Guía de usuario de Broadcom® NetXtreme® BCM57XX

Última revisión: Febrero de 2015

2CS57XX-CDUM513-R

Última revisión: Febrero de 2015

2CS57XX-CDUM513-R

Table of Contents

Sección 1: Características y funcionalidad

Descripción funcional

Los adaptadores Broadcom NetXtremeGigabit Ethernet conectan un sistema que cumple con PCI Express™ a una red Gigabit Ethernet. Los adaptadores Broadcom NetXtreme Gigabit Ethernet incorporan una tecnología que transfiere datos a una velocidad máxima de 1 gigabit por segundo, 10 veces la velocidad de los adaptadores Fast Ethernet.

Si utiliza el software de equipos de Broadcom, puede dividir la red en redes LAN virtuales (VLAN) y agrupar múltiples adaptadores de red en equipos para obtener la funcionalidad de balanceo de carga y la tolerancia a fallas de la red. Consulte Equipos y Servicios de equipos Broadcom Gigabit Ethernet para obtener información detallada. Consulte Redes LAN virtuales, para obtener una descripción de las VLAN. Consulte Configuración de equipos para obtener instrucciones sobre cómo configurar equipos y crear redes VLAN en los sistemas operativos Windows.

Características

La siguiente es una lista de las características del adaptador Broadcom NetXtreme Gigabit Ethernet para todos los sistemas operativos compatibles:

- Transceptores SerDes de cuatro puertos 10/100/1000BASE-T y de cuatro puertos 1000BASE-X/SGMII 1,25 Gbaud integrados
- Energy Efficient Ethernet™ (Ethernet con uso eficiente de energía) compatible con Norma IEEE 802.3az-2010
- Autonegociación de Cláusula 73 de IEEE 802.3ap
- MAC con dúplex completo y dúplex medio de cuatro puertos 10/100/1000BASE-T
- MAC con dúplex completo y dúplex medio de cuatro puertos 1000BASE-X/SGMII
- Cruzamiento MDI automático
- x4 PCI Express v2.0 a 5 GT/s o 2,5 GT/s
- Capacidades MSI y MSI-X, de hasta 17 vectores MSIX
- Soporte de virtualización de E/S para VMware NetQueue y Microsoft VMQ
  - 17 colas de recepción y 16 colas de transmisión
  - 17 vectores MSI-X que soportan interrupciones al host por cola
- Vector MSI-X flexible para transmitir/recibir asociación por cola
- Sugerencias de procesamiento TLP (TPH) ECN en la especificación de base PCI Express v2.0
- Restablecimiento en nivel de función
- Cambio de escala en el extremo de recibo (RSS), con soporte de vector MSI-X por cola y soporte para UDP tipo RSS hash
- Cambio de escala en el extremo de transmisión (SAT) y cola multitransmisión (multi-Tx) con soporte de vector MSI-X por cola
- Soporte de tramas gigantes de hasta 9600 bytes de cargo
- Soporte LAN virtual (VLAN), etiquetado de VLAN IEEE 802.1q
- Descarga de checksum TCP, IP, UDP
- Descarga de envío grande (LSO), Descarga de segmentación TCP (TSO)
- Asistencia de Hardware para IEEE 1588 e implementaciones de sincronización de tiempo IEEE 802.1AS
- Control de flujo IEEE 802.3x
- Interfaz SMBus 2.0
- Estadísticas para SNMP MIB II, MIB tipo Ethernet y Ethernet MIB (IEEE 802.3z, Cláusula 30)
- Cumplimiento de administración de energía ACPI
- Administración de energía avanzada a través de una Unidad de administración de energía central (CPMU)
- Controlador regulador de conmutación integrado eficiente
- Control de temperatura en chip
- Soporte CLKREQ PCI Express
- Administración de energía de descarga (PM Offload)
- Memoria flash serial y soporte NVRAM EEPROM; configuración automática de memoria flash
- Detección y corrección de error ECC en SRAM interna
- Soporte de escaneo de límite JTAG

Power Management (Administración de energía)

Compatible con Wake on LAN (Magic Packet, Trama de Wake Up, patrón específico).

Nota: La conexión de velocidad del adaptador cuando el sistema está caído y esperando una señal de reactivación es de 10 Mbps o 100 Mbps, pero puede volver a 1000 Mbps cuando el sistema está activo y funcionando si está conectado a un conmutador con capacidad de 1000 Mbps. Los sistemas que intentan usar WOL deberán conectarse a un conmutador con capacidad de velocidad de 1000 y de 10/100 Mbps.

Frecuencia de interrupción adaptativa

El controlador del adaptador ajusta en forma inteligente la frecuencia de interrupción del host sobre la base de las condiciones de tráfico, a fin de incrementar el desempeño general de la aplicación. Cuando el tráfico es bajo, el controlador del adaptador interrumpe al host para cada paquete recibido, reduciendo al mínimo la latencia. Cuando el tráfico es pesado, el adaptador emite una interrupción del host para múltiples paquetes entrantes fondo contra fondo, preservando los ciclos de CPU del host.

Canales DMA duales

La interfaz PCIe en los adaptadores Broadcom NetXtremeGigabit Ethernet contiene dos canales DMA independientes para operaciones simultáneas de lectura y escritura.

ASIC con Procesador RISC intercalado

El control principal para los adaptadores Broadcom NetXtreme Gigabit Ethernet reside en un ASIC de alto desempeño firmemente integrado. El ASIC incluye un procesador RISC. Esta funcionalidad brinda flexibilidad para agregar nuevas características a la tarjeta y adaptarla a los requisitos de red futuros a través de la descarga de software.

Las operaciones de capacidad de manejo de Broadcom NetXtremecomo DMTF, SMASH, DASH y NC-SI pass-through funcionan con un motor de procesador de aplicaciones de alto rendimiento (APE), que se encuentra separado del motor de procesamiento de red tradicional.

Broadcom Advanced Control Suite

Broadcom Advanced Control Suite (BACS), un componente del software de equipos de Broadcom, es una utilidad integrada que ofrece información útil sobre cada adaptador de red instalado en su sistema. La utilidad BACS también le permite realizar pruebas, diagnósticos y análisis detallados en cada adaptador, como también modificar valores de propiedad y ver estadísticas de tráfico para cada adaptador. BACS se utiliza en sistemas operativos Windows para configurar equipos y agregar redes VLAN. Consulte Uso de Broadcom Advanced Control Suite para obtener información e instrucciones detalladas.

Entornos de operación con soporte

El adaptador Broadcom NetXtreme Gigabit Ethernet cuenta con soporte de software para los siguientes sistemas operativos:

- Microsoft® Windows® (32 bits y 64 bits extendido)
- LinLux® (32 bits y 64 bits extendido)
- VMware
- Oracle Solaris

Indicación de enlace de red y actividad

Para conexiones Ethernet de cable de cobre, el estado del enlace de red y actividad se indican a través de LED en el conector RJ-45, tal como se describe en Tabla 1: “Enlace de red y actividad indicada por los LED de puerto RJ-45,” en la página 14. Broadcom Advanced Control Suite también ofrece información sobre el estado del enlace de red y de la actividad (consulte Visualización de información del adaptador).

Tabla 1. Enlace de red y actividad indicada por los LED de puerto RJ-45

LED de puerto	*Apariencia del LED*	*Network Status (Estado de red)*
LED de enlace	OFF	Sin enlace (cable desconectado)
	Continuamente iluminado	Enlace
LED de actividad	OFF	No hay actividad de red
	Parpadeante	Actividad de red

Sección 2: Configuración de equipos

Nota: Consulte Servicios de equipos Broadcom Gigabit Ethernet para obtener información detallada sobre los siguientes temas:

- Glosario de términos y acrónimos
- Conceptos de equipo
- Componentes de software
- Requisitos del hardware
- Funciones con soporte por tipo de equipo
- Selección de un tipo de equipo
- Mecanismos de equipo
- Arquitectura
- Tipos de equipos
- Soporte de controladores por sistema operativo
- Velocidades de equipos soportadas
- Equipos y otras funciones avanzadas de conexión en red
- Aspectos generales de redes
- Aspectos relativos a las aplicaciones
- Detección y solución de problemas de equipos
- Preguntas formuladas con frecuencia
- Mensajes del registro de eventos

Resumen

Los equipos de adaptadores le permiten agrupar adaptadores de red para que funcionen como un equipo. La función de equipos incluye la asociación a VLAN, brindando balanceo de carga entre adaptadores y tolerancia a fallas. Estos beneficios pueden combinarse de manera que sea posible combinar la funcionalidad del balanceo de carga para los miembros de balance de carga y la capacidad de emplear tolerancia a fallas cuando el equipo se integra a diferentes VLAN.

Broadcom Advanced Server Program (BASP) es el software de equipos de Broadcom. En el caso de los sistemas operativos Windows, BASP se configura a través de la utilidad Broadcom Advanced Control Suite (BACS). Para los sistemas operativos Linux los equipos se forman por medio del entrelazado de canales (ver Equipos con entrelazado de canales).

BASP soporta cuatro tipos de equipos de balanceo de carga:

- Balanceo de carga inteligente y tolerancia a fallas (fail-over).
- Agregación de enlaces (802.3ad)
- Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static.
- SLB (Auto-Fallback Disable) (Auto-Fallback deshabilitada).

Load Balancing (Balanceo de carga) y tolerancia a fallas

El equipo provee balanceo de carga (load balancing) de tráfico y tolerancia a fallas (operación del adaptador redundante en caso de que falle una conexión de red). Cuando múltiples adaptadores se encuentran instalados en el mismo sistema, se pueden agrupar hasta en 16 equipos.

Cada equipo consta de hasta ocho adaptadores, con uno de ellos de reserva para los equipos Smart Load Balancing y Failover (SLB) o SLB (Auto-Fallback deshabilitada). Si no se identifica el tráfico en ninguna de las conexiones del equipo del adaptador debido a falla de este último, del cable o del conmutador, la carga será distribuida a los restantes miembros del equipo con una conexión activa. En caso de que todos los adaptadores primarios fallen, el tráfico será distribuido al adaptador de reserva. Se mantienen las sesiones existentes y no se produce ningún impacto en el usuario.

Tipos de equipos

En la siguiente tabla se indican los tipos de equipos disponibles para los sistemas operativos con soporte:

Tabla 2. Tipos de equipos

Sistema operativo:	Tipos de equipos disponibles
Windows Server 2008 y Windows Server 2012	Balanceo de carga inteligente y tolerancia a fallas (fail-over). Agregación de enlaces (802.3ad) Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static. SLB (Auto-Fallback Disable) (Auto-Fallback deshabilitada). **NOTA**: Windows Server 2012 ofrece soporte integrado para equipos, denominado Equipos NIC. No se recomienda que los usuarios permitan equipos a través de Equipos NIC y BASP al mismo tiempo en los mismos adaptadores.
Linux	Adaptadores de equipos que utilizan el módulo de kernel de entrelazado y una interfaz de entrelazado de canales: Consulte la documentación de Linux para obtener más información.

Balance de carga inteligente y tolerancia a fallas (fail-over).

El Balanceo de carga inteligente (Smart Load Balancing™) y la tolerancia a fallas (Failover) es la puesta en marcha por parte de Broadcom del balanceo de carga sobre la base del flujo de IP. Esta función soporta el balanceo de tráfico de IP a través de múltiples adaptadores (miembros de equipos) en forma bidireccional. En este tipo de equipo, todos los adaptadores del equipo tienen direcciones MAC separadas. Este tipo de equipo ofrece detección autómatica de fallas y traspaso dinámico a otro miembro del equipo o a un miembro en espera directo. Esto se realiza independientemente del protocolo de capa 3 (IP); en efecto, funciona con los conmutadores de capa 2 y 3 existentes. Para que funcione un equipo SLB no es necesario realizar la configuración del conmutador (como troncalización (trunking), agregación de enlaces (link aggregation)).

NOTAS:

- Si no habilita LiveLink™ al configurar los equipos SLB, se recomienda deshabilitar el protocolo STP (Protocolo de árbol de tramos) en el conmutador o puerto. De esta manera se minimiza el tiempo de inactividad que genera la determinación del bucle del árbol de tramos en casos de tolerancia a fallas. LiveLink mitiga estos problemas.
- Si un miembro del equipo está enlazado a 1000 Mbits/s y otro miembro del equipo está enlazado a 100 Mbits/s, la mayoría del tráfico será manejado por el miembro del equipo de 1000 Mbits/s.

Agregación de enlaces (802.3ad)

Este modo soporta el agregado de enlace y cumple con la especificación IEEE 802.3ad (LACP). El software de configuración le permite configurar dinámicamente aquellos adaptadores que desea que participen en un equipo determinado. Si el socio del enlace no está configurado correctamente para la configuración de enlace 802.3ad, se detectan y anotan los errores. Con este modo, todos los adaptadores del equipo se configuran para recibir paquetes para la misma dirección MAC. Nuestro controlador BASP determina el esquema de balanceo de carga saliente. El socio de enlace de equipo determina el esquema de balance de carga para los paquetes de entrada. En este modo, por lo menos uno de los socios de enlace debe estar en modo activo.

Troncalización genérica (Generic Trunking) (FEC/GEC)/ 802.3ad-Draft Static.

El tipo de equipo de Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static es muy similar al tipo de agregación de enlaces (Link aggregation) (802.3ad) en cuanto a que todos los adaptadores del equipo se configuran para recibir paquetes de la misma dirección MAC. Sin embargo, el tipo de equipo de Truncado genérico (FEC/GEC/802.3ad-Draft Static) no brinda soporte de LACP ni de protocolo marcador. Este tipo de equipo ofrece soporte para una variedad de entornos en que los socios del enlace del adaptador se configuran de manera estática para soportar un mecanismo de troncalizado patentado. Por ejemplo, este tipo de equipo podría usarse para soportar OpenTrunk de Lucent o Fast EtherChannel (FEC) de Cisco. Básicamente, se trata de una versión reducida del tipo de equipo de Agregado de enlace (802.3ad). Este enfoque es mucho más simple ya que no hay un protocolo de control de agregación de enlaces formalizado (LACP). Como con otros tipos, la creación de equipos y la asignación de adaptadores físicos a varios equipos se realizan estáticamente a través del software de configuración del usuario.

El tipo de equipo de Truncado genérico (FEC/GEC/802.3ad-Draft Static) da soporte al balanceo de carga y a la recuperación de fallas para el tráfico entrante y saliente.

SLB (Auto-Fallback Disable) (Auto-Fallback deshabilitada).

El tipo de equipo SLB (Auto-Fallback deshabilitada) es idéntico al tipo de Smart Load Balancing (Balanceo de carga inteligente) y Failover (Tolerancia a fallas), con la siguiente excepción: cuando el miembro en espera está activo, si un miembro primario vuelve a estar en línea, el equipo continúa usando al miembro en espera en vez de conmutar nuevamente al miembro primario.

Si algún adaptador primario asignado al equipo se desconecta, el equipo funciona como un equipo tipo balance de carga inteligente y tolerancia a fallas en el que ocurre una restauración.

Todas las interfaces primarias de un equipo participan en las operaciones de balanceo de carga (load balancing) enviando y recibiendo una parte del tráfico total. Las interfaces en espera se activan en caso de que todas las interfaces primarias hayan perdido sus enlaces.

Los equipos de tolerancia a fallas (failover teaming) realizan la operación de adaptador redundante (tolerancia a fallas) en caso de que falle una conexión de red. Si se desconecta el adaptador primario de un equipo debido a una falla del adaptador, cable o puerto de conmutador, el miembro del equipo secundario pasa a estar activo, redireccionando el tráfico entrante y saliente asignado originariamente al adaptador primario. Las sesiones se mantendrán, sin provocar ningún impacto para el usuario.

Limitaciones de los tipos de equipo Smart Load Balancing y Failover/SLB (Auto-Fallback deshabilitada)

El Balanceo de carga inteligente (Smart Load Balancing™/SLB) es un esquema de protocolo específico.

Tabla 3: Balanceo de carga inteligente

Sistema operativo:	***Failover/Fallback — Todos los de Broadcom***	***Failover/Fallback — Múltiples proveedores***
Protocolo	***IP***	***IP***
Windows Server 2008	S	S
Windows Server 2008 R2	S	S
Windows Server 2012	S	S
Sistema operativo:	***Load Balance — Todos los de Broadcom***	***Load Balance — Múltiples proveedores***
Protocolo	***IP***	***IP***
Windows Server 2008	S	S
Windows Server 2008 R2	S	S
Windows Server 2012	S	S
Windows Server 2012 R2	S	S

Leyenda: S = sí
N = no

N/S = no soportado

El tipo de equipo de Balanceo de carga inteligente (Smart Load Balancing) funciona con todos los conmutadores Ethernet sin que sea necesario configurar los puertos de los conmutadores en un modo de troncalizado especial. Solo se balancea la carga del tráfico IP en las direcciones entrantes y salientes. Los paquetes de otros protocolos se envían y reciben a través de una interfaz primaria exclusivamente. La tolerancia a fallas (failover) para tráfico que no es de IP se soporta sólo para los adaptadores de red de Broadcom. El tipo de equipo de Troncalizado genérico (Generic Trunking) requiere que el conmutador Ethernet soporte alguna forma de troncalizado de puertos (por ejemplo, Gigabit EtherChannel de Cisco o el modo de Agregación de enlaces (Link Aggregation) de otros proveedores de conmutadores). El tipo de equipo de Troncalizado genérico (Generic Trunking) es independiente del protocolo y todo el tráfico debe contar con balanceo de carga y tolerancia a fallas.

Nota: Si no habilita LiveLink™ al configurar los equipos, se recomienda deshabilitar el protocolo STP (Protocolo de árbol de tramos) en el conmutador. De esta manera se minimiza el tiempo de inactividad que genera la determinación del bucle del árbol de tramos en casos de tolerancia a fallas. LiveLink mitiga estos problemas.

Funcionalidad LiveLink™

La funcionalidad LiveLink™ es una característica de BASP que sólo se ofrece para el tipo de equipo Smart Load Balancing™ y Failover (Tolerancia a fallas). El propósito de LiveLink es detectar la conectividad de red más allá del conmutador y direccionar el tráfico sólo a través de los miembros del equipo que tienen un enlace activo. Esta función se habilita a través del software de equipos (see Configuración de LiveLink para un equipo Smart Load Balancing y Failover (Balance de carga inteligente y tolerancia a fallas) y SLB (Auto-Fallback Disable) (SLB) (Recuperación automática de fallas desactivada).). El software de equipos sondea periódicamente (emite un paquete de enlace desde cada miembro del equipo) uno o varios dispositivos de red de destino especificados. Los destinos de la sonda responden cuando reciben el paquete de enlace. Si un miembro del equipo no detecta la respuesta dentro de un período especificado después de una cantidad especificada de reintentos, el software de equipos interrumpe la transferencia del tráfico a través de ese miembro. Posteriormente, si ese miembro comienza a detectar una respuesta de un destino de la sonda, esto indica que se restableció el enlace y el software de equipos reanuda automáticamente la transferencia del tráfico a través de ese miembro. LiveLink sólo opera con los protocolos TCP/IP.

La funcionalidad LiveLink™ cuenta con soporte en los sistemas operativos Windows de 32 y 64 bits. Para una funcionalidad similar en sistemas operativos Linux, consulte la información sobre Entrelazado de canales en la documentación de Linux.

Equipos y soporte de Large Send Offload/ Checksum Offload (Descarga de envío grande/ Descarga de la suma de comprobación)

Las propiedades Large Send Offload (LSO) y Checksum Offload se habilitan para un equipo únicamente cuando todos los miembros soportan y están configurados para esa función.

Sección 3: Servicios de equipos Gigabit Ethernet de Broadcom

Introducción

Esta sección describe los aspectos tecnológicos y de implementación que deben tenerse en cuenta al trabajar con los servicios de equipos de redes que ofrece el software de Broadcom que se envía junto con los sistemas. El objetivo de los servicios de equipos de Broadcom es brindar tolerancia a fallas y agregación de enlaces para un equipo de dos o más adaptadores. La información que contiene este documento se proporciona para brindar asistencia a los profesionales de TI durante la implementación y solución de problemas de aplicaciones de sistema que requieren tolerancia a fallas y balanceo de carga.

Glosario

Tabla 4: Glosario

Elemento	Definición
ARP	Protocolo de resolución de dirección
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program (controlador intermedio)
DNS	Servicio de nombres de dominio
G-ARP	Protocolo gratuito de resolución de dirección
Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static.	Tipo de equipo de fallas y balanceo de carga que depende del conmutador en el que el controlador intermedio administra el tráfico saliente y el conmutador administra el tráfico entrante.
HSRP	Protocolo de enrutamiento de reserva directa
ICMP	Protocolo de control de mensajes de Internet
IGMP	Protocolo de administración de grupos de Internet
IP	Protocolo de Internet
LACP	Protocolo de control de agregación de vínculos
Agregación de enlaces (802.3ad)	Tipo de equipo de fallas y balanceo de carga con LACP que depende del conmutador en el que el controlador intermedio administra el tráfico saliente y el conmutador administra el tráfico entrante.
LOM	LAN en la placa base
MAC	Control de acceso a medio
NDIS	Especificación de Interfaz del Controlador de Dispositivos de Red
NLB	Network Load Balancing (Balanceo de carga de la red) de Microsoft
PXE	Entorno de ejecución de arranque previo
RAID	conjunto redundante de discos económicos

Tabla 4: Glosario

Elemento	Definición
Balance de carga inteligente y tolerancia a fallas.	Tipo de equipo independiente del conmutador en el que el miembro de equipo primario maneja todo el tráfico entrante y saliente mientras que el miembro de equipo en espera se mantiene ocioso hasta que ocurre un evento de falla (por ejemplo, una pérdida de enlace). El controlador intermedio (BASP) administra el tráfico entrante/saliente.
Balanceo de carga inteligente (SLB)	Tipo de equipo de fallas y balanceo de carga independiente del conmutador en el que el controlador intermedio administra el tráfico saliente/entrante.
TCP	Protocolo de control de transmisión
UDP	Protocolo de datagrama del usuario
WINS	Servicio de nombres de Internet de Windows
WLBS	Servicio de balanceo de carga de Windows

Conceptos de equipo

Direccionamiento de red

Para comprender el funcionamiento de los equipos, es importante comprender de qué modo funcionan los nodos de comunicación en una red Ethernet. Este documento parte de la premisa de que el lector se encuentra familiarizado con los conceptos básicos de los IP y las comunicaciones de redes Ethernet. La siguiente información brinda un resumen de alto nivel de los conceptos de direccionamiento de red que se utilizan en las redes Ethernet.

Todas las interfaces de las redes Ethernet de una plataforma host como un sistema computarizado, requieren de una dirección global única de capa 2 y al menos una dirección global única de capa 3. La capa 2 es la capa de enlace de datos y la capa 3 es la capa de red como se define en el modelo OSI (Interconexión de sistemas abiertos). La dirección de capa 2 se asigna al hardware y a menudo se la denomina dirección MAC o dirección física. Esta dirección se programa previamente en la fábrica y se almacena en NVRAM en una tarjeta de interfaz de red o en la placa base de sistema para una interfaz LAN intercalada. Las direcciones de capa 3 se denominan el protocolo o la dirección lógica que asignan a la pila de software. La IP es un ejemplo de un protocolo de capa 3. Además, la capa 4 (capa de transporte) utiliza los números de puerto para cada protocolo de red de nivel superior, como Telnet o FTP. Estos números de puerto se utilizan para diferenciar los flujos de tráfico de las aplicaciones. Los protocolos como TCP o UDP se utilizan más comúnmente en las redes de hoy en día. La combinación de la dirección IP y el número de puerto TCP se denomina socket.

Los dispositivos Ethernet se comunican con otros dispositivos Ethernet por medio de la dirección MAC, no de la dirección IP. Sin embargo, la mayoría de las aplicaciones funcionan con un nombre de host que se traduce en una dirección IP por medio de un servicio de asignación de nombres como WINS y DNS. Por lo tanto, se necesita de un método de identificación de la dirección MAC asignada a la dirección IP. El Protocolo de resolución de dirección de la red IP brinda este mecanismo. Una dirección de unidifusión corresponde a una única dirección MAC o IP. La dirección de transmisión se envía a todos los dispositivos de la red.

Los equipos y las direcciones de red

Un equipo de adaptadores funciona como una interfaz virtual de red única y para otros dispositivos de red es, en apariencia, igual a otros adaptadores no agrupados en equipos. Un adaptador de red virtual anuncia una única dirección de capa 2 o una o más direcciones de capa 3. Cuando se inicializa el controlador de equipos, selecciona una dirección MAC desde uno de los adaptadores físicos que componen el equipo como dirección MAC del equipo. Esta dirección en general se toma del primer adaptador que inicializa el controlador. Cuando el sistema que alberga el equipo recibe una solicitud ARP, selecciona una dirección MAC de entre los adaptadores físicos del equipo para utilizarla como dirección MAC de origen en la respuesta ARP. En los sistemas operativos de Windows, el comando IPCONFIG /all muestra la dirección IP y MAC del adaptador virtual y no las de los adaptadores físicos individuales. La dirección IP del protocolo se asigna a la interfaz de red virtual y no a los adaptadores físicos individuales.

Para los modos de equipos independientes de los conmutadores, todos los adaptadores físicos que componen un adaptador virtual deben utilizar una dirección MAC única asignada cuando transmiten datos. Es decir, las tramas que envían cada uno de los adaptadores físicos del equipo deben utilizar una única dirección MAC para cumplir con las normas IEEE. Es importante tener en cuenta que las entradas ARP de la caché no se obtienen de las tramas recibidas, sino de las solicitudes y las respuestas ARP.

Descripción de los tipos de equipos

- Balanceo de carga inteligente y tolerancia a fallas (fail-over).
- Troncalización genérica
- Agregación de enlaces (IEEE 802.3ad LACP)
- SLB (Auto-Fallback Disable) (Auto-Fallback deshabilitada).

Existen tres métodos para la clasificación de los tipos de equipos compatibles:

- Uno se basa en si la configuración del puerto de conmutación también debe coincidir con el tipo de equipo del adaptador.
- El segundo se basa en la funcionalidad del equipo, si soporta el balanceo de carga y la tolerancia a fallas o únicamente la tolerancia a fallas.
- El tercero se basa en si se utiliza el protocolo de control de agregación de vínculos.

Tabla 5 contiene un resumen de los tipos de equipos y su clasificación.

Tabla 5: Tipos de equipos disponibles

Tipo de equipo	Depende del conmutador (El conmutador debe ser compatible con un tipo de equipo específico)	El conmutador debe ser compatible con el protocolo de control de agregación de vínculos	Balanceo de carga	Tolerancia a fallas
Balanceo de carga inteligente y tolerancia a fallas (failover) (con dos a ocho miembros para el balanceo de carga)			•	•
SLB (Auto-Fallback Disable) (Auto-Fallback deshabilitada).				•
Agregación de enlaces (802.3ad)	•	•	•	•
Troncalización genérica (Generic Trunking) (FEC/ GEC)/802.3ad-Draft Static.	•		•	•

Balanceo de carga inteligente y tolerancia a fallas (fail-over).

El tipo de equipo de Smart Load Balancing™ (Balanceo de carga inteligente) y tolerancia a fallas brinda balanceo de carga y tolerancia a fallas y sólo tolerancia a fallas cuando así se lo configura. Funciona con cualquier conmutador Ethernet y no requiere que el conmutador se encuentre configurado para la troncalización. El equipo anuncia múltiples direcciones MAC y una o más direcciones IP (cuando utiliza direcciones IP secundarias). La dirección MAC del equipo se selecciona de una lista de miembros de balanceo de carga. Cuando el sistema recibe una solicitud ARP, la pila de software de red siempre envía una respuesta ARP con la dirección MAC del equipo. Para comenzar el proceso de balanceo de carga, el controlador

de equipo modifica esta respuesta ARP cambiando la dirección MAC de origen de modo que coincida con la de uno de los demás adaptadores físicos.

El balanceo de carga inteligente permite la transmisión y recepción del balaceo de carga en base a la dirección IP de capa 3/capa 4 y el número de puerto TCP/UDP. En otras palabras, el balanceo de carga no se realiza a nivel de los bytes o de las tramas, sino en base a una sesión TCP/UDP. Esta metodología es necesaria para mantener una entrega ordenada de tramas que pertenecen a la misma conversación de socket. El balanceo de carga cuenta con el soporte de 2 a 8 puertos. Estos puertos pueden incluir cualquier combinación de adaptadores incorporados y dispositivos LAN en la placa base(LOM). El balanceo de la carga de transmisión se logra mediante la creación de una tabla de direccionamiento calculado que utilice las direcciones IP de destino y los números de puertos TCP/UDP. La misma combinación de dirección IP de origen y destino y números de puerto TCP/UDP en general producen el mismo índice de direccionamiento calculado y por lo tanto señalan al mismo puerto del equipo. Cuando se selecciona un puerto para transmitir todas las tramas de un socket determinado, en la trama se incluye la dirección MAC única del adaptador físico, no la dirección MAC del equipo. Esto es necesario para cumplir con la norma IEEE 802.3. Si dos adaptadores transmiten utilizando la misma dirección MAC, ocurre una situación de duplicación de direcciones MAC y el conmutador no cumple con su función.

El balanceo de carga de recepción se logra a través de un controlador intermedio que envía ARP gratuitos cliente por cliente utilizando la dirección de unidifusión de cada cliente como dirección de destino de la solicitud ARP (conocida también como ARP direccionado). Esto se considera balanceo de carga del cliente y no balanceo de carga de tráfico. Cuando el controlador intermedio detecta un desequilibrio de carga significativo entre los adaptadores físicos de un equipo SLB, genera G-ARP a fin de redistribuir las tramas entrantes. El controlador intermedio (BASP) no responde a las solicitudes ARP, únicamente la pila de protocolo de software brinda la respuesta ARP solicitada. Es importante comprender que el balanceo de carga de recepción es una función de una cantidad de clientes que se conectan al sistema a través de la interfaz del equipo.

El balanceo de carga de recepción SLB intenta balancear la carga del tráfico entrante de las máquinas cliente en los puertos físicos del equipo. Utiliza un ARP gratuito modificado para anunciar una dirección MAC diferente para la dirección IP del equipo en la dirección física y de protocolo del remitente. Este G-ARP se envía a un único destino con la dirección MAC e IP de una máquina cliente en la dirección de destino física y de protocolo respectivamente. Esto hace que el cliente de destino actualice su caché ARP con un nuevo mapa de dirección MAC hacia la dirección IP del equipo. Los G-ARP no se transmiten porque provocaría que todos los clientes envíen su tráfico al mismo puerto. En consecuencia, se eliminarían los beneficios que se obtienen a través del balanceo de carga del cliente y podría generarse una entrega de tramas desordenada. Este esquema de recepción de balanceo de carga funciona siempre que todos los clientes y el sistema del equipo se encuentren en la misma subred o dominio de transmisión.

Cuando los clientes y el sistema se encuentran en diferentes subredes y el tráfico entrante debe atravesar un enrutador, la carga del tráfico recibido para el sistema no se balancea. El adaptador físico que el controlador intermedio ha seleccionado para transmitir el flujo IP transmite todo el tráfico. Cuando el enrutador envía una trama a la dirección IP del equipo, transmite una solicitud ARP (si no se encuentra en la caché ARP). La pila de software del servidor genera una respuesta ARP con la dirección MAC del equipo, pero el controlador intermedio modifica la respuesta ARP y la envía a través de un adaptador físico determinado, estableciendo así el flujo para dicha sesión.

Por este motivo el ARP no es un protocolo enrutable. No cuenta con un encabezado IP; por lo tanto, no se lo envía al enrutador o puerta predeterminada. El ARP es únicamente un protocolo de subred local. Además, dado que el G-ARP no es un paquete de transmisión, el enrutador no lo procesará y no actualizará su propia caché ARP.

La única manera de que el enrutador procese un ARP destinado para otro dispositivo de red es que haya un ARP Proxy habilitado y que el host no tenga una puerta predeterminada. Esto es muy poco común y no se recomienda para la mayoría de las aplicaciones.

La carga de transmisión de tráfico a través de un enrutador se balanceará porque el balanceo de la carga de transmisión se basa en las direcciones IP de origen y destino, y en el número del puerto TCP/UDP. Dado que los enrutadores no alteran las direcciones IP de origen y destino, el algoritmo de balanceo de carga funciona como fue concebido.

La configuración de los enrutadores para el Protocolo de enrutamiento de reserva directa (HSRP) no permite que ocurra el balanceo de la carga de recepción en el equipo de adaptador. En general, HSRP permite que dos enrutadores funcionen como un único enrutador anunciando una dirección IP y una dirección MAC virtuales. Un enrutador físico es la interfaz activa mientras que el otro se encuentra en espera. A pesar de que el HSRP también puede cargar nodos compartidos (utilizando diferentes puertas en los nodos host) en múltiples enrutadores en grupos HSRP, siempre apunta hacia la dirección MAC primaria del equipo.

Troncalización genérica

La troncalización genérica es un modo de equipo asistido por el conmutador y requiere que se configuren los puertos en ambos extremos del enlace: interfaces del servidor y puertos del conmutador. Con frecuencia se lo denomina Fast EtherChannel o Gigabit EtherChannel de Cisco. Además, la troncalización genérica es compatible con implementaciones similares de conmutadores de otros OEM como Load Sharing de Extreme Networks y el modo estático de agregación de enlaces de Bay Networks o IEEE 802.3ad. En este modo, el equipo anuncia una dirección MAC y una dirección IP cuando la pila de protocolo responde a las solicitudes ARP. Además, al transmitir tramas cada adaptador físico del equipo utiliza la misma dirección MAC del equipo. Esto es posible dado que el conmutador del otro extremo del vínculo reconoce el modo de equipo y maneja el uso de una única dirección MAC por cada uno de los puertos del equipo. La tabla de envíos del conmutador refleja la troncal como un puerto virtual único.

En este modo de equipo, el controlador intermedio controla el balanceo de carga y la tolerancia a fallas únicamente del tráfico saliente, mientras que el tráfico entrante está controlado por el firmware y el hardware del conmutador. Como en el caso del balanceo de carga inteligente, el controlador intermedio BASP utiliza las direcciones de origen y destino IP/TCP/UDP para balancear la carga del tráfico de transferencia del servidor. La mayoría de los conmutadores implementan direccionamiento calculado XOR de las direcciones MAC de origen y de destino.

Agregación de enlaces (IEEE 802.3ad LACP)

La agregación de enlaces es similar a la troncalización genérica salvo porque utiliza el protocolo de control de agregación de vínculos para negociar los puertos que formarán parte del equipo. El LACP debe estar habilitado en ambos extremos del enlace para que el equipo funcione. Si el LACP no se encuentra disponible en ambos extremos del enlace, 802.3ad ofrece una agregación manual que requiere únicamente que ambos extremos del enlace se encuentren en estado de conexión. Dado que la agregación manual permite la activación de un enlace miembro sin realizar los intercambios de mensajes del LACP, no debe considerarse tan confiable y sólida como un enlace negociado a través del LACP. El LACP determina automáticamente qué enlaces miembros pueden agregarse y luego los agrega. Permite el agregado y eliminación controlados de enlaces físicos en el proceso de agregación de enlaces de modo que no se pierdan ni dupliquen las tramas. La eliminación de un enlace miembro agregado es suministrada por el protocolo marcador que puede activarse opcionalmente para los enlaces agregados habilitados por medio del Protocolo de Control de Agregado de Enlaces (LACP).

El grupo de agregación de enlaces anuncia una única dirección MAC para todos los puertos de la troncal. La dirección MAC del agregador puede ser las direcciones MAC de uno de los MAC que conforman el grupo. El LACP y los protocolos marcadores utilizan una dirección de destino multidifusión.

La función de control de agregación de enlaces determina qué enlaces pueden agregarse y luego vincula los puertos a una función Aggregator (Agregador) del sistema y controla las condiciones a fin de determinar si es necesario realizar un cambio en el grupo de agregación. La agregación de enlaces combina la capacidad individual de múltiples enlaces para formar un enlace virtual de alto rendimiento. La falla o reemplazo de un enlace en una troncal LACP no provoca falta de conectividad. El tráfico simplemente se traslada a los enlaces restantes de la troncal.

SLB (Auto-Fallback Disable) (Auto-Fallback deshabilitada).

Este tipo de equipo es idéntico al del Balance de carga inteligente y tolerancia a fallas (fail-over), con la siguiente excepción: cuando el miembro en espera está activo, si un miembro primario vuelve a la línea, el equipo continúa usando el miembro en espera en vez de volver al miembro primario. Este tipo de equipo se admite sólo para situaciones en las que el cable de red está desconectado y se vuelve a conectar al adaptador de red. No tiene soporte para los casos en que el adaptador se extrae/instala mediante el Administrador de Dispositivos o un Conector directo PCI.

Si algún adaptador primario asignado al equipo se desconecta, el equipo funciona como un equipo tipo balance de carga inteligente y tolerancia a fallas en el que ocurre una restauración.

Componentes de software

Los equipos se implementan a través de un controlador intermedio NDIS en el entorno del sistema operativo Windows. Este componente de software funciona con el controlador de minipuerto, la capa NDIS y la pila de protocolo para activar la arquitectura de equipos (ver Figura 1). El controlador de minipuerto controla directamente el controlador LAN del host para habilitar funciones tales los envíos, recepciones e interrupciones de procesos. El controlador intermedio se ubica entre el controlador de minipuerto y la capa de protocolos, multiplexa diversas instancias del controlador de minipuerto y crea un adaptador virtual que para la capa NDIS tiene la apariencia de un adaptador único. NDIS ofrece un conjunto de funciones de biblioteca para activar las comunicaciones entre controladores de minipuerto o controladores intermedios y la pila de protocolo. Una dirección de protocolo como una dirección IP se asigna a cada instancia de dispositivo de minipuerto, pero cuando se instala un controlador intermedio, la dirección de protocolo se asigna al adaptador de equipo virtual y no a los dispositivos de minipuerto individuales que conforman el equipo.

El soporte para equipos de Broadcom se proporciona por medio de tres componentes de software independientes que funcionan de manera conjunta se soportan como un paquete. Cuando se actualiza un componente, todos los demás componentes deben actualizarse a las versiones soportadas. Tabla 6 describe los tres componentes de software y sus archivos asociados para los sistemas operativos compatibles.

Tabla 6: Componente del software de equipos de Broadcom

Componente de Software	Nombre de Broadcom	Windows	Linux
Controlador de minipuerto	Controlador base de Broadcom	b57nd60X.sys	tg3
Controlador intermedio	Broadcom Advanced Server Program (BASP)	Basp.sys	Entrelazado
Interfaz del usuario de configuración	Broadcom Advanced Control Suite (BACS)	BACS	BACS CLI
Controlador NDIS 6	Controlador x86 para Windows Vista y posteriores Controlador x64 para Windows Vista y posteriores	b57nd60x.sys b57nd60a.sys	N/A

La utilidad Broadcom Advanced Control Suite (BACS) ha sido diseñada para ejecutarse en la familia de sistemas operativos Windows Server de 32 bits y 64 bits. BACS se utiliza para configurar equipos de balanceo de carga y tolerancia a fallas y VLAN. Además, muestra la dirección MAC, la versión del controlador e información del estado de los adaptadores de red. BACS también incluye una serie de herramientas de diagnóstico como el diagnóstico de hardware, pruebas de cables y prueba de topología de red.

Requisitos del hardware

- Conmutador Ethernet
- Enrutador

Los diversos modos de equipo descritos en este documento imponen ciertas restricciones al equipo de red que se utiliza para conectar clientes a sistemas agrupados en equipos. Cada tipo de tecnología de interconexión de red tiene su efecto sobre los equipos tal como se describe en las siguientes secciones.

Conmutador Ethernet

Los conmutadores Ethernet permiten la división de una red Ethernet en varios dominios de transmisión. El conmutador es responsable de enviar paquetes Ethernet entre hosts basados únicamente en direcciones MAC Ethernet. Un adaptador de red física que se conecta a un conmutador puede funcionar en modo dúplex medio o dúplex completo.

Para brindar soporte para truncado genérico y agregación de enlaces IEEE 802.3ad. es necesario un conmutador que cuente con soporte específico para dicha funcionalidad. Si el conmutador no soporta estos protocolos, igualmente puede utilizarse para el balanceo de carga inteligente.

Enrutador

Los enrutadores están diseñados para enrutar el tráfico de red basado en protocolos de capa 3 o superiores, aunque a menudo funcionan como dispositivos de capa 2 con funciones de conmutación. Los equipos de puertos conectados directamente al enrutador no cuentan con soporte.

Funciones con soporte por tipo de equipo

Tabla 7 ofrece una función de comparación de los tipos de equipos que cuentan con el soporte de Broadcom NIC. Utilice esta tabla para determinar cuál es el mejor tipo de equipo para su aplicación. El software de equipos soporta hasta 8 puertos en un mismo equipo y hasta 16 equipos en un único sistema. Estos equipos pueden ser cualquier combinación de los tipos de equipos admitidos, pero cada uno debe estar en una red o subred independiente.

Tabla 7: Comparación de los tipos de equipo

Tipo de equipo	Tolerancia a fallas	Balanceo de carga	Troncalización estática que depende del conmutador	Independientes del conmutador Agregación dinámica de enlaces (IEEE 802.3ad)
Función	SLB con espera[a]	SLB	Troncalización genérica	Agregación de enlaces
Cantidad de puertos por equipo (igual dominio de transmisión)	2–8	2–8	2–8	2–8
Cantidad de equipos	16	16	16	16
Tolerancia a fallas del adaptador	Sí	Sí	Sí	Sí
Tolerancia a fallas del enlace del conmutador (igual dominio de transmisión)	Sí	Sí	Depende del conmutador	Depende del conmutador

Tabla 7: Comparación de los tipos de equipo (Cont.)

