßnahme
1	Failed to allocate memory for the device block. (Speicher für Geräteblock konnte nicht zugewiesen werden.) Check system memory resource usage. (Überprüfen Sie die Auslastung der Systemspeicherressourcen.)	Der Treiber kann keinen Betriebssystemspeicher zuweisen.	Schließen Sie laufende Anwendungen, um Speicher freizugeben.
2	Failed to allocate map registers. (Es konnten keine Map-Register zugewiesen werden.)	Der Treiber kann aus dem Betriebssystem keine Map-Register zuordnen.	Entfernen Sie andere Treiber, die möglicherweise Map-Register zuordnen.
3	Failed to access configuration information. (Auf die Konfigurationsdaten konnte nicht zugegriffen werden.) Reinstall the network driver. (Installieren Sie den Netzwerktreiber neu.)	Der Treiber kann nicht auf die PCI-Konfigurationsregister auf dem Adapter zugreifen.	Bei zusätzlichen Adaptern: Setzen Sie den Adapter erneut in den Steckplatz ein, wählen Sie einen anderen PCI-Steckplatz für den Adapter aus, oder tauschen Sie den Adapter aus.
4	The network link is down. (Die Netzwerkverbindung ist nicht aktiv.) Check to make sure the network cable is properly connected. (Überprüfen Sie, ob das Netzwerkkabel richtig angeschlossen ist.)	Der Adapter hat die Verbindung zum Verbindungspartner verloren.	Überprüfen Sie, ob das Netzwerkkabel angeschlossen und vom richtigen Typ ist und ob der Verbindungspartner (z. B. Switch oder Hub) korrekt funktioniert.

Tabelle 11. Ereignisprotokollmeldungen für Basistreiber (Forts.)

Benachrichtigung Nummer	Benachrichtigung	Ursache	Korrekturmaßnahme
5	The network link is up. (Die Netzwerkverbindung ist aktiv.)	Der Adapter hat eine Verbindung hergestellt.	Meldung nur zur Information. Keine Maßnahme erforderlich.
6	Network controller configured for 10Mb half-duplex link. (Netzwerkcontroller ist für 10-Mb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
7	Network controller configured for 10Mb full-duplex link. (Netzwerkcontroller ist für 10-Mb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
8	Network controller configured for 100Mb half-duplex link. (Netzwerkcontroller ist für 100-Mb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
9	Network controller configured for 100Mb full-duplex link. (Netzwerkcontroller ist für 100-Mb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
10	Network controller configured for 1Gb half-duplex link. (Netzwerkcontroller ist für 1-Gb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
11	Network controller configured for 1Gb full-duplex link. (Netzwerkcontroller ist für 1-Gb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
12	Medium not supported. (Medium wird nicht unterstützt.)	Das IEEE 802.3-Medium wird vom Betriebssystem nicht unterstützt.	Starten Sie das Betriebssystem neu, führen Sie eine Virenüberprüfung durch, führen Sie eine Festplattenüberprüfung durch (chkdsk), und installieren Sie das Betriebssystem neu.
13	Unable to register the interrupt service routine. (Interrupt Service Routine konnte nicht registriert werden.)	Der Gerätetreiber kann den Interrupt-Handler nicht installieren.	Starten Sie das Betriebssystem neu. Entfernen Sie andere Gerätetreiber, die u. U. dieselbe IRQ verwenden.

Tabelle 11. Ereignisprotokollmeldungen für Basistreiber (Forts.)

Benachrichtigung Nummer	Benachrichtigung	Ursache	Korrekturmaßnahme
14	Unable to map IO space. (IO-Space kann nicht zugewiesen werden.)	Der Gerätetreiber kann keine im Speicher abgebildete Ein-/Ausgabe (I/O) für den Zugriff auf Treiberregister zuweisen.	Entfernen Sie andere Adapter aus dem System, verringern Sie die Menge des installierten physischen Speichers, und tauschen Sie den Adapter aus.
15	Driver initialized successfully. (Treiber wurde erfolgreich initialisiert.)	Der Treiber wurde erfolgreich geladen.	Meldung nur zur Information. Keine Maßnahme erforderlich.
16	NDIS is resetting the miniport driver. (NDIS setzt den Miniport-Treiber zurück.)	Die NDIS-Schicht hat ein Problem beim Senden/Empfangen von Paketen entdeckt und setzt den Treiber zurück, um das Problem zu lösen.	Führen Sie das Broadcom Advanced Control Suite-Diagnoseprogramm aus; überprüfen Sie das Netzwerkkabel auf Beschädigungen.
18	Unknown PHY detected. (Unbekannte PHY entdeckt.) Using a default PHY initialization routine. (Es wird eine Standard-Routine zur PHY-Initialisierung verwendet.)	Der Treiber konnte die PHY-ID nicht lesen.	Tauschen Sie den Adapter aus.
19	This driver does not support this device. (Der Treiber bietet keine Unterstützung für dieses Gerät.) Upgrade to the latest driver. (Aktualisieren Sie auf den neuesten Treiber.)	Der Treiber erkennt den installierten Adapter nicht.	Aktualisieren Sie auf eine Treiberversion, die diesen Adapter unterstützt.
20	Driver initialization failed. (Treiberinitialisierung fehlgeschlagen.)	Unspezifizierter Fehler bei der Treiberinitialisierung.	Installieren Sie den Treiber neu, aktualisieren Sie auf eine aktuellere Treiberversion, führen Sie das Broadcom Advanced Control Suite-Diagnoseprogramm aus, oder tauschen Sie den Adapter aus.
21	Ethernet@Wirespeed ist aktiviert und konnte nicht die maximale Verbindungsgeschwindigkeit aushandeln.	Das Kabel oder die Verbindung ist möglicherweise fehlerhaft.	Schließen Sie das Kabel wieder an oder ersetzen Sie das Kabel.
22	Gerätetreiber kann nicht für den veralteten Netzwerkcontroller für dieses Betriebssystem installiert werden.	Der neueste externe Treiber unterstützt keine veralteten Geräte mehr.	Nutzen Sie den internen Treiber oder ersetzen Sie das Gerät mit dem aktuellsten.
256	Nicht genügend zusammenhängender physischer Speicher für verknüpften Pool.	Treiber kann nicht genügend gemeinsam genutzten Speicher für die Verknüpfung von Paketpuffern zuweisen.	Entfernen/Deaktivieren anderer Adapter aus dem System oder Systemspeicher erhöhen.

Intermediate-Treiber (Virtueller Adapter/Team)

Tabelle 12 listet die Ereignisprotokollmeldungen auf, die vom Intermediate-Treiber unterstützt werden, erläutert die Ursache der jeweiligen Meldung und informiert über die empfohlenen Maßnahmen.

Tabelle 12. Ereignisprotokollmeldungen für Intermediate-Treiber

Systemereignis Meldungsnummer	Benachrichtigung	Ursache	Korrekturmaßnahme
1	Unable to register with NDIS. (Registrierung an NDIS nicht möglich.)	Der Treiber kann sich nicht an der NDIS-Schnittstelle registrieren.	Entfernen Sie andere NDIS-Treiber.
2	Unable to instantiate the management interface. (Managementschnittstelle konnte nicht instanziiert werden.)	Der Treiber kann keine Geräteinstanz erstellen.	Starten Sie das Betriebssystem neu.
3	Unable to create symbolic link for the management interface. (Es konnte keine symbolische Verknüpfung für die Managementschnittstelle erstellt werden.)	Ein anderer Treiber hat einen Gerätenamen erstellt, der potentiell Konflikte verursacht.	Entfernen Sie den Gerätetreiber, der den Namen *Blf* verwendet und potentiell Konflikte verursacht.
4	Broadcom Advanced Server Program Driver has started. (Der Broadcom Advanced Server Program-Treiber wurde gestartet.)	Ein anderer Treiber hat einen Gerätenamen erstellt, der potentiell Konflikte verursacht.	Meldung nur zur Information. Keine Maßnahme erforderlich.
5	Broadcom Advanced Server Program Driver has stopped. (Der Broadcom Advanced Server Program-Treiber wurde angehalten.)	Der Treiber wurde angehalten.	Meldung nur zur Information. Keine Maßnahme erforderlich.
6	Could not allocate memory for internal data structures. (Es konnte kein Speicher für interne Datenstrukturen zugewiesen werden.)	Der Treiber kann keinen Betriebssystemspeicher zuweisen.	Schließen Sie laufende Anwendungen, um Speicher freizugeben.
7	Could not bind to adapter. (Bindung an Adapter nicht möglich.)	Der Treiber konnte keinen der physischen Adapter im Team öffnen.	Entfernen Sie und laden Sie den Treiber des physischen Adapters neu, installieren Sie einen aktualisierten Treiber für den physischen Adapter, oder tauschen Sie den physischen Adapter aus.
8	Successfully bind to adapter. (Bindung an Adapter erfolgreich.)	Der Treiber hat den physischen Adapter geöffnet.	Meldung nur zur Information. Keine Maßnahme erforderlich.
9	Network adapter is disconnected. (Netzwerkadapter ist getrennt.)	Der physische Adapter ist nicht mit dem Netzwerk verbunden (es wurde keine Verbindung hergestellt).	Überprüfen Sie, ob das Netzwerkkabel angeschlossen und vom richtigen Typ ist und ob der Verbindungspartner (Switch oder Hub) korrekt funktioniert.

Tabelle 12. Ereignisprotokollmeldungen für Intermediate-Treiber (Forts.)

Systemereignis Meldungsnummer	Benachrichtigung	Ursache	Korrekturmaßnahme
10	Network adapter is connected. (Netzwerkadapter ist verbunden.)	Der physische Adapter ist mit dem Netzwerk verbunden (es wurde eine Verbindung hergestellt).	Meldung nur zur Information. Keine Maßnahme erforderlich.
11	Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System. (Der Broadcom Advanced Program Features-Treiber ist nicht für den Betrieb unter dieser Version des Betriebssystems ausgelegt.)	Der Treiber bietet keine Unterstützung für das Betriebssystem, auf dem er installiert wurde.	Lesen Sie in den Versionshinweisen zum Treiber nach, und installieren Sie den Treiber unter einem unterstützten Betriebssystem, oder aktualisieren Sie den Treiber.
12	Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter. (Hot-Standby-Adapter ist als primärer Adapter für ein Team ohne einen Adapter für Lastausgleich ausgewählt.)	Es wurde ein Standby-Adapter aktiviert.	Ersetzen Sie den ausgefallenen physischen Adapter.
13	Network adapter does not support Advanced Failover. (Netzwerkadapter bietet keine Unterstützung für erweitertes Failover.)	Broadcom NIC Extension (NICE) wird vom physischen Adapter nicht unterstützt.	Ersetzen Sie den Adapter durch einen anderen, der NICE unterstützt.
14	Network adapter is enabled via management interface. (Netzwerkadapter wurde über Managementschnittstelle aktiviert.)	Der Treiber hat erfolgreich einen physischen Adapter über die Managementschnittstelle aktiviert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
15	Network adapter is disabled via management interface. (Netzwerkadapter wurde über Managementschnittstelle deaktiviert.)	Der Treiber hat erfolgreich einen physischen Adapter über die Managementschnittstelle deaktiviert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
16	Network adapter is activated and is participating in network traffic. (Netzwerkadapter wurde aktiviert und nimmt am Netzwerkverkehr teil.)	Ein physischer Adapter wurde dem Team hinzugefügt oder in einem Team aktiviert.	Meldung nur zur Information. Keine Maßnahme erforderlich.
17	Network adapter is de-activated and is no longer participating in network traffic. (Netzwerkadapter wurde deaktiviert und nimmt nicht länger am Netzwerkverkehr teil.)	Der Treiber erkennt den installierten Adapter nicht.	Meldung nur zur Information. Keine Maßnahme erforderlich.

Abschnitt 4: Virtuelle LANs

VLAN-Überblick

Virtuelle LANs (VLANs) ermöglichen es Ihnen, das physische LAN logisch zu unterteilen, Arbeitsgruppen logisch zu segmentieren und für jedes logische Segment Sicherheitsrichtlinien festzulegen. Jedes definierte VLAN verhält sich wie ein separates Netzwerk, dessen Datenverkehr und Broadcasts von den anderen Netzwerken getrennt sind, so dass die Bandbreiteneffizienz innerhalb der einzelnen logischen Gruppen erhöht wird. Für jeden Broadcom-Adapter auf dem Server können Sie bis zu 64 VLANs (63 markierte und 1 unmarkiertes) definieren, je nachdem, wie viel Speicherplatz in Ihrem System verfügbar ist.

VLANs können zu Teams hinzugefügt werden, um mehrere VLANs mit unterschiedlichen VLAN-IDs zu ermöglichen. Für jedes hinzugefügte VLAN wird ein virtueller Adapter erstellt.

VLANs werden normalerweise verwendet, um einzelne Broadcast-Domänen bzw. separate IP-Subnetze einzurichten. Es kann sich jedoch unter Umständen als nützlich erweisen, wenn ein Server gleichzeitig in mehreren VLANs verfügbar ist. Broadcom-Adapter unterstützen mehrere VLANs auf Port- oder auf Teambasis und ermöglichen so äußerst flexible Netzwerkkonfigurationen.

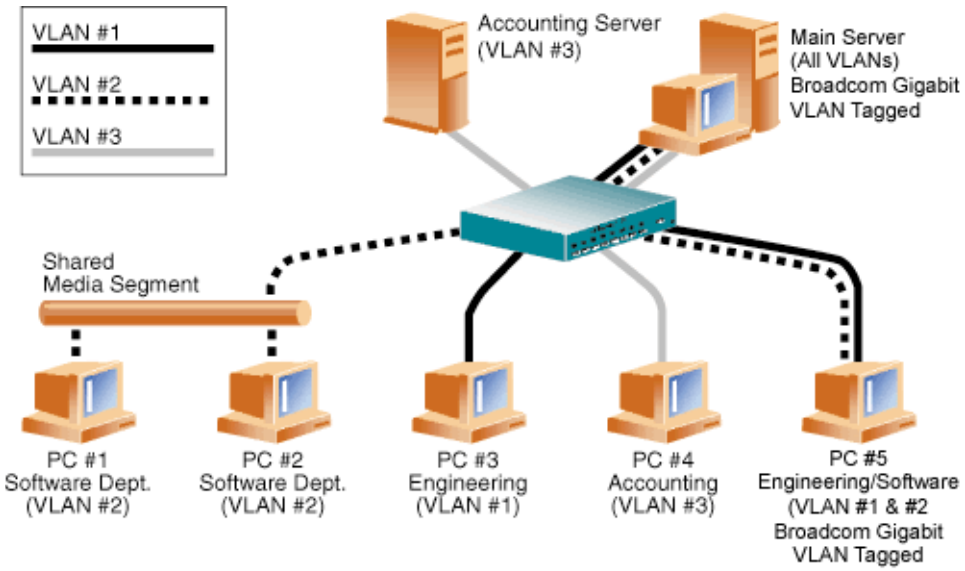


Abbildung 7: Beispiel für die Unterstützung mehrerer markierter VLANs durch Server

Abbildung 7 zeigt ein Netzwerk mit mehreren VLANs. In diesem Netzwerk besteht das physische LAN aus einem Switch, zwei Servern und fünf Clients. Das LAN ist logisch in drei verschiedene VLANs unterteilt, von denen jedes ein anderes IP-Subnetz darstellt. Die Funktionen dieses Netzwerks werden in Tabelle 13 beschrieben:

Tabelle 13. Beispiel für eine VLAN-Netzwerktopologie

Komponente	*Beschreibung*
VLAN 1	IP-Subnetz, das den Haupt-Server, PC 3 und PC 5 umfasst. Dieses Subnetz stellt eine Technikergruppe dar.
VLAN 2	Umfasst den Haupt-Server, PC 1 und PC 2 (über ein gemeinsam genutztes Mediensegment) sowie PC 5. Bei diesem VLAN handelt es sich um eine Software-Entwicklergruppe.
VLAN 3	Umfasst den Haupt-Server, den Buchhaltungs-Server und PC 4. Bei diesem VLAN handelt es sich um eine Buchhaltungsgruppe.
Primärer Nameserver	Ein sehr häufig verwendeter Server, der von allen VLANs und IP-Subnetzen aus erreichbar sein muss. Auf dem Haupt-Server ist ein Broadcom-Adapter installiert. Der Zugriff auf die drei IP-Subnetze erfolgt über eine physische Adapterschnittstelle. Der Server ist mit einem Switch-Port verbunden, der für VLAN 1, 2 und 3 konfiguriert ist. Sowohl für den Adapter als auch für den verbundenen Switch-Port ist die Markierung aktiviert. Da beide Geräte in der Lage sind, VLANs zu markieren, kann der Server über alle drei IP-Subnetze in diesem Netzwerk kommunizieren, behandelt die drei Subnetze beim Broadcasting aber weiterhin als separate Einheiten.
Buchhaltungs-Server	Nur für VLAN 3 verfügbar. Der Buchhaltungs-Server ist vom gesamten Datenverkehr in VLAN 1 und VLAN 2 getrennt. Bei dem mit diesem Server verbundenen Switch-Port ist die Markierung deaktiviert.
PC 1 und 2	Sind an einen gemeinsam genutzten Medien-Hub angeschlossen, der wiederum mit dem Switch verbunden ist. PC 1 und PC 2 sind nur in VLAN 2 eingebunden und befinden sich logisch im gleichen IP-Subnetz wie der Haupt-Server und PC 5. Bei dem an dieses Segment angeschlossenen Switch-Port ist die Markierung deaktiviert.
PC 3	PC 3 ist in VLAN 1 eingebunden und kann nur mit dem Haupt-Server und PC 5 kommunizieren. Bei dem Switch-Port von PC 3 ist die Markierung deaktiviert.
PC 4	PC 4 ist in VLAN 3 eingebunden und kann nur mit den Servern kommunizieren. Bei dem Switch-Port von PC 4 ist die Markierung deaktiviert.
PC 5	PC 5 ist in VLAN 1 und VLAN 2 eingebunden und verfügt über einen Broadcom-Adapter. Er ist an Switch-Port 10 angeschlossen. Der Adapter und der Switch-Port sind für VLAN 1 und VLAN 2 konfiguriert, und bei beiden ist die Markierung aktiviert.

Hinweis: Das Markieren von VLANs muss nur bei Switch-Ports, die Trunk-Verbindungen zu anderen Switches herstellen, oder Ports, die an markierungsfähige Endstationen wie Server oder Arbeitsstationen mit Broadcom-Adaptern angeschlossen sind, aktiviert sein.

Hinzufügen von VLANs zu Teams

Jedes Team unterstützt bis zu 64 VLANs (63 markierte und 1 unmarkiertes). Sind mehrere VLANs mit einem Adapter verbunden, können Sie einen Server in mehreren IP-Subnetzen logisch verfügbar machen. Sind mehrere VLANs in ein Team eingebunden, können Sie einen Server in mehreren IP-Subnetzen verfügbar machen und die Vorteile der Lastausgleich- und Failover-Funktionen nutzen. Anweisungen zum Hinzufügen eines VLANs in ein Team finden Sie für Windows-Betriebssysteme unter "Hinzufügen eines VLANs".

Hinweis: Adapter, die zu einem Failover-Team gehören, können auch so konfiguriert werden, dass sie VLANs unterstützen. Netzwerkkarten von Drittanbietern unterstützen keine VLANs. Wenn ein Failover-Team eine Netzwerkkarte eines Drittanbieters umfasst, können daher keine VLANs für dieses Team konfiguriert werden.

Abschnitt 5: Verwaltungsfunktionen

CIM

Beim CIM-Modell (*Common Information Model;* Gemeinsames Informationsmodell) handelt es sich um einen von dem Standardisierungsgremium DMTF (*Distributed Management Task Force*) festgelegten Industriestandard. Microsoft implementiert CIM auf Windows Plattformen wie Windows Server 2008. Broadcom unterstützt CIM auf Windows Server 2008-Plattformen.

Durch das Implementieren von CIM stehen über CIM-Clientanwendungen verschiedene Klassen zur Informationsbereitstellung für Benutzer zur Verfügung. Beachten Sie, dass der Broadcom CIM-Datenprovider nur Daten zur Verfügung stellt. Benutzer können zum Durchsuchen der vom Broadcom CIM-Provider bereitgestellten Daten eine beliebige CIM-Clientsoftware verwenden.

Die Klassen, durch die vom Broadcom CIM-Provider Informationen bereitgestellt werden, heißen BRCM_NetworkAdapter und BRCM_ExtraCapacityGroup. Die BRCM_NetworkAdapter-Klasse bietet Netzwerkadapter-Informationen, die zu einer Gruppe von Adaptern gehören, einschließlich Controller von Broadcom und anderen Herstellern. Die BRCM_ExtraCapacityGroup-Klasse ist für die Teamkonfiguration für Broadcom Advanced Server Program (BASP) verantwortlich. Die derzeitige Implementierung bietet Teaminformationen und Informationen zu den physischen Netzwerkadaptern im Team.

Broadcom Advanced Server Program stellt Ereignisse über Ereignisprotokolle bereit. Benutzer können diese Ereignisse über die Ereignisanzeige von Windows Server 2008 oder über CIM anzeigen bzw. überwachen. Der Broadcom CIM-Provider stellt außerdem Ereignisinformationen über das generische Ereignismodell von CIM bereit Bei diesen Ereignissen handelt es sich um __InstanceCreationEvent, __InstanceDeletionEvent und __InstanceModificationEvent, die durch CIM festgelegt werden. Die Clientanwendung muss die Ereignisse aus der Anwendung bei CIM registrieren, damit Ereignisse erfolgreich empfangen werden können. Dies erfolgt mit Hilfe von Abfragen (siehe nachfolgende Beispiele).

```
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"
```

Detaillierte Informationen zu diesen Ereignissen finden Sie in der CIM-Dokumentation unter http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf.

SNMP

BASP-Subagent

Der BASP-Subagent, baspmgnt.dll, ist für den Windows Server 2008-SNMP-Dienst vorgesehen. Der SNMP-Dienst muss vor der Installation des BASP-Subagenten installiert werden.

Mit dem BASP-Subagenten kann die SNMP-Manager-Software die Konfigurationen und Leistung der Broadcom Advanced Server-Funktionen aktiv überwachen. Der Subagent stellt außerdem eine Warn-Trap-Funktion für einen SNMP-Manager zur Verfügung, mit der der Manager über Änderungen an den Konditionen der BASP-Komponente informiert wird.

Mit dem BASP-Subagenten können Sie die Konfigurationen und Statistiken der BASP-Teams, der physischen NIC-Adapter in einem Team und der virtuellen NIC-Adapter, die als Ergebnis der Teaming-Funktion erstellt wurden, überwachen. NIC-Adapter, die nicht Bestandteil von Teams sind, werden zu diesem Zeitpunkt noch nicht überwacht. Die BASP-Konfigurationsdaten umfassen Informationen wie Team-IDs, physische, virtuelle, VLAN- und Team-Adapter-IDs, die dazugehörigen Beschreibungen sowie die MAC-Adressen der Adapter.

Die Statistiken beinhalten detaillierte Informationen zu übertragenen und eingegangenen Datenpaketen für die physischen, virtuellen, VLAN- und Team-Adapter.

Die Warn-Trap-Funktion leitet Informationen zu den Änderungen an der Konfiguration der physischen Adapter in einem Team weiter (z. B. aktive oder inaktive Verbindung, installierter Adapter, entfernte Ereignisse usw.)

Zum Überwachen dieser Informationen muss der SNMP-Manager die Broadcom BASP MIB-Datenbankdateien hochladen. Die nachfolgend aufgeführten Dateien sind auf dem Treibermedium enthalten:

baspcfg.mib

baspstat.mib

basptrap.mib

BASP Extensible-Agent

Der Broadcom NetXtreme Gigabit Ethernet Controller Extended Information SNMP Extensible-Agent, bcmif.dll, ist für den Windows Server SNMP-Dienst vorgesehen.

Der Extensible-Agent ermöglicht der SNMP-Manager-Software das aktive Überwachen der Konfigurationen des Broadcom NetXtreme-Adapters. Darüber hinaus sollen die bereits durch die standardmäßige SNMP-Management-Netzwerkschnittstelle bereitgestellten Informationen ergänzt werden.

Der Extensible-Agent stellt detaillierte Informationen zu einem Broadcom NetXtreme-Adapter bereit, z. B.:

- MAC-Adresse
- Gebundene IP-Adresse
- IP-Subnetzmaske
- Status der physischen Verbindung
- Adapterstatus
- Übertragungsrate
- Duplexmodus

- Speicherbereich
- Interrupt-Einstellung
- Busnummer
- Gerätenummer
- Funktionsnummer

Zum Überwachen dieser Informationen muss der SNMP-Manager die Broadcom Extended Information MIB-Datei laden. Diese Datei, bcmif.mib, ist auf der Installations-CD des Broadcom NetXtreme-Adapters enthalten.

Auf der zu überwachenden Arbeitsstation müssen der Broadcom Extended Information SNMP Extensible-Agent, bcmif.dll, installiert und der Microsoft Windows Server 2008-SNMP-Dienst installiert und geladen sein.

Abschnitt 6: Installieren der Hardware

Hinweis: Dieser Abschnitt gilt nur für zusätzliche Netzwerkkartenmodelle der Broadcom NetXtreme Gigabit Ethernet-Adapter.

Sicherheitsvorkehrungen

Vorsicht! Der Adapter wird in einem System installiert, dessen Betriebsspannungen tödlich sein können. Vor dem Entfernen der Systemabdeckung müssen Sie folgende Maßnahmen zum persönlichen Schutz und zur Vermeidung von Schäden an Systemkomponenten durchführen:

- Entfernen Sie alle Metallobjekte oder Schmuck von Händen und Handgelenken.
- Stellen Sie sicher, dass Sie ausschließlich isolierte bzw. nichtleitende Werkzeuge verwenden.
- Stellen Sie sicher, dass das System ausgeschaltet und der Netzstecker gezogen ist, bevor Sie interne Komponenten berühren.
- Installieren oder entfernen Sie Adapter in einer Umgebung, die nicht elektrostatisch aufgeladen ist. Das Tragen einer ordnungsgemäß geerdeten Erdungsmanschette am Handgelenk und die Verwendung anderer Antistatik-Geräte sowie einer antistatischen Fußmatte wird ausdrücklich empfohlen.

Vor der Installation – Checkliste

1. Überprüfen Sie, ob der Server das neueste BIOS verwendet.
2. Wenn in Ihrem System ein Betriebssystem gestartet ist, fahren Sie das Betriebssystem ordnungsgemäß herunter.
3. Wenn das System vollständig heruntergefahren ist, schalten Sie es aus, und ziehen Sie den Netzstecker.
4. Halten Sie die Adapterkarte an den Seiten fest, entfernen Sie die Verpackung, und legen Sie die Karte auf einer antistatischen Oberfläche ab.
5. Prüfen Sie den Adapter und insbesondere den Stiftsockel der Karte auf sichtbare Anzeichen von Schäden. Installieren Sie niemals einen beschädigten Adapter.

Installieren des Adapters

Die folgenden Anweisungen gelten für die Installation des Broadcom NetXtremeGigabit Ethernet-Adapters (zusätzliche Netzwerkkarte) auf den meisten Servern. Weitere Informationen, wie die Installation auf Ihrem Server auszuführen ist, finden Sie in den Handbüchern, die im Lieferumfang Ihres Servers enthalten waren.

1. Lesen Sie nochmals die Abschnitte Sicherheitsvorkehrungen und Vor der Installation – Checkliste. Vor der Installation des Adapters müssen Sie sicherstellen, dass das System AUSGESCHALTET und der Netzstecker gezogen ist. Außerdem müssen entsprechende Erdungsmaßnahmen durchgeführt worden sein.
2. Öffnen Sie die Systemabdeckung, und wählen Sie einen leeren PCI Express-Steckplatz aus.
3. Entfernen Sie die Abdeckplatte vom ausgewählten Steckplatz.
4. Richten Sie die Steckerleiste des Adapters an der Buchsenleiste des Systems aus.
5. Drücken Sie gleichmäßig auf die beiden Ecken der Karte, und schieben Sie die Adapterkarte in den Steckplatz, bis sie fest sitzt. Wenn der Adapter ordnungsgemäß eingesetzt worden ist, sind die Portanschlüsse an der Steckplatzöffnung ausgerichtet, und die Frontplatte schließt genau mit dem Systemgehäuse ab.

Vorsicht! Beim Einsetzen der Karte sollte nicht übermäßig viel Kraft aufgewendet werden, da dies zu Schäden am System oder am Adapter führen kann. Wenn sich der Adapter nicht einsetzen lässt, nehmen Sie ihn wieder heraus, richten Sie ihn nochmals aus, und versuchen Sie es erneut.

6. Befestigen Sie den Adapter mit der Adapterklemme oder -schraube.
7. Schließen Sie das Systemgehäuse, und entfernen Sie Ihre Antistatik-Geräte.

Anschließen der Netzwerkkabel

Kupfer

Der Broadcom NetXtremeGigabit Ethernet-Adapter verfügt einen oder mehrere RJ-45-Anschlüsse, über die der Rechner mit einem Ethernet-Kupferdrahtsegment verbunden werden kann.

Hinweis: Der Broadcom NetXtreme Gibabit Ethernet-Adapter unterstützt Automatic MDI Crossover (MDIX), so dass zum Vernetzen von Computern keine Crossover-Kabel erforderlich sind. Mit einem Straight-Through-Kabel der Kategorie 5 können Rechner miteinander kommunizieren, wenn sie direkt miteinander verbunden sind.

1. Wählen Sie ein geeignetes Kabel aus. Tabelle 14: "10/100/1000BASE-T-Kabelspezifikationen" führt die Eigenschaften von Kabeln für den Anschluss an 10/100/1000BASE-T-Ports auf:

Tabelle 14. 10/100/1000BASE-T-Kabelspezifikationen

Porttyp	*Anschluss*	*Speichermedien*	*Maximale Länge*
10BASE-T	RJ-45	UTP-Kabel der Kategorie 3, 4 oder 5	100 m
100/1000BASE-T[1]	RJ-45	UTP-Kabel der Kategorie 5[2]	100 m

[1] Bei 1000BASE-T-Signalisierung sind vier TP-Kabel der Kategorie 5 für symmetrische Verkabelung gemäß ISO/IEC 11801:1995 und EIA/TIA-568-A (1995) erforderlich, die mit den in TIA/EIA TSB95 definierten Verfahren getestet wurden.

[2] Mindestens Kategorie 5. Kategorie 5e und Kategorie 6 werden vollständig unterstützt.

2. Schließen Sie ein Kabelende an den Adapter an.
3. Schließen Sie das andere Kabelende an den RJ-45 Ethernet-Netzwerkport an.

Hinweis: Wenn das Kabel auf beiden Seiten korrekt angeschlossen ist, sollten die Port-LEDs am Adapter aufleuchten. In Tabelle 14: "10/100/1000BASE-T-Kabelspezifikationen" auf Seite 67 finden Sie eine Beschreibung der Netzwerkverbindung und der Betriebsanzeige.

Abschnitt 7: Erstellen einer Treiberdiskette

Anweisungen zum Erstellen einer Treiberdiskette finden Sie in der Dokumentation, die im Lieferumfang Ihres Systems enthalten war.

Abschnitt 8: Broadcom Boot Agent-Treibersoftware

Überblick

Die Broadcom NetXtreme Gigabit Ethernet-Adapter unterstützen Preboot Execution Environment (PXE), Remote Program Load (RPL), iSCSI Boot und Bootstrap Protocol (BootP). Multi-Boot Agent (MBA) ist ein Software-Modul, das dem an das Netzwerk angeschlossenen System ermöglicht, mit einem von den Remote-Systemen im Netzwerk zur Verfügung gestellten Betriebssystem-Images zu booten. Der Broadcom MBA-Treiber entspricht der PXE-Spezifikation 2.1 und wird mit monolithischen und geteilten Binär-Images zur Verfügung gestellt. Dies gewährleistet Flexibilität für Benutzer in verschiedenen Umgebungen, deren Systemplatine u. U. nicht über einen integrierten Basis-Code verfügt.

Das MBA-Modul wird in einer Client-System-Umgebung eingesetzt. Ein Netzwerk besteht aus einem oder mehreren Boot-Systemen, die Boot-Images mehreren Systemen über das Netzwerk zur Verfügung stellen. Die Broadcom MBA-Modul-Implementierung wurde in den folgenden Umgebungen erfolgreich getestet:

- **Linux® Red Hat® PXE-Server.** Broadcom PXE-Clients können einen Remote-Boot durchführen, Netzwerk-Ressourcen (NFS-Mount usw.) verwenden und Linux-Installationen vornehmen. Bei einem Remote-Boot-Vorgang wird der Linux-Universaltreiber nahtlos an die Broadcom UNDI (Universelle Netzwerktreiber-Schnittstelle) angebunden, wodurch der unter Linux im Fernzugriff gestarteten Client-Umgebung eine Netzwerkschnittstelle zur Verfügung steht.
- **Intel® APITEST:** Der Broadcom PXE-Treiber besteht alle Testprogramme für die Prüfung der API-Kompatibilität.
- **Windows Deployment Service (WDS)**: Für Windows Server wurde RIS durch WDS ersetzt, so dass ein Broadcom PXE-Client Windows-Betriebssysteme installieren kann, u. a. Windows Server 2008.

Einrichten von MBA Agent in einer Client-Umgebung

Bei zusätzlichen Netzwerkkarten gehen Sie folgendermaßen vor. Weitere Informationen zu LOMs finden Sie im Systemhandbuch zu Ihrem Computer.

Das Einrichten von MBA Agent in einer Client-Umgebung umfasst folgende Schritte:

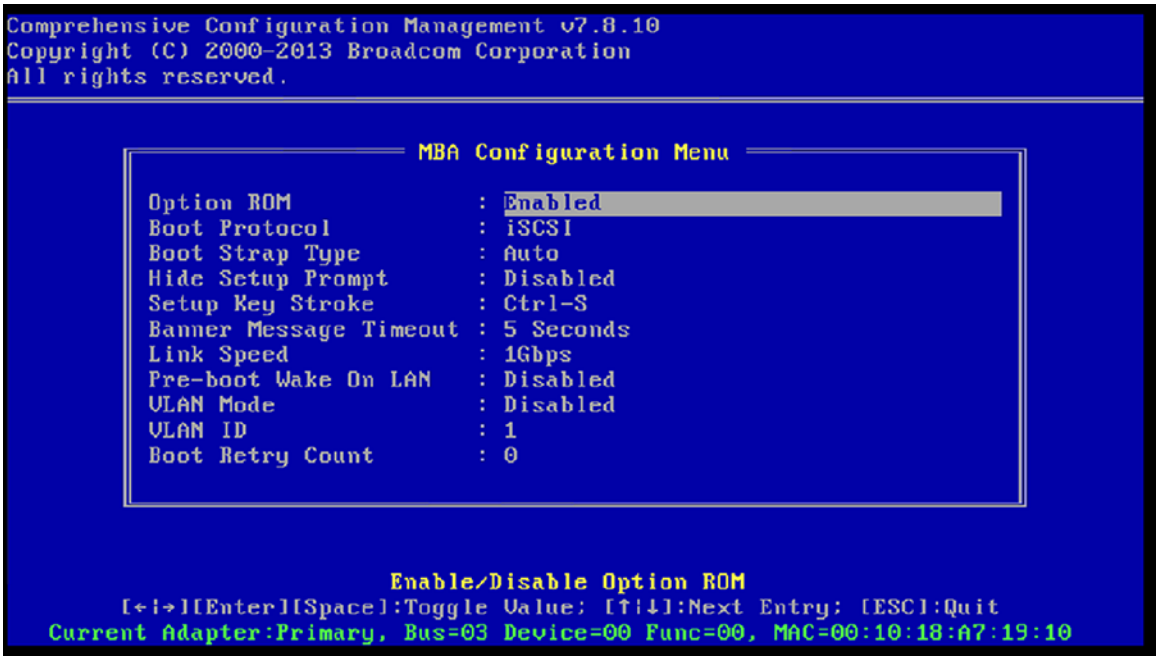
1. Konfigurieren des MBA-Treibers.
2. Einrichten von BIOS für die Boot-Reihenfolge

Konfigurieren des MBA-Treibers

Dieser Abschnitt gilt für die Konfiguration des MBA-Treibers bei zusätzlichen Netzwerkkartenmodellen der Broadcom-Adapter. Informationen zur Konfiguration des MBA-Treibers bei LOM-Modellen der Broadcom-Adapter finden Sie in Ihrer Systemdokumentation.

Verwenden von CCM

1. Starten Sie Ihr System neu.
2. Drücken Sie die Tasten **STRG + S**.Für diesen Vorgang stehen Ihnen nach entsprechender Aufforderung bis zu vier Sekunden Zeit zur Verfügung. Es wird eine Liste mit Adaptern angezeigt.
   a. Wählen Sie den zu konfigurierenden Adapter aus, und drücken Sie die **Eingabetaste**. Es wird das Hauptmenü angezeigt.
   b. Wählen Sie **MBA Configuration** (MBA-Konfiguration) aus, um das MBA-Konfigurationsmenü zu öffnen.



3. Verwenden Sie die Pfeil-nach-oben- oder die Pfeil-nach-unten-Taste, um das Menüelement **Boot Protocol**

auszuwählen. Verwenden Sie anschließend die Pfeil-nach-rechts- oder die Pfeil-nach-links-Taste, um das gewünschte Boot-Protokoll auszuwählen, wenn andere Boot-Protokolle neben PXE (Preboot Execution Environment) verfügbar sind. Diese eventuell verfügbaren Boot-Protokolle umfassen Remote Program Load (RPL) und Bootstrap Protocol (BOOTP).

Hinweis: Für einige, aber nicht alle, iSCSI-bootfähige LOMs wird das Boot-Protokoll über das BIOS festgelegt. Weitere Informationen erhalten Sie in Ihrer Systemdokumentation.

Hinweis: Wenn Ihr System über mehrere Adapter verfügt und Sie unsicher sind, welchen Adapter Sie konfigurieren, drücken Sie die Tasten **STRG + F6**. Dies führt dazu, das die Port-LEDs auf dem Adapter zu blinken beginnen.

4. Verwenden Sie die Pfeil-nach-oben-, die Pfeil-nach-unten-, die Pfeil-nach-links- und die Pfeil-nach-rechts-Taste, um bei Bedarf die Werte der anderen Menüelemente zu ändern.
5. Drücken Sie auf **F4**, um Ihre Einstellungen zu speichern.
6. Drücken Sie nach dem Speichern der Einstellungen auf **ESC**.

Verwenden von uEFI

1. Starten Sie Ihr System neu.
2. Rufen Sie das Konfigurationsmenü für die Systemeinrichtung oder die Geräteeinstellungen auf.
3. Wählen Sie das Gerät aus, bei dem Sie die MBA-Einstellungen ändern möchten.
4. Wählen Sie **MBA Configuration Menu** (MBA-Konfigurationsmenü) aus.
5. Verwenden Sie das Dropdown-Menü, um das gewünschte Boot-Protokoll auszuwählen, falls neben Preboot Execution Environment (PXE) andere Boot-Protokolle zur Verfügung stehen. Falls verfügbar, gehören zu den anderen Boot-Protokollen iSCSI und Bootstrap Protocol (BOOTP).

Hinweis: Für iSCSI-bootfähige LOMs wird das Boot-Protokoll über das BIOS festgelegt. Weitere Informationen erhalten Sie in Ihrer Systemdokumentation.

6. Verwenden Sie die Pfeil-nach-oben-, die Pfeil-nach-unten-, die Pfeil-nach-links- und die Pfeil-nach-rechts-Taste, um bei Bedarf die Werte der anderen Menüelemente zu ändern.
7. Wählen Sie **Back** (Zurück) aus, um zum Hauptmenü zurückzukehren.
8. Wählen Sie **Finish** (Fertig stellen) zum Speichern und Beenden aus.

Einrichten von BIOS

Legen Sie den MBA-aktivierten Adapter als erstes bootfähiges Gerät unter BIOS fest, um ein Booten mit dem MBA vom Netzwerk zu ermöglichen. Dieses Verfahren hängt von der BIOS-Implementierung des Systems ab. Weitere Informationen finden Sie im Benutzerhandbuch des Systems.

Abschnitt 9: iSCSI-Protokoll

iSCSI Boot

Broadcom NetXtreme Gigabit Ethernet-Adapter unterstützen iSCSI-Boot, wodurch Systeme ohne Laufwerk über das Netzwerk booten können. Mit iSCSI-Boot kann ein Windows- oder Linux-Betriebssystem über ein herkömmliches IP-Netzwerk auf einem Remote-iSCSI-Zielcomputer gestartet werden.

Sowohl für Windows- als auch Linux-Betriebssysteme, kann iSCSI-Boot so konfiguriert werden, dass mit den allgemeinen Parametern wie in Tabelle 15 dargestellt gestartet wird.

Unterstützte Betriebssysteme für iSCSI-Boot

iSCSI-Boot wird von den Broadcom NetXtreme Gigabit Ethernet-Adaptern für die folgenden Betriebssysteme unterstützt:

- Windows Server-Betriebssystem
- Enterprise Linux-Distribution

Einrichten von iSCSI-Boot

Dieser Abschnitt bezieht sich auf den BIOS-Modus für iSCSI-Boot. Informationen zur Einrichtung von UEFI iSCSI-Boot finden Sie in der Systemdokumentation.

iSCSI-Boot wird im BIOS-Modus nicht unterstützt, wenn ein lokaler Speicher (besonders RAID) aufgrund von Speicherbeschränkungen genutzt wird.

Das Einrichten von iSCSI-Boot besteht aus den folgenden Schritten:

- Konfigurieren des iSCSI-Ziels
- Konfigurieren der iSCSI-Bootparameter
- Vorbereiten des iSCSI-Boot-Image
- Booten

Konfigurieren des iSCSI-Ziels

Das Konfigurieren des iSCSI-Ziels erfolgt bei den Zielen der verschiedensten Hersteller auf unterschiedliche Weise. Informationen über das Konfigurieren des iSCSI-Ziels finden Sie in der vom Hersteller mitgelieferten Dokumentation. Die allgemeinen Schritte sind:

1. Einrichten eines iSCSI-Ziels

2. Einrichten eines virtuellen Laufwerks
3. Zuweisen des virtuellen Laufwerks an das in Schritt 1 eingerichtete virtuelle Laufwerk
4. Verknüpfen eines iSCSI-Initiators mit dem iSCSI-Ziel
5. Notieren des Namens des iSCSI-Ziels, der TCP-Portnummer, der iSCSI-LUN (Logical Unit Number), des Internet Qualified Name (IQN) des Ziels und der Einzelheiten zur CHAP-Authentifizierung
6. Nach dem Konfigurieren des iSCSI-Ziels verfügen Sie über die folgenden Informationen:
   - IQN des Ziels
   - Ziel-IP-Adresse
   - TCP-Portnummer des Ziels
   - LUN des Ziels
   - IQN des Initiators
   - CHAP-ID und CHAP-Kennwort

Konfigurieren der iSCSI-Bootparameter

Konfigurieren Sie die Broadcom iSCSI-Bootsoftware entweder auf statische oder auf dynamische Konfiguration. Informationen über die im Bildschirm "Allgemeine Parameter" verfügbaren Konfigurationsoptionen finden Sie unter Tabelle 15.

Tabelle 15 enthält sowohl Parameter für IPv4 als auch für IPv6. Parameter, die nur für IPv4 bzw. IPv6 gelten, sind entsprechend gekennzeichnet.

Hinweis: Die Verfügbarkeit von iSCSI-Boot für IPv6 ist plattform- bzw. geräteabhängig.

Tabelle 15. Konfigurationsoptionen

Option	*Beschreibung*
TCP/IP-Parameter über DHCP	Diese Option gilt nur für IPv4. legt fest, ob die iSCSI-Boothost-Software die IP-Adresse über DHCP erhält (aktiviert) oder eine statische IP-Konfiguration verwendet (deaktiviert)
IP-Autokonfiguration	Diese Option gilt nur für IPv6. Sie legt fest, ob die iSCSI-Boothost-Software eine zustandslose link-local-Adresse und/oder eine zustandbehaftete Adresse konfigurieren soll, wenn DHCPv6 vorhanden und in Verwendung ist ("Aktiviert"). Router-Solicitation-Pakete werden bis zu dreimal in einem Abstand von 4 Sekunden zwischen den einzelnen Wiederholungen gesendet. Sie können aber auch eine statische IP-Konfiguration verwenden ("Deaktivieren").
iSCSI-Parameter über DHCP	legt fest, ob die iSCSI-Boothost-Software die Parameter des ISCSI-Ziels über DHCP (aktiviert) oder über eine statische Konfiguration (deaktiviert) erhält. Die statischen Informationen werden im Bildschirm "Konfigurieren der Parameter für iSCSI-Initiator" eingegeben.
CHAP-Authentifizierung	legt fest, ob die iSCSI-Boothost-Software eine CHAP-Authentifizierung für den Verbindungsaufbau zum iSCSI-Ziel verwendet. Wenn CHAP-Authentifizierung aktiviert ist, werden CHAP-ID und CHAP-Kennwort im Bildschirm "Konfigurieren der Parameter für iSCSI-Initiator" eingegeben.
DHCP Vendor ID	legt fest, wie die iSCSI-Boothost-Software bei DHCP das Feld "Vendor Class ID" interpretiert. Wenn das Feld "Vendor Class ID" im DHCP Offer Packet dem Wert in diesem Feld entspricht, sucht die iSCSI-Boothost-Software in den Feldern "DHCP Option 43" nach den angeforderten iSCSI-Boot-Erweiterungen. Bei deaktiviertem DHCP muss kein Wert festgelegt werden.

Tabelle 15. Konfigurationsoptionen (Forts.)

Option	*Beschreibung*
Verzögerung nach Verbindungsaufbau	legt die Wartezeit (in Sekunden) für die iSCSI-Boothost-Software zwischen dem Aufbau einer Ethernet-Verbindung und dem Senden von Daten über das Netzwerk fest. Die gültigen Werte liegen im Bereich zwischen 0 und 255. Ein Benutzer muss z. B. möglicherweise einen Wert für diese Option festlegen, wenn ein Netzwerkprotokoll, wie z. B. Spanning Tree, an der Switch-Schnittstelle zum Client-System aktiviert ist.
TCP-Zeitstempel verwenden	aktiviert bzw. deaktiviert die Option "TCP-Zeitstempel"
Ziel als erstes HDD	legt fest, dass das iSCSI-Ziellaufwerk als erste Festplatte im System erscheint
Anzahl Wiederholungen bei "LUN besetzt"	legt die Anzahl der Wiederholungen des Verbindungsaufbaus durch den iSCSI-Boot-Initiator bei nicht erreichbarer iSCSI-Ziel-LUN fest
IP-Version	Diese Option gilt nur für IPv6. Schaltet zwischen dem IPv4- und dem IPv6-Protokoll um. Wenn Sie von einer Protokollversion zur anderen wechseln, gehen alle IP-Einstellungen verloren.

Konfigurieren des MBA-Bootprotokolls

So konfigurieren Sie das Bootprotokoll

1. Starten Sie Ihr System neu.
2. Drücken Sie im PXE-Banner **CTRL+S**. Das Menü "MBA-Konfigurationsmenü" wird angezeigt (siehe Broadcom Boot Agent).
3. Wechseln Sie im "MBA-Konfigurationsmenü" mit Hilfe von **Pfeil-nach-oben** bzw. **Pfeil-nach-unten** zur Option **Bootprotokoll**. Ändern Sie mit Hilfe von **Pfeil-nach-links** bzw. **Pfeil-nach-rechts** die Option **Bootprotokoll** zu **iSCSI**.

Hinweis: Weitere Informationen zu Plattformen, auf denen das Bootprotokoll über das BIOS eingestellt wird, finden Sie in der Systemdokumentation.

4. Wählen Sie im **Hauptmenü** die Option **iSCSI-Boot-Konfiguration** aus.

Hinweis: Wenn im NetXtreme Netzwerkadapter keine iSCSI-Boot-Firmware programmiert ist, hat das Auswählen von **iSCSI-Boot-Konfiguration** keinerlei Effekt.

iSCSI-Boot-Konfiguration

- Konfigurieren einer statischen iSCSI-Boot-Konfiguration
- Konfigurieren einer dynamischen iSCSI-Boot-Konfiguration

Konfigurieren einer statischen iSCSI-Boot-Konfiguration

Bei einer statischen Konfiguration müssen Sie die IP-Adresse des Systems, den Initiator-IQN des Systems und die unter Konfigurieren des iSCSI-Ziels erhaltenen Parameter des Ziels eingeben. Informationen über Konfigurationsoptionen finden Sie unter Tabelle 15.

So konfigurieren Sie die iSCSI-Boot-Parameter in einer statischen Konfiguration

1. Nehmen Sie im Menübildschirm **Allgemeine Parameter** die folgenden Einstellungen vor:
   - **TCP/IP-Parameter über DHCP**: Deaktiviert. (Für IPv4.)
   - **IP-Autokonfiguration**: Deaktiviert. (Für IPv6)
   - **iSCSI-Parameter über DHCP**: Deaktiviert.

- **CHAP-Authentifizierung**: Deaktiviert.
- **Booten von iSCSI-Ziel**: Deaktiviert.
- **DHCP-Hersteller-ID**: BRCM ISAN
- **Verzögerung nach Verbindungsaufbau**: 0
- **TCP-Zeitstempel verwenden**: Aktiviert (bei einigen Zielen wie dem Dell/EMC AX100i, muss **TCP-Zeitstempel verwenden** aktiviert sein).
- **Ziel als erstes HDD**: Deaktiviert.
- **Anzahl Wiederholungen bei "LUN besetzt"**: 0
- **IP-Version**: IPv6. (Für IPv6)

2. Drücken Sie **ESC**, um zum **Hauptmenü** zurückzukehren.
3. Wählen Sie im **Hauptmenü** die Option **Initiator-Parameter** aus.
4. Geben Sie im Bildschirm **Initiatorparameter** die folgenden Werte ein:
   - IP-Adresse (nicht angegebene IPv4- und IPv6-Adressen sollten jeweils "0.0.0.0" und "::" lauten**)**
   - Präfix für Subnetzmaske
   - Standard-Gateway
   - Primärer DNS
   - Sekundärer DNS
   - iSCSI-Name (entspricht dem vom Client-System zu verwendenden Namen des iSCSI-Initiators)

Hinweis: Geben Sie die IP-Adresse ein. Achten Sie dabei auf die korrekte Eingabe. Die IP-Adresse wird nicht auf Fehler im Hinblick auf Dopplungen oder falsche Zuweisungen zu einem Segment/Netzwerk geprüft.

5. Drücken Sie **ESC**, um zum **Hauptmenü** zurückzukehren.
6. Wählen Sie im **Hauptmenü** die Option **Parameter des ersten Ziels** aus.
7. Aktivieren Sie im Bildschirm **Parameter des ersten Ziels** die Option **Verbinden** , um eine Verbindung zum iSCSI-Ziel aufzubauen. Geben Sie die folgenden Werte ein, die auch beim Konfigurieren des iSCSI-Ziels verwendet wurden:
   - IP-Adresse
   - TCP-Port
   - Boot-LUN
   - iSCSI-Name:
8. Drücken Sie **ESC**, um zum **Hauptmenü** zurückzukehren.
9. Drücken Sie **ESC** und wählen Sie die Option **Beenden und Konfiguration speichern** aus.
10. Drücken Sie **F4**, um die MBA-Konfiguration zu speichern.

Konfigurieren einer dynamischen iSCSI-Boot-Konfiguration

Bei einer dynamischen Konfiguration müssen Sie lediglich vorgeben, dass die IP-Adresse des Systems und die Daten für Ziel/Initiator über DHCP bereitgestellt werden sollen (siehe Konfiguration von IPv4 und IPv6 unter Konfigurieren des DHCP-Servers auf Unterstützung von iSCSI-Boot). Bei IPv4 werden mit Ausnahme des Initiator-iSCSI-Namens sämtliche Einstellungen auf den Bildschirmen für die Parameter des Initiators, die Parameter des ersten Ziels und die des zweiten Ziels ignoriert und müssen daher nicht gelöscht werden. Bei IPv6 werden mit Ausnahme von CHAP-ID und CHAP-Kennwort sämtliche Einstellungen auf den Bildschirmen für die Parameter des Initiators, die Parameter des ersten Ziels und die des zweiten Ziels ignoriert und müssen daher nicht gelöscht werden. Informationen über Konfigurationsoptionen finden Sie unter Tabelle 15.

HINWEISE:

- Bei Verwendung eines DHCP-Servers werden die Einträge des DNS-Servers durch die vom DHCP-Server bereitgestellten Werte überschrieben. Dies tritt selbst dann auf, wenn die lokal bereitgestellten Werte gültig sind und der DHCP-Server keine Daten über den DNS-Server zur Verfügung stellt. Wenn der DHCP-Server keine Daten über den DNS-Server zur Verfügung stellt, werden die Werte sowohl für den primären als auch für den sekundären DNS-Server auf 0.0.0.0 eingestellt. Wenn das Betriebssystem Windows die Steuerung übernimmt, fragt der Microsoft iSCSI Initiator die Parameter des iSCSI Initiators ab und konfiguriert die entsprechenden Register statisch. Dabei werden die zuvor konfigurierten Werte immer überschrieben. Da der DHCP-Daemon in der Umgebung von Windows als Benutzerprozess ausgeführt wird, müssen alle TCP/IP-Parameter statisch festgelegt werden, bevor der Stack in der iSCSI-Boot-Umgebung aufgebaut wird.
- Bei Verwendung von "DHCP Option 17" werden die Daten über das Ziel vom DHCP-Server bereitgestellt, und als Initiator-iSCSI-Name wird der im Bildschirm "Initiator-Parameter" eingegebene Name verwendet. Wenn kein Wert ausgewählt wird, nimmt der Controller standardmäßig diesen Namen an:

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

wobei die Zeichenfolge `11.22.33.44.55.66` der MAC-Adresse des Controllers entspricht.

Bei Verwendung von "DHCP Option 43" (nur IPv4) werden sämtliche Einstellungen auf den Bildschirmen für die Parameter des Initiators, die Parameter des ersten Ziels und die des zweiten Ziels ignoriert und müssen daher nicht gelöscht werden.

So konfigurieren Sie die iSCSI-Boot-Parameter mit Hilfe einer dynamischen Konfiguration

1. Nehmen Sie im Menübildschirm **Allgemeine Parameter** die folgenden Einstellungen vor:
   - **TCP/IP-Parameter über DHCP**: Aktiviert. (Für IPv4.)
   - **IP-Autokonfiguration**: Aktiviert. (Für IPv6)
   - **iSCSI-Parameter über DHCP**: Aktiviert
   - **CHAP-Authentifizierung**: Deaktiviert.
   - **Booten von iSCSI-Ziel**: Deaktiviert.
   - **DHCP-Hersteller-ID**: BRCM ISAN
   - **Verzögerung nach Verbindungsaufbau**: 0
   - **TCP-Zeitstempel verwenden**: Aktiviert (bei einigen Zielen wie dem Dell/EMC AX100i, muss **TCP-Zeitstempel verwenden** aktiviert sein).
   - **Ziel als erstes HDD**: Deaktiviert.
   - **Anzahl Wiederholungen bei "LUN besetzt"**: 0
   - **IP-Version**: IPv6. (Für IPv6)
2. Drücken Sie **ESC**, um zum **Hauptmenü** zurückzukehren.

Hinweis: Die Daten in den Bildschirmen **Initiator-Parameter** und **Parameter des ersten Ziels** werden ignoriert; ein Löschen dieser Daten ist nicht erforderlich.

3. Wählen Sie **Beenden und Konfigurationen speichern** aus.

Aktivieren der CHAP-Authentifizierung

Stellen Sie sicher, dass die CHAP-Authentifizierung für das Ziel deaktiviert wurde.

CHAP-Authentifizierung aktivieren

1. Stellen Sie im Bildschirm **Allgemeine Parameter** die Option **CHAP-Authentifizierung** auf "Aktiviert" ein.
2. Geben Sie im Bildschirm **Initiatorparameter** die folgenden Werte ein:
   - CHAP-ID (bis zu 128 Byte)
   - CHAP-Kennwort (wenn eine Authentifizierung erforderlich ist, muss aus mindestens 12 Zeichen bestehen)
3. Drücken Sie **ESC**, um zum **Hauptmenü** zurückzukehren.
4. Wählen Sie im **Hauptmenü** die Option **Parameter des ersten Ziels** aus.
5. Geben Sie im Bildschirm **Parameter des ersten Ziels** die folgenden Werte ein, die auch beim Konfigurieren des iSCSI-Ziels verwendet wurden:
   - CHAP-ID (optional, bei Zweiweg-CHAP)
   - CHAP-Kennwort (optional, bei Zweiweg-CHAP, muss aus mindestens 12 Zeichen bestehen)
6. Drücken Sie **ESC**, um zum **Hauptmenü** zurückzukehren.
7. Drücken Sie **ESC** und wählen Sie die Option **Beenden und Konfiguration speichern** aus.

Konfigurieren des DHCP-Servers auf Unterstützung von iSCSI-Boot

Bei dem DHCP-Server handelt es sich um eine optionale Komponente, die nur benötigt wird, wenn Sie eine Konfiguration für dynamisches iSCSI-Boot einrichten (siehe Konfigurieren einer dynamischen iSCSI-Boot-Konfiguration).

Die Konfiguration des DHCP-Servers zur Unterstützung von iSCSI-Boot ist für IPv4 und IPv6 unterschiedlich.

- DHCP-Konfigurationen für iSCSI-Boot bei IPv4
- DHCP-Konfiguration für iSCSI-Boot bei IPv6

DHCP-Konfigurationen für iSCSI-Boot bei IPv4

Das DHCP-Protokoll beinhaltet eine Anzahl von Optionen, die Konfigurationsinformationen an den DHCP-Client übermitteln. Die Broadcom-Adapter unterstützen die folgenden DHCP-Konfigurationen für iSCSI-Boot:

- DHCP Option 17, Root Path
- DHCP Option 43, Herstellerspezifische Informationen

DHCP Option 17, Root Path

Mit Hilfe von Option 17 werden Informationen über das iSCSI-Ziel an den iSCSI-Client übermittelt.

Das Format für das Wurzelverzeichnis ist in IETC RFC 4173 definiert und lautet:

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

Die Definitionen der Parameter finden Sie weiter unten.

Tabelle 16. Definition der Parameter von "DHCP Option 17"

Parameter	*Definition*
`"iscsi:"`	eine festgelegte Zeichenfolge
`<servername>`	die IP-Adresse oder FQDN des iSCSI-Ziels
`":"`	Trennzeichen
`<protocol>`	das IP-Protokoll für den Zugriff auf das iSCSI-Ziel Zurzeit wird ausschließlich TCP unterstützt, das Protokoll lautet daher "6".
`<port>`	die dem Protokoll zugeordnete Portnummer Die Standardportnummer für iSCSI lautet "3260".
`<LUN>`	Dies ist die für das iSCSI-Ziel zu verwendende Logical Unit Number. Der Wert der LUN muss im hexadezimalen Format angegeben sein. Eine LUN mit einer ID OF 64 muss im Parameter zu "Option 17" des DHCP-Servers als 40 konfiguriert werden.
`<targetname>`	der Name des Ziels, entweder im IQN-Format oder im EUI-Format (Details zu den Formaten IQN und EUI finden Sie in RFC 3720). Ein Beispiel für einen IQN-Namen wäre "iqn.1995-05.com.broadcom:iscsi-target".

DHCP Option 43, Herstellerspezifische Informationen

DHCP Option 43 (herstellerspezifische Informationen) stellt dem iSCSI-Client mehr Konfigurationsoptionen zur Verfügung als DHCP Option 17. In dieser Konfiguration werden drei zusätzliche Unteroptionen angeboten, die den Initiator-IQN dem iSCSI-Boot-Client zuweisen und zusätzlich zwei iSCSI-Ziel-IQN bereitstellen, die zum Booten verwendet werden können. Das Format des iSCSI-Ziel-IQN ist mit dem Format von DHCP Option 17 identisch, beim iSCSI-Initiator-IQN handelt es sich einfach um den IQN des Initiators.

Hinweis: DHCP Option 43 wird nur bei IPv4 unterstützt.

Im Folgenden sind die Unteroptionen aufgeführt.

Tabelle 17. Definition der Unteroptionen von DHCP Option 43

Unteroption	*Definition*
201	Informationen über das erste iSCSI-Ziel im Standardformat für das Wurzelverzeichnis `"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Informationen über das zweite iSCSI-Ziel im Standardformat für das Wurzelverzeichnis `"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	iSCSI-Initiator-IQN

Bei Verwendung der DHCP Option 43 sind umfangreichere Konfigurationsschritte vorzunehmen als bei DHCP Option 17, die Umgebung ist jedoch reichhaltiger und es stehen mehr Konfigurationsoptionen zur Verfügung. Broadcom empfiehlt beim Ausführen einer dynamischen iSCSI-Boot-Konfiguration die Verwendung von DHCP Option 43.

Konfigurieren des DHCP-Servers

Konfigurieren Sie den DHCP-Server so, dass er Option 17 oder Option 43 unterstützt.

Hinweis: Bei Verwendung von Option 43 muss zusätzlich Option 60 konfiguriert werden. Der Wert von Option 60 muss dem Wert von **DHCP Vendor ID** entsprechen. Der Wert von **DHCP Vendor ID** lautet "BRCM ISAN", wie im Bildschirm **Allgemeine Parameter** des Menüs "iSCSI-Boot-Konfiguration" angezeigt.

DHCP-Konfiguration für iSCSI-Boot bei IPv6

Der DHCPv6-Server stellt eine Reihe von Optionen zur Verfügung, darunter eine zustandslose oder zustandbehaftete IP-Konfiguration sowie Informationen für den DHCPv6-Client. Die Broadcom-Adapter unterstützen die folgenden DHCP-Konfigurationen für iSCSI-Boot:

- DHCPv6 Option 16, Vendor Class-Option
- DHCPv6 Option 17, Herstellerspezifische Informationen

Hinweis: Die DHCPv6-Standardoption "Root Path" ist noch nicht verfügbar. Broadcom empfiehlt für die Unterstützung von dynamischem iSCSI-Boot bei IPv6 die Verwendung von Option 16 oder Option 17.

DHCPv6 Option 16, Vendor Class-Option

DHCPv6 Option 16 (Vendor Class-Option) muss vorhanden sein und eine Zeichenfolge enthalten, die mit dem Parameter **DHCP Vendor ID** übereinstimmt. Der Wert von **DHCP Vendor ID** lautet "BRCM ISAN", wie im Bildschirm **Allgemeine Parameter** des Menüs "iSCSI-Boot-Konfiguration" angezeigt.

Der Inhalt von Option 16 sollte <2 Byte Länge> <DHCP Vendor ID> sein.

DHCPv6 Option 17, Herstellerspezifische Informationen

DHCPv6 Option 17 (herstellerspezifische Informationen) stellt dem iSCSI-Client weitere Konfigurationsoptionen zur Verfügung. In dieser Konfiguration werden drei zusätzliche Unteroptionen angeboten, die den Initiator-IQN dem iSCSI-Boot-Client zuweisen und zusätzlich zwei iSCSI-Ziel-IQN bereitstellen, die zum Booten verwendet werden können.

Im Folgenden sind die Unteroptionen aufgeführt.

Tabelle 18. Definition der Unteroptionen von DHCP Option 17

Unteroption	*Definition*
201	Informationen über das erste iSCSI-Ziel im Standardformat für das Wurzelverzeichnis `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Informationen über das zweite iSCSI-Ziel im Standardformat für das Wurzelverzeichnis `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	iSCSI-Initiator-IQN

Hinweis: Die Klammern [ ] in Tabelle 18 sind für IPv6-Adressen erforderlich.

Der Inhalt von Option 17 sollte <2 Byte Optionsnummer 201|202|203> <2 Byte Länge> <Daten> sein.

Konfigurieren des DHCP-Servers

Konfigurieren Sie den DHCP-Server so, dass er Option 16 und Option 17 unterstützt.

Hinweis: Die Formate der DHCPv6-Option 16 und der Option 17 sind in RFC 3315 vollständig definiert.

Vorbereiten des iSCSI-Boot-Image

Einrichten von iSCSI-Boot für Windows Server 2008 R2 und SP2

Windows Server 2008 R2 und Windows Server 2008 SP2 unterstützen iSCSI-Booting. Das folgende Verfahren bezieht sich auf Windows Server 2008 R2, gilt aber auch für Windows Server 2008 SP2.

Erforderliches CD/ISO-Image:

- Windows Server 2008 R2 x64 mit eingefügten Broadcom-Treibern. Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel KB974072 unter support.microsoft.com.

Hinweis: Weitere Informationen zur Extraktion der einzelnen Windows NetXtreme-Treiber finden Sie in der Datei *silent.txt* für das spezifische Treiberinstallationsprogramm.

Sonstige erforderliche Software:

- Bindview.exe (nur Windows Server 2008 R2; siehe KB976042)

Verfahren:

1. Entfernen Sie alle lokalen Festplatten auf dem zu bootenden System (dem "Remote-System").
2. Laden Sie die aktuellsten Broadcom MBA- und iSCSI-Boot-Images auf den NVRAM des Adapters.
3. Konfigurieren Sie BIOS auf dem Remote-System so, dass das Broadcom MBA das erste bootfähige Gerät und das DVD-ROM-Laufwerk das zweite bootfähige Gerät ist.
4. Konfigurieren Sie das iSCSI-Ziel, um eine Verbindung vom Remote-Gerät zuzulassen. Vergewissern Sie sich, dass das Ziel über ausreichend Speicherplatz für die neue Betriebssysteminstallation verfügt.
5. Booten Sie das Remote-System. Wenn das Preboot Execution Environment (PXE)-Banner angezeigt wird, drücken Sie **Strg + S**, um das PXE-Menü aufzurufen.
6. Legen Sie im PXE-Menü für **Boot-Protokoll iSCSI** fest.
7. Geben Sie die Parameter für das iSCSI-Ziel ein.
8. Setzen Sie in den allgemeinen Parametern den Parameter **Booten von Ziel** auf **Einmalige Deaktivierung.**
9. Speichern Sie die Einstellungen, und starten Sie das System neu.

   Das Remote-System sollte eine Verbindung zum iSCSI-Ziel herstellen und dann vom DVDROM-Gerät booten.
10. Booten Sie von der DVD, und starten Sie die Installation.
11. Beantworten Sie alle Installationsfragen entsprechend (geben Sie das zu installierende Betriebssystem an, akzeptieren Sie die Lizenzbedingungen usw.).

    Wenn das Fenster **Wo möchten Sie Windows installieren?** angezeigt wird, sollte das Ziellaufwerk sichtbar sein. Dies ist ein Laufwerk, das über das iSCSI-Boot-Protokoll angeschlossen ist und sich im externen iSCSI-Ziel befindet.
12. Wählen Sie **Weiter** aus, um mit der Windows Server 2008 R2-Installation fortzufahren.

    Nach einigen Minuten wird der Installationsvorgang von der Windows Server 2008 R2-DVD gestartet, und anschließend wird das System neu gestartet. Nach dem Neustart sollte die Windows Server 2008 R2-Installation fortgesetzt und die Installation abgeschlossen werden.
13. Überprüfen Sie nach einem erneuten Systemneustart, ob das Remote-System vom Desktop gebootet werden kann.

14. Laden Sie nach dem Booten von Windows Server 2008 R2 den Treiber, und führen Sie die Datei "Bindview.exe" aus.
    a. Wählen Sie **Alle Dienste** aus.
    b. Unter **WFP Lightweight-Filter** sollten für die AUT **Bindungspfade** angezeigt werden. Klicken Sie mit der rechten Maustaste darauf, und deaktivieren Sie sie. Wenn Sie fertig sind, schließen Sie die Anwendung.
15. Stellen Sie sicher, dass das Betriebssystem und das System funktionsfähig sind und Daten übertragen können, indem Sie die IP eines externen Systems anpingen usw.

Einrichten von iSCSI-Boot für Windows Server 2012

Windows Server 2012 unterstützt iSCSI-Booting und -Installationen. Broadcom erfordert die Verwendung einer "Slipstream"-DVD mit den neuesten Broadcom-Treibern. Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel KB974072 unter support.microsoft.com.

Hinweis: Das Verfahren von Microsoft fügt nur die NDIS-Treiber hinzu. Broadcom empfiehlt, dass alle Treiber (VBD, BXND, OIS und NetXtreme I NDIS) hinzugefügt werden.

Das folgende Verfahren bereitet das Image auf die Installation und das Booten vor:

1. Entfernen Sie alle lokalen Festplatten auf dem zu bootenden System (dem "Remote-System").
2. Laden Sie die aktuellsten Broadcom MBA- und iSCSI-Boot-Images auf den NVRAM des Adapters.
3. Konfigurieren Sie BIOS auf dem Remote-System so, dass das Broadcom MBA das erste bootfähige Gerät und das DVD-ROM-Laufwerk das zweite bootfähige Gerät ist.
4. Konfigurieren Sie das iSCSI-Ziel, um eine Verbindung vom Remote-Gerät zuzulassen. Vergewissern Sie sich, dass das Ziel über ausreichend Speicherplatz für die neue Betriebssysteminstallation verfügt.
5. Booten Sie das Remote-System. Wenn das Preboot Execution Environment (PXE)-Banner angezeigt wird, drücken Sie **Strg + S**, um das PXE-Menü aufzurufen.
6. Legen Sie im PXE-Menü für **Boot-Protokoll iSCSI** fest.
7. Geben Sie die Parameter für das iSCSI-Ziel ein.
8. Setzen Sie in den allgemeinen Parametern den Parameter **Booten von Ziel** auf **Einmalige Deaktivierung**.
9. Speichern Sie die Einstellungen, und starten Sie das System neu.

   Das Remote-System sollte eine Verbindung zum iSCSI-Ziel herstellen und dann vom DVDROM-Gerät booten.
10. Booten Sie von der DVD, und starten Sie die Installation.
11. Beantworten Sie alle Installationsfragen entsprechend (geben Sie das zu installierende Betriebssystem an, akzeptieren Sie die Lizenzbedingungen usw.).

    Wenn das Fenster **Wo möchten Sie Windows installieren?** angezeigt wird, sollte das Ziellaufwerk sichtbar sein. Dies ist ein Laufwerk, das über das iSCSI-Boot-Protokoll angeschlossen ist und sich im externen iSCSI-Ziel befindet.
12. Wählen Sie **Weiter** aus, um mit der Windows 2012-Installation fortzufahren.

    Nach einigen Minuten wird der Installationsvorgang von der Windows 2012-DVD gestartet, und anschließend wird das System neu gestartet. Nach dem Neustart sollte die Windows 2012-Installation fortgesetzt und dann abgeschlossen werden.
13. Überprüfen Sie nach einem erneuten Systemneustart, ob das Remote-System vom Desktop gebootet werden kann.
14. Nachdem Windows 2012 das Betriebssystem gebootet hat, empfiehlt Broadcom, das Treiberinstallationsprogramm auszuführen, um die Installation von Broadcom-Treibern und -Anwendungen abzuschließen.

Einrichten von iSCSI-Boot für Linux

iSCSI-Boot für Linux wird von Red Hat Enterprise Linux 5.5 und höher sowie von SUSE Linux Enterprise Server 11 SP1 und höher unterstützt. Beachten Sie, dass SLES 10.x und SLES 11 nur den Non-Offload-Pfad unterstützen.

1. Um den Treiber zu aktualisieren, besorgen Sie die aktuelle Broadcom Linux-Treiber-CD.
2. Konfigurieren Sie die iSCSI-Boot-Parameter für die direkte Installation in das Zielsystem von DVD, indem Sie die Option zum Booten vom Zielsystem auf dem Netzwerkadapter deaktivieren.
3. Ändern Sie die Boot-Reihenfolge wie folgt:
   a. Booten vom Netzwerkadapter.
   b. Booten vom CD-/DVD-Treiber.
4. Starten Sie das System neu.
5. Das System stellt eine Verbindung zum iSCSI-Ziel her und bootet anschließend vom CD-/DVD-Laufwerk.
6. Befolgen Sie die entsprechenden Anweisungen für Ihr Betriebssystem.
   a. RHEL 5.5: Geben Sie bei der Aufforderung "boot:" den Befehl "linux dd" ein, und drücken Sie die Eingabetaste.
   b. SuSE 11.x: Wählen Sie **Installation** und geben Sie als Boot-Option **withiscsi=1 netsetup=1** ein. Wenn ein Treiber-Update erwünscht ist, wählen Sie für die F6-Treiberoption **JA** aus.
7. Wenn ein Treiber-Update gewünscht ist, befolgen Sie die Anweisungen zum Einlegen der Treiber-CD. Andernfalls überspringen Sie diesen Schritt.
8. Wählen Sie bei der Aufforderung "networking device" den gewünschten Netzwerkadapterport aus, und drücken Sie **OK**.
9. Konfigurieren Sie bei Anzeige von "configure TCP/IP" die Art der IP-Adresszuweisung des Systems, und drücken Sie **OK**.
10. Wenn Sie eine statische IP auswählen, müssen Sie IP-Informationen für den iscsi-Initiator eingeben.
11. (RHEL) Überspringen Sie den Medientest.
12. Setzen Sie die Installation wie gewünscht fort. Zu diesem Zeitpunkt steht ein Laufwerk zur Verfügung. Entnehmen Sie nach Abschluss des Kopiervorgangs die CD/DVD, und starten Sie das System neu.
13. Aktivieren Sie beim Systemneustart die Option zum Booten vom Zielsystem in den iSCSI-Boot-Parametern, und schließen Sie die Installation ab.

Zu diesem Zeitpunkt ist die Erstinstallationsphase abgeschlossen. Der restliche Vorgang bezieht sich auf die Erstellung eines neuen benutzerdefinierten initrd-Image für jedes neue Komponenten-Update:

14. Aktualisieren Sie gegebenenfalls den iscsi-Initiator. Sie müssen zunächst den vorhandenen Initiator mit **rpm -e** entfernen.
15. Stellen Sie sicher, dass alle Ausführungsebenen des Netzwerkdiensts aktiviert sind:
    `chkconfig network on`
16. Stellen Sie sicher, dass Ausführungsebenen 2, 3 und 5 des iscsi-Diensts aktiviert sind.
    `chkconfig -level 235 iscsi on`
17. Stellen Sie bei Red Hat 6.0 sicher, dass der Network Manager-Dienst beendet und deaktiviert ist.
18. Installieren Sie ggf. iscsiuio (für SuSE 10 nicht erforderlich).
19. Installieren Sie ggf. das linux-nx2-Paket.
20. Installieren Sie das Paket bibt.
21. Entfernen Sie ifcfg-eth*.
22. Führen Sie einen Neustart durch.
23. Befolgen Sie bei SUSE 11.1 den unten gezeigten Workaround für die dezentrale DVD-Installation.

24. Melden Sie sich nach dem Systemneustart an, ändern Sie den Ordner in /opt/bcm/bibt, und führen Sie das Skript iscsi_setup.sh zum Erstellen des initrd-Image aus.
25. Kopieren Sie das initrd-Image in das /boot-Verzeichnis.
26. Ändern Sie das grub-Menü so, dass auf das neue initrd-Image gezeigt wird.
27. Zum Aktivieren von CHAP ist eine Änderung von iscsid.conf erforderlich (nur Red Hat).
28. Führen Sie einen Neustart durch, und ändern Sie gegebenenfalls die CHAP-Parameter.
29. Setzen Sie das Booten in das iSCSI-Boot-Image fort, und wählen Sie eines der erstellten Images aus. Sie sollten dabei Ihre Auswahl im Abschnitt zu den iSCSI-Boot-Parametern berücksichtigen. Wenn HBA Boot-Modus in den iSCSI-Boot-Parametern aktiviert wurde, müssen Sie das Offload-Image booten. Bei SLES 10.x und SLES 11 wird kein Offload unterstützt.
30. Für IPv6 können Sie nun in der NVRAM-Konfiguriation die gewünschte IPv6-Adresse sowohl für den Initiator aus auch für das Ziel festlegen.

Booten

Nachdem das System für ein iSCSI-Booten vorbereitet wurde und sich das Betriebssystem auf dem iSCSI-Ziel befindet, wird in einem letzten Schritt der tatsächliche Bootvorgang ausgeführt. Das System bootet Windows oder Linux über das Netzwerk und verhält sich so, als würde sich das Betriebssystem auf der lokalen Festplatte befinden.

1. Booten Sie den Server neu.
2. Drücken Sie **STRG+S**.
3. Wählen Sie im **Hauptmenü** die Option **Allgemeine Parameter** aus, und setzen Sie die Option **Booten von iSCSI-Ziel** auf **Aktiviert**.

Wenn eine CHAP-Authentifizierung erforderlich ist, aktivieren Sie die CHAP-Authentifizierung, nachdem Sie festgestellt haben, dass der Bootvorgang ordnungsgemäß erfolgt (siehe Aktivieren der CHAP-Authentifizierung).

Weitere Hinweise zu iSCSI-Boot

Bei der Konfiguration eines Systems für iSCSI-Booten sind einige zusätzliche Faktoren zu beachten.

Ändern der Einstellungen für Übertragungsrate und Duplex in Windows-Umgebungen

Das Booten über den NDIS-Pfad wird unterstützt. Die Einstellungen für Übertragungsrate und Duplex können mithilfe des Dienstprogramms BACS für den iSCSI-Boot über die NDIS-Pfade geändert werden.

Lokal verwaltete Adresse

Für iSCSI-bootfähige Geräte wird eine auf der BACS-Konfigurationsregisterkarte im Bereich Erweitert anhand der Eigenschaft Lokal verwaltete Adresse zugewiesene benutzerdefinierte MAC-Adresse nicht unterstützt.

Virtuelle LANs

VLAN-Markierung (virtuelles LAN) wird für iSCSI-Boot mit dem Microsoft iSCSI Software Initiator nicht unterstützt.

Fehlerbehebung bei iSCSI-Boot

Im Folgenden finden Sie einige nützliche Tipps für die Problembehandlung bei iSCSI-Boot.

Problem: Das iSCSI-Absturzspeicherabbild-Dienstprogramm von Broadcom kann ein Speicherabbild nicht richtig erfassen, wenn die Verbindungsgeschwindigkeit für iSCSI-Boot auf 10 Mbit/s oder 100 Mbit/s festgelegt ist.
Lösung: Das iSCSI-Absturzspeicherabbild-Dienstprogramm wird unterstützt, wenn die Verbindungsgeschwindigkeit für iSCSI-Boot auf 1 Gbit/s festgelegt ist. 10 Mbit/s oder 100 Mbit/s werden nicht unterstützt.

Problem: Das iSCSI-Absturzspeicherabbild-Dienstprogramm von Broadcom kann ein Speicherabbild nicht richtig erfassen, wenn die Verbindungsgeschwindigkeit für iSCSI-Boot auf 10 Mbit/s oder 100 Mbit/s festgelegt ist.
Lösung: Das iSCSI-Absturzspeicherabbild-Dienstprogramm wird unterstützt, wenn die Verbindungsgeschwindigkeit für iSCSI-Boot auf 1 Gbit/s oder 10 Gbit/s festgelegt ist. 10 Mbit/s oder 100 Mbit/s werden nicht unterstützt.

Problem: Ein iSCSI-Ziel wird nicht als Installationsziel erkannt, wenn Windows Server 2008 über eine IPv6-Verbindung installiert wird.
Lösung: Dies ist ein bekanntes Problem, das durch ein Drittanbieterprodukt verursacht wird. Weitere Informationen finden Sie in der Microsoft Knowledge Base KB 971443 unter http://support.microsoft.com/kb/971443.

Problem: Das iSCSI-Konfigurationsprogramm kann nicht gestartet werden.
Lösung: Stellen Sie sicher, dass die iSCSI-Boot-Firmware im NVRAM installiert ist.

Problem: Nachdem die iSCSI-Boot-LUN auf den Wert 255 festgelegt wurde, kommt es bei der Ausführung von iSCSI-Boot zu einem Systemabsturz.
Lösung: Zwar unterstützt die iSCSI-Lösung von Broadcom einen LUN-Bereich von 0 bis 255; dies ist jedoch beim Microsoft iSCSI Software Initiator nicht der Fall. Legen Sie für die LUN einen Wert zwischen 0 und 254 fest.

Problem: Posteingangstreiber kann nicht aktualisiert werden, wenn eine Hardware-ID ohne Posteingang vorhanden ist.
Lösung: Erstellen Sie ein eigenes Slipstream-DVD-Image mit unterstützten Treibern, die auf den Installationsmedien vorhanden sind.

iSCSI-Absturzspeicherabbild

Wenn Sie das Broadcom-Dienstprogramm für das iSCSI-Absturzspeicherabbild verwenden, ist es wichtig, dass Sie sich bei der Installation des iSCSI-Absturzspeicherabbild-Treibers genau an die Installationsanleitung halten. Weitere Informationen finden Sie unter Verwenden des Installationsprogramms.

Abschnitt 10: Installation von Treibern und Management-Anwendung unter Linux

Verfügbare Pakete

Der Linux TG3-Treiber ist in den folgenden Paketformaten (Dateinamen) verfügbar:

- Quell-RPM (tg3-*Version*.3dkms.src.rpm)
- Quell-RPM (tg3-*Version*.3dkms.noarch.rpm)
- Ergänzend (tg3_sup-*Version*.tar.gz)
- Komprimiertes TAR-Format (tg3-*Version*.tar.gz)

Sowohl das RPM- als auch das TAR-Quellpaket enthalten identische Quelldateien zum Erstellen des Treibers. Die TAR-Datei enthält zusätzliche Elemente wie Patches und Datenträger-Images mit Treibern für die Netzwerkinstallation.