Tipo de equipo	Tolerancia a fallas	Balanceo de carga	Troncalización estática que depende del conmutador	Independientes del conmutador Agregación dinámica de enlaces (IEEE 802.3ad)
Balanceo de carga TX	No	Sí	Sí	Sí
Balanceo de carga RX	No	Sí	Sí (a cargo del conmutador)	Sí (a cargo del conmutador)
Requiere un conmutador compatible	No	No	Sí	Sí
Realiza transacciones de control para verificar la conectividad	No	No	No	No
Medios combinados (adaptadores con medios diferentes)	Sí	Sí	Sí (depende del conmutador)	Sí
Velocidades combinadas (adaptadores que no son compatibles con una velocidad común, pero que pueden funcionar a velocidades diferentes)	Sí	Sí	No	No
Velocidades combinadas (adaptadores que son compatibles con una velocidad común, pero que pueden funcionar a velocidades diferentes)	Sí	Sí	No (debe ser la misma velocidad)	Sí
Balanceo de carga TCP/IP	No	Sí	Sí	Sí
Equipos de proveedores combinados	Sí[b]	Sí[b]	Sí[b]	Sí[b]
Balanceo de carga no IP	No	Sí (Sólo tráfico IPX saliente)	Sí	Sí
Igual dirección MAC para todos los miembros del equipo	No	No	Sí	Sí
Igual dirección IP para todos los miembros del equipo	Sí	Sí	Sí	Sí
Balanceo de carga por dirección IP	No	Sí	Sí	Sí
Balanceo de carga por dirección MAC	No	Sí (utilizado para no IP/IPX)	Sí	Sí

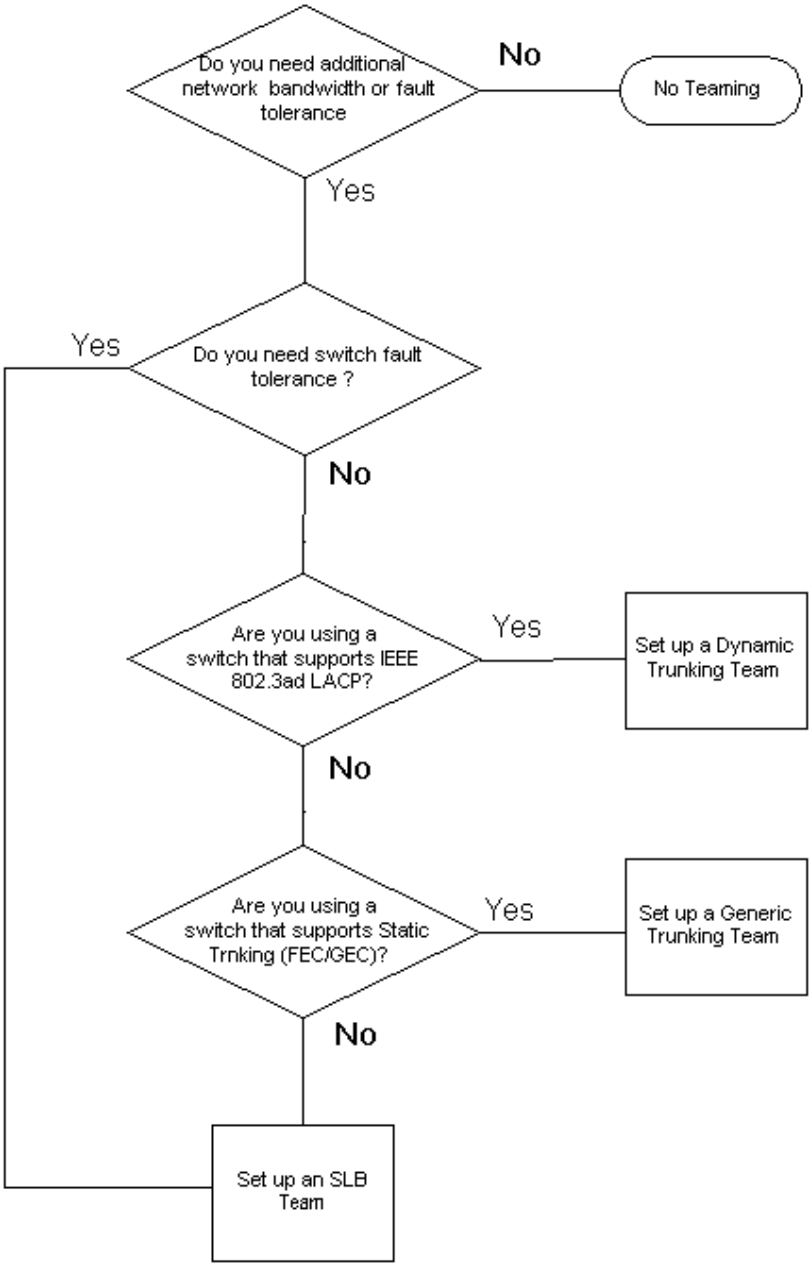
[a] SLB con un miembro primario y un miembro en espera.

[b] Requiere al menos un adaptador Broadcom en el equipo.

Selección de un tipo de equipo

El siguiente diagrama de flujo grafica el flujo de las decisiones al momento de crear equipos. El primer fundamento para la creación de equipos es la necesidad de ancho de banda de red y tolerancia a fallas adicionales. Los equipos ofrecen agregación de enlaces y tolerancia a fallas para satisfacer estos requisitos. La preferencia de los equipos debe seleccionarse en el siguiente orden: agregado de enlaces como la primera opción, troncalización genérica como la segunda opción y equipos SLB como la tercera opción cuando se utilizan conmutadores no administrados o conmutadores que no sean compatibles con las dos primeras opciones. Si la tolerancia a fallas del conmutador es un requisito, SLB es la única opción (ver Figura 1).

Figura 1: Proceso de selección de un tipo de equipo

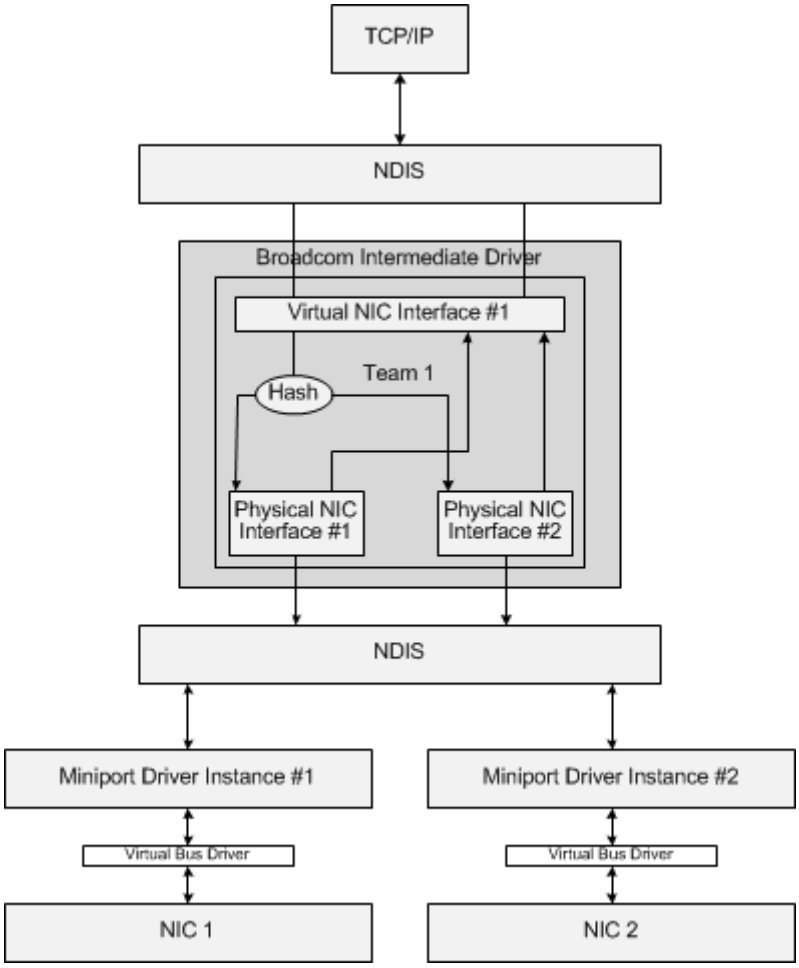


Mecanismos de equipo

Arquitectura

Broadcom Advanced Server Program se implementa como un controlador intermedio NDIS (ver Figura 2). Funciona bajo pilas de protocolo, como TCP/IP, y aparece como un adaptador virtual. Este adaptador virtual hereda la dirección MAC del primer puerto que inicializa el equipo. También debe configurarse una dirección de capa 3 para el adaptador virtual. La función primaria de BASP es balancear el tráfico entrante (para SLB) y saliente (para todos los modos de equipos) entre los adaptadores físicos instalados en el sistema seleccionado para la creación de equipos. Los algoritmos entrantes y salientes son independientes y ortogonales entre sí. Es posible asignar el tráfico saliente para una sesión en particular a un puerto dado y asignar el tráfico entrante correspondiente a un puerto diferente.

Figura 2: Controlador intermedio



Flujo de tráfico saliente

El controlador intermedio Broadcom administra el flujo de tráfico saliente para todos los tipos de equipos. Para el tráfico saliente, todos los paquetes se clasifican primero en un flujo y luego se distribuyen al adaptador físico seleccionado para su distribución. La clasificación del flujo un cálculo eficaz del direccionamiento calculado de los campos de protocolo conocidos. El valor resultante del cálculo de direccionamiento se utiliza para indexar una Tabla de direccionamiento calculado de flujo saliente. La entrada de direccionamiento calculado de flujo de salida seleccionada contiene el índice del adaptador físico seleccionado a cargo de la transmisión de dicho flujo. La dirección MAC de origen de los paquetes pasará a ser la dirección MAC del adaptador físico seleccionado. El paquete modificado luego se pasa al adaptador físico seleccionado para su transmisión.

Los paquetes TCP y UDP salientes se clasifican utilizando información de encabezado de capa 3 y capa 4. Este esquema mejora la distribución de carga de los servicios de protocolos de Internet más populares utilizando puertos conocidos como HTTP y FTP. Por lo tanto, BASP realiza el balanceo de carga en base a las sesiones TCP, no en base a los paquetes.

En las entradas de direccionamiento calculado de flujo de salida, los contadores de estadísticas también se actualizan después de la clasificación. El motor de balanceo de carga utiliza estos contadores para distribuir periódicamente los flujos entre los puertos en equipo. La ruta del código saliente ha sido diseñada para lograr mejor concurrencia posible cuando se habilitan múltiples accesos simultáneos a la tabla de direccionamiento calculado de flujo saliente.

Para los protocolos que no son TCP/IP, siempre se seleccionará el primer adaptador físico para los paquetes salientes. La excepción es el Protocolo de resolución de dirección (ARP), que se maneja de manera diferente a fin de lograr el balanceo de la carga entrante.

Flujo de tráfico entrante (Sólo SLB)

El controlador intermedio Broadcom administra el flujo de tráfico entrante para el modo de equipo SLB. A diferencia del balanceo de la carga saliente, el balanceo de la carga entrante sólo puede aplicarse a direcciones IP que se encuentran ubicadas en la misma subred que el servidor de balanceo de carga. El balanceo de carga entrante explota una característica única del Protocolo de resolución de dirección (RFC0826), en la que cada host IP utiliza su propia caché ARP para encapsular el datagrama en una trama Ethernet. BASP manipula cuidadosamente la respuesta ARP para direccionar cada host IP para enviar el paquete IP entrante al adaptador físico deseado. Por lo tanto, el balanceo de la carga entrante es un esquema que planifica con antelación en base al historial estadístico de los flujos entrantes. Las conexiones nuevas entre un cliente y el sistema siempre se establecen a través del adaptador físico primario (porque la respuesta ARP que genera la pila de protocolo del sistema operativo siempre asociará la dirección IP lógica con la dirección MAC del adaptador físico primario).

Como en el caso del flujo saliente, existe una Tabla de direccionamiento calculado del flujo entrante. Cada entrada de la tabla cuenta con una lista vinculada individualmente y cada vínculo (Entradas de flujo entrante) representa un host IP ubicado en la misma subred.

Cuando llega un datagrama IP, la entrada de flujo entrante correspondiente se localiza mediante el cálculo del direccionamiento de la dirección IP del datagrama IP. También se actualizan dos contadores estadísticos almacenados en la entrada seleccionada. El motor de balanceo de carga utiliza estos contadores del mismo modo que los contadores salientes para reasignar los flujos periódicamente al adaptador físico.

En la ruta del código entrante, la tabla de direccionamiento calculado de flujo entrante también se encuentra diseñada para el acceso simultáneo. Las listas de enlaces de las entradas de flujo entrante sólo aparecen como referencia en caso de proceso de paquetes ARP y balanceo periódico de carga. No existe una referencia por paquete en las entradas de flujo entrante. A pesar de que las listas de enlaces no se encuentran vinculadas, la sobrecarga en el procesamiento de cada paquete no ARP es siempre una constante. Sin embargo, el procesamiento de paquetes ARP, tanto salientes como entrantes, depende de la cantidad de enlaces dentro de la lista de enlaces correspondiente.

En la ruta de procesamiento entrante, también se emplea el filtrado para evitar que los paquetes transmitidos retornen a través del sistema desde otros adaptadores físicos.

Soporte de protocolo

La carga de los flujos ARP y IP/TCP/UDP se balancea. Si el paquete es un protocolo IP como ICMP o IGMP, todo el flujo de datos hacia una dirección IP en particular saldrá a través del mismo adaptador físico. Si el paquete utiliza TCP o UDP para el protocolo L4, se agrega el número de puerto al algoritmo de cálculo de direccionamiento, de modo que dos flujos L4 independientes puedan atravesar dos adaptadores físicos independientes hacia la misma dirección IP.

Por ejemplo, supongamos que el cliente tiene una dirección IP 10.0.0.1. Todo el tráfico IGMP e ICMP pasará a través del mismo adaptador físico porque sólo la dirección IP se utiliza para el direccionamiento calculado. La secuencia tendrá un aspecto similar al siguiente:

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

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

Si el servidor también envía flujo TCP y UDP a la misma dirección 10.0.0.1, pueden estar el mismo adaptador físico como IGMP e ICMP o en adaptadores físicos completamente diferentes desde ICMP e IGMP. La secuencia tendrá un aspecto similar al siguiente:

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

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

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

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

O las secuencias tendrán un aspecto similar al siguiente:

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

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

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

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

La asignación real entre adaptadores puede cambiar con el paso del tiempo, pero todo protocolo que no esté basado en TCP/UDP pasa por el mismo adaptador físico porque sólo la dirección IP se utiliza en el direccionamiento calculado.

Rendimiento

Las tarjetas de interfaz de red modernas ofrecen diversas funciones de hardware que reducen la utilización de la CPU mediante la descarga de ciertas operaciones intensivas para la CPU (ver Equipos y otras propiedades avanzadas de conexión en red). Por el contrario, el controlador intermedio BASP es una función puramente de software que debe examinar todos los paquetes recibidos de las pilas de protocolo y reaccionar ante su contenido antes de enviarlo a través de una interfaz física en particular. A través del controlador BASP puede procesar cada uno de los paquetes salientes de manera casi constante; algunas aplicaciones que pueden estar vinculadas con la CPU pueden presentar problemas si se las ejecuta por medio de una interfaz de equipo. Tales aplicaciones pueden ser más convenientes para aprovechar las capacidades de tolerancia a fallas del controlador intermedio en lugar de las funciones de balanceo de carga o pueden funcionar de manera más eficaz sobre un único adaptador físico que ofrezca una función de hardware en particular como Large Send Offload (Descarga de envío grande).

Soporte de controladores por sistema operativo

Como se indicó anteriormente, BASP es compatible con los entornos del sistema operativo Windows Server 2008 y 2012.

Las distintas funciones del modo de equipo se resumen en la siguiente tabla.

Tabla 8: Características del modo de equipos

Características	Soporte para Windows
Smart Load Balancing™	
Interfaz del usuario	BACS[a]
Cantidad de equipos	16
Cantidad de adaptadores por equipo	8
Reemplazo directo	Sí
Agregado directo	Sí
Eliminación directa	Sí
Soporte de velocidad de enlace	Velocidades diferentes
Protocolo de la trama	IP
Administración de paquetes entrantes	BASP
Administración de paquetes salientes	BASP
Evento de falla	Pérdida de enlace o evento LiveLink
Tiempo de falla	<500 ms
Tiempo de restauración	1,5 s[b] (aproximadamente)
Soporte LiveLink	Sí
Dirección MAC	Diferente
Equipos de múltiples proveedores	Sí
Troncalización genérica	
Interfaz del usuario	BACS
Cantidad de equipos	16
Cantidad de adaptadores por equipo	8
Reemplazo directo	Sí
Agregado directo	Sí
Eliminación directa	Sí
Soporte de velocidad de enlace	Velocidades diferentes
Protocolo de la trama	Todos
Administración de paquetes entrantes	Conmutador
Administración de paquetes salientes	BASP
Evento de falla	Pérdida de enlace únicamente
Tiempo de falla	500 ms
Tiempo de restauración	1,5 s[b] (aproximadamente)
Dirección MAC	La misma para todos los adaptadores
Equipos de múltiples proveedores	Sí
Troncalización dinámica	
Interfaz del usuario	BACS

Tabla 8: Características del modo de equipos (Cont.)

Características	Soporte para Windows
Cantidad de equipos	16
Cantidad de adaptadores por equipo	8
Reemplazo directo	Sí
Agregado directo	Sí
Eliminación directa	Sí
Soporte de velocidad de enlace	Velocidades diferentes
Protocolo de la trama	Todos
Administración de paquetes entrantes	Conmutador
Administración de paquetes salientes	BASP
Evento de falla	Pérdida de enlace únicamente
Tiempo de falla	<500 ms
Tiempo de restauración	1,5 s[b] (aproximadamente)
Dirección MAC	La misma para todos los adaptadores
Equipos de múltiples proveedores	Sí

[a] Broadcom Advanced Control Suite
[b] Asegúrese de que Port Fast o Edge Port (Puerto rápido o puerto de borde) se encuentren habilitados.

Velocidades de equipos soportadas

Las diferentes velocidades de enlace que soporta cada tipo de equipo se enumeran en Tabla 9. Velocidad combinada se refiere a la capacidad de los adaptadores de equipos que funcionan a diferentes velocidades de enlace.

Tabla 9: Velocidades de enlace en los equipos

Tipo de equipo	*Velocidad de enlace*	*Dirección del tráfico*	*Soporte de velocidad*
SLB	10/100/1000	Entrante/Saliente	Velocidad combinada
FEC	100	Entrante/Saliente	Igual velocidad
GEC	1000	Entrante/Saliente	Igual velocidad
IEEE 802.3ad	10/100/1000	Entrante/Saliente	Velocidad combinada

Equipos y otras propiedades avanzadas de conexión en red

Antes de crear un equipo, agregar o eliminar miembros de un equipo, o modificar los parámetros avanzados de un miembro de un equipo, asegúrese de que todos los miembros del equipo tengan una configuración similar. Los parámetros que deben controlarse incluyen VLAN y QoS Packet Tagging (Etiquetado de paquetes QoS), tramas gigantes y las diferentes descargas. Las propiedades avanzadas del adaptador y el soporte para equipos se encuentran enumerados en la Tabla 10.

Tabla 10: Propiedades avanzadas del adaptador y soporte para equipos

Propiedad del adaptador	Con soporte del adaptador virtual de equipos
Checksum Offload (Descarga de la suma de comprobación)	Sí
Etiquetado QoS IEEE 802.1p	No
Large Send Offload (Descarga de envío grande).	Sí[a]
Tramas gigantes	Sí[b]
IEEE 802.1Q VLANs	Sí
Wake On LAN	No
Entorno de ejecución de arranque previo(PXE)	Sí[c]

[a] Todos los adaptadores del equipo deben soportar esta característica. Si IPMI también se encuentra habilitado, es posible que algunos adaptadores no admitan esta función.
[b] Debe contar con el soporte de todos los adaptadores del equipo.
[c] Como servidor PXE exclusivo, no como cliente.

Checksum Offload (Descarga de la suma de comprobación)

La descarga de la suma de comprobación es una propiedad de los adaptadores de red de Broadcom que permiten que el hardware del adaptador calcule las sumas de comprobación TCP/IP/UDP del tráfico enviado y recibido en lugar de la CPU host. En situaciones de alto tráfico, esta característica puede permitir que un sistema maneje las conexiones con mayor eficacia que si la CPU estuviera obligada a calcular las sumas de comprobación. Esta propiedad es inherente del hardware y no obtiene beneficio alguno de una implementación de software únicamente. Un adaptador que soporta la descarga de la suma de comprobación anuncia esta capacidad al sistema operativo de modo que no sea necesario calcular la suma de comprobación en la pila de protocolo; dado que el controlador intermedio se encuentra ubicado directamente entre la capa de protocolo, la capa de protocolo no puede descargar ninguna suma de comprobación.

Etiquetado QoS IEEE 802.1p

La norma IEEE 802.1 incluye un campo de 3 bits (que soporta un máximo de 8 niveles de prioridad), que permite priorizar el tráfico. El controlador intermedio BASP no soporta el etiquetado QoS IEEE 802.1p.

Large Send Offload (Descarga de envío grande).

La descarga de envío grande (LSO) es una característica que ofrecen los adaptadores de red de Broadcom que evita que un protocolo superior como el TCP divida un gran paquete de datos en una serie de paquetes más pequeños y les inserte un encabezado. La pila de protocolo sólo debe generar un único encabezado para un paquete de 64 KB y el hardware adaptador divide el búfer de datos en tramas Ethernet de tamaños adecuados con encabezados en la secuencia correcta (basado en el encabezado único provisto originalmente).

Tramas gigantes

El controlador intermedio BASP soporta tramas gigantes, siempre que todos los adaptadores físicos del equipo también lo hagan y se configure el mismo tamaño para todos los adaptadores del equipo.

IEEE 802.1Q VLANs

La norma 802.3ac del IEEE define las extensiones de formato de trama para admitir el etiquetado de Red Virtual de Área Local Puenteada en redes Ethernet tal como lo indica la especificación IEEE 802.1Q. El protocolo VLAN permite insertar una etiqueta en una trama Ethernet a fin de identificar la VLAN a la cual pertenece. Si se encuentra presente, la etiqueta VLAN de cuatro bytes se inserta en la trama Ethernet entre la dirección MAC de origen y el campo longitud/tipo. Los primeros 2 bytes de la etiqueta VLAN constan del tipo de etiqueta IEEE 802.1Q, mientras que los segundos 2 bytes incluyen un campo de prioridad del usuario y el identificador VLAN (VID). Las redes LAN virtuales (VLAN) permiten que el usuario divida la LAN física segmentos lógicos. Cada red VLAN definida se comporta como una red independiente, con su tráfico y sus transmisiones aisladas de las otras, aumentando así la eficiencia del ancho de banda dentro de cada grupo lógico. Las redes VLAN también permiten que el administrador implemente políticas de seguridad y calidad de servicio (QoS) adecuadas. BASP soporta la creación de 64 redes VLAN por equipo o adaptador: etiquetadas y 1 sin etiquetar. Sin embargo, el sistema operativo y los recursos del sistema limitan la cantidad real de redes VLAN. El soporte para redes

VLAN se brinda de acuerdo con la norma IEEE 802.1q y cuenta con soporte tanto en entornos de equipos así como en un único adaptador. Observe que las redes VLAN cuentan con soporte con equipos homogéneos y no en entornos de equipos de diferentes proveedores. El controlador intermedio BASP soporta el etiquetado VLAN. Es posible vincular una o más redes VLAN a una única instancia del controlador intermedio.

Wake On LAN

Wake on LAN (WOL) es una función que permite activar un sistema que se encontraba inactivo mediante la llegada de un paquete específico a través de la interfaz Ethernet. Dado que se implementa un adaptador virtual como dispositivo exclusivo de software, carece de características de hardware para implementar wake on LAN y no puede habilitarse para activar el sistema a través del adaptador virtual. Sin embargo, el adaptador físico soporta esta propiedad incluso cuando forma parte de un equipo.

Entorno de ejecución de arranque previo (PXE)

El Entorno de ejecución de arranque previo (PXE) permite que un sistema se arranque desde una imagen de un sistema operativo en la red. Por definición, PXE se invoca antes de cargar un sistema operativo, por lo que el controlador intermedio BASP no puede cargar y habilitar un equipo. Por consiguiente, los equipos no cuentan con soporte como cliente PXE, aunque es posible utilizar como cliente PXE un adaptador físico que participa en un equipo cuando se carga el sistema operativo. Mientras que no es posible utilizar un adaptador de equipo como cliente PXE, sí es posible utilizarlo como servidor PXE, que brinda imágenes del sistema operativo a los clientes PXE por medio de una combinación del Protocolo de control del host dinámico (DHCP) y del Protocolo de transferencia de archivos trivial (TFTP). Ambos protocolos funcionan sobre IP y cuentan con soporte en todos los modos de equipos.

Aspectos generales de redes

Equipos entre conmutadores

Los equipos SLB pueden configurarse entre conmutadores. Sin embargo, los conmutadores deben estar conectados. La troncalización genérica y la agregación de enlaces no funcionan entre conmutadores porque cada una de estas implementaciones requiere que todos los adaptadores físicos del equipo compartan la misma dirección MAC Ethernet. Es importante observar que SLB sólo puede detectar la pérdida de enlace entre los puertos de un equipo y su socio de enlace inmediato. SLB no tiene manera de reaccionar ante otras fallas de hardware de los conmutadores y no puede detectar las pérdidas de enlace de otros puertos.

Tolerancia a fallas del enlace del conmutador

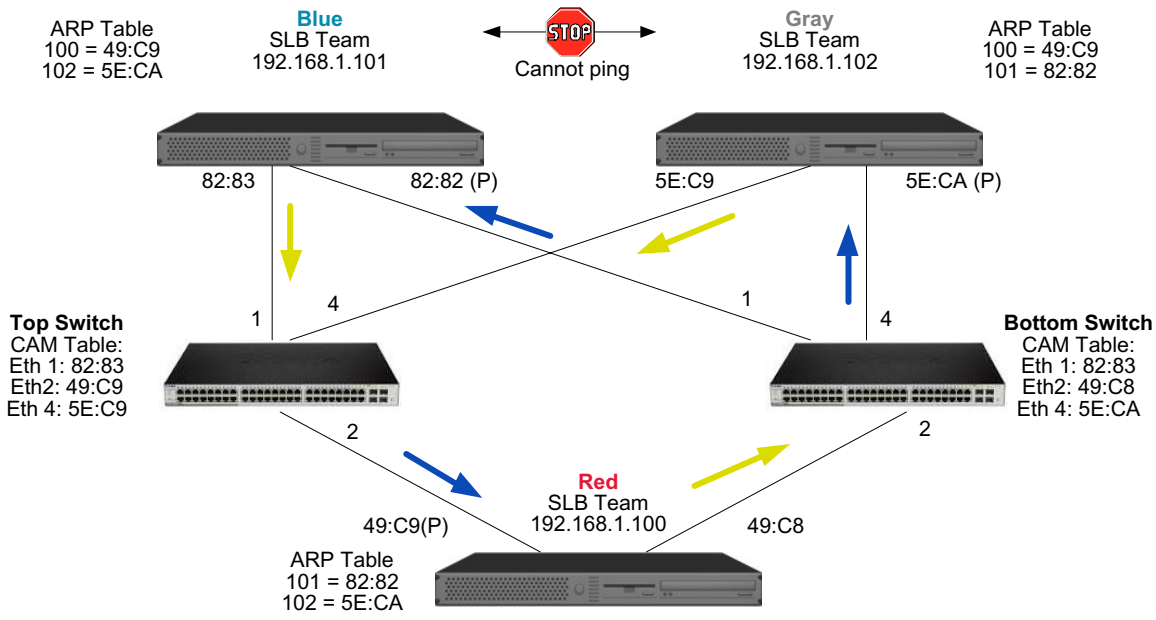
Los diagramas que aparecen a continuación describen el funcionamiento de un equipo SLB en una configuración de conmutador con tolerancia a fallas. Mostramos el mapeo de la solicitud de ping y las respuestas de ping en un equipo SLB con dos miembros activos. Todos los servidores (Azul, Gris y Rojo) realizan un ping continuo entre sí. Figura 3 es una configuración sin el cable de interconexión entre los dos conmutadores. Figura 4 tiene el cable de interconexión colocado y Figura 5 es un ejemplo de un evento de falla con el cable de interconexión colocado. Estas situaciones describen el comportamiento de los equipos entre dos conmutadores y la importancia del enlace de interconexión.

Los diagramas muestran que el miembro secundario del equipo envía solicitudes ICMP de eco (flechas amarillas) mientras que el miembro primario del equipo recibe las respuestas ICMP de eco correspondientes (flechas azules). Los mismos ilustran una característica clave del software de equipos. Los algoritmos de balanceo de carga no sincronizan el modo en el que se balancea la carga de las tramas cuando se las envía o recibe. En otras palabras, las tramas de una conversación en particular pueden salir y recibirse en diferentes interfaces del equipo. Esto ocurre para todos los tipos de equipos soportados por Broadcom. Por lo tanto, es necesario colocar un enlace de interconexión entre los conmutadores que conectan los puertos de un mismo equipo.

En la configuración sin interconexión, sale una solicitud ICMP del sistema Azul al Gris a través del puerto 82:83 con destino al puerto Gris 5E:CA, pero el conmutador superior no tiene manera de enviarla porque no puede alcanzar al puerto 5E:C9 del sistema Gris. Una situación similar se da cuando el sistema Gris intenta realizan un ping al sistema Azul. Sale una solicitud ICMP del puerto 5E:C9 con destino al puerto 82:82 del sistema Azul, pero no puede llegar. El conmutador superior no cuenta con una entrada para 82:82 en su tabla CAM porque no existe interconexión entre ambos conmutadores. Sin embargo, los pings fluyen entre el sistema Rojo y el Azul y entre el sistema Rojo y el Gris.

Además, un evento de falla puede provocar una pérdida adicional de conectividad. Considere una desconexión de cable del puerto 4 del conmutador superior. En este caso, el sistema Gris podría enviar la solicitud ICMP al puerto 49:C9 del sistema rojo, pero como el conmutador inferior no cuenta con una entrada para 49:C9 en su tabla CAM, la trama se envía a todos los puertos pero no puede llegar a 49:C9.

Figura 3: Equipos entre conmutadores sin enlace



El agregado de un enlace entre los conmutadores permite que el tráfico de/a Azul y Gris llegue a destino sin problemas. Observe las entradas adicionales en la tabla CAM para ambos conmutadores. El enlace de interconexión es esencial para el funcionamiento adecuado del equipo. En consecuencia, se recomienda contar con una troncal de agregación de enlaces para interconectar los dos conmutadores a fin de asegurar una gran disponibilidad para la conexión.

Figura 4: Equipos entre conmutadores con interconexión

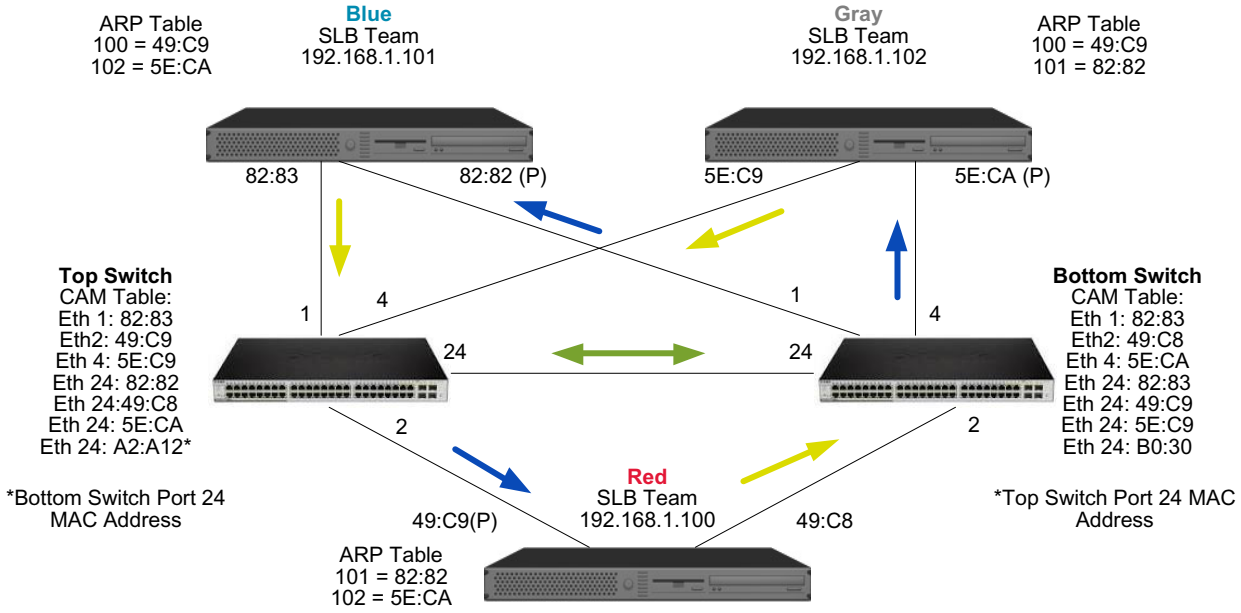
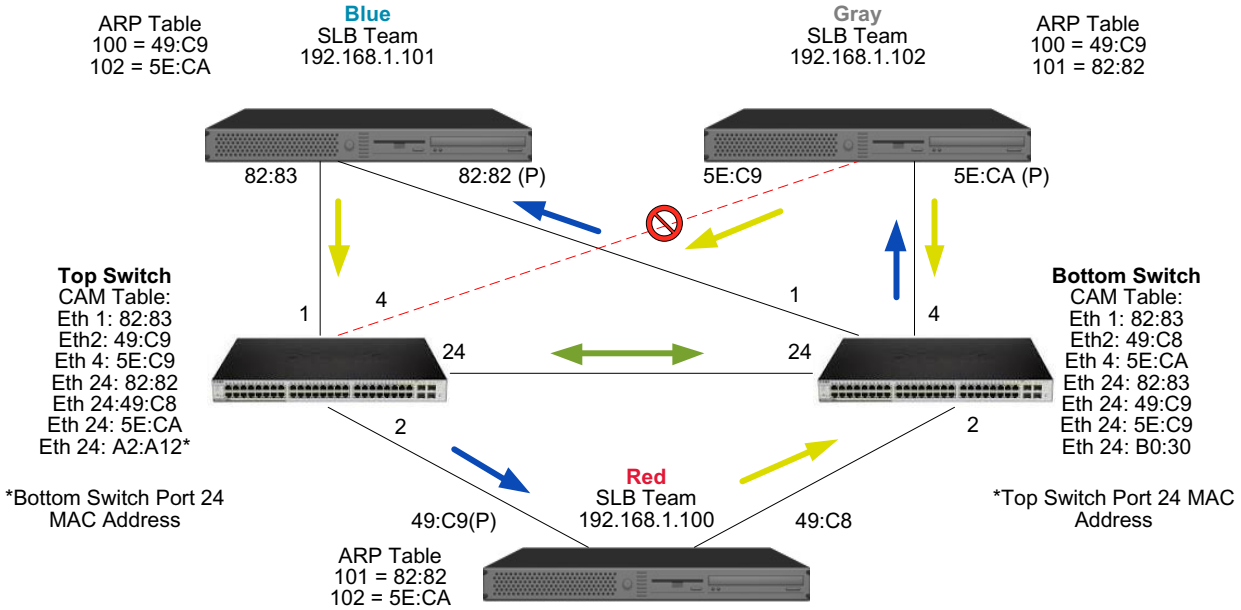


Figura 5 representa un evento de falla en el que el cable se desconecta del puerto 4 del conmutador superior. Se trata de una falla superada con éxito ya que todas las estaciones realizan un ping entre sí y no hay pérdida de conectividad.

Figura 5: Evento de falla



Algoritmo del árbol de expansión

- Aviso de cambio de topología (TCN)
- Port Fast / Edge Port (Puerto rápido/ puerto de borde)

En las redes Ethernet, sólo puede existir una ruta activa entre dos puentes o conmutadores. La presencia de múltiples rutas activas entre conmutadores puede provocar bucles en la red. Cuando ocurren los bucles, algunos conmutadores reconocen estaciones en ambos extremos del conmutador. Esta situación provoca una falla del algoritmo de envíos y permite la duplicación de las tramas que se enviarán. Los algoritmos del árbol de expansión brindan redundancia de las rutas mediante la definición de un árbol que expande todos los conmutadores a una red extendida y luego lleva ciertas rutas de datos redundante a un estado de espera (bloqueo). A intervalos regulares, los conmutadores de la red envían y reciben paquetes del árbol de expansión que utilizan para identificar la ruta. Si no es posible alcanzar un segmento de la red o si cambian los costos del árbol de expansión, el algoritmo del árbol de expansión reconfigura la topología del árbol de expansión y restablece el enlace mediante la activación de la ruta en espera. El funcionamiento del árbol de expansión es transparente para las estaciones finales, las que no detectan si se encuentran conectadas a un único segmento LAN o a una LAN conmutada de múltiples segmentos.

El protocolo del árbol de expansión (STP) es un protocolo de capa 2 diseñado para ejecutarse sobre puentes y conmutadores. La especificación para el STP se encuentra definida en la norma IEEE 802.1d. El objetivo principal del STP es asegurar que no ocurra una situación de bucle que genere rutas redundantes en su red. STP detecta/desactiva los bucles de la red y proporciona enlaces de respaldo entre los conmutadores o puentes. Permite que el dispositivo interactúe con otros dispositivos de su red que cumplen con el STP a fin de asegurar que exista sólo una ruta entre dos estaciones de la red.

Una vez establecida una topología de red estable, todos los puertos detectan mensajes BPDU (Unidad de datos del protocolo puente) "hello" que se transmiten desde el puente raíz. Si un puente no recibe un mensaje BPDU "hello" después de un intervalo predeterminado (Edad máx.), el puente supone que el enlace al puente raíz se encuentra desactivado. Luego, dicho puente inicia negociaciones con otros puentes para configurar la red a fin de restablecer una topología de red válida. El proceso de creación de una nueva topología puede demorar hasta 50 segundos. Durante este lapso las comunicaciones de extremo a extremo se interrumpen.

El uso del árbol de expansión no se recomienda para los puertos conectados a estaciones finales, porque por definición, una estación final no crea un bucle en un segmento Ethernet. Además, cuando un adaptador de equipo se conecta a un puerto con el árbol de expansión conectado, los usuarios pueden experimentar problemas de conectividad inesperados. Por ejemplo, considere un adaptador de equipo que ha perdido un enlace en uno de sus adaptadores físicos. Si el adaptador físico se reconecta (también conocido como restauración), el controlador inmediato detecta que el enlace se ha restablecido y comienza a transferir tráfico a través del puerto. Si el puerto se encuentra bloqueado por el protocolo del árbol de expansión, el tráfico se pierde.

Aviso de cambio de topología (TCN)

Un puente/conmutador crea una tabla de envíos de direcciones MAC y números de puertos registrando la dirección MAC de origen que recibe en un puerto en particular. La tabla se utiliza para enviar tramas a un puerto específico en lugar de enviar la trama a todos los puertos. En general, el tiempo de caducidad máximo de las entradas de la tabla es de 5 minutos. Únicamente cuando un host ha permanecido en silencio durante 5 minutos su entrada se elimina de la tabla. En ocasiones resulta beneficioso reducir el tiempo de caducidad. Un ejemplo se da cuando un enlace de envío pasa al bloqueo y otro enlace pasa del bloqueo al envío. Este cambio puede demorar hasta 50 segundos. Al finalizar el nuevo cálculo del STP habrá una nueva ruta disponible para las comunicaciones entre las estaciones finales. Sin embargo, dado que la tabla de envíos seguirá conteniendo entradas basadas en la topología anterior, no podrán restablecerse las comunicaciones hasta 5 minutos después de que se eliminen de la tabla las entradas de los puertos afectados. El tráfico se reenviará a todos los puertos y adquirirá nuevamente. En este caso resulta beneficioso reducir el tiempo de caducidad. Este es el objetivo del BPDU de aviso de cambio de topología (TCN). El TCN se envía desde el puente/conmutador afectado hacia el puente/conmutador raíz. En cuanto un puente/conmutador detecta un cambio de topología (un enlace que se desconecta o un puerto que pasa al modo de envío) envía un TCN al puente raíz a través de su puerto raíz. El puente raíz anuncia un BPDU con un Cambio de Topología a toda la red. Esto hace que todos los puentes reduzcan el tiempo de caducidad de la tabla MAC a 15 segundos durante un lapso especificado. Esto permite que el conmutador adquiera nuevamente las direcciones MAC en cuanto el STP converja nuevamente.

Los mensajes BPDU de Aviso de Cambio de Topología se envían cuando un puerto que se encontraba enviando cambia a bloquear o pasa a enviar. Un BPDU TCN no inicia una recalculación del STP. Afecta solamente el tiempo de caducidad de las entradas de la tabla de envíos del conmutador. No modifica la topología de la red ni crea bucles. Los nodos finales como servidores o clientes generan cambios de topología cuando se apagan y se encienden nuevamente.

Port Fast / Edge Port (Puerto rápido/ puerto de borde)

A fin de reducir el efecto de los TCN en la red (por ejemplo, el incremento de envíos en los puertos del conmutador), los nodos finales que se encienden / apagan a menudo deben utilizar el parámetro Port Fast o Edge Port en el puerto del conmutador al que están conectados. Port Fast o Edge Port es un comando que se aplica a puertos específicos y tiene los siguientes efectos:

- Los puertos que pasan de un enlace desconectado a un enlace conectado se colocarán en el modo STP de envío en lugar de pasar de detección a adquisición y luego a envío. STP sigue ejecutándose en estos puertos.
- El conmutador no genera un Aviso de Cambio de Topología cuando el puerto se activa o se desactiva.

Equipos con Microsoft NLB/WLBS

El modo de equipo SLB *no* funciona con el modo de unidifusión de Network Load Balancing (NLB) de Microsoft, únicamente funciona en el modo de multidifusión. Debido al mecanismo utilizado por el servicio NLB, la configuración de equipo recomendada en este entorno es Failover (tolerancia a fallas), (SLB con un NIC en espera) debido a que el balanceo de carga está administrado por NLB.

Aspectos relativos a las aplicaciones

Equipos y clústeres—Software de clústeres de Microsoft

En cada nodo de clústeres se recomienda encarecidamente que los clientes instalen al menos dos adaptadores de red (se aceptan adaptadores incorporados). Estas interfaces cumplen con dos funciones. Un adaptador se utiliza exclusivamente para comunicaciones *de transacciones de control* entre clústeres. Se denomina *adaptador privado* y a menudo reside en una subred privada independiente. El otro adaptador se utiliza para las comunicaciones de los clientes y se denomina *adaptador público*.

Es posible utilizar múltiples adaptadores para cada uno de loas siguientes fines: comunicaciones privadas, entre clústeres y comunicaciones públicas y externas de los clientes. Todos los modos de equipos de Broadcom cuentan con el soporte del software para clústeres de Microsoft Cluster únicamente para el adaptador público. Los equipos de adaptadores de redes privadas no cuentan con soporte. Microsoft indica que el uso de equipos en la interconexión privada de un clúster de servidor no cuenta con soporte por las demoras que podrían ocurrir en la transmisión y recepción de paquetes de transacciones de control entre los nodos. Para obtener mejores resultados, cuando desee obtener redundancia para la interconexión privada, desactive los equipos y utilice los puertos disponibles para crear una segunda interconexión privada. De esta manera se obtiene el mismo resultado final y se logran rutas de comunicación sólidas y duales para las comunicaciones entre nodos.

Para crear equipos en un entorno de clústeres, se recomienda que los clientes utilicen la misma marca de adaptadores.

Nota: Microsoft Network Load Balancing no cuenta con soporte en el software de clústeres de Microsoft.

Los equipos y las copias de respaldo de la red

Cuando realiza copias de respaldo de la red en un entorno sin equipos, el flujo total del servidor de copias de respaldo puede verse fácilmente afectado por el tráfico excesivo y la sobrecarga del adaptador. Dependiendo de la cantidad de servidores de copias de respaldo, secuencias de datos y velocidad de la unidad de cinta, el tráfico de las copias de respaldo puede consumir un alto porcentaje del ancho de banda del enlace de la red, generando un impacto negativo sobre el rendimiento de los datos de producción y las copias de respaldo en cinta. La realización de copias de respaldo de las redes en general consiste en un servidor dedicado con software de copias de respaldo en cinta como NetBackup, Galaxy o Backup Exec. Al servidor de copias de respaldo se conecta una unidad de cinta de copia de respaldo SCSI o una biblioteca de copia de respaldo conectada a través de una red de área de almacenamiento (SAN) fibre channel. Los sistemas de los que se realizan copias de respaldo a través de la red se denominan clientes o servidores remotos y en general tienen instalado un agente de software de copias de respaldo.

Dado que existen cuatro servidores cliente, el servidor de realización de copias de respaldo puede enviar una secuencia de cuatro tareas de copia de respaldo (una por cliente) a un autocargador de múltiples unidades. Sin embargo, a raíz del único enlace entre el conmutador y el servidor de realización de copias de respaldo, una copia de respaldo de 4 secuencias puede saturar fácilmente el adaptador y el enlace. Si el adaptador del servidor de copias de respaldo funciona a 1 Gbps (125 MB/s) y cada uno de los clientes puede enviar secuencias de datos a 20 MB/s durante la realización de la copia de respaldo en cinta, el desempeño entre el servidor de realización de copias de respaldo y el conmutador será de 80 MB/s (20 MB/s x 4), lo que equivale al 64 % del ancho de banda de la red. A pesar de que este valor se encuentra dentro del rango del ancho de banda de la red, el 64% constituye un alto porcentaje, en especial si otras aplicaciones comparten el mismo enlace.

Balanceo de carga y tolerancia a fallas

A medida que aumenta la cantidad de secuencias de copias de respaldo, incrementa el rendimiento general. Sin embargo, las secuencias de los clientes no pueden mantener el mismo rendimiento de una única cadena de copia de respaldo de 25 MB/s. En otras palabras, a pesar de que un servidor de copias de datos puede enviar una cadena de datos de un cliente a 25 MB/s, no se espera que cuatro tareas de copia de respaldo simultáneas se envíen en una secuencia de 100 MB/s (25 MB/s x 4 secuencias). A pesar de que el rendimiento general se incrementa en la medida en la que incrementan las secuencias de copias de respaldo, cada secuencia de copia de respaldo puede verse afectada por las limitaciones del software de cinta o de la pila de red.

Para que un servidor de copias de respaldo utilice de manera confiable el rendimiento del adaptador y el ancho de banda de la red al momento de hacer copias de respaldo de los clientes, la infraestructura de red debe implementar equipos como el balanceo de carga y la tolerancia a fallas. Los centros de datos deben incorporar conmutadores redundantes, agregación de enlaces y troncalización como parte de su solución de tolerancia a fallas. A pesar de que los controladores de los dispositivos de equipos manejan el modo en el que los datos fluyen a través de las interfaces de equipos y rutas de tolerancia a fallas, es transparente para las aplicaciones de realización de copias de respaldo y no interrumpe ningún sistema remoto en la red. Figura 6 muestra una topología de red que refleja las copias de respaldo en un entorno Broadcom de equipos y de qué modo el balanceo de carga inteligente puede *balancear la carga* de los datos de las copias de respaldo a través de adaptadores de equipos.

Existen cuatro rutas que el servidor cliente puede utilizar para enviar datos al servidor de realización de copias de respaldo, pero sólo una de estas rutas se designa durante la transferencia de datos. Una ruta posible que el servidor cliente rojo puede utilizar para enviar datos al servidor de realización de copias de respaldo es:

Ejemplo de ruta: El servidor cliente rojo envía datos a través del Adaptador A, Conmutador 1, Adaptador A del servidor de copias de respaldo.

La ruta designada se determina por medio de dos factores:

1. Caché ARP del servidor cliente; que apunta a la dirección MAC del servidor de realización de copias de respaldo. Esto se determina por medio algoritmo de balanceo de carga entrante del controlador intermedio de Broadcom.
2. La interfaz del adaptador físico del servidor cliente rojo se utilizará para transmitir los datos. Esto se determina por medio algoritmo de balanceo de carga saliente del controlador intermedio de Broadcom (ver Flujo de tráfico saliente y Flujo de tráfico entrante (Sólo SLB)).

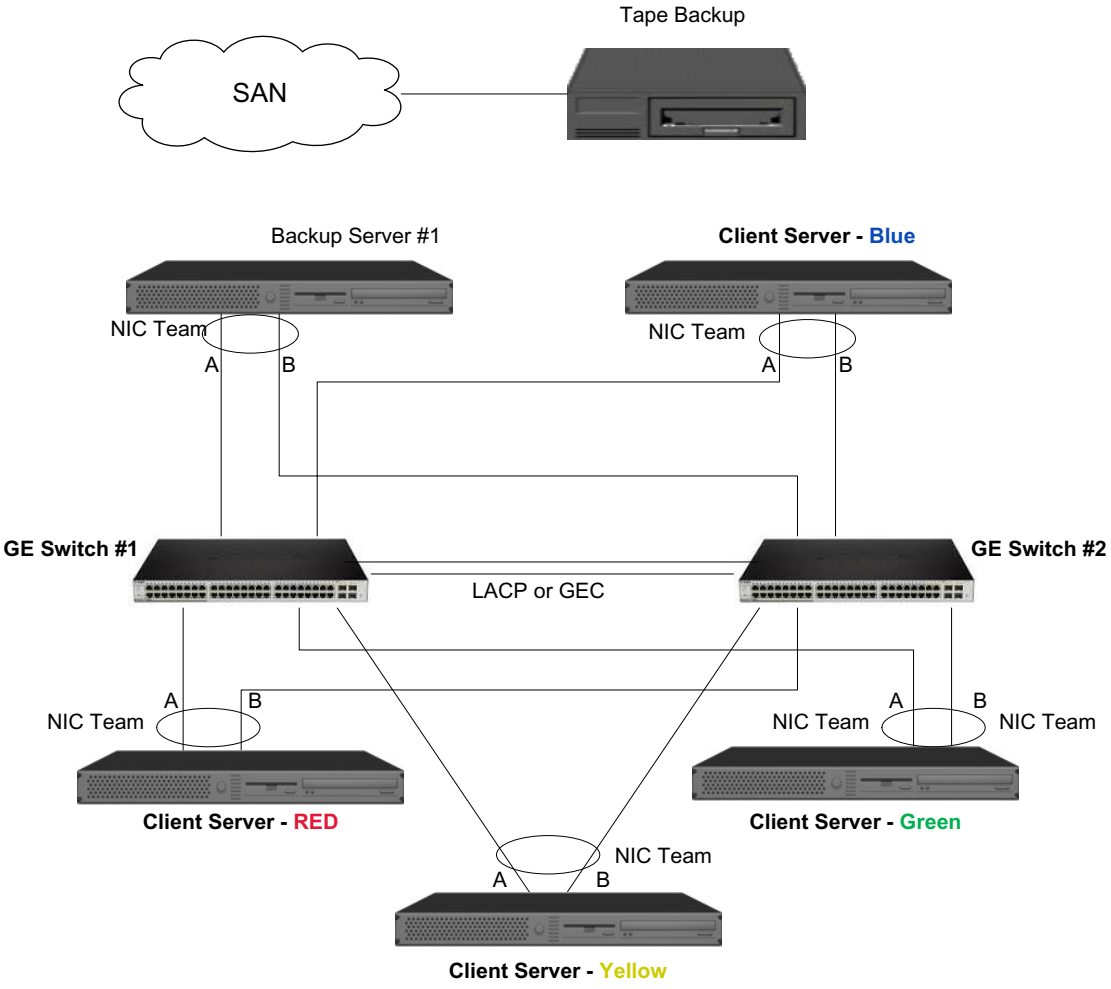
La interfaz de equipo del servidor de copias de respaldo transmite un protocolo de resolución de direcciones gratuito (G-ARP) al servidor cliente rojo, el que a su vez, hace que la caché ARP del servidor cliente se actualice con la dirección MAC del servidor de copias de respaldo. El mecanismo de balanceo de la carga de la interfaz de equipo determina la dirección MAC incorporada en el G-ARP. La dirección MAC seleccionada es básicamente el destino de la transferencia de datos desde el servidor cliente. En el servidor cliente rojo, el algoritmo de equipo SLB determinará cuál de las dos interfaces de adaptador se utilizará para transmitir los datos. En este ejemplo, los datos del servidor cliente rojo se reciben en la interfaz del adaptador A del servidor de copias de respaldo. Para demostrar el mecanismo SLB cuando se coloca una carga adicional en la interfaz de equipo, tenga en cuenta la situación que se da cuando el servidor de copias de respaldo inicia una segunda operación de copia de respaldo: una hacia el servidor cliente rojo y una hacia el servidor cliente azul. La ruta que utiliza el servidor cliente azul para enviar datos al servidor de copias de respaldo depende de la caché ARP, que apunta a la dirección MAC del servidor de copias de respaldo. Dado que el adaptador A del servidor de copias de respaldo ya cuenta con la carga de su tarea de realización de copias de respaldo del servidor cliente rojo, el servidor de copias de respaldo invoca su algoritmo SLB para *informar* al servidor cliente azul (a través de un G-ARP) que actualice su caché ARP para reflejar la dirección MAC del adaptador B del servidor de copias de respaldo. Cuando el servidor cliente azul necesita transmitir datos, utiliza una de sus interfaces de adaptador, que se determina por medio de su algoritmo SLB. Lo importante es que los datos del servidor cliente azul se reciben en la interfaz del adaptador B del servidor de copias de respaldo y no en su interfaz del adaptador A. Esto es importante porque con ambas secuencias de copia de respaldo ejecutándose de manera simultánea, el servidor de copia de respaldo debe *balancear la carga* de las secuencias de datos de diferentes clientes. Con ambas secuencias ejecutándose, cada interfaz de adaptador del servidor de copia de respaldo se procesa con una carga equivalente y de ese modo se balancea la carga de los datos a través de ambas interfaces de adaptador.

El mismo algoritmo se aplica si se inicia una tercera o cuarta operación desde el servidor de copias de respaldo. La interfaz de equipo del servidor de copias de respaldo transmiten un G-ARP de unidifusión a los clientes de los que se realiza una copia de respaldo, para informarles que actualicen su caché ARP. Luego, cada uno de los clientes transmite datos de la copia de respaldo a través de una ruta hacia la dirección MAC de destino del servidor de copia de respaldo.

Tolerancia a fallas

Si falla un enlace de red durante las operaciones de copia de respaldo en cinta, todo el tráfico entre el servidor de copias de respaldo y el cliente se interrumpe y las tareas de copia de respaldo fallan. Sin embargo, si la topología de la red se encuentra configurada para SLB de Broadcom y tolerancia a fallas del conmutador, esto permitirá que continúen las operaciones de realización de copias de respaldo sin interrupción durante la falla del enlace. Todos los procesos de tolerancia a fallas dentro de la red son transparentes a las aplicaciones de software de copias de respaldo en cinta. Para comprender cómo se direccionan las secuencias de datos de copias de respaldo durante el proceso de tolerancia a fallas de la red, tenga en cuenta la topología de la Figura 6. El servidor cliente rojo se encuentra transmitiendo datos a través de la ruta 1, pero ocurre una falla de enlace entre el servidor de copias de respaldo y el conmutador. Dado que los datos ya no pueden enviarse desde el conmutador #1 a la interfaz del adaptador A del servidor de copias de respaldo, los datos se redireccionen desde el conmutador #1 a través del conmutador #2, a la interfaz del adaptador B del servidor de copias de respaldo. Esto ocurre sin que la aplicación de copias de respaldo lo sepa porque todas las operaciones con tolerancia a fallas se encuentran manejadas por la interfaz del equipo de adaptadores y parámetros de troncales de los conmutadores. Desde el punto de vista del cliente, continúa funcionando como si transmitiese datos a través de la ruta original.

Figura 6: Realización de copias de respaldo con equipos SLB entre dos conmutadores



Detección y solución de problemas de equipos

Es posible que cuando se ejecute un analizador de protocolos sobre una interfaz de un equipo de adaptadores, la dirección MAC que aparece en las tramas transmitidas no sea la correcta. El analizador no muestra las tramas tal como las interpreta el BASP y muestra la dirección MAC del equipo y no la dirección MAC de la interfaz que transmite la trama. Se recomienda utilizar el siguiente procedimiento para controlar un equipo:

1. Replique todos los puertos de enlace ascendente desde el equipo del conmutador.
2. Si el equipo se extiende a dos conmutadores, replique también la troncal entre enlaces.
3. Realice un muestreo de todos los puertos replicados por separado.
4. En el analizador, utilice un adaptador y controlador que no filtren la información QoS y VLAN.

Consejos de configuración de equipos

Al solucionar problemas de conectividad de red o de funcionalidad de equipos, asegúrese de que la siguiente información coincida con su configuración.

1. Se recomienda que, para un equipo SLB, todos los adaptadores tengan la misma velocidad de enlace.
2. Si LiveLink no se encuentra habilitado, desactive el protocolo del árbol de expansión y habilite un modo STP que pase por alto la fase inicial (por ejemplo, Port Fast, Edge Port) para los puertos del conmutador conectados a un equipo.
3. Todos los conmutadores a los que el equipo se encuentra comunicado directamente deben tener la misma revisión de hardware, de firmware y de software para contar con soporte.
4. Para poder formar parte de un equipo, los adaptadores deben formar parte de la misma VLAN. En caso de que se configuren múltiples equipos, cada uno debe estar en una red independiente.
5. No ingrese una dirección de multidifusión o de difusión en el campo Locally Administered Address (Dirección administrada localmente).
6. No asigne la dirección administrada localmente a ningún adaptador físico que sea parte de un equipo.
7. Verifique que la administración de energía se encuentre deshabilitada para todos los miembros físicos de cualquier equipo (la casilla de verificación **Allow the computer to turn off this device to save power** (Permitir que la computadora apague el dispositivo para ahorrar energía) de la ficha **Power Management** (Administración de energía) de las **Properties** (Propiedades) del adaptador debe estar vacía—ver Configuración de las opciones de administración de energía en “Instalación del controlador y aplicación de Windows”).
8. Elimine cualquier dirección IP estática de los miembros físicos independientes del equipo antes de proceder a la creación del mismo.
9. Los equipos que requieren el máximo rendimiento deben utilizar LACP o GEC\FEC. En estos casos, el controlador intermedio sólo es responsable del balanceo de la carga saliente, mientras que el conmutador se encarga del balanceo de la carga entrante.
10. Los equipos agregados (802.3ad \ LACP y GEC\FEC) deben conectarse sólo a un conmutador único que soporte IEEE 802.3a, LACP o GEC/FEC.
11. No se recomienda conectar ningún equipo a un concentrador, dado que los concentradores solo soportan dúplex medio. Los concentradores deben conectarse a los equipos únicamente con el fin de solucionar problemas. Deshabilitar el controlador del dispositivo de un adaptador de red que participa en un equipo LACP o GEC/FEC puede ocasionar

efectos adversos en la conectividad de la red. Broadcom recomienda primero desconectar físicamente el adaptador del conmutador antes de deshabilitar el controlador del dispositivo a fin de evitar una pérdida de conectividad de la red.

12. Verifique que los controladores de base (Minipuerto) y de equipo (intermedio) pertenezcan al mismo paquete de versión.
13. Compruebe la conectividad de cada uno de los adaptadores físicos antes de crear equipos.
14. Compruebe la conducta de la tolerancia a fallas y la restauración del equipo antes de colocarlos en un entorno de producción.
15. Al pasar de una red no productiva a una red de producción se recomienda comprobar nuevamente la tolerancia a fallas y la recuperación.
16. Compruebe el rendimiento del equipo antes de colocarlo en un entorno de producción.

Pautas de detección y solución de problemas

Antes de llamar al soporte, asegúrese de haber llevado a cabo los siguientes pasos para detectar y solucionar problemas de conectividad de red cuando el servidor utiliza equipos de adaptadores.

1. Asegúrese de que la luz de Ethernet LINK se encuentre ENCENDIDA en todos los adaptadores y de que todos los cables se encuentren conectados.
2. Verifique que todos los controladores coincidentes de base e intermedios pertenezcan al mismo paquete de versión y que se encuentren cargados correctamente.
3. Verifique que exista una dirección IP válida por medio del comando **ipconfig** para Windows.
4. Verifique que el STP se encuentre deshabilitado o Edge Port/Port Fast (Puerto rápido/ puerto de borde) se encuentre habilitado en los puertos del conmutador conectados al equipo o que LiveLink se encuentre en uso.
5. Verifique que todos los adaptadores y el conmutador tengan la misma configuración para Link Speed (Velocidad de enlace) y Duplex (Dúplex).
6. Si es posible, divida el equipo y verifique la conectividad de cada uno de los componentes por separado a fin de confirmar que el problema está relacionado directamente con el equipo.
7. Verifique que todos los puertos del conmutador conectados al equipo se encuentren en la misma VLAN.
8. Verifique que los puertos del conmutador se encuentren configurados correctamente para el tipo de equipo Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static y que coincida con el tipo de equipo del adaptador. Si el sistema se encuentra configurado para el tipo de equipo SLB, asegúrese de que los puertos del conmutador correspondientes *no* se encuentren configurados para los tipos de equipos Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static.

Preguntas formuladas con frecuencia

Pregunta:	¿En qué circunstancias no se balancea la carga del tráfico? ¿Por qué la carga de todo el tráfico no se balancea uniformemente entre los miembros del equipo?
Respuesta:	La mayor parte del tráfico no utiliza IP/TCP/UDP o la mayor parte de los clientes se encuentra en una red diferente. El balanceo de carga entrante no es una función de la carga de tráfico, si no que es una función de la cantidad de clientes que se encuentran conectados al sistema.

Pregunta:	¿La carga de qué protocolos se balancea cuando forman parte de un equipo?
Respuesta:	El software de equipos de Broadcom soporta únicamente tráfico IP/TCP/UDP. Todo el tráfico de otro tipo se envía al adaptador primario.

Pregunta:	¿La carga de qué protocolos se balancea con SLB y la de cuáles no?
Respuesta:	Sólo la carga de los protocolos IP/TCP/UDP se balancea en ambas direcciones: enviar y recibir.

Pregunta:	¿Puedo formar un equipo con un puerto que funciona a 100 Mbps y otro puerto que funciona a 1000 Mbps?
Respuesta:	Las velocidades de enlace combinadas en un equipo cuentan con soporte únicamente para los equipos Smart Load Balancing™ y 802.3ad , tal como se especificó anteriormente.

Pregunta:	¿Puedo formar un equipo con un adaptador de fibra y un adaptador Gigabit Ethernet de cobre?
Respuesta:	Sí, con SLB. Y sí, si el conmutador lo permite en FEC/GEC y 802.3ad.

Pregunta:	¿Cuál es la diferencia entre el balanceo de carga del adaptador y Network Load Balancing de Microsoft (NLB)?
Respuesta:	El balanceo de carga del adaptador se realiza a nivel de una sesión de red, mientras que NLB se realiza a nivel de la aplicación del sistema.

Pregunta:	¿Puedo conectar el equipo de adaptadores a los puertos de un enrutador?
Respuesta:	No. Todos los puertos del equipo deben formar parte de la misma red; sin embargo, en un enrutador, por definición, cada uno de los puertos es una red independiente. Todos los modos de equipos requieren que el socio de enlace sea un conmutador de capa 2.

Pregunta:	¿Puedo crear equipos con los Servicios de Clúster de Microsoft?
Respuesta:	Sí. La creación de equipos cuenta con soporte únicamente en la red pública, no en la red privada que se utiliza para el enlace de transacciones de control.

Pregunta:	¿PXE funciona con un adaptador virtual (equipo)?
Respuesta:	Los clientes PXE funcionan en un entorno antes de que se cargue el sistema operativo; en consecuencia, los adaptadores virtuales todavía no se han cargado. Si el adaptador físico soporta PXE, puede utilizarse como cliente PXE, sea parte o no de un adaptador virtual en el momento en el que se carga el sistema operativo. Los servidores PXE pueden funcionar con un adaptador virtual.

Pregunta:	¿WOL funciona con un adaptador virtual (equipo)?
Respuesta:	La funcionalidad Wake-on-LAN funciona en un entorno antes de que se cargue el sistema operativo. WOL ocurre cuando el sistema se encuentra apagado o en espera, de modo que no existen equipos configurados.

Pregunta:	¿Cuál es la cantidad máxima de puertos que pueden conformar un equipo?
Respuesta:	Es posible asignar hasta 8 puertos a un equipo.

Pregunta:	¿Cuál es la cantidad máxima de equipos que pueden configurarse en el mismo sistema?
Respuesta:	Es posible configurar hasta 16 equipos en el mismo sistema.

Pregunta:	¿Por qué mi equipo pierde conectividad durante los primeros 30 a 50 segundos posteriores a la restauración del adaptador primario?
Respuesta:	Porque el protocolo de árbol de expansión está haciendo que el puerto pase de bloqueo a envío. Debe habilitar Port Fast o Edge Port (Puerto rápido o puerto de borde) en los puertos del conmutador o utilizar LiveLink compensar la demora del STP.

Pregunta:	¿Puedo conectar un equipo entre múltiples conmutadores?
Respuesta:	Smart Load Balancing puede utilizarse con múltiples conmutadores porque cada adaptador físico del equipo utiliza una dirección MAC Ethernet única. La agregación de enlaces y la troncalización genérica no pueden funcionar entre conmutadores porque requieren que todos los adaptadores físicos compartan la misma dirección MAC Ethernet.

Pregunta:	¿Cómo actualizo el controlador intermedio (BASP)?
Respuesta:	No es posible actualizar el controlador intermedio a través de las propiedades de la conexión de área local. Deba actualizarse por medio del instalador Setup.

Pregunta:	¿Cómo puedo determinar las estadísticas de rendimiento de un adaptador virtual (equipo)?
Respuesta:	En Broadcom Advanced Control Suite, haga clic en la ficha BASP Statistics (Estadísticas BASP) para el adaptador virtual.

Pregunta:	¿Puedo configurar NLB y crear equipos simultáneamente?
Respuesta:	Sí, pero únicamente cuando ejecute NLB en modo multidifusión (Los servicios de clústeres de Microsoft no soportan NLB).

Pregunta:	¿El sistema de copias de respaldo y los sistemas cliente deben conformar un equipo?
Respuesta:	Dado que el sistema de copias de respaldo posee la mayor carga de datos, siempre debe formar parte de un equipo para contar con agregación de enlaces y tolerancia a fallas. Sin embargo, una red completamente redundante requiere que tanto los conmutadores como los clientes de los que se realizan copias de respaldo conformen un equipo para obtener tolerancia a fallas y agregación de enlaces.

Pregunta:	Durante las tareas de realización de copias de respaldo, ¿el algoritmo de equipos del adaptador balancea los datos a nivel de los bytes o a nivel de la sesión?
Respuesta:	Cuando se utilizan equipos de adaptadores, se balancea la carga de los datos únicamente a nivel de sesión y no a nivel de los bytes a fin de evitar tramas desordenadas. El balanceo de carga de los equipos de adaptadores no funciona de la misma manera que otros mecanismos de balanceo de carga como EMC PowerPath.

Pregunta:	¿Se requiere de alguna configuración especial del software de copias de respaldo en cinta o del hardware para funcionar con los equipos de adaptadores?
Respuesta:	No se requiere ninguna configuración especial del software de cinta para funcionar con equipos. Los equipos son transparentes ante las aplicaciones de copias de seguridad.

Pregunta:	¿Cómo sé qué controlador estoy utilizando?
Respuesta:	En todos los sistemas operativos, el método más preciso para verificar la revisión del controlador es ubicar físicamente el archivo del controlador y ver sus propiedades.

Pregunta:	¿SLB puede detectar una falla de conmutador en una configuración de Tolerancia de fallas del conmutador?
Respuesta:	No. SLB solo puede detectar la pérdida de enlace entre el puerto del equipo y su socio de enlace inmediato. SLB no puede detectar fallas de enlace en otros puertos. Para obtener más información, consulte Funcionalidad LiveLink™.

Pregunta:	¿Dónde controlo las estadísticas en tiempo real para un equipo de adaptadores en un sistema Windows?
Respuesta:	Utilice Broadcom Advanced Control Suite (BACS) para controlar contadores generales, IEEE 802.3 y personalizados.

Mensajes del registro de eventos

Mensajes del registro de eventos de sistema de Windows

Los mensajes de estado básicos e intermedios conocidos del registro de eventos de sistema de Windows para los adaptadores Broadcom NetXtreme Gigabit Ethernet se enumeran en la siguiente sección. A medida que se carga el controlador del adaptador de Broadcom, Windows coloca un código de estado en el visor de eventos del sistema. Pueden existir dos clases de entradas para estos códigos de eventos dependiendo de si ambos controladores se encuentran cargados (un conjunto para el controlador de base o de minipuerto y otro para el controlador intermedio o de equipos).

Controlador de base (Adaptador físico/minipuerto)

Tabla 11 enumera los mensajes del registro de eventos que soporta el controlador de base, explica las causas del mensaje y brinda las acciones recomendadas.

Tabla 11: Mensajes del registro de eventos del controlador de base

Mensaje Número	Mensaje	Causa	Acción correctiva
1	Failed to allocate memory for the device block. (No se pudo asignar memoria para el bloque de dispositivos). Check system memory resource usage. (Verifique el uso de los recursos de memoria del sistema).	El controlador no puede asignar memoria del sistema operativo.	Cierre las aplicaciones que se estén ejecutando a fin de liberar memoria
2	Failed to allocate map registers (No se puede asignar registros de mapas).	El controlador no puede asignar registros de mapas del sistema operativo.	Descargue otros controladores que puedan asignar registros de mapas.
3	Failed to access configuration information. (No se pudo acceder a la información de configuración) Reinstall the network driver. (Reinstale el controlador de red).	El controlador no puede acceder a los registros del espacio de configuración PCI del adaptador.	Para adaptadores incorporados: coloque nuevamente en adaptador en la ranura, coloque el adaptador en otra ranura PCI o reemplace el adaptador.
4	The network link is down. (El enlace de red está desactivado). Check to make sure the network cable is properly connected. (Asegúrese de que el cable se encuentra conectado correctamente).	El adaptador ha perdido su conexión con su socio de enlace.	Controle que el cable de red se encuentre conectado, controle que el cable de red sea del tipo correcto y verifique que el socio de enlace (por ejemplo un conmutador o un concentrador) funcione correctamente.

Tabla 11: Mensajes del registro de eventos del controlador de base (Cont.)

Mensaje Número	Mensaje	Causa	Acción correctiva
5	The network link is up. (El enlace de red está activado).	El adaptador ha establecido una conexión con el enlace.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
6	Network controller configured for 10Mb half-duplex link. (Controlador de red configurado para enlace dúplex medio de 10 Mb).	El adaptador se ha configurado manualmente para la velocidad de línea y parámetros dúplex seleccionados.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
7	Network controller configured for 10Mb full-duplex link. (Controlador de red configurado para enlace dúplex completo de 10 Mb).	El adaptador se ha configurado manualmente para la velocidad de línea y parámetros dúplex seleccionados.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
8	Network controller configured for 100Mb half-duplex link. (Controlador de red configurado para enlace dúplex medio de 100 Mb).	El adaptador se ha configurado manualmente para la velocidad de línea y parámetros dúplex seleccionados.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
9	Network controller configured for 100Mb full-duplex link. (Controlador de red configurado para enlace dúplex completo de 100 Mb).	El adaptador se ha configurado manualmente para la velocidad de línea y parámetros dúplex seleccionados.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
10	Network controller configured for 1Gb half-duplex link. (Controlador de red configurado para enlace dúplex medio de 1 Gb).	El adaptador se ha configurado manualmente para la velocidad de línea y parámetros dúplex seleccionados.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
11	Network controller configured for 1Gb full-duplex link. (Controlador de red configurado para enlace dúplex completo de 1 Gb).	El adaptador se ha configurado manualmente para la velocidad de línea y parámetros dúplex seleccionados.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
12	Medium not supported. (medio no soportado).	El sistema operativo no soporta el medio IEEE 802.3.	Vuelva a arrancar el sistema operativo, ejecute el antivirus, ejecute una verificación de disco (chkdsk) y reinstale el sistema operativo.
13	Unable to register the interrupt service routine. (No se puede registrar la rutina de interrupción de servicio).	El dispositivo no puede instalar el manipulador de interrupción.	Vuelva a arrancar el sistema operativo; elimine los controladores de otros dispositivos que puedan estar compartiendo el mismo IRQ.
14	Unable to map IO space. (No sep puede mapear el espacio de E/S).	El controlador del dispositivo no puede asignar E/S mapeada por la memoria para acceder a los registros del controlador.	Elimine otros adaptadores del sistema, reduzca la cantidad de memoria física instalada y reemplace el adaptador.
15	Driver initialized successfully. (Controlador iniciado con éxito).	El controlador se cargó con éxito.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.

Tabla 11: Mensajes del registro de eventos del controlador de base (Cont.)

Mensaje Número	Mensaje	Causa	Acción correctiva
16	NDIS is resetting the miniport driver. (NDIS está restableciendo el controlador del minipuerto).	La capa NDIS ha detectado un problema al enviar/recibir paquetes y está restableciendo el controlador para resolver el problema.	Ejecute el diagnóstico de Broadcom Advanced Control Suite; verifique que el cable de red se encuentre en buenas condiciones.
18	Unknown PHY detected. (Se detectó un PHY desconocido). Using a default PHY initialization routine. (Se está utilizando una rutina de inicialización PHY predeterminada).	El controlador no puede leer la PHY ID.	Reemplace el adaptador.
19	This driver does not support this device. (Este controlador no soporta este dispositivo). Upgrade to the latest driver. (Actualice el controlador con la versión más reciente).	El controlador no reconoce el adaptador instalado.	Actualice el controlador con la versión más reciente que soporte este adaptador.
20	Driver initialization failed. (Falló la inicialización del controlador).	Falla no especificada durante la inicialización del controlador.	Reinstale el controlador, actualice el controlador, ejecute el diagnóstico de Broadcom Advanced Control Suite o reemplace el adaptador.
21	Ethernet@WireSpeed is enabled and could not negotiate maximum link speed. (Ethernet@WireSpeed está habilitado y no podrá negociar la velocidad máxima de enlace).	Posible problema con el cable o la conexión.	Vuelva a conectar o cambie el cable.
22	Unable to install device driver for obsolete network controller for this Operating System. (No puede instalar el controlador del dispositivo debido a un controlador de red obsoleto para este sistema operativo).	El último controlador de bandeja de salida ya no es compatible con el dispositivo.	Utilice el controlador de bandeja de entrada SO o reemplace el dispositivo por uno más reciente.
256	Not enough contiguous physical memory for coalescing pool. (No hay suficiente memoria física contigua para el grupo de fusión).	El controlador no puede asignar suficiente memoria compartida para los búfers de paquete de fusión.	Elimine o desactive otro adaptador del sistema o aumente la memoria del sistema.

Controlador intermedio (Adaptador virtual/ equipo)

Tabla 12 enumera los mensajes del registro de eventos que soporta el controlador intermedio, explica las causas del mensaje y brinda las acciones recomendadas.

Tabla 12: Mensajes del registro de eventos del controlador intermedio

Evento del sistema Número de mensaje	Mensaje	Causa	Acción correctiva
1	Unable to register with NDIS. (No se puede registrar en NDIS).	El controlador no puede registrarse con la interfaz NDIS.	Descargue otros controladores NDIS.
2	Unable to instantiate the management interface. (No se puede crear instancias de la interfaz de administración).	El controlador no puede creare una instancia del dispositivo.	Vuelva a arrancar el sistema operativo.
3	Unable to create symbolic link for the management interface. (No puede crearse un enlace simbólico para la interfaz de administración).	Otro controlador ha creado un nombre de dispositivo conflictivo.	Descargue el controlador de dispositivo conflictivo que utiliza el nombre *Blf*.
4	Broadcom Advanced Server Program Driver has started. (Se ha inicializado el controlador de Broadcom Advanced Server Program).	Otro controlador ha creado un nombre de dispositivo conflictivo.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
5	Broadcom Advanced Server Program Driver has stopped. (Se ha interrumpido Broadcom Advanced Server Program).	El controlador se ha detenido.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
6	Could not allocate memory for internal data structures. (No se pudo asignar memoria para las estructuras de datos internas).	El controlador no puede asignar memoria del sistema operativo.	Cierre las aplicaciones que se estén ejecutando a fin de liberar memoria
7	Could not bind to adapter. (No se puede vincular al adaptador).	El controlador no pudo abrir uno de los adaptadores físicos del equipo.	Descargue y cargue nuevamente el controlador del físico, instale un controlador de adaptador físico actualizado o reemplace el adaptador físico.
8	Successfully bind to adapter. (La vinculación con el adaptador se realizó con éxito).	El controlador abrió el adaptador físico con éxito.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
9	Network adapter is disconnected. (El adaptador de red se encuentra desconectado).	El adaptador físico no se encuentra conectado a la red (no ha establecido un enlace).	Controle que el cable de red se encuentre conectado, controle que el cable de red sea del tipo correcto y verifique que el socio de enlace (un conmutador o un concentrador) funcione correctamente.
10	Network adapter is connected. (El adaptador de red se encuentra conectado).	El adaptador físico se encuentra conectado a la red (ha establecido un enlace).	Se trata sólo de un mensaje informativo. No se requiere acción alguna.

Tabla 12: Mensajes del registro de eventos del controlador intermedio (Cont.)

Evento del sistema Número de mensaje	Mensaje	Causa	Acción correctiva
11	Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System. (Broadcom Advanced Program Features Driver no está diseñado para funcionar con esta versión de sistema operativo).	El controlador no soporta el sistema operativo en el que ha sido instalado.	Consulte las notas de la versión del controlador e instale el controlador en un sistema operativo soportado o actualice el controlador.
12	Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter. (El adaptador de espera directa está seleccionado como adaptador primario para un equipo sin un adaptador de balanceo de carga).	Se ha activado un adaptador en espera.	Reemplace el adaptador físico que presenta fallas.
13	Network adapter does not support Advanced Failover. (El adaptador de red no soporta la restauración avanzada).	El adaptador físico no soporta la extensión de NIC de Broadcom (NICE).	Reemplace el adaptador por uno que soporte NICE.
14	Network adapter is enabled via management interface. (El adaptador de red se encuentra habilitado a través de la interfaz de administración).	El controlador ha habilitado con éxito un adaptador físico a través de la interfaz de administración.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
15	Network adapter is disabled via management interface. (El adaptador de red se encuentra deshabilitado a través de la interfaz de administración).	El controlador ha deshabilitado con éxito un adaptador físico a través de la interfaz de administración.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
16	Network adapter2 is activated and is participating in network traffic. (El adaptador de red se encuentra activado y participa del tráfico de red).	Un adaptador físico se ha sumado o activado dentro de un equipo.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.
17	Network adapter is de-activated and is no longer participating in network traffic. (El adaptador de red se encuentra desactivado y ya no participa del tráfico de red).	El controlador no reconoce el adaptador instalado.	Se trata sólo de un mensaje informativo. No se requiere acción alguna.

Sección 4: Redes LAN virtuales

Descripción general de las redes VLAN

Las LAN virtuales (VLAN) le permiten dividir su LAN física en partes lógicas, para crear una segmentación lógica de grupos de trabajo y para poner en marcha políticas de seguridad entre cada segmento lógico. Cada red VLAN definida se comporta como una red independiente, con su tráfico y sus transmisiones aisladas de las otras, aumentando así la eficiencia del ancho de banda dentro de cada grupo lógico. Se pueden definir hasta 64 VLAN (63 con etiquetas y 1 sin etiqueta) para cada adaptador Broadcom de su servidor, de acuerdo con la cantidad de memoria disponible en su sistema.

Se pueden agregar redes VLAN a un equipo para admitir múltiples redes VLAN con diferentes ID de VLAN. Se crea un adaptador virtual para cada VLAN agregada.

Si bien las VLAN se usan generalmente para crear dominios de transmisión individuales y/o subredes IP separadas, a veces resulta útil que un servidor tenga presencia en más de una VLAN simultáneamente. Los adaptadores de Broadcom soportan múltiples VLAN por puerto o por equipo, permitiendo configuraciones de red muy flexibles.

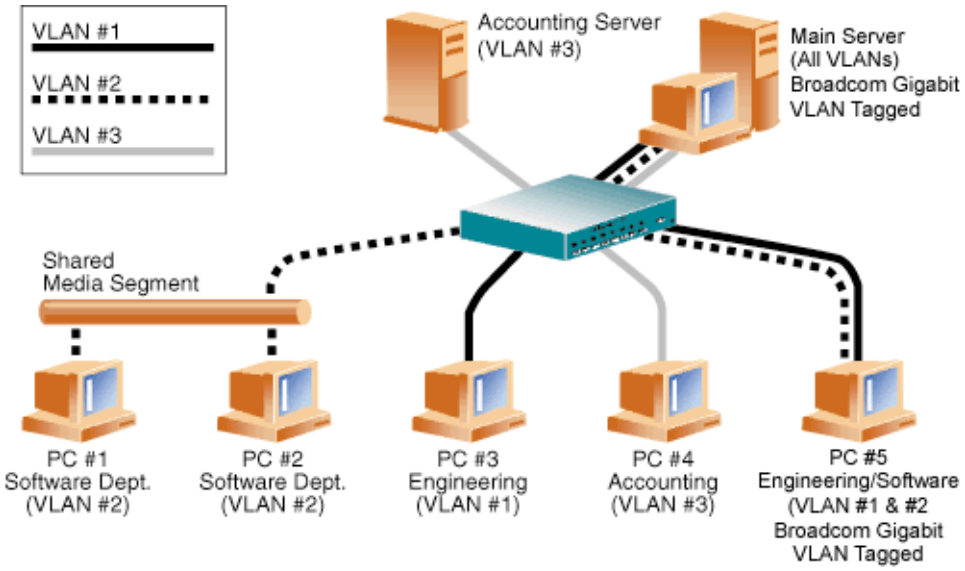


Figura 7: Ejemplo de servidores que soportan múltiples VLAN con etiquetas

Figura 7 muestra un ejemplo de una red que utiliza VLAN. En este ejemplo de red, la LAN física consta de un conmutador, dos servidores y cinco clientes. La LAN se organiza lógicamente en tres VLAN diferentes; cada una representa una subred IP diferente. Las características de esta red se describen en Tabla 13:

Tabla 13: Ejemplo de Topología de red VLAN

Componente	*Descripción*
VLAN #1	Una subred IP que consta del Servidor principal, PC #3 y PC #5. Esta subred representa un grupo de ingeniería.
VLAN #2	Incluye el Servidor principal, PC #1 y #2 a través del segmento de medio compartido y PC #5. Esta VLAN es un grupo de desarrollo de software.
VLAN #3	Incluye el Servidor principal, el Servidor contable y PC #4. Esta VLAN es un grupo contable.
Nombre de servidor primario	Un servidor de alto uso al que se debe acceder desde todas las VLAN y subredes IP. El Servidor principal tiene un adaptador Broadcom instalado. Se accede a las tres subredes IP a través de la única interfaz de adaptador físico. El servidor está conectado a una de las bocas del conmutador, que está configurada para las VLAN #1, #2 y #3. Tanto el adaptador como el puerto del conmutador conectado tienen activa las etiquetas. Debido a las capacidades de etiquetado de VLAN de ambos dispositivos, el servidor puede comunicarse en las tres subredes de IP de esta red, pero continúa manteniendo separación de transmisión entre todas ellas.
Servidor contable	Sólo disponible para VLAN #3. El Servidor contable está aislado de todo el tráfico de las VLAN #1 y #2. El puerto del conmutador conectado al servidor tiene inactivo el etiquetado.
PC #1 y #2	Conectado a un concentrador de medios compartido que luego se conecta al conmutador. Las PC #1 y #2 pertenecen sólo a la VLAN #2 y están lógicamente en la misma subred IP que el Servidor principal y PC #5. El puerto del conmutador conectado a este segmento tiene inactivo el etiquetado.
PC #3	Un miembro de la VLAN #1, PC #3 puede comunicarse sólo con el Servidor principal y PC #5. El etiquetado no está activo en el puerto del conmutador PC #3.
PC #4	Un miembro de la VLAN #3, PC #4 sólo puede comunicarse con los servidores. El etiquetado no está activo en el puerto del conmutador PC #4.
PC #5	Un miembro de las VLAN #1 y #2, PC #5 tiene instalado un adaptador de Broadcom. Está conectado al puerto #10 del conmutador. Tanto el adaptador como el puerto del conmutador están configurados para las VLAN #1 y #2 y tienen el etiquetado activo.

Nota: El etiquetado de VLAN sólo debe estar habilitado en puertos de conmutador que crean enlaces troncalizados a otros conmutadores o en puertos conectados a estaciones finales con capacidad de etiquetado, tales como servidores o estaciones de trabajo con adaptadores Broadcom.

Cómo agregar una VLAN a un equipo

Cada equipo soporta hasta 64 VLAN (63 con etiquetas y 1 sin etiqueta). Con múltiples VLAN en un adaptador, un servidor con un solo adaptador puede tener una presencia lógica en múltiples subredes IP. Con múltiples VLAN en un equipo, un servidor puede tener una presencia lógica en múltiples subredes IP y aprovechar el balanceo de cargas y fallas. Para obtener instrucciones acerca de cómo agregar una VLAN a un equipo, consulte Agregue una red VLAN para los sistemas operativos Windows.

Nota: Los adaptadores que son miembros de un equipo de fallas también se pueden configurar para soportar las VLAN. Como las VLAN no son compatibles con un NIC de terceros, si un NIC de terceros es un miembro de un equipo de fallas, las VLAN no se podrán configurar para dicho equipo.

Sección 5: Capacidad de manejo

CIM

El Modelo de información común (CIM) es un estándar de la industria definido por la Distributed Management Task Force (DMTF). Microsoft instala CIM en plataformas de Windows tales como Windows Server 2008. Broadcom admitirá CIM en plataformas Windows Server 2008.

La instalación de CIM realizada por Broadcom provee varias clases para brindar información a los usuarios a través de aplicaciones cliente de CIM. Recuerde que el proveedor de datos CIM de Broadcom solo proveerá datos y los usuarios pueden elegir su software cliente CIM preferido para analizar la información expuesta por el proveedor CIM de Broadcom.

El proveedor CIM de Broadcom brinda información a través de las clases BRCM_NetworkAdapter y BRCM_ExtraCapacityGroup. La clase BRCM_NetworkAdapter provee información del adaptador de red perteneciente a un grupo de adaptadores que incluyen controladores de Broadcom y de otros proveedores. La clase BRCM_ExtraCapacityGroup provee configuración de equipo para el Programa de servidor avanzado de Broadcom (BASP). La instalación actual provee información de equipo e información de adaptadores de red físicos en el equipo.

El Programa servidor avanzado de Broadcom provee los eventos a través de registros cronológicos de eventos. Los usuarios pueden utilizar el "Visualizador de Eventos" provisto por las plataformas Windows Server 2008, o utilizar CIM para inspeccionar o monitorear estos eventos. El proveedor CIM de Broadcom también proveerá información de eventos a través del modelo de eventos genéricos de CIM. Estos eventos son __InstanceCreationEvent, __InstanceDeletionEvent y __InstanceModificationEvent y son definidos por CIM. CIM requiere que la aplicación cliente registre los eventos desde la aplicación cliente, usando consultas como los ejemplos que se exhiben abajo para recibir correctamente los eventos.

```
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"
```

Para obtener información detallada sobre estos eventos, consulte la documentación de CIM en http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf.

SNMP

Subagente BASP

El subagente BASP, baspmgnt.dll, está diseñado para el servicio SNMP de Windows Server 2008. Es obligatorio instalar el servicio SNMP antes de instalar el subagente BASP.

El subagente BASP permite que un software administrador de SNMP monitoree de manera activa las configuraciones y el rendimiento de las características del Servidor avanzado de Broadcom. El subagente también provee una captura de alarma para que un administrador de SNMP informe al administrador sobre cualquier cambio en las condiciones del componente BASP.

El subagente BASP permite el monitoreo de las configuraciones y estadísticas para los equipos BASP, los adaptadores NIC físicos que participan en un equipo y los adaptadores NIC virtuales creados como resultado del equipo. En este momento no se monitorean los adaptadores NIC que no están en equipos. Los datos de configuración BASP incluyen información del tipo ID de equipos, ID de adaptador físico/virtual/VLAN/de equipo, descripciones de adaptador físico/virtual/VLAN/equipo y direcciones MAC de los adaptadores.

Las estadísticas incluyen información detallada del tipo paquetes de datos transmitidos y recibidos para los adaptadores físicos/virtuales/VLAN/de equipo.

La captura de alarmas envía información sobre los cambios de configuración de los adaptadores físicos que participan en un equipo, tal como eventos de enlace activo/inactivo del adaptador físico y adaptador instalado/extraído.

Para monitorear esta información, un administrador SNMP debe cargar los archivos de la base de datos MIB BASP de Broadcom para permitir el monitoreo de la información descrita más arriba. Los archivos que se indican a continuación están incluidos en los medios fuente del controlador:

baspcfg.mib

baspstat.mib

basptrap.mib

Agente extensible BASP

El agente extensible SNMP de información extendida del Controlador Broadcom NetXtreme Gigabit Ethernet (bcmif.dll) está diseñado para el servicio SNMP de Windows Server.

El agente extensible permite que el software del administrador SNMP monitoree de manera activa las configuraciones del adaptador Broadcom NetXtreme. Tiene como fin ser suplemento de la información ya provista por la información de la Interfaz de red de administración SNMP estándar.