Installieren der TG3-Treibersoftware

Installieren des Quell-RPM-Pakets

Voraussetzungen:

- Linux-Kernel-Quelle
- C-Compiler

Verfahren:

1. Installieren Sie das RPM-Paket.
   `rpm -ivh tg3-version.src.rpm`
2. Wechseln Sie zum Verzeichnis des RPM-Pfads, und erstellen Sie den Binärtreiber für Ihren Kernel (der RPM-Pfad ist von der jeweiligen Linux-Distribution abhängig).
   ```
   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)
   ```

   Hinweis: Beim Installieren eines Quell-RPM-Pakets wird unter Umständen die folgende Meldung angezeigt:

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

   Die Ursache des Fehlers ist wahrscheinlich, dass das rpm-build-Paket nicht installiert wurde. Öffnen Sie das rpm-build-Paket vom Linux-Installationsdatenträger, und installieren Sie es unter Verwendung folgenden Befehls:

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

   Schließen Sie die Installation des Quell-RPM-Pakets ab.
3. Installieren Sie das neu erstellte Paket (Treiber und Man-Page).
   `rpm -ivh RPMS/i386/tg3-version.i386.rpm`

   Der Treiber wird je nach Kernel unter dem folgenden Pfad installiert:

   2.6.x-Kernel:

   /lib/modules/*Kernel_Version*/kernel/drivers/net/tg3.ko
4. Laden Sie den Treiber.
   `modprobe tg3`

Weitere Informationen zur Konfiguration des Netzwerkprotokolls sowie der Netzwerkadresse finden Sie in der Dokumentation der jeweiligen Linux-Version.

Erstellen des Treibers aus der Quell-TAR-Datei

1. Erstellen Sie ein Verzeichnis (tg3-*Version*), und extrahieren Sie die TAR-Dateien in dieses Verzeichnis.
   `tar xvzf tg3-version.tgz`
2. Erstellen Sie den Treiber **tg3.o** als ladbares Modul für den ausgeführten Kernel.
   ```
   CD tg3-version
   make clean
   make; make install
   ```
3. Testen Sie den Treiber, indem Sie ihn laden.
   ```
   rmmod tg3
   modprobe tg3
   ```
   Bei korrekter Ausführung dieses Befehls wird keine Meldung angezeigt.

Hinweis: Entnehmen Sie die Angaben zum Speicherort des installierten Treibers den oben aufgeführten RPM-Anweisungen.

4. Schlagen Sie die Anleitungen zum Konfigurieren des Netzwerkprotokolls sowie der Netzwerkadresse im Handbuch zu Ihrem Betriebssystem nach.

Netzwerkinstallationen

Für die Installation über NFS, FTP oder HTTP (über eine Netzwerk-Boot-Disk oder PXE), verwenden Sie den tg3-Treiber, der Teil des Betriebssystems Linux ist.

Schließen/Entfernen des TG3-Treibers

Schließen/Entfernen des Treibers aus einer RPM-Installation

Verwenden Sie **ifconfig**, um alle durch den Treiber geöffneten *ethX*-Schnittstellen zu schließen, und führen Sie dann den folgenden Befehl aus:

```
rmmod tg3
```

Wenn der Treiber mit **rpm** installiert wurde, entfernen Sie ihn anhand des folgenden Befehls:

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

Entfernen des Treibers aus einer TAR-Installation

Wenn der Treiber unter Verwendung von make install aus der TAR-Datei installiert wurde, muss die Treiberdatei tg3.o manuell aus dem Betriebssystem gelöscht werden. Unter Installieren des Quell-RPM-Pakets finden Sie Informationen zum Speicherort des installierten Treibers.

Wenn eine Schnittstellenkonfiguration vorhanden ist, die mit dem TG3-Treiber verwandt ist, schließen Sie zunächst die Schnittstelle, indem Sie **ifconfig ethx down** und anschließend **rmod tg3** verwenden.

Treibermeldungen

Die nachfolgende Auflistung zeigt die gängigsten Beispielmeldungen, die in der Datei */var/log/messages* protokolliert werden können. Verwenden Sie **dmesg -n *Ebene***, um die Ebene zu steuern, auf der Meldungen an der Konsole angezeigt werden. Die meisten Systeme sind standardmäßig auf die Ebene 6 eingestellt.

Treiberanmeldung

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

Netzwerkkarte gefunden

```
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
```

Flow Control (Flusskontrolle):

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

Übertragungsrate und aktive Verbindung

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

Nicht aktive Verbindung

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

Teaming-Funktion mit Channel Bonding

Mit dem TG3-Treiber können Sie Adapter in einem Team gruppieren, indem Sie Bonding-Kernel-Module und eine Channel Bonding-Schnittstelle verwenden. Weitere Informationen über die Installation unter Linux Channel Bonding finden Sie in der Linux-Dokumentation.

Installation der Linux-Management-Anwendung

Überblick

Die Broadcom Advanced Control Suite Version 4 (BACS4) ist eine Management-Anwendung zum Konfigurieren von NetXtreme I-Adaptern. Die BACS4-Software funktioniert unter Server- und Clientbetriebssystemen von Windows und Linux.

Dieses Kapitel beschreibt, wie Sie die BACS4-Management-Anwendung auf Linux-Systemen installieren. Für Windows-Systeme wird ein Installationsprogramm mitgeliefert, das die Windows-Treiber und die Management-Anwendungen installiert, einschließlich BACS4 (siehe Installation von Treibern und Management-Anwendung unter Windows für Anweisungen).

Es gibt zwei Hauptkomponenten des BACS4-Dienstprogramms: die Provider-Komponente und die Clientsoftware. Der Provider wird auf einem Server oder "Managed Host" installiert, der ein oder mehrere CNAs enthält. Der Provider sammelt Informationen über die CNAs und stellt sie für den Abruf von einem Management-PC bereit, auf dem die Clientsoftware installiert ist. Die Clientsoftware ermöglicht die Anzeige von Informationen der Provider und Konfiguration der CNAs. Die BACS-Clientsoftware enthält und eine Befehlszeilenoberfläche (CLI).

Kommunikationsprotokolle

Ein Kommunikationsprotokoll ermöglicht den Informationsaustausch zwischen dem Provider und der Clientsoftware. Dies sind eigene Implementierungen oder Open-Source-Implementierungen der Standards Web-Based Enterprise Management (WBEM) und Common Information Model (CIM) von der Distributed Management Task Force (DMTF). Netzwerkadministratoren können abhängig von dem vorherrschenden Standard bei ihrem Netzwerk die beste Möglichkeit wählen.

Die folgende Tabelle zeigt die verfügbaren Optionen basierend auf den Betriebssystemen an, die auf dem Managed Host und dem Client installiert sind.

Wenn der Client dieses Betriebssystem verwendet:	*Und der Managed Host dieses Betriebssystem verwendet:*	*Dann kann BACS diese Kommunikationsprotokolle verwenden:*
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)

Wenn der Client dieses Betriebssystem verwendet:	*Und der Managed Host dieses Betriebssystem verwendet:*	*Dann kann BACS diese Kommunikationsprotokolle verwenden:*

- WMI = Windows Management Instrumentation.
- WS-MAN = Web Service-Management. WinRM ist eine auf Windows basierende Implementierung, und OpenPegasus ist eine Open-Source-Implementierung, die unter Linux funktioniert.
- CIM-XML = Eine auf XML basierende Version von OpenPegasus.

Wenn zu Ihrem Netzwerk eine Mischung aus Windows- und Linux-Clients gehört, die auf Windows- und Linux-Server zugreifen, ist WS-MAN eine geeignete Wahl. Wenn Linux das einzige auf den Servern installierte Betriebssystem ist, ist CIM-XML eine Möglichkeit. Wenn zu Ihrem Netzwerk nur Windows-Server und -Clients gehören, ist WMI eine Möglichkeit. WMI ist sehr einfach zu konfigurieren, wird aber nur unter Windows unterstützt. (Siehe Installation von Treibern und Management-Anwendung unter Windows für Anweisungen zum Installieren und Konfigurieren von Windows-Protokollen)

Bei der BACS-Installation werden auch die Provider-Komponente auf dem Managed Host und die Clientsoftware auf der Verwaltungsstation installiert. Der Installationsvorgang unterscheidet sich je nach den Betriebssystemen, die auf dem Client und dem Managed Host installiert sind, und den ausgewählten Kommunikationsprotokollen.

Installieren von WS-MAN oder CIM-XML auf einem Linux-Server

Schritt 1: Installieren von OpenPegasus

Unter Red Hat Linux stehen zwei Installationsoptionen zur Verfügung:

- Vom internen RPM (Nur Red Hat)
- Von der Source (Red Hat und SUSE)

Unter SUSE Linux Enterprise Server 11 (SLES11) müssen Sie das Quell-RPM verwenden.

Hinweis: Das interne RPM unterstützt nicht das WS-MAN-Kommunikationsprotokoll. Um WS-MAN zu verwenden, müssen Sie OpenPegasus von der Source installieren.

Vom internen RPM (Nur Red Hat)

Bei Red Hat Linux steht ein internes OpenPegasus RPM als `tog-pegasus-<version>.<arch>.rpm` zur Verfügung.

1. Verwenden Sie den folgenden Befehl, um tog-pegasus zu installieren:
   `rpm -ivh tog-openpegasus-<version>.<arch>.rpm`
2. Verwenden Sie den folgenden Befehl, um Pegasus zu starten:
   `/etc/init.d/tog-pegasus start`

Hinweis: Bei SUSE Linux ist das interne OpenPegasus RPM nicht verfügbar. OpenPegasus muss wie folgt beschrieben von der Source installiert werden.

Beachten Sie, dass im internen Pegasus HTTP nicht standardmäßig aktiviert ist. Nachdem das interne OpenPegasus erfolgreich installiert wurde und keine weitere Konfiguration erforderlich ist, befolgen Sie die Anweisungen in Schritt 4: Installieren des Broadcom-CMPI-Providers. Um HTTP zu aktivieren, siehe Aktivieren von HTTP.

Von der Source (Red Hat und SUSE)

Die OpenPegasus-Source kann unter www.openpegasus.org heruntergeladen werden.

Hinweis: Falls nicht bereits installiert, laden Sie die Dateien openssl- und libopenssl-devel-rpm herunter, und installieren Sie diese. Dieser Schritt ist optional und nur nötig, wenn Sie HTTPS zur Verbindung zwischen dem Client und dem Managed Host verwenden möchten.

Einrichten der Umgebungsvariablen

Richten Sie die Umgebungsvariablen zur Erstellung von OpenPegasus wie folgt ein.

Umgebungsvariable	*Beschreibung*
PEGASUS_ROOT	Der Speicherort des Pegasus-Verzeichnisbaums
PEGASUS_HOME	Der Speicherort des Programms, das Repository; z. B. Unterordner $PEGASUS_HOME/bin, PEGASUS_HOME/lib, $PEGAUS_HOME/repository und $PEGASUS_HOME/mof.
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Für 32-Bit-Linux-Systeme: "LINUX_IX86_GNU" Für 64-Bit-Linux-Systeme: "LINUX_X86_64_GNU"
PEGASUS_HAS_SSL	Optional. Für HTTPS-Support auf "true" setzen.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Optional. Für WSMAN-Protokollsupport auf "true" setzen.

Zusätzliche Einstellungen

Die Variable $PEGASUS_HOME muss in der Shell-Umgebung eingerichtet werden, und $PEGASUS_HOME/bin muss an die $PATH-Umgebung angehängt sein.

Beispiele

- 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

Fügen Sie für SSL-Support die folgende Umgebungsvariable hinzu:

- export PEGASUS_HAS_SSL=true

Fügen Sie für WS-MAN-Support die folgende Umgebungsvariable hinzu:

- export PEGASUS_ENABLE_PROTOCOL_WSMAN=true

CIM-XML und WSMAN verwenden in OpenPegasus dieselben Ports für HTTP oder HTTPS. Die Standardportnummern für HTTP und HTTPS sind jeweils 5989 und 5989.

Hinweis: Sie können diese Exporte am Ende der Datei .bash_profile hinzufügen. Diese Datei befindet sich im / root-Verzeichnis.

- Die Umgebungsvariablen werden eingerichtet, wenn sich ein Benutzer über PuTTY anmeldet.
- Führen Sie beim Linux-System bei jedem Terminal, für das die Umgebungsvariablen nicht eingerichtet werden, den folgenden Befehl aus:
  `source /root/.bash_profile`
- Wenn Sie sich ab- und wieder anmelden, werden die Umgebungsvariablen eingerichtet.

Erstellen und Installieren von OpenPegasus

Führen Sie unter $PEGASUS_ROOT (dem Speicherort des Pegasus-Quellstammverzeichnisses) die folgenden Befehle aus:

```
make clean
make
make repository
```

Hinweis: Immer wenn OpenPegasus von der Source installiert wird, werden alle Konfigurationen auf die Standardwerte zurückgesetzt. Wenn Sie OpenPegasus erneut installieren, müssen Sie die Konfigurationen neu einrichten, wie in Schritt 3: Konfigurieren von OpenPegasus auf dem Server beschrieben.

Schritt 2: Starten von CIM Server auf dem Server

Verwenden Sie den Befehl `cimserver`, um CIM-Server zu starten. Um CIM-Server zu beenden, verwenden Sie den Befehl `cimserver -s`.

Um zu überprüfen, ob OpenPegasus ordnungsgemäß installiert wurde, geben Sie den folgenden Befehl ein:

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

Hinweis: Damit OpenPegasus von der Quelle kompiliert wird, muss PEGASUS_HOME beim Start von CIM-Server definiert werden. Sonst kann CIM-Server das Repository nicht richtig laden. Sie können PEGASUS_HOME in der Datei ".bash_profile" einrichten.

Schritt 3: Konfigurieren von OpenPegasus auf dem Server

Verwenden Sie den Befehl `cimconfig`, um OpenPegasus zu konfigurieren, wie in der folgenden Tabelle angegeben:

Befehl	*Beschreibung*
`cimconfig -l`	Auflisten aller gültigen Eigenschaftsnamen.
`cimconfig -l -c`	Auflisten aller gültigen Eigenschaftsnamen und deren Werten.
`cimconfig -g <property name>`	Abfragen einer bestimmten Eigenschaft.
`cimconfig -s <property name>=<value> -p`	Einrichten einer bestimmten Eigenschaft.
`cimconfig --help`	Weitere Informationen über den Befehl.

CIM-Server muss vor dem Ausführen von `cimconfig` gestartet und zum Übernehmen der Konfigurationsänderungen neu gestartet werden.

Aktivieren der Authentifizierung

Die folgenden OpenPegasus-Eigenschaften müssen wie in diesem Abschnitt beschrieben eingerichtet werden. Sonst funktioniert der Broadcom CIM-Provider nicht ordnungsgemäß. Stellen Sie sicher, dass folgende Werte eingerichtet sind, bevor Sie BACS starten und eine Verbindung zum Provider herstellen.

Starten Sie CIM-Server, falls nicht bereits geschehen. Richten Sie anschließend folgende Werte ein:

- `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`

Wenn Sie möchten, dass für Root-Benutzer eine Remote-Verbindung möglich ist:

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

Benutzerkonfiguration mit Berechtigung: Für die OpenPegasus-Authentifizierung werden Linux-Systembenutzer verwendet. Die Systembenutzer müssen mit `cimuser` zu OpenPegasus hinzugefügt werden, damit eine Verbindung über BACS hergestellt werden kann:

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

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

Aktivieren von HTTP

1. Wenn CIM-Server noch nicht gestartet wurde, führen Sie den Start jetzt durch.
2. Verwenden Sie den folgenden Befehl, um einen HTTP-Port einzurichten (optional):
   `cimconfig -s httpPort=5988 -p`

   Diese Eigenschaft ist nicht für das interne OpenPegasus verfügbar.
3. Verwenden Sie den folgenden Befehl, um eine HTTP-Verbindung zu aktivieren:
   `cimconfig -s enableHttpConnection=true -p`
4. Verwenden Sie die Befehle `cimserver -s` und `cimserver`, um CIM-Server zu beenden und neu zu starten, damit die neue Konfiguration übernommen wird.

Aktivieren von HTTPS

1. Wenn CIM-Server noch nicht gestartet wurde, führen Sie den Start jetzt durch.
2. Verwenden Sie den folgenden Befehl, um einen HTTPS-Port einzurichten (optional):
   `cimconfig -s httpsPort=5989 -p`

Diese Eigenschaft ist nicht für das interne OpenPegasus verfügbar.

3. Verwenden Sie den folgenden Befehl, um eine HTTPS-Verbindung zu aktivieren:
   `cimconfig -s enableHttpsConnection=true -p`
4. Verwenden Sie die Befehle `cimserver -s` und `cimserver`, um CIM-Server zu beenden und neu zu starten, damit die neue Konfiguration übernommen wird.

Schritt 4: Installieren des Broadcom-CMPI-Providers

Stellen Sie vor der Installation von CMPI Provider sicher, dass OpenPegasus ordnungsgemäß installiert ist.

Installieren

Geben Sie den folgenden Befehl ein, um Broadcom CMPI Provider zu installieren:

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

Deinstallieren

Geben Sie den folgenden Befehl ein, um Broadcom CMPI Provider zu deinstallieren:

```
% rpm -e BRCM_CMPIProvider
```

Schritt 5: Durchführen der Linux-Firewallkonfiguration, falls erforderlich

Befolgen Sie diese Schritte, um die passenden Ports in der Firewall zu öffnen.

Red Hat

1. Klicken Sie auf **System**, wählen Sie **Administration** aus, und wählen Sie dann **Firewall** aus.
2. Wählen Sie **Andere Ports** aus.
3. Wählen Sie im Dialogfeld "Port und Protokoll" **Benutzerdefiniert** aus.
4. Fügen Sie im Feld **Port/Port-Bereich** die Portnummer hinzu.
5. Fügen Sie im Feld **Protokoll** das Protokoll als TCP oder UDP usw. ein.
6. Klicken Sie auf **Übernehmen**, damit die Firewallregeln übernommen werden.

Beispiel:

- Für CIM-XML über HTTP werden Portnummer 5988 und das Protokoll TCP verwendet.
- Für CIM-XML über HTTPS werden Portnummer 5989 und das Protokoll TCP verwendet.

SUSE

1. Klicken Sie auf **Berechnen** und dann auf **YaST**.
2. Wählen Sie **Sicherheit & Benutzer** im linken Bereich aus.
3. Doppelklicken Sie im rechten Bereich auf **Firewall**.
4. Wählen Sie im linken Bereich **Benutzerdefinierte Regeln** aus.
5. Klicken Sie im rechten Bereich auf **Hinzufügen**.
6. Geben Sie die folgenden Werte ein:
   - **Quellnetzwerk**: 0/0 (alle)
   - **Protokoll**: TCP (oder das passende Protokoll)
   - **Zielport**: <*Portnummer*> oder <*Portnummernbereich*>
   - **Quellport**: leer lassen
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, damit die Firewallregeln übernommen werden.

Beispiel:

Verwenden Sie für CIM-XML die folgenden Werte:

- **Quellnetzwerk**: 0/0 (alle)
- **Protokoll**: TCP
- **Zielport**: 5988:5989
- **Quellport**: leer lassen

Schritt 6: Installieren von BACS und zugehörigen Managementanwendungen

Siehe Installieren der Broadcom Advanced Control Suite-Software.

Installieren von WS-MAN oder CIM-XML auf einem Linux-Client

Es sind auf dem Linux-Client keine speziellen Softwarekomponenten erforderlich, um HTTP zu verwenden. Es muss lediglich die BACS-Management-Anwendung installiert werden. Allerdings können sie bei WS-MAN-Installationen optional das HTTPS-Protokoll für die Verwendung mit BACS konfigurieren.

Konfigurieren von HTTPS auf einem Linux-Client

Befolgen Sie diese Schritte, wenn Sie HTTPS statt HTTP verwenden möchten (nur WS-MAN):

Generieren eines selbstsignierten Zertifikats für Windows-/Linux-Server

OpenSSL für Linux oder Windows kann verwendet werden, um das selbstsignierte Zertifikat wie folgt zu generieren:

Hinweis: Sie können openssl unter http://gnuwin32.sourceforge.net/packages/openssl.htm herunterladen und installieren.

1. Geben Sie den folgenden Befehl ein, um einen privaten Schlüssel zu erstellen:
   `openssl genrsa -des3 -out server.key 1024`
2. Sie werden zur Eingabe einer Passphrase aufgefordert. Merken Sie sich die Passphrase.
3. Führen Sie die folgenden Schritte zum Generieren einer Zertifikatsignieranforderung (CSR) aus.

   Während der Erzeugung der CSR werden Sie nach verschiedenen Informationen gefragt. Wenn Sie aufgefordert werden, den "Allgemeinen Namen" einzugeben, geben Sie den Hostnamen oder die IP-Adresse des Windows-Servers ein.

   Geben Sie den folgenden Befehl ein (Beispielantworten angezeigt):

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

   Wenn dieser Befehl nicht funktioniert, versuchen Sie Folgendes:

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

   Die Datei openssl.cnf sollte im gleichen Verzeichnis wie openssl gespeichert werden. OpenSSL.cnf befindet sich im Ordner C:\Program Files (x86)\GnuWin32\share.

Die folgenden Informationen werden angezeigt:

- Land (zweistelliger Code) []: **US**
- Bundesstaat oder Provinz (vollständiger Name) []: **Kalifornien**
- Standortname (z. B. Stadt) []: **Irvine**
- Name der Organisation (z. B. Firma) []: **Broadcom Corporation**
- Name der Organisationseinheit (z. B. Abteilung) []: **Engineering**
- Allgemeiner Name (z. B. IHR Name) []: Geben Sie den Hostnamen oder die IP-Adresse des Windows-Servers ein. Geben Sie bei IPv6 den allgemeinen Namen im Format [xyxy:xxx:….::xxx] **einschließlich der Klammern [ ]** ein.
- (Optional) E-Mail-Adresse []:

Geben Sie folgende zusätzliche Attribute ein, die mit der Zertifikatanforderung gesendet werden:

- Kennwort in Frage stellen []:**linux1**
- Ein optionaler Name des Unternehmens []:

4. Entfernen Sie die Passphrase aus dem Schlüssel.

Geben Sie die folgenden Befehle ein:

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

5. Generieren eines selbstsignierten Zertifikats:

Um ein selbstsigniertes Zertifikat zu generieren, das für 365 Tage aktiv ist, geben Sie den folgenden Befehl ein:

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

Die folgende Ausgabe wird angezeigt:

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

6. Geben Sie den folgenden Befehl ein, um das generierte selbstsignierte Zertifikat zu überprüfen.
`openssl verify server.crt`

Die folgende Ausgabe wird angezeigt:

```
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
```

Ignorieren Sie die Fehlermeldung "error 18 at 0 depth lookup:self signed certificate". Dieser Fehler weist darauf hin, dass dies ein selbstsigniertes Zertifikat ist.

7. Konvertieren Sie das Zertifikat wie folgt vom "crt"- in das "PKCS12"-Format:

Für einen Windows-Server sollte das Zertifikat im PKCS12-Format vorliegen. Geben Sie den folgenden Befehl ein:

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

Sie erhalten folgende Eingabeaufforderung:

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

Geben Sie das Kennwort ein, und stellen Sie sicher, dass Sie es sich merken. Das Kennwort ist erforderlich, wenn Sie das Zertifikat in den Windows-Server und -Client importieren.

8. Erstellen Sie eine Kopie der Zertifikatdatei "server.crt", und speichern Sie sie auf dem Server, auf dem BACS installiert wird, sodass sie importiert werden kann. Wenn Sie einen Windows- oder Linux-Client verwenden möchten, um eine Verbindung zum Server herzustellen, auf dem BACS ausgeführt wird, muss das Zertifikat ebenfalls an das Clientsystem

übertragen (kopiert und eingefügt) werden.

Unter Linux sollte das Zertifikat die Erweiterung ".pem" besitzen. Die Erweiterung ".crt" und ".pem" sind gleich. Sie müssen also nicht den Befehl `openssl` ausführen, um von .crt zu .pem zu konvertieren. Sie können einfach die Datei kopieren.

Hinweis: Ein separates Zertifikat muss für eine IPv4-Adresse, IPv6-Adresse und einen Hostname generiert werden.

Importieren eines selbstsignierten Zertifikats auf einem Linux-Client

Beachten Sie bei Linux-Distributionen das folgende Zertifikatsverzeichnis:

- Bei allen SUSE-Versionen lautet das Zertifikatsverzeichnis `/etc/ssl/certs`.
- Bei Red Hat kann sich das Zertifikatsverzeichnis je nach Version unterscheiden. Bei einigen Versionen lautet es `/etc/ssl/certs` oder `/etc/pki/tls/certs`. Suchen Sie bei anderen Versionen das Zertifikatsverzeichnis.

Kopieren Sie *hostname.pem*, das Sie in Generieren eines selbstsignierten Zertifikats für Windows-/Linux-Server erstellt haben, in das Zertifikatsverzeichnis des Linux-Clients. Wenn das Zertifikatsverzeichnis z. B. `/etc/ssl/certs` lautet, kopieren Sie *hostname.pem* in `/etc/ssl/certs`.

1. Ändern Sie das Verzeichnis in `/etc/ssl/certs`.
2. Erstellen Sie einen Hashwert, indem Sie den folgenden Befehl ausführen:
   `openssl x509 -noout -hash -in hostname.pem`

   Es wird ein Wert ausgegeben, der z. B. wie folgt aussehen kann:

   `100940db`
3. Erstellen Sie eine symbolische Verknüpfung zum Hash-Wert, indem Sie den folgenden Befehl ausführen:
   `ln -s hostname.pem 100940db.0`

Testen der HTTPS/SSL-Verbindung von einem Linux-Client

Verwenden Sie den folgenden Befehl, um zu testen, ob das Zertifikat korrekt unter Linux installiert wurde:

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

Wenn dies fehlschlägt, wurde das Zertifikat nicht korrekt installiert, und es wird eine Fehlermeldung mit der Aufforderung angezeigt, dass Sie eine Korrekturmaßnahme durchführen sollen.

Installieren der Broadcom Advanced Control Suite-Software

Die Broadcom Advanced Control Suite (BACS)-Software kann auf einem Linux-System mit dem Linux-RPM-Paket installiert werden. Diese Installation enthält eine CLI-Client.

Vor dem Start:

- Vergewissern Sie sich, dass der/die Broadcom-Netzwerkadapter in das System eingesetzt wurde(n) und dass der passende Gerätetreiber für die NIC auf dem System installiert wurde, das von diesem Dienstprogramm verwaltet werden soll.
- Vergewissern Sie sich, dass der CIM-Provider ordnungsgemäß auf dem System installiert wurde, das von diesem Dienstprogramm verwaltet werden soll.

- Vergewissern Sie sich für die Verwaltung von iSCSI auf Linux-Hosts, dass die open-iscsi- und sg-Dienstprogramme auf dem Linux-Host installiert sind.

So installieren Sie BACS

1. Laden Sie das neueste RPM-Paket für die BACS-Management-Anwendung herunter.
2. Installieren Sie das RPM-Paket mit dem folgenden Befehl:
   ```
   % rpm -i BACS-{version}.{arch}.rpm
   ```

Um BACS CLI zu verwenden, lesen Sie die Datei BACSCLI_Readme.txt, die mit den Dateien mitgeliefert wird.

So deinstallieren Sie BACS

Verwenden Sie den folgenden Befehl, um das RPM-Paket zu deinstallieren:

```
% rpm -e BACS
```

Abschnitt 11: VMware-Treibersoftware

Verfügbare Pakete

Der VMware-Treiber ist in den folgenden Paketformaten verfügbar.

Tabelle 19. VMware-Treiberpakete

Merkmal	*Treiber*
VMware-VIB	vmware-esx-drivers-net-tg3-version.x86_64.vib

Treiber

Herunterladen, Installieren und Aktualisieren von Treibern

Informationen zum Herunterladen, Installieren und Aktualisieren des VMware ESX/ESXi-Treibers für NetXtreme I GbE-Netzwerkadapter finden Sie unter http://www.vmware.com/support.

Treiberparameter

NetQueue

Der optionale Parameter **force_netq** kann verwendet werden, um die Anzahl von Rx- und Tx-Warteschlangen festzulegen. Zu den BCM57XX-Geräten, die NetQueue unterstützen, gehören die Geräte BCM5718, BCM5719, BCM5720, BCM5721 und BCM5722.

Standardmäßig versucht der Treiber, die optimale Anzahl an NetQueues zu verwenden. Um die Anzahl der Warteschlangen selbst festzulegen, stellen Sie die Anzahl der NetQueues pro Port mit dem folgenden Befehl ein:

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

Gültige Werte für x sind -1 bis 15:

- 1-15 legt die Anzahl der NetQueues für die jeweilige Netzwerkkarte fest.
- 0 deaktiviert NetQueue.
- -1 gibt an, den Standardtreiber-NetQueue-Wert zu verwenden.

Die Anzahl von "x"-Einträgen kann bis zu 32 betragen, was bedeutet, dass maximal 32 Netzwerkkarten unterstützt werden.

Anwendungsbeispiel:

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

- tg3 NIC 0: Verwenden Sie die Standardanzahl der NetQueues.
- tg3 NIC 1: Deaktivieren Sie den NetQueue-Funktion.
- tg3 NIC 2: Verwenden Sie 1 NetQueue.
- tg3 NIC 3: Verwenden Sie 2 NetQueues.

Beachten Sie, dass die oben angegebene NIC-Zahl nicht der vmnic-Zahl entspricht. Die NIC-Nummer ist die Nummer der System-vmnic-Testreihenfolge. Im Idealfall entspricht die Anzahl der NetQueues der Anzahl der CPUs im Computer.

Treiberparameter

Sie können mehrere optionale Parameter als Befehlszeilenargument für den Befehl vmkload_mod angeben. Diese Parameter können auch über den Befehl esxcfg-module festgelegt werden. Weitere Informationen erhalten Sie auf der Man-Page.

Treiberstandards

Tabelle 20. VMware-Treiberstandards

Parameter	*Standardwert*
Übertragungsrate	Die automatische Aushandlung wird für alle Übertragungsraten angekündigt.
Flow Control (Flusskontrolle):	Die automatische Aushandlung wird für Rx und Tx angekündigt
MTU	1500 (Bereich von 46 bis 9000)
Rx-Ringgröße	200 (Bereich von 0 bis 511). Einige Chips haben eine feste Größe von 64.
Rx-Jumbo-Ringgröße	100 (Bereich von 0 bis 255). Nicht alle Chips unterstützen den großen Ring, und einige Chips, die große Frames unterstützen, verwenden nicht den großen Ring.
Tx-Ringgröße	511 (Bereich von (MAX_SKB_FRAGS+1) bis 511). MAX_SKB_FRAGS ändert sich je nach Kernel und Architektur. Bei einem 2.6-Kernel für x86 liegt MAX_SKB_FRAGS bei 18.
Verknüpfter Empfang Mikrosekunden	20 (Bereich von 0 bis 1023)
Verknüpfter Empfang Mikrosekunden IRQ	20 (Bereich von 0 bis 255)
Verknüpfter Empfang Rahmen	5 (Bereich von 0 bis 1023)
Verknüpfter Empfang Rahmen IRQ	5 (Bereich von 0 bis 255)
Verknüpfte Übertragung Mikrosekunden	72 (Bereich von 0 bis 1023)
Verknüpfte Übertragung usecs IRQ	20 (Bereich von 0 bis 255)
Verknüpfte Übertragung Rahmen	53 (Bereich von 0 bis 1023)

Tabelle 20. VMware-Treiberstandards

Parameter	*Standardwert*
Verknüpfte Übertragung Rahmen IRQ	5 (Bereich von 0 bis 255)
Verknüpfter Status usecs	1000000 (ca. 1 Sek.). Einige verknüpfte Parameter werden nicht verwendet oder besitzen bei einigen Chips andere Standardwerte.
MSI	Aktiviert (falls vom Chip unterstützt und bei Bestehen des Interrupt-Tests).
WoL	Deaktiviert

Treibermeldungen

Die nachfolgende Auflistung zeigt die gängigsten Beispielmeldungen, die in der Datei /var/log/messages protokolliert werden können. Verwenden Sie `dmesg -n <Ebene>`, um die Ebene zu steuern, auf der Meldungen an der Konsole angezeigt werden. Die meisten Systeme sind standardmäßig auf die Ebene 6 eingestellt. Wenn Sie alle Meldungen sehen möchten, setzen Sie die Ebene höher fest.

Treiberanmeldung

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

Netzwerkkarte gefunden

```
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
```

Übertragungsrate und aktive Verbindung

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

Nicht aktive Verbindung

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

Abschnitt 12: Installation von Treibern und Management-Anwendung unter Windows

Installieren der Treibersoftware

Hinweis: Diese Anweisungen basieren auf der Annahme, dass der Broadcom NetXtreme-Adapter nicht werksseitig installiert wurde. Wenn der Controller werksseitig installiert wurde, ist auch die Treibersoftware installiert worden.

Wenn Windows das erste Mal nach der Installation eines Hardware-Geräts (wie beispielsweise eines Broadcom NetXtreme-Adapters) bzw. nach dem Entfernen eines bereits vorhandenen Gerätetreibers gestartet wird, erkennt das Betriebssystem automatisch die Hardware und fordert Sie auf, die Treibersoftware für dieses Gerät zu installieren.

Es stehen ein grafischer, interaktiver Installationsmodus (siehe "Verwenden des Installationsprogramms") sowie ein Befehlszeilenmodus für die Hintergrundinstallation (siehe "Verwenden der Hintergrundinstallation") zur Verfügung.

HINWEISE:

- Prüfen Sie vor dem Installieren der Treibersoftware, dass Ihr Windows-Betriebssystem mit dem neuesten Service Pack auf die aktuelle Version aufgerüstet ist.
- Vor der Verwendung des Broadcom NetXtreme Gigabit Ethernet-Adapters muss auf Ihrem Windows-Betriebssystem ein Netzwerkgerätetreiber installiert werden. Treiber befinden sich auf der Installations-CD.
- Bei Verwendung der Installationsoption "Server Core" für Microsoft Windows Server 2008 R2 wird BACS nicht unterstützt.

Verwenden des Installationsprogramms

Neben den Broadcom-Gerätetreibern installiert das Installationsprogramm auch die Management-Anwendungen. Folgende Anwendungen werden installiert, wenn das Installationsprogramm ausgeführt wird:

- **Broadcom-Gerätetreiber**: Installiert die Broadcom-Gerätetreiber.
- **Control Suite**: Broadcom Advanced Control Suite (BACS).
- **BASP**: Installiert Broadcom Advanced Server Program.
- **SNMP**: Installiert den Simple Network Management Protocol-Subagenten (SNMP-Subagent).
- **CIM Provider**: Installiert den Common Information Model Provider.
- **iSCSI-Absturzspeicherabbild-Treiber**. Installiert den Treiber für das iSCSI-Absturzspeicherabbild-Dienstprogramm.

Hinweis: Die Installation der BACS-Software und der dazugehörigen Management-Anwendungen ist optional, aber die Broadcom-Gerätetreiber müssen bei Verwendung des Installationsprogramms installiert werden.

Hinweis: BASP ist auf Windows Small Business Server (SBS) 2008 nicht verfügbar.

So installieren Sie den Microsoft iSCSI Software Initiator für das iSCSI-Absturzspeicherabbild

Wenn das Broadcom-Dienstprogramm für das iSCSI-Absturzspeicherabbild unterstützt wird und Sie es verwenden möchten, ist es wichtig, dass Sie sich an die Installationsreihenfolge halten:

- Führen Sie das Installationsprogramm aus
- Installieren Sie Microsoft iSCSI Software Initiator zusammen mit dem Patch (MS KB939875)

Hinweis: Wenn Sie über das Installationsprogramm eine Aktualisierung der Gerätetreiber vornehmen, aktivieren Sie **iSCSI-Absturzspeicherabbild** im Abschnitt "Erweitert" der BACS-Registerkarte "Konfiguration" erneut.

Gehen Sie nach dem Ausführen des Installationsprogramms wie folgt vor, um die Gerätetreiber und die Management-Anwendungen zu installieren.

1. Installieren Sie Microsoft iSCSI Software Initiator (Version 2.06 oder höher), wenn dieser nicht bereits in Ihrem Betriebssystem enthalten ist. Informationen dazu, wie Sie herausfinden können, in welchen Fällen Microsoft iSCSI Software Initiator installiert werden muss, finden Sie unter Tabelle 21. Microsoft iSCSI Software Initiator können Sie unter http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986 herunterladen.
2. Installieren Sie den Microsoft-Patch für die Erstellung der iSCSI-Absturzspeicherabbilddatei (Microsoft KB939875) (Download unter http://support.microsoft.com/kb/939875). Informationen dazu, wie Sie herausfinden können, ob Sie den Microsoft-Patch installieren müssen, finden Sie unter Tabelle 21.

Tabelle 21. Windows-Betriebssysteme und iSCSI-Absturzspeicherabbild

Betriebssystem	*MS iSCSI Software Initiator erforderlich*	*Microsoft-Patch (MS KB939875) erforderlich*
NDIS		
Windows Server 2008	Ja (im Betriebssystem enthalten)	Nein
Windows Server 2008 R2	Ja (im Betriebssystem enthalten)	Nein
Windows Server 2012	Ja (im Betriebssystem enthalten)	Nein
OIS		
Windows Server 2008	Nein	Nein
Windows Server 2008 R2	Nein	Nein
Windows Server 2012	Nein	Nein

Verwenden der Hintergrundinstallation

HINWEISE:

- Bei allen Befehlen muss die Groß-/Kleinschreibung beachtet werden.
- Ausführlichere Anleitungen und Informationen zur Hintergrundinstallation finden Sie im Ordner Driver_Management_Apps_Installer in der Datei **Silent.txt**.

Weitere Informationen finden Sie in der Datei "readme.txt" im Installationsordner für Befehlszeilenanweisungen.

Hinweis: Der Switch REINSTALL darf nur verwendet werden, wenn dasselbe Installationsprogramm bereits auf dem System installiert ist. Wenn Sie ein Upgrade auf eine frühere Version des Installationsprogramms durchführen, geben Sie, wie oben angegeben, `setup /s /v/qn` ein.

Ändern der Treibersoftware

So ändern Sie die Treibersoftware:

1. Doppelklicken Sie in der Systemsteuerung auf **Software**.
2. Wählen Sie die **Broadcom-Treiber und Management-Anwendungen** aus, und klicken Sie auf **Ändern**.
3. Klicken Sie auf **Weiter**, um fortzufahren.
4. Klicken Sie auf **Ändern, Hinzufügen oder Entfernen**, um Programmelemente zu ändern. Mit dieser Option werden keine Treiber für neue Adapter installiert. Informationen zum Installieren von Treibern für neue Adapter finden Sie unter Reparieren oder Neuinstallieren der Treibersoftware.
5. Klicken Sie auf **Weiter**, um fortzufahren.
6. Klicken Sie auf ein Symbol, um die Installationsweise für ein Element zu ändern.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Installieren**.
9. Klicken Sie zum Schließen des Assistenten auf **Fertig stellen**.
10. Das Installationsprogramm bestimmt, ob ein Neustart des Systems nötig ist. Befolgen Sie die Anweisungen auf dem Bildschirm.

Reparieren oder Neuinstallieren der Treibersoftware

So reparieren oder installieren Sie die Treibersoftware neu:

1. Doppelklicken Sie in der Systemsteuerung auf **Software**.
2. Wählen Sie die **Broadcom-Treiber und Management-Anwendungen** aus, und klicken Sie auf **Ändern**.
3. Klicken Sie auf **Weiter**, um fortzufahren.
4. Klicken Sie auf **Reparieren oder Neu installieren**, um Fehler zu beheben oder Treiber für neue Adapter zu installieren.
5. Klicken Sie auf **Weiter**, um fortzufahren.
6. Klicken Sie auf **Installieren**.
7. Klicken Sie zum Schließen des Assistenten auf **Fertig stellen**.
8. Das Installationsprogramm bestimmt, ob ein Neustart des Systems nötig ist. Befolgen Sie die Anweisungen auf dem Bildschirm.

Entfernen der Gerätetreiber

Wenn Sie die Gerätetreiber entfernen, werden alle installierten Management-Anwendungen ebenfalls entfernt.

Hinweis: Windows Server 2008 und Windows Server 2008 R2 verfügen über die Rollback-Funktion für Gerätetreiber, um einen Gerätetreiber durch einen bereits installierten Treiber zu ersetzen. Die komplexe Softwarearchitektur des NetXtreme-Geräts stellt jedoch möglicherweise ein Problem dar, wenn die Rollback-Funktion für eins der einzelnen Komponenten verwendet wird. Daher empfehlen wir, dass Änderungen an Treiberversionen nur über ein Treiberinstallationsprogramm vorgenommen werden.

So entfernen Sie Gerätetreiber:

1. Doppelklicken Sie in der Systemsteuerung auf **Software**.
2. Wählen Sie die **Broadcom-Treiber und Management-Anwendungen** aus, und klicken Sie auf **Entfernen**. Befolgen Sie die Anweisungen auf dem Bildschirm.
3. Starten Sie Ihr System neu, um die Treiber vollständig zu entfernen. Wenn Sie das System nicht neu starten, lassen sich die Treiber nicht erfolgreich installieren.

Anzeigen oder Ändern der Adapter-Eigenschaften

So zeigen Sie die Eigenschaften des Broadcom-Netzwerkadapters an bzw. ändern sie:

1. Klicken Sie in der Systemsteuerung auf **Broadcom Control Suite 4**.
2. Klicken Sie in der Registerkarte **Konfigurationen** auf den Bereich Erweitert.

Einstellen der Optionen zur Energieverwaltung

Sie können die Optionen zur Energieverwaltung so einstellen, dass das Betriebssystem den Controller abschalten kann, um Energie zu sparen, bzw. dass der Controller den Computer reaktivieren kann. Wenn das Gerät gerade einen Vorgang (z. B. Abwicklung einer Verbindung) ausführt, schaltet das Betriebssystem das Gerät jedoch nicht ab. Das Betriebssystem versucht nur dann, alle möglichen Geräte herunterzufahren, wenn der Computer in den Ruhezustand wechseln will. Wenn der Controller jederzeit eingeschaltet sein soll, aktivieren Sie nicht das Kontrollkästchen **Computer kann Gerät ausschalten, um Energie zu sparen**.

Hinweis: Auf Blade-Servern stehen Optionen zur Energieverwaltung nicht zur Verfügung.

HINWEISE:

- Die Registerkarte **Energieverwaltung** ist nur bei Servern verfügbar, die Energieverwaltung unterstützen.
- Aktivieren Sie das Kontrollkästchen **Gerät kann den Computer aus dem Standbymodus aktivieren**, um die Funktion "Wake-on LAN" (WOL) im Standby-Modus zu aktivieren.
- Wenn Sie die Option **Nur Verwaltungsstationen können Standbycomputer aktivieren** aktivieren, kann *nur Magic Packet* den Standby-Modus des Computers aufheben.

Vorsicht! Aktivieren Sie für keinen Adapter, der Mitglied eines Teams ist, das Kontrollkästchen **Computer kann Gerät ausschalten, um Energie zu sparen**.

Konfigurieren des Kommunikationsprotokolls zur Verwendung mit BACS4

Es gibt zwei Hauptkomponenten der BACS4-Managementanwendung: die Provider-Komponente und die Clientsoftware. Der Provider wird auf einem Server oder "Managed Host" installiert, der ein oder mehrere CNAs enthält. Der Provider sammelt Informationen über die CNAs und stellt sie für den Abruf von einem Management-PC bereit, auf dem die Clientsoftware installiert ist. Die Clientsoftware ermöglicht die Anzeige von Informationen der Provider und Konfiguration der CNAs. Die BACS-Clientsoftware enthält eine grafische Benutzeroberfläche (GUI) und eine Befehlszeilenoberfläche (CLI).

Ein Kommunikationsprotokoll ermöglicht die Kommunikation zwischen dem Provider und der Clientsoftware. Abhängig von der Mischung an Betriebssystemen (Linux, Windows oder beides) auf den Clients und Managed Hosts in Ihrem Netzwerk können Sie ein passendes Kommunikationsprotokoll auswählen, das verwendet werden soll. Unter "Installation der Linux-Management-Anwendung" finden Sie eine Beschreibung der verfügbaren Kommunikationsprotokolle für jede Netzwerkkonfiguration.

Die Anweisungen in diesem Kapitel betreffen nur das Szenario, in dem Windows Managed Hosts mit Windows-Clients kommunizieren. In diesen Szenarien können Sie entweder das WMI- oder das WS-MAN (WinRM)-Kommunikationsprotokoll verwenden. Wenn Sie das in diesem Kapitel beschriebene Treiberinstallationsprogramm zur Installation sowohl des Treibers als auch der Management-Anwendungen verwenden, wird der Provider für WMI sowie für WS-MAN auf dem verwalteten Host installiert. Darüber hinaus wird das BACS4-Dienstprogramm auf dem Client installiert. Die folgenden Abschnitte bieten zusätzliche Konfigurationsschritte für das ausgewählte Kommunikationsprotokoll.

Bei Linux-Installationen wird der Treiber separat von den Management-Anwendungen installiert. Weitere Informationen zum Thema finden Sie unter .

Verwenden von WS-MAN

Führen Sie die Anweisungen in den folgenden Bereichen aus, um das WS-MAN-Kommunikationsprotokoll zu verwenden:

- WS-MAN Windows Server-Konfiguration
- WS-MAN Windows-Client-Installation

WS-MAN Windows Server-Konfiguration

Schritt 1: Installieren der WinRM-Softwarekomponente auf dem Server

Bei den folgenden Betriebssystemen ist WinRM 2.0 vorinstalliert:

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

Installieren Sie bei Windows Server 2008 das Windows Management Framework-Kernpaket, das WinRM 2.0 und Windows PowerShell 2.0 umfasst, über den folgenden Link:

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

Schritt 2: Grundlegende Konfiguration auf dem Server

Die Windows-Firewall muss aktiviert werden, damit WinRM ordnungsgemäß funktionieren kann. Detaillierte Informationen zur Konfiguration der Firewall finden Sie unter Schritt 7: Zusätzliche Serverkonfiguration. Nachdem die Firewall konfiguriert ist, öffnen Sie eine Befehlszeile, und führen Sie den folgenden Befehl aus, um die Remoteverwaltung auf dem Windows-Server zu aktivieren:

```
winrm quickconfig
```

Sie können den folgenden Befehl verwenden, um die Konfigurationsdaten für den Service anzuzeigen:

```
winrm get winrm/config
```

Schritt 3: Benutzerkonfiguration auf dem Server

Um eine Verbindung mit WinRM herzustellen, muss das Konto ein Mitglied der lokalen Administratorgruppe auf dem lokalen oder Remotecomputer sein. Die Ausgabe des Befehls `get winrm/config` lautet wie folgt:

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

BA steht für BUILTIN\Administrators.

Um eine weitere Benutzergruppe zur Liste der zulässigen Verbindungen in WinRM hinzuzufügen, können Sie die RootSDDL so ändern, dass die neue Benutzergruppe enthalten ist. Sie benötigen die SDDL-ID für die neue Gruppe. Beispielsweise fügt der folgende Befehl die neue Benutzergruppe mit SDDL ID S-1-5-21-1866529496-2433358402-1775838904-1021 hinzu.

```
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)"}
```

Schritt 4: HTTP-Konfiguration auf dem Server

Um die BACS-GUI zu verwenden, müssen Sie das HTTP-Protokoll wie folgt konfigurieren:

Hinweis: Der Standard-HTTP-Port für WinRM 2.0 ist 5985.

1. Klicken Sie auf **Start** (oder drücken Sie die Windows-Taste), und wählen Sie **Ausführen**.
2. Geben Sie **gpedit.msc** ein, um den lokalen Gruppenrichtlinien-Editor zu öffnen.
3. Öffnen Sie unter **Computerkonfiguration** den Ordner **Administrative Vorlagen** und dann den Ordner **Windows-Komponenten**.
4. Wählen Sie **Windows-Remoteverwaltung (WinRM)**.
5. Wählen Sie unter **Windows-Remoteverwaltung (WinRM) WinRM-Client**.
6. Doppelklicken Sie unter **WinRM-Client** auf **Vertrauenswürdige Hosts**.
7. Geben Sie in der Liste **TrustedHostsList** den Hostnamen des Clients ein. Wenn alle Clients vertrauenswürdig sind, geben Sie nur ein Sternchen (*) ein.
8. Wählen Sie **WinRM-Dienst**.

9. Aktivieren Sie **Standardauthentifizierung zulassen**.
10. Aktivieren Sie **Unverschlüsselten Verkehr zulassen**.
11. Schließen Sie das Fenster **Gruppenrichtlinie**.
12. Führen Sie über die Befehlszeile den folgenden Befehl aus, um WinRM mit den Standardeinstellungen zu konfigurieren:
    `winrm qc or winrm quickconfig`
13. Wenn das Tool **Diese Änderungen vornehmen [j/n]?** anzeigt, geben Sie "**j**" ein.
14. Geben Sie einen der folgenden Befehle ein, um zu überprüfen, ob ein HTTP-Listener erstellt wurde:
    `winrm enumerate winrm/confg/listener`

    oder

    `winrm e winrm/config/Listener`
15. Geben Sie den folgenden Befehl in der Befehlszeile ein, um lokal zu testen.
    `winrm id`

Schritt 5: HTTPS-Konfiguration auf dem Server (zur Verwendung von HTTPS statt HTTP)

Dieser Schritt besteht aus zwei unterschiedlichen Prozessen: Generieren eines selbstsignierten Zertifikats, wenn das Zertifikat nicht vorhanden ist, und Importieren auf einen Windows-Server. Wenn kein Zertifikat vorhanden ist, müssen Sie ein selbstsigniertes Zertifikat auf dem Windows-Server konfigurieren, um die HTTPS/SSL-Kommunikation mit der BACS-GUI des Windows-Clients zu aktivieren. Der Windows-Client muss zudem mit dem selbstsignierten Zertifikat konfiguriert werden. Siehe Durchführen einer HTTPS-Konfiguration (wenn Sie HTTPS verwenden möchten).

Hinweis: Das selbstsignierte Zertifikat kann auf jedem Windows-Server erstellt werden. BACS muss nicht auf dem Server installiert sein. Das auf einem beliebigen Windows-Server generierte selbstsignierte Zertifikat sollte in das lokale Laufwerk des Client kopiert werden.

1. Klicken Sie auf **Start** (oder drücken Sie die Windows-Taste), und wählen Sie **Ausführen**.
2. Geben Sie **gpedit.msc** ein, um den lokalen Gruppenrichtlinien-Editor zu öffnen.
3. Öffnen Sie unter **Computerkonfiguration** den Ordner **Administrative Vorlagen** und dann den Ordner **Windows-Komponenten**.
4. Wählen Sie **Windows-Remoteverwaltung (WinRM)**.
5. Wählen Sie unter **Windows-Remoteverwaltung (WinRM) WinRM-Client**.
6. Doppelklicken Sie unter **WinRM-Client** auf **Vertrauenswürdige Hosts**.
7. Geben Sie in der Liste **TrustedHostsList** den Hostnamen des Clients ein. Wenn alle Clients vertrauenswürdig sind, geben Sie nur ein Sternchen (*) ein.
8. Wählen Sie **WinRM-Dienst**.
9. Aktivieren Sie **Standardauthentifizierung zulassen**.

So erstellen Sie ein selbstsigniertes Zertifikat für Windows Server:

OpenSSL für Windows kann verwendet werden, um das selbstsignierte Zertifikat wie folgt zu generieren:

1. Geben Sie den folgenden Befehl ein, um einen privaten Schlüssel zu erstellen:
   `openssl genrsa -des3 -out server.key 1024`
2. Sie werden zur Eingabe einer Passphrase aufgefordert. Merken Sie sich die Passphrase.
3. Führen Sie die folgenden Schritte zum Generieren einer Zertifikatsignieranforderung (CSR) aus.

   Während der Erzeugung der CSR werden Sie nach verschiedenen Informationen gefragt. Wenn Sie aufgefordert werden, den "Allgemeinen Namen" einzugeben, geben Sie den Hostnamen oder die IP-Adresse des Windows-Servers ein.

Geben Sie den folgenden Befehl ein (Beispielantworten angezeigt):

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

Wenn dieser Befehl nicht funktioniert, versuchen Sie Folgendes:

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

Die Datei openssl.cnf sollte im gleichen Verzeichnis wie openssl gespeichert werden. OpenSSL.cnf befindet sich im Ordner C:\Program Files (x86)\GnuWin32\share.

Die folgenden Informationen werden angezeigt:

- Land (zweistelliger Code) []: **US**
- Bundesstaat oder Provinz (vollständiger Name) []: **Kalifornien**
- Standortname (z. B. Stadt) []: **Irvine**
- Name der Organisation (z. B. Firma) []: **Broadcom Corporation**
- Name der Organisationseinheit (z. B. Abteilung) []: **Engineering**
- Allgemeiner Name (z. B. IHR Name) []: Geben Sie den Hostnamen oder die IP-Adresse des Windows-Servers ein. Geben Sie bei IPv6 den allgemeinen Namen im Format [xyxy:xxx:….::xxx] **einschließlich der Klammern [ ]** ein.
- (Optional) E-Mail-Adresse []:

Geben Sie folgende zusätzliche Attribute ein, die mit der Zertifikatanforderung gesendet werden:

- Kennwort in Frage stellen []: **Kennwort1**
- Ein optionaler Name des Unternehmens []:

4. Entfernen Sie die Passphrase aus dem Schlüssel.

Geben Sie die folgenden Befehle ein:

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

5. Generieren eines selbstsignierten Zertifikats:

Um ein selbstsigniertes Zertifikat zu generieren, das für 365 Tage aktiv ist, geben Sie den folgenden Befehl ein:

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

Die folgende Ausgabe wird angezeigt:

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

6. Geben Sie den folgenden Befehl ein, um das generierte selbstsignierte Zertifikat zu überprüfen.
`openssl verify server.crt`

Die folgende Ausgabe wird angezeigt:

```
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
```

Ignorieren Sie die Fehlermeldung "error 18 at 0 depth lookup:self signed certificate". Dieser Fehler weist darauf hin, dass dies ein selbstsigniertes Zertifikat ist.

7. Konvertieren Sie das Zertifikat wie folgt vom "crt"- in das "PKCS12"-Format:

Für einen Windows-Server sollte das Zertifikat im PKCS12-Format vorliegen. Geben Sie den folgenden Befehl ein:

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

Sie erhalten folgende Eingabeaufforderung:

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

Geben Sie das Kennwort ein, und stellen Sie sicher, dass Sie es sich merken. Das Kennwort ist erforderlich, wenn Sie das Zertifikat in den Windows-Server und -Client importieren.

8. Erstellen Sie eine Kopie der Zertifikatdatei "server.crt", und speichern Sie sie auf dem Server, auf dem BACS installiert wird, sodass sie importiert werden kann. Wenn Sie einen Windows-Client verwenden möchten, um eine Verbindung zum Server herzustellen, auf dem BACS ausgeführt wird, muss das Zertifikat ebenfalls an das Clientsystem übertragen (kopiert und eingefügt) werden.

Hinweis: Ein separates Zertifikat muss für eine IPv4-Adresse, IPv6-Adresse und einen Hostname generiert werden.

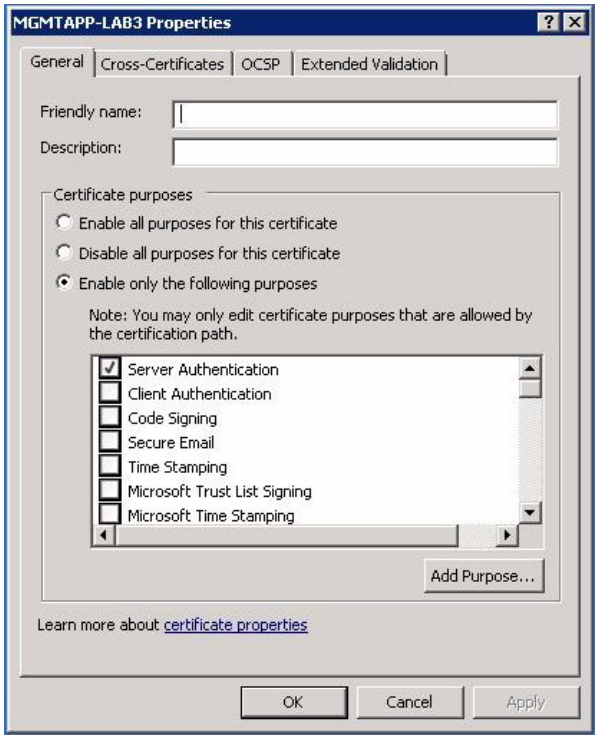
So installieren Sie das selbstsignierte Zertifikat auf dem Windows-Server:

Übertragen Sie vor der Installation des Zertifikats die Datei *hostname*.pfx, die Sie generiert haben, auf den Windows-Server:

1. Klicken Sie auf **Start** (oder drücken Sie die Windows-Taste), und wählen Sie **Ausführen**.
2. Geben Sie **MMC** ein, und klicken Sie auf **OK**.
3. Klicken Sie auf **Datei** > **Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie **Zertifikate**, und klicken Sie auf **Hinzufügen**.
6. Wählen Sie **Computerkonto**.
7. Klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**.
8. Klicken Sie auf **Schließen**, und klicken Sie dann auf **OK**.
9. Öffnen Sie den Ordner **Zertifikate (Lokaler Computer)**, und öffnen Sie dann den **persönlichen** Ordner.
10. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, wählen Sie **Alle Aufgaben**, und klicken Sie dann auf **Importieren**.
11. Klicken Sie **Weiter**, um den Zertifikatimport-Assistenten zu starten.
12. Navigieren Sie zu **hostname.pfx**.
13. Wenn Sie aufgefordert werden, das Kennwort für den privaten Schlüssel einzugeben, geben Sie das gleiche Kennwort ein, das Sie unter So erstellen Sie ein selbstsigniertes Zertifikat für Windows Server: erstellt haben.
14. Befolgen Sie die Anweisungen, wählen Sie die Standardwerte, und fahren Sie fort.

    Das Zertifikat wird auf der rechten Seite des Fensters als installiert angezeigt. Der Name entspricht dem von Ihnen angegebenen Namen beim Erstellen eines selbstsignierten Zertifikats.
15. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Eigenschaften**.

    Ein Dialogfeld wird wie folgt angezeigt:



16. Stellen Sie sicher, dass nur **Serverauthentifizierung** aktiviert ist, wie in der Abbildung gezeigt.

17. Öffnen Sie **Vertrauenswürdige Stammzertifizierungsstellen** und anschließend **Zertifikate**.

18. Befolgen Sie die Anweisungen von Schritt 11. bis Schritt 17..

Hinweis: Anweisungen zum Importieren des selbstsignierten Zertifikats in einen Client finden Sie unter Durchführen einer HTTPS-Konfiguration (wenn Sie HTTPS verwenden möchten).

Schritt 6: Konfigurieren von WinRM HTTPS/SSL auf dem Server

1. Erstellen Sie wie folgt einen WinRM-Listener:

a. Klicken Sie auf **Start** (oder drücken Sie die Windows-Taste), und wählen Sie **Ausführen**.

b. Geben Sie **MMC** ein, und klicken Sie auf **OK**.

c. Wählen Sie das selbstsignierte Zertifikat aus dem persönlichen Speicher aus.

Wenn das Zertifikat z. B. mit dem Hostnamen erstellt wurde, wird der Hostname angezeigt.

d. Doppelklicken Sie auf das Zertifikat, um es zu öffnen.

e. Klicken Sie auf die Registerkarte **Details**.

f. Blättern Sie nach unten, und wählen Sie das Feld **Fingerabdruck**.

g. Wählen und kopieren Sie den Fingerabdruck im Fenster **Details**, um ihn im nächsten Schritt einzufügen.

h. Kehren Sie zur Befehlszeile zurück.

i. Geben Sie den folgenden Befehl ein:

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

HINWEISE:

- Wenn das Zertifikat mit dem Hostnamen generiert wurde, geben Sie den Hostnamen ein. Wenn es mit der IP-Adresse generiert wurde, geben Sie die IP-Adresse ein. Schließen Sie bei IPv6-Adressen die Adresse in eckigen Klammern [ ] ein.
- Wenn HTTPS auf Ihrem System konfiguriert ist, muss der Listener vor dem Erstellen eines neuen HTTPS-Listeners gelöscht werden. Verwenden Sie den folgenden Befehl:
  `winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`

j. Der obige Befehl erstellt einen Listener auf dem HTTPS-Port (5986) mit einer beliebigen/allen Netzwerkadressen des Servers und dem mit my SelfSSL-generierten Zertifikat.

k. Sie können den `winrm`-Befehl zum Ändern oder Festlegen des HTTPS-Listeners verwenden, da WinRM-Listener auf jedem benutzerdefinierten Port konfiguriert werden können.

l. Führen Sie von einer Befehlszeile aus den folgenden Befehl aus, um zu überprüfen, ob der/die Listener konfiguriert wurden:
```
winrm e winrm/config/listener
```

2. Testen Sie die HTTPS/SSL-Verbindung auf dem Server.

   a. Führen Sie über die Befehlszeile auf dem Server den folgenden Befehl aus:
   ```
   winrs -r:https://yourserver:5986 -u:username -p:password hostname
   ```

   b. Bei ordnungsgemäßer Einrichtung zeigt die Ausgabe des Befehls den Hostnamen des Servers an.

   c. Um die Konfiguration des WinRM-Diensts zu überprüfen, führen Sie den folgenden Befehl aus:
   ```
   winrm get winrm/config/service
   ```

Schritt 7: Zusätzliche Serverkonfiguration

Ändern Sie gegebenenfalls die Firewallregeln wie folgt:

Windows Server 2008 R2

1. Öffnen Sie im Menü **Verwaltungstools** die Option **Windows-Firewall mit erweiterter Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Eingehende Regeln**, und wählen Sie **Neue Regel** aus.

   Der Assistent für neue Regeln wird geöffnet.
3. Wählen Sie die Option **Port** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie im Bildschirm **Protokoll und Ports TCP** aus, und geben Sie den spezifischen Port ein, z. B. 5985 für HTTP oder 5986 für HTTPS.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie im Bildschirm **Aktion** die Option **Verbindung zulassen**, und klicken Sie auf **Weiter**.
7. Unter **Profil** können Sie alle drei Profile auswählen, wenn Ihr Server sich in einer Arbeitsgruppe befindet.
8. Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Fertig stellen**.
9. Stellen Sie sicher, dass die neue Regel aktiviert ist (das grüne Kontrollkästchen ist aktiviert).

Windows XP

1. Klicken Sie auf **Start** > **Systemsteuerung**, und doppelklicken Sie dann auf **Windows-Firewall**.
2. Klicken Sie auf die Registerkarte **Ausnahmen**.
3. Klicken Sie auf **Port hinzufügen**.
4. Geben Sie einen aussagekräftigen **Namen** ein, z. B. "WinRM-Regel" und die Portnummer, z. B. 5985 für HTTP oder 5986 für HTTPS.
5. Klicken Sie auf **OK**.

Nützliche WinRM-Befehle

Befehl	*Beschreibung*
`winrm quickconfig or winrm qc`	Konfiguriert WinRM mit Standardeinstellungen.
`winrm enumerate winrm/config/Listener` or `winrm e winrm/config/Listener`	Hilft zu prüfen, welche Dienst-Listener aktiviert sind und welchen Port und welche IP-Adresse sie abhören.
`winrm get winrm/config/Service`	Prüft die Konfiguration des WinRM-Diensts.
`winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`	Löscht einen Listener (in diesem Fall einen HTTPS-Listener).

Nützliche WinRM-Websites

- 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
- Folgende Artikel auf http://support.microsoft.com:
  - "Configuring WINRM for HTTPS"
  - "Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0 und BITS 4.0)"

WS-MAN Windows-Client-Installation

Führen Sie im Windows-Client folgende Konfigurationsschritte aus.

1. Durchführen einer HTTP-Konfiguration (wenn Sie HTTP verwenden möchten)
   a. Klicken Sie auf **Start** (oder drücken Sie die Windows-Taste), und wählen Sie **Ausführen**.
   b. Geben Sie **gpedit.msc** ein, um den lokalen Gruppenrichtlinien-Editor zu öffnen.
   c. Öffnen Sie unter **Computerkonfiguration** den Ordner **Administrative Vorlagen** und dann den Ordner **Windows-Komponenten**.
   d. Wählen Sie **Windows-Remoteverwaltung (WinRM)**.
   e. Wählen Sie unter **Windows-Remoteverwaltung (WinRM) WinRM-Client**.
   f. Doppelklicken Sie unter **WinRM-Client** auf **Vertrauenswürdige Hosts**.
   g. Geben Sie in der Liste **TrustedHostsList** den Hostnamen des Clients ein, und klicken Sie auf **OK**. Wenn alle Clients vertrauenswürdig sind, geben Sie nur "*" ein.
   h. Wählen Sie **WinRM-Dienst**.
   i. Aktivieren Sie **Standardauthentifizierung zulassen**, und klicken Sie auf **OK**.
   j. Geben Sie den folgenden Befehl in der Befehlszeile ein, um die Verbindung zu testen.
      `winrm id -remote:<remote machine Hostname or IP Address>`
2. Durchführen einer HTTPS-Konfiguration (wenn Sie HTTPS verwenden möchten)

   Nachdem Sie ein selbstsigniertes Zertifikat wie in So erstellen Sie ein selbstsigniertes Zertifikat für Windows Server: beschrieben generiert haben, können Sie das Zertifikat in dem Client importieren, um die Verbindung zwischen Server und Client zu vereinfachen. Bevor Sie mit den folgenden Schritten fortfahren, stellen Sie sicher, dass alle erwähnten Schritte in Abschnitt So erstellen Sie ein selbstsigniertes Zertifikat für Windows Server: abgeschlossen sind, einschließlich des Kopierens von *hostname.pfx* an einen Speicherort, auf den der Client zugreifen kann.

   a. Klicken Sie auf **Start** (oder drücken Sie die Windows-Taste), und wählen Sie **Ausführen**.
   b. Geben Sie **MMC** ein, und klicken Sie auf **OK**.
   c. Klicken Sie auf **Datei**, und wählen Sie **Snap-In hinzufügen/entfernen**.
   d. Klicken Sie auf **Hinzufügen**.

e. Wählen Sie **Zertifikate**, und klicken Sie auf **Hinzufügen**.

f. Wählen Sie **Computerkonto**, und klicken Sie auf **Weiter**.

g. Klicken Sie auf **Fertig stellen**.

h. Klicken Sie auf **Schließen** und dann auf **OK**.

i. Klicken Sie unter **Zertifikate (Lokaler Computer)** mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen**, wählen Sie **Alle Aufgaben**, und wählen Sie **Importieren**.

j. Klicken Sie **Weiter**, um den Zertifikatimport-Assistenten zu starten.

k. Navigieren Sie zur in So erstellen Sie ein selbstsigniertes Zertifikat für Windows Server: generierten PFX-Datei. Ändern Sie die Auswahl in der Liste **Dateien vom Typ** zu **Personal Information Exchange (*.pfxas, *.p12)**, wählen Sie die Datei *hostname.pfx* aus, und klicken Sie anschließend auf **Öffnen**.

l. Geben Sie das Kennwort ein, das Sie dem privaten Schlüssel zugewiesen haben, und klicken Sie auf **Weiter**.

3. Konfigurieren von WinRM HTTPS/SSL

Sie können `winrm` von einem Client zum Abrufen von Informationen vom Server über eine WinRM HTTPS-Verbindung ausführen. Führen Sie die folgenden Schritte zum Testen der WinRM HTTPS/SSL-Verbindung auf dem Client aus:

a. Um die Betriebssysteminformationen des Servers abzurufen, geben Sie den folgenden Befehl ein.
```
winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername -u:username
-p:password -skipCAcheck
```

b. Um die Informationen zur WinRM-Identität des Servers abzurufen, geben Sie den folgenden Befehl ein.
```
winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
```

c. Um die Windows-Dienste auf dem Server aufzuzählen, geben Sie den folgenden Befehl ein.
```
winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -
skipCAcheck
```

Hinweis: Verwenden Sie unbedingt den Schalter `-skipCAcheck` beim Testen mit `winrm` in der Befehlszeile, da das Zertifikat selbstgeneriert und nicht in den Client importiert ist. Ansonsten wird die folgende Fehlermeldung angezeigt: `WSManFault.`

Verwenden von WMI

Für die Verwendung von WMI auf dem Windows-Client ist keine besondere Konfiguration erforderlich. Führen Sie die Schritte in den folgenden Abschnitten aus, um WMI auf dem Windows-Server zu konfigurieren.

Schritt 1: Einrichten von Namespacesicherheit mit der WMI-Steuerung

Die WMI-Steuerung bietet eine Möglichkeit zur Verwaltung der Namespacesicherheit. Sie können die WMI-Steuerung von der Befehlszeile aus mit diesem Befehl starten:

```
wmimgmt
```

Verwenden Sie auf Windows 9x- oder Windows NT4-Computern mit WMI stattdessen diesen Befehl:

```
wbemcntl.exe
```

Alternativ können Sie wie folgt auf die WMI-Steuerung und die Registerkarte "Sicherheit" zugreifen:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und anschließend auf **Verwalten**.
2. Doppelklicken Sie auf **Dienste und Anwendungen**, und doppelklicken Sie anschließend auf **WMI-Steuerung**.
3. Klicken Sie mit der rechten Maustaste auf **WMI-Steuerung**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie unter **WMI-Steuerung** auf die Registerkarte "Sicherheit".
5. Es sollte ein Ordner mit dem Namen "Root" und einem Pluszeichen (+) angezeigt werden. Erweitern Sie diese Struktur wie nötig, um den Namespace zu finden, für den Sie die Berechtigungen festlegen möchten.
6. Klicken Sie auf **Sicherheit**.

   Es wird eine Liste der Benutzer und deren Berechtigungen angezeigt. Wenn der Benutzer in der Liste aufgeführt wird, ändern Sie die Berechtigungen nach Bedarf. Wenn der Benutzer nicht in der Liste aufgeführt wird, klicken Sie auf **Hinzufügen**, und fügen Sie den Benutzer aus dem Speicherort (lokaler Rechner, Domain usw.) hinzu, an dem sich das Konto befindet.

HINWEISE: Sie können diese Exporte am Ende der Datei .bash_profile hinzufügen. Diese Datei befindet sich im /root-Verzeichnis.

- Um die Namespacesicherheit anzuzeigen und festzulegen, muss der Benutzer über Berechtigungen "Sicherheit lesen" und "Sicherheit bearbeiten" verfügen. Administratoren verfügen standardmäßig über diese Berechtigungen und können die Berechtigungen nach Bedarf anderen Benutzerkonten zuweisen.
- Wenn der Benutzer per Remotezugriff auf den Namespace zugreifen muss, müssen Sie die Berechtigung "Remoteaktivierung" auswählen.
- Standardmäßig gelten Benutzerberechtigungen für einen Namespace nur auf diesem Namespace. Wenn Sie möchten, dass der Benutzer Zugriff auf einen Namespace und alle untergeordneten Namespaces in der Strukturansicht oder nur auf die untergeordneten Namespaces erhält, klicken Sie auf **Erweitert**. Klicken Sie auf **Bearbeiten**, und geben Sie den Umfang des Zugriffs im angezeigten Dialogfeld an.

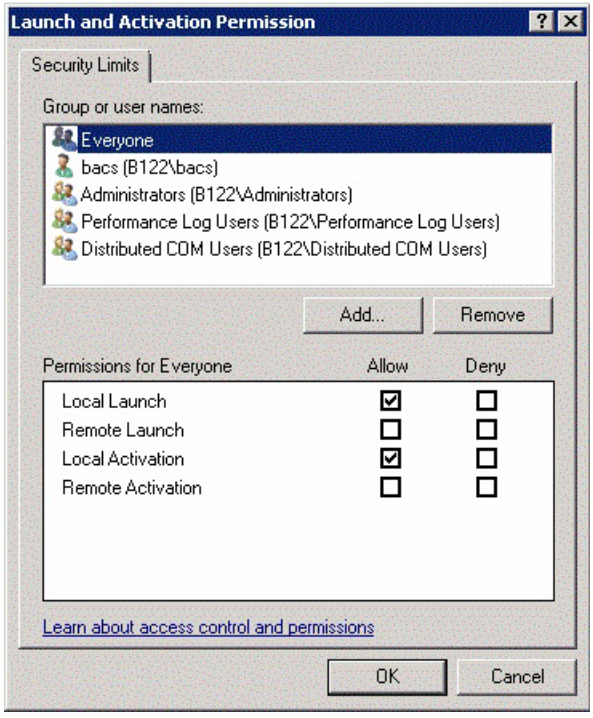
Schritt 2: Gewähren der Remote-Start- und Aktivierungsberechtigungen für DCOM

In der Windows-Domänenumgebung verfügt das Administratorkonto der Domäne über die notwendige Berechtigungsstufe für den Zugriff auf die WMI-Komponente für die BACS-Verwaltung, weshalb keine spezielle Konfiguration erforderlich ist. In einem großen Unternehmen jedoch hat ein Benutzer, der mit der BACS4-Client-GUI auf den lokalen oder Remotehost zugreift, nicht immer die Berechtigung des Domänenadministratorkontos. Sie müssen den WMI-Sicherheitszugriff auf dem Remotehost konfigurieren, damit der Benutzer mit der BACS4-Client-GUI eine Verbindung herstellen kann.

Diese Konfiguration kann einfach mit dem folgenden Verfahren vorgenommen werden. Wenn Sie nicht über ausreichende Berechtigungen verfügen, um die Sicherheit für den WMI-Zugriff zu konfigurieren, wenden Sie sich an Ihren Netzwerkadministrator.

1. Klicken Sie auf **Start** > **Ausführen**, geben Sie **DCOMCNFG** ein, und klicken Sie auf **OK**.
2. Das Dialogfeld "Komponentendienste" wird angezeigt.
3. Öffnen Sie **Komponentendienste** und anschließend **Computer**.
4. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und anschließend auf **Eigenschaften**.
5. Klicken Sie unter **Computereigenschaften** auf die Registerkarte **COM-Sicherheit**.
6. Klicken Sie unter **Start- und Aktivierungsberechtigungen** auf **Limits bearbeiten**.
7. Führen Sie diese Schritte aus, wenn Ihr Name oder Ihre Gruppe nicht in der Liste **Gruppen- oder Benutzernamen** aufgeführt wird.
   a. Klicken Sie im Dialogfeld "Startberechtigung" auf **Hinzufügen**.
   b. Fügen Sie im Dialogfeld "Benutzer, Computer oder Gruppen auswählen" Ihren Namen und die Gruppe im Feld **Geben Sie die Namen der auszuwählenden Objekte ein** hinzu, und klicken Sie anschließend auf **OK**.
   c. Wählen Sie im Dialogfeld "Startberechtigung" Ihren Benutzer und die Gruppe in der Liste **Gruppen- oder Benutzernamen** aus.
   d. Wählen Sie im Bereich **Berechtigungen für Benutzer Zulassen** für **Remotestart** und **Remoteaktivierung** aus, und klicken Sie dann auf **OK**.

Abbildung 8: Start- und Aktivierungsberechtigungen



Weitere Informationen finden Sie unter Securing a Remote WMI Connection auf der Microsoft Developer Network-Website.

Besondere Konfiguration für WMI auf anderen Systemen

Um unter Windows Vista und Windows 7 alle Benutzer in der Administratorgruppe eine Verbindung über den WMI-Namespace herstellen zu lassen, muss der Benutzer u. U. die LocalAccountTokenFilterPolicy nach Bedarf ändern.

Abschnitt 13: Verwenden der Broadcom Advanced Control Suite 4

Broadcom Advanced Control Suite – Überblick

Bei der Broadcom Advanced Control Suite (BACS) handelt es sich um ein integriertes Dienstprogramm, das nützliche Informationen über jeden der auf dem System installierten Netzwerkadapter zur Verfügung stellt. Mit der BACS können Sie außerdem ausführliche Tests, Diagnosen und Analysen für jeden Adapter ausführen, Eigenschaftswerte abrufen und ändern sowie Datenverkehrsstatistiken für Netzwerkobjekte anzeigen. BACS funktioniert unter Windows- und Linux-Betriebssystemen.

Mit dem in der Broadcom Advanced Control Suite integrierten Broadcom Advanced Server Program (BASP) können Teams für "Load Balancing" (Lastverteilung), Fehlertoleranz und VLANs (Virtual Local Area Networks) konfiguriert werden. Die Funktionen des BASP sind nur auf Systemen mit mindestens einem Broadcom-Netzwerkadapter verfügbar. BASP funktioniert nur unter Windows-Betriebssystemen.

Hinweis: Einige Funktionen von BACS sind nur für bestimmte Adapter relevant. Da eine einzige Instanz der BACS verwendet werden kann, um mit mehreren Hosts und Adaptertypen zu kommunizieren, beschreibt dieses Thema alle BACS-Funktionen.

Die BACS-Anwendung enthält eine grafische Benutzeroberfläche und eine Befehlszeilenoberfläche (BACSCLI). Die BACS-GUI und die BACS-CLI sind mit folgenden Betriebssystemen kompatibel:

- Windows
- Windows-Server
- Linux-Server

Informationen zu den neuesten unterstützten Betriebssystemversionen finden Sie in der Release-Dokumentation Ihrer Software.

Starten der Broadcom Advanced Control Suite

Klicken Sie in der Systemsteuerung auf **Broadcom Control Suite 4**, oder klicken Sie in der Symbolleiste am unteren Rand des Windows- oder Windows Server-Desktops auf das BACS-Symbol.

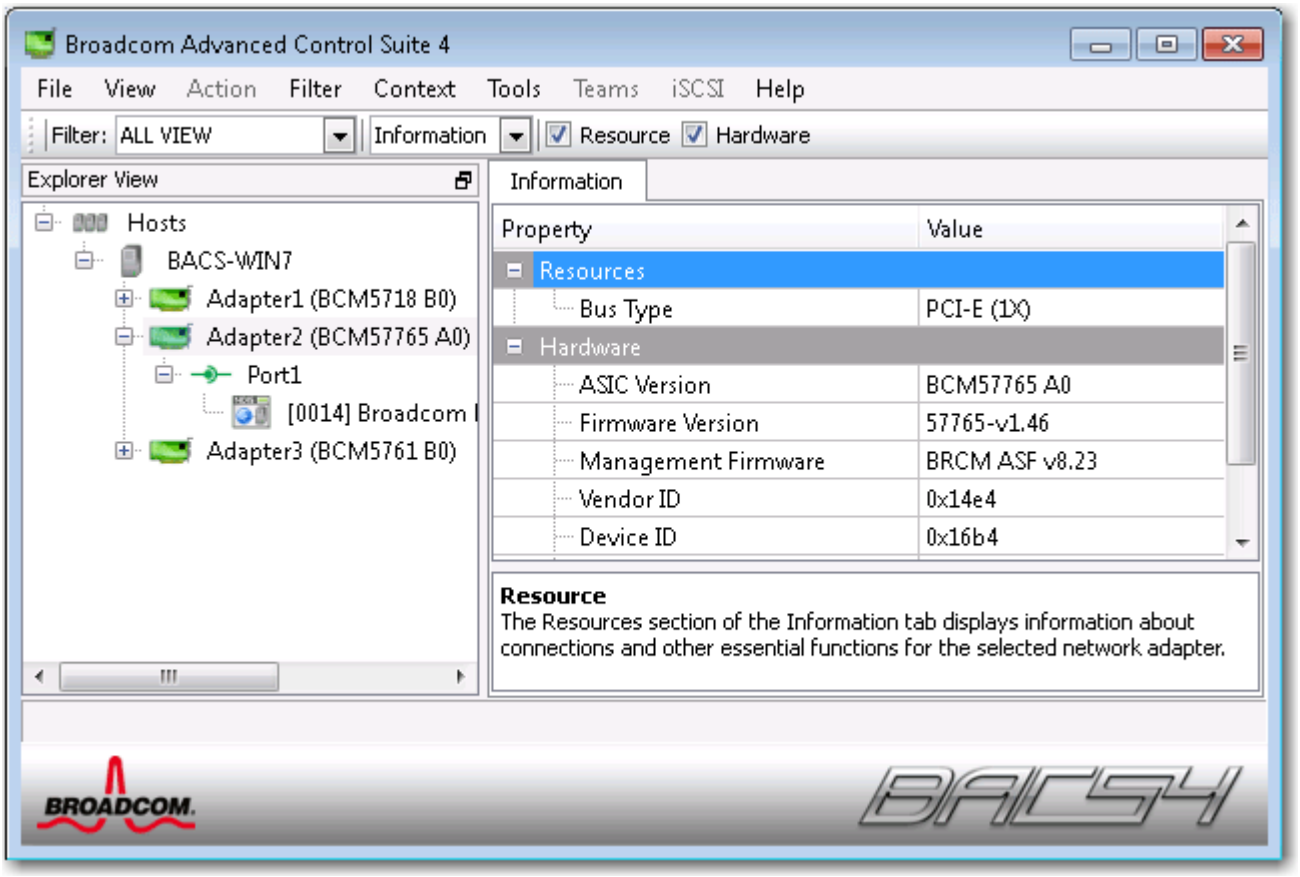
Doppelklicken Sie bei Linux-Systemen auf das BACS4-Desktopsymbol, oder greifen Sie über die Taskleiste unter **Systemwerkzeuge** auf das BACS-Programm zu. (Wenn Sie Probleme haben sollten, BACS auf einem Linux-System zu starten, lesen Sie das verwandte Thema in BACS-Problembehebung.)