El agente extensible provee información cabal sobre un adaptador Broadcom NetXtreme, tal como:

- Dirección MAC
- Dirección IP vinculada
- Máscara de subred IP
- Estado del enlace físico
- Estado del adaptador

- Velocidad de línea
- Modo dúplex
- Rango de memoria
- Configuración de interrupciones
- Núm. de bus
- Núm. de dispositivo
- Núm. de función

Para monitorear esta información, un administrador SNMP debe cargar el archivo MIB de información Extendida de Broadcom para permitir el monitoreo de la información descrita más arriba. Este archivo, bcmif.mib, se incluye con el CD de instalación del adaptador Broadcom NetXtreme.

La estación de trabajo monitoreada requiere la instalación del agente extensible SNMP de Información extendida de Broadcom, bcmif.dll, y requiere que esté instalado y cargado el servicio SNMP de Microsoft Windows Server 2008.

Sección 6: Instalación del hardware

Nota: Esta sección sólo se aplica a los modelos NIC integrados de los adaptadores Broadcom NetXtreme Gigabit Ethernet.

Precauciones de seguridad

¡Precaución! El adaptador se está instalando en un sistema que funciona con tensión que puede ser letal. Antes de extraer la tapa de su sistema, debe cumplir con las siguientes precauciones para protegerse contra lesiones y evitar daños a los componentes del sistema:

- Quítese los objetos metálicos o alhajas que pudiera tener en sus manos y muñecas.
- Asegúrese de usar sólo herramientas aisladas o no conductoras.
- Verifique que el sistema esté apagado y desenchufado antes de tocar los componentes internos.
- Instale o extraiga los adaptadores en un ambiente libre de estática. Se recomienda usar una pulsera de descarga a tierra u otro dispositivo personal antiestática y una almohadilla antiestática.

Lista de verificación previa a la instalación

1. Verifique que su servidor esté usando el último BIOS.
2. Si se inicia el sistema con un sistema operativo, apague con precaución SO.
3. Una vez completado el cierre del sistema, apáguelo y desenchufe el cable de alimentación.
4. Sosteniendo la tarjeta del adaptador por los bordes, extráigala del envoltorio y colóquela sobre una superficie antiestática.
5. Verifique que no haya signos de daños visibles en el adaptador, particularmente en el conector del borde de la tarjeta. Nunca intente instalar un adaptador dañado.

Instalación del adaptador

Las siguientes instrucciones se aplican a la instalación de un adaptador Broadcom NetXtreme Gigabit Ethernet (NIC integrado) en la mayoría de los servidores. Remítase a los manuales provistos con su servidor, para obtener información sobre la realización de estas tareas en su servidor.

1. Revise Precauciones de seguridad y Lista de verificación previa a la instalación. Antes de instalar el adaptador, asegúrese de que el sistema esté APAGADO y desenchufado del toma de alimentación y de que se han cumplido los procedimientos correctos de descarga a tierra.
2. Abra el gabinete del sistema y seleccione una ranura PCI Express vacía.
3. Retire la cubierta ciega de la ranura que ha seleccionado.
4. Alinee el borde del conector del adaptador con la ranura del conector en el sistema.
5. Aplicando presión pareja en ambos extremos de la tarjeta, empuje la tarjeta del adaptador hasta que quede correctamente asentada. Cuando el adaptador esté correctamente asentado, los conectores del puerto del adaptador se alinea con la apertura de la ranura y la placa se desliza contra el chasis del sistema.

¡Precaución! No ejerza demasiada fuerza para encajar la tarjeta, ya que se puede dañar el sistema o el adaptador. Si tiene dificultades al encajar el adaptador, extráigalo, vuelva a alinearlo e inténtelo nuevamente.

6. Asegure el adaptador con el gancho o el tornillo provisto.
7. Cierre el gabinete del sistema y desconecte cualquier dispositivo personal antiestática.

Conexión de los cables de red

Cobre

El controlador Broadcom NetXtreme Gigabit Ethernet tiene uno o más conectores RJ-45 que se utilizan para conectar el sistema a un segmento de cable de cobre Ethernet.

Nota: El adaptador Broadcom NetXtreme Gigabit Ethernet soporta el cruzamiento MDI automático (MDIX), que elimina la necesidad de cruzar cables cuando se conectan máquinas fondo contra fondo. Un cable de categoría 5 directo permite que las máquinas se comuniquen cuando se conectan juntas directamente.

1. Seleccione un cable apropiado. Tabla 14: “Especificaciones de cable 10/100/1000BASE-T” indica los requisitos de cables para conectar a puertos 10/100/1000BASE-T:

Tabla 14: Especificaciones de cable 10/100/1000BASE-T

Tipo de puerto	*Conector*	*Medios*	*Distancia máxima*
10BASE-T	RJ-45	Pares trenzados no recubiertos categoría 3, 4 ó 5 (UTP)	100 metros (328 pies)
100/1000BASE-T[1]	RJ-45	Categoría 5[2] UTP	100 metros (328 pies)

[1] La señalización 1000BASE-T requiere cuatro pares roscados de cableado balanceado Categoría 5, según lo especificado en ISO/IEC 11801:1995 y EIA/TIA-568-A (1995) y probado usando los procedimientos definidos en TIA/EIA TSB95.

[2]El requerimiento mínimo es categoría 5. Soporte completo para categoría 5e y categoría 6.

2. Conecte un extremo del cable al adaptador.
3. Conecte el otro extremo del cable a un puerto de red RJ-45 Ethernet.

Nota: Cuando el cable está correctamente conectado en ambos extremos, los LED del puerto del adaptador deben funcionar. Consulte Tabla 14: “Especificaciones de cable 10/100/1000BASE-T,” en la página 67 para obtener la descripción de las indicaciones de enlace de red y de actividad.

Sección 7: Creación de un disco de controladores

Consulte la documentación provista con su sistema para obtener las instrucciones para crear un disco de controladores.

Sección 8: Software del controlador Broadcom Boot Agent

Resumen

Los adaptadores Broadcom NetXtreme Gigabit Ethernet admiten Preboot Execution Environment (PXE), Remote Program Load (RPL), iSCSI boot y Bootstrap Protocol (BootP). Multi-Boot Agent (MBA) es un módulo de software que permite a su sistema conectado en red arrancarse con las copias de programa proporcionadas por los sistemas remotos a lo largo de la red. El controlador Broadcom MBA cumple con la especificación PXE 2.1 y se incluye con imágenes monolíticas y binarias divididas. Esto ofrece mayor flexibilidad a los usuarios en distintos entornos donde la placa base puede tener o no una codificación integrada.

El módulo MBA opera en un entorno cliente/sistema. Una red consta de uno o más sistemas de arranque que proporcionan copias de arranque a sistemas múltiples a lo largo de la red. La implementación por parte de Broadcom del módulo MBA ha cumplido con las pruebas satisfactoriamente en los siguientes entornos:

- **Servidor Linux® Red Hat® PXE.** Los clientes Broadcom PXE pueden arrancar y usar remotamente los recursos de red (montaje NFS y demás) y ejecutar instalaciones de Linux. En el caso de un arranque remoto, el controlador universal de Linux se une uniformemente con la Interfaz del Controlador de Red Universal de Broadcom (UNDI) y ofrece una interfaz de red en el entorno de cliente arrancado remotamente de Linux.
- **Intel® APITEST.** El controlador Broadcom PXE satisface todas las series de pruebas de cumplimiento de la norma API.
- **Windows Deployment Service (WDS, Servicio de implementación de Windows)**. En el caso de Windows Server, RIS fue reemplazado por WDS, que ofrece un cliente Broadcom PXE para instalar sistemas operativos Windows, incluido Windows Server 2008.

Configuración de MBA en un Entorno de cliente

Utilice el siguiente procedimiento para los NIC incorporados. Para los LOM, consulte la guía del sistema de su computadora.

La configuración del MBA en un entorno de cliente requiere los siguientes pasos:

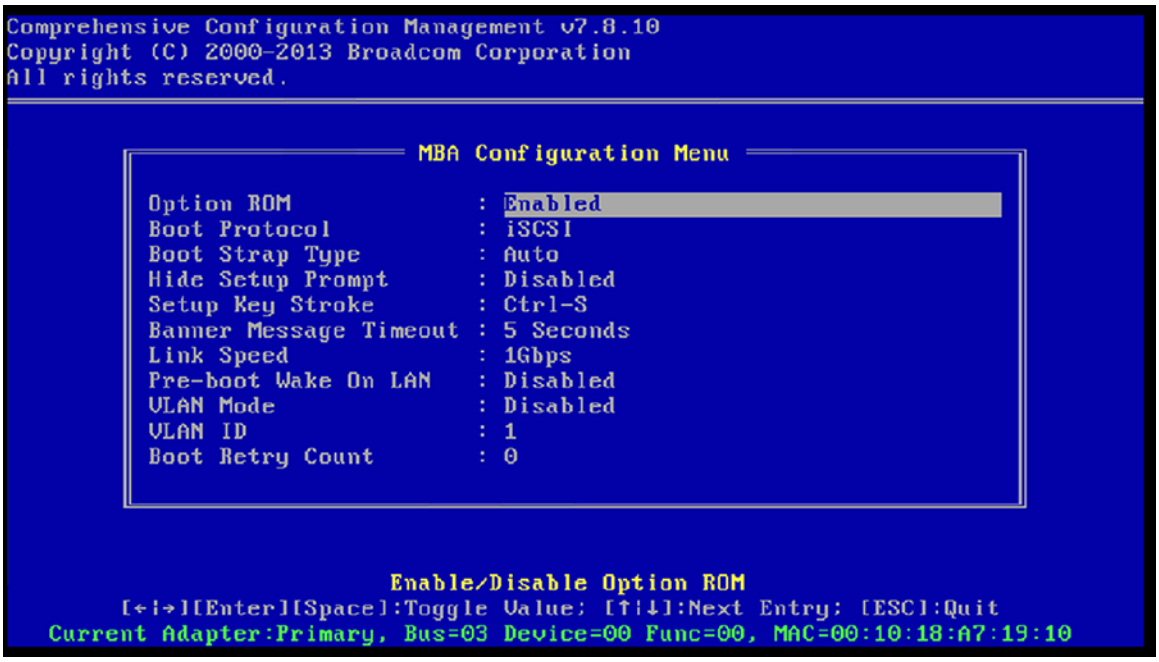
1. Configuración del controlador MBA.
2. Configuración del BIOS para el orden de arranque.

Configuración del controlador MBA

Esta sección trata sobre la configuración del controlador MBA en los modelos NIC integrados del adaptador de red Broadcom. Para configurar el controlador MBA en los modelos LOM del adaptador de red Broadcom, consulte la documentación de su sistema.

Uso de CCM

1. Reinicie el sistema.
2. Oprima **CTRL+S** dentro de los 4 segundos posteriores al momento en que se le indicó hacerlo. Aparece una lista de adaptadores.
   a. Seleccione el adaptador para configurar y presione **Enter**. Aparece Main Menu (Menú principal).
   b. Seleccione **MBA Configuration** (Configuración de MBA) parar ver el menú de configuración de MBA.



3. Utilice las teclas FLECHA ARRIBA y FLECHA ABAJO para desplazarse al elemento del menú Boot Protocol. Luego utilice las teclas FLECHA DER. y FLECHA IZQ. para seleccionar el protocolo de arranque de su preferencia si se encuentran disponibles otros protocolos de inicio además del Preboot Execution Environment (Entorno pre-inicio) (PXE). Si se encuentran disponible, otros protocolos incluyen Remote Program Load (Carga remota de programas)

(RPL) y el protocolo Bootstrap (BOOTP).

Nota: Para los LOM que se pueden iniciar con algunos, pero no todos los iSCI, el protocolo de inicio se configura mediante la BIOS. Consulte la documentación del sistema para obtener más información.

Nota: Si usted tiene múltiples adaptadores en su sistema y no está seguro de cuál es el adaptador que está configurando, oprima **CTRL+F6**, lo que causa que el LED del puerto del adaptador comience a parpadear.

4. Utilice las teclas FLECHA ARRIBA, FLECHA ABAJO, FLECHA IZQ. y FLECHA DER. para desplazarse y cambiar los valores de otros elementos del menú, si lo desea.
5. Oprima **F4** para guardar su configuración.
6. Oprima **ESC** cuando haya terminado.

Uso de uEFI

1. Reinicie el sistema.
2. Acceda al menú de configuración System Setup (Configuración del sistema) o Device Setting (Configuración del dispositivo).
3. Seleccione el dispositivo en el que desea cambiar la configuración MBA.
4. Seleccione **MBA Configuration Menu** (Menú de configuración de MBA).
5. Use el menú desplegable para seleccionar el protocolo de inicio de su elección, si existen protocolos de inicio disponibles que no sean Preboot Execution Environment (PXE) (Entorno de ejecución de arranque previo). Si está disponible, otros protocolos de inicio incluyen iSCSI y Bootstrap Protocol (BOOTP).

Nota: Para los LOM que se pueden iniciar con iSCSI, el protocolo de inicio se configura mediante la BIOS. Consulte la documentación del sistema para obtener más información.

6. Utilice las teclas FLECHA ARRIBA, FLECHA ABAJO, FLECHA IZQ. y FLECHA DER. para desplazarse y cambiar los valores de otros elementos del menú, si lo desea.
7. Seleccione **Back** (Atrás) para volver al menú principal
8. Seleccione **Finish** (Finalizar) para guardar y salir.

Configuración del BIOS

Para iniciar el sistema desde la red con el MBA, haga que el adaptador con el MBA habilitado sea el primer dispositivo iniciable en el BIOS. Este procedimiento depende de la implementación del BIOS del sistema. Consulte el manual del usuario del sistema para más instrucciones.

Sección 9: Protocolo iSCSI

Inicio iSCSI

Los adaptadores Broadcom NetXtreme Gigabit Ethernet admiten el inicio iSCSI, lo que permite el arranque de redes de sistemas operativos en sistemas sin disco. El inicio iSCSI le permite a un sistema operativo Windows o Linux iniciarse desde una máquina de destino iSCSI ubicada en un sitio remoto por una red de IP estándar.

Para los sistemas operativos Windows y Linux, se puede configurar el arranque iSCSI para que se inicie con los parámetros generales se muestra en la Tabla 15.

Sistemas operativos compatibles con inicio iSCSI

Los adaptadores Broadcom NetXtreme Gigabit Ethernet admiten el inicio iSCSI en los siguientes sistemas operativos:

- Sistema operativo Windows Server
- Distribución Linux Enterprise

Configuración de inicio iSCSI

El inicio iSCI no tiene soporte en el modo BIOS cuando existe almacenamiento local (especialmente en RAID) debido a limitaciones de memoria de EBDA.

La configuración de inicio iSCSI consiste en:

- Configuración del destino iSCSI
- Configuración de los parámetros de inicio iSCSI
- Preparación de la imagen de inicio iSCSI
- Inicio

Configuración del destino iSCSI

La configuración del destino iSCSI varía según los proveedores de destino. Para obtener más información sobre la configuración de destinos iSCSI, consulte la documentación suministrada por el proveedor. Los pasos generales incluyen:

1. Crear un destino iSCSI.
2. Crear un disco virtual.
3. Trazar el mapa desde el disco virtual al destino iSCSI creado en el paso 1.
4. Asociar el software de inicio iSCSI con el destino iSCSI.

5. Registre el nombre del destino iSCSI, el número del puerto TCP, el número de unidad lógica (LUN) de iSCSI, el nombre calificado de Internet (IQN) del iniciador y los detalles de autenticación de CHAP.
6. Después de configurar el destino iSCSI, deberá obtener lo siguiente:
   - IQN de destino
   - Dirección IP de destino
   - Número de puerto TCP de destino
   - LUN de destino
   - IQN de iniciador
   - ID y secreto de CHAP

Configuración de los parámetros de inicio iSCSI

Defina el software de inicio iSCSI de Broadcom para una configuración estática o dinámica. Consulte Tabla 15 para obtener las opciones de configuración disponibles a través de la pantalla General Parameters (Parámetros generales).

Tabla 15 enumera parámetros para IPv4 e IPv6. Se registran los parámetros específicos para IPv4 o IPv6.

Nota: La disponibilidad del inicio iSCSI IPv6 depende de la plataforma/dispositivo.

Tabla 15: Opciones de configuración

Opción	*Descripción*
TCP/IP parameters via DHCP	Esta opción es específica para IPv4. Controla si el software del host de inicio iSCSI adquiere la información sobre la dirección IP a través de DHCP (Habilitado) o si utiliza una configuración de IP estática (Deshabilitado).
IP Autoconfiguration	Esta opción es específica para IPv6. Controla si el software del host de inicio iSCSI configurará una dirección local de enlace sin estado y/o una dirección con estado si DHCPv6 está presente y se utiliza (Habilitado). Se envían paquetes de solicitudes de enrutador hasta tres veces con intervalos de 4 segundos entre cada reintento. O utilice una configuración de IP estática (Deshabilitado).
iSCSI parameters via DHCP	Controla si el software del host de inicio iSCSI adquiere los parámetros de destino iSCSI a través de DHCP (Habilitado) o mediante una configuración estática (Deshabilitado). La información estática se ingresa a través de la pantalla iSCSI Initiator Parameters Configuration (Configuración de parámetros de iniciador de iSCSI).
CHAP Authentication	Controla si el software del host de inicio iSCSI utiliza la autenticación de CHAP cuando se conecta al destino iSCSI. Si la Autenticación de CHAP está habilitada, la ID y el secreto de CHAP se ingresan en la pantalla iSCSI Initiator Parameters Configuration.
DHCP Vendor ID	Controla si el software del host de inicio iSCSI interpreta el campo Vendor Class ID (ID de clase del proveedor) utilizado durante el DHCP. Si el campo Vendor Class ID que aparece en el paquete de oferta del DHCP coincide con el valor indicado en el campo, el software del host de inicio iSCSI busca en el campo Option 43 (Opción 43) de DHCP las extensiones de inicio iSCSI requeridas. Si DHCP está deshabilitado, no es necesario definir este valor.
Link Up Delay Time	Controla cuántos segundos espera el software del host de inicio iSCSI una vez establecido el enlace Ethernet antes de enviar los datos a través de la red. Los valores permitidos son de 0 a 255. A modo de ejemplo, es posible que un usuario deba establecer un valor para esta opción si un protocolo de red como un árbol de expansión, por ejemplo, está habilitado en la interfaz del conmutador al sistema del cliente.

Tabla 15: Opciones de configuración (Cont.)

Opción	*Descripción*
Use TCP Timestamp	Controla si la opción TCP Timestamp está habilitada o deshabilitada.
Target as First HDD	Permite especificar si la unidad de destino iSCSI aparecerá como el primer disco duro del sistema.
LUN Busy Retry Count	Controla la cantidad de veces que el iniciador de iSCSI intentará lograr la conexión si el LUN de destino iSCSI está ocupado.
IP Version	Esta opción es específica para IPv6. Alterna entre el protocolo IPv4 o el IPv6. Todos los valores IP se perderán cuando pase de una versión de protocolo a la otra.

Configuración del protocolo de inicio MBA

Para configurar el protocolo de inicio

1. Reinicie el sistema.
2. Desde el identificador de PXE, seleccione **CTRL+S**. Aparecerá el MBA Configuration Menu (Menú de configuración de MBA) (consulte Broadcom Boot Agent).
3. Desde MBA Configuration Menu, use la **FLECHA ARRIBA** o la **FLECHA ABAJO** para ir a la opción **Boot Protocol** (Protocolo de arranque). Use la **FLECHA IZQUIERDA** o la **FLECHA DERECHA** para cambiar la opción **Boot Protocol** a **iSCSI**.

Nota: Para las plataformas en las que se establece el protocolo de arranque a través de la BIOS, consulte la documentación del sistema para obtener más información.

4. Seleccione **iSCSI Boot Configuration (Configuración de inicio iSCSI)** desde **Main Menu (Menú Principal)**.

Nota: Si el firmware de inicio iSCSI no está programado en el adaptador de red NetXtreme, seleccionar **iSCSI Boot Configuration (Configuración de inicio iSCSI)** no arrojará ningún resultado.

Configuración de inicio iSCSI

- Configuración estática de inicio iSCSI
- Configuración dinámica de inicio iSCSI

Configuración estática de inicio iSCSI

En una configuración estática, debe ingresar los datos correspondientes a la dirección IP del sistema, el IQN del iniciador del sistema y los parámetros de destino obtenidos en Configuración del destino iSCSI. Para obtener más información sobre las opciones de configuración, consulte Tabla 15.

Para configurar los parámetros de inicio iSCSI mediante la configuración estática:

1. En la pantalla **General Parameters Menu?(Menú de parámetros generales)**, defina lo siguiente:
   - **TCP/IP parameters via DHCP**: Deshabilitado. (Para IPv4.)
   - **IP Autoconfiguration**: Deshabilitado. (Para IPv6)
   - **iSCSI parameters via DHCP**: Deshabilitado
   - **CHAP Authentication**: Deshabilitado
   - **Boot to iSCSI target**: Deshabilitado
   - **DHCP Vendor ID**: BRCM ISAN
   - **Link Up Delay Time**: 0

- **Use TCP Timestamp**: Habilitado (para algunos destinos como Dell/EMC AX100i, es necesario habilitar **Use TCP Timestamp**)
- **Target as First HDD**: Deshabilitado
- **LUN Busy Retry Count**: 0
- **Versión IP**: IPv6. (Para IPv6)

2. Seleccione **ESC** para regresar al menú **Main**.
3. Desde el menú **Main**, seleccione **Initiator Parameters** (Parámetros de iniciador).
4. Desde la pantalla **Initiator Parameters**, indique valores para los siguientes campos:
   - IP Address (Dirección IP) (las direcciones IPv4 e IPv6 sin especificar deben ser “0.0.0.0” y “::”, respectivamente**)**
   - Subnet Mask Prefix (Prefijo de máscara de subred)
   - Default Gateway (Puerta predeterminada)
   - Primary DNS (DNS primario)
   - Secondary DNS (DNS secundario)
   - iSCSI Name (Nombre de iSCSI) (concuerda con el nombre del iniciador de iSCSI que usará el sistema del cliente)

Nota: Ingrese con cuidado la dirección IP. No se realiza ninguna verificación de errores contra la dirección IP para comprobar la existencia de duplicados o de asignación de segmento/red incorrectos.

5. Seleccione **ESC** para regresar al menú **Main**.
6. Desde el menú **Main**, seleccione **1st Target Parameters** (Parámetros de destino primario).
7. Desde la pantalla **1st Target Parameters**, habilite la opción **Connect** (Conectar) para conectarse al destino iSCSI. Ingrese valores para los siguientes campos según los valores usados para configurar el destino iSCSI:
   - IP Address (Dirección IP)
   - TCP Port (Puerto TCP)
   - Boot LUN (LUN de inicio)
   - iSCSI Name (Nombre de iSCSI)
8. Seleccione **ESC** para regresar al menú **Main**.
9. Seleccione **ESC** y luego **Exit and Save Configuration** (Salir y guardar configuración).
10. Seleccione **F4** para guardar la configuración MBA.

Configuración dinámica de inicio iSCSI

En una configuración dinámica, sólo debe especificar que la información sobre la dirección IP y el iniciador/destino es suministrada por un servidor DHCP (consulte las configuraciones de IPv4 y IPv6 en Configuración del servidor DHCP para que admita el inicio iSCSI). Para IPv4, a excepción del nombre del iniciador de iSCSI, toda configuración que aparezca en las pantallas Initiator Parameters, 1st Target Parameters o 2nd Target Parameters será ignorada y no será necesario borrarla. Para IPv6, a excepción de la ID y secreto de CHAP, toda configuración que aparezca en las pantallas Initiator Parameters, 1st Target Parameters o 2nd Target Parameters será ignorada y no será necesario borrarla. Para obtener más información sobre las opciones de configuración, consulte Tabla 15.

NOTAS:

- Al utilizar un servidor DHCP, los valores suministrados por este servidor sobrescriben las entradas del servidor DNS. Esto sucede incluso cuando los valores suministrados localmente son válidos y el servidor DHCP no brinda información sobre el servidor DNS. Cuando el servidor DHCP no brinda información sobre el servidor DNS, tanto los valores primarios como los secundarios del servidor DNS están configurados en 0.0.0.0. Cuando se activa el sistema operativo Windows, el software de inicio iSCSI de Microsoft recupera los parámetros y configura los registros apropiados estáticamente. Sobrescribirá todo lo que esté configurado. Como el daemon de DHCP se ejecuta en el entorno de Windows como un proceso del usuario, todos los parámetros TCP/IP deben estar configurados estáticamente antes de que se active la pila en el entorno de inicio iSCSI.
- Si se utiliza la Opción 17 de DHCP, la información sobre el destino es suministrada por el servidor DHCP y el nombre del iniciador de iSCSI se recupera del valor programado en la pantalla Initiator Parameters. Si no se seleccionó ningún valor, el controlador empleará el nombre predeterminado:

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

en el que la cadena `11.22.33.44.55.66` corresponde a la dirección MAC del controlador.

Si se utiliza la opción 43 del DHCP (IPv4 solamente), toda configuración que aparezca en las pantallas Initiator Parameters, 1st Target Parameters o 2nd Target Parameters será ignorada y no será necesario borrarla.

Para configurar los parámetros de inicio iSCSI mediante la configuración dinámica:

1. En la pantalla **General Parameters Menu?(Menú de parámetros generales)**, defina lo siguiente:
   - **TCP/IP parameters via DHCP**: Habilitado. (Para IPv4.)
   - **IP Autoconfiguration**: Habilitado. (Para IPv6)
   - **iSCSI parameters via DHCP**: Habilitado
   - **CHAP Authentication**: Deshabilitado
   - **Boot to iSCSI target**: Deshabilitado
   - **DHCP Vendor ID**: BRCM ISAN
   - **Link Up Delay Time**: 0
   - **Use TCP Timestamp**: Habilitado (para algunos destinos como Dell/EMC AX100i, es necesario habilitar **Use TCP Timestamp)**
   - **Target as First HDD**: Deshabilitado
   - **LUN Busy Retry Count**: 0
   - **Versión IP**: IPv6. (Para IPv6)
2. Seleccione **ESC** para regresar al menú **Main**.

Nota: La información que aparece en las pantallas **Initiator Parameters** (Parámetros de iniciador) y **1st Target Parameters** (Parámetros de destino primario) será ignorada y no será necesario borrarla.

3. Seleccione **Exit and Save Configurations** (Salir y guardar configuración).

Habilitar la autenticación de CHAP

Asegúrese de que la autenticación de CHAP está habilitada en el destino.

Para habilitar la opción CHAP authentication:

1. Desde la pantalla **General Parameters**, configure la opción **CHAP Authentication** como Enabled (Habilitada).
2. Desde la pantalla **Initiator Parameters**, indique valores para los siguientes campos:
   - CHAP ID (ID de CHAP) (hasta 128 bytes)
   - CHAP Secret (Secreto de CHAP) (si se requiere la autenticación y debe tener una longitud de 12 caracteres o más)
3. Seleccione **ESC** para regresar al menú **Main**.
4. Desde el menú **Main**, seleccione **1st Target Parameters** (Parámetros de destino primario).
5. Desde la pantalla **1st Target Parameters**, ingrese los valores para los siguientes campos según los valores usados al configurar el destino iSCSI:
   - CHAP ID (ID de CHAP) (opcional si el CHAP es de dos vías)
   - CHAP Secret (Secreto de CHAP) (opcional si el CHAP es de dos vías y debe tener una longitud de 12 caracteres o más)
6. Seleccione **ESC** para regresar al menú **Main**.
7. Seleccione **ESC** y luego **Exit and Save Configuration** (Salir y guardar configuración).

Configuración del servidor DHCP para que admita el inicio iSCSI

El servidor DHCP es un componente opcional y sólo es necesario si va a realizar una configuración dinámica de inicio iSCSI (consulte Configuración dinámica de inicio iSCSI).

La configuración del servidor DHCP para que admita el inicio iSCSI es distinta para IPv4 y IPv6.

- Configuraciones de inicio iSCSI en DHCP para IPv4
- Configuración de inicio de iSCSI en DHCP para IPv6

Configuraciones de inicio iSCSI en DHCP para IPv4

El protocolo DHCP incluye una variedad de opciones que ofrecen al cliente de DHCP información relacionada con la configuración. En el caso del inicio iSCSI, los adaptadores de Broadcom admiten las siguientes configuraciones de DHCP:

- DHCP Option 17, (Opción 17 de DHCP), Ruta de raíz
- DHCP Option 43, (Opción 43 de DHCP), Información específica del proveedor

DHCP Option 17, (Opción 17 de DHCP), Ruta de raíz

La Opción 17 se usa para pasar la información sobre el destino iSCSI al cliente de iSCSI.

El formato de la ruta de raíz según se define en IETC RFC 4173 es:

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

Los parámetros se definen a continuación.

Tabla 16: Definición de parámetros de la Opción 17 de DHCP

Parámetro	*Definición*
"iscsi:"	Una cadena literal
<servername>	La dirección IP o FQDN del destino iSCSI
":"	Separador
<protocol>	El protocolo IP usado para acceder al destino iSCSI. En la actualidad, sólo TCP es compatible, de manera que el protocolo es 6.
<port>	El número de puerto asociado con el protocolo. El número de puerto estándar para iSCSI es 3260.
<LUN>	El número de unidad lógica que se usará en el destino iSCSI. El valor del LUN debe estar representado en formato hexadecimal. Un LUN con ID de 64 debe configurarse como 40 dentro del parámetro de la opción 17 del servidor DHCP.
<targetname>	El nombre del destino en formato IQN o EUI (consulte RFC 3720 para obtener detalles sobre ambos formatos). Un ejemplo de un nombre IQN sería: “iqn.1995-05.com.broadcom:iscsi-target”.

DHCP Option 43, (Opción 43 de DHCP), Información específica del proveedor

La Opción 43 de DHCP (información específica del proveedor) ofrece más opciones de configuración al cliente iSCSI que la Opción 17 de DHCP. En esta configuración, se suministran tres subopciones más que asignan el IQN del iniciador al cliente de inicio iSCSI y dos IQN de destino iSCSI que pueden usarse para iniciar el sistema. El formato del IQN del destino iSCSI es el mismo que el de la Opción 17 de DHCP, mientras que el IQN del iniciador iSCSI es simplemente el IQN del iniciador.

Nota: La Opción 43 de DHCP es compatible con IPv4 solamente.

A continuación se detallan las subopciones:

Tabla 17: Definición de subopciones de la Opción 43 de DHCP

Subopción	*Definición*
201	Información sobre el destino iSCSI primario en el formato estándar de ruta de raíz "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
202	Información sobre el destino iSCSI secundario en el formato estándar de ruta de raíz "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
203	IQN del iniciador iSCSI

El uso de la Opción 43 de DHCP requiere mayor configuración que la Opción 17, pero ofrece un entorno más rico y más opciones de configuración. Broadcom recomienda a los clientes el uso de la Opción 43 de DHCP para llevar a cabo la configuración dinámica de inicio iSCSI.

Configuración del servidor DHCP

Configure el servidor DHCP de manera que admita las Opciones 17 o 43.

Nota: Si va a utilizar la Opción 43, también deberá configurar la Opción 60. El valor de la Opción 60 debe coincidir con el valor del campo **DHCP Vendor ID** (ID de proveedor de DHCP). El valor de **DHCP Vendor ID** (ID de proveedor de DHCP) es BRCM ISAN, según se indica en **General Parameters** (Parámetros generales) del menú iSCSI Boot Configuration (Configuración de inicio iSCSI).

Configuración de inicio de iSCSI en DHCP para IPv6

El servidor DHCPv6 puede ofrecer una cantidad de opciones, incluyendo configuración de IP con o sin estado, así como información al cliente de DHCPv6. En el caso del inicio iSCSI, los adaptadores de Broadcom admiten las siguientes configuraciones de DHCP:

- DHCPv6 Opción 16, opción de clase de proveedor
- Opción 17 de DHCPv6, información específica del proveedor

Nota: La opción DHCPv6 standard Root Path (ruta de raíz estándar de DHCPv6) aún no está disponible. Broadcom sugiere que se utilice la Opción 16 o la Opción 17 para admitir el inicio iSCSI IPv6.

DHCPv6 Opción 16, opción de clase de proveedor

La Opción 16 de DHCPv6 (opción de clase de proveedor) debe estar presente y debe contener una cadena que coincida con su parámetro **DHCP Vendor ID** (ID de proveedor de DHCP) configurado. El valor de **DHCP Vendor ID** (ID de proveedor de DHCP) es BRCM ISAN, según se indica en **General Parameters** (Parámetros generales) del menú iSCSI Boot Configuration (Configuración de inicio iSCSI).

El contenido de la Opción 16 debe ser <2-byte length> <DHCP Vendor ID>.

Opción 17 de DHCPv6, información específica del proveedor

La Opción 17 de DHCPv6 (información específica del proveedor) ofrece más opciones de configuración al cliente de iSCSI. En esta configuración, se suministran tres subopciones más que asignan el IQN del iniciador al cliente de inicio iSCSI y dos IQN de destino iSCSI que pueden usarse para iniciar el sistema.

A continuación se detallan las subopciones:

Tabla 18: Definición de subopciones de la Opción 17 de DHCP

Subopción	*Definición*
201	Información sobre el destino iSCSI primario en el formato estándar de ruta de raíz `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Información sobre el destino iSCSI secundario en el formato estándar de ruta de raíz `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	IQN del iniciador iSCSI

Nota: En Tabla 18, se requieren corchetes [ ] para las direcciones IPv6.

El contenido de la opción 17 debe ser <2-byte Option Number 201|202|203> <2-byte length> <data>.

Configuración del servidor DHCP

Configure el servidor DHCP para que admita la Opción 16 y la Opción 17.

Nota: El formato de la Opción 16 y la Opción 17 de DHCPv6 están completamente definidos en RFC 3315.

Preparación de la imagen de inicio iSCSI

Configuración de inicio de Windows Server 2008 R2 y SP2 iSCSI

Windows Server 2008 R2 y Windows Server 2008 SP2 admiten inicio de iSCSI. El siguiente procedimiento hace referencia a Windows Server 2008 R2, pero el procedimiento es común para Windows Server 2008 R2 y SP2.

Imagen CD/ISO requerida:

- Windows Server 2008 R2 x64 con controladores Broadcom inyectados. Consulte el tema de la base de artículos informativos Microsoft KB974072 en support.microsoft.com.

Nota: Consulte la aplicación de instalación del controlador específico en el archivo *silent.txt* para obtener instrucciones sobre cómo extraer los controladores individuales de Windows NetXtreme.

Otro software requerido:

- Bindview.exe (Solo Windows Server 2008 R2; consulte KB976042)

Procedimiento:

1. Retire los discos duros locales en el sistema que se iniciará (el “sistema remoto”).
2. Cargue las imágenes de inicio MBA e iSCSI de Broadcom más recientes en NVRAM del adaptador.
3. Configure el BIOS en el sistema remoto para que Broadcom MBA sea el primer dispositivo iniciable y el DVDROM como el segundo dispositivo.
4. Configure el destino iSCSI para permitir una conexión desde el dispositivo remoto. Asegúrese de que el destino tenga suficiente espacio en el disco para contener la instalación del nuevo SO.
5. Inicie el sistema remoto. Cuando aparezca el identificador del Entorno de ejecución de arranque previo (PXE), presione **Ctrl+S** para ingresar al menú PXE.
6. En el menú PXE, configure **Boot Protocol** en **iSCSI**.
7. Ingrese los parámetros de destino iSCSI.
8. En General Parameters (Parámetros generales), configure el parámetro **Boot to Target** en **One-Time Disabled.**
9. Guarde la configuración y reinicie el sistema.

   El sistema remoto debe conectarse al destino iSCSI y luego iniciarse desde el dispositivo DVDROM.
10. Inicie el DVD?y comience la instalación.
11. Responda todas las preguntas de instalación como corresponde (especifique el sistema operativo que desea instalar, acepte los términos de licencia, etc.).

    Cuando aparezca la ventana **¿Dónde quiere instalar Windows?**, la unidad de destino debe estar visible. Esta es una unidad conectada a través del protocolo de inicio iSCSI, ubicado en el objetivo iSCSI remoto.
12. Seleccione **Siguiente** para continuar con la instalación de Windows Server 2008 R2.

    Unos minutos después de iniciar el proceso de instalación de Windows Server 2008 R2 DVD, se producirá un reinicio del sistema. Después del reinicio, la rutina de instalación de Windows Server 2008 R2 debe reanudarse y completarse.
13. Después de otro reinicio del sistema, revise y verifique que el sistema remoto pueda iniciarse en el escritorio.

14. Después de que se inicie Windows Server 2008 R2, cargue todos los controladores y ejecute el archivo Bindview.exe.
    a. Seleccione: **All Services** (Todos los servicios).
    b. En **WFP Lightweight Filter** debe ver **Binding paths** para AUT. Haga clic con el botón derecho y deshabilítelas. Cuando termine, cierre la aplicación.
15. Verifique que el sistema operativo funcione y pueda transferir tráfico realizando un ping del IP del sistema remoto, etc.

Configuración de inicio iSCSI de Windows Server 2012

Windows Server 2012 es compatible con el inicio y la instalación de iSCSI. Broadcom requiere el uso de un DVD “integrado” DVD con los más recientes controladores Broadcom inyectados. Consulte el tema de la base de artículos informativos Microsoft KB974072 en support.microsoft.com.

Nota: El procedimiento de Microsoft inyecta solo los controladores NDIS. Broadcom recomienda que se inyecten todos los controladores (VBD, BXND, OIS y NetXtreme I NDIS).

El siguiente procedimiento prepara la imagen para la instalación e inicio:

1. Retire los discos duros locales en el sistema que se iniciará (el “sistema remoto”).
2. Cargue las imágenes de inicio MBA e iSCSI de Broadcom más recientes en NVRAM del adaptador.
3. Configure el BIOS en el sistema remoto para que Broadcom MBA sea el primer dispositivo iniciable y el DVDROM como el segundo dispositivo.
4. Configure el destino iSCSI para permitir una conexión desde el dispositivo remoto. Asegúrese de que el destino tenga suficiente espacio en el disco para contener la instalación del nuevo SO.
5. Inicie el sistema remoto. Cuando aparezca el identificador del Entorno de ejecución de arranque previo (PXE), presione **Ctrl+S** para ingresar al menú PXE.
6. En el menú PXE, configure **Boot Protocol** en **iSCSI**.
7. Ingrese los parámetros de destino iSCSI.
8. En General Parameters (Parámetros generales), configure el parámetro **Boot to Target** en **One-Time Disabled.**
9. Guarde la configuración y reinicie el sistema.

   El sistema remoto debe conectarse al destino iSCSI y luego iniciarse desde el dispositivo DVDROM.
10. Inicie el DVD?y comience la instalación.
11. Responda todas las preguntas de instalación como corresponde (especifique el sistema operativo que desea instalar, acepte los términos de licencia, etc.).

    Cuando aparezca la ventana **¿Dónde quiere instalar Windows?**, la unidad de destino debe estar visible. Esta es una unidad conectada a través del protocolo de inicio iSCSI, ubicado en el objetivo iSCSI remoto.
12. Seleccione **Next** (Siguiente) para continuar con la instalación de Windows 2012.

    Unos minutos después de que comienza el proceso de instalación de Windows 20012 DVD, se producirá un reinicio del sistema. Después del reinicio, la rutina de instalación de Windows 2012 debe reanudarse y completarse.
13. Después de otro reinicio del sistema, revise y verifique que el sistema remoto pueda iniciarse en el escritorio.
14. Después de que Windows 2012 inicia el SO, Broadcom recomienda ejecutara el instalador de controlador para completar la instalación del controlador Broadcom y la aplicación.

Configuración de inicio iSCSI de Linux

El inicio Linux iSCSI es compatible con Red Hat Enterprise Linux 5.5 y versiones posteriores y con SUSE Linux Enterprise Server 11 SP1 y posteriores. Considere que SLES 10.x y SLES 11 solo soncompatibles para la ruta no de descarga.

1. Para obtener una actualización del controlador, obtenga el último CD de controlador de Linux de Broadcom.
2. Configure los parámetros de inicio iSCSI para la instalación directa de DVD a destino al deshabilitar el Inicio desde la opción destino en el adaptador de red.
3. Cambie la orden de inicio de la siguiente manera:
   a. Inicie desde el adaptador de red.
   b. Inicie desde la unidad de CD/DVD.
4. Reinicie el sistema.
5. El sistema se conectará al destino iSCSI, luego se iniciará desde la unidad de CD/DVD.
6. Sigas las instrucciones del sistema operativo correspondientes.
   a. RHEL 5.5: escriba “linux dd” en el indicador “boot:” y presione Intro
   b. SuSE 11.X: seleccione **instalación** y escriba **withiscsi=1 netsetup=1** en la opción inicio. Si desea actualizar el controlador, seleccione **SÍ** para la opción de controlador F6.
7. Si desea actualizar el controlador, siga las instrucciones para cargar el CD de controlador; de lo contrario, omita este paso.
8. En el indicador "networking device", seleccione el puerto del adaptador de red deseado y presione **Aceptar**.
9. En el indicador "configure TCP/IP", configure la forma en que el sistema adquiere la dirección IP y presione **Aceptar**.
10. Si se seleccionó una IP estática, debe ingresar información IP para el iniciador iscsi.
11. (RHEL) Seleccione "saltar" la prueba de medios.
12. Continúe la instalación según lo deseado. Habrá un disco disponible en este punto. Una vez finalizada la copia de los archivos, retire el CD/DVD y reinicie el sistema.
13. Cuando se reinicia el sistema, habilite "iniciar desde destino" en los parámetros de inicio iSCSI y continúe con la instalación hasta finalizar.

En este punto, la fase inicial de instalación está completa. El resto del procedimiento corresponde a la creación de un nuevo initrd personalizado para cualquier actualización reciente de componentes:

14. Actualice el iniciador iscsi, si lo desea. Primero necesitará eliminar el iniciador existente utilizando **rpm -e**.
15. Asegúrese de que todos los niveles de ejecución del servicio de red estén activados:
    `chkconfig network on`
16. Asegúrese de que los niveles de ejecución 2, 3 y 5 del servicio iscsi estén activados.
    `chkconfig -level 235 iscsi on`
17. Para Red Hat 6.0, asegúrese de que el Administrador de red esté detenido y deshabilitado.
18. Instale iscsiuio, si lo desea (no es obligatorio para SuSE 10).
19. Instale el paquete linux-nx2, si lo desea.
20. Instale el paquete bibt.
21. Elimine ifcfg-eth*.
22. Reinicie.
23. Para SUSE 11.1, siga la solución alternativa para la instalación remota del DVD que se muestra a continuación.
24. Después del reinicio del sistema, inicie sesión, cambie a la carpeta /opt/bcm/bibt y ejecute el script iscsi_setup.sh para crear la imagen initrd.

25. Copie la imágen initrd a la carpeta /boot.
26. Cambie el menú grub para señalar las nuevas imágenes initrd.
27. Para habilitar CHAP, necesitará modificar iscsid.conf (solo para Red Hat).
28. Reinicie y cambie los parámetros CHAP si lo desea.
29. Continúe iniciando en la imagen de inicio iSCSI y seleccione la imagen que creó.
30. Para IPv6, ahora puede cambiar la dirección IP para el iniciador y el destino a la dirección IPv6 deseada en la configuración NVRAM.

Inicio

Una vez que el sistema esté preparado para un inicio iSCSI y el sistema operativo esté presente en el destino iSCSI, el último paso es reiniciar el sistema. El sistema se iniciará en Windows o Linux a través de la red y funcionará como si fuese un disco duro local.

1. Reinicie el servidor.
2. Seleccione **CTRL+S**.
3. Desde el menú **Main**, seleccione **General Parameters** y configure la opción **Boot to iSCSI target** como **Enabled** (Habilitado).

De ser necesario, habilite la opción CHAP authentication tras determinar que el sistema se haya reiniciado correctamente (consulte Habilitar la autenticación de CHAP).

Otras consideraciones sobre el inicio iSCSI

Hay varios otros factores que deben considerarse al configurar un sistema de inicio iSCSI.

Modificación de la configuración de velocidad y dúplex en entornos de Windows.