BACS-Schnittstelle

Die BACS-Schnittstelle besteht aus den folgenden Bereichen:

- Fenster "Explorer-Ansicht"
- Kontextansichtauswahl
- Fenster "Kontextansicht"
- Menüleiste
- Fenster "Beschreibung"

Standardmäßig ist das Fenster "Explorer-Ansicht" an der linken Seite des Hauptfensters angedockt, das Fenster "Kontextansicht" befindet sich rechts, die Kontextansichtsauswahl unterhalb der Menüleiste und das Fenster "Beschreibung" unterhalb des Fensters "Kontextansicht". Ziehen Sie die Trennlinie zwischen zwei Fenstern, um die Größe der Fenster zu ändern.



Fenster "Explorer-Ansicht"

Sie können das Fenster "Explorer-Ansicht" links, rechts, oben oder unten am Hauptfenster andocken.

Im Fenster "Explorer-Ansicht" werden die Objekte aufgeführt, die über BACS angezeigt, analysiert, getestet oder konfiguriert werden können. Wenn ein Element im Fenster "Explorer-Ansicht" ausgewählt wird, werden die Registerkarten, auf denen die Informationen und Optionen zu dem Element angezeigt werden, im Fenster "Kontext-Ansicht" angezeigt.

Dieses Fenster ist so organisiert, dass die verwaltbaren Objekte auf dieselbe hierarchische Weise wie Treiber und Unterkomponenten angezeigt werden. Dadurch wird die Verwaltung der verschiedenen Elemente des konvergierten Netzwerkschnittstellen-Controllers (C-NIC, Converged Network Interface Controller) vereinfacht. Die obere Ebene der Hierarchie ist der Host-Container, in dem alle von BACS verwalteten Hosts aufgelistet sind. Unterhalb der Hosts befinden sich die installierten Netzwerkadapter und unterhalb der Adapter die verwaltbaren Elemente, z. B. physikalischer Port, NDIS und iSCSI.

Das Symbol neben jedem Gerät im Bereich "Explorer-Ansicht" zeigt den Status an. Ein Symbol neben einem Gerätenamen, das normal dargestellt wird, bedeutet, dass das Gerät verbunden ist und ordnungsgemäß funktioniert.

- **X.** Wenn ein rotes "X" auf dem Symbol des Geräts angezeigt wird, ist das Gerät derzeit nicht mit dem Netzwerk verbunden.
- **Ausgegraut.** Ein ausgegrautes Gerätesymbol gibt an, dass das Gerät derzeit deaktiviert ist.

Kontextansichtsauswahl

Die Kontextansichtsauswahl wird unterhalb der Menüleiste angezeigt und enthält den Filter und Registerkartenkategorien. Sie können zwar die im Fenster "Kontextansicht" auf den Registerkarten angezeigten Kategorien erweitern und ausblenden, alternativ können Sie jedoch auch eine Kategorie durch Auswählen des Felds neben dem Namen der Kategorie anzeigen.

Filteransicht

In einer Umgebung mit mehreren Hosts, in der verschiedene C-NICs verwendet werden, können pro Adapter zahlreiche verwaltbare Elemente vorhanden sein, deren Anzeige, Konfiguration und Verwaltung schwierig und umständlich sein können. Verwenden Sie den Filter, um eine bestimmte Gerätefunktion auszuwählen. Zu den möglichen Filteransichten gehören:

- Alle
- TEAMANSICHT
- NDIS-ANSICHT
- iSCSI-ANSICHT
- iSCSI-ZIEL-ANSICHT

Fenster "Kontextansicht"

Im Fenster "Kontextansicht" werden alle Parameter angezeigt, die für das im Fenster "Explorer-Ansicht" ausgewählte Objekt angezeigt werden können. Die Parameter werden je nach Parametertyp nach Registerkarten und Kategorien gruppiert. Die verfügbaren Registerkarten sind "Informationen", "Konfiguration", "Diagnose" und "Statistik". Da die BACS-Schnittstelle kontextsensitiv ist, können nur die Parameter, die auf das ausgewählte Objekt zutreffen, im Fenster "Kontextansicht" angezeigt oder konfiguriert werden.

Menüleiste

Folgendes wird auf der Menüleiste angezeigt. Da jedoch Menüelemente kontextsensitiv sind, sind nicht alle Elemente jederzeit verfügbar:

Menü "Datei"

- Team speichern unter: Zum Speichern der aktuellen Teamkonfigurationen in einer Datei.
- Team wiederherstellen: Zum Wiederherstellen einer gespeicherten Teamkonfiguration aus einer Datei.

Menü "Aktion"

- Host entfernen: Zum Entfernen des ausgewählten Hosts.
- Host aktualisieren: Zum Aktualisieren des ausgewählten Hosts.

Menü "Ansicht"

- Explorer-Ansicht: Zum Anzeigen/Ausblenden des Fensters "Explorer-Ansicht".
- Symbolleiste: Zum Anzeigen/Ausblenden der Symbolleiste.
- Statusleiste: Zum Anzeigen/Ausblenden der Statusleiste.
- Broadcom-Logo: Zum Anzeigen/Ausblenden des Broadcom-Logos in BACS zur Optimierung des maximal nutzbaren Anzeigeplatzes.

Menü "Extras"

- Optionen: Zum Konfigurieren der BACS-Einstellungen.

Teams (nur Windows)

- Team erstellen: Zum Erstellen von neuen Teams entweder mit dem Teaming-Assistenten oder im Erweiterten Modus.
- Team verwalten: Zum Verwalten vorhandener Teams entweder mit dem Teaming-Assistenten oder im Erweiterten Modus.

Fenster "Beschreibung"

Im Fenster "Beschreibung" werden Informationen, Konfigurationsanweisungen und Optionen für den ausgewählten Parameter im Fenster "Kontextansicht" bereitgestellt.

Konfigurieren von Einstellungen unter Windows

So aktivieren und deaktivieren Sie das BACS-Taskleistensymbol unter Windows

BACS speichert bei Windows-Systemen während der Installation ein Symbol in der Windows-Taskleiste. Über das Fenster **Optionen** können Sie dieses Symbol aktivieren und deaktivieren.

1. Wählen Sie im Menü **Extras** die Option **Optionen**.
2. Aktivieren oder deaktivieren Sie **BACSTray aktivieren**. (Diese Option ist standardmäßig aktiviert.)
3. Klicken Sie auf **OK**.

Festlegen des Teaming-Modus unter Windows

1. Wählen Sie im Menü **Extras** die Option **Optionen**.
2. Wenn Sie auf den Teaming-Assistenten zum Erstellen von Teams verzichten möchten, wählen Sie **Experten-Modus** aus. Andernfalls wählen Sie **Assistenten-Modus** aus.
3. Klicken Sie auf **OK**.

Festlegen der Aktualisierungszeit für die Explorer-Ansicht unter Windows

1. Wählen Sie im Menü **Extras** die Option **Optionen**.
2. Wählen Sie **Automatisch** aus, um die Aktualisierungszeit für die Explorer-Ansicht auf 5 Sekunden festzulegen. Andernfalls wählen Sie Benutzerdefiniert und dann die Zeit in Sekunden aus.
3. Klicken Sie auf **OK**.

Herstellen einer Verbindung mit einem Host

Sie können Windows- oder Linux-Host zur Verwaltung durch BACS hinzufügen.

So fügen Sie einen lokalen Host hinzu:

1. Klicken Sie im Menü **Aktion** auf **Host hinzufügen**.
2. Ändern Sie weder für Windows- noch für Linux-Hosts die Standardeinstellungen. Zum Herstellen einer Verbindung zum lokalen Host sind weder **Benutzername** noch **Kennwort** erforderlich.
3. Wählen Sie **Aufrecht erhalten** aus, wenn BACS die Informationen für diesen Host speichern soll.
4. Klicken Sie auf **OK**. Nun können Sie mit BACS Informationen anzeigen und den Host verwalten.

So fügen Sie einen Remote-Host hinzu:

1. Klicken Sie im Menü **Aktion** auf **Host hinzufügen**.
2. Geben Sie im Feld **Host** Hostname oder IP-Adresse des Remote-Hosts ein.
3. Wählen Sie aus der Liste **Protokoll** das Protokoll aus. Die Protokolloptionen für Windows sind **WMI**, **WSMan** oder **Alle versuchen**. Die Protokolloptionen für Linux sind **CimXML**, **WSMan** oder **Alle versuchen**. Durch die Option **Alle versuchen** wird der GUI-Client gezwungen, alle Optionen zu versuchen.
4. Wählen Sie das **HTTP**-Schema oder für höhere Sicherheit das **HTTPS**-Schema aus.
5. Geben Sie den zum Konfigurieren des Hosts verwendeten Wert für **Portnummer** ein, sofern sich dieser Wert von **5985** unterscheidet.
6. Geben Sie **Benutzername** und **Kennwort** ein.
7. Wählen Sie **Aufrecht erhalten** aus, wenn BACS die Informationen für diesen Host speichern soll. Der Host wird im Explorer-Fenster angezeigt, wenn Sie BACS öffnen. Die IP-Adresse oder der Hostname muss zum Herstellen der Verbindung nicht erneut eingegeben werden. Aus Sicherheitsgründen müssen Sie jedoch jedes Mal **Benutzername** und **Kennwort** eingeben.
8. Klicken Sie auf **OK**.

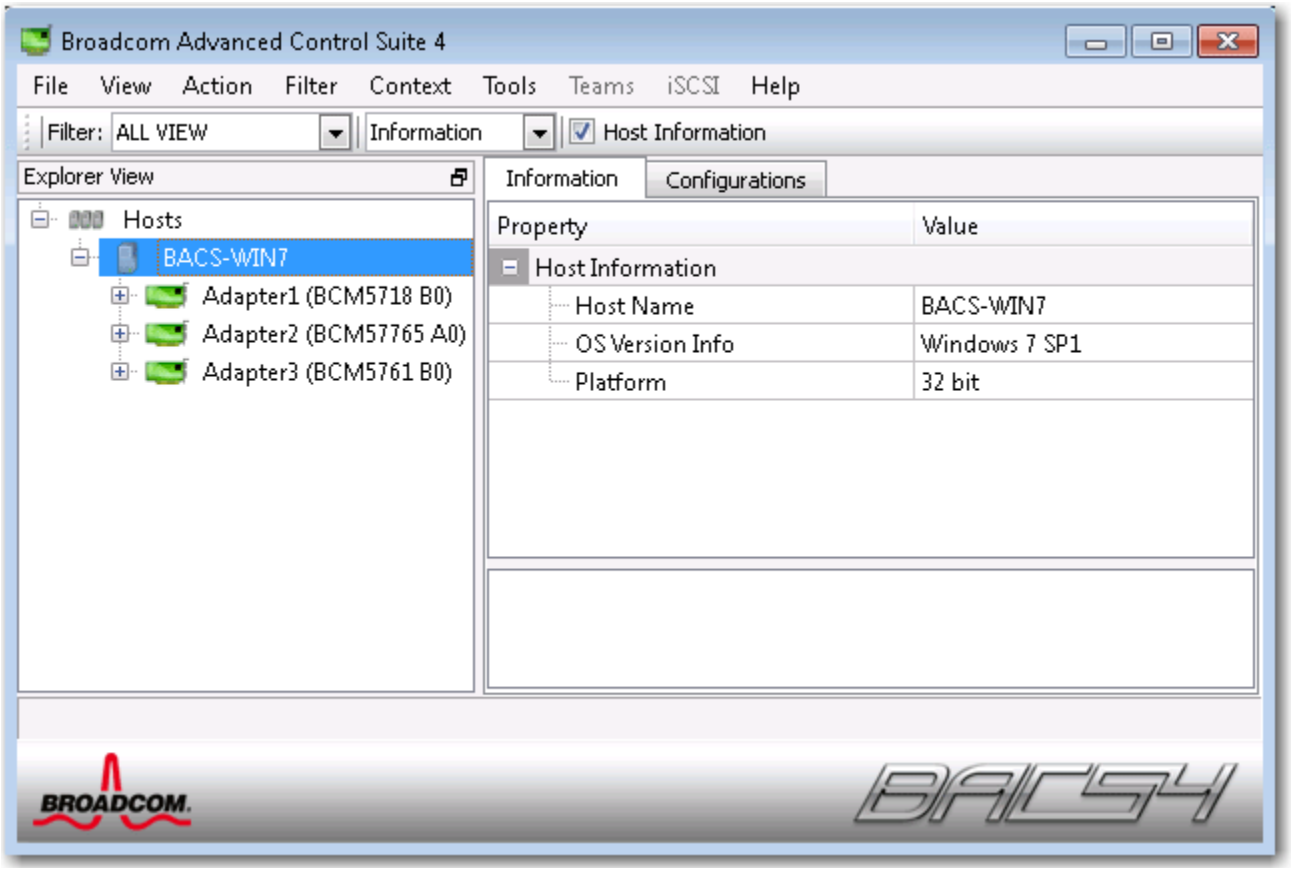
Verwalten des Hosts

Auf Hostebene können Sie auf den folgenden Registerkarten Hostinformationen anzeigen und Parameter konfigurieren.

- Informationen
- Konfiguration

So zeigen Sie Hostinformationen an:

Wählen Sie im Fenster **Explorer-Ansicht** den Host aus. Wählen Sie dann die Registerkarte **Informationen** aus, um Informationen auf Hostebene anzuzeigen.



Registerkarte "Informationen": Hostinformationen

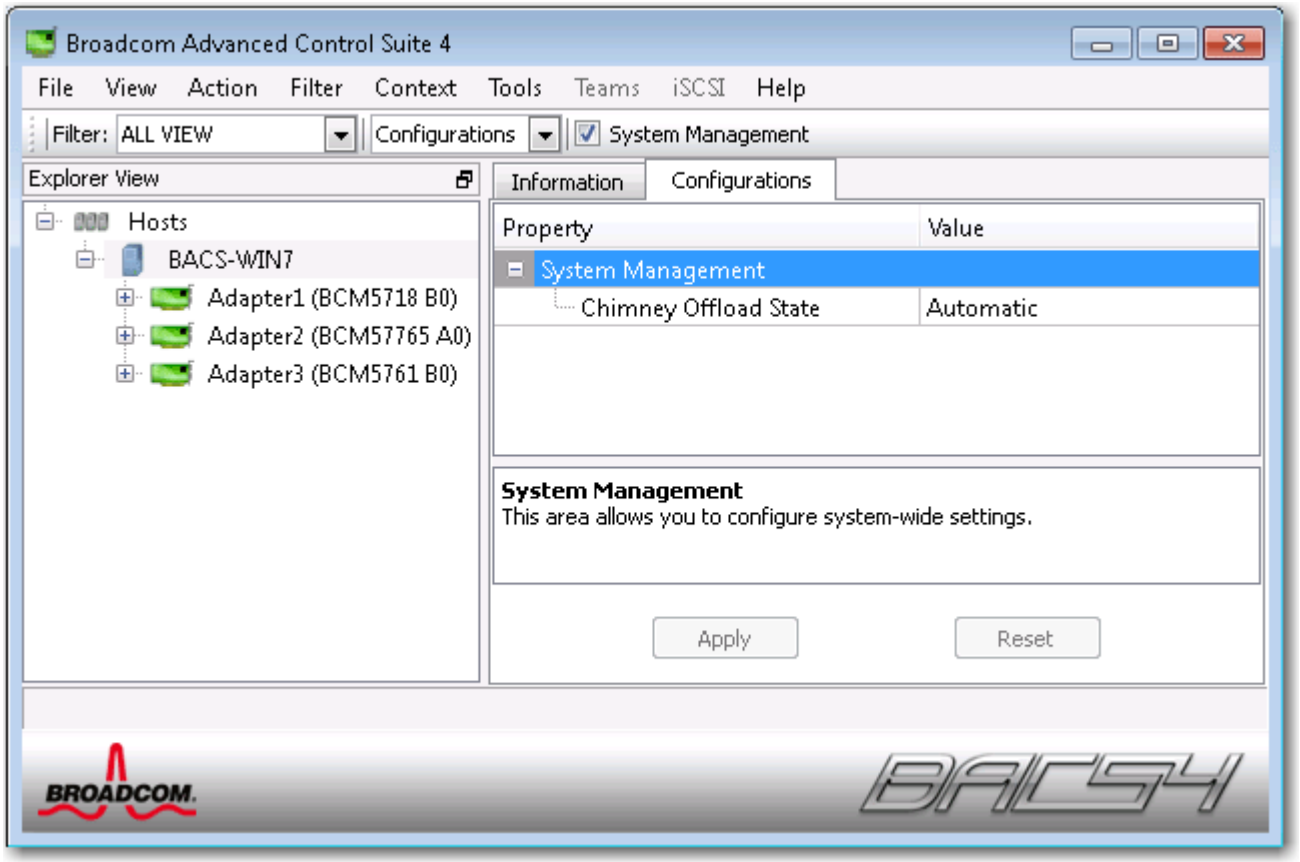
Host-Name. Hier wird der Name des Hosts angezeigt.

OS-Versionsinformationen. Hier wird das Betriebssystem, einschließlich Version, angezeigt.

Plattform. Hier wird die Hardwarearchitekturplattform angezeigt (z. B. 32 Bit oder 64 Bit).

So konfigurieren Sie den Host:

Wählen Sie im Fenster **Explorer-Ansicht** den Host aus. Wählen Sie dann die Registerkarte **Konfiguration** aus, um Parameter auf Hostebene zu konfigurieren.



Verwalten der Netzwerkadapter

Die installierten Adapter werden eine Ebene unterhalb des Hosts in der hierarchischen Struktur im Fenster "Explorer-Ansicht" angezeigt. Auf Adapterebene können Sie auf den folgenden Registerkarten Informationen anzeigen und Parameter konfigurieren.

- Informationen
- Konfiguration

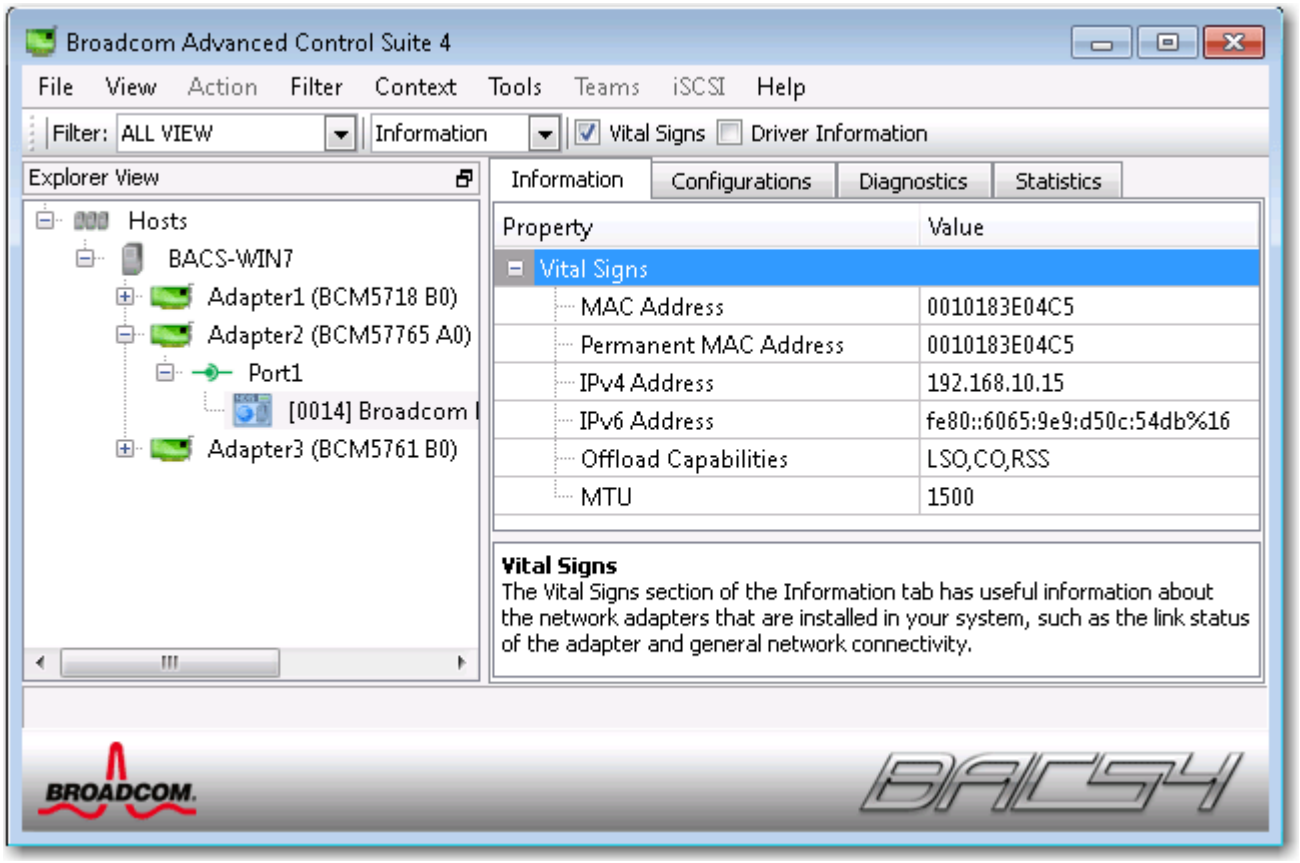
Anzeigen von Adapterinformationen

Im Bereich **Statusinformationen** auf der Registerkarte **Informationen** finden sich nützliche Informationen zu den Netzwerkadaptern, die in Ihrem System installiert sind, beispielsweise der Verbindungsstatus des Adapters und die allgemeine Netzwerkkonnektivität.

Wählen Sie im Fenster **Explorer-Ansicht** den Netzwerkadapter aus. Wählen Sie dann die Registerkarte **Informationen** aus, um Informationen auf Adapterebene anzuzeigen.

HINWEISE:

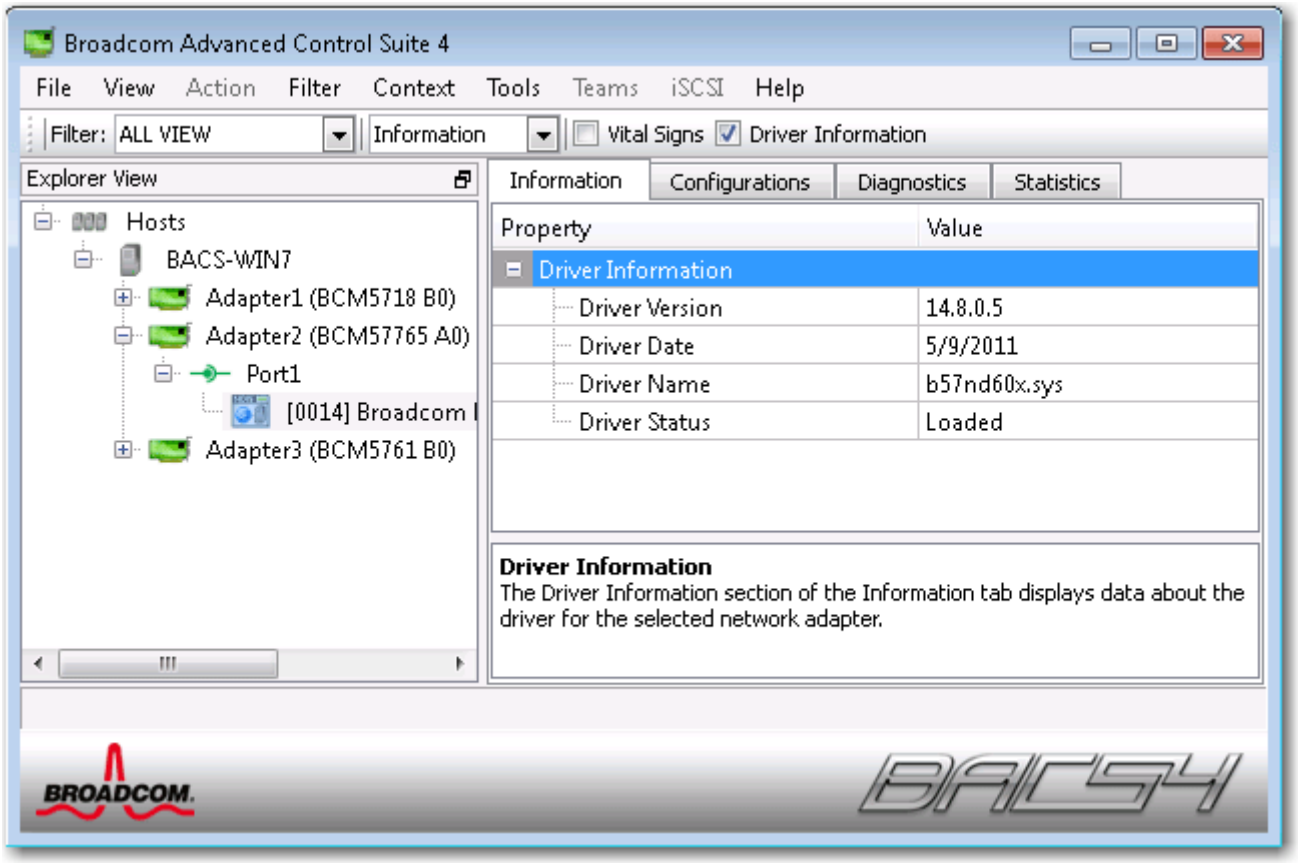
- Die Informationen zu den Broadcom Netzwerkadaptern sind möglicherweise umfassender als die Informationen zu Netzwerkadaptern anderer Hersteller.
- Einige Informationen sind möglicherweise nicht für alle Broadcom-Netzwerkadapter verfügbar.


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

Anzeigen von Treiberinformationen

Im Bereich **Treiberinformationen** der Registerkarte **Informationen** werden Daten zum Treiber des ausgewählten Netzwerkadapters angezeigt.

Zum Anzeigen der Treiberinformationen für einen beliebigen installierten Netzwerkadapter klicken Sie auf den Namen des Adapters, der im Fenster "Explorer-Ansicht" aufgeführt ist. Klicken sie dann auf die Registerkarte **Informationen**.



Treiberstatus. Der Status des Adaptertreibers.

- **Geladen**: Normaler Betriebsmodus. Der Adaptertreiber wurde von Windows geladen und funktioniert ordnungsgemäß.
- **Nicht geladen**: Der mit dem Adapter verbundene Treiber wurde von Windows nicht geladen.
- **Nicht verfügbar**: Über den Treiber, der mit dem ausgewählten Adapter verbunden ist, sind keine Informationen verfügbar.

Treibername. Der Dateiname des Adaptertreibers.

Treiberversion. Die aktuelle Version des Adaptertreibers.

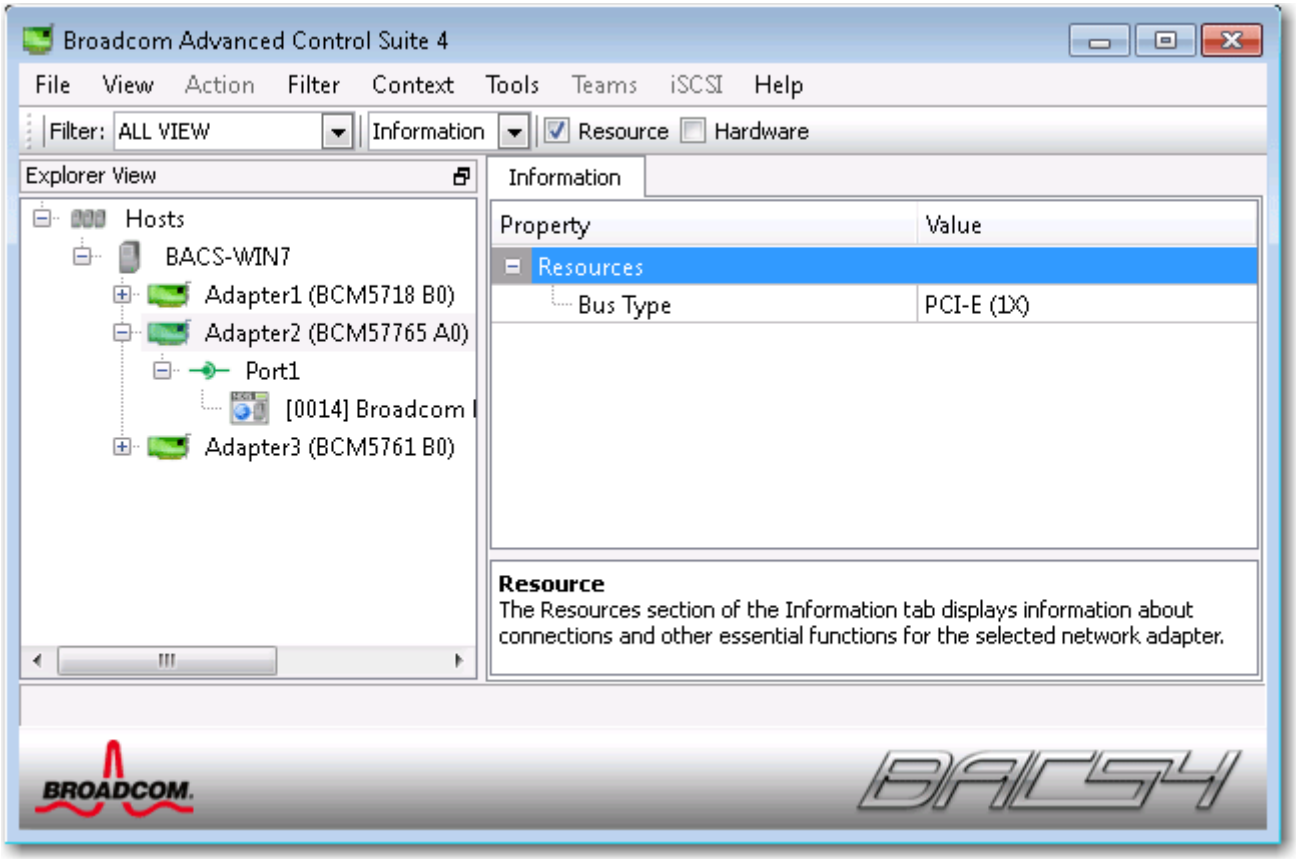
Treiberdatum. Das Erstellungsdatum des Adaptertreibers.

Anzeigen von Ressourceninformationen

Im Bereich **Ressourcen** der Registerkarte **Informationen** werden Informationen zu Verbindungen und anderen wichtigen Funktionen des ausgewählten Netzwerkadapters angezeigt.

Zum Anzeigen der Ressourcen für einen beliebigen installierten Netzwerkadapter klicken Sie auf den Namen des Adapters, der im Fenster "Explorer-Ansicht" aufgeführt ist. Klicken sie dann auf die Registerkarte **Informationen**.

Hinweis: Einige Informationen sind möglicherweise nicht für alle Broadcom-Netzwerkadapter verfügbar.



Bus-Typ. Die Art der vom Adapter verwendeten Eingangs-/Ausgangs-Verbindung.

Steckplatznr. Die durch den Adapter belegte Steckplatznummer auf der Systemplatine. Diese Option ist für PCI-Express-Adapter nicht verfügbar.

Bus-Taktrate (MHz). Die vom Adapter verwendete Bus-Clock-Signalfrequenz. Diese Option ist für PCI-Express-Adapter nicht verfügbar.

Bus-Breite (Bit). Die Anzahl an Bits, die der Bus jeweils in einem Vorgang an den Adapter übertragen bzw. vom Adapter empfangen kann. Diese Option ist für PCI-Express-Adapter nicht verfügbar.

Busnr. Gibt die Nummer für den Bus an, auf dem der Adapter installiert ist.

Gerätenr. Die dem Adapter vom Betriebssystem zugewiesene Nummer.

Funktionsnr. Die Portnummer des Adapters. Die Funktionsnummer für einen Einzel-Port-Adapter ist 0. Für einen Adapter mit zwei Ports ist die Funktionsnummer für den ersten Port 0 und die Funktionsnummer für den zweiten Port 1.

Interrupt-Anforderung. Die Interrupt-Zeilennummer, die mit dem Adapter verbunden ist. Der gültige Bereich reicht von 2 bis 25.

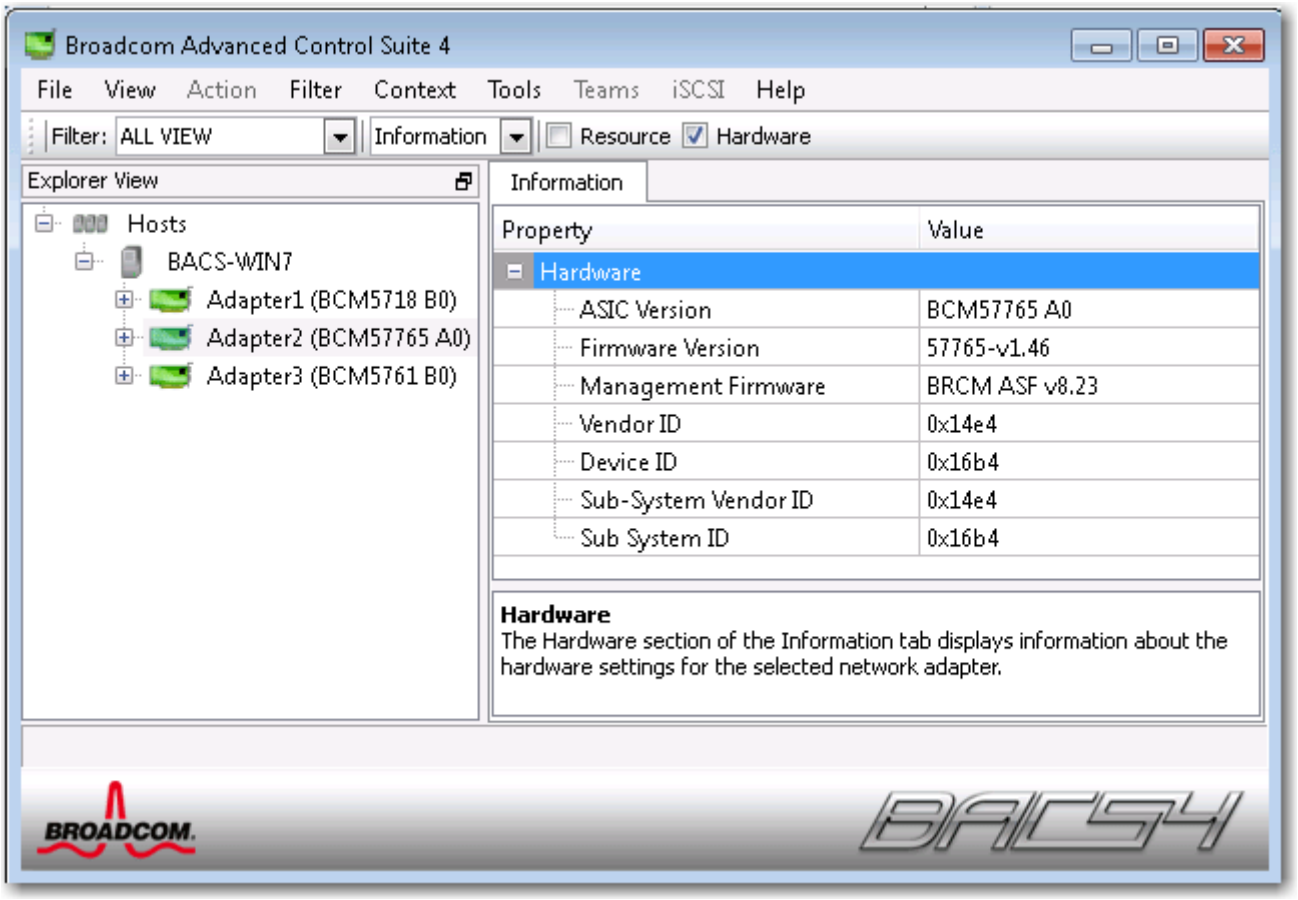
Speicheradresse. Die im Speicher abgebildete Adresse, die dem ausgewählten Adapter zugewiesen ist. Dieser Wert ist niemals Null.

Anzeigen von Hardwareinformationen

Im Bereich **Hardware** der Registerkarte **Informationen** werden Informationen zu den Hardwareeinstellungen des ausgewählten Netzwerkadapters angezeigt.

Zum Anzeigen der Hardware für einen beliebigen installierten Netzwerkadapter klicken Sie auf den Namen des Adapters, der im Fenster "Explorer-Ansicht" aufgeführt ist. Klicken sie dann auf die Registerkarte "Informationen".

Hinweis: Einige Informationen sind möglicherweise nicht für alle Broadcom-Netzwerkadapter verfügbar.



ASIC-Version. Die Chip-Version des Broadcom-Adapters (für Adapter von anderen Herstellern sind diese Informationen nicht verfügbar).

Firmware-Version. Die Firmware-Version des Broadcom-Adapters (für Adapter von anderen Herstellern sind diese Informationen nicht verfügbar). Diese Informationen stehen nur für Broadcom NetXtreme-Adapter zur Verfügung.

Händler-ID. Die Identifikationsnummer des Händlers.

Geräte-ID. Die Adapter-ID.

Händler-ID des untergeordneten Systems. Die Identifikationsnummer des Händlers des untergeordneten Systems.

ID des untergeordneten Systems. Die Identifikationsnummer des untergeordneten Systems.

Testen des Netzwerks

Über die Option **Netzwerktest** auf der Registerkarte **Diagnose** können Sie die IP-Netzwerkkonnektivität testen. Bei diesem Test wird festgestellt, ob der Treiber ordnungsgemäß installiert wurde. Zusätzlich wird die Anbindung an ein Gateway oder eine andere angegebene IP-Adresse auf demselben Subnetz überprüft. Der Netzwerktest nutzt TCP/IP, um ICMP-Pakete an entfernte Systeme zu senden, und wartet dann auf eine Antwort.

Hinweis: Die Option für den Netzwerktest steht nicht für Adapter zur Verfügung, die in einem Team gruppiert sind (siehe Konfigurieren der Teaming-Funktion).

So führen Sie den Netzwerktest aus

1. Klicken Sie im Fenster "Explorer-Ansicht" auf den Namen des zu testenden Adapters.
2. Wählen Sie aus der Liste **Auszuführenden Test auswählen** die Option **Netzwerktest**. Wenn die Option **Netzwerktest** nicht zur Verfügung steht, wählen Sie auf der rechten Seite des Fensters auf der Registerkarte **Kontextansicht** die Option **Diagnose** und anschließend **Netzwerktest**.
3. Um die Ziel-IP-Adresse zu ändern, wählen Sie **Ping an IP-Adresse** aus. Geben Sie im Fenster für den Netzwerktest eine Ziel-IP-Adresse ein, und klicken Sie auf **OK**.
4. Klicken Sie auf **Testen**.

Die Ergebnisse des Netzwerktests werden im Feld **Status** angezeigt.

Ausführen von Diagnosetests

Über die Option **Diagnosetests** auf der Registerkarte **Diagnose** können Sie den Zustand der physischen Komponenten eines Broadcom Netzwerkadapters überprüfen. Sie können die Tests manuell auslösen oder festlegen, dass BACS 3 sie regelmäßig automatisch ausführt. Wenn der Test regelmäßig automatisch ausgeführt wird, werden bei jeder Ausführung die Anzahl der bestandenen und nicht bestandenen Tests im Feld **Ergebnis** aufgeführt. Wenn ein Test beispielsweise viermal ausgeführt wird und kein Fehler aufgetreten ist, wird im Feld **Ergebnis** für diesen Test der Wert 4/0 angezeigt. Wenn jedoch drei Vorgänge erfolgreich ausgeführt werden und bei einem ein Fehler aufgetreten ist, wird im Feld **Ergebnis** der Wert 3/1 angezeigt.

HINWEISE:

- Sie benötigen Administratorrechte, um diese Diagnosetests auszuführen.
- Die Netzwerkverbindung wird beim Ausführen dieser Tests vorübergehend unterbrochen.
- Nicht alle Broadcom-Adapter unterstützen jeden Test.