Se soporta el inicio mediante la ruta de NDIS. La configuración de velocidad y dúplex puede modificarse con la utilidad de administración BACS para el inicio de iSCSI mediante la ruta de NDIS.

Locally Administered Address (Dirección administrada localmente)

Los dispositivos con inicio iSCSI no admiten una dirección MAC definida por el usuario asignada a través de la propiedad Locally Administered Address (Dirección administrada localmente) de la sección Advanced (Avanzado) de la ficha BACS Configurations (Configuraciones de BACS).

Redes LAN virtuales

El inicio iSCSI no admite el etiquetado LAN virtual (VLAN) con el software de inicio iSCSI de Microsoft.

Detección y solución de problemas del inicio iSCSI

Los siguientes consejos para la detección y solución de problemas le serán de utilidad para el inicio iSCSI.

Problema: Un destino iSCSI no se reconoce como destino de instalación al intentar instalar Windows Server 2008 con una conexión IPv6.
Solución: Este es un conocido problema de terceros. Consulte la base de artículos informativos de Microsoft KB 971443, http://support.microsoft.com/kb/971443.

Problema: No se puede ejecutar la utilidad de configuración iSCSI.
Solución: Asegúrese de que el firmware de inicio iSCSI esté instalado en NVRAM.

Problema: Después de configurar el LUN de inicio iSCSI en 255, aparece una pantalla azul del sistema cuando se ejecuta el inicio iSCSI.
Solución: Aunque la solución iSCSI de Broadcom admite un rango de LUN de 0 a 255, el software de inicio iSCSI de Microsoft no admite una LUN de 255. Configure un valor de LUN de 0 a 254.

Problema: No se puede actualizar el controlador de bandeja de entrada si hay una ID de hardware que no es de bandeja de entrada.
Solución: Cree una imagen de DVD de integración de la solución personalizada con controladores compatibles presentes en los medios de instalación.

Vuelco para caída del sistema iSCSI

Si va a usar la utilidad de vuelco para caída del sistema iSCSI de Broadcom, es importante que siga el procedimiento de instalación para instalar el controlador de vuelco para caída del sistema iSCSI. Consulte Uso del instalador para obtener más información.

Sección 10: Instalación del controlador y aplicación de administración de Linux

Paquetes

El controlador de Linux TG3 se distribuye en los siguientes formatos de paquetes (nombres de archivo):

- RPM fuente (tg3-*version*.3dkms.src.rpm)
- RPM fuente (tg3-*version*.3dkms.noarch.rpm)
- Supplemental (tg3_sup-*version*.tar.gz)
- Archivo tar comprimido (tg3-*version*.tar.gz)

Se incluyen archivos fuente idénticos para la creación del controlador en los paquetes fuente RPM y TAR. El archivo tar contiene utilidades adicionales tales como parches e imágenes de disco de controladores para la instalación de red.

Instalación del software del controlador TG3

Instalación de un paquete RPM fuente

Prerrequisitos

- Fuente kernel de Linux
- Compilador C

Procedimiento:

1. Instale el paquete RPM fuente.
   `rpm -ivh tg3-version.src.rpm`
2. Cambie el directorio a la ruta de acceso del RPM y cree el controlador binario para su kernel (la ruta de acceso del RPM es distinta para cada una de las distribuciones de Linux).
   `cd /usr/src/redhat,OpenLinux,turbo,packages,rpm …`
   `rpm -bb SPECS/tg3.spec or rpmbuild -bb SPECS/tg3.spec`
   `rpmbuild -bb SPECS/tg3.spec (for RPM version 4.x.x)`

   Nota: Mientras intenta instalar un paquete RPM fuente, puede aparecer el siguiente mensaje:

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

   La causa más probable del error es que el paquete rpm-build no haya sido instalado. Ubique el paquete rpm-build en el medio de instalación de Linux e instálelo usando el siguiente comando:

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

   Complete la instalación del RPM fuente.
3. Instale el nuevo paquete creado (controlador y página de manual).
   `rpm -ivh RPMS/i386/tg3-version.i386.rpm`

   Según el kernel, el controlador se instala en una de las siguientes rutas de acceso:

   Kernels 2.6.x:

   /lib/modules/*kernel_version*/kernel/drivers/net/tg3.ko
4. Cargue el controlador.
   `modprobe tg3`

Para configurar el protocolo y la dirección de red, consulte la documentación de Linux correspondiente a la versión específica.

Creación del controlador desde el archivo TAR

1. Cree un directorio (tg3-*version*) y extraiga los archivos TAR en ese directorio.
   `tar xvzf tg3-version.tgz`
2. Cree el controlador tg3.o como un módulo cargable para el kernel en uso.
   ```
   CD tg3-version
   make clean
   make; make install
   ```
3. Cargue el controlador para probarlo.
   ```
   rmmod tg3
   modprobe tg3
   ```
   No debe aparecer ningún mensaje si el comando se ejecuta correctamente.

Nota: Remítase a las instrucciones de RPM anteriores para conocer la ubicación del controlador instalado.

4. Para configurar el protocolo y dirección de red, consulte la documentación provista con su sistema operativo.

Instalaciones de red

Para las instalaciones de red a través de NFS, FTP o HTTP (mediante un disco de arranque de red o PXE), utilice el controlador tg3 que es parte de la distribución del sistema operativo Linux.

Descarga/eliminación del controlador TG3

Descarga/eliminación del controlador de una instalación RPM

Para descargar el controlador, use **ifconfig** para desactivar todas las interfaces *ethX* abiertas por el controlador y luego escriba lo siguiente:

```
rmmod tg3
```

Si el controlador se instaló mediante **rpm**, haga lo siguiente para extraerlo:

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

Eliminación del controlador de una instalación TAR

Si el controlador se instaló mediante el comando make install desde el archivo tar, el archivo del controlador tg3.o debe borrarse manualmente del sistema operativo. Remítase a Instalación de un paquete RPM fuente para conocer la ubicación del controlador instalado.

Si existe una configuración de interfaz relacionada con el controlador tg3, desactive la interfaz primero usando **ifconfig ethx down** y luego **rmmod tg3**.

Mensajes del controlador

A continuación se enumeran los mensajes más comunes que se registran en el archivo */var/log/messages*. Utilice **dmesg -n** *level* para controlar el nivel en el que los mensajes aparecen en la consola. La mayoría de los sistemas están configurados de forma predeterminada en el nivel 6.

Entrada del controlador

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

NIC detectado

```
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
```

Control de flujo

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

Indicación de enlace activado y velocidad

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

Indicación de enlace desactivado

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

Equipos con entrelazado de canales

Con el controlador TG3, puede configurar equipos de adaptadores usando el módulo de kernel de entrelazado y una interfaz de entrelazado de canales. Consulte la documentación de Linux para obtener más información sobre Entrelazado de canales de Linux.

Instalación de la aplicación de administración de Linux

Resumen

La versión 4 de Broadcom Advanced Control Suite (BACS4) es una aplicación de administración para configurar las familias de adaptadores NetXtreme I. El software de BACS4 opera en los sistemas operativos de servidor y cliente de Windows y Linux.

Este capítulo describe cómo instalar la aplicación de administración BACS4 en los sistemas Linux. Para los sistemas de Windows, se proporciona un programa de instalación que instala tanto los controladores de Windows como las aplicaciones de administración, incluido BACS4 (consulte Instalación del controlador y aplicación de administración de Windows para recibir instrucciones).

Existen dos componentes principales de la utilidad de BACS4: el componente proveedor y el software del cliente. Se instala un proveedor en un servidor, o “host administrado”, que contiene uno o más NIC. El proveedor recolecta información sobre los NIC y la pone a disposición para recuperarla desde una PC de administración donde está instalado el software cliente. El software cliente permite ver información de los proveedores y configurar los NIC. El software cliente BACS incluye una interfaz gráfica de usuario (GUI) y una interfaz de línea de comando (CLI).

Protocolos de comunicación

Un protocolo de comunicación permite el intercambio de información entre el proveedor y el software cliente. Estas son implementaciones de propiedad o de código abierto de los estándares Web-Based Enterprise Management (WBEM) y Common Information Model (CIM) desde la Distributed Management Task Force (DMTF). Los administradores de red pueden elegir la mejor opción según el estándar que prevalece en su red.

La siguiente tabla muestra las opciones disponibles según los sistemas operativos instalados en el host y el cliente administrados.

Si el cliente usa:	*Y el host administrado usa:*	*BACS puede usar estos protocolos de comunicación:*
Windows	Windows	WMI WS-MAN (WinRM)
Windows	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)
Linux	Windows	WS-MAN (WinRM)
Linux	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)

Si el cliente usa:	*Y el host administrado usa:*	*BACS puede usar estos protocolos de comunicación:*

- WMI = Windows Management Instrumentation.
- WS-MAN = Web Service-Management. WinRM es una implementación basada en Windows y OpenPegasus es una implementación de código abierto que opera en Linux.
- CIM-XML = Una versión basada en XML de OpenPegasus.

Si la red incluye una combinación de clientes Windows y Linux que acceden a los servidores Windows y Linux, WS-MAN es la opción adecuada. Si Linux es el único SO instalado en los servidores, CIM-XML es una opción. Si la red incluye solo servidores y clientes Windows, WMI es una opción. WMI es de configuración muy sencilla, pero solo es compatible con el sistema operativo Windows. (Consulte Instalación del controlador y aplicación de administración de Windows para recibir instrucciones sobre la instalación y configuración de los protocolos de Windows.)

La instalación BACS incluye la instalación del componente del proveedor en el host administrado y el software del cliente en la estación de administración. El proceso de instalación difiere según la combinación de sistemas operativos instalados en el cliente y el host administrado y del protocolo de comunicación seleccionado.

Instalación de WS-MAN o CIM-XML en el servidor Linux

Paso 1: Instale OpenPegasus

En el SO de Red Hat Linux, hay disponibles dos opciones de instalación:

- Desde el Inbox RPM (Solo Red Hat)
- Desde el origen (Red Hat y SuSE)

En el SO SUSE Linux Enterprise Server 11 (SLES11), debe usar el RPM de origen.

Nota: El Inbox RPM no es compatible con el protocolo de comunicación WS-MAN. Para usar WS-MAN, debe instalar OpenPegasus desde el origen.

Desde el Inbox RPM (Solo Red Hat)

En Red Hat Linux, un Inbox OpenPegasus RPM está disponible como `tog-pegasus-<version>.<arch>.rpm`.

1. Use el siguiente comando para instalar tog-pegasus:
   `rpm -ivh tog-openpegasus-<version>.<arch>.rpm`
2. Use el siguiente comando para iniciar Pegasus:
   `/etc/init.d/tog-pegasus start`

Nota: En SuSE Linux, el Inbox OpenPegasus RPM no está disponible. OpenPegasus debe estar instalado desde el origen, según se describió en el siguiente procedimiento.

Tenga en cuenta que en inbox Pegasusa, HTTP no está habilitado de manera predeterminada. Después de que Inbox OpenPegasus se instala correctamente, si no se requiere configuración adicional, siga las instrucciones en Paso 4: Instale el proveedor CMPI de Broadcom. Para activar HTTP, consulte Activar HTTP.

Desde el origen (Red Hat y SuSE)

El origen de OpenPegasus se puede descargar desde www.openpegasus.org.

Nota: Si aún no lo instala, descargue e instale openssl y libopenssl-devel rpm. Este paso es optativo y se requiere solo si está planificando usar HTTPS para conectar el cliente con el host administrado.

Configurar las variables del entorno

Configure las variables del entorno para crear OpenPegasus de la siguiente manera.

Variable del entorno	*Descripción*
PEGASUS_ROOT	La ubicación del árbol de fuente Pegasus
PEGASUS_HOME	La ubicación para el repositorio ejecutable creado; ej., subdirectorios $PEGASUS_HOME/bin, PEGASUS_HOME/lib, $PEGAUS_HOME/repository y $PEGASUS_HOME/mof
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	Verdadero
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Para sistemas Linux de 32 bit: "LINUX_IX86_GNU" Para sistemas Linux de 64 bit: "LINUX_X86_GNU"
PEGASUS_HAS_SSL	Opcional. Configurar en "verdadero" para el soporte HTTPS.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Opcional. Configurar en "verdadero" para el soporte del protocolo WSMAN.

Configuración adicional

La variable $PEGASUS_HOME debe configurarse en el entorno de la capa exterior y $PEGASUS_HOME/bin debe anexarse en el entorno $PATH.

Ejemplos

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

Para soporte de SSL, agregue la siguiente variable de entorno:

- exportar PEGASUS_HAS_SSL=true

Para soporte de WS-MAN, agregue la siguiente variable de entorno:

- exportar PEGASUS_ENABLE_PROTOCOL_WSMAN=true

CIM-XML y WSMAN en OpenPegasus use los mismos puertos para HTTP o HTTPS. Los números predeterminados de puertos para HTTP y HTTPS son 5989 y 5989, respectivamente.

Nota: Puede agregar estas exportaciones al final de .bash_profile. Este archivo se ubica en el directorio /root (raíz).

- Las variables del entorno se configurarán cuando un usuario inicie sesión utilizando PuTTY.
- En el sistema Linux, para cada terminal donde las variables del entorno no están configuradas, ejecute el siguiente comando:
  `source /root/.bash_profile`
- Cuando cierre sesión e inicie sesión, se configurarán las variables del entorno.

Crear e instalar OpenPegasus

Desde $PEGASUS_ROOT (la ubicación del directorio raíz de origen Pegasus), ejecute lo siguiente:

```
make clean
make
make repository
```

Nota: Cuando OpenPegasus se cree desde el origen, todas las configuraciones se restablecen a los valores predeterminados. Si está recreando OpenPegasus, debe rehacer la configuración como se mencionó en Paso 3: Configure OpenPegasus en el servidor.

Paso 2: Inicie el servidor CIM en el servidor

Use el comando `cimserver` para iniciar el servidor CIM. Para detener el servidor CIM, use el comando `cimserver -s`.

Para verificar si OpenPegasus se instaló correctamente, ingrese el siguiente comando:

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

Nota: Para OpenPegasus compilado desde el origen, PEGASUS_HOME debe definirse cuando inicia el servidor CIM. De lo contrario, el servidor CIM no cargará correctamente el repositorio. Considere configurar PEGASUS_HOME en el archivo ".bash_profile".

Paso 3: Configure OpenPegasus en el servidor

Use el comando `cimconfig` para configurar OpenPegasus, como se muestra en la siguiente tabla:

Comando	*Descripción*
`cimconfig -l`	Haga una lista de todos los nombres válidos de propiedad.
`cimconfig -l -c`	Haga una lista de todos los nombres válidos de propiedad y su valor
`cimconfig -g <property name>`	Consulta de una propiedad particular.
`cimconfig -s <property name>=<value> -p`	Configure una propiedad particular.
`cimconfig --help`	Sepa más acerca del comando.

El servidor CIM debe iniciarse antes de ejecutar `cimconfig`, y debe reiniciarse para que se apliquen los cambios de configuración.

Activar autenticación

Las siguientes propiedades de OpenPegasus deben configurarse como se describe en esta sección. De lo contrario, el proveedor de Broadcom CIM no funcionará correctamente. Asegúrese de configurar lo siguiente antes de iniciar BACS y conectarse con el proveedor.

Configure el servidor CIM si aún no se ha iniciado. Luego, configure lo siguiente:

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

Si quiere que el usuario raíz se conecte de manera remota:

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

Configuración de usuario con privilegios: Los usuarios de sistema Linux se utilizan para la autenticación de OpenPegasus. Los usuarios del sistema deben agregarse a OpenPegasus utilizando `cimuser` para conectarse a través de BACS:

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

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

Activar HTTP

1. Si no se ha iniciado el servidor CIM, inícielo.
2. Use el siguiente comando para configurar un puerto HTTP (opcional):
   `cimconfig -s httpPort=5988 -p`

   Esta propiedad no está disponible para Inbox OpenPegasus.
3. Use el siguiente comando para activar la conexión HTTP:
   `cimconfig -s enableHttpConnection=true -p`
4. Use los comandos `cimserver -s` y `cimserver`, respectivamente, para detener y reiniciar el servidor CIM para que se aplique la nueva configuración.

Activar HTTPS

1. Si no se ha iniciado el servidor CIM, inícielo.
2. Configure el puerto HTTPS con el siguiente comando (opcional):
   `cimconfig -s httpsPort=5989 -p`

Esta propiedad no está disponible para inbox OpenPegasus.

3. Activar la conexión HTTPS con el siguiente comando:
   `cimconfig -s enableHttpsConnection=true -p`
4. Use los comandos `cimserver -s` y `cimserver`, respectivamente, para detener y reiniciar el servidor CIM para que se aplique la nueva configuración.

Paso 4: Instale el proveedor CMPI de Broadcom

Asegúrese de que OpenPegasus esté instalado adecuadamente antes de instalar CMPI Provider.

Instalar

Ingrese el siguiente comando para instalar Broadcom CMPI Provider.

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

Desinstalar

Ingrese el siguiente comando para desinstalar Broadcom CMPI Provider:

```
% rpm -e BRCM_CMPIProvider
```

Paso 5: Configure Linux Firewall, si fuera necesario

Siga estos procedimientos para abrir los puertos adecuados en el firewall:

Red Hat

1. Haga clic en **System** (Sistema), seleccione **Administration** (Administración) y luego **Firewall**.
2. Seleccione **Other Ports** (Otros puertos).
3. En el cuadro de diálogo Port and Protocol (Puerto y protocolo), seleccione **Definido por usuario**.
4. En el campo **Port/Port Range** (Puerto/Rango de puerto) agregue el número de puerto.
5. En el campo **Protocol** (Protocolo), agregue el protocolo como TCP o UDP, etc.
6. Haga clic en **Apply** (Aplicar) para que se apliquen las reglas del firewall.

Ejemplo:

- Para CIM-XML en HTTP, el número de puerto es 5988 y el protocolo es TCP.
- Para CIM-XML en HTTPS, el número de puerto es 5989 y el protocolo es TCP.

SuSE

1. Haga clic en **Computar** y luego en **YaST**.
2. Seleccione **Security & Users** (Seguridad y usuarios) en el panel de la izquierda.
3. En el panel de la derecha, haga doble clic en **Firewall**.
4. Seleccione **Custom Rules** (Personalizar reglas) del panel de la izquierda.
5. En el panel derecho, haga clic en **Agregar**.
6. Ingrese los siguientes valores:
   - **Red de origen**: 0/0 (significa todas)
   - **Protocolo**: TCP (o el protocolo adecuado)
   - **Puerto de destino**: *<Número de puerto>* o *<Rango de números de puerto>*
   - **Puerto de origen**: Deje en blanco.
7. Haga clic en **Next** (Siguiente) y luego haga clic en **Finish** (Finalizar) para que se apliquen las reglas de firewall.

Ejemplo:

Para CIM-XML, use los siguientes valores:

- **Red de origen**: 0/0 (significa todas)
- **Protocolo**: TCP
- **Puerto de destino**: 5988:5989
- **Puerto de origen**: Deje en blanco.

Paso 6: Instale BACS y aplicaciones de administración relacionadas

Consulte Instalación de la aplicación Broadcom Advanced Control Suite.

Instalación de WS-MAN o CIM-XML en el cliente Linux

No se requieren componentes de software especiales en el sistema de cliente Linux para usar el HTTP excepto la instalación de la aplicación de administración BACS. Sin embargo, para instalaciones de WS-MAN, puede configurar opcionalmente el protocolo HTTPS para usarlo con BACS.

Configurar HTTPS en el cliente Linux

Siga estos pasos si desea usar HTTPS en lugar de HTTP (solo WS-MAN):

Generar un certificado autofirmado para el servidor Windows/Linux

Puede utilizarse Openssl en Linux o Windows para generar el certificado autofirmado de la siguiente manera:

Nota: Puede descargar e instalar openssl desde http://gnuwin32.sourceforge.net/packages/openssl.htm.

1. Ingrese el siguiente comando para generar una clave privada:
   `openssl genrsa -des3 -out server.key 1024`
2. Se le indica que ingrese una frase de contraseña. Asegúrese de recordarla.
3. Siga estos pasos para crear una Solicitud de firma de certificado (CSR).

   Durante la generación de la CSR, se le indica que ingrese varios datos. Cuando se indica “Nombre común”, ingrese el nombre del host o la dirección IP del servidor Windows.

   Ingrese el siguiente comando (se muestran ejemplos de respuestas):

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

   Si este comando no funciona, intente el siguiente:

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

   El archivo openssl.cnf debe estar ubicado en el mismo directorio donde está openssl. Openssl.cnf está ubicado en la carpeta C:\Program Files (x86)\GnuWin32\share.

   Se solicita la siguiente información:

   - Nombre del país (código de 2 letras) []:**US**
   - Nombre del estado o provincia (completo) []: **California**
   - Nombre de la localidad (por ejemplo, ciudad) []: **Irvine**
   - Nombre de la organización (por ejemplo, compañía) []: **Broadcom Corporation**
   - Nombre de la unidad de organización (por ejemplo, sección) []: **Ingeniería**
   - Nombre común (por ejemplo, SU nombre) []: ingrese el nombre del host o la dirección IP del servidor Windows. Para iPv6, ingrese el nombre común en el formato [xyxy:xxx:….::xxx], **incluyendo los paréntesis [ ]**.
   - Dirección de correo electrónico (opcional) []:

   Ingrese los siguientes atributos adicionales con su solicitud de certificado:

   - Una contraseña de comprobación []:**linux1**
   - Un nombre de compañía opcional []:
4. Elimine la frase de contraseña de la clave.

   Ingrese los siguientes comandos:

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

5. Genere un certificado autofirmado:

   Para generar un certificado autofirmado activo durante 365 días, ingrese el siguiente comando:

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

   Aparece la siguiente salida:

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

6. Ingrese el siguiente comando para verificar el certificado autofirmado generado.
   `openssl verify server.crt`

   Aparece la siguiente salida:

   ```
   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
   ```

   Ignore el mensaje de error “error 18 at 0 depth lookup:self signed certificate”. Este error indica que es un certificado autofirmado.

7. Convierta el certificado de formato “crt” a “pkcs12” de la siguiente manera:

   Para un servidor Windows, el certificado debe estar en el formato pkcs12. Ingrese el siguiente comando:

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

   Se le indicará lo siguiente:

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

   Ingrese la contraseña y asegúrese de recordarla. Es necesaria para importar el certificado del servidor y cliente Windows.

8. Haga una copia del archivo del certificado server.crt y ubíquelo en el servidor donde se instalará BACS, de modo que pueda importarse. Si desea utilizar un cliente Windows o Linux para conectarse al servidor que ejecuta BACS, el certificado también debe transferirse (copiarse y pegarse) al sistema cliente.

   En Linux, el certificado debe tener la extensión “.pem”. Las extensiones “.crt” y “.pem” son las mismas, por lo que no hay necesidad de utilizar el comando `openssl` para convertir de .crt a .pem. Puede simplemente copiar el archivo tal cual está.

Nota: Debe generarse un certificado por separado para una dirección IPv4, IPv6 y nombre de host.

Importar el certificado autofirmado en el cliente Linux

En las distribuciones de Linux, fíjese en el siguiente directorio de certificado:

- Para todas las versiones de SuSE, el directorio de certificado es `/etc/ssl/certs`.
- Para Red Hat, el directorio de certificado puede ser distinto para cada versión. Para algunas versiones, es `/etc/ssl/certs` o `/etc/pki/tls/certs`. Para otras versiones, encuentre el directorio del certificado.

Copie *hostname.pem*, que creó en Generar un certificado autofirmado para el servidor Windows/Linux, en el directorio de certificado del cliente Linux. Por ejemplo, si el directorio de certificado es `/etc/ssl/certs`, copie *hostname.pem* en `/etc/ssl/certs`.

1. Cambie el directorio a `/etc/ssl/certs`.

2. Cree un valor del cálculo de direccionamiento para ejecutar el siguiente comando.
   `openssl x509 -noout -hash -in hostname.pem`

   Un valor como el siguiente será devuelto.

   `100940db`

3. Cree un enlace simbólico en el valor del cálculo de direccionamiento ejecutando el siguiente comando:
   `ln -s hostname.pem 100940db.0`

Pruebe la conexión HTTPS/SSL desde el cliente Linux

Use el siguiente comando para probar si el certificado se instaló correctamente en Linux:

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

Si esto falla, el certificado no se instaló correctamente y aparece un mensaje de error que indica corregir.

Instalación de la aplicación Broadcom Advanced Control Suite

El software Broadcom Advanced Control Suite (BACS) se puede instalar en un sistema Linux utilizando el paquete Linux RPM. Esta instalación incluye un cliente de CLI.

Antes de empezar:

- Asegúrese de que los adaptadores de red Broadcom se instalen físicamente y que el controlador del dispositivo adecuado para NIC esté instalado en el sistema para que sea administrado por esta utilidad.
- Asegúrese de que CIM provider esté instalado correctamente en el sistema que será administrado por esta utilidad. Consulte
- Para administrar iSCSI en hosts Linux, asegúrese de que las utilidades open-iscsi y sg estén instaladas en el host Linux.

Para instalar BACS CLI

1. Descargue el paquete RPM de la aplicación de administración BACS más reciente.
2. Instale el paquete RPM utilizando el siguiente comando:
   `% rpm -i BACS-{version}.{arch}.rpm`

Para usar BACS CLI, revise el archivo BACSCLI_Readme.txt proporcionado con los archivos de distribuidos.

Para eliminar BACS

Para desinstalar el paquete RPM, use el siguiente comando:

```
% rpm -e BACS
```

Sección 11: Software del controlador VMware

Paquetes

El controlador VMware se distribuye en el siguiente formato de paquete.

Tabla 19: Paquete del controlador de VMware

Formato	*Controladores*
VMware VIB	vmware-esx-drivers-net-tg3-version.x86_64.vib

Controladores

Descargar, instalar y actualizar controladores

Para descargar, instalar o actualizar el controlador de VMware ESX/ESXi para los adaptadores de red NetXtreme I GbE, consulte http://www.vmware.com/support.

Parámetros del controlador

NetQueue

El parámetro opcional **force_netq** se puede usar para configurar el número de colas de red Rx y Tx. Los dispositivos BCM57XX compatibles con NetQueue son BCM5718, BCM5719, BCM5720, BCM5721 y BCM5722.

De manera predeterminada, el controlador intenta usar el número óptimo de NetQueues. Para obligar explícitamente el número de colas, configure el número de NetQueues por puerto a través del siguiente comando:

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

Los valores permitidos para x son –1 a 15:

- 1–15 obligará al número de NetQueues el NIC asignado.
- 0 deshabilita NetQueue.
- –1 específica usar el valor NetQueue del controlador predeterminado.

El número “x” entradas puede llegar a 32, lo que significa que los NIC máximos permitidos = 32.

Ejemplo de uso:

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

- tg3 NIC 0: Utilice el número predeterminado de NetQueues.
- tg3 NIC 1: Deshabilite la función NetQueue.
- tg3 NIC 2: Utilice 1 NetQueue.
- tg3 NIC 3: Utilice 2 NetQueues.

Tenga en cuenta que NIC # anterior no corresponde a vmnic<#>. El número NIC es el número de orden de sonda vmnic del sistema. Idealmente, el número de NetQueues coincide con el número de CPU de la máquina.

Parámetros del controlador

Se pueden proporcionar varios parámetros opcionales como una línea de comando al comando vmkload_mod. Estos parámetros también se pueden establecer mediante el comando esxcfg-module. Consulte la página del manual para obtener más información.

Valores predeterminados del controlador

Tabla 20: Valores predeterminados de VMware

Parámetro	*Valor predeterminado*
Speed (Velocidad).	Autonegociación con todas las velocidades anunciadas
Control de flujo	Autonegociación con los rx y tx anunciados
MTU	1500 (rango de 46 a 9000)
Tamaño de Rx Ring	200 (rango de 0–511). Algunos chips son fijos a 64.
Tamaño de RX Jumbo Ring:	100 (rango de 0–255). No todos los chips admiten el anillo gigante y algunos chips compatibles con las tramas gigantes no usan el anillo gigante.
Tamaño de TX Ring	511 (rango (MAX_SKB_FRAGS+1) – 511). MAX_SKB_FRAGS varía con los diferentes kernels y las diferentes arquitecturas. Con un kernel 2.6 para x86, MAX_SKB_FRAGS es 18.
Aleación RX microsegundos	20 (rango de 0–1023)
Aleación RX microsegundos irq	20 (rango de 0–255)
Aleación tramas rx	5 (rango de 0–1023)
Aleación tramas rx irq	5 (rango de 0–255)
Aleación TX microsegundos	72 (rango de 0–1023)
Aleación tx usecs irq	20 (rango de 0–255)
Aleación tramas tx	53 (rango de 0–1023)
Aleación tramas tx irq	5 (rango de 0–255)
Aleación estad. usecs	1000000 (aprox. 1 seg.). Algunos parámetros fusionados no se usan o tienen valores predeterminados distintos en algunos chips.
MSI	Activado (si es compatible con el chip y aprobó la prueba de interrupción).
WoL	Deshabilitado.

Mensajes del controlador

A continuación se enumeran los mensajes de muestra más comunes que se pueden registrar en el archivo /var/log/messages. Use `dmesg -n <level>` para controlar el nivel en el que aparecen los mensajes en la consola. La mayoría de los sistemas están configurados de forma predeterminada en el nivel 6. Para ver todos los mensajes, configure un nivel más elevado.

Entrada del controlador

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

NIC detectado

```
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
```

Indicación de enlace activado y velocidad

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

Indicación de enlace desactivado

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

Sección 12: Instalación del controlador y aplicación de administración de Windows

Instalación del software del controlador

Nota: Estas instrucciones se basan en la premisa de que su adaptador Broadcom NetXtreme no se instaló en fábrica. Si la controladora se instaló en fábrica, el software de los controladores ya está instalado.

Cuando Windows se inicia por primera vez después de haber instalado un dispositivo de hardware (tal como un adaptador Broadcom NetXtreme), o después de haberse quitado el controlador de dispositivo existente, el sistema operativo detecta automáticamente el hardware y le pide que instale el software del controlador para ese dispositivo.

Tanto el modo de instalación gráfica interactiva (ver Uso del instalador) como un modo silencioso de línea de comando para instalación desatendida (ver Cómo usar la instalación silenciosa) se encuentran disponibles.

NOTAS:

- Antes de instalar el software del controlador, verifique que el sistema operativo Windows haya sido actualizado a la última versión con el último paquete de servicios aplicado.
- Se debe instalar un controlador de dispositivos de red antes de que se pueda usar el adaptador Broadcom NetXtreme Gigabit Ethernet con su sistema operativo Windows. Los controladores están ubicados en el CD de instalación.
- BACS no cuenta con soporte para la opción de instalación Server Core de Microsoft Windows Server 2008 R2.

Uso del instalador

Además de los controladores de dispositivos de Broadcom, el instalador instala las aplicaciones de administrador. Si se encuentra disponible, cuando se ejecuta el instalador, se instala lo siguiente:

- **Controladores de dispositivos Broadcom**. Instala los controladores de dispositivos Broadcom.
- **Control Suite**. Broadcom Advanced Control Suite (BACS).
- **BASP**. Instala Broadcom Advanced Server Program.
- **SNMP**. Instala el subagente del protocolo de administración de red simplificada.
- **CIM Provider**. Instala el proveedor de modelo de información común.
- **Controlador de vuelco para caída del sistema iSCSI**. Instala el controlador necesario para la utilidad de vuelco para caída del sistema iSCSI.

Nota: Aunque la instalación del software BACS y de las aplicaciones de administración relacionadas es opcional, los controladores de dispositivos Broadcom deben instalarse cuando se utiliza el instalador.

Nota: BASP no está disponible en Windows Small Business Server (SBS) 2008.

Para instalar el software de inicio iSCSI de Microsoft para el vuelco para caída del sistema iSCSI.

Si es compatible y utilizará la utilidad de vuelco para caída del sistema iSCSI de Broadcom, es importante que siga la secuencia de instalación:

- Ejecute el instalador
- Instale el software de inicio iSCSI de Microsoft junto con el parche (MS KB939875)

Nota: Si realiza una actualización de los controladores de dispositivos desde el instalador, vuelva a habilitar **iSCSI Crash Dump** (Vuelco para caída del sistema iSCSI) en la sección Advanced (Avanzado) de la ficha BACS Configuration (Configuración de BACS).

Lleve a cabo este procedimiento después de ejecutar el instalador para instalar los controladores del dispositivo y las aplicaciones de administración.

1. Instale Microsoft iSCSI Software Initiator (versión 2.06 o posterior) si no está incluido en su sistema operativo. Para determinar cuándo debe instalar el Microsoft iSCSI Software Initiator, consulte Tabla 21. Para descargar el iniciador de software iSCSI desde Microsoft, vaya a http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986.
2. Instale el parche de Microsoft para la generación del archivo de vuelco para caída del sistema iSCSI (Microsoft KB939875) desde http://support.microsoft.com/kb/939875. Para determinar si es necesario instalar el parche de Microsoft, consulte Tabla 21.

Tabla 21: Sistemas operativos de Windows y Vuelco para caída del sistema iSCSI

Sistema operativo:	*Se requiere MS iSCSI Software Initiator*	*Se requiere el parche de Microsoft (MS KB939875)*
NDIS		
Windows Server 2008	Sí (incluido en el sistema operativo)	No
Windows Server 2008 R2	Sí (incluido en el sistema operativo)	No
Windows Server 2012	Sí (incluido en el sistema operativo)	No
OIS		
Windows Server 2008	No	No
Windows Server 2008 R2	No	No
Windows Server 2012	No	No

Cómo usar la instalación silenciosa

NOTAS:

- Todos los comandos distinguen mayúsculas y minúsculas.
- Para obtener instrucciones e información más detallada sobre las instalaciones desatendidas, consulte el archivo Silent.txt file de la carpeta Driver_Management_Apps_Installer.

Consulte el archivo readme.txt ubicado en la carpeta de instalación para las instrucciones de la línea de comandos.

Nota: El comando REINSTALL (reinstalar) debe utilizarse únicamente si el mismo instalador ya se encuentra instalado en el sistema. Si se encuentra actualizando una versión anterior del instalador, utilice el comando `setup /s /v/qn`, como se especificó anteriormente.

Modificación del software del controlador

Para modificar el software del controlador

1. En el Panel de Control, haga doble clic en **Add or Remove Programs (Agregar o quitar programas)**.
2. Haga clic en **Broadcom Drivers and Management Applications (Controladores y aplicaciones de administración Broadcom)** y luego haga clic en **Change (Cambiar)**.
3. Haga clic en **Next (Siguiente)** para continuar.
4. Haga clic en **Modify, Add, or Remove (Modificar, Agregar o Quitar)** para modificar las características del programa. Esta opción no instala controladores para adaptadores nuevos. Para obtener información sobre la instalación de adaptadores nuevos, consulte Reparación o reinstalación del software del controlador.
5. Haga clic en **Next (Siguiente)** para continuar.
6. Haga clic en un icono para modificar la instalación de una característica.
7. Haga clic en **Siguiente.**
8. Haga clic en **Install (Instalar)**.
9. Haga clic en **Finish (Finalizar)** para cerrar el instalador.
10. El instalador determinará si es necesario reiniciar el sistema. Siga las instrucciones que aparecen en la pantalla.

Reparación o reinstalación del software del controlador

Para reparar o reinstalar el software del controlador

1. En el Panel de Control, haga doble clic en **Add or Remove Programs (Agregar o quitar programas)**.
2. Haga clic en **Broadcom Drivers and Management Applications (Controladores y aplicaciones de administración Broadcom)** y luego haga clic en **Change (Cambiar)**.
3. Haga clic en **Next (Siguiente)** para continuar.
4. Haga clic en **Repair or Reinstall (Reparar o reinstalar)** para reparar errores o instalar controladores para adaptadores nuevos.
5. Haga clic en **Next (Siguiente)** para continuar.
6. Haga clic en **Install (Instalar)**.
7. Haga clic en **Finish (Finalizar)** para cerrar el instalador.
8. El instalador determinará si es necesario reiniciar el sistema. Siga las instrucciones que aparecen en la pantalla.

Cómo quitar los controladores de dispositivos

Si elimina los controladores de dispositivos, también se quitan las aplicaciones de administración instaladas.

Nota: Windows Server 2008 y Windows Server 2008 R2 ofrecen la función Device Driver Rollback para reemplazar un controlador de dispositivo por otro previamente instalado. Sin embargo, la compleja arquitectura del software del dispositivo NetXtreme puede presentar problemas si esta característica de reinstalación se utiliza con uno de los componentes individuales. Por lo tanto, recomendamos que los cambios de versiones del controlador se realicen únicamente a través de un instalador de controladores.

Para eliminar controladores de dispositivos.

1. En el Panel de Control, haga doble clic en **Add or Remove Programs (Agregar o quitar programas)**.
2. Haga clic en **Broadcom Drivers and Management Applications (Controladores y aplicaciones de administración Broadcom)** y luego haga clic en **Remove (Eliminar)**. Siga las instrucciones que aparecen en la pantalla.
3. Reinicie su sistema para eliminar completamente los controladores. Si no reinicia su sistema, no podrá instalar con éxito los controladores.

Cómo visualizar o cambiar las propiedades del adaptador

Para ver o cambiar las propiedades del adaptador de red Broadcom

1. En el Panel de control, haga clic en **Broadcom Control Suite 4**.
2. Haga clic en la sección Advanced (Avanzado) de la ficha **Configurations** (Configuración).

Configuración de las opciones de administración de energía

Podrá configurar las opciones de administración de energía para permitir que el sistema operativo apague la controladora para ahorrar energía o para que la controladora active el sistema. Sin embargo, si el dispositivo está ocupado haciendo algo (por ejemplo, atendiendo un llamado), el sistema operativo no apagará el dispositivo. El sistema operativo trata de apagar todos los dispositivos posibles únicamente cuando la computadora trata de entrar en hibernación. Para que la controladora permanezca activa en todo momento, no haga clic en el casillero **Permitir que la computadora apague el dispositivo para ahorrar energía**.

Nota: Las opciones de administración de energía no se encuentran disponibles para los servidores blade.

NOTAS:

- La ficha Power Management (Administración de energía) sólo está disponible para los servidores que soportan la administración de energía.
- Para habilitar Wake on LAN (WOL) cuando la computadora se encuentre en standby (espera), haga clic en la casilla **Allow the device to bring the computer out of standby (Permitir a este dispositivo reactivar el equipo)**.
- Si selecciona **Only allow management stations to bring the computer out of standby** (Permitir que solo las estaciones de administración saquen la computadora del estado en espera), la computadora puede salir del estado en espera *solo a través de Magic Packet*.

¡Precaución! No seleccione **Allow the computer to turn off the device to save power (Permitir que la computadora apague el dispositivo para ahorrar energía)** para ningún adaptador que forme parte de un equipo.

Configuración del protocolo de comunicación para utilizar con BACS4

La aplicación de administración BACS4 tiene dos componentes principales: el componente del proveedor y el software cliente. Se instala un proveedor en un servidor, o “host administrado”, que contiene uno o más NIC. El proveedor recolecta información sobre los NIC y la pone a disposición para recuperarla desde una PC de administración donde está instalado el software cliente. El software cliente permite ver información de los proveedores y configurar los NIC. El software cliente BACS incluye una interfaz gráfica de usuario (GUI) y una interfaz de línea de comando (CLI).

Permiten la comunicación entre el proveedor y el software cliente. Dependiendo de la mezcla de sistemas operativos (Linux, Windows o ambos) en los clientes y hosts administrados de la red, puede elegir usar un protocolo de comunicación adecuado. Consulte Instalación de la aplicación de administración Linux para acceder a una descripción de los protocolos de comunicación disponibles para cada configuración de red.

Las instrucciones de este capítulo abordan únicamente la situación donde los hosts administrados Windows se están comunicando con los clientes Windows. En estas situaciones, puede usar los protocolos de comunicación WMI o WS-MAN (WinRM). Al utilizar el instalador del controlador descrito en este capítulo para instalar el controlador y las aplicaciones de administración, el proveedor de WMI y WS-MAN se instala en el host administrado. Además, la utilidad BACS4 se instala en el cliente. Las siguientes secciones entregan pasos adicionales de configuración para el protocolo de comunicación seleccionado.

Para instalaciones de Linux, el controlador se instala de manera separada desde las aplicaciones de administración. Consulte para obtener instrucciones relacionadas.

Uso de WS-MAN

Para usar el protocolo de comunicación WS-MAN, siga las instrucciones de las secciones a continuación:

- Configuración del servidor de Windows WS-MAN
- Instalación del cliente de Windows WS-MAN

Configuración del servidor de Windows WS-MAN

Paso 1: instale el componente de software WinRM en el servidor

En los siguientes sistemas operativos, WinRM 2.0 está preinstalado:

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

Para Windows Server 2008, instale Windows Management Framework Core, que incluye WinRM 2.0 y Windows Powershell 2.0, desde el siguiente enlace:

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

Paso 2: lleve a cabo la configuración básica en el servidor

El firewall de Windows debe estar habilitado para que WinRM funcione correctamente. Para obtener información detallada sobre la configuración del firewall, consulte Paso 7: Configuración adicional del servidor. Después de la configuración del firewall, abra el Símbolo del sistema y ejecute el siguiente comando para habilitar la administración remota en el servidor Windows:

```
winrm quickconfig
```

Puede utilizar el siguiente comando para ver la información de configuración del servicio:

```
winrm get winrm/config
```

Paso 3: lleve a cabo la configuración del usuario en el servidor

Para conectarse con WinRM, la cuenta debe ser miembro del grupo de administradores locales en el equipo local o remoto. La salida del comando `get winrm/config` será la siguiente:

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

BA significa BUILTIN\Administrators.

Para agregar otro grupo de usuarios a la lista de conexiones permitidas de WinRM, puede modificar RootSDDL para incluir el nuevo grupo de usuarios. Necesitará la Id. de SSDL para el grupo nuevo. Por ejemplo, el siguiente comando agrega el nuevo grupo de usuarios con la Id. de SDDL S-1-5-21-1866529496-2433358402-1775838904-1021.

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

Paso 4: lleve a cabo la configuración HTTP en el servidor

Para utilizar la GUI de BACS, debe configurar el protocolo HTTP de la siguiente manera:

Nota: El puerto HTTP predeterminado es 5985 para WinRM 2.0.

1. Haga clic en **Inicio** (o presione la tecla con el logotipo de Windows) y seleccione **Ejecutar**.
2. Escriba **gpedit.msc** para abrir el editor local de directivas de grupo.
3. En **Configuración del equipo**, abra la carpeta **Plantillas administrativas** y luego la carpeta **Componentes de Windows**.
4. Seleccione **Administración remota de Windows (WinRM)**.
5. En **Administración remota de Windows (WinRM)**, seleccione **Cliente WinRM**.
6. En **Cliente WinRM**, haga doble clic en **Hosts de confianza**.
7. En la **Lista de hosts de confianza**, ingrese los nombres de los hosts de los clientes. Si todos los clientes son de confianza, ingrese solo un asterisco (*).
8. Seleccione **Servicio WinRM**.
9. Habilite **Permitir autenticación básica**.

10. Habilite **Permitir tráfico sin cifrado**.
11. Cierre la ventana **Directivas de grupo**.
12. En el Símbolo del sistema, ejecute el siguiente comando para configurar WinRM con los valores predeterminados:
    `winrm qc or winrm quickconfig`
13. Cuando la herramienta muestre "**¿Realizar estos cambios? [s/n]**", ingrese "**s**".
14. Ingrese uno de los siguientes comandos para verificar si se crea un agente de escucha HTTP:
    `winrm enumerate winrm/confg/listener`

    o

    `winrm e winrm/config/Listener`
15. Ingrese el siguiente comando en el Símbolo del sistema para realizar una prueba local.
    `winrm id`

Paso 5: lleve a cabo la configuración HTTPS en el servidor (para utilizar HTTPS en lugar de HTTP)

Este paso consiste en dos procesos distintos: generación de un certificado autofirmado, si no existe, e importarlo a un servidor Windows. Si no existe, debe configurar un certificado autofirmado en el servidor Windows para habilitar la comunicación HTTPS/SSL con la GUI de BACS GUI en el cliente Windows. El cliente Windows también debe configurarse con el certificado autofirmado. Consulte Lleve a cabo la configuración HTTPS (si desea utilizar HTTPS).