So führen Sie die Diagnosetests einmal durch

1. Klicken Sie im Fenster "Explorer-Ansicht" auf den Namen des zu testenden Adapters, und wählen Sie dann die Registerkarte "Diagnose" aus.
2. Wählen Sie aus der Liste **Auszuführenden Test auswählen** die Option **Diagnosetest**.
3. Wählen Sie den Diagnosetest aus, den Sie ausführen möchten. Klicken Sie auf **Alles auswählen**, um alle Tests auszuwählen, oder auf **Alle abwählen**, um die gesamte Testauswahl zu löschen.
4. Wählen Sie unter **Anzahl der Schleifen** aus, wie oft die Tests ausgeführt werden sollen.
5. Klicken Sie auf **Test ausführen**.
6. Klicken Sie im Fenster mit der Fehlerwarnung, die darauf hinweist, dass die Netzwerkverbindung zeitweilig unterbrochen wird, auf **Ja**. Die Ergebnisse für jeden Test werden im Feld **Ergebnis** angezeigt.

Kontrollregister. Mit diesem Test wird die Schreib- und Lesefunktion für die Register des Netzwerkadapters überprüft, indem verschiedene Werte in die Register geschrieben und die Ergebnisse kontrolliert werden. Der Adaptertreiber verwendet diese Register, um Netzwerkfunktionen wie z. B. das Senden und Empfangen von Informationen auszuführen. Ein fehlgeschlagener Test weist darauf hin, dass der Adapter u. U. nicht ordnungsgemäß funktioniert.

MII-Register. Mit diesem Test wird die Schreib- und Lesefunktion der Register der physischen Schicht (PHY) überprüft. Mit der physischen Schicht werden die elektrischen Signale in der Leitung und für die Konfiguration von Netzwerk-Übertragungsraten wie 1000 Mbit/s gesteuert.

EEPROM. Mit diesem Test wird der Inhalt des EEPROMs überprüft, indem ein Teil des EEPROMs ausgelesen und die Prüfsumme berechnet wird. Wenn sich die berechnete Prüfsumme von der im EEPROM gespeicherten Prüfsumme unterscheidet, wurde der Test nicht bestanden. Für diesen Test ist kein Codewechsel bei einer Aktualisierung des EEPROM-Inhalts erforderlich.

Interner Speicher. Mit diesem Test wird überprüft, ob der interne Speicher des Adapters ordnungsgemäß funktioniert. Dazu werden Werte nach einem bestimmten Muster in den Speicher geschrieben und dann die Ergebnisse wieder ausgelesen. Wenn ein Wert beim Auslesen falsch ist, wurde dieser Test nicht bestanden. Der Adapter kann nicht funktionieren, wenn der interne Speicher nicht ordnungsgemäß funktioniert.

Chip-CPU. Mit diesem Test wird die Funktion der internen CPUs im Adapter überprüft.

Interrupt. Mit diesem Test wird überprüft, ob der NDIS-Treiber Interrupts vom Adapter empfangen kann.

MAC-Prüfschleife. Dieser Test überprüft, ob der NDIS-Treiber Pakete senden und vom Adapter empfangen kann.

PHY-Prüfschleife. Dieser Test überprüft, ob der NDIS-Treiber Pakete senden und vom Adapter empfangen kann.

LED-Test. Bei diesem Test blinken alle Port-LEDs zum Identifizieren des Adapters fünfmal auf.

Analysieren von Kabeln

Mit der Option **Kabelanalyse** auf der Registerkarte **Diagnose** können Sie den Zustand der Kabelpaare in einer Kabelverbindung über Ethernet Kategorie 5 innerhalb eines Ethernet-Netzwerks überwachen. Bei dieser Analyse wird die Kabelqualität gemessen und auf Übereinstimmung mit IEEE-Standard 802.3ab überprüft.

HINWEISE:

- Sie müssen über Administratorrechte verfügen, um den Kabelanalysetest ausführen zu können.
- Die Netzwerkverbindung wird während der Analyse vorübergehend unterbrochen.
- Bei Broadcom NetXtreme-Adaptern kann der Kabelanalysetest nur für Verbindungen mit Gigabit-Übertragungsraten durchgeführt werden und wenn keine Verbindung besteht.
- Diese Option ist nicht für alle Broadcom-Netzwerkadapter verfügbar.

So führen Sie eine Kabelanalyse aus:

1. Schließen Sie das Kabel an den Anschluss eines Switch an, bei dem der Anschluss auf **Auto** sowie die Treibereinstellungen für Übertragungsrate und Duplex auf **Auto** eingestellt sind.
2. Klicken Sie im Fenster "Explorer-Ansicht" auf den Namen des zu testenden Adapters.
3. Wählen Sie aus der Liste **Auszuführenden Test auswählen** die Option **Kabelanalyse**. Wenn die Option **Kabelanalyse** nicht zur Verfügung steht, wählen Sie auf der rechten Seite des Fensters auf der Registerkarte **Kontextansicht** die Option **Diagnose** und anschließend **Kabelanalyse**.
4. Klicken Sie auf **Ausführen**.
5. Klicken Sie im Fenster mit der Fehlerwarnung, die darauf hinweist, dass die Netzwerkverbindung zeitweilig unterbrochen wird, auf **Ja**.

Länge. Die gültige Kabellänge in Metern (außer wenn das Ergebnis Rauschen ausgegeben wird).

Status. Dies zeigt den Link-Typ dieses Kabelpaars an.

- **Gut**: Gute Kabel/PCB-Signalpfade, aber keine Gigabit-Verbindung.
- **Überlagert**: Kurze Pin oder Überlagerung entlang mindestens zweier Kabel/PCB-Signalpfade.
- **Offen**: Eines oder beide Pins sind für ein TP-Kabel offen.
- **Kurz**. Zwei Pins desselben TP-Kabels sind gekürzt.
- **Rauschen**: Dauerhaftes Rauschen (wahrscheinliche Ursache: 10/100).
- **GB-Verbindung**: Funktionierende Gigabit-Verbindung aktiv.
- **k.A**. Der Algorithmus konnte kein Ergebnis erzielen.

Verknüpfung. Die Verbindungsgeschwindigkeit und der Duplexmodus.

Status. Der Status nach Ausführen des Tests (abgeschlossen oder fehlgeschlagen).

Die Testergebnisse können von mehreren Faktoren beeinflusst werden:

- **Verbindungspartner**. Verschiedene Switch- und Hub-Hersteller implementieren unterschiedliche PHYs. Einige PHYs sind nicht IEEE-kompatibel.
- **Kabelqualität**. Die Testergebnisse können durch Kabel der Kategorie 3, 4, 5 und 6 beeinflusst werden.
- **Elektrische Störung**. Die Testergebnisse können von der Testumgebung beeinflusst werden.

Einstellen der Adaptereigenschaften

Über die Option **Erweitert** auf der Registerkarte **Konfigurationen** können Sie Werte der verfügbaren Eigenschaften des ausgewählten Adapters anzeigen und ändern. Die potenziell verfügbaren Eigenschaften sowie ihre entsprechenden Einstellungen werden im Folgenden beschrieben.

HINWEISE:

- Sie müssen über Administratorrechte verfügen, um die Werte einer Eigenschaft ändern zu können.
- Die Liste der verfügbaren Eigenschaften für Ihren Adapter kann unterschiedlich ausfallen.
- Manche Eigenschaften sind möglicherweise nicht für alle Netzwerkadapter von Broadcom verfügbar.

So legen Sie die Adaptereigenschaften fest

1. Klicken Sie im Fenster "Explorer-Ansicht" auf den Namen des Adapters, und wählen Sie dann die Registerkarte **Konfigurationen** aus.
2. Wählen Sie im Bereich **Erweitert** die Eigenschaft aus, die Sie einstellen möchten.
3. Um den Wert einer Eigenschaft zu ändern, wählen Sie ein Element aus der Eigenschaftsliste aus, oder geben Sie einen neuen Wert ein. (Die Auswahloptionen variieren je nach Eigenschaft.)
4. Klicken Sie auf **Übernehmen**, um die Änderungen an allen Eigenschaften zu bestätigen. Klicken Sie auf **Zurücksetzen**, um die Eigenschaften auf ihre Ursprungswerte zurückzusetzen.

802.1p QOS (Dienstgüte): Diese Eigenschaft aktiviert die *Dienstgüte* (QoS) Hierbei handelt es sich um eine Spezifikation des IEEE (*Institute of Electrical and Electronics Engineers*), die verschiedene Netzwerkauslastungsarten unterschiedlich behandelt, um den erforderlichen Zuverlässigkeits- und Latenzanforderungen gemäß der jeweiligen Netzwerkauslastungsart zu entsprechen. Diese Eigenschaft ist standardmäßig deaktiviert. Aktivieren Sie diese Eigenschaft nur, wenn die Netzwerkinfrastruktur QoS unterstützt. Andernfalls können Probleme auftreten.

Flow Control (Flusskontrolle):. Aktiviert und deaktiviert den Empfang oder die Übertragung von PAUSE Frames. Mit PAUSE Frames können der Netzwerkadapter und ein Switch die Übertragungsrate steuern. Diejenige Seite, die den PAUSE Frame empfängt, unterbricht für einen Augenblick die Übertragung.

- **Auto** (Standard): Der Empfang und die Übertragung von PAUSE-Rahmen werden optimiert.
- **Disable** (Deaktivieren): Der Empfang und die Übertragung von PAUSE-Rahmen werden deaktiviert.
- **Rx PAUSE**: Der Empfang von PAUSE-Rahmen wird aktiviert.
- **Rx/Tx PAUSE**: Der Empfang und die Übertragung von PAUSE-Rahmen werden aktiviert.
- **Tx PAUSE**: Die Übertragung von PAUSE-Rahmen wird aktiviert.

Speed & Duplex (Übertragungsrate und Duplexmodus). Mit der Eigenschaft **Speed & Duplex** (Übertragungsrate und Duplexmodus) werden die Übertragungsrate und der Modus dem Netzwerk angepasst. Hinweis: Im Vollduplex-Modus kann der Adapter Netzwerkdaten gleichzeitig übertragen und empfangen.

- **10 Mb Full** (10 MB Voll): Legt eine Übertragungsrate von 10 Mbit/s und den Vollduplex-Modus fest.

- **10 Mb Half** (10 MB Halb): Legt eine Übertragungsrate von 10 Mbit/s und den Halbduplex-Modus fest.
- **100 Mb Full** (100 MB Voll): Legt eine Übertragungsrate von 100 Mbit/s und den Vollduplex-Modus fest.
- **100 Mb Half** (100 MB Halb): Legt eine Übertragungsrate von 100 Mbit/s und den Halbduplex-Modus fest.
- **Auto** (Standard): Stellt die Übertragungsrate und den Modus auf die optimale Netzwerkverbindung ein (empfohlen).

HINWEISE:

- Die empfohlene Einstellung ist Auto (Standard). Bei dieser Einstellung kann der Netzwerkadapter die Übertragungsrate des Netzwerks dynamisch erkennen. Sollte sich die Übertragungsleistung des Netzwerks ändern, erkennt der Netzwerkadapter dies automatisch und stellt die neue Übertragungsrate und den Duplexmodus ein. Durch die Auswahl von Auto wird eine Übertragungsrate von 1 GBit/s aktiviert, wenn diese unterstützt wird.
- "1 Gb Full Auto" muss an einen Verbindungspartner angeschlossen werden, der ebenfalls eine Verbindung von 1 GBit/s verarbeiten kann. Da die Verbindung ausschließlich mit 1 GBit/s arbeitet, wird die Funktion "Ethernet@Wirespeed" deaktiviert. Wenn der Verbindungspartner ausschließlich eine Verbindung mit 1 GBit/s unterstützt, funktioniert die Funktion "Wake on LAN" möglicherweise nicht. Bei Nichtvorhandensein eines Betriebssystems kann zusätzlich der Verwaltungsdatenverkehr beeinträchtigt werden.
- Mit den Einstellungen **10 Mb Half** (10 MB Halb) und **100 Mb Half** (100 MB Halb) wird der Netzwerkadapter gezwungen, eine Verbindung mit dem Netzwerk im Halbduplex-Modus herzustellen. Beachten Sie, dass der Netzwerkadapter u. U. nicht funktioniert, wenn die Konfiguration des Netzwerks nicht auf den gleichen Modus eingestellt ist.
- Mit den Einstellungen **10 Mb Full** (10 MB Voll) und **100 Mb Full** (100 MB Voll) wird der Netzwerkadapter gezwungen, eine Verbindung mit dem Netzwerk im Vollduplex-Modus herzustellen. Wenn die Konfiguration des Netzwerks nicht auf den gleichen Modus eingestellt ist, funktioniert der Netzwerkadapter u. U. nicht.

Wake Up Capabilities (Reaktivierungsfunktion): Ermöglicht es dem Netzwerkadapter, aus einem Bereitschaftsmodus aufzuwachen, wenn er einen Wake Up Frame aus dem Netzwerk empfängt. Die folgenden zwei Arten von Reaktivierungsrahmen sind möglich: Magic Packet und Wake Up Frame.

Diese Eigenschaft steht nur für Broadcom NetXtreme-Adapter zur Verfügung.

- **Both** (Beide) (Standard): Mit dieser Einstellung werden sowohl **Magic Packet** als auch **Wake Up Frame** als Wake Up Frame aktiviert.
- **Magic Packet**: Mit dieser Einstellung wird **Magic Packet** als Wake Up Frame aktiviert.
- **None** (Ohne): Es wird kein Wake Up Frame ausgewählt.
- **Wake Up Frame**: Mit dieser Einstellung wird Wake Up Frame als Wake Up Frame aktiviert. Der Netzwerkadapter kann das System reaktivieren, wenn Ereignisse, wie beispielsweise Ping- oder ARP-Anforderungen (*Address Resolution Protocol*), empfangen werden. Diese Option ist an den Stromsparmodus des Betriebssystems gekoppelt und funktioniert nicht, wenn die Eigenschaft **WOL Speed** (WOL-Übertragungsrate) im **Energiesparmodus** nicht aktiviert wird.

Priorität und VLAN. Aktiviert die Priorisierung des Netzwerkverkehrs sowie die VLAN-Markierung. Die VLAN-Markierung erfolgt nur, wenn für die Einstellung **VLAN ID** (VLAN-ID) ein anderer Wert als 0 (null) konfiguriert wurde.

- **Priority & VLAN Enabled** (Priorität und VLAN aktiviert) (Standard): Ermöglicht die Paketpriorisierung und VLAN-Markierung.
- **Priority & VLAN Disabled** (Priorität und VLAN deaktiviert) (Standard): Verhindert die Paketpriorisierung und VLAN-Markierung.
- **Priorität aktiviert**: Lässt nur die Paketpriorisierung zu.
- **VLAN aktiviert**: Lässt nur die VLAN-Markierung zu.

Hinweis: Wenn der Netzwerkadapter für die VLAN-Markierung von einem Intermediate-Treiber verwaltet wird, sollten die Einstellungen **Priorität und VLAN deaktiviert** und **Priorität aktiviert** nicht verwendet werden. Verwenden Sie die Einstellung **Priorität und VLAN aktiviert**, und ändern Sie die **VLAN-ID** in 0 (null).

VLAN-ID. Aktiviert die VLAN-Markierung und konfiguriert die VLAN-ID, wenn **Priorität und VLAN aktiviert** als **Priorität & VLAN-Einstellung** ausgewählt wurde. Die VLAN-ID kann ein Wert zwischen 1 und 4094 sein und muss mit dem VLAN-Tag-Wert auf dem angeschlossenen Switch identisch sein. Mit dem Wert "0" (Standard) in diesem Feld wird die VLAN-Markierung deaktiviert.

Risikobewertung der VLAN-Markierung durch den NDIS Miniport-Treiber

Der NDIS 6.0 Miniport-Treiber von Broadcom ermöglicht die Verbindung eines Systems mit Broadcom-Adapter mit einem markierten VLAN. Im Gegensatz zu BASP unterstützt der NDIS 6.0-Treiber nur eine VLAN-ID für die VLAN-Teilnahme.

Außerdem ermöglicht der NDIS 6.0-Treiber im Gegensatz zu BASP nur die VLAN-Markierung des ausgehenden Pakets, jedoch keine Filterung eingehender Pakete nach VLAN-ID-Mitgliedschaft. Dies ist das Standardverhalten aller Miniport-Treiber. Während die fehlende Filterung von Paketen nach VLAN-Mitgliedschaft ein Sicherheitsrisiko darstellen kann, bietet folgende Möglichkeit eine Risikoabschätzung auf der Basis dieser Treibereinschränkung für ein IPv4-Netzwerk:

Ein ordnungsgemäß konfiguriertes Netzwerk mit mehreren VLANs sollte für jedes VLAN über separate IP-Segmente verfügen. Der Grund dafür ist, dass die Routing-Tabelle festlegt, über welchen Adapter (virtuell oder physisch) der ausgehende Datenverkehr geleitet wird, und die Adapterwahl nicht auf der Basis der VLAN-Mitgliedschaft getroffen wird.

Da sich die Unterstützung der VLAN-Markierung auf dem NDIS 6.0-Treiber von Broadcom auf den gesendeten Datenverkehr beschränkt, besteht die Gefahr, dass eingehender Datenverkehr von einem anderen VLAN an das Betriebssystem weitergeleitet wird. Ist jedoch das Netzwerk ordnungsgemäß konfiguriert, können die IP-Segmentierung und/oder die VLAN-Switch-Konfiguration eine zusätzliche Filterung bieten, um das Risiko zu begrenzen.

In einem Back-to-Back-Verbindungsszenario können zwei Computer im selben IP-Segment ungeachtet ihrer VLAN-Konfiguration kommunizieren, da keine Filterung nach VLAN-Mitgliedschaft erfolgt. Dieses Szenario setzt jedoch voraus, dass die Sicherheit bereits verletzt wurde, da dieser Verbindungstyp in VLAN-Umgebungen untypisch ist.

Wenn dieses Risiko ausgeschlossen werden soll und eine Filterung nach VLAN-ID-Mitgliedschaft notwendig ist, ist die Unterstützung durch einen Intermediate-Treiber erforderlich.

Anzeigestatistik

Mit den Informationen auf der Registerkarte **Statistik** können Sie sich über die Datenverkehrsstatistiken für Broadcom Netzwerkadapter und die Adapter anderer Hersteller informieren. Bei den Broadcom-Adaptern werden im Vergleich zu Fremdgeräten erheblich mehr statistische Daten angezeigt.

Zum Anzeigen der Statistikinformationen für einen beliebigen installierten Netzwerkadapter klicken Sie auf den Namen des Adapters, der im Fenster "Explorer-Ansicht" aufgeführt ist. Klicken sie dann auf die Registerkarte "Statistik".

Klicken Sie auf **Aktualisieren**, um die neuestens Werte für die Statistiken anzuzeigen. Klicken Sie auf **Zurücksetzen**, um alle Werte auf Null zu setzen.

HINWEISE:

- Die Teamstatistik für ein Broadcom-Netzwerkadapter wird nicht kompiliert, wenn dieses deaktiviert ist.
- Einige Statistiken sind möglicherweise nicht für alle Broadcom-Netzwerkadapter verfügbar.

Allgemeine Statistik

Die allgemeine Statistik gibt die übermittelten und empfangenen Statistiken vom und zum Adapter an.

Frames Tx OK. Anzahl der Frames, die erfolgreich übertragen wurden. Bei erfolgreicher Übertragung wird der Zähler um eins erhöht.

Frames Rx OK. Anzahl der Frames, die erfolgreich empfangen wurden. Nicht berücksichtigt werden zu lange Frames, Frames mit Frame-Prüfsummen- (FCS), Längen- oder Ausrichtungsfehlern, oder Frames, die aufgrund von internen MAC-Teilschichtfehlern verloren gegangen sind. Bei erfolgreichem Empfang wird der Zähler um eins erhöht.

Gerichtete Frames Tx. Anzahl der gerichteten Daten-Frames, die erfolgreich übertragen wurden.

Multicast Frames Tx. Anzahl der Frames, die erfolgreich an eine andere Gruppenzieladresse als die Broadcast-Adresse übertragen wurden.

Broadcast Frames Tx. Anzahl der Frames, die erfolgreich an die Broadcast-Adresse übertragen wurden. Frames, die an Multicast-Adressen übertragen werden, sind keine Broadcast-Frames und werden daher ausgeschlossen.

Gerichtete Frames Rx. Anzahl der gerichteten Daten-Frames, die erfolgreich empfangen wurden.

Multicast Frames Rx. Anzahl der Frames, die erfolgreich empfangen und an eine aktive Nicht-Broadcast-Gruppenadresse gerichtet wurden. Nicht berücksichtigt werden zu lange Frames, Frames mit FCS-, Längen- oder Ausrichtungsfehlern, oder Frames, die aufgrund von internen MAC-Teilschichtfehlern verloren gegangen sind. Bei erfolgreichem Empfang wird der Zähler um eins erhöht.

Broadcast Frames Rx. Anzahl der Frames, die erfolgreich empfangen und an eine Broadcast-Gruppenadresse gerichtet wurden. Nicht berücksichtigt werden zu lange Frames, Frames mit FCS-, Längen- oder Ausrichtungsfehlern, oder Frames, die aufgrund von internen MAC-Teilschichtfehlern verloren gegangen sind. Bei erfolgreichem Empfang wird der Zähler um eins erhöht.

Frames Rx mit CRC-Fehler. Anzahl der Frames, die mit CRC-Fehlern empfangen wurden.

Konfigurieren der Teaming-Funktion

Mit der Teaming-Funktion können Sie beliebige verfügbare Netzwerkadapter zu einem Team zusammenfassen. Mit der Teaming-Funktion kann ein virtuelles NIC erstellt werden (eine Gruppe aus mehreren Adaptern wird zu einem Adapter zusammengefasst). Der Vorteil davon ist, dass dadurch **Load Balancing** (Lastausgleich) und **Failover** (Ausfallsicherung) aktiviert werden. Teaming erfolgt über die BASP-Software (Broadcom Advanced Server Program). Eine umfangreiche Beschreibung der zu berücksichtigenden Technologie und Implementierung der Teaming-Software finden Sie im Benutzerhandbuch Ihres Broadcom-Netzwerkadapters im Abschnitt "Broadcom Gigabit Ethernet Teaming Services".

Teaming kann mit einer der folgenden Methoden ausgeführt werden:

- Verwenden des Teaming-Assistenten von Broadcom
- Verwenden des Experten-Modus

HINWEISE:

- Weitere Informationen zu Teaming-Protokollen finden Sie im Benutzerhandbuch Ihres Broadcom-Netzwerkadapters unter "Teaming".
- Wenn Sie LiveLink™ beim Konfigurieren von Teams nicht aktivieren, wird empfohlen, das Spanning Tree Protocol (STP) auf dem Switch zu deaktivieren. Dadurch werden die Ausfallzeiten beim Failover auf Grund der Schleifen-Berechnung nach dem Spanning Tree-Algorithmus reduziert. Probleme dieser Art werden von LiveLink entschärft.
- BASP ist nur verfügbar, wenn in einem System ein oder mehrere Broadcom-Netzwerkadapter installiert sind.
- Die Eigenschaften für Large Send Offload (LSO) und Prüfsummenverschiebung (CO) werden nur dann für ein Team aktiviert, wenn alle Mitglieder diese Funktionen unterstützen und dafür konfiguriert wurden.
- Sie müssen über Administratorrechte verfügen, um Teams erstellen oder ändern zu können.
- Der Lastausgleichsalgorithmus bevorzugt in einer Teamumgebung, in der Mitglieder mit unterschiedlichen Übertragungsraten verbunden sind, bis zu einem bestimmten Schwellenwert diejenigen Mitglieder, die über eine Gigabit Ethernet-Verbindung verfügen, gegenüber den Mitgliedern, die über eine Verbindung mit niedrigeren Übertragungsraten (100 Mbit/s oder 10 Mbit/s) verfügen. Dieses Verhalten ist vollkommen normal.
- Mit Wake on LAN (WOL) kann der Ruhemodus eines Systems beendet werden, wenn ein bestimmtes Paket über die Ethernet-Schnittstelle eingeht. Da ein virtueller Adapter als reines Softwaregerät implementiert ist, fehlen ihm die Hardwarefunktionen zur Implementierung von WOL. Über einen virtuellen Adapter kann der Ruhemodus eines Systems deshalb nicht beendet werden. Die physischen Adapter hingegen unterstützen diese Eigenschaft auch dann, wenn sie Teil eines Teams sind.

Teamarten

Sie können vier Arten von Lastausgleichteams erstellen:

- "Smart Load Balance" und "Failover"
- Link Aggregation (802.3ad)
- Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static
- SLB (Auto-Fallback deaktiviert): Die Funktion **SLB (Auto-Fallback deaktiviert)** ist im Teaming-Assistenten für die Teamart **"Smart Load Balance" und "Failover"** konfiguriert.

Eine Beschreibung dieser Datentypen finden Sie unter "Lastausgleich und Fehlertoleranz" im *Broadcom® NetXtreme® BCM57xx-Benutzerhandbuch*.

Verwenden des Teaming-Assistenten von Broadcom

Sie können den Teaming-Assistenten von Broadcom verwenden, um ein Team zu erstellen, ein bestehendes Team zu konfigurieren, wenn bereits ein Team erstellt wurde, oder ein VLAN zu erstellen.

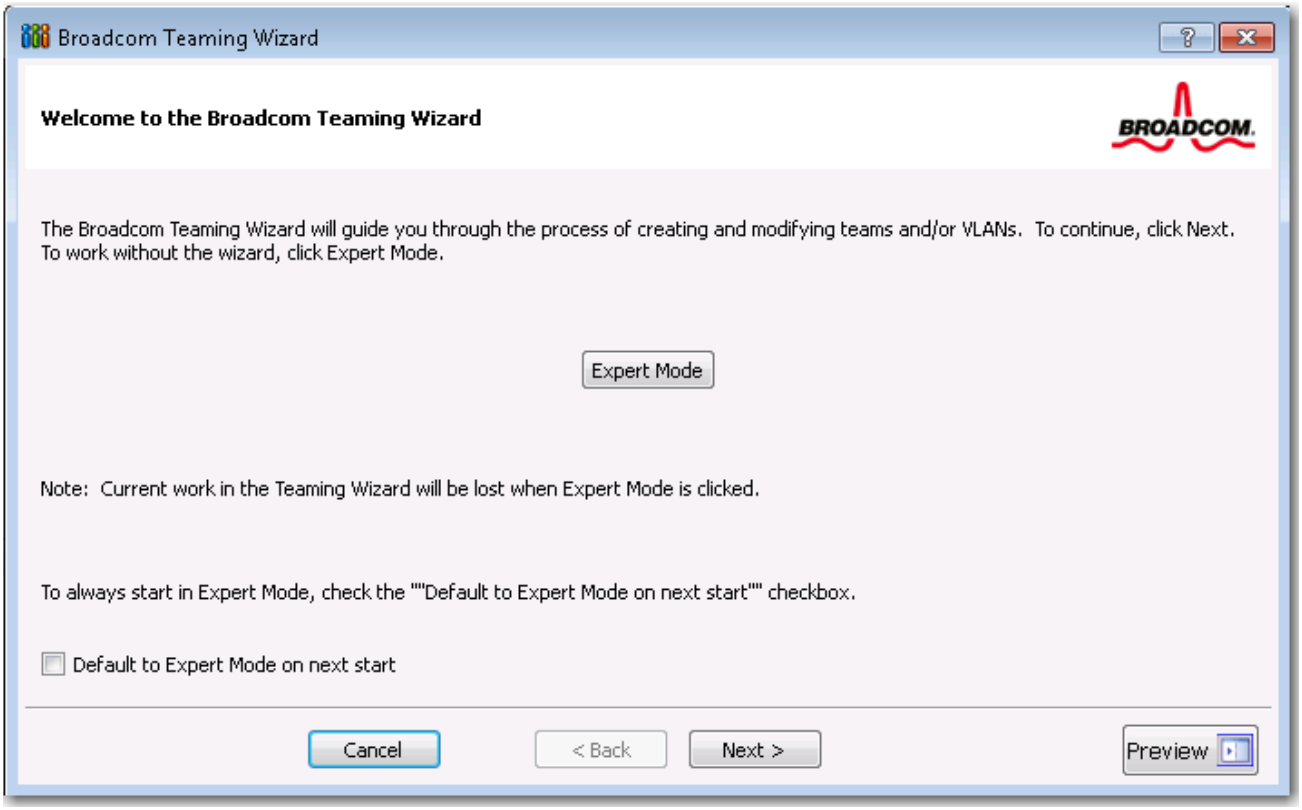
1. So erstellen oder bearbeiten Sie ein Team:

   Um ein neues Team zu erstellen, wählen Sie aus dem Menü **Team** die Option **Team erstellen**, oder klicken Sie mit der rechten Maustaste auf eine der Geräte im Bereich **Nicht zugewiesene Adapter**, und wählen Sie **Team erstellen**. Diese Option steht nicht zur Verfügung, wenn unter **Nicht zugewiesene Adapter** keine Geräte aufgeführt sind – was bedeutet, dass alle Adapter bereits in Teams gruppiert sind.

   Zum Konfigurieren eines vorhandenen Teams klicken Sie mit der rechten Maustaste auf eines der Teams in der Liste, und wählen Sie dann **Team bearbeiten** aus. Diese Option steht nur zur Verfügung, wenn bereits ein Team erstellt wurde, das im Fenster **Teamverwaltung** aufgeführt wird.

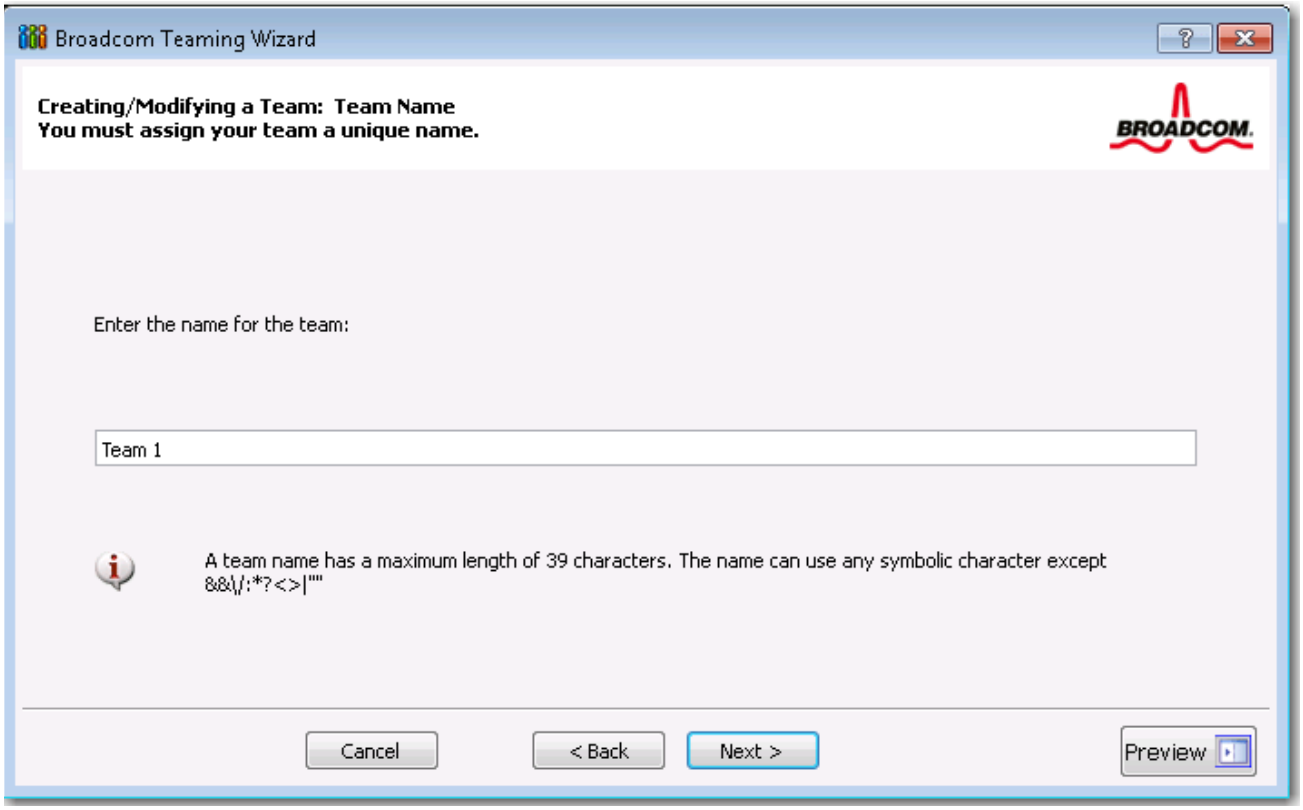
Hinweis: Wenn Sie zunächst ohne den Assistenten arbeiten möchten, klicken Sie auf **Experten-Modus**. Wenn Sie für die Erstellung eines Teams immer den Experten-Modus verwenden möchten, wählen Sie die Option **Beim Starten Experten-Modus**. Siehe Verwenden des Experten-Modus.

2. Klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren.

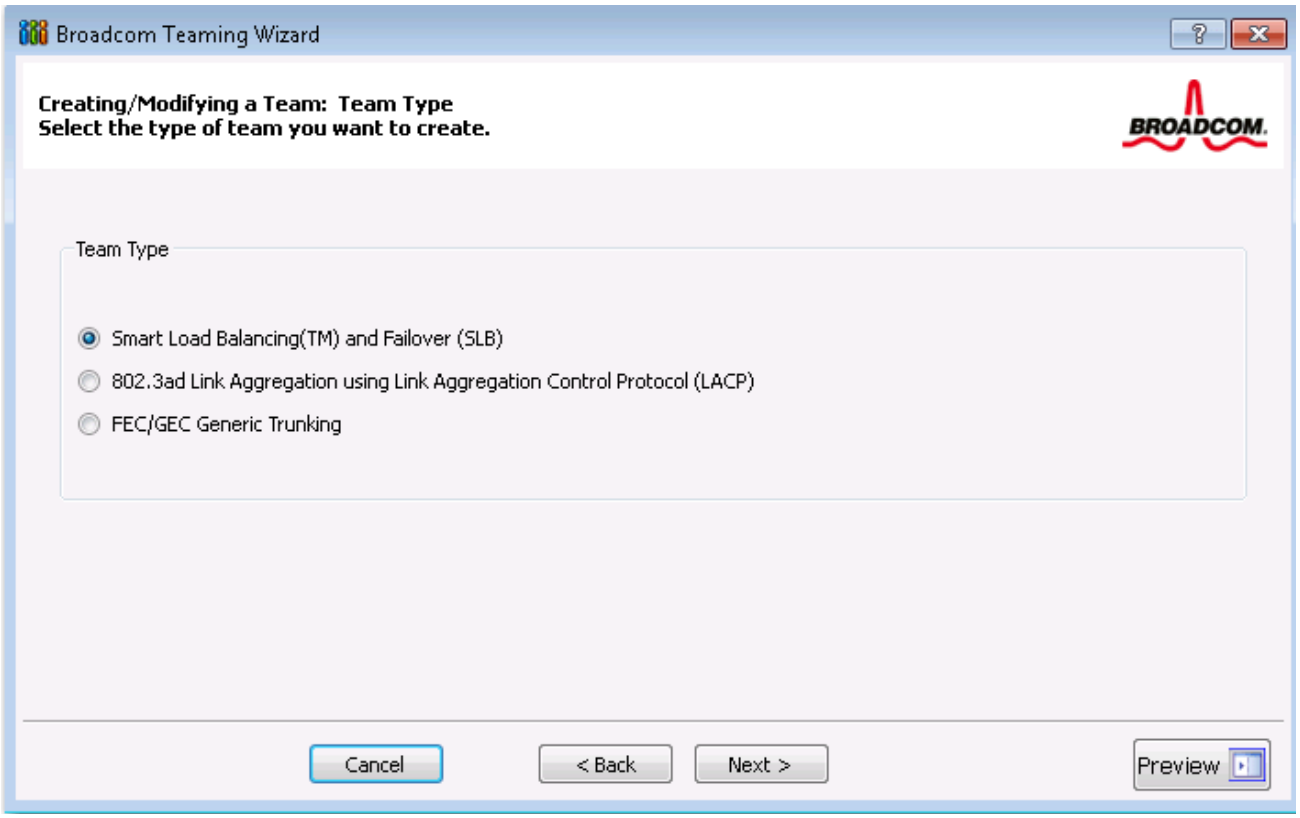


3. Geben Sie den Teamnamen ein, und klicken Sie auf **Weiter**. Wenn Sie eine Ihrer Einstellungen überprüfen oder ändern möchten, klicken Sie auf **Zurück**. Klicken Sie auf **Abbrechen**, um Ihre Einstellungen zu verwerfen und den Assistenten zu beenden.

Hinweis: Der Teamname darf maximal 39 Zeichen enthalten, er darf nicht mit einem Leerzeichen beginnen und keines der folgenden Zeichen enthalten: & \ / : * ? < > |



4. Wählen Sie die Teamart aus, die Sie erstellen möchten. Wenn es sich bei der Teamart um ein SLB-Team handelt, klicken Sie auf **Weiter**. Wenn es sich bei der Teamart nicht um ein SLB-Team handelt, wird ein Dialogfeld angezeigt. Stellen Sie sicher, dass die Konfiguration des Netzwerk-Switches, der mit den Teammitgliedern verbunden ist, für die Teamart korrekt ist, und klicken Sie auf **OK**, um fortzufahren.

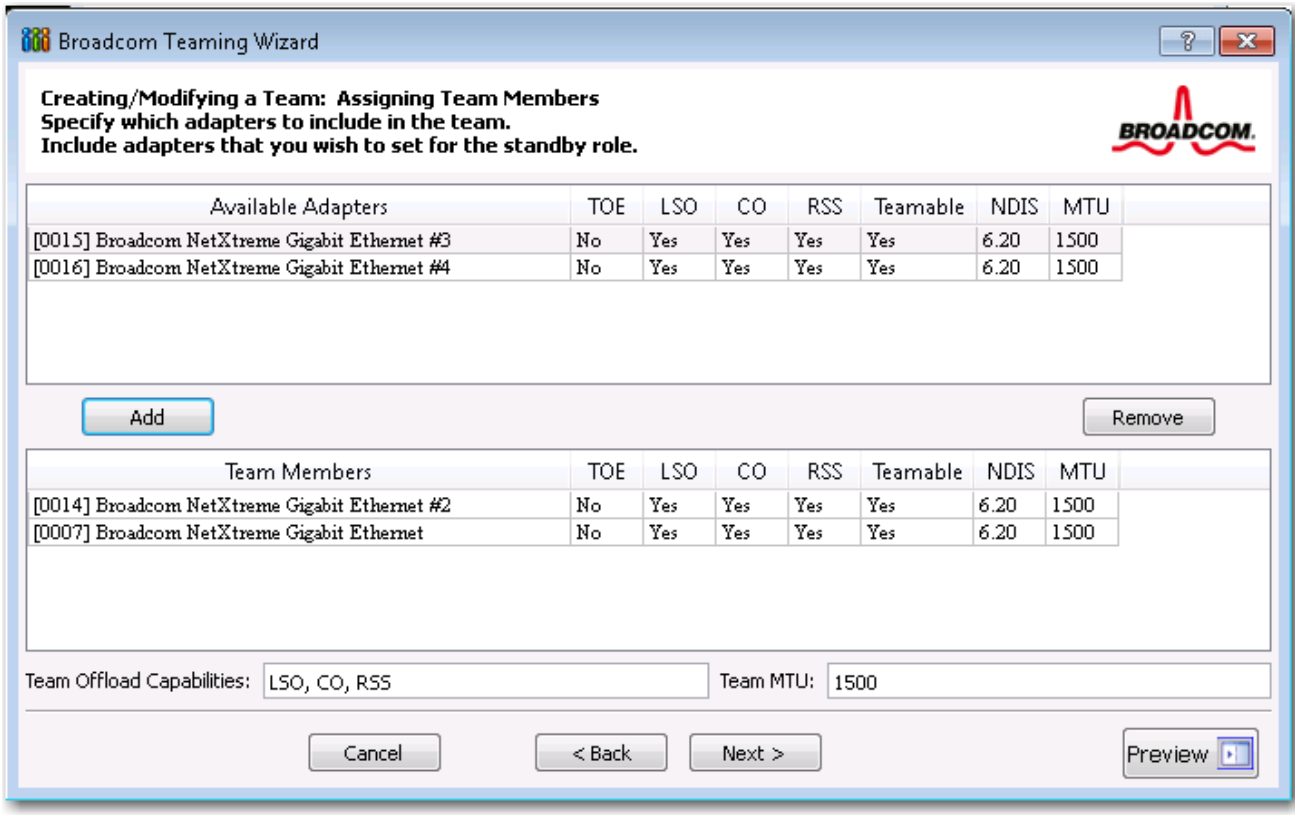


5. Klicken Sie in der Liste **Verfügbare Adapter** auf den Adapter, den Sie dem Team hinzufügen möchten, und klicken Sie anschließend auf **Hinzufügen**. Entfernen Sie Teammitglieder aus der Liste **Teammitglieder**, indem Sie auf den Adapter und dann auf **Entfernen** klicken. Klicken Sie auf **Weiter**.

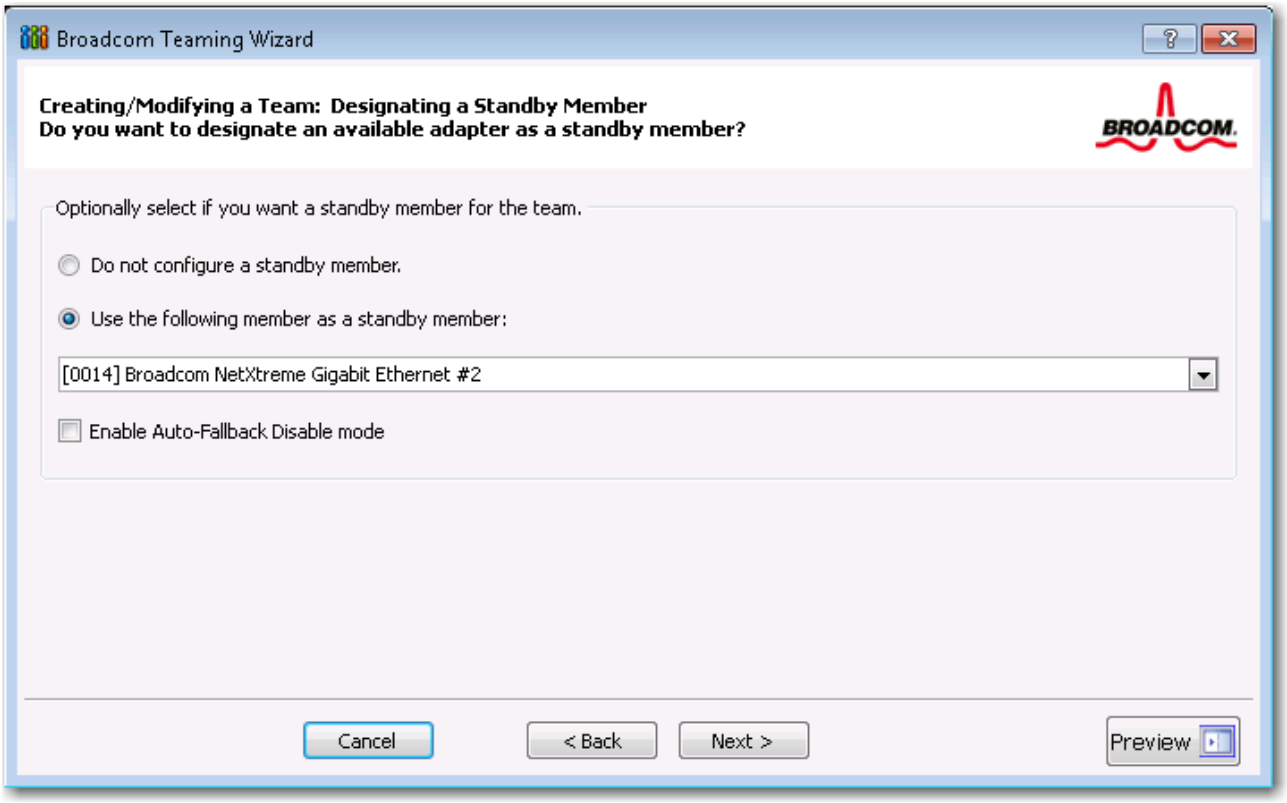
Hinweis: Dem Team muss mindestens ein Broadcom-Netzwerkadapter zugewiesen werden.

Die Spalten Large Send Offload (LSO) (Large Send-Verschiebung, LSO) und Checksum Offload (CO) (Prüfsummenverschiebung, CO) geben an, ob die LSO- und/oder die CO-Eigenschaften für den Adapter unterstützt werden. Die LSO- und CO-Eigenschaften werden nur dann für ein Team aktiviert, wenn alle Mitglieder die Funktion unterstützen und dafür konfiguriert wurden. Ist dies der Fall, wird die Offload-Fähigkeit des Teams unten im Bildschirm angezeigt.

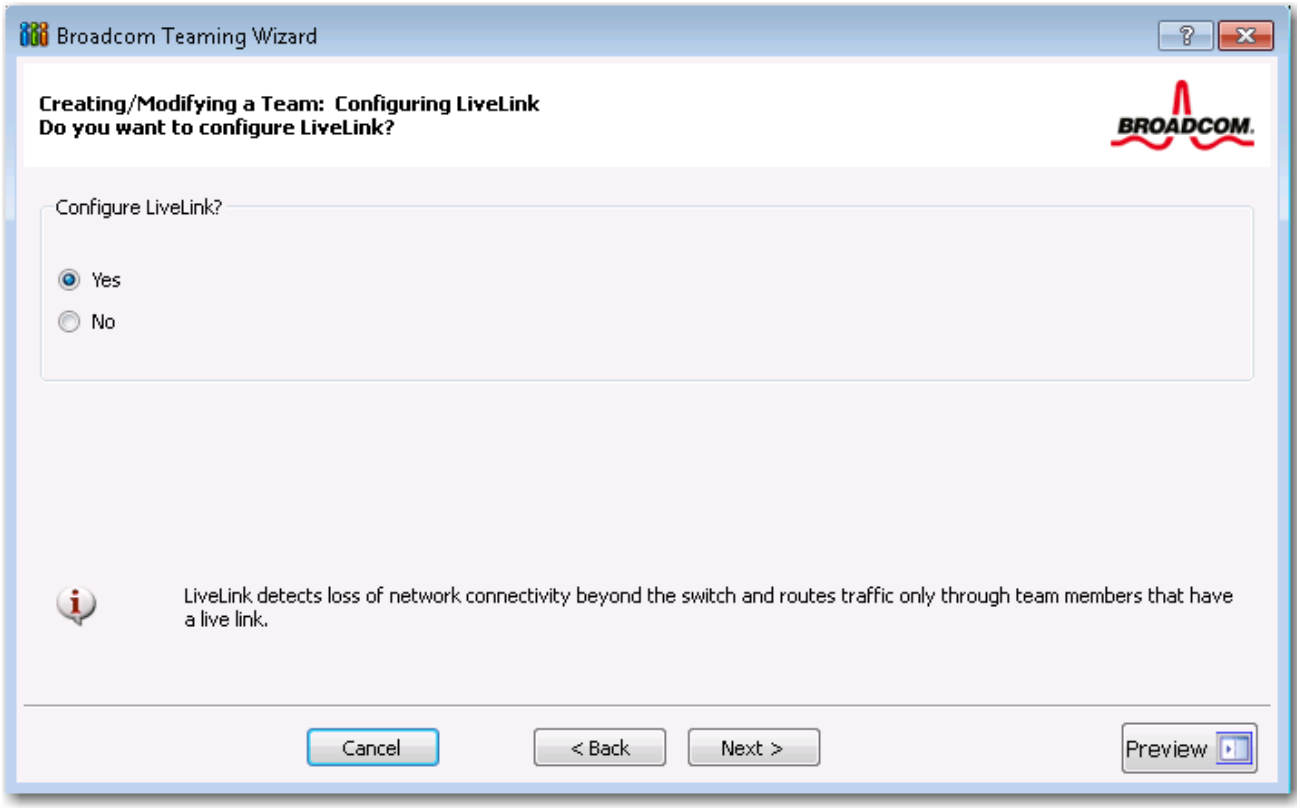
Hinweis: Wird einem Team ein Netzwerkadapter hinzugefügt, dessen Treiber deaktiviert ist, kann dies die Offload-Fähigkeit des Teams beeinträchtigen. Dies kann sich auf die Leistung des Teams auswirken. Aus diesem Grund ist es ratsam, nur Netzwerkadapter mit aktiviertem Treiber als Mitglieder eines Teams hinzuzufügen.



6. Wenn Sie einen der Adapter als Standby-Element festlegen möchten (optional), wählen Sie **Folgendes Element als Standby-Element verwenden**, und wählen Sie das Standby-Element aus der Adapterliste aus.
7. Im Modus **Auto-Fallback deaktiviert** kann das Team weiterhin das Standby-Element verwenden, statt auf das primäre Mitglied umzuschalten, wenn die Verbindung zum primären Mitglied wiederhergestellt wurde. Um diese Funktion zu aktivieren, wählen Sie **Modus "Auto-Fallback deaktiviert" aktivieren**. Klicken Sie auf **Weiter**.



8. Wenn Sie LiveLink konfigurieren möchten, wählen Sie **Ja**. Wählen Sie andernfalls **Nein**, und klicken Sie auf **Weiter**.



9. Legen Sie das Prüfintervall (die Dauer in Sekunden zwischen Übertragungen von Verbindungspaketen zum Prüfziel) und die maximale Anzahl an Prüfwiederholungen (die Anzahl von aufeinander folgenden fehlgeschlagenen Antworten eines Prüfziels, bevor ein Failover ausgelöst wird) fest.
10. Legen Sie die Prüf-VLAN-ID so fest, dass eine Anbindung an Prüfziele auf dem markierten VLAN möglich ist. Die festgelegte Zahl muss mit der VLAN-ID der Prüfziele sowie dem Anschluss/den Anschlüssen auf dem mit dem Team verbundenen Switch übereinstimmen.

Hinweis: Jedes für LiveLink aktivierte Team kann nur mit Prüfzielen auf einem einzigen VLAN kommunizieren. Die VLAN-ID 0 entspricht einem nicht markiertem Netzwerk. Wenn die Test-VLAN-ID auf einen anderen Wert als Null gesetzt ist, muss ein VLAN mit einem identischen VLAN-Tag-Wert erstellt werden (siehe Schritt 16.).

11. Klicken Sie am Anfang der Liste auf das Prüfziel und anschließend auf **Ziel-IP-Adresse bearbeiten**. Geben Sie im Feld **IP-Adresse** die Ziel-IP-Adresse eines oder aller Prüfziele ein, und klicken Sie auf **OK**. Klicken Sie auf **Weiter**.

Hinweis: Nur das erste Prüfziel wird benötigt. Sie können bis zu drei zusätzliche Prüfziele als Backups festlegen, indem Sie den anderen Prüfzielen IP-Adressen zuweisen.

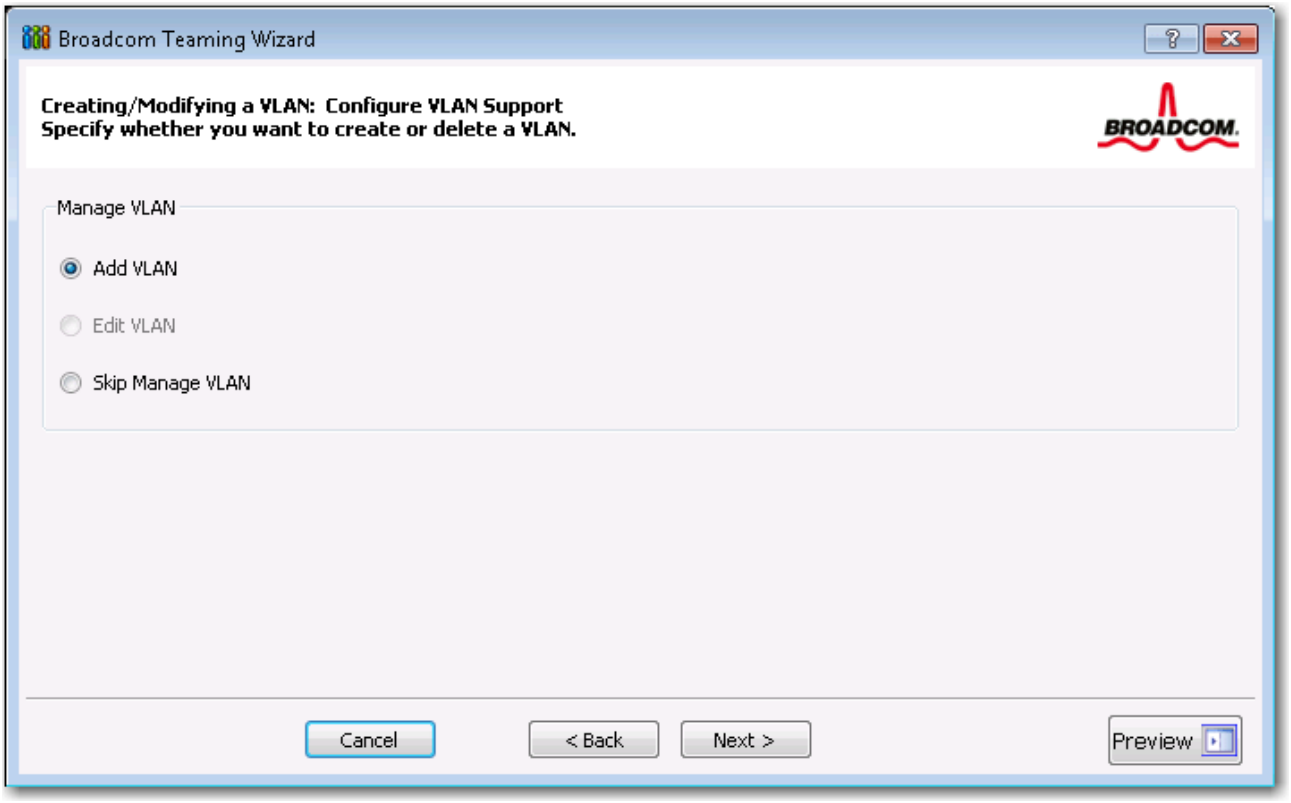
12. Wählen Sie eines der aufgeführten Teammitglieder aus, klicken Sie auf **Mitglieder-IP-Adresse bearbeiten**, und geben Sie in das Feld **IP-Adresse** die IP-Adresse des Mitglieds ein. Wiederholen Sie diesen Schritt für alle aufgeführten Teammitglieder, und klicken Sie auf **OK**. Klicken Sie auf **Weiter**.

Hinweis: Alle Mitglieder-IP-Adressen müssen demselben Subnetz angehören wie die Prüfziele.

13. Wenn Sie ein VLAN für das Team erstellen möchten, wählen Sie VLAN hinzufügen, oder, wenn Sie die Einstellungen eines vorhandenen VLAN ändern möchten, klicken Sie auf VLAN bearbeiten und dann auf Weiter. Wenn Sie kein VLAN erstellen oder bearbeiten möchten, wählen Sie VLAN-Verwaltung überspringen und Weiter, und fahren Sie auf dem Bildschirm Fertig stellen mit dem Assistenten fort (siehe Schritt 18. dieses Vorgangs).

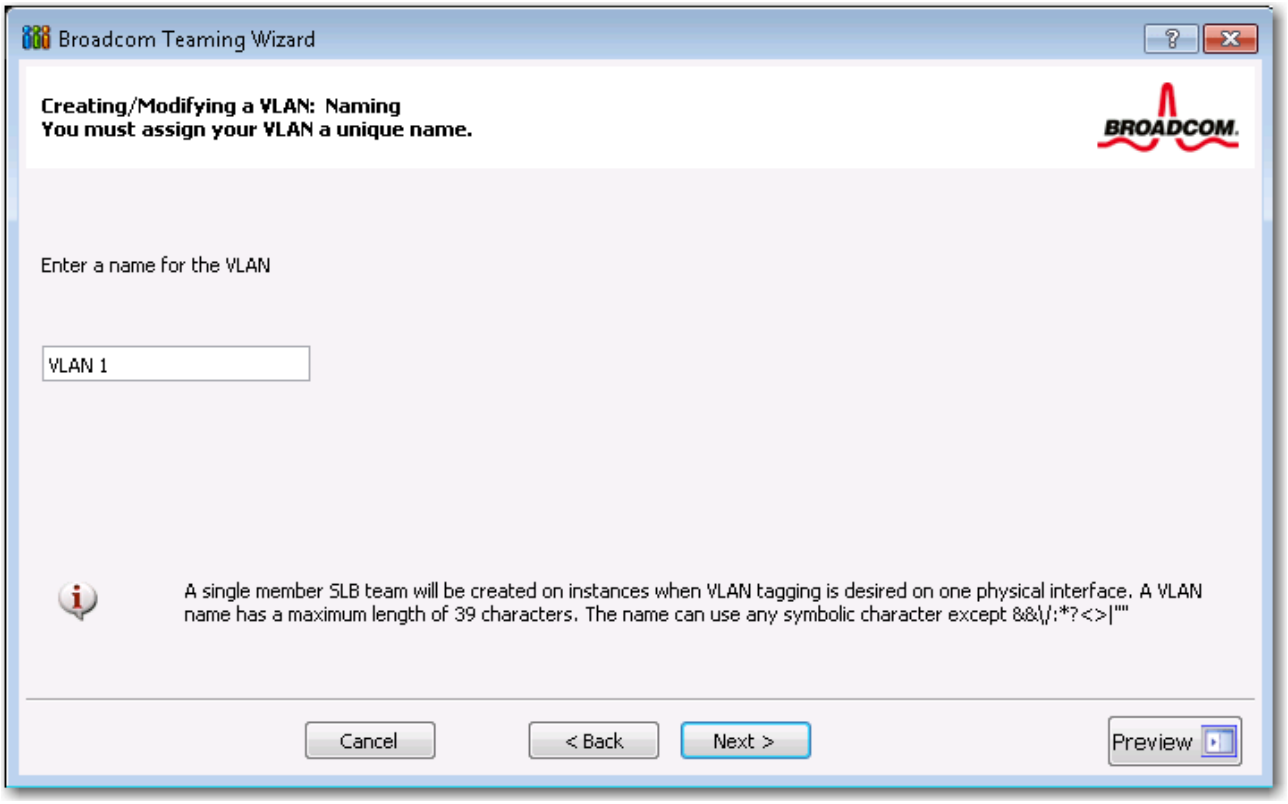
Mit VLANs können Sie mehrere virtuelle Adapter hinzufügen, die sich in verschiedenen Subnetzen befinden. Der Vorteil davon ist, dass das System über einen Netzwerkadapter verfügt, der zu mehreren Subnetzen gehört.

Hinweis: VLANs können nur dann erstellt werden, wenn alle Teammitglieder Broadcom-Adapter sind.

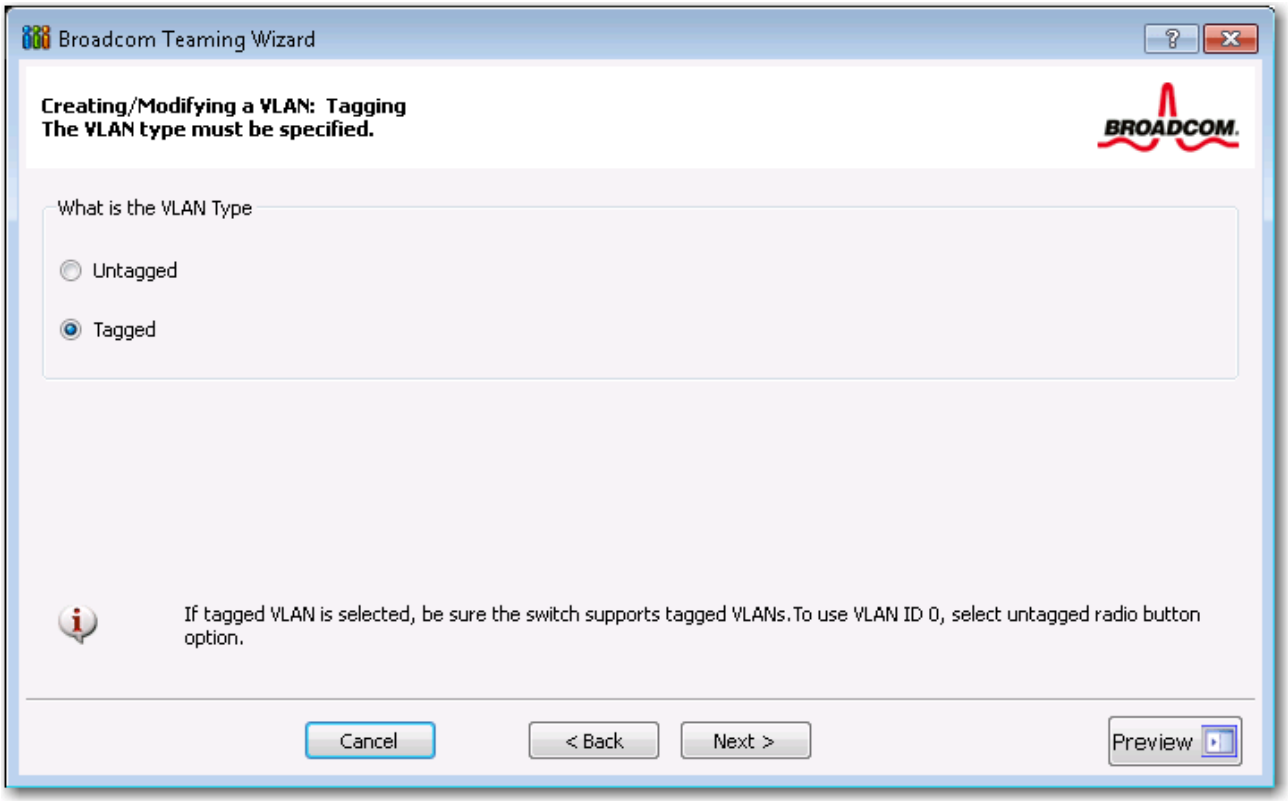


14. Geben Sie den VLAN-Namen ein, und klicken Sie auf **Weiter**.

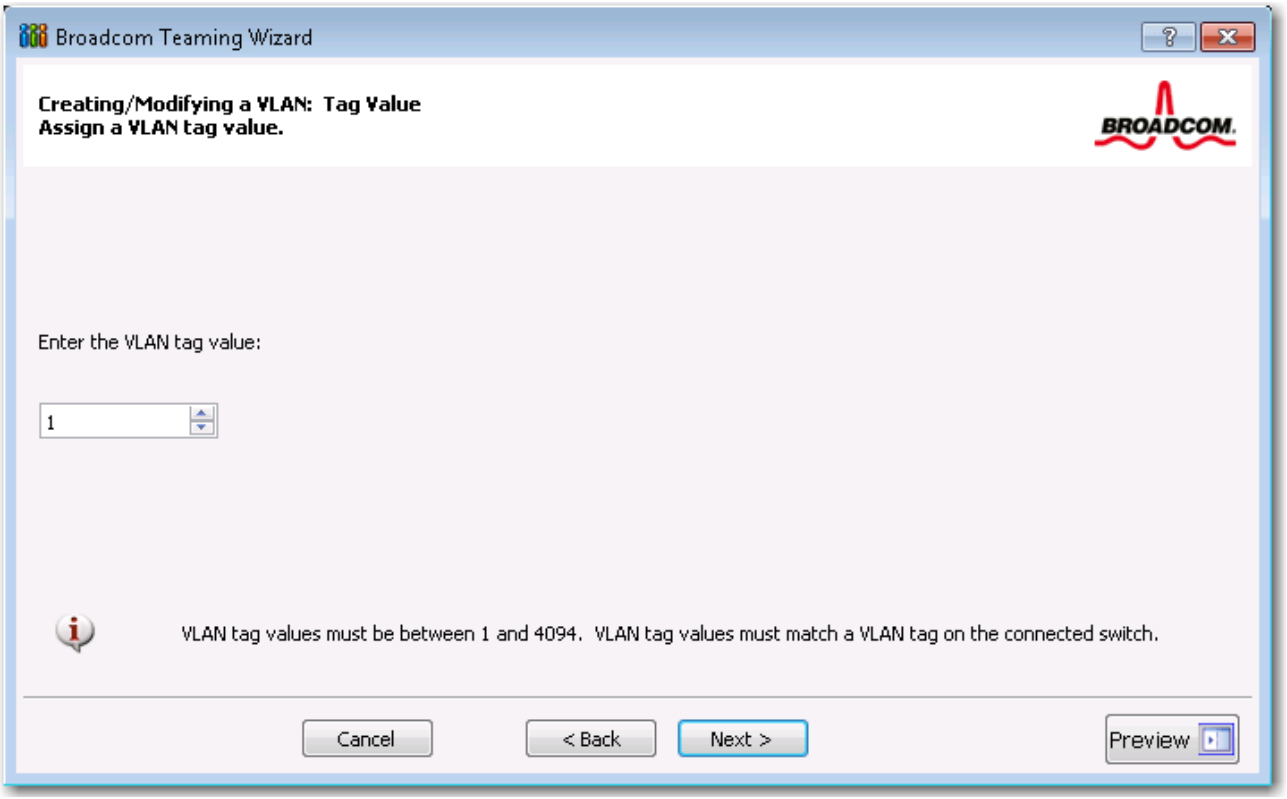
Hinweis: Der Teamname darf maximal 39 Zeichen enthalten, er darf nicht mit einem Leerzeichen beginnen und keines der folgenden Zeichen enthalten: & \ / : * ? < > |



15. Wählen Sie **Markiert**, um das VLAN zu markieren, und klicken Sie anschließend auf **Weiter**. Wählen Sie andernfalls **Unmarkiert**, klicken Sie auf **Weiter**, und fahren Sie mit dem Assistenten fort, um weitere VLANs hinzuzufügen (siehe Schritt 17. dieser Anleitung).



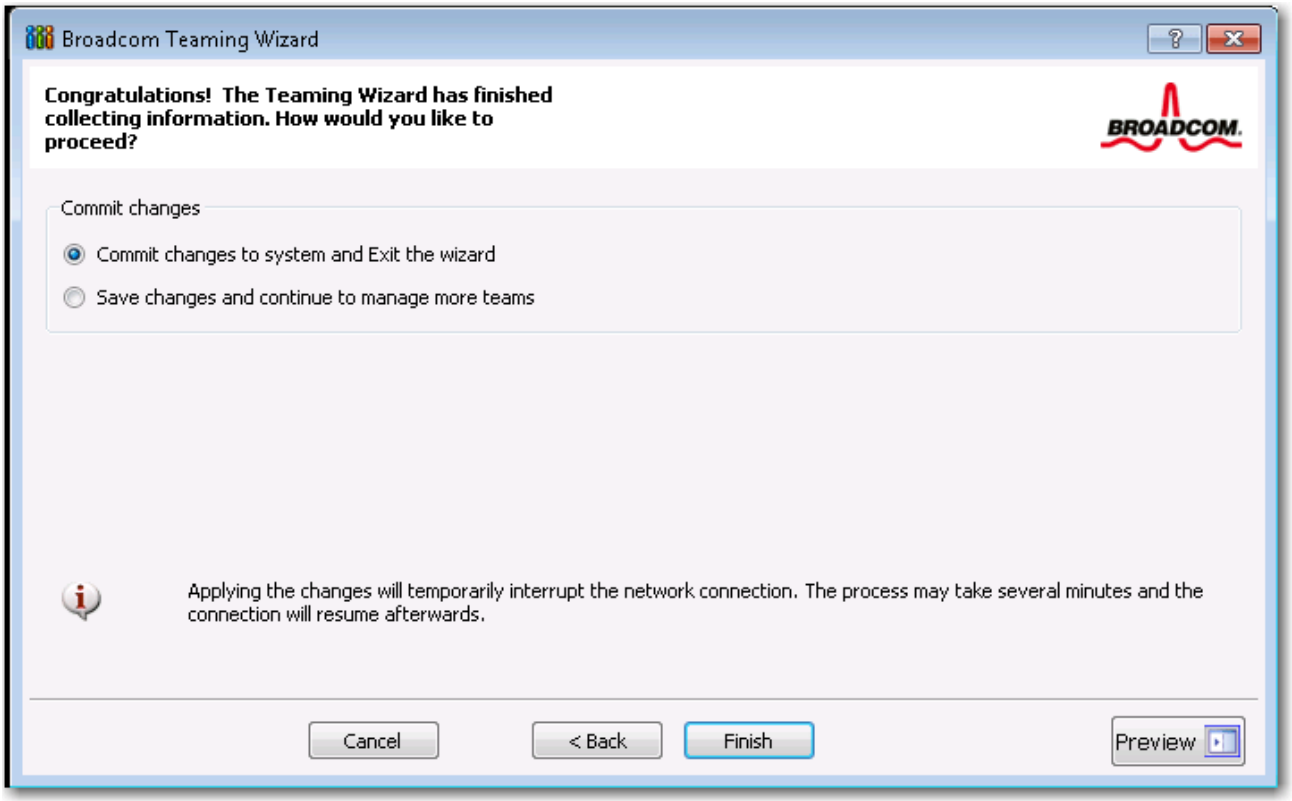
16. Geben Sie den VLAN-Tag-Wert für die Markierung ein, und klicken Sie auf **Weiter**. Der Wert muss eine Zahl zwischen 1 und 4094 sein.



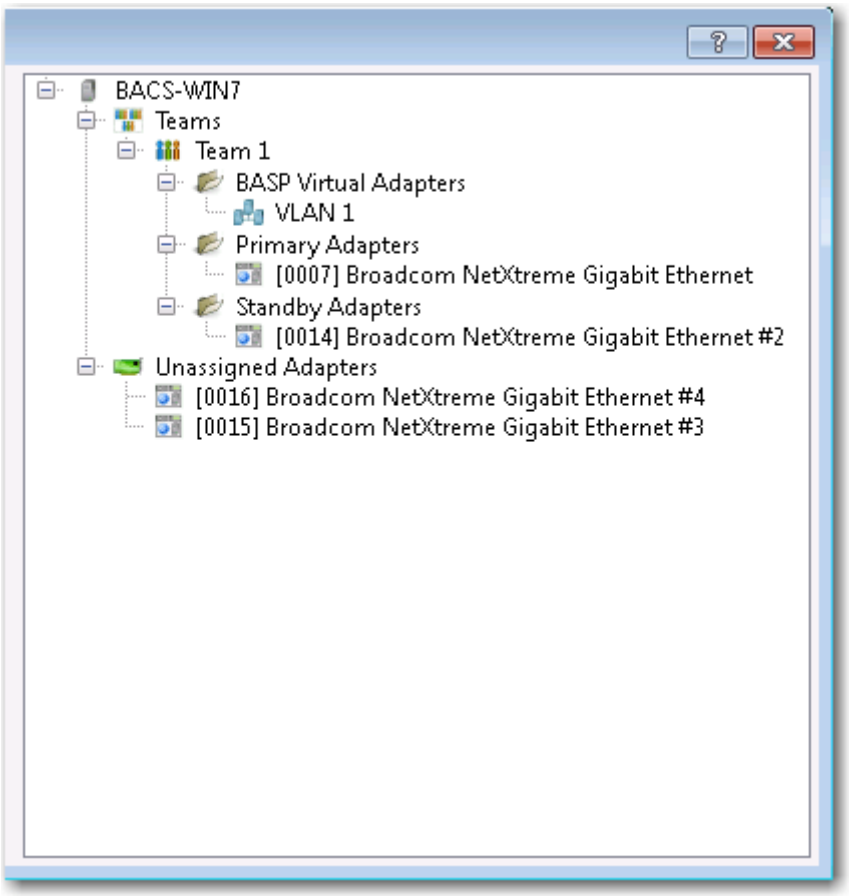
17. Wählen Sie **Ja**, um ein weiteres VLAN hinzuzufügen oder zu bearbeiten, und klicken Sie auf **Weiter**. Wiederholen Sie diese Schritte, bis Sie alle gewünschten VLANs hinzugefügt oder bearbeitet haben.

Hinweis: Sie können bis zu 64 VLANs pro Team definieren (63 markierte und 1 unmarkiertes). Durch Hinzufügen mehrerer VLANs kann eventuell aufgrund der Arbeitsspeicher- und Prozessorauslastung jedes einzelnen VLANs die Reaktionszeit für die Windows-Benutzeroberfläche beeinträchtigt werden. Wie stark die Ausführung von Windows beeinträchtigt wird, hängt von der Systemkonfiguration ab.

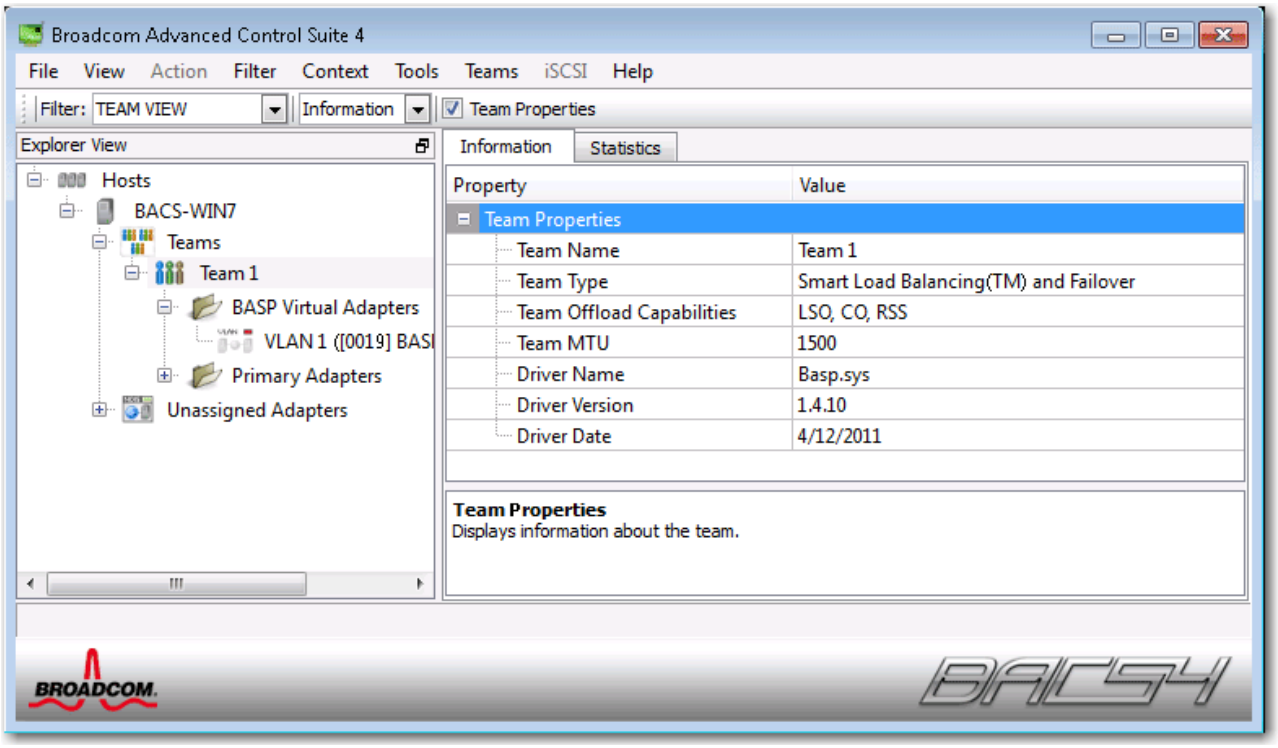
18. Um die Änderungen auf das Team anzuwenden und zu speichern, wählen Sie **Änderungen auf das System anwenden und Assistenten beenden**. Um die Änderungen anzuwenden, aber weiterhin mit dem Assistenten zu arbeiten, wählen Sie **Änderungen speichern und weitere Teams verwalten**. Klicken Sie auf Fertig stellen.



Hinweis: Bevor Sie die Änderungen übernehmen, können Sie zu jedem beliebigen Zeitpunkt des Broadcom Teaming-Assistenten auf **Vorschau** klicken, um eine visuelle Darstellung des Teams zu erhalten.



19. Klicken Sie im Fenster "Teamverwaltung" auf den Teamnamen, um die Eigenschaften des Teams auf der Registerkarte **Informationen** anzuzeigen. Auf der Registerkarte **Statistik** können Sie Daten senden und empfangen.



Verwenden des Experten-Modus

Verwenden Sie den Experten-Modus, um ein Team zu erstellen, Änderungen an einem Team vorzunehmen, ein VLAN hinzuzufügen und LiveLink für ein Team der Art **"Smart Load Balance" und "Failover"** und **SLB (Auto-Fallback deaktiviert)** zu konfigurieren. Informationen zum Erstellen eines Teams unter Verwendung des Assistenten finden Sie unter Verwenden des Teaming-Assistenten von Broadcom.

Zum Festlegen des Standard-Teaming-Modus wählen Sie im Menü **Extras Optionen** und dann **Experten-Modus** oder **Assistenten-Modus** aus (Standard ist Assistenten-Modus).

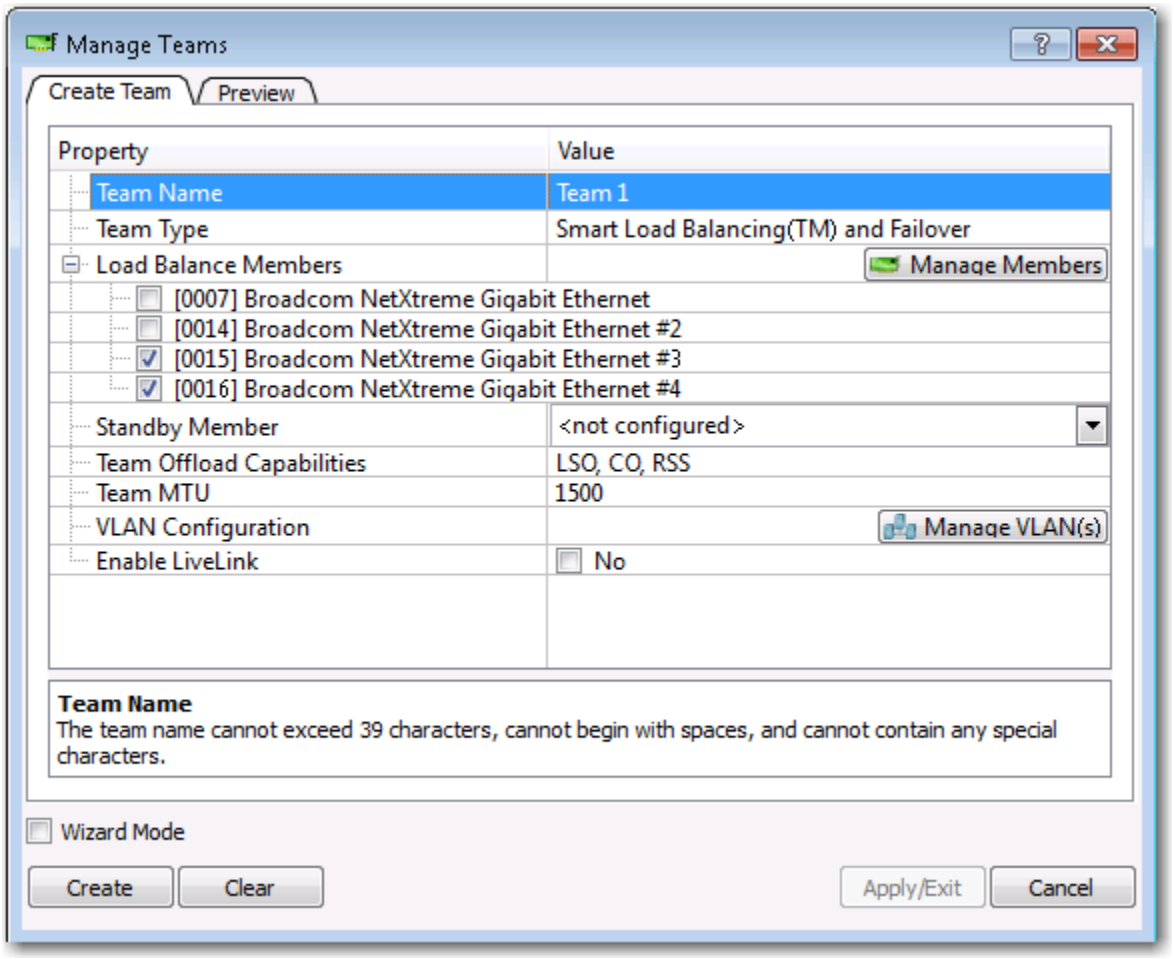
Erstellen eines Teams

Hinweis: Das Aktivieren von DHCP (Dynamic Host Configuration Protocol) ist für Mitglieder eines Teams der Art SLB nicht empfehlenswert.

1. Wählen Sie aus dem Menü Team die Option Team erstellen aus, oder klicken Sie mit der rechten Maustaste auf eines der Geräte im Bereich "Nicht zugewiesene Adapter" und wählen Sie Team erstellen aus. Diese Option steht nicht zur Verfügung, wenn unter Nicht zugewiesene Adapter keine Geräte aufgeführt sind – was bedeutet, dass alle Adapter bereits in Teams gruppiert sind.
2. Klicken Sie auf **Experten-Modus**.

Hinweis: Wenn Sie für die Erstellung eines Teams immer den Experten-Modus verwenden möchten, wählen Sie die Option **Beim Starten Experten-Modus**.

3. Klicken Sie auf die Registerkarte **Team erstellen**.



Hinweis: Die Registerkarte **Team erstellen** wird nur angezeigt, wenn Adapter zur Verfügung stehen, die in Teams gruppiert werden können.