Nota: El certificado autofirmado puede crearse en cualquier servidor Windows. El servidor no requiere la instalación de BACS. El certificado autofirmado generado en cualquier servidor Windows debe copiarse en el disco local del cliente.

1. Haga clic en **Inicio** (o presione la tecla con el logotipo de Windows) y seleccione **Ejecutar**.
2. Escriba **gpedit.msc** para abrir el editor local de directivas de grupo.
3. En **Configuración del equipo**, abra la carpeta **Plantillas administrativas** y luego la carpeta **Componentes de Windows**.
4. Seleccione **Administración remota de Windows (WinRM)**.
5. En **Administración remota de Windows (WinRM)**, seleccione **Cliente WinRM**.
6. En **Cliente WinRM**, haga doble clic en **Hosts de confianza**.
7. En la **Lista de hosts de confianza**, ingrese los nombres de los hosts de los clientes. Si todos los clientes son de confianza, ingrese solo un asterisco (*).
8. Seleccione **Servicio WinRM**.
9. Habilite **Permitir autenticación básica**.

Para generar un certificado autofirmado para el servidor Windows:

Puede utilizarse Openssl en Windows para generar el certificado autofirmado de la siguiente manera:

1. Ingrese el siguiente comando para generar una clave privada:
   `openssl genrsa -des3 -out server.key 1024`
2. Se le indica que ingrese una frase de contraseña. Asegúrese de recordarla.
3. Siga estos pasos para crear una Solicitud de firma de certificado (CSR).

   Durante la generación de la CSR, se le indica que ingrese varios datos. Cuando se indica "Nombre común", ingrese el nombre del host o la dirección IP del servidor Windows.

   Ingrese el siguiente comando (se muestran ejemplos de respuestas):

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

Si este comando no funciona, intente el siguiente:

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

El archivo openssl.cnf debe estar ubicado en el mismo directorio donde está openssl. Openssl.cnf está ubicado en la carpeta C:\Program Files (x86)\GnuWin32\share.

Se solicita la siguiente información:

- Nombre del país (código de 2 letras) []:**US**
- Nombre del estado o provincia (completo) []: **California**
- Nombre de la localidad (por ejemplo, ciudad) []: **Irvine**
- Nombre de la organización (por ejemplo, compañía) []: **Broadcom Corporation**
- Nombre de la unidad de organización (por ejemplo, sección) []: **Ingeniería**
- Nombre común (por ejemplo, SU nombre) []: ingrese el nombre del host o la dirección IP del servidor Windows. Para iPv6, ingrese el nombre común en el formato [xyxy:xxx:….::xxx], **incluyendo los paréntesis [ ]**.
- Dirección de correo electrónico (opcional) []:

Ingrese los siguientes atributos adicionales con su solicitud de certificado:

- Una contraseña de comprobación []:**contraseña1**
- Un nombre de compañía opcional []:

4. Elimine la frase de contraseña de la clave.

Ingrese los siguientes comandos:

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

5. Genere un certificado autofirmado:

Para generar un certificado autofirmado activo durante 365 días, ingrese el siguiente comando:

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

Aparece la siguiente salida:

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

6. Ingrese el siguiente comando para verificar el certificado autofirmado generado.

```
openssl verify server.crt
```

Aparece la siguiente salida:

```
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
```

Ignore el mensaje de error “error 18 at 0 depth lookup:self signed certificate”. Este error indica que es un certificado autofirmado.

7. Convierta el certificado de formato “crt” a “pkcs12” de la siguiente manera:

Para un servidor Windows, el certificado debe estar en el formato pkcs12. Ingrese el siguiente comando:

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

Se le indicará lo siguiente:

```
Enter Export Password:
```

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

Ingrese la contraseña y asegúrese de recordarla. Es necesaria para importar el certificado del servidor y cliente Windows.

8. Haga una copia del archivo del certificado server.crt y ubíquelo en el servidor donde se instalará BACS, de modo que pueda importarse. Si desea utilizar un cliente Windows para conectarse al servidor que ejecuta BACS, el certificado también debe transferirse (copiarse y pegarse) al sistema cliente.

Nota: Debe generarse un certificado por separado para una dirección IPv4, IPv6 y nombre de host.

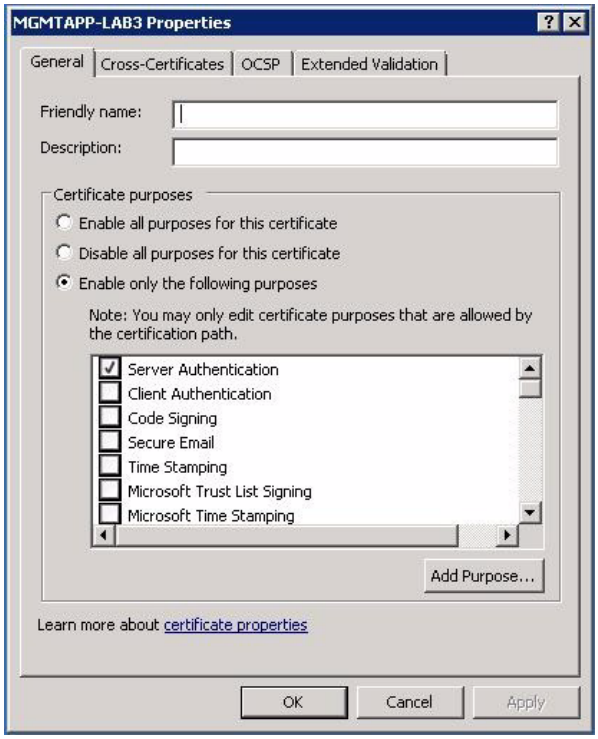
Para instalar el certificado autofirmado en el servidor Windows:

Transfiera el archivo *hostname*.pfx generado en el servidor Windows antes de instalar el certificado:

1. Haga clic en **Inicio** (o presione la tecla con el logotipo de Windows) y seleccione **Ejecutar**.
2. Ingrese **MMC** y haga clic en **Aceptar**.
3. Haga clic en **Archivo** > **Agregar/quitar complemento**.
4. Haga clic en **Agregar**.
5. Seleccione **Certificados** y haga clic en **Agregar**.
6. Seleccione **Cuenta de equipo**.
7. Haga clic en **Siguiente** y luego en **Finalizar**.
8. Haga clic en **Cerrar** y luego en **Aceptar**.
9. Abra la carpeta **Certificados (equipo local)** y la carpeta **Personal**.
10. Haga clic con el botón derecho en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.
11. Haga clic en **Siguiente** para iniciar el Asistente de importación de certificados.
12. Examine para seleccionar **hostname.pfx**.
13. Cuando se le indique que ingrese la contraseña de la clave privada, ingrese la misma contraseña creada en Para generar un certificado autofirmado para el servidor Windows:.
14. Siga las instrucciones, seleccione los valores predeterminados y continúe.

    El certificado aparece como instalado al lado derecho de la ventana. El nombre será el especificado al crear un certificado autofirmado.
15. Haga clic con el botón secundario en el certificado y seleccione **Propiedades**.

    Aparece el siguiente cuadro de diálogo:



16. Asegúrese de que sólo **Autenticación de servidor** esté habilitado, como se muestra en la figura.

17. Abra **Entidades de certificación raíz de confianza** y luego **Certificados**.

18. Siga las instrucciones de Paso 11. a Paso 17.

Nota: Consulte Lleve a cabo la configuración HTTPS (si desea utilizar HTTPS) para obtener instrucciones sobre la importación del certificado autofirmado en un cliente.

Paso 6: configure WinRM HTTPS/SSL en el servidor

1. Cree un agente de escucha de WinRM de la siguiente manera:

a. Haga clic en **Inicio** (o presione la tecla con el logotipo de Windows) y seleccione **Ejecutar**.

b. Ingrese **MMC** y haga clic en **Aceptar**.

c. Seleccione el certificado autofirmado en el Almacén personal.

Por ejemplo, si el certificado se crea con un nombre de host, este aparecerá.

d. Haga doble clic en el certificado para abrirlo.

e. Haga clic en la ficha **Detalles**.

f. Desplácese hacia abajo y seleccione el campo **Huella digital**.

g. Seleccione y copie la huella digital en la ventana **Detalles** para insertarla en el paso siguiente.

h. Regrese al Símbolo del sistema.

i. Ingrese el siguiente comando:

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

NOTAS:

- Si el certificado se generó utilizando el nombre del host, ingrese el nombre. Si se generó con la dirección IP, ingrese la dirección IP. Para una dirección IPv6, utilice paréntesis [ ] alrededor de la dirección.
- Si HTTPS está configurado en su sistema, el agente de escucha debe eliminarse antes de crear un agente de escucha HTTPS nuevo. Utilice el siguiente comando:
  `winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`

j. El comando de escucha crea un agente de escucha en el puerto HTTPS (5986) con cualquiera o todas las direcciones de red del servidor, y el certificado generado con SelfSSL.

k. Puede utilizar el comando `winrm` para modificar o configurar el agente de escucha HTTPS y los agentes de escucha WinRM pueden configurarse en cualquier puerto definido por el usuario.

l. En el Símbolo del sistema, ejecute el siguiente comando para verificar los agentes de escucha configurados:
```
winrm e winrm/config/listener
```

2. Pruebe la conexión HTTPS/SSL en el servidor.

a. En el indicador de comando del servidor, ingrese el siguiente comando:
```
winrs -r:https://yourserver:5986 -u:username -p:password hostname
```

b. Si la configuración es correcta, la salida del comando muestra el nombre del host del servidor.

c. Para verificar la configuración del servicio WinRM, ejecute el siguiente comando:
```
winrm get winrm/config/service
```

Paso 7: Configuración adicional del servidor

Si es necesario, modifique las reglas del firewall de la siguiente manera:

Windows Server 2008 R2

1. En el menú **Herramientas administrativas**, abra **Firewall de Windows con seguridad avanzada**.

2. Haga clic con el botón derecho en **Reglas de entrada** y seleccione **Nueva regla**.

Se abre el asistente de nuevas reglas.

3. Seleccione **Puerto** y haga clic en **Siguiente**.

4. En la pantalla **Protocolo y puertos**, seleccione **TCP** e ingrese el puerto específico, por ejemplo 5985 para HTTP o 5986 para HTTPS.

5. Haga clic en **Siguiente.**

6. En la pantalla **Acción**, seleccione **Permitir la conexión** y haga clic en **Siguiente**.

7. En **Perfil**, puede seleccionar los tres perfiles si su servidor está en un grupo de trabajo.

8. Especifique un nombre para la regla y haga clic en **Finalizar**.

9. Asegúrese de que la nueva regla esté habilitada (que la casilla de verificación verde esté seleccionada).

Windows XP

1. Haga clic en **Inicio** > **Panel de control** y haga doble clic en **Firewall de Windows**.

2. Haga clic en la ficha **Excepciones**

3. Haga clic en **Agregar puerto**.

4. Ingrese un **nombre** con sentido, por ejemplo “regla WinRM” y el número de puerto, por ejemplo 5985 para HTTP o 5986 para HTTPS.

5. Haga clic en **Aceptar**.

Comandos WinRM útiles

Comando	*Descripción*
`winrm quickconfig or winrm qc`	Configura WinRM con los valores predeterminados
`winrm enumerate winrm/config/Listener or winrm e winrm/config/Listener`	Ayuda a verificar cuál agente de escucha de servicio está habilitado y detectar en cuál puerto y dirección IP.
`winrm get winrm/config/Service`	Verifica la configuración de servicio de WinRM Service.
`winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`	Elimina un agente de escucha (en este caso un agente de escucha HTTPS).

Sitios Web útiles de WinRM

- 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
- Los siguientes artículos en http://support.microsoft.com:
  - “Configurar WINRM para HTTPS”
  - “Marco de administración de Windows (Windows PowerShell 2.0, WinRM 2.0 y 4.0 de BITS)”

Instalación del cliente de Windows WS-MAN

En el cliente Windows, lleve a cabo los siguientes pasos de configuración.

1. Lleve a cabo la configuración HTTP (si desea utilizar HTTP)
   a. Haga clic en **Inicio** (o presione la tecla con el logotipo de Windows) y seleccione **Ejecutar**.
   b. Escriba **gpedit.msc** para abrir el editor local de directivas de grupo.
   c. En **Configuración del equipo**, abra la carpeta **Plantillas administrativas** y luego la carpeta **Componentes de Windows**.
   d. Seleccione **Administración remota de Windows (WinRM)**.
   e. En **Administración remota de Windows (WinRM)**, seleccione **Cliente WinRM**.
   f. En **Cliente WinRM**, haga doble clic en **Hosts de confianza**.
   g. En la **Lista de hosts de confianza**, ingrese los nombres de los hosts de los clientes y haga clic en **Aceptar**. Si todos los clientes son de confianza, ingrese solo “*”.
   h. Seleccione **Servicio WinRM**.
   i. Habilite **Permitir autenticación básica** y haga clic en **Aceptar**.
   j. Ejecute el siguiente comando en el Símbolo del sistema para realizar una prueba de la conexión.
      `winrm id -remote:<remote machine Hostname or IP Address>`
2. Lleve a cabo la configuración HTTPS (si desea utilizar HTTPS)

   Después de generar un certificado autofirmado, como se describe en Para generar un certificado autofirmado para el servidor Windows:, puede importar el certificado del cliente para facilitar la conexión entre servidor y cliente. Asegúrese de que se completen todos los pasos de la sección Para generar un certificado autofirmado para el servidor Windows:, incluida la copia de *hostname.pfx* en la ubicación desde donde el cliente pueda acceder al archivo, antes de continuar con los pasos siguientes.

   a. Haga clic en **Inicio** (o presione la tecla con el logotipo de Windows) y seleccione **Ejecutar**.
   b. Ingrese **MMC** y haga clic en **Aceptar**.
   c. Haga clic en **Archivo** y seleccione **Agregar/quitar complemento**.
   d. Haga clic en **Agregar**.

e. Seleccione **Certificados** y haga clic en **Agregar**.

f. Seleccione **Cuenta de equipo** y haga clic en **Siguiente**.

g. Haga clic en **Finish (Finalizar)**.

h. Haga clic en **Cerrar** y luego en **Aceptar**.

i. En **Certificates (Local Computer)** (Certificados, Equipo local), haga clic con el botón derecho en **Trusted Root Certification Authorities** (Entidades de certificación raíz de confianza), seleccione **All Task** (Todas las tareas) y seleccione **Import** (Importar).

j. Haga clic en **Siguiente** para iniciar el Asistente de importación de certificados.

k. Examine para seleccionar el archivo .pfx generado en Para generar un certificado autofirmado para el servidor Windows:. Cambie la selección en la lista **Archivos de tipo** a **Intercambio de información personal (*.pfxas, *.p12)**, seleccione el archivo *hostname.pfx* y haga clic en **Abrir**.

l. Ingrese la contraseña asignada a la clave privada y haga clic en **Siguiente**.

3. Configurar WinRM HTTPS/SSL

Puede ejecutar `winrm` desde un cliente para recuperar información desde la conexión de WinRM HTTPS. Siga estos pasos para probar la conexión de WinRM HTTPS/SSL desde el cliente:

a. Para recuperar la información del sistema operativo del servidor, ingrese el siguiente comando.
```
winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername -u:username
-p:password -skipCAcheck
```

b. Para recuperar la información de identidad de WinRM, ingrese el siguiente comando.
```
winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
```

c. Para enumerar los servicios de Windows en el servidor, ingrese el siguiente comando.
```
winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -
skipCAcheck
```

Nota: Es importante utilizar el conmutador `-skipCAcheck` en la prueba de la línea de comandos `winrm`, ya que el certificado es autogenerado y no importado en el cliente. De lo contrario aparece el siguiente mensaje de error: `WSManFault.`

Uso de WMI

No se requiere configuración especial para utilizar WMI en el cliente Windows. Lleve a cabo los pasos de las siguientes secciones para configurar WMI en el servidor Windows.

Paso 1: configure la seguridad de espacio de nombres con Control WMI

El Control WMI ofrece una manera de administrar la seguridad de espacio de nombres. Puede inicial el Control WMI desde un indicador de comandos con el siguiente comando:

```
wmimgmt
```

En Windows 9x o Windows NT4, las computadoras con WMI instalado utilizan este comando:

```
wbemcntl.exe
```

De forma alternativa, puede acceder al Control WMI y la ficha Seguridad de la siguiente manera:

1. Haga clic con el botón secundario en **Mi PC** y haga clic en **Administrar**.
2. Haga doble clic en **Servicios y aplicaciones** y luego doble clic en **Control WMI**.
3. Haga clic con el botón secundario en **Control WMI** y haga clic en **Propiedades**.
4. En Propiedades de Control WMI, haga clic en la ficha **Seguridad**.
5. Debe aparecer una carpeta con el nombre Raíz, con un signo más (+) al lado. Expanda este árbol si es necesario para ubicar el espacio de nombres para el cual desea configurar permisos.
6. Haga clic en **Security**.

   Aparece una lista de usuarios y sus permisos. Si el usuario está en la lista, modifique los permisos según corresponda. Si el usuario no está en la lista, haga clic en **Agregar** y agregue el usuario desde la ubicación (máquina local, dominio, etc.) donde se ubica la cuenta.

NOTAS: Puede agregar estas exportaciones al final de .bash_profile. Este archivo se ubica en el directorio /root (raíz).

- Para ver y configurar la seguridad de espacio de nombres, el usuario debe tener permisos de lectura y edición de seguridad. Los administradores tienen estos permisos de manera predeterminada y pueden asignar los permisos a otras cuentas de usuario de ser necesario.
- Si este usuario necesita acceder al espacio de nombres de manera remota, debe seleccionar el permiso de habilitación remota.
- De manera predeterminada, los permisos para los usuarios configurados en un espacio de nombres solo se aplican a dicho espacio de nombres. Si desea que el usuario tenga acceso a un espacio de nombres y todos los espacios de nombres del árbol inferior, o solo en los espacios de nombres secundarios, haga clic en **Avanzado**. Haga clic en **Editar** y especifique el ámbito de acceso en el cuadro de diálogo que aparece.

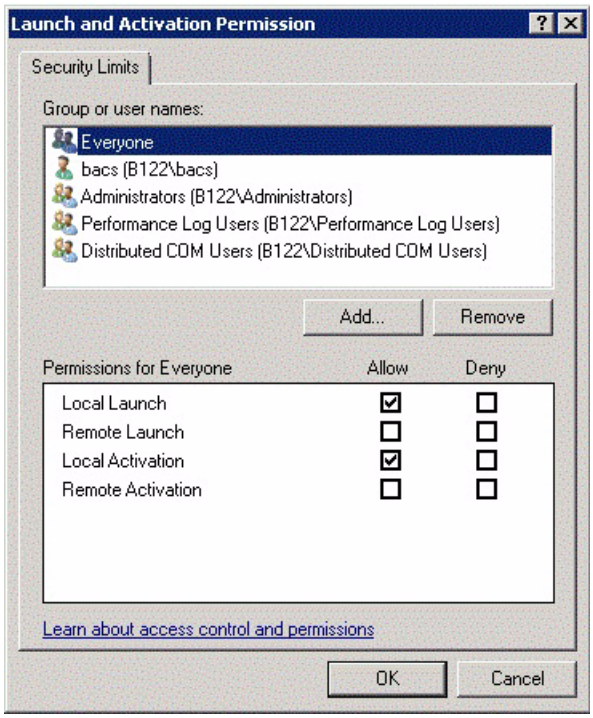
Paso 2: otorgue permisos de inicio y activación remotos de DCOM

En el entorno de dominio Windows, la cuenta del administrador de dominio tiene los privilegios necesario para acceder al componente WMI para la administración BACS, por lo que no se requiere configuración especial. Sin embargo, en una gran empresa, es posible que un usuario que acceda al host local o remoto con la GUI del cliente BACS4 no siempre cuente con los privilegios de la cuenta del administrador de dominio. Es necesario configurar el acceso a la seguridad de WMI en el host remoto para permitir que el usuario se conecte mediante la GUI del cliente BACS4.

Esta configuración es fácil de hacer con el siguiente procedimiento. Si no tiene suficientes privilegios para configurar la seguridad del acceso a WMI, comuníquese con su administrador de red.

1. Haga clic en **Inicio**, haga clic en **Ejecutar**, escriba **DCOMCNFG** y haga clic en **Aceptar**.
2. Aparece el cuadro de diálogo Servicios de componentes.
3. Abra **Servicios de componentes** y luego **Equipos**.
4. Haga clic con el botón derecho en **Mi PC** y haga clic en **Propiedades**.
5. En **Propiedades de mi PC** haga clic en la ficha **Seguridad COM**.
6. En **Permisos de inicio y activación**, haga clic en **Editar límites**.
7. Siga estos pasos si su nombre o grupo no aparece en la lista **Nombres de grupos o usuarios**.
   a. En el cuadro de diálogo Permiso de inicio y haga clic en **Agregar**.
   b. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, agregue su nombre y el grupo en el cuadro **Escriba los nombres de objeto que desea seleccionar** y haga clic en **Aceptar**.
   c. En el cuadro de diálogo Permiso de inicio, seleccione su grupo y usuario en la lista **Nombres de grupos o usuarios**.
   d. En el área **Permisos para el usuario**, seleccione **Permitir** para **Inicio remoto** y **Activación remota** y haga clic en **Aceptar**.

Figura 8: Permiso de inicio y activación



Para obtener más información, consulte Asegurar una conexión WMI remota en el sitio de Microsoft Developer Network.

Configuración especial para WMI en sistemas diferentes

En Windows Vista y Windows 7, para permitir que todos los usuarios del grupo de administradores se conecten con el espacio de nombres WMI, es posible que el usuario necesite cambiar LocalAccountTokenFilterPolicy.

Sección 13: Uso de Broadcom Advanced Control Suite 4

Generalidades de Broadcom Advanced Control Suite

Broadcom Advanced Control Suite (BACS) es una utilidad integrada que ofrece información útil sobre cada adaptador de red instalado en su sistema. BACS también le permite realizar pruebas, diagnósticos y análisis detallados de cada adaptador, como también ver y modificar los valores de propiedad, y ver estadísticas de tráfico para objetos de red. BACS opera en sistemas operativos Wndows y Linux.

La aplicación Broadcom Advanced Server Program (BASP), que se ejecuta en Broadcom Advanced Control Suite, se usa para configurar equipos para el balance de carga, la tolerancia a fallas y las redes de área local virtuales (VLAN). La funcionalidad BASP está disponible sólo en sistemas que usan, por lo menos, un adaptador de red de Broadcom. BASP opera solo en sistemas operativos Windows.

Nota: Algunas funciones de BACS son pertinentes solo para adaptadores específicos. Debido a que una instancia única de BACS puede ser utilizada para comunicarse con varios hosts y tipos de adaptadores, este documento describe todas las características de BACS.

La aplicación BACS incluye una interfaz gráfica de usuario y una interfaz de línea de comando (BACSCLI). BACS GUI y BACS CLI funcionan en las siguientes familias de sistemas operativos:

- Windows
- Windows Server
- Linux Server

Para obtener más información sobre las últimas versiones de SO compatibles, consulte la documentación de versión proporcionada en la distribución de su software.

Arranque de Broadcom Advanced Control Suite

En el Panel de control, haga clic en **Broadcom Control Suite 4**, o haga clic en el icono BACS en la barra de tareas ubicada en la parte inferior del escritorio de Windows o Windows Server.

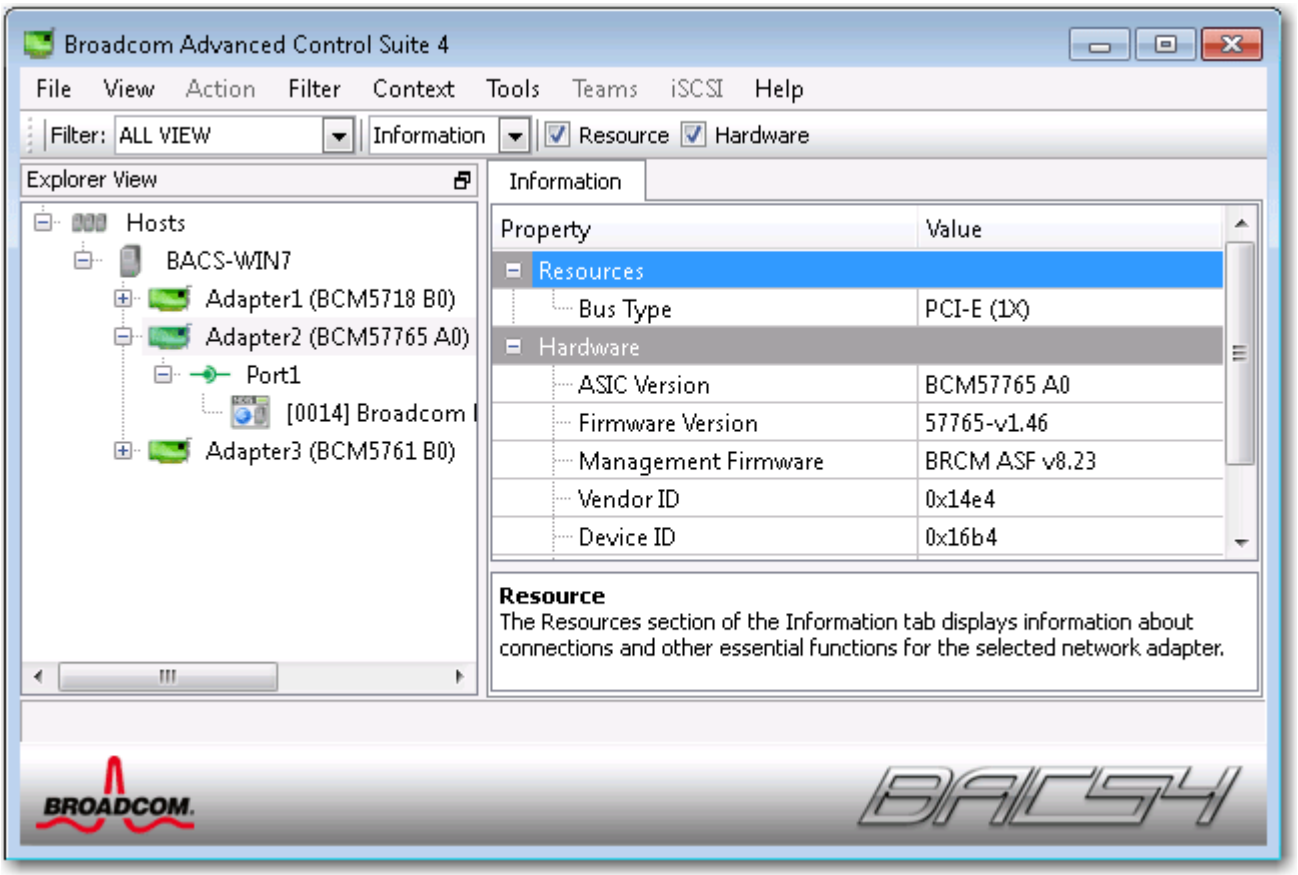
En los sistemas Linux, puede hacer doble clic en el icono de escritorio BACS4 o acceder al programa BACS desde la barra de tareas en **System Tools** (Herramientas del sistema) (Si tiene problemas para iniciar BACS en un sistema Linux, consulte el tema relacionado en Detección y solución de problemas de BACS.)

Interfaz de BACS

La interfaz de BACS está compuesta por las siguientes regiones:

- Panel Explorer View (Ver explorador)
- Selector Context View (Ver contexto)
- Panel Context View (Ver contexto)
- Barra de Menús
- Panel Description (Descripción)

De manera predeterminada, el panel Explorer View está acoplado y sujeto a la izquierda de la ventana principal, el panel Context View se encuentra a la derecha, el selector Context View debajo de la barra de menús y el panel Description debajo del panel Context View. Arrastre el separador entre cualquiera de los paneles para modificarles el tamaño.



Panel Explorer View (Ver explorador)

Puede acoplar y sujetar el panel Explorer View ya sea a la izquierda, a la derecha, arriba o abajo de la ventana principal.

El panel Explorer View enumera los objetos que BACS puede ver, analizar, probar o configurar. Cuando se selecciona un elemento en el panel Explorer View, aparecen las fichas que muestran la información y las opciones disponibles para el elemento en el panel Context View.

La organización de este panel está diseñada para presentar los objetos manejables de la misma manera jerárquica que los controladores y sus subcomponentes. Esto simplifica el manejo de diversos elementos del controlador de interfaz de red convergente. El nivel superior de la jerarquía es el contenedor del host, que enumera todos los hosts administrados por BACS. Debajo de los hosts se encuentran los adaptadores de red instalados, con los elementos manejables, tales como el puerto físico, NDIS e iSCSI debajo de los adaptadores.

El icono junto a cada dispositivo en el panel Explorer View muestra su estado. Un icono junto al nombre de un dispositivo que aparece normal significa que está conectado y que funciona.

- **X.** Una “X” roja que aparece en el icono del dispositivo indica que el dispositivo no está actualmente conectado a la red.
- **Deshabilitado.** El icono de un dispositivo que aparece con color grisáceo indica que el dispositivo está actualmente desactivado.

Selector Ver contexto

El selector Context View aparece debajo de la barra de menús e incluye las categorías de filtro y ficha. Si bien puede expandir y contraer las categorías que aparecen en las fichas en el panel Context View, también puede mostrar una categoría al seleccionar la casilla que está junto al nombre de la categoría.

Filter View (Ver filtro)

En un entorno de múltiples host que utilizan varios C-NIC, puede haber una gran cantidad de elementos manejables por adaptador que pueden resultar difíciles y complicados de ver, configurar y administrar. Utilice el filtro para seleccionar una función en particular del dispositivo. Las posibles vistas de filtros incluyen:

- Todos
- Ver Team (Equipo)
- Ver NDIS
- Ver iSCSI
- Ver destino iSCSI

Panel Context View (Ver contexto)

El panel Context View muestra todos los parámetros que puede ver para el objeto seleccionado en el panel Explorer View. Los parámetros se agrupan por fichas y categorías, según el tipo de parámetro. Las fichas disponibles son Information (Información), Configuration (Configuración), Diagnostics (Diagnóstico) y Statistics (Estadísticas). Debido a que la interfaz de BACS distingue el contexto, solo pueden verse o configurarse en el panel Context View los parámetros que se aplican al objeto seleccionado.

Barra de Menús

Las siguientes opciones aparecen en la barra de menús, pero como los elementos del menú distinguen el contexto, no todos estarán disponibles en todo momento:

Menú File (Archivo)

- Team Save As (Guardar como equipo): guarda las configuraciones de equipo actuales en un archivo
- Team Restore (Restaurar equipo): restaura cualquier configuración guardada desde un archivo

Menú Action (Acción)

- Remove Host (Eliminar host): elimina el host seleccionado.
- Refresh Host (Actualizar host): actualiza el host seleccionado.

Menú View (Ver)

- Explorer View (Ver explorador): muestra/oculta el panel Explorer View (Ver explorador).
- Tool Bar (Barra de herramientas): muestra/oculta la barra de herramientas.
- Status Bar (Barra de estado): muestra/oculta la barra de estado.
- Broadcom Logo (Logo de Broadcom): muestra/oculta el logo de Broadcom en BACS para optimizar el máximo espacio visible.

Menú Tools (Herramientas)

- Options (Opciones): se utiliza para configurar las preferencias de BACS.

Equipos (solo Windows)

- Create Teams (Crear equipos): crea nuevos equipos ya sea con el Asistente para equipos o en el modo Advanced (Avanzado).
- Manage Teams (Administrar equipos): administra equipos existentes ya sea con el Asistente para equipos o en el modo Advanced (Avanzado).

Panel Description (Descripción)

El panel Description proporciona información, instrucciones de configuración y opciones para el parámetro seleccionado en el panel Context View.

Configuración de preferencias en Windows

Para activar o desactivar el icono de la bandeja BACS en Windows

En los sistemas Windows, BACS coloca un icono en la barra de tareas de Windows cuando se instala el programa. Utilice la ventana Opciones para activar o desactivar este icono.

1. Desde el **menú** Tools (Herramientas), seleccione **Options (Opciones)**.
2. Seleccione o borre la opción **Enable BACSTray** (Activar la barra de aplicaciones BACS) (la opción se activa de manera predeterminada).
3. Haga clic en **Aceptar**.

Configuración del modo de equipo en Windows

1. Desde el menú **Tools** (Herramientas), seleccione **Options** (Opciones).
2. Seleccione **Expert Mode** (Modo experto) si no necesita la ayuda del asistente para equipos para crear equipos; de lo contrario, seleccione **Wizard Mode** (Modo asistente).
3. Haga clic en **Aceptar**.

Configuración del tiempo de actualización de Explorer View en Windows

1. Desde el menú **Tools** (Herramientas), seleccione **Options** (Opciones).
2. Seleccione **Auto** (Automático) para establecer el tiempo de actualización de Explorer View en 5 segundos. De lo contrario, seleccione Custom (Personalizado) y seleccione un tiempo, en segundos.
3. Haga clic en **Aceptar**.

Conexión a un host

Puede agregar uno o más hosts de Windows o Linux para administrar desde BACS.

Para agregar un host local

1. Desde el menú **Action** (Acción), haga clic en **Add Host** (Agregar host).
2. Para los hosts de Windows y Linux, no modifique los valores predeterminados. No se requieren el **Nombre de usuario** y **Contraseña** al conectarse al host local.
3. Seleccione **Persist** (Conservar) si desea que BACS guarde la información de este host.
4. Haga clic en **Aceptar**. Ahora se puede utilizar BACS para ver la información y administrar el host.

Para agregar un host remoto

1. Desde el menú **Acción**, haga clic en **Agregar host**.
2. Escriba el nombre del host remoto o la dirección IP en la casilla **Host**.
3. Seleccione el protocolo de la lista **Protocol** (Protocolo). Las opciones de protocolo para Windows son **WMI**, **WinRM** o **Try All**. Las opciones de protocolo para Linux son **CimXML**, **WinRM** o **Try All**. La opción **Try All** obliga al cliente GUI a probar todas las opciones.
4. Seleccione el esquema **HTTP** o el esquema **HTTPS** para mayor seguridad.
5. Escriba el valor de **Port Number** (Número de puerto) que utilizó para configurar el host, si difiere del valor predeterminado de **5985**.
6. Escriba el **Nombre de usuario** y **Contraseña**.
7. Seleccione **Persist** (Conservar) si desea que BACS guarde la información de este host. El host aparece en el panel Explorer (Explorador) cada vez que vuelve a abrir BACS, y no será necesario ingresar la dirección IP o el nombre del host al conectarse al host. Por razones de seguridad, debe ingresar el **Nombre de usuario** y **Contraseña** cada vez.
8. Haga clic en **Aceptar**.

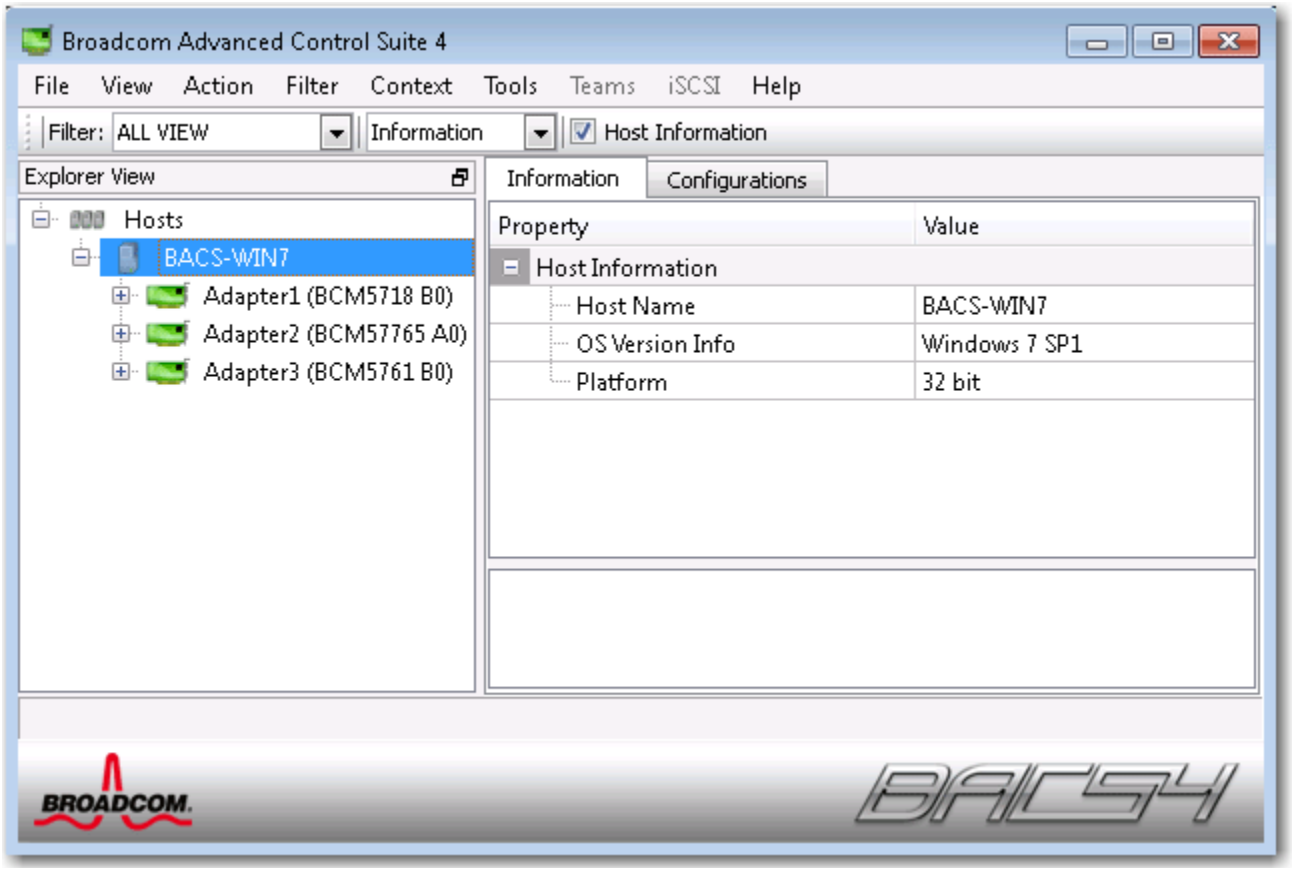
Administración del host

En el nivel del host, puede ver la información del host y configurar parámetros desde las siguientes fichas:

- Información
- Configurar

Para ver la información del host

Seleccione el host en el panel **Explorer View** (Ver explorador) y luego seleccione la ficha **Information** (Información) para ver información a nivel del host.



Ficha Information (Información): Host Information (Información del host)

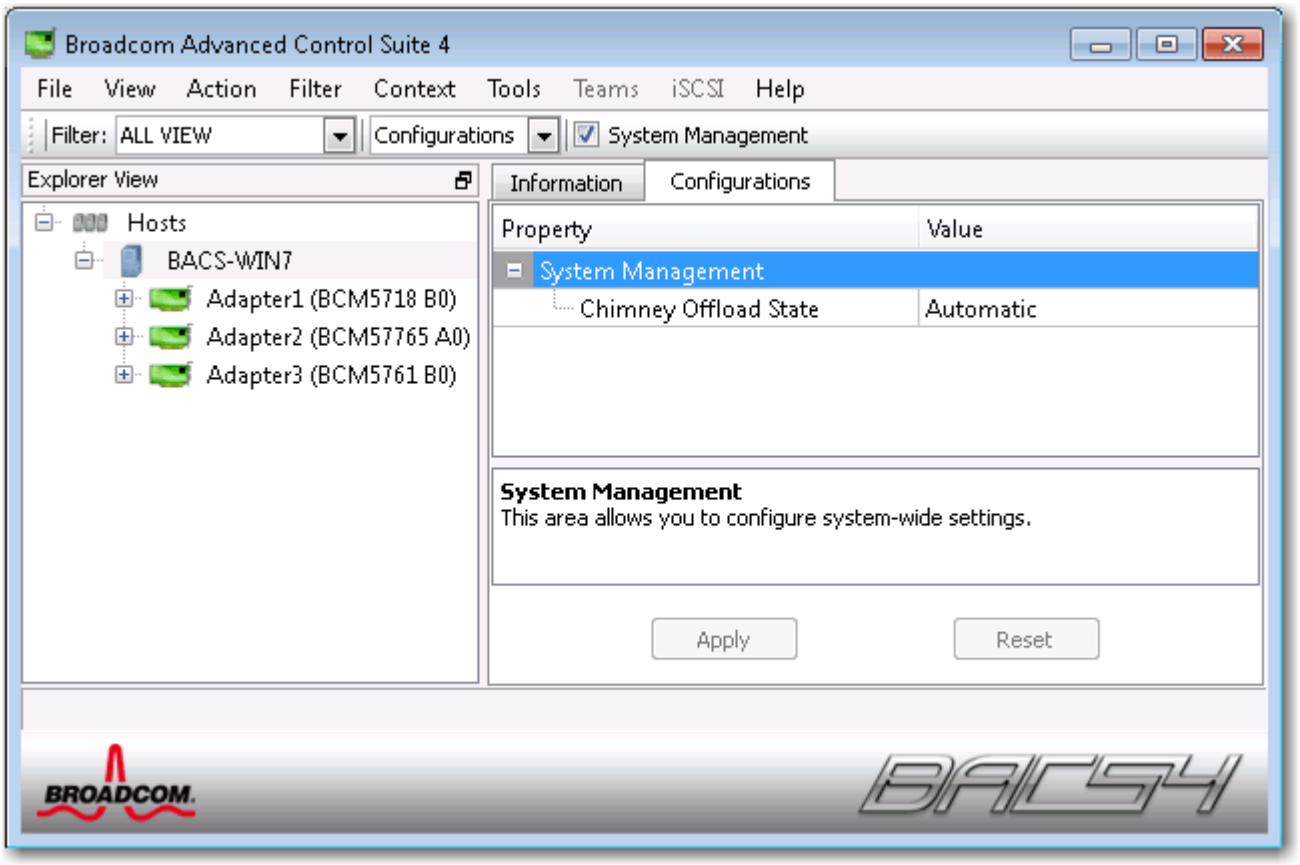
Host Name (Nombre del host). Muestra el nombre del host.

OS Version Info (Información de la versión del SO). Muestra el sistema operativo, incluida la versión.

Platform (Plataforma). Muestra la plataforma de arquitectura del hardware (por ejemplo, 32 bits o 64 bits)

Para configurar el host

Seleccione el host en el panel **Explorer View** (Ver explorador) y luego seleccione la ficha **Configuration** (Configuración) para configurar parámetros a nivel del host.