4. Klicken Sie auf das Feld **Teamname**, um einen Namen für das Team einzugeben.
5. Klicken Sie auf das Feld **Teamart**, um eine Teamart auszuwählen.
6. Weisen Sie dem Team einen oder mehrere verfügbare Adapter zu, indem Sie den entsprechenden Adapter aus der Liste **Lastausgleichsmitglieder** auswählen. In der Liste **Lastausgleichsmitglieder** muss mindestens ein Adapter ausgewählt sein.
7. Sie können alle verfügbaren Adapter als Standby-Element definieren, indem Sie sie aus der Liste **Standby-Element** auswählen.

Hinweis: Dem Team muss mindestens ein Broadcom-Netzwerkadapter zugewiesen werden.

Die Spalten "Large Send Offload (LSO) (Large Send-Verschiebung, LSO)", "Checksum Offload (CO) (Prüfsummenverschiebung, CO)" und "RSS" geben an, ob die LSO-, CO- und/oder RSS-Eigenschaften für den Adapter unterstützt werden. Die LSO-, CO- und RSS-Eigenschaften werden nur dann für ein Team aktiviert, wenn alle Mitglieder die Funktion unterstützen und dafür konfiguriert wurden.

Hinweis: Wird einem Team ein Netzwerkadapter hinzugefügt, dessen Treiber deaktiviert ist, kann dies die Offload-Fähigkeit des Teams beeinträchtigen. Dies kann sich auf die Leistung des Teams auswirken. Aus diesem Grund ist es ratsam, nur Netzwerkadapter mit aktiviertem Treiber als Mitglieder eines Teams hinzuzufügen.

8. Geben Sie den Wert für **Team-MTU** ein.
9. Klicken Sie auf **Erstellen**, um die Teaminformationen zu speichern.
10. Wiederholen Sie die Schritte 4. bis 9., um zusätzliche Teams zu definieren. Nachdem Sie die Teams definiert haben, können Sie sie aus der Teamliste auswählen. Sie wurden jedoch noch nicht erstellt. Klicken Sie vor dem Anwenden der Änderungen auf die Registerkarte **Vorschau**, um die Teamstruktur anzuzeigen.
11. Klicken Sie auf **Übernehmen/Beenden**, um alle definierten Teams zu erstellen und das Fenster für die Teamverwaltung zu schließen.
12. Klicken Sie auf **Ja**, wenn eine Meldung angezeigt wird, die auf eine vorübergehende Unterbrechung der Netzwerkverbindung hinweist.

HINWEISE:

- Der Teamname darf maximal 39 Zeichen enthalten, er darf nicht mit einem Leerzeichen beginnen und keines der folgenden Zeichen enthalten: & \ / : * ? < > |
- Ein Teamname muss eindeutig sein. Wenn Sie einen Teamnamen mehr als einmal eingeben, wird eine Fehlermeldung angezeigt, die Sie darauf hinweist, dass der eingegebene Name bereits vorhanden ist.
- Die maximale Anzahl von Teammitgliedern beträgt 8.
- Wenn die Teamkonfiguration korrekt ausgeführt wurde, wird für jedes konfigurierte Team ein Adaptertreiber für ein virtuelles Team erstellt.
- Wenn Sie ein virtuelles Team deaktivieren und es später wieder aktivieren wollen, müssen Sie vor dem erneuten Aktivieren erst alle Teammitglieder deaktivieren und dann wieder aktivieren.
- Wenn Sie ein Team der Art Allgemeines Trunking oder Link Aggregation erstellen, können Sie kein Standby-Element angeben. Standby-Elemente können nur bei Teams der Art "Smart Load Balancing" und "Failover" sowie SLB (Auto-Fallback deaktiviert) angegeben werden.
- Wenn Sie bei einem Team der Art SLB (Auto-Fallback deaktiviert) den Verkehr vom Standby-Element wieder auf die Lastausgleichsmitglieder umstellen möchten, klicken Sie auf der Registerkarte Teameigenschaften auf die Schaltfläche Fallback.
- Obwohl das Verbinden von Teammitgliedern mit einem Hub zu Testzwecken unterstützt wird, wird beim Konfigurieren von SLB-Teams empfohlen, die Teammitglieder mit einem Switch zu verbinden.
- Nicht alle Netzwerkadapter von Fremdherstellern werden unterstützt oder sind vollständig für das Teaming zertifiziert.

13. Konfigurieren Sie die IP-Adresse des Teams.
    a. Doppelklicken Sie in der Systemsteuerung auf Netzwerkverbindungen.
    b. Klicken Sie mit der rechten Maustaste auf den Namen des zu konfigurierenden Teams, und klicken Sie anschließend auf Eigenschaften.
    c. Klicken Sie auf der Registerkarte Allgemein auf die Option Internetprotokoll (TCP/IP), und klicken Sie anschließend auf Eigenschaften.
    d. Konfigurieren Sie die IP-Adresse und alle erforderlichen TCP/IP-Konfigurationseinstellungen für das Team, und klicken Sie anschließend auf OK.

Ändern eines Teams

Nachdem Sie ein Team erstellt haben, können Sie folgende Änderungen vornehmen:

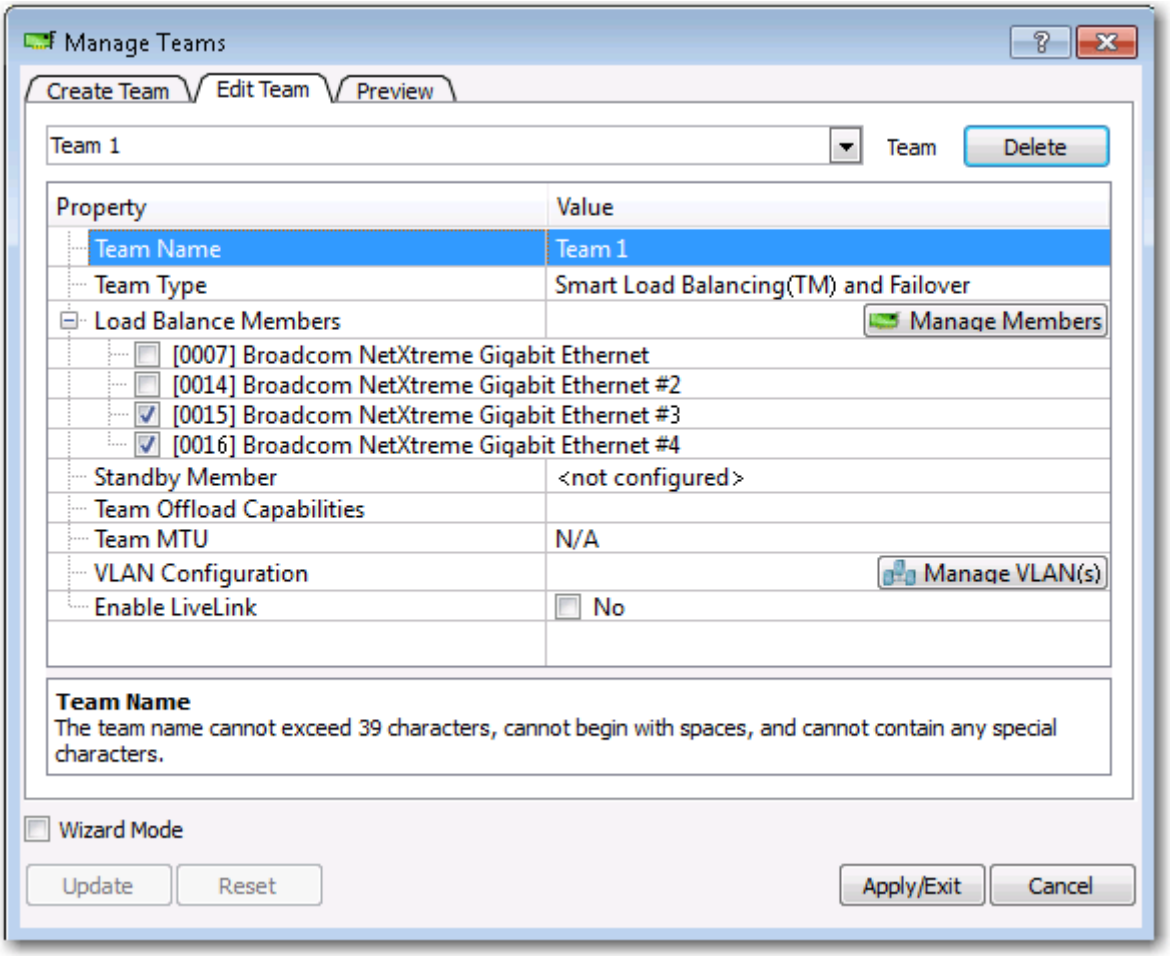
- Ändern der Teamart
- Ändern der dem Team zugewiesenen Mitglieder
- Hinzufügen eines VLANs
- Vornehmen von Änderungen an einem VLAN (im Experten-Modus)
- Entfernen eines Teams oder eines VLANs (im Experten-Modus)

So ändern Sie ein Team:

1. Klicken Sie im Menü **Team** auf **Team bearbeiten**, oder klicken Sie mit der rechten Maustaste auf eines der Teams in der Liste, und wählen Sie **Team bearbeiten**. Diese Option steht nur zur Verfügung, wenn bereits ein Team erstellt wurde, das im Fenster **Teamverwaltung** aufgeführt wird.
2. Der Begrüßungsbildschirm des Assistenten wird angezeigt. Klicken Sie auf **Weiter**, um mithilfe des Assistenten ein Team zu ändern, oder auf **Experten-Modus**, um im Experten-Modus zu arbeiten.

Hinweis: Im Experten-Modus wird die Registerkarte **Team bearbeiten** nur angezeigt, wenn im System Teams konfiguriert sind.

3. Klicken Sie auf die Registerkarte **Team bearbeiten**.



4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie anschließend auf **Aktualisieren**. Die Änderungen wurden noch nicht gespeichert; klicken Sie auf die Registerkarte **Vorschau**, um die aktualisierte Teamstruktur anzuzeigen, bevor Sie die Änderungen übernehmen.
5. Klicken Sie auf **Übernehmen/Beenden**, um die Aktualisierungen zu speichern und das Fenster für die Teamverwaltung zu schließen.
6. Klicken Sie auf **Ja**, wenn eine Meldung angezeigt wird, die auf eine vorübergehende Unterbrechung der Netzwerkverbindung hinweist.

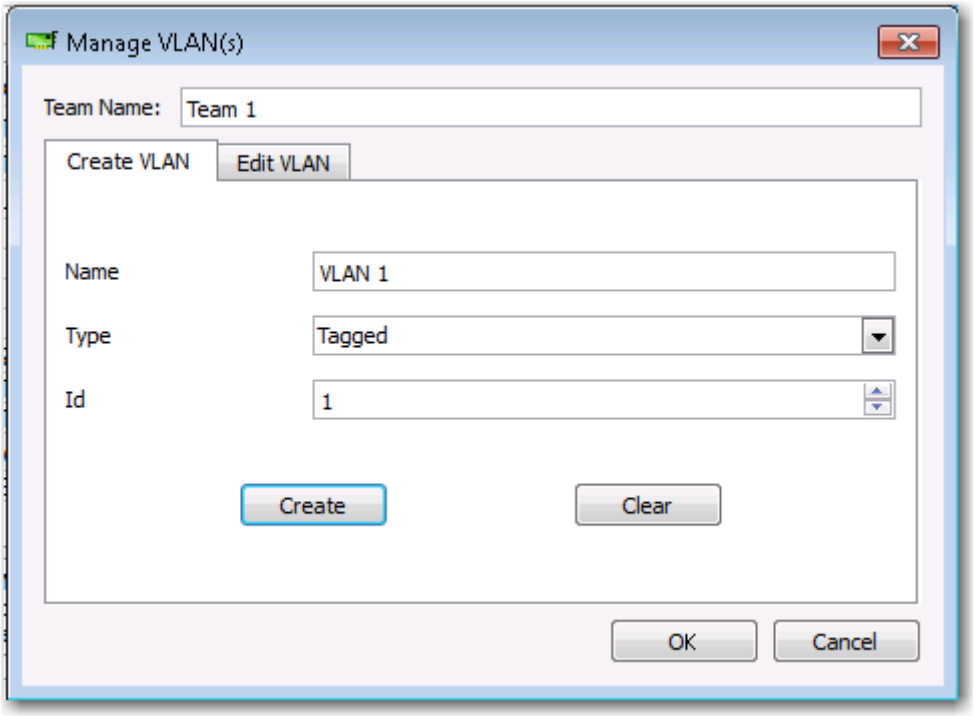
Hinzufügen eines VLANs

Einem Team können virtuelle LANs (VLANs) hinzugefügt werden. Dadurch können Sie mehrere virtuelle Adapter hinzufügen, die sich in verschiedenen Subnetzen befinden. Der Vorteil davon ist, dass das System über einen Netzwerkadapter verfügt, der zu mehreren Subnetzen gehört. Mit einem VLAN können Sie die Lastausgleichsfunktion für die Lastausgleichsmitglieder mit einem Failover-Adapter koppeln.

Sie können bis zu 64 VLANs pro Team definieren (63 markierte und 1 unmarkiertes). VLANs können nur dann erstellt werden, wenn alle Teammitglieder Broadcom-Adapter sind. Wenn Sie ein VLAN mit einem Adapter eines anderen Herstellers erstellen möchten, wird eine Fehlermeldung angezeigt.

So konfigurieren Sie ein Team mit einem VLAN:

1. Wählen Sie aus dem Menü **Teams** die Option **VLAN hinzufügen**.
2. Der Begrüßungsbildschirm wird angezeigt.
3. Klicken Sie auf **Experten-Modus**.
4. Klicken Sie auf der Registerkarte **Team erstellen** im Fenster **Teams verwalten** auf **VLAN(s) verwalten**.
5. Geben Sie den Namen des VLANs ein, und wählen Sie die Art und die ID aus.
6. Klicken Sie auf **Erstellen**, um die VLAN-Informationen zu speichern. Nachdem Sie die VLANs definiert haben, können Sie sie aus der Teamnamenliste auswählen. Sie wurden jedoch noch nicht erstellt.
7. Fahren Sie mit diesen Schritten fort, bis alle VLANs definiert sind. Klicken Sie dann zum Erstellen auf **OK**.



8. Klicken Sie auf **Ja**, wenn eine Meldung angezeigt wird, die auf eine vorübergehende Unterbrechung der Netzwerkverbindung hinweist.

Hinweis: Das System sollte über 64 MB Arbeitsspeicher für jedes der acht VLANs pro Adapter verfügen, damit eine optimale Adapterleistung gewährleistet wird.

So zeigen Sie die VLAN-Eigenschaften und -Statistik an und führen Sie VLAN-Tests aus:

So zeigen Sie die VLAN-Eigenschaften und -Statistik an und führen Sie VLAN-Tests aus:

1. Wählen Sie eines der aufgeführten VLANs aus.
2. Klicken Sie auf die Registerkarte **Informationen**, um die Eigenschaften des VLAN-Adapters anzuzeigen.
3. Klicken Sie auf die Registerkarte **Statistik**, um die Statistik für den VLAN-Adapter anzuzeigen.
4. Klicken Sie auf die Registerkarte **Diagnose**, um einen Netzwerktest für den VLAN-Adapter auszuführen.

Löschen eines VLANs

Der nachfolgende Vorgang gilt für den Experten-Modus.

So löschen Sie ein VLAN:

1. Wählen Sie das zu löschende VLAN aus.
2. Wählen Sie aus dem Menü **Teams** die Option **VLAN entfernen**.
3. Klicken Sie auf **Übernehmen**.
4. Klicken Sie auf **Ja**, wenn eine Meldung angezeigt wird, die auf eine vorübergehende Unterbrechung der Netzwerkverbindung hinweist.

Hinweis: Beim Löschen eines Teams werden auch alle für das Team konfigurierten VLANs gelöscht.

Konfigurieren von LiveLink für ein Team aus Smart Load Balancing and Failover und SLB (Auto-Fallback deaktivieren)

LiveLink ist eine Funktion von BASP, die für die Teamarten Smart Load Balancing (SLB) und SLB (Auto-Fallback deaktiviert) zur Verfügung stehen. LiveLink dient dazu, einen Verbindungsverlust hinter dem Switch zu erkennen und den Datenverkehr nur durch die Teammitglieder zu leiten, die über eine Live-Verbindung verfügen.

Lesen Sie vor dem Konfigurieren von LiveLink folgende Hinweise.

HINWEISE:

- Lesen Sie sich nochmals die Beschreibung von LiveLink durch, bevor Sie mit dem Konfigurieren von LiveLink™ beginnen. Überprüfen Sie außerdem, ob alle Prüfziele, die Sie festlegen möchten, verfügbar sind und funktionieren. Sollte sich die IP-Adresse des Prüfziels ändern, muss LiveLink erneut konfiguriert werden. Sollte sich die MAC-Adresse des Prüfziels ändern, müssen Sie das Team neu starten (siehe "Problembehebung").
- Ein Prüfziel muss sich in demselben Subnetz wie das Team befinden. Es muss über eine gültige, statisch zugewiesene IP-Adresse verfügen (keine Broadcast-, Multicast- oder Unicast-Adresse) und muss ständig verfügbar (eingeschaltet) sein.
- Führen Sie den Ping-Befehl aus dem Team aus, um die Netzwerkanbindung des Prüfziels zu überprüfen.
- Sie können bis zu vier Prüfziele festlegen.
- Weder die einem Prüfziel noch die einem Teammitglied zugewiesene IP-Adresse darf für das erste oder letzte Oktett den Wert Null aufweisen.

So konfigurieren Sie LiveLink:

1. Wählen Sie aus dem Menü **Teams** die Option **Team bearbeiten**.
2. Klicken Sie auf "Experten-Modus" (zum Konfigurieren von LiveLink mit Hilfe des Teaming-Assistenten siehe Verwenden des Teaming-Assistenten von Broadcom).
3. Klicken Sie im Fenster "Mitglieder verwalten" auf die Registerkarte **Team bearbeiten**.
4. Wählen Sie **LiveLink aktivieren**. Die LiveLink-Konfigurationsoptionen werden unten angezeigt.
5. Es wird empfohlen, die Standardwerte für **Probe interval** (Prüfintervalle) - die Anzahl von Sekunden zwischen Übertragungen von Verbindungspaketen zum Prüfziel - und für **Probe maximum retries** (Maximale Prüfwiederholungen) - die Anzahl von aufeinanderfolgend fehlgeschlagenen Antworten eines Prüfziels, bevor ein Failover ausgelöst wird - zu übernehmen. Um andere Werte festzulegen, wählen Sie in der Liste **Probe interval (seconds)** (Prüfintervall (Sekunden)) das gewünschte Prüfintervall aus, und klicken Sie in der Liste **Probe maximum**

retries (Maximale Prüfwiederholungen) auf die gewünschte Anzahl von Prüfwiederholungen.

6. Legen Sie die **Test-VLAN-ID** entsprechend des VLANs fest, in dem sich das bzw. die Testziele befinden. Dadurch wird das entsprechende VLAN-Tag auf Basis der gemeinsam verwendeten Konfiguration des bzw. der angeschlossenen Switch-Ports auf das Verbindungspaket angewendet.

Hinweis: Jedes für LiveLink aktivierte Team kann nur mit Prüfzielen auf einem einzigen VLAN kommunizieren. Die VLAN-ID 0 entspricht einem nicht markiertem Netzwerk.

7. Wählen Sie **Prüfziel 1**, und geben sie die Ziel-IP-Adresse für ein oder alle Prüfziele ein.

Hinweis: Nur das erste Prüfziel wird benötigt. Sie können bis zu drei zusätzliche Prüfziele als Backups festlegen, indem Sie den anderen Prüfzielen IP-Adressen zuweisen.

8. Wählen Sie eines der aufgeführten Teammitglieder, und geben Sie die IP-Adresse des Mitglieds ein.

Hinweis: Alle Mitglieder-IP-Adressen müssen demselben Subnetz angehören wie die Prüfziele.

9. Klicken Sie auf **Aktualisieren**. Wiederholen Sie diese Schritte für alle anderen aufgeführten Teammitglieder.
10. Klicken Sie auf **Übernehmen/Beenden**.

Speichern und Wiederherstellen einer Konfiguration

So speichern Sie eine Konfiguration:

1. Klicken Sie im Menü **Datei** auf **Team speichern unter**.
2. Geben Sie *den Pfad und den Dateinamen der neuen Konfigurationsdatei* ein, und klicken Sie anschließend auf **Speichern** (die Erweiterung .bcg wird hinzugefügt).

   Die Konfigurationsdatei ist eine Textdatei und kann in jedem Texteditor angezeigt werden. Die Datei enthält Informationen über den Adapter und die Teamkonfiguration.

So stellen Sie eine Konfiguration wieder her:

1. Klicken Sie im Menü **Datei** auf **Team wiederherstellen**.
2. Klicken Sie auf den Namen der wiederherzustellenden Datei, und klicken Sie anschließend auf **Öffnen**.

Hinweis: Wechseln Sie bei Bedarf zum Ordner, in dem sich die Datei befindet.

3. Klicken Sie auf **Übernehmen**.
4. Klicken Sie auf **Ja**, wenn eine Meldung angezeigt wird, die auf eine vorübergehende Unterbrechung der Netzwerkverbindung hinweist.
5. Wenn bereits eine Konfiguration geladen ist, werden Sie in einer Meldung gefragt, ob Sie die aktuelle Konfiguration speichern möchten. Klicken Sie auf **Ja**, um die aktuelle Konfiguration zu speichern. Andernfalls gehen die aktuell geladenen Konfigurationsdaten verloren.

Hinweis: Die Wiederherstellung eines Teams ist möglicherweise sehr langwierig, wenn das Team mit vielen VLANs und einer statischen IP-Adresse konfiguriert ist.

Anzeigen von BASP-Statistiken

Im Bereich **Statistik** werden Leistungsinformationen zu den Netzwerkadaptern in einem Team angezeigt.

Um die BASP-Statistikinformationen für einen Teammitgliedadapter oder das Team als Ganzes anzuzeigen, klicken Sie im Fenster **Teamverwaltung** auf den Namen des Adapters bzw. des Teams, und klicken Sie auf die Registerkarte **Statistik**.

Klicken Sie auf **Aktualisieren**, um die neuestens Werte für die Statistiken anzuzeigen. Klicken Sie auf **Zurücksetzen**, um alle Werte auf Null zu setzen.

Tx. Paket. Dies ist die Anzahl der eingegangenen Pakete.

Tx. Paketübertragung verworfen. Dies ist die Anzahl der verworfenen Paketübertragungen.

Tx. Paketübertragung in Warteschlange. Dies ist die Anzahl der Paketübertragungen in Warteschlange.

Rx. Paket. Dies ist die Anzahl der empfangenen Pakete.

Rx. Paketübertragung verworfen. Dies ist die Anzahl der verworfenen Paketübertragungen.

Tests wiederholt. Dies ist die Anzahl der aufeinanderfolgend fehlgeschlagenen Antworten eines Prüfziels, bevor ein Failover ausgelöst wird.

Konfigurieren mit dem CLI-Dienstprogramm

Ein zu BACS alternatives Verfahren zur Konfiguration von Broadcom-Netzwerkadaptern basiert auf der Verwendung von BACSCLI. Dabei handelt es sich um ein Broadcom-Dienstprogramm, mit dem Sie über eine Konsole in einem nicht-interaktiven CLI-Modus oder in einem interaktiven Modus Informationen anzeigen oder Netzwerkadapter konfigurieren können. Wie BACS bietet auch BACSCLI Informationen über die einzelnen Netzwerkadapter und gibt Ihnen die Möglichkeit, ausführliche Tests durchzuführen, Diagnosen vorzunehmen, Statistiken anzuzeigen und Eigenschaftswerte zu ändern. Mit BACSCLI können Sie außerdem Netzwerkadapter für Lastausgleich und Failover-Unterstützung zu Teams zusammenstellen.

Eine vollständige Liste der verfügbaren Befehle und Beispiele finden Sie in der Info-Textdatei zu BACSCLI auf der von Dell bereitgestellten CD.

Auf einem System mit einem Broadcom NetXtreme I- oder NetXtreme II-Netzwerkadapter wird BACSCLI installiert, wenn BACS mit dem Installationsprogramm installiert wird.

BACS-Problembehebung

Problem: Beim Versuch, BACS bei einem Linux-System zu öffnen, wird die folgende Fehlermeldung angezeigt:

> "Es scheint eine andere Instanz des BACS-Clients auf diesem System ausgeführt zu werden. Es kann nur eine Instanz des BACS-Clients gleichzeitig ausgeführt werden. Wenn Sie sicher sind, dass kein anderer BACS-Client ausgeführt wird, wurde möglicherweise eine frühere Instanz unerwartet beendet."

Lösung: Diese Meldung wird angezeigt, wenn Sie versuchen, eine zweite Instanz von BACS auszuführen. Wenn Sie diese Meldung erhalten, aber sicher sind, dass derzeit keine Instanz von BACS ausgeführt wird, wurde möglicherweise eine frühere Instanz von BACS unerwartet beendet. Um diese Instanz zu löschen, entfernen Sie die Datei "/dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0}."

Abschnitt 14: Spezifikationen

10/100/1000BASE-T-Kabelspezifikationen

Tabelle 22. 10/100/1000BASE-T-Kabelspezifikationen

Porttyp	Anschluss	Speichermedien	Maximale Länge
10BASE-T	RJ-45	UTP-Kabel der Kategorie 3, 4 oder 5	100 m
100/1000BASE-T[1]	RJ-45	UTP-Kabel der Kategorie 5[2]	100 m

[1] Bei 1000BASE-T-Signalisierung sind vier TP-Kabel der Kategorie 5 für symmetrische Verkabelung gemäß ISO/IEC 11801:1995 und ANSI/EIA/TIA-568-A (1995) erforderlich, die mit den in TIA/EIA TSB95 definierten Verfahren auf zusätzliche Leistung getestet wurden.

[2] Mindestens Kategorie 5. Kategorie 5e und Kategorie 6 werden vollständig unterstützt.

Leistungsspezifikationen

Tabelle 23. Leistungsspezifikationen

Leistungsmerkmal	Spezifikationen
PCI-Express™-Controller (BCM57XX-Controller)	
PCI-Express-Schnittstelle	x1, x2, x4 Linkbreite
PCI-Express-Gesamtbandbreite (Übermittlung und Empfang)	2,5 Gbit/s oder 5,0 Gbit/s
10/100/1000BASE-T	10/100/1000 Mbit/s (Vollduplex)

Abschnitt 15: Technische Vorschriften

FCC Klasse B-Hinweis

Broadcom NetXtreme Gigabit Ethernet Controller
BCM95721A211
BCM95722A2202

Dieses Gerät entspricht Abschnitt 15 der FCC-Richtlinien. Der Betrieb unterliegt den beiden folgenden Bedingungen: 1) Dieses Gerät darf keine gefährdenden Störungen verursachen. 2) Dieses Gerät muss jede empfangene Störung akzeptieren, einschließlich einer Störung, die zu unerwünschtem Betrieb führen könnte.

Dieses Gerät wurde getestet und erfüllt die Anforderungen für digitale Geräte der Klasse B gemäß Teil 15 der Richtlinien der Federal Communications Commission (FCC). Diese Anforderungen gewährleisten angemessenen Schutz gegen Empfangsstörungen im Wohnbereich. Das Gerät erzeugt und verwendet Signale im Frequenzbereich von Rundfunk und Fernsehen und kann diese abstrahlen. Wenn das Gerät nicht gemäß den Anweisungen installiert und betrieben wird, kann es Störungen beim Empfang verursachen. Es kann jedoch nicht garantiert werden, dass solche Störungen nicht in bestimmten Installationen auftreten. Wenn das Gerät Störungen im Rundfunk- oder Fernsehempfang verursacht, was durch vorübergehendes Ausschalten des Gerätes überprüft werden kann, versuchen Sie, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung oder den Standort der Empfangsantenne.
- Erhöhen Sie den Abstand zwischen dem Gerät und Ihrem Rundfunk- oder Fernsehempfänger.
- Schließen Sie das Gerät an einen anderen Hausstromkreis an als den Rundfunk- oder Fernsehempfänger.
- Wenden Sie sich an Ihren Händler oder an einen ausgebildeten Rundfunk- und Fernsehtechniker.

Änderungen mechanischer oder elektrischer Art an dem Gerät sind untersagt.

Hinweis: Veränderungen oder Modifikationen des Adapters ohne vorherige Genehmigung von Broadcom können zum Erlöschen der Betriebserlaubnis führen.

Broadcom Corporation
190 Mathilda Place
Sunnyvale, California 94086, USA

VCCI Klasse B-Hinweis

Dies ist ein Produkt der Klasse B nach der vom Voluntary Control Council for Interference (VCCI) für Datenverarbeitungsgeräte festgelegten Norm. Wird dieses Gerät in der Nähe eines Radio- oder Fernsehempfangsgerätes in einem Wohnbereich eingesetzt, kann es zu Funkstörungen kommen. Beachten Sie bei der Aufstellung und dem Einsatz des Geräts die Anweisungen der Bedienungsanleitung.

Vorsicht! Bei Vorhandensein einer leitungsgeführten Hochfrequenzstrahlung im Frequenzbereich zwischen 59 und 66 MHz kann der Betrieb des Geräts gestört werden. Der Normalbetrieb stellt sich nach Entfernen der Hochfrequenzstrahlung wieder ein.

VCCI Class B Statement (Japan)

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-Hinweis

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.

Konformitätserklärung für Kanada

Industry Canada, Class B

This Class B digital apparatus complies with Canadian ICES-003.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by Broadcom could void your authority to operate this equipment.

Industry Canada, classe B

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Avis : Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par Broadcom y sont apportés.

MIC-Hinweis (nur für die Republik Korea)

Gerät der Klasse B

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

Dieses Gerät wurde für die Verwendung zu privaten Zwecken geprüft und zugelassen und kann in jeder Umgebung, einschließlich Wohngebieten, verwendet werden.

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。

Abschnitt 16: Problembehebung

Hardware-Diagnose

Zur Überprüfung der Adapterhardware stehen Prüfschleifen-Diagnosetests zur Verfügung. Diese Tests ermöglichen den Zugriff auf die interne bzw. externe Diagnose des Adapters, wobei Paketinformationen über die physische Verbindung übertragen werden. Für Windows-Umgebungen finden Sie diese Anweisungen und Informationen unter Ausführen von Diagnosetests).

Fehler bei BACS-Diagnosetests

Wenn einer der folgenden Tests fehlschlägt, während die Diagnosetests über die Registerkarte Ausführen von Diagnosetests in BACS ausgeführt werden, liegt möglicherweise bei der im System installierten Netzwerkkarte bzw. beim LOM ein Hardwareproblem vor.

- Kontrollregister
- MII-Register
- EEPROM
- Interner Speicher
- Chip-CPU
- Interrupt
- Prüfschleife: MAC
- Prüfschleife: PHY
- LED-Test

Im Folgenden werden Schritte zur Problembehebung aufgelistet.

1. Entfernen Sie das fehlerhafte Gerät, und setzen Sie es wieder in den Steckplatz ein. Achten Sie darauf, dass die Karte fest im Steckplatz installiert ist.
2. Führen Sie den Test erneut aus.
3. Wenn die Karte weiterhin fehlerhaft ist, ersetzen Sie sie durch eine andere Karte desselben Modells und führen Sie den Test erneut aus. Wenn der Test mit der neuen Karte fehlerfrei ausgeführt werden kann, wenden Sie sich an den Hardwarehersteller, um Hilfe zum fehlerhaften Gerät zu erhalten.

4. Fahren Sie den Computer herunter, schalten Sie ihn aus, und starten Sie das System neu.
5. Deinstallieren Sie die Diagnosesoftware, und installieren Sie sie neu.
6. Wenden Sie sich an den Hardwarehersteller.

Fehler bei BACS-Netzwerktests

Normalerweise sind Fehler beim BACS-Testen des Netzwerks auf ein Konfigurationsproblem im Netzwerk oder der IP-Adressen zurückzuführen. Im Folgenden werden allgemeine Schritte aufgelistet, die Sie zur Behebung von Netzwerkproblemen ausführen können.

1. Stellen Sie sicher, dass das Kabel angeschlossen ist und die Verbindung hergestellt wurde.
2. Überprüfen Sie, ob die Treiber geladen und aktiviert wurden.
3. Ziehen Sie das Kabel ab, das an die Netzwerkkarte bzw. am LOM angeschlossen ist, und schließen Sie es wieder an.
4. Überprüfen Sie, ob die IP-Adresse korrekt zugewiesen wurde. Verwenden Sie hierzu den Befehl "ipconfig" oder das Betriebssystemtool zum Zuweisen von IP-Adressen.
5. Stellen Sie sicher, dass die IP-Adresse für das Netzwerk, mit dem die Adapter verbunden sind, korrekt eingegeben wurde.

Problembehebung – Checkliste

Vorsicht! Bevor Sie das Systemgehäuse öffnen, lesen Sie die Sicherheitsvorkehrungen.

Die folgende Checkliste empfiehlt Maßnahmen zur Behebung von Problemen, die bei der Installation des Broadcom NetXtreme Gigabit Ethernet-Adapter beziehungsweise dessen Betrieb in Ihrem System auftreten können.

- Überprüfen Sie alle Kabel und Anschlüsse. Überprüfen Sie, ob alle Kabel ordnungsgemäß am Netzwerkadapter und am Switch angeschlossen sind. Überprüfen Sie, ob die Kabellänge und die Kabelauslegung den unter Anschließen der Netzwerkkabel aufgeführten Anforderungen entsprechen.
- Überprüfen Sie die Adapterinstallation anhand der Angaben unter Installieren der Hardware. Überprüfen Sie, ob der Adapter fest im Steckplatz sitzt. Suchen Sie nach spezifischen Hardwareproblemen, beispielsweise nach einer offensichtlichen Beschädigung einer Platinenkomponente oder des PCI-Stiftsockels.
- Überprüfen Sie die Eigenschaftseinstellungen und ändern Sie diese, falls sie den Einstellungen anderer Komponenten widersprechen.
- Überprüfen Sie, ob Ihr System das neueste BIOS verwendet.
- Versuchen Sie, den Adapter in einem anderen Steckplatz zu installieren. Wenn die neue Installationsposition funktioniert, ist unter Umständen der ursprüngliche Systemsteckplatz defekt.
- Tauschen Sie den nicht funktionierenden Adapter gegen einen Adapter aus, von dem Sie wissen, dass er korrekt funktioniert. Wenn der zweite Adapter in dem Steckplatz funktioniert, in dem der erste Adapter nicht betrieben werden konnte, ist der erste Adapter vermutlich defekt.
- Installieren Sie den Adapter in einem anderen funktionierenden System, und führen Sie die Tests erneut durch. Wenn der Adaptertest im neuen System erfolgreich ausgeführt werden kann, ist möglicherweise das ursprüngliche System defekt.
- Entfernen Sie alle anderen Adapter aus dem System, und führen Sie die Tests erneut durch. Wenn der Adaptertest erfolgreich verläuft, liegt unter Umständen ein Konflikt mit den anderen Adaptern vor.

Überprüfen der Netzwerkverbindung/des Netzwerkbetriebs

Informationen zum Überprüfen des Netzwerkverbindungsstatus und des Betriebsstatus finden Sie im Abschnitt Testen der Netzwerkanbindung oder Anzeigen von Adapterinformationen.

Überprüfen der geladenen Treiber

Windows

Unter Anzeigen von Adapterinformationen finden Sie alle wichtigen Informationen über den Adapter, den Verbindungsstatus und die Netzwerkanbindung.

Linux

Überprüfen Sie, ob der Linux-Treiber TG3 korrekt geladen ist. Führen Sie dazu folgenden Befehl aus:

```
lsmod | grep tg3
```

Wenn der Treiber geladen ist, wird eine Zeile ähnlich der folgenden angezeigt. Hierbei gibt *Größe* die Größe des Treibers in Byte und *n* die Anzahl der konfigurierten Adapter an.

Tabelle 24. Linux-Treiber

Modul	*Größe*	*Verwendet von*
TG3	*Größe*	*n*

Durchführen eines Kabellängentests

In Windows-Umgebungen kann ein Kabeltest durchgeführt werden. Informationen zum Durchführen eines Kabeltests finden Sie unter Analysieren von Kabeln.

Testen der Netzwerkanbindung

Hinweis: Stellen Sie bei der Verwendung erzwungener Übertragungsraten sicher, dass sowohl für den Adapter als auch für den Switch dieselbe Übertragungsrate erzwungen wird oder für beide Seiten die automatische Aushandlung konfiguriert ist.

Windows

Mit dem Befehl ping können Sie herausfinden, ob eine Netzwerkverbindung besteht.

Hinweis: Sie können die Netzwerkanbindung auch mit der Funktion Testen des Netzwerks der Broadcom Advanced Control Suite 2 testen.

1. Überprüfen Sie, ob die Treiber geladen und aktiviert wurden.
2. Stellen Sie sicher, dass das Kabel angeschlossen ist und die Verbindung hergestellt wurde.
3. Klicken Sie auf **Start** und anschließend **Ausführen**.
4. Geben Sie in das Feld **Öffnen cmd** ein, und klicken Sie dann auf **OK**.
5. Geben Sie **ipconfig /all** ein, um die zu testende Netzwerkverbindung anzuzeigen.
6. Stellen Sie sicher, dass die IP-Adresse für das Netzwerk, mit dem die Adapter verbunden sind, korrekt eingegeben wurde.
7. Geben Sie **ping IP address** ein, und drücken Sie dann die Eingabetaste.

Die angezeigte Ping-Statistik gibt an, ob eine Netzwerkverbindung besteht.

Linux

Vergewissern Sie sich, dass die Ethernet-Schnittstelle aktiviert ist und korrekt funktioniert. Führen Sie dazu **ifconfig** aus, und überprüfen Sie den Status der Ethernet-Schnittstelle. Mit **netstat -i** können Sie die Statistiken der Ethernet-Schnittstelle überprüfen. Weitere Informationen zu **ifconfig** und **netstat** finden Sie unter Linux-Treibersoftware.

Senden Sie einen Ping-Befehl an einen IP-Host im Netzwerk, um zu überprüfen, ob die Verbindung hergestellt wurde:

Geben Sie in der Befehlszeile **ping IP-Adresse** ein, und drücken Sie dann die Eingabetaste.

Die angezeigte Ping-Statistik gibt an, ob eine Netzwerkverbindung besteht.

Broadcom Boot Agent

Problem: Es können mit PXE keine Netzwerkeinstellungen über DHCP abgefragt werden.
Lösung: Vergewissern Sie sich, dass an dem Port, mit dem der PXE-Client verbunden ist, Spanning Tree Protocol (STP) deaktiviert oder der Portfast-Modus (für Cisco) aktiviert ist, um einen ordnungsgemäßen Betrieb zu gewährleisten. Stellen Sie beispielsweise **spantree portfast 4/12 enable** ein.

Broadcom Advanced Server Program (BASP)

Problem: Nachdem eine NIC, die Teil eines Teams war, physisch getrennt und ein Neustart durchgeführt wurde, zeigte das Team nicht die erwarteten Leistungen.
Lösung: Um eine Team-NIC von einem System zu trennen, müssen Sie die NIC zunächst im Team löschen. Wird dies vor dem Abschalten nicht durchgeführt, könnte das Team beim anschließenden Neustart beschädigt werden, sodass sich das Team in der Folge möglicherweise nicht wie erwartet verhält.

Problem: Die Änderungen, die ich für ein Team mithilfe von INETCFG vorgenommen habe, treten nicht in Kraft.
Lösung: Wenn Sie ein Team mithilfe von INETCFG ändern, müssen Sie das System unter Umständen nach der Neuinitialisierung neu starten, damit die Änderungen in Kraft treten können.

Kernel-Debugging über Ethernet

Problem: Beim Kernel-Debugging über ein Ethernet-Netzwerk unter Windows 8.0 oder Windows Server 2012 kann das System nicht neu gestartet werden. Dieses Problem kann mit einigen Adaptern auftreten, wenn Windows 8.0 oder Windows Server 2012 für den UEFI-Modus konfiguriert ist. Möglicherweise wird eine Firmware-Fehlermeldung auf dem Bildschirm angezeigt, die Sie darauf hinweist, dass im UEFI-Preboot-Environment eine "Non Maskable Interrupt"-Ausnahme auftrat.

Lösung: Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel KB974072, "Non Maskable Interrupt-Fehler beim Start eines Systems, das für Kernel-Debugging über Ethernet konfiguriert wurde".

Sonstiges

Problem: LSO (Large-Send-Verschiebung) und CO (Prüfsummenverschiebung) funktionieren nicht in meinem Team.
Lösung: Wenn einer der Adapter eines Teams LSO nicht unterstützt, funktioniert LSO für dieses Team nicht. Entfernen Sie den Adapter aus dem Team, der LSO nicht unterstützt, und ersetzen Sie ihn durch einen Adapter, der LSO unterstützt. Dasselbe gilt für Checksum Offload.