Administración del adaptador de red

Los adaptadores de red instalados aparecen un nivel abajo del host en el árbol jerárquico en el panel Explorer View. En el nivel del adaptador, puede ver información y configurar parámetros desde las siguientes fichas:

- Información
- Configurar

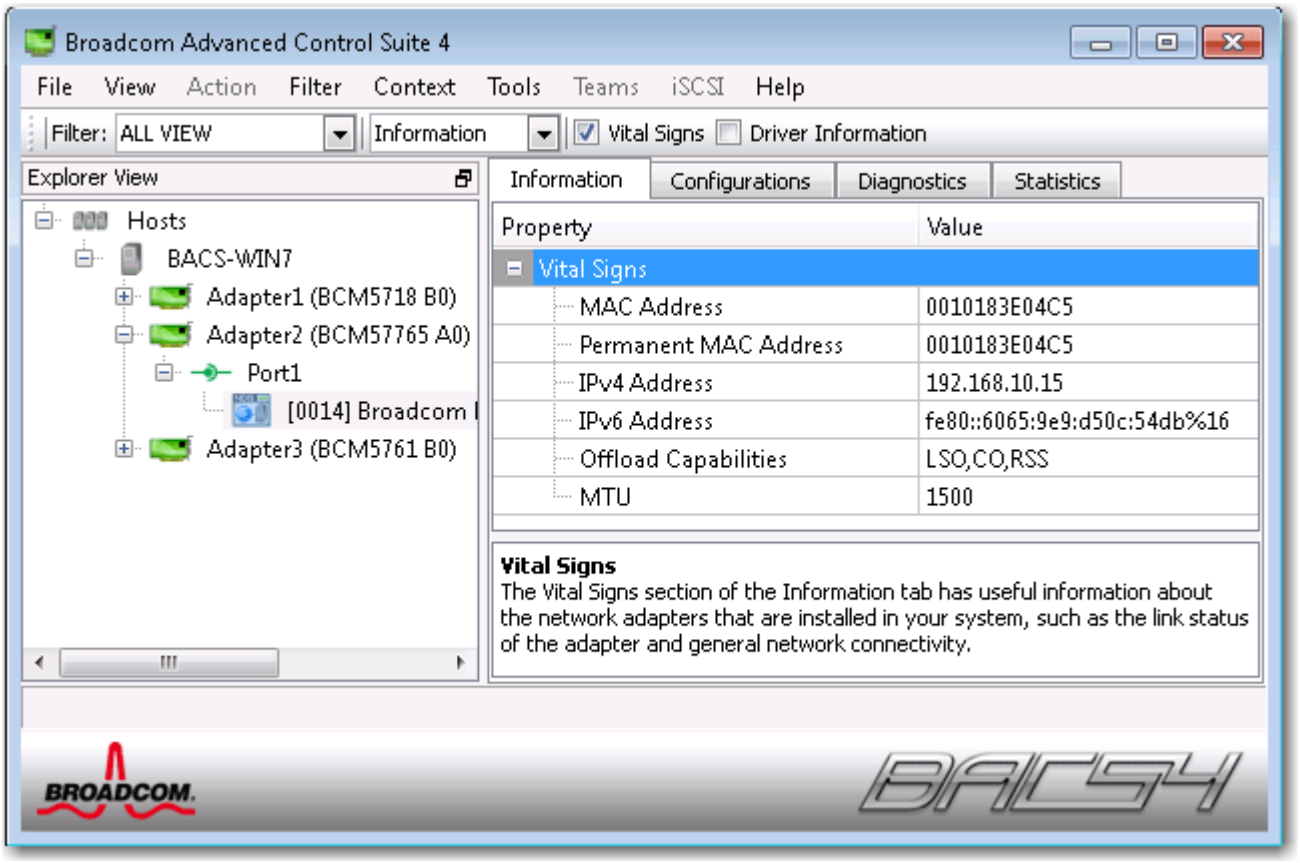
Visualización de información del adaptador

La sección **Vital Signs** (Signos vitales) de la ficha **Information** (Información) tiene información útil sobre los adaptadores de red instalados en su sistema, como el estado de enlace del adaptador y la conectividad de red general.

Seleccione el adaptador de red en el panel **Explorer View** (Ver explorador) y luego seleccione la ficha **Information** (Información) para ver información a nivel del adaptador.

NOTAS:

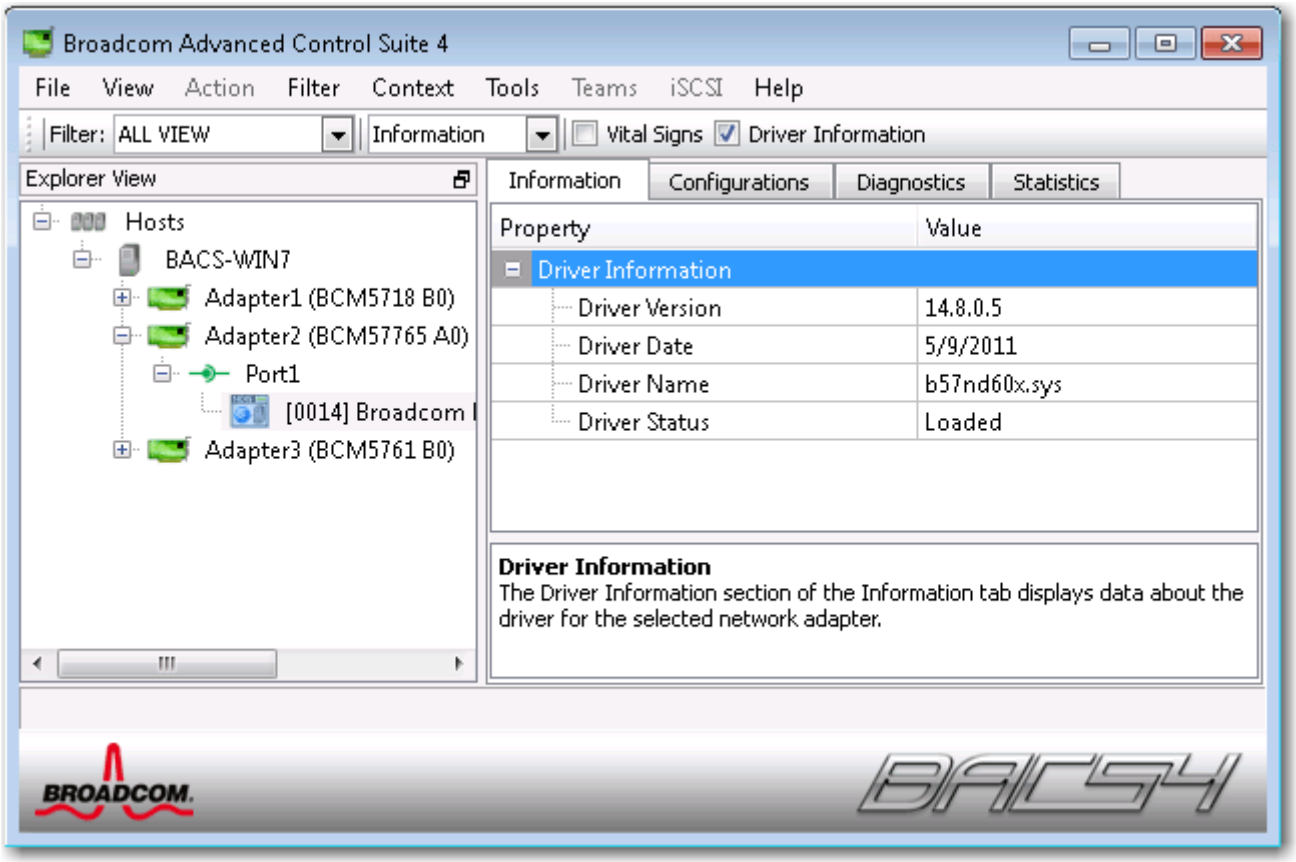
- La información sobre los adaptadores de red Broadcom puede ser más completa que la información sobre los adaptadores de red fabricados por terceros.
- Algunos datos pueden no estar disponibles para todos los adaptadores de red Broadcom.


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

Visualización de la información del controlador

La sección **Driver Information** (Información del controlador) de la ficha **Information** (Información) muestra datos sobre el controlador para el adaptador de red seleccionado.

Para ver la Información del controlador de cualquier adaptador de red instalado, haga clic en el nombre del adaptador enumerado en el panel Explorer View y luego haga clic en la ficha **Information** (Información).



Driver Status (Estado del controlador). El estado del controlador del adaptador.

- **Loaded** (Cargado). Modo de operación normal. Windows ha cargado el controlador del adaptador y está funcionando.
- **Not Loaded** (No cargado) Windows no ha cargado el controlador asociado con el adaptador.
- **Información no disponible**. El valor no se puede obtener del controlador que está asociado con el adaptador.

Driver Name (Nombre del controlador). El nombre de archivo del controlador del adaptador.

Driver Version (Versión del controlador). La versión actual del controlador del adaptador.

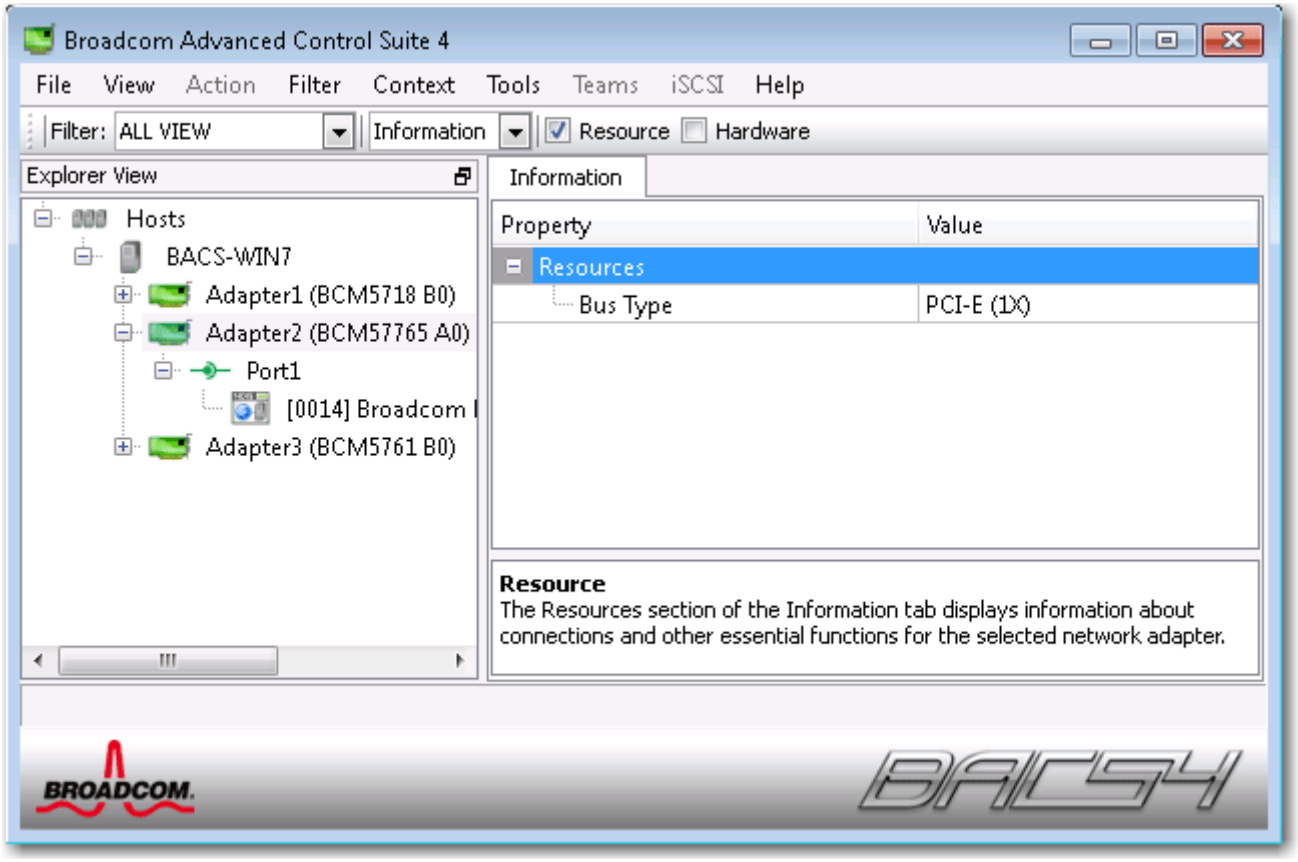
Driver Date (Fecha del controlador). La fecha de creación del controlador del adaptador.

Visualización de la información de recursos

La sección **Resources** (Recursos) de la ficha **Information** (Información) muestra información sobre las conexiones y otras funciones esenciales para el adaptador de red seleccionado.

Para ver Recursos de cualquier adaptador de red instalado, haga clic en el nombre del adaptador enumerado en el panel Explorer View y luego haga clic en la ficha **Information** (Información).

Nota: Algunos datos pueden no estar disponibles para todos los adaptadores de red Broadcom.



Bus Type (tipo de bus). El tipo de interconexión de entrada/salida (E/S) utilizado por el adaptador

Número de ranura. El número de ranura en la placa del sistema que ocupa el adaptador. Este elemento no está disponible para adaptadores del tipo PCI Express.

Velocidad de bus (MHz). La frecuencia de señal del reloj de bus utilizada por el adaptador. Este elemento no está disponible para adaptadores del tipo PCI Express.

Ancho de bus (bit). El número de bits que el bus puede transferir al mismo tiempo desde y hacia el adaptador. Este elemento no está disponible para adaptadores del tipo PCI Express.

Núm. de bus. Indica el número del bus en el que está instalado el adaptador.

Núm. de dispositivo. El número que el sistema operativo asigna al adaptador

Núm. de función. El número de puerto del adaptador. Para un adaptador de un solo puerto, el número de función es 0. Para un adaptador de dos puertos, el número de función para el primer puerto es 0 y el número de función para el segundo puerto es 1.

Solicitud de interrupción. El número de línea de interrupción asociado con el adaptador. Los números válidos están entre 2 y 25.

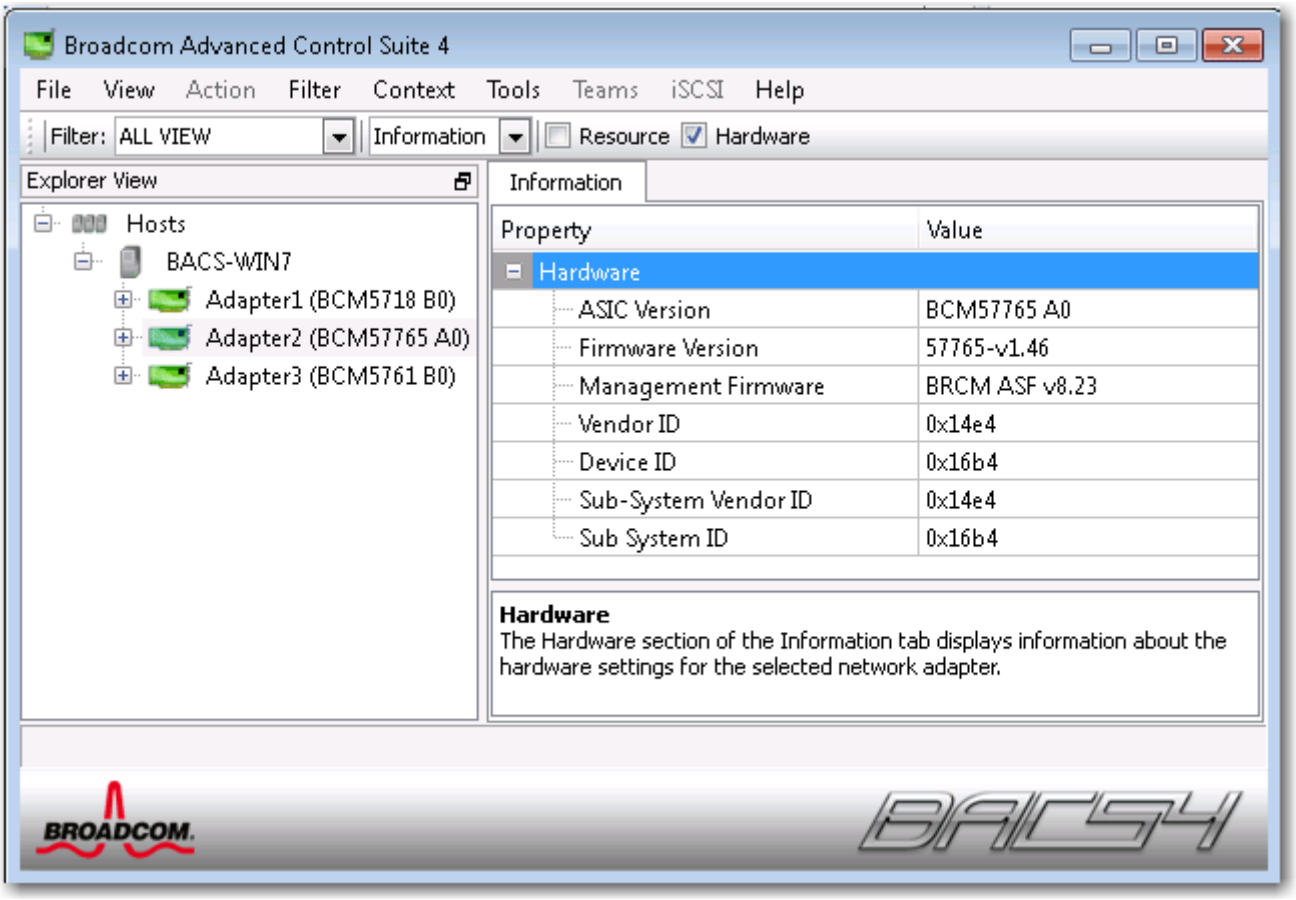
Memory Address (Dirección de memoria). La dirección mapeada de memoria que se asigna al adaptador. Este valor nunca puede ser 0.

Visualización de la información de hardware

La sección Hardware de la **Information tab** (ficha Información) muestra información sobre las configuraciones de hardware para el adaptador de red seleccionado.

Para ver Hardware de cualquier adaptador de red instalado, haga clic en el nombre del adaptador enumerado en el panel Explorer View y luego haga clic en la ficha Information (Información).

Nota: Algunos datos pueden no estar disponibles para todos los adaptadores de red Broadcom.



ASIC Version (Versión ASIC). La versión de chip del adaptador Broadcom (esta información no está disponible para adaptadores fabricados por terceros).

Firmware Version (Versión de firmware). La versión de firmware del adaptador Broadcom (esta información no está disponible para adaptadores fabricados por terceros). Esta información se encuentra disponible únicamente para los adaptadores Broadcom NetXtreme.

Vendor ID (ID del proveedor). La ID del proveedor.

Device ID (ID del dispositivo). La ID del adaptador.

Subsystem Vendor ID. La ID del proveedor del subsistema.

Subsystem ID. La ID del subsistema.

Prueba de red

La opción **Network Test** (Prueba de red) en la ficha **Diagnostics** (Diagnóstico) le permite verificar la conectividad de red IP. Esta prueba verifica si el controlador se ha instalado correctamente y prueba la conectividad a una puerta de enlace o

a otra dirección IP especificada en la misma subred. La prueba de red utiliza TCP/IP para enviar paquetes ICMP a sistemas remotos y luego, espera una respuesta.

Nota: La opción de prueba de red no está disponible en los adaptadores agrupados en un equipo (consulte Configuración de equipos:).

Para ejecutar la prueba de red

1. Haga clic en el nombre del adaptador para probarlo en el panel Explorer View.
2. Desde la lista **Select a test to run** (Seleccione una prueba para ejecutar), seleccione **Network Test** (Prueba de red). Si la opción **Network Test** (Prueba de red) no está disponible, desde la ficha **Context View** (Ver contexto) a la derecha de la ventana, seleccione **Diagnostics** (Diagnóstico) y luego, seleccione **Network Test (Prueba de red)**.
3. Para cambiar la dirección IP de destino, seleccione **IP address to ping** (dirección IP para hacer ping). En la ventana Prueba de red, ingrese una dirección IP de destino y luego, haga clic en **OK** (Aceptar).
4. Haga clic en **Test** (Prueba).

Los resultados de la prueba de red se muestran en el campo **Status** (Estado).

Ejecución de las pruebas de diagnóstico

La opción **Diagnostic Tests** (Pruebas de diagnóstico) en la ficha **Diagnostics** (Diagnóstico) le permite verificar el estado de los componentes físicos de un adaptador de red Broadcom. Puede activar las pruebas manualmente o elegir que BACS 3 las lleve a cabo continuamente. Si las pruebas se llevan a cabo continuamente, el número de correctos e incorrectos en el campo **Result** (Resultado) para cada prueba se incrementa cada vez que se realicen las pruebas. Por ejemplo, si se realiza una prueba cuatro veces y no hay fallas, el valor del campo **Result** (Estado) para esa prueba es 4/0. Sin embargo, si hubo 3 correctas y 1 incorrecta, el valor del campo **Result** (Estado) es 3/1.

NOTAS:

- Debe tener privilegios de administrador para ejecutar las pruebas de diagnóstico.
- La conexión de la red se pierde momentáneamente mientras se ejecutan estas pruebas.
- No todos los adaptadores Broadcom son compatibles con cada prueba.

Para ejecutar las pruebas de diagnóstico una vez

1. Haga clic en el nombre del adaptador para probarlo en el panel Explorer View y seleccione la ficha Diagnostics (Diagnóstico).
2. Desde la lista **Select a test to run** (Seleccione una prueba para ejecutar), seleccione **Diagnostics Test** (Prueba de diagnóstico).
3. Seleccione las pruebas de diagnóstico que desea ejecutar. Haga clic en **Select All** (Seleccionar todo) para seleccionar todas las pruebas o haga clic en **Clear All** (Borrar todo) para borrar todas las selecciones de las pruebas.
4. Seleccione la cantidad de veces que se ejecutarán las pruebas desde **Number of loops** (Cantidad de bucles).
5. Haga clic en **Run test(s)** (Ejecutar prueba(s)).
6. En la ventana de mensaje de error que le advierte que la conexión de red está temporalmente interrumpida, haga clic en **Yes** (Sí). Los resultados se muestran en el campo **Result** (Resultado) para cada prueba.

Registros de control. Esta prueba verifica la capacidad de lectura y escritura de los registros del adaptador de red escribiendo diversos valores en los registros y verificando los resultados. El controlador del adaptador usa estos registros para realizar funciones de red, tales como envío y recibo de información. Una falla de la prueba indica que el adaptador quizás no esté funcionando correctamente.

Registros MII. Esta prueba verifica las capacidades de lectura y escritura de los registros de la capa física (PHY). La capa física se utiliza para controlar las señales eléctricas en el cable y para configurar las velocidades de red, tales como 1000 Mbit/seg.

EEPROM. Esta prueba verifica el contenido de la memoria de sólo lectura programable y borrable eléctricamente (EEPROM) leyendo una porción de la EEPROM y calculando el checksum. La prueba falla si el checksum calculado es diferente del checksum almacenado en el EEPROM. Una ampliación de la copia de EEPROM no requiere un cambio de código para esta prueba.

Memoria interna. Esta prueba verifica que la memoria interna del adaptador esté funcionando correctamente. La prueba escribe valores en patrón en la memoria y vuelve a leer los resultados. La prueba falla si se lee un valor erróneo. El adaptador no puede funcionar si su memoria interna no está funcionando correctamente.

CPU en chip. Esta prueba verifica la operación de las CPUs internas en el adaptador.

Interrumpir. Esta prueba verifica que el controlador Especificación de Interfaz del Controlador de Dispositivos de Red (NDIS) pueda recibir interrupciones desde el adaptador.

LoopBack MAC. Esta prueba verifica que el controlador NDIS puede enviar y recibir paquetes desde el adaptador.

LoopBack PHY. Esta prueba verifica que el controlador NDIS puede enviar y recibir paquetes desde el adaptador.

Prueba de LED. Esta prueba hace que los LED de puerto parpadeen 5 veces con el propósito de identificar el adaptador.

Análisis de cables

La **opción Cable Analysis** (Análisis de cable) en la ficha **Diagnostics** (Diagnóstico), puede monitorear las condiciones de una conexión de cable Ethernet Categoría 5 dentro de una red Ethernet. El análisis mide la calidad del cable y la compara con la especificación IEEE 802.3ab para confirmar su cumplimiento.

NOTAS:

- Debe tener privilegios de administrador para realizar la prueba de análisis de cable.
- La conexión de red se pierde provisoriamente durante un análisis.
- Para los adaptadores Broadcom NetXtreme, la prueba de análisis del cable únicamente puede realizarse para conexiones de velocidad del enlace gigabit y cuando la conexión no está disponible.
- Esta opción no está disponible para todos los adaptadores de red Broadcom.

Para ejecutar una prueba de Análisis de cable

1. Conecte el cable a un puerto de un conmutador en el que el puerto esté definido como **Auto** y los parámetros Speed & Duplex (Velocidad y Dúplex) también estén configurados como **Auto**.
2. Haga clic en el nombre del adaptador para probarlo en el panel Explorer View.
3. Desde la lista **Select a test to run** (Seleccione una prueba para ejecutar), seleccione **Cable Analysis** (Análisis de cable). Si la opción **Cable Analysis** (Análisis de cable) no está disponible, desde la ficha **Context View** (Ver contexto) a la derecha de la ventana, seleccione **Diagnostics** (Diagnóstico) y luego, seleccione **Cable Analysis** (Análisis de cable).
4. Haga clic en **Run** (Ejecutar).
5. En la ventana de mensaje de error que le advierte que la conexión de red está temporalmente interrumpida, haga clic en **Yes** (Sí).

Distancia. La distancia válida de cable en metros (excepto cuando aparece el resultado del Noise (Ruido)).

Estado. Ésto muestra el tipo de enlace en este par de cables.

- **Good** (Bueno). Buena ruta de cable/señal PCB, pero sin enlace gigabit.
- **Crossed** (Cruzado). Cortocircuito o interferencia del pin en dos o más rutas de señal de cable/PCB.
- **Open** (Abierto). Uno o ambos pins se encuentran abiertos para un par trenzado.
- **Short** (Corto). Dos pins del mismo par trenzado se encuentran cortocircuitados.
- **Noise** (Ruido). Presencia de ruido persistente (probablemente provocado por 10/100 obligatorio).
- **GB Link** (Enlace GB). El enlace Gigabit está activo y funcionando.
- **N/A**. El algoritmo no pudo llegar a una conclusión.

Enlace. La velocidad de conexión de enlace y el modo dúplex.

Estado. El estado después de la ejecución de la prueba es completado o falló.

Hay varios factores que podrían afectar los resultados de la prueba:

- **Link partner** (Socio de enlace). Diversos fabricantes de conmutadores y concentradores implementan diferentes PHY. Algunos PHY no cumplen con la norma IEEE.
- **Cable quality** (Calidad del cable). Las categorías 3, 4, 5 y 6 podrían afectar los resultados de la prueba.
- **Electrical interference** (Interferencia eléctrica). El entorno de prueba puede afectar los resultados de la prueba.

Configuración de las propiedades del adaptador

Advanced (Avanzado) en la ficha **Configurations** (Configuraciones) le permite ver y cambiar los valores de las propiedades disponibles del adaptador seleccionado. A continuación se describen las propiedades potencialmente disponibles y sus configuraciones respectivas.

NOTAS:

- Debe tener privilegios de administrador para cambiar los valores de una propiedad.
- La lista de propiedades disponibles para su adaptador en particular puede ser diferente.
- Algunas propiedades pueden no estar disponibles para todos los adaptadores de red Broadcom.

Para fijar las propiedades del adaptador

1. Haga clic en el nombre del adaptador en el panel Explorer View y haga clic en la ficha **Configurations** (Configuraciones).
2. Desde la sección **OOB Management** (Administración OOB), seleccione la propiedad que desea establecer.
3. Para cambiar el valor de una propiedad, seleccione un elemento de la lista de propiedad o escriba un valor nuevo, según corresponda (las opciones de selección son distintas para las diferentes propiedades).
4. Haga clic en **Apply** (Aplicar) para confirmar los cambios realizados a todas las propiedades. Haga clic en **Reset** (Reestablecer) para devolver las propiedades a sus valores originales.

802.1p QoS (Compatibilidad con 802.1p). Activa la *calidad de servicio*, que es una especificación del *Institute of Electrical and Electronics Engineering* (IEEE) que considera los distintos tipos de tráfico de red en forma diferente para asegurar los niveles requeridos de confiabilidad y latencia según el tipo de tráfico. Esta propiedad está deshabilitada de manera predeterminada. Salvo que la infraestructura de la red soporte QoS, no habilite QoS. De lo contrario, se pueden producir problemas.

Control de flujo. Habilita o deshabilita el recibo o la transmisión de las tramas de PAUSA. Las tramas de PAUSA habilitan al adaptador de red y a la central para que controlen la velocidad de transmisión. El lado que está recibiendo la trama de PAUSA detiene momentáneamente la transmisión.

- **Auto** (valor predeterminado). Optimiza el recibo y transmisión de tramas de PAUSA.
- **Disable** (Deshabilitar). El recibo y la transmisión de tramas de PAUSA quedan deshabilitados.
- **Rx PAUSE** (Pausa de Rx). El recibo de tramas de PAUSA está habilitado.
- **Rx/Tx PAUSE** (Pausa de Rx/Tx). El recibo y la transmisión de tramas de PAUSA está habilitado.
- **Tx PAUSE** (Pausa de Tx). Habilita la transmisión de tramas de PAUSA.

Speed & Duplex (Velocidad y Dúplex). La propiedad Speed & Duplex (Velocidad y Dúplex) configura la velocidad de conexión y el modo con los de dicha red. Observe que el modo Full-Duplex (Dúplex completa) permite que el adaptador transmita y reciba datos de red simultáneamente.

- **10 Mb Full** (10 Mb completo). Configura la velocidad en 10 Mbit/s y el modo en Full-Duplex

- **10 Mb Half** (10 Mb medio). Configura la velocidad en 10 Mbit/s y el modo en Half-Duplex.
- **100 Mb Full** (100 Mb completo). Configura la velocidad en 100 Mbit/s y el modo en Full-Duplex.
- **100 Mb Half** (100 Mb medio). Configura la velocidad en 100 Mbit/s y el modo en Half-Duplex
- **Auto** (valor predeterminado). Configura la velocidad y el modo para una óptima conexión de red (recomendada).

NOTAS:

- Auto es la configuración recomendada. Esta configuración permite que el adaptador de red detecte en forma dinámica la velocidad de línea de la red. Cada vez que cambia la capacidad de la red, el adaptador de red la detecta automáticamente y se ajusta a la nueva velocidad de línea y modo dúplex. Se puede habilitar una velocidad de 1 Gbps al seleccionar Auto, siempre y cuando se apoye esa velocidad.
- 1 Gb Full Auto debe conectarse a un socio de enlace que también admita una conexión de 1 Gb. Como la conexión está limitada sólo a una conexión de 1 Gb, la función Ethernet@Wirespeed estará deshabilitada. Si el socio de enlace sólo admite una conexión de 1 Gb es posible que no pueda utilizar la función Wake on LAN. Además, ante la ausencia de un sistema operativo, la administración del tráfico también puede verse afectada.
- Las configuraciones de 10 Mb Half y 100 Mb Half obligan al adaptador de red a conectarse a la red en modo Half-Duplex. Tenga en cuenta que quizás no funcione el adaptador de red si la red no está configurada para funcionar en el mismo modo.
- Las configuraciones de 10 Mb Full y 100 Mb Full obligan al adaptador de red a conectarse a la red en modo Full-Duplex. Quizás no funcione el adaptador de red si la red no está configurada para funcionar en el mismo modo.

Wake Up Capabilities (Capacidades de reactivación). Habilita al adaptador de red a activarse después de un modo de baja energía cuando recibe una trama de reactivación de la red. Hay dos tipos de tramas de activación posibles: Magic Packet y Wake Up Frame (Trama de reactivación).

Esta propiedad se encuentra disponible únicamente para los adaptadores Broadcom NetXtreme.

- **Ambas** (valor predeterminado). Selecciona Magic Packet (Paquete mágico) y Wake Up Frame (Trama de reactivación) como las tramas de activación.
- **Magic Packet** (Paquete mágico). Selecciona Magic Packet (Paquete mágico) como la trama de activación.
- **None** (Ninguna). No selecciona ninguna trama de reactivación.
- **Wake Up Frame** (Trama de reactivación). Selecciona Wake Up Frame como trama de reactivación y permite que el adaptador de red active el sistema operativo cuando se recibe un evento del tipo ping o una solicitud del Protocolo de Resolución de Direcciones (ARP). Esta opción funciona junto con el modo de ahorro de energía del sistema operativo y no funciona si la configuración Ahorro de energía no habilita WOL.

Priority & VLAN (Prioridad y VLAN). Permite habilitar tanto la prioridad de tráfico de red como el etiquetado de VLAN. El etiquetado de VLAN sólo ocurre cuando la configuración de ID de VLAN tiene un valor diferente de 0 (cero).

- **Priority & VLAN Enabled (default)** (Prioridad y VLAN habilitadas, predeterminado). Permite dar prioridad a los paquetes y el etiquetado de VLAN.
- **Priority & VLAN Disabled** (Prioridad y VLAN deshabilitadas). Impide dar prioridad a los paquetes y el etiquetado de VLAN.
- **Priority Enabled** (Prioridad habilitada). Sólo permite dar prioridad a los paquetes.
- **VLAN Enabled** (VLAN habilitada). Sólo permite el etiquetado de VLAN.

Nota: Si un controlador intermedio maneja el adaptador de red para el etiquetado de VLAN, no se deben utilizar las configuraciones **Priority & VLAN Disabled** y **Priority Enabled**. Utilice las configuraciones **Priority & VLAN Enabled** y cambie la **ID de VLAN** a 0 (cero).

ID de red VLAN. Permite el etiquetado de VLAN y configura la ID de VLAN ID cuando se selecciona **Priority & VLAN Enabled** como la configuración de **Prioridad y VLAN**. El rango de la ID de VLAN es de 1 a 4094 y debe coincidir con el

valor de la etiqueta VLAN en el conmutador conectado. Un valor de 0 (predeterminado) en este campo deshabilita el etiquetado de VLAN.

Evaluación del riesgo del etiquetado de VLAN a través del controlador de minipuerto NDIS

El controlador de minipuerto NDIS 6.0 de Broadcom ofrece los medios para permitir que un sistema que contiene un adaptador Broadcom pueda conectarse a una VLAN con etiqueta. Sin embargo, a diferencia de BASP el soporte del controlador NDIS 6 para la participación de VLAN sólo es para una única ID de VLAN.

Asimismo, a diferencia de BASP, el controlador NDIS 6.0 sólo ofrece etiquetado de VLAN del paquete saliente, pero no ofrece filtrado de los paquetes entrantes según la pertenencia a la ID de VLAN. Este es el comportamiento predeterminado de todos los controladores de minipuerto. Si bien la falta de paquetes de filtrado basados en pertenencia a VLAN puede presentar un problema de seguridad, a continuación se ofrece una evaluación del riesgo según la limitación de este controlador para una red IPv4:

Una red bien configurada que posee VLAN múltiples deben mantener segmentos IP individuales para cada VLAN. Esto es necesario, ya que el tráfico saliente depende de la tabla de enrutamiento para identificar a través de que adaptador (virtual o físico) transmitirá tráfico y no determina el adaptador según la pertenencia a VLAN.

Debido a que el soporte para etiquetado de VLAN en el controlador NDIS 6.0 de Broadcom se limita solamente al tráfico de transmisión (Tx), existe el riesgo de que pase tráfico entrante (Rx) de una VLAN diferente al sistema operativo. No obstante, teniendo en cuenta la premisa de una red bien configurada mencionada anteriormente, la segmentación IP y/o la configuración VLAN del conmutador pueden ofrecer filtrado adicional para limitar este riesgo.

En una situación de conexión fondo contra fondo, dos computadoras en el mismo segmento IP pueden comunicarse independientemente de su configuración de VLAN, ya que no hay filtrado de pertenencia a VLAN. No obstante, esta situación supone una posible violación de la seguridad, ya que este tipo de conexión no es típico en un entorno de VLAN.

Si no se quiere correr el riesgo anterior y se requiere el filtrado de pertenencia a VLAN, sería necesario contar con soporte a través de un controlador intermedio.

Visualización de estadísticas

La información proporcionada en la ficha Estadística le permite ver las estadísticas de tráfico de los adaptadores de red Broadcom y los adaptadores de red fabricados por terceros. La información estadística y cobertura son más amplias para los adaptadores Broadcom.

Para ver la información de Estadística de cualquier adaptador de red instalado, haga clic en el nombre del adaptador enumerado en el panel Explorer View y luego haga clic en la ficha Statistics (Estadística).

Haga clic en **Refresh** (Actualizar) para obtener los valores más recientes para cada estadística. Haga clic en **Reset** (Reestablecer) para cambiar todos los valores a cero.

NOTAS:

- No se exhiben las estadísticas del equipo para un adaptador de red Broadcom si está inhabilitado.
- Algunas estadísticas pueden no estar disponibles para todos los adaptadores de red Broadcom.

Estadísticas generales

Estadísticas generales muestra las estadísticas transmitidas y recibidas hacia y desde el adaptador.

Frames Tx OK (Tramas Tx correctamente). Un conteo de las tramas que se transmitieron correctamente. El contador aumenta cuando el estado de transmisión se indica como correcto (Transmit OK).

Tramas Rx OK. Un conteo de las tramas que se recibieron correctamente. Esto no incluye tramas recibidas con errores de trama demasiado larga, de secuencia de verificación de trama (FCS), de longitud o alineación, o tramas perdidas debido a errores internos de la subcapa de MAC. El contador aumenta cuando el estado de recepción se indica como correcto (Receive OK).

Tramas dirigidas Tx. Un conteo de tramas de datos dirigidas que se transmitieron correctamente.

Tramas multidifusión Tx. Un conteo de tramas que se transmitieron correctamente (según lo indica el valor de estado de transmisión correcta [Transmit OK]) a una dirección de destino de grupo que no es la dirección de difusión.

Multicast Frames Tx (Tramas Tx difusión). Un conteo de tramas transmitidas correctamente (según lo indica el estado de transmisión correcta (Transmit OK)) a la dirección de difusión (broadcast address). Las tramas transmitidas a las direcciones multidifusión no son tramas de difusión y por lo tanto se excluyen.

Tramas dirigidas Rx. Un conteo de tramas de datos dirigidas que se recibieron correctamente.

Tramas multidifusión Rx. Un conteo de tramas recibidas correctamente, que se dirigen a una dirección activa de grupo que no es de difusión. Esto no incluye tramas recibidas con errores de trama demasiado larga, FCS, de longitud o alineación, o tramas perdidas a raíz de errores internos de la subcapa MAC. El contador aumenta según lo indicado por el estado de recepción correcta (Receive OK).

Tramas de amplia difusión Rx. Un conteo de tramas recibidas correctamente, que se dirigen a una dirección de grupo de difusión. Esto no incluye tramas recibidas con errores de trama demasiado larga, FCS, de longitud o alineación, o tramas perdidas a raíz de errores internos de la subcapa MAC. El contador aumenta según lo indicado por el estado de recepción correcta (Receive OK).

Tramas Rx con error de CRC. El número de tramas recibidas con errores de CRC.

Configuración de equipos:

La función de equipo le permite agrupar cualquier adaptador de red disponible para funcionar como un equipo. La configuración de equipos es un método de creación de una NIC virtual (un grupo de múltiples adaptadores que funciona como un solo adaptador). El beneficio de este enfoque es que permite el balanceo de la carga y tolerancia a fallas. Los equipos se configuran a través del software Broadcom Advanced Server Program. Para una descripción integral de los aspectos tecnológicos y de implementación del software de equipos, consulte la sección "Servicios de equipos Broadcom Gigabit Ethernet" de la Guía del usuario de su adaptador de red Broadcom.

Los equipos pueden formarse mediante cualquiera de los siguientes métodos:

- Uso del Asistente para equipos de Broadcom
- Uso del Expert Mode (Modo experto)

NOTAS:

- Para obtener más información sobre los protocolos de equipos, consulte la sección "Equipos" de la Guía del usuario de su adaptador Broadcom.
- Si no habilita LiveLink™ al configurar los equipos, se recomienda deshabilitar el protocolo STP (Protocolo de árbol de tramos) en el conmutador. De esta manera se minimiza el tiempo de inactividad que genera la determinación del bucle del árbol de tramos en casos de tolerancia a fallas. LiveLink mitiga estos problemas.
- BASP está disponible solamente si un sistema tiene uno o más adaptadores de red Broadcom instalados.
- Las propiedades Large Send Offload (LSO) y Checksum Offload se habilitan para un equipo únicamente cuando todos los miembros soportan y están configurados para esa función.
- Debe tener privilegios de administrador para crear o modificar un equipo.
- El algoritmo de balance de carga en un entorno de equipo en el que los miembros se conectan a distintas velocidades favorece a los miembros conectados con un enlace Gigabit Ethernet respecto de aquellos conectados con enlaces de velocidades inferiores (100 Mbps o 10 Mbps) hasta que se alcanza el umbral. Este comportamiento es normal.
- Wake on LAN (WOL) es una función que permite activar un sistema que se encontraba inactivo mediante la llegada de un paquete específico a través de la interfaz Ethernet. Dado que se implementa un adaptador virtual como dispositivo exclusivo de software, carece de características de hardware para implementar WOL y no puede habilitarse para activar el sistema a través del adaptador virtual. Sin embargo, el adaptador físico soporta esta propiedad incluso cuando forma parte de un equipo.

Tipos de equipos

Puede crear cuatro tipos de equipos de balance de carga:

- Balance de carga inteligente y tolerancia a fallas.
- Agregación de enlaces (802.3ad)
- Troncalización genérica (Generic Trunking) (FEC/GEC)/802.3ad-Draft Static.
- SLB (Autoreserva deshabilitada): la característica Autoreserva deshabilitada se configura para los equipos de balance de carga inteligente y tolerancia a fallas en el Asistente para equipos.

Para obtener una descripción de estos tipos, consulte "Balanceo de carga y tolerancia a fallas" en la Guía de usuario *Broadcom® NetXtreme® BCM57XX*.

Uso del Asistente para equipos de Broadcom

Puede utilizar el Asistente para equipos de Broadcom para crear un equipo, configurar un equipo existente si ya se ha creado un equipo o crear una VLAN.

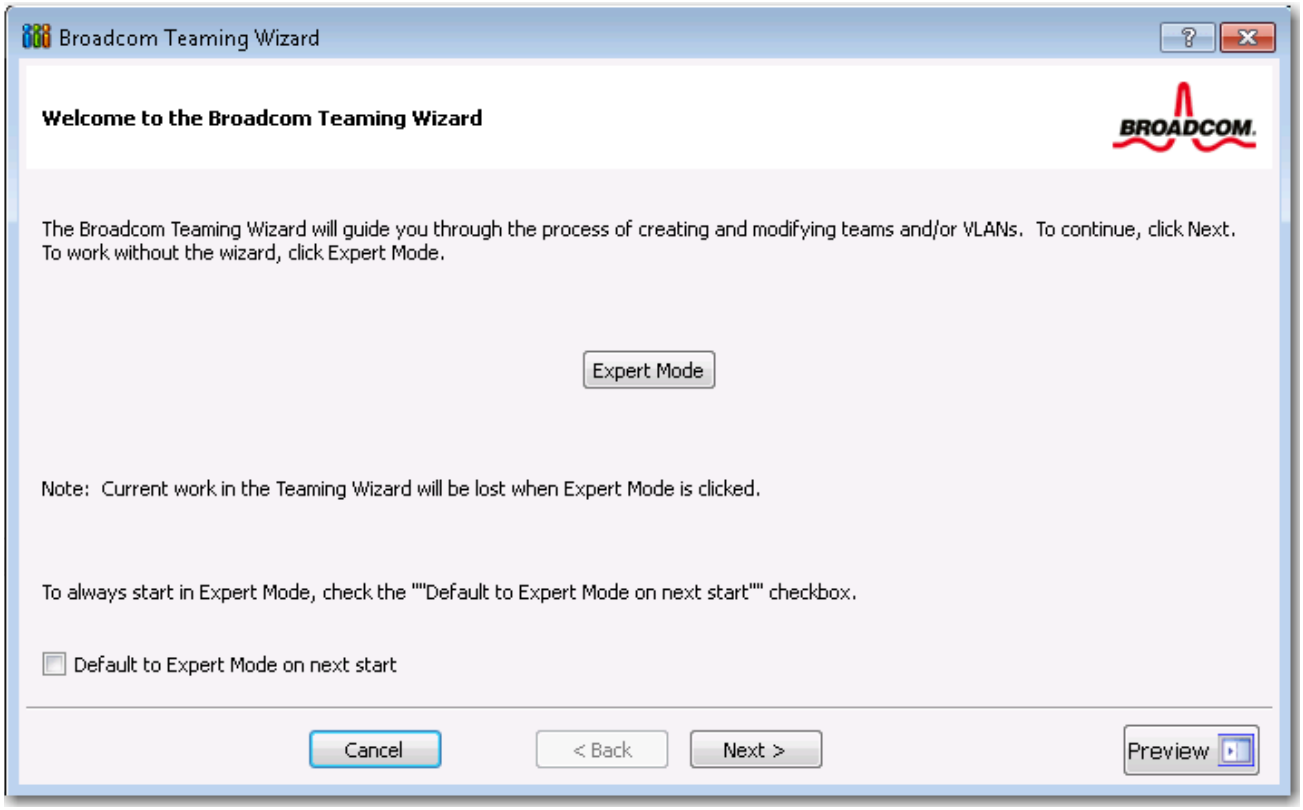
1. Crear o editar un equipo:

   Para crear un equipo nuevo, seleccione **Create a Team** (Crear un equipo) del menú **Team** (Equipo) o haga clic con el botón derecho sobre uno de los dispositivos de la sección "Adaptadores no asignados" y seleccione **Create a Team** (Crear un equipo). Esta opción no se encuentra disponible si no hay dispositivos enumerados en las secciones "Adaptadores no asignados", lo que significa que todos los adaptadores han sido asignados a equipos.

   Para configurar un equipo existente, haga clic con el botón derecho sobre uno de los equipos y seleccione **Edit Team** (Editar equipo). Esta opción se encuentra únicamente disponible si ya se ha creado un equipo y éste se encuentra en el panel Administración de equipos.

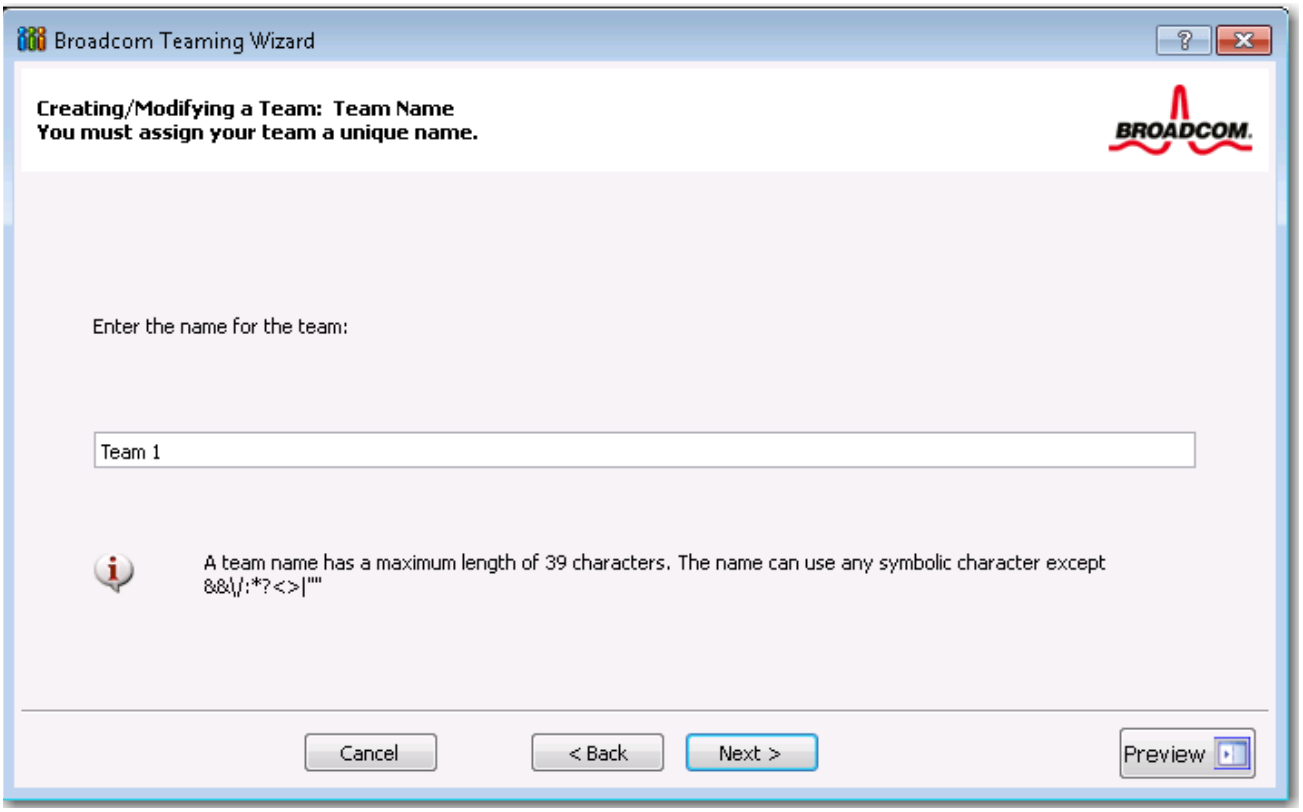
Nota: Si prefiere trabajar sin el asistente, haga clic en **Expert Mode** (Modo experto). Si desea utilizar siempre el Modo experto para crear un equipo, seleccione **Default to Expert Mode on next start** (Emplear el Modo experto predeterminado en el próximo inicio). Consulte Uso del Expert Mode (Modo experto).

2. Para continuar usando el asistente, haga clic en **Next** (Siguiente).

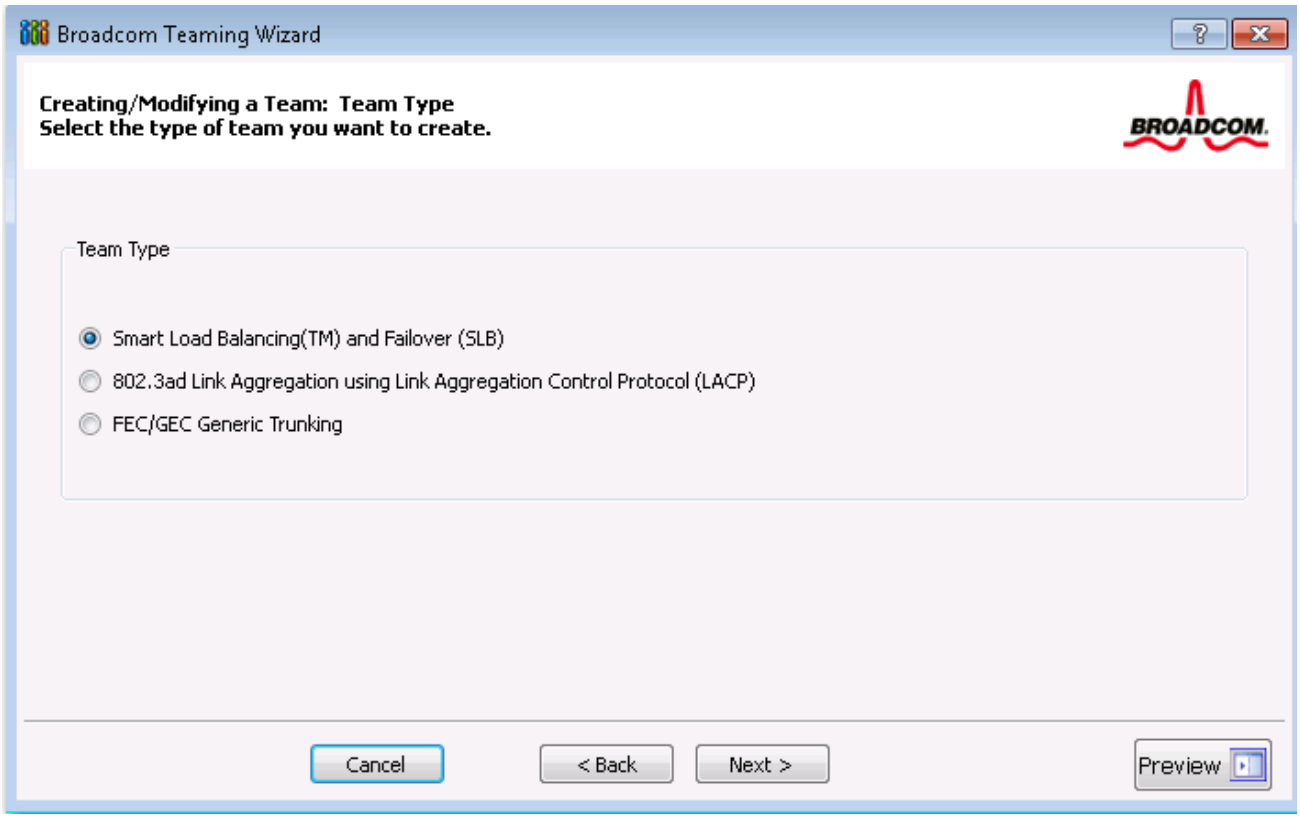


3. Escriba el nombre del equipo y luego haga clic en **Next (Siguiente)**. Si desea revisar o cambiar cualquiera de sus configuraciones, haga clic en **Back** (Atrás). Haga clic en **Cancel** (Cancelar) para descartar sus configuraciones y salir del asistente.

Nota: El nombre del equipo no puede exceder 39 caracteres, no puede comenzar con espacios y no puede contener ninguno de los siguientes caracteres: & \ / : * ? < > |



4. Seleccione el tipo de equipo que desea crear. Si el tipo de equipo es un equipo de tipo SLB, haga clic en **Next** (Siguiente). Si el tipo de equipo no es un equipo de tipo SLB, se abre un cuadro de diálogo. Verifique que el conmutador de red conectado a los miembros del equipo esté configurado correctamente para el tipo de equipo, haga clic en **OK** (Aceptar) para continuar.

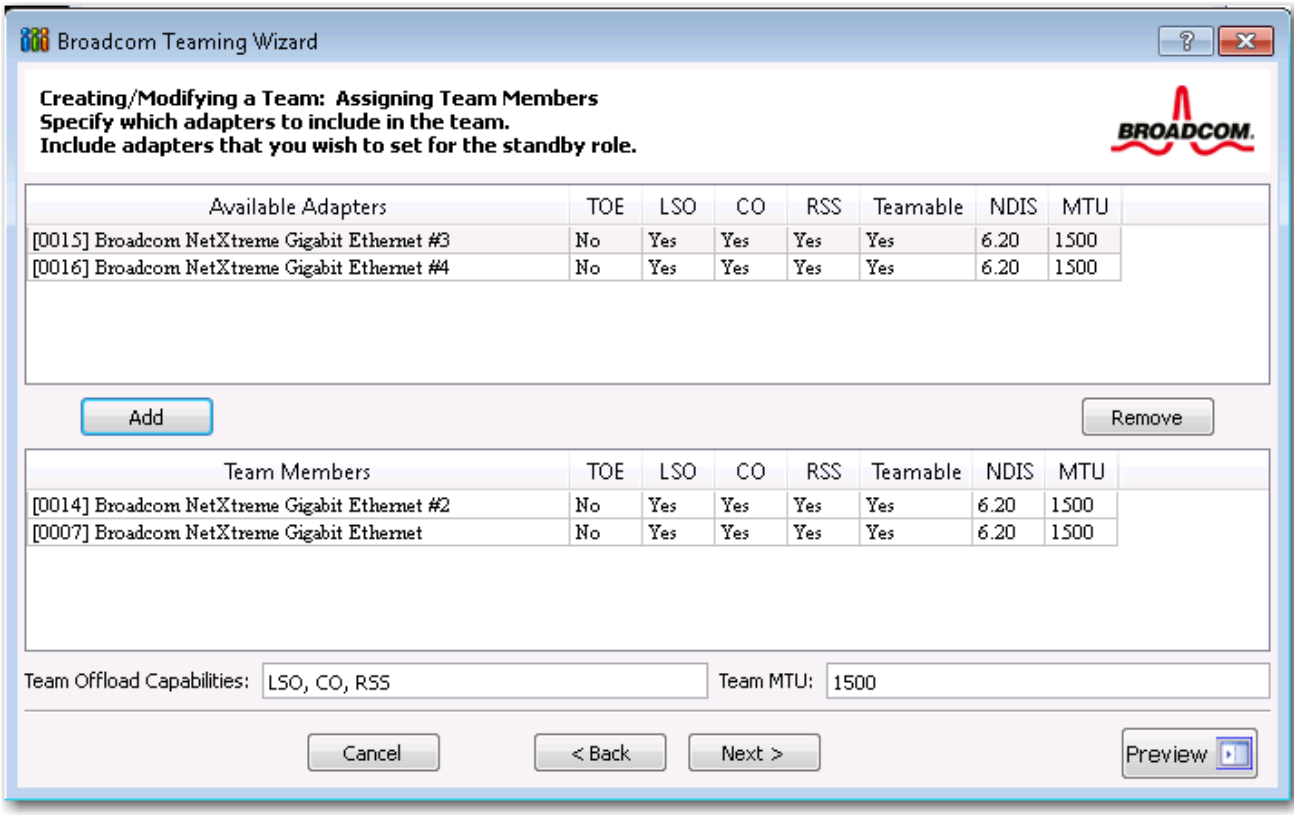


5. Desde la lista **Available Adapters (Adaptadores disponibles)** haga clic en el adaptador que desea agregar al equipo y luego haga clic en **Add (Agregar)**. Elimine miembros del equipo desde la lista **Team Members (Miembros del equipo)** haciendo clic en el adaptador y luego en **Remove (Eliminar).** Haga clic en **Siguiente.**

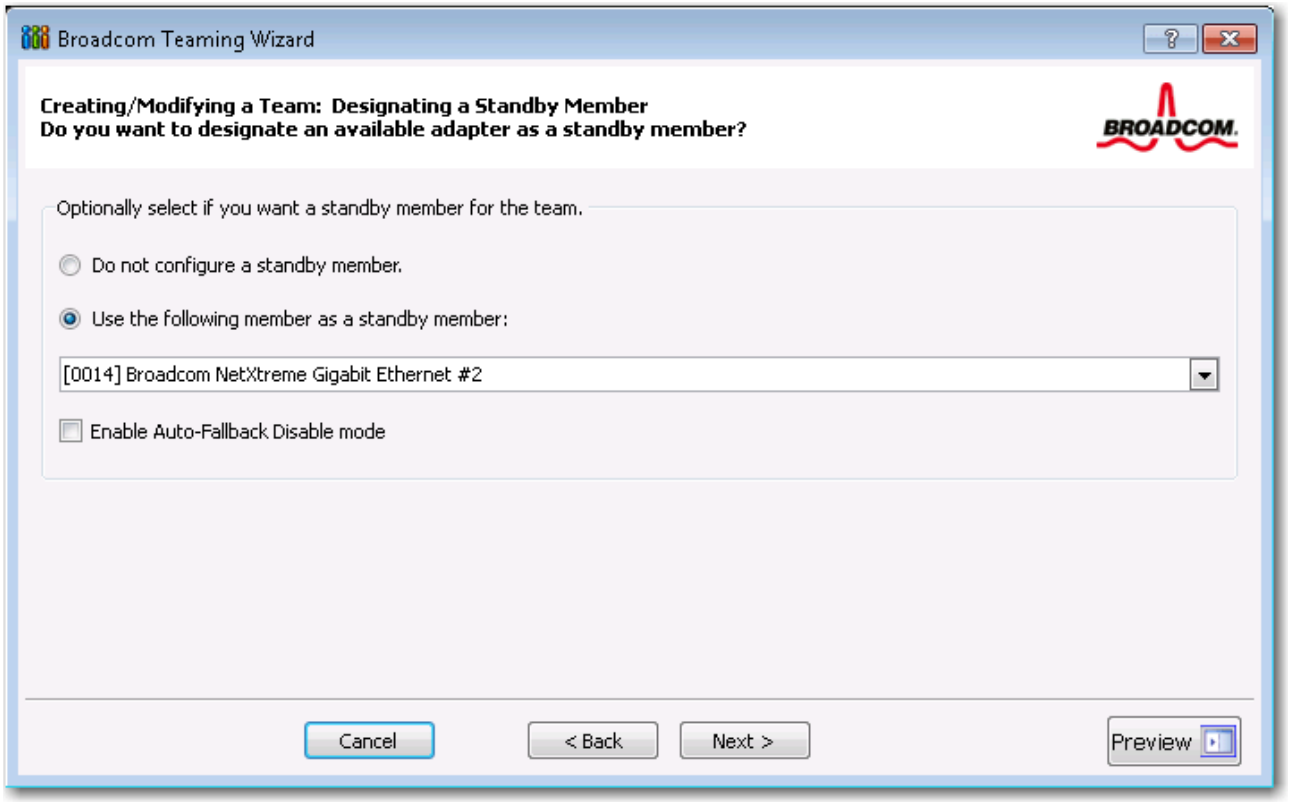
Nota: Debe haber, por lo menos, un adaptador de red Broadcom asignado al equipo.

Las columnas Large Send Offload (LSO) y Checksum Offload (CO) indican si las propiedades LSO y/o CO cuentan con soporte para el adaptador. Las propiedades LSO, y CO están habilitadas para un equipo solo cuando todos los miembros cuentan con soporte y están configurados para la función. Si este es el caso, entonces las capacidades de descarga del equipo aparecen en la parte inferior de la pantalla.

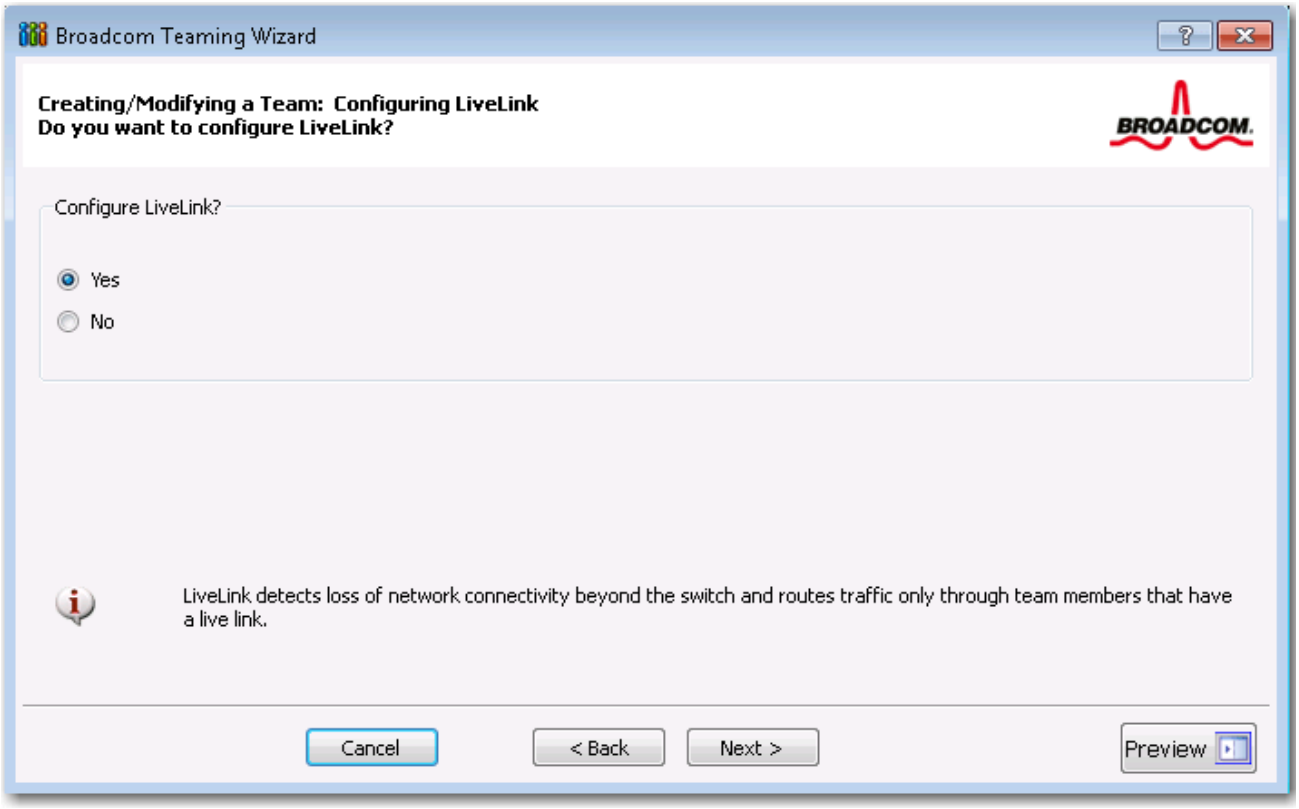
Nota: Agregar un adaptador de red a un equipo que tiene el controlador deshabilitado podría afectar negativamente las capacidades de descarga del equipo. Esto podría afectar el rendimiento del equipo. Por lo tanto, se recomienda agregar adaptadores de red con controladores habilitados como miembro de un equipo.



6. Si desea designar uno de los adaptadores como un miembro en espera (opcional), seleccione **Use the following member as a standby member** (Usar el siguiente miembro como miembro en espera) y luego elija el miembro en espera de la lista de adaptadores.
7. La función del modo Autoreserva deshabilitada permite al equipo seguir usando el miembro en espera en lugar de volver al miembro primario si el miembro primario vuelve a la línea. Para habilitar esta característica, seleccione **Enable Auto-Fallback Disable mode** (Activar el modo Autoreserva deshabilitada). Haga clic en **Siguiente.**



8. Si desea configurar LiveLink, seleccione **Yes** (Sí). De lo contrario, seleccione **No** (No) y luego haga clic en **Next** (Siguiente).



9. Seleccione el intervalo de la sonda (la cantidad de segundos entre cada retransmisión de un paquete de enlace al destino de la sonda) y la cantidad máxima de reintentos de la sonda (la cantidad de respuestas consecutivas perdidas de un destino de la sonda antes de que se active la tolerancia a fallas).

10. Configure la ID de sonda VLAN para permitir la conectividad con los destinos de sonda que residen en una red VLAN con etiquetas. El número especificado debe coincidir con la ID de la red VLAN de los destinos de la sonda así como los puertos del conmutador al cual se encuentra conectado el equipo.

Nota: Los equipos con habilitación para LiveLink sólo pueden comunicarse con destinos de sonda a través un una única red VLAN. Además, VLAN ID 0 equivale a una red sin etiquetas. Si Comprobar ID de VLAN se establece en un valor que no sea 0, entonces debe crearse una VLAN con un valor de etiqueta VLAN idéntico (consulte Paso 16.).

11. Haga clic en el destino de la sonda en la parte superior de la lista, haga clic en **Edit Target IP Address (Editar dirección IP de destino)**, escriba la dirección IP de destino para uno o todos los destinos de la sonda en el cuadro **IP Address (Dirección IP)** y haga clic en **OK (Aceptar)**. Haga clic en **Siguiente.**

Nota: Sólo se requiere el primer destino de la sonda. Puede especificar hasta tres destinos adicionales de la sonda como respaldos de seguridad, asignando direcciones IP a otros destinos de la sonda.

12. Seleccione un miembro de equipo indicado, haga clic en **Edit Member IP Address** (Editar dirección IP de miembro) y luego escriba la dirección IP de miembro en el cuadro IP Address (Dirección IP). Repita esta operación para todos los miembros del equipo enumerados y luego haga clic en **OK (Aceptar)**. Haga clic en **Siguiente.**

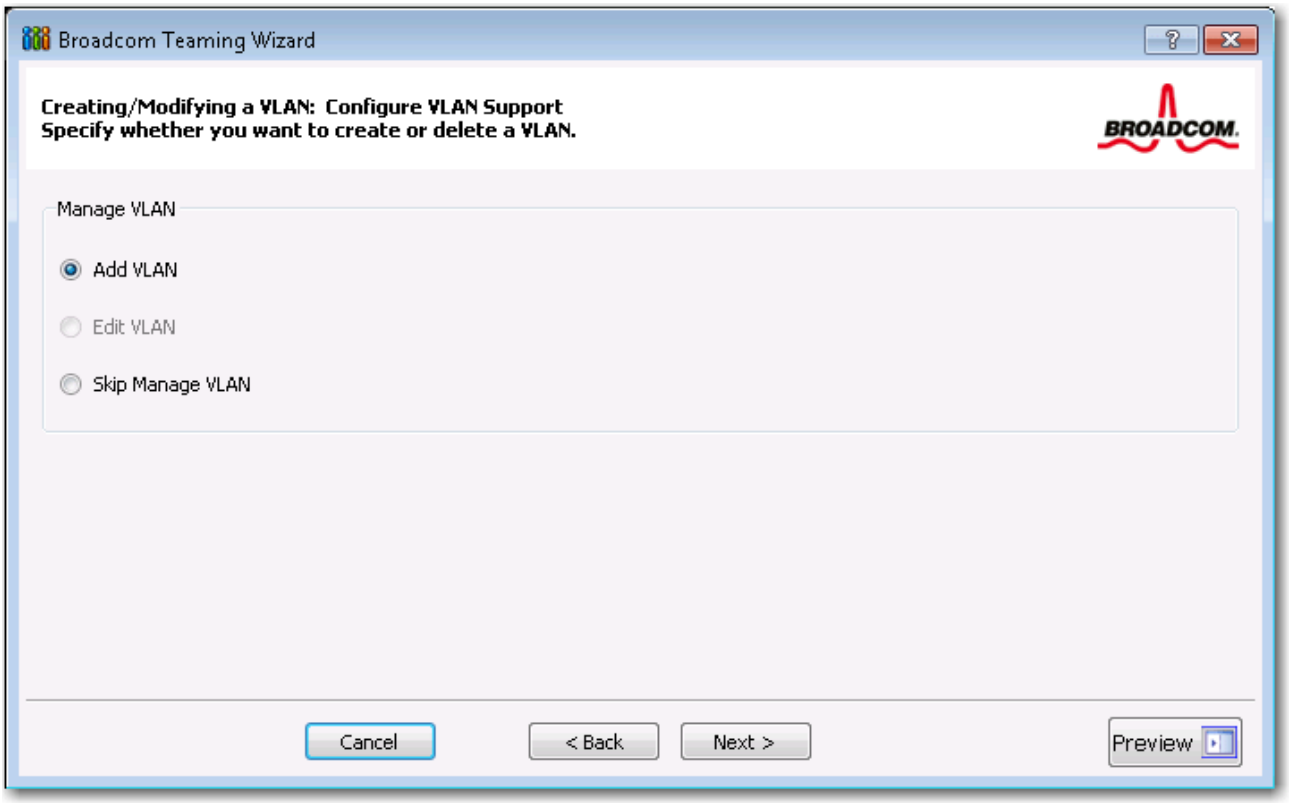
Nota: Todas las direcciones IP de miembro deben estar en la misma subred que los destinos de la sonda.

13. Si desea crear una red VLAN en el equipo, seleccione **Add VLAN** (Agregar red VLAN) o si desea cambiar la

configuración de una VLAN existente, seleccione **Edit VLAN** (Editar red VLAN) y luego haga clic en **Next** (Siguiente). Si no desea crear o editar una red VLAN, seleccione **Skip Manage VLAN** (Saltear administración de VLAN), luego haga clic en **Next** (Siguiente) y continúe con el asistente desde la pantalla Finish (Finalizar) (consulte Paso 18. de este procedimiento).

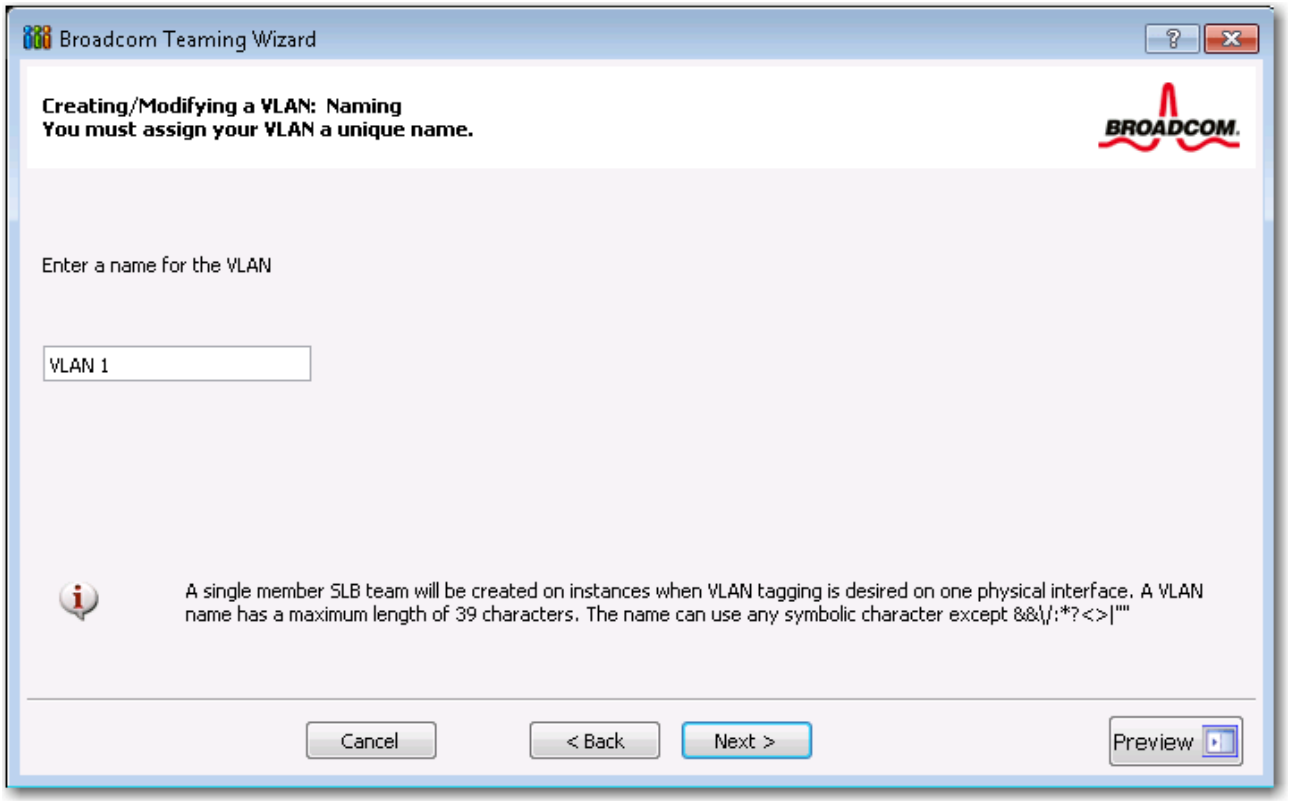
Las redes VLAN le permiten agregar múltiples adaptadores virtuales que se encuentran en subredes diferentes. El beneficio de esto es que su sistema puede tener un adaptador de red que puede pertenecer a múltiples subredes.

Nota: Las VLAN sólo pueden crearse cuando todos los miembros del equipo son adaptadores Broadcom.

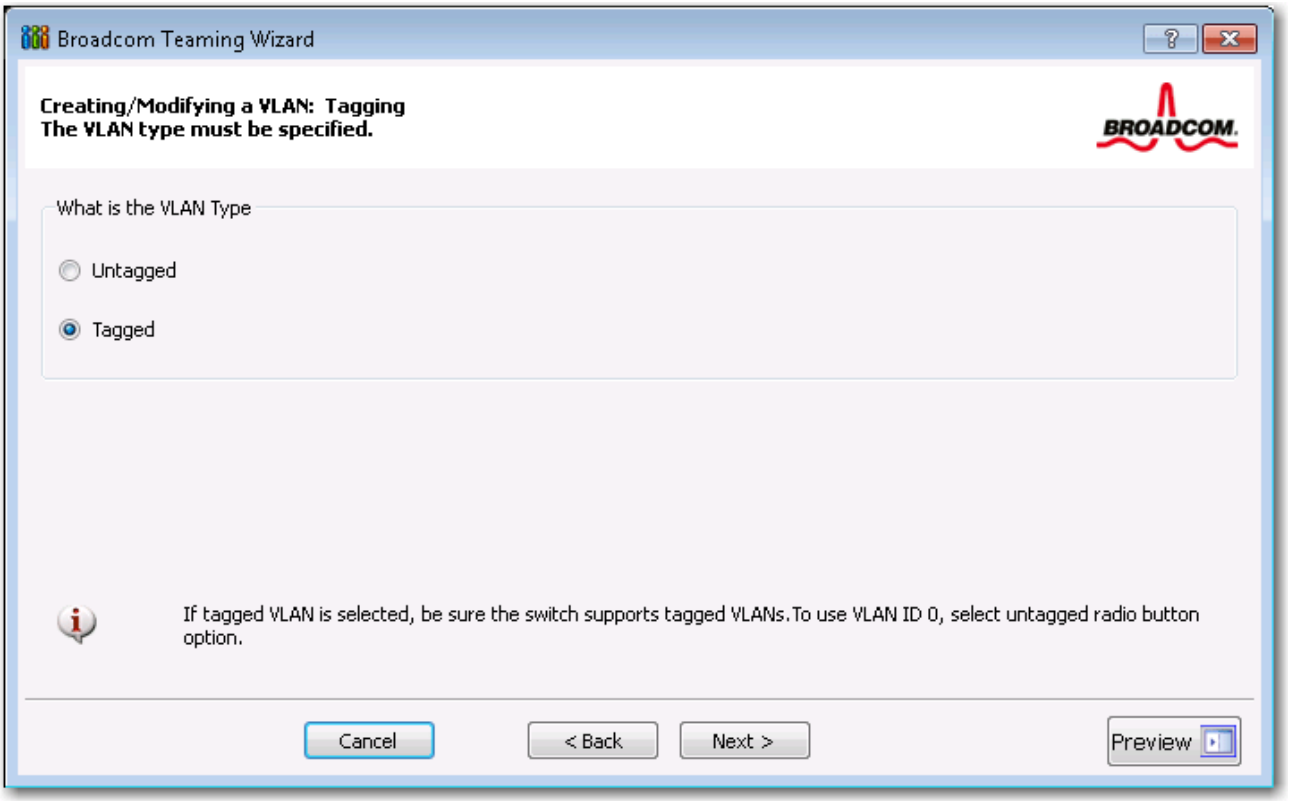


14. Escriba el nombre de la red VLAN y luego haga clic en **Next (Siguiente)**.

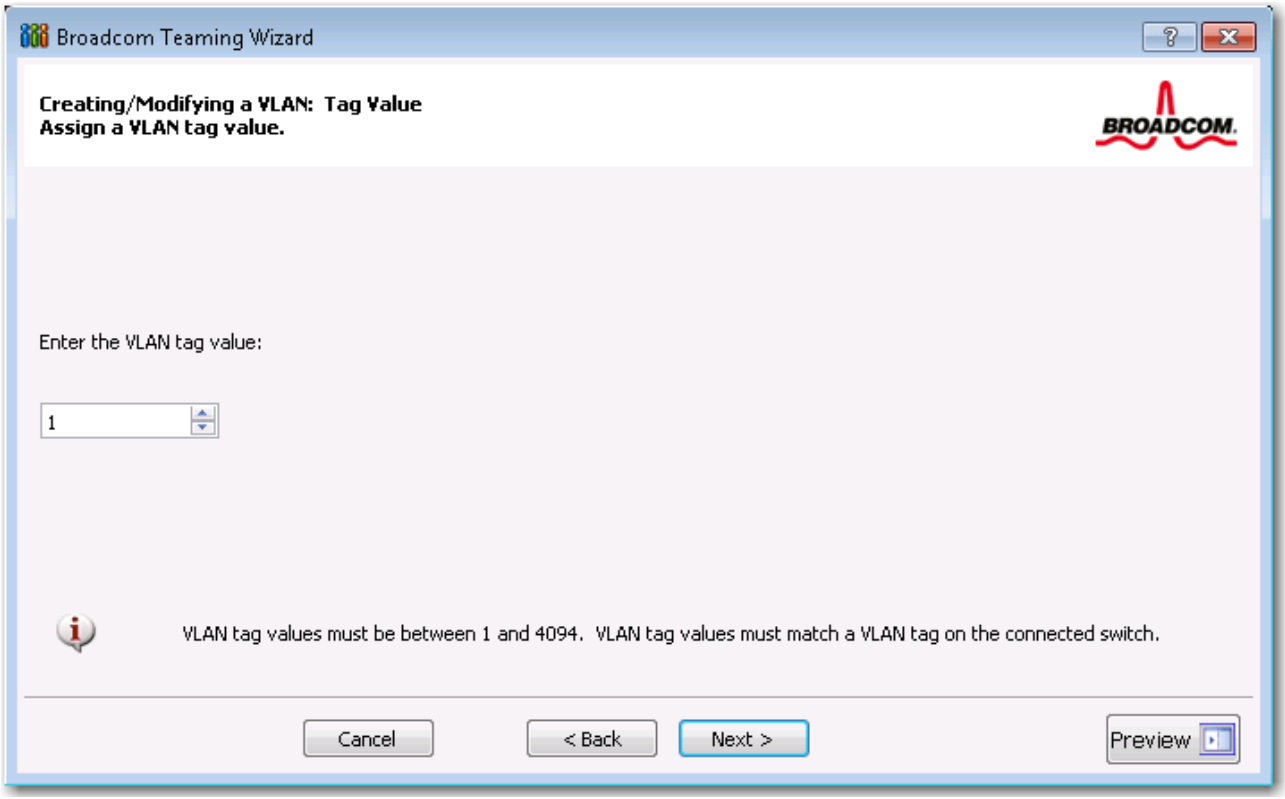
Nota: El nombre del equipo no puede exceder 39 caracteres, no puede comenzar con espacios y no puede contener ninguno de los siguientes caracteres: & \ / : * ? < > |



15. Para etiquetar la red VLAN, seleccione **Tagged** (Con etiqueta) y luego haga clic en **Next** (Siguiente). De lo contrario, haga clic en **Untagged** (Sin etiqueta), haga clic en **Next** (Siguiente) y continúe con el Asistente para agregar redes VLAN adicionales (consulte Paso 17. de este procedimiento).



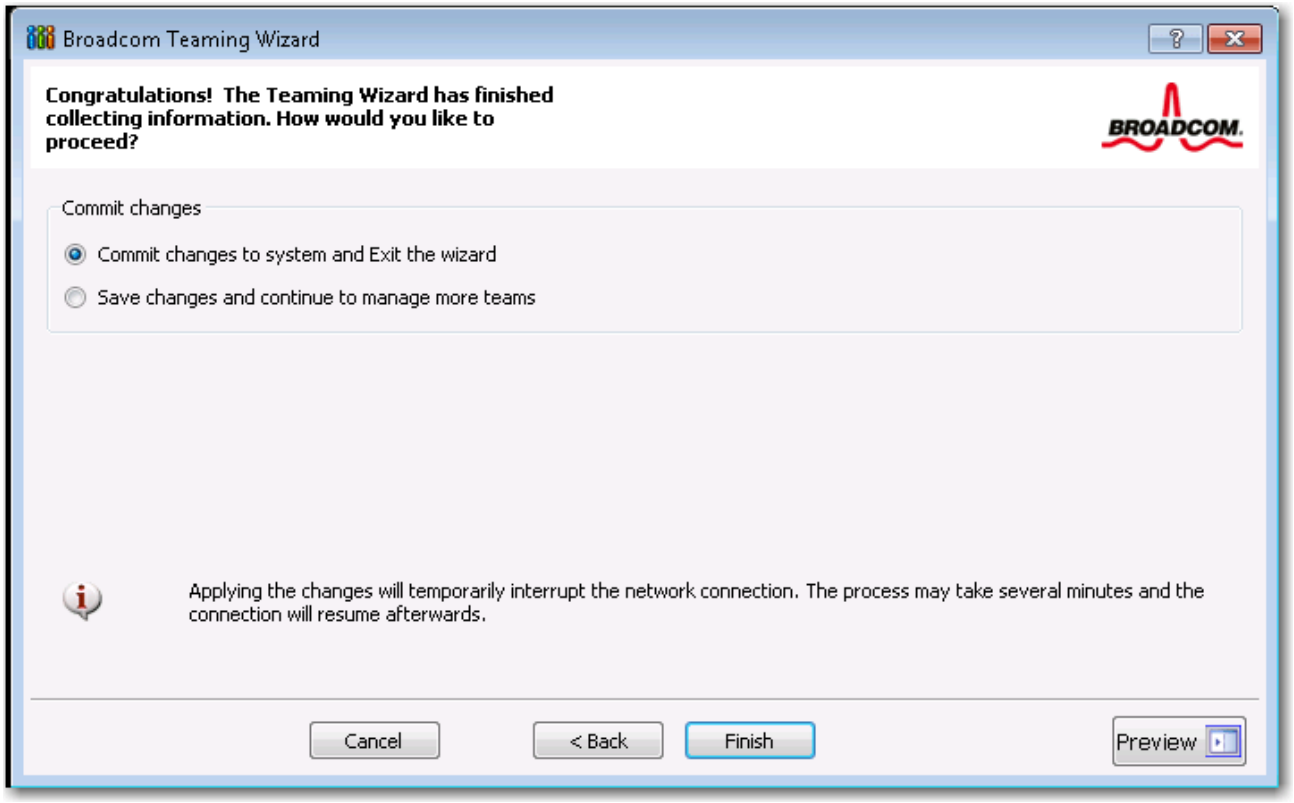
16. Escriba el nombre de la red VLAN y luego haga clic en **Next** (Siguiente). El valor debe estar entre 1 y 4094.



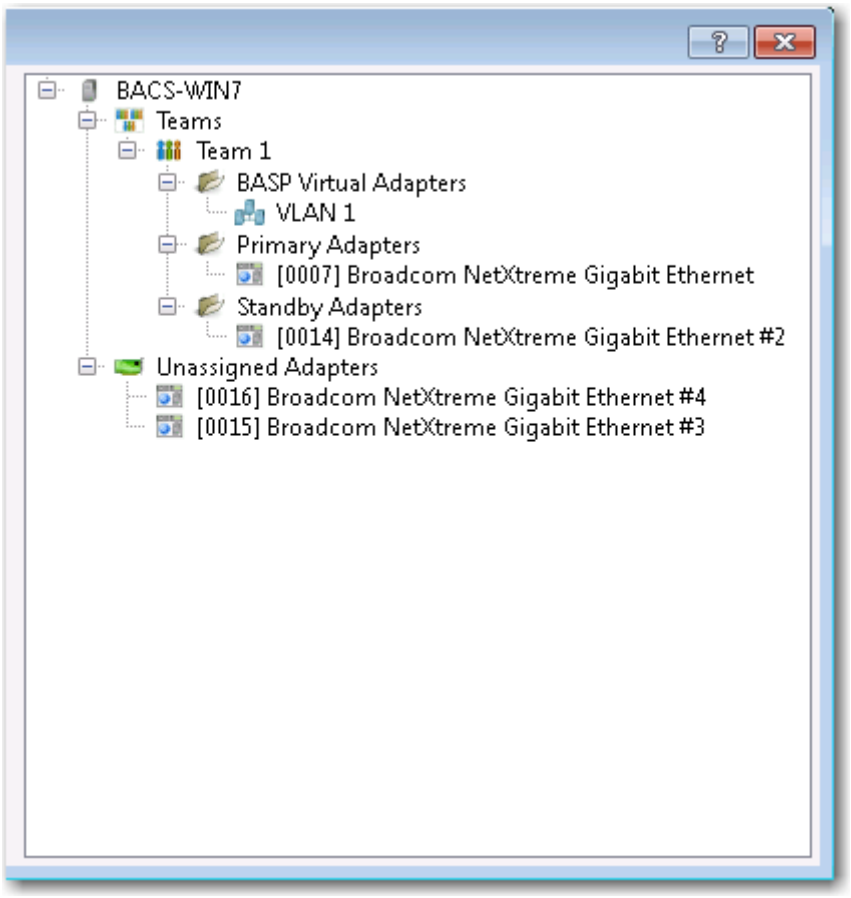
17. Seleccione **Yes** (Sí) para agregar o administrar otra red VLAN y luego haga clic en **Next** (Siguiente). Repita el procedimiento hasta que haya agregado o administrado todas las VLAN que desea.

Nota: Puede definir hasta 64 VLAN por equipo (63 VLAN que tienen etiquetas y 1 VLAN que no tiene etiqueta). Agregar varias redes VLAN puede hacer más lento el tiempo de reacción de la interfaz de Windows debido al uso del tiempo del procesador y la memoria para cada red VLAN. El grado en que puede verse afectado el rendimiento de Windows depende de la configuración del sistema.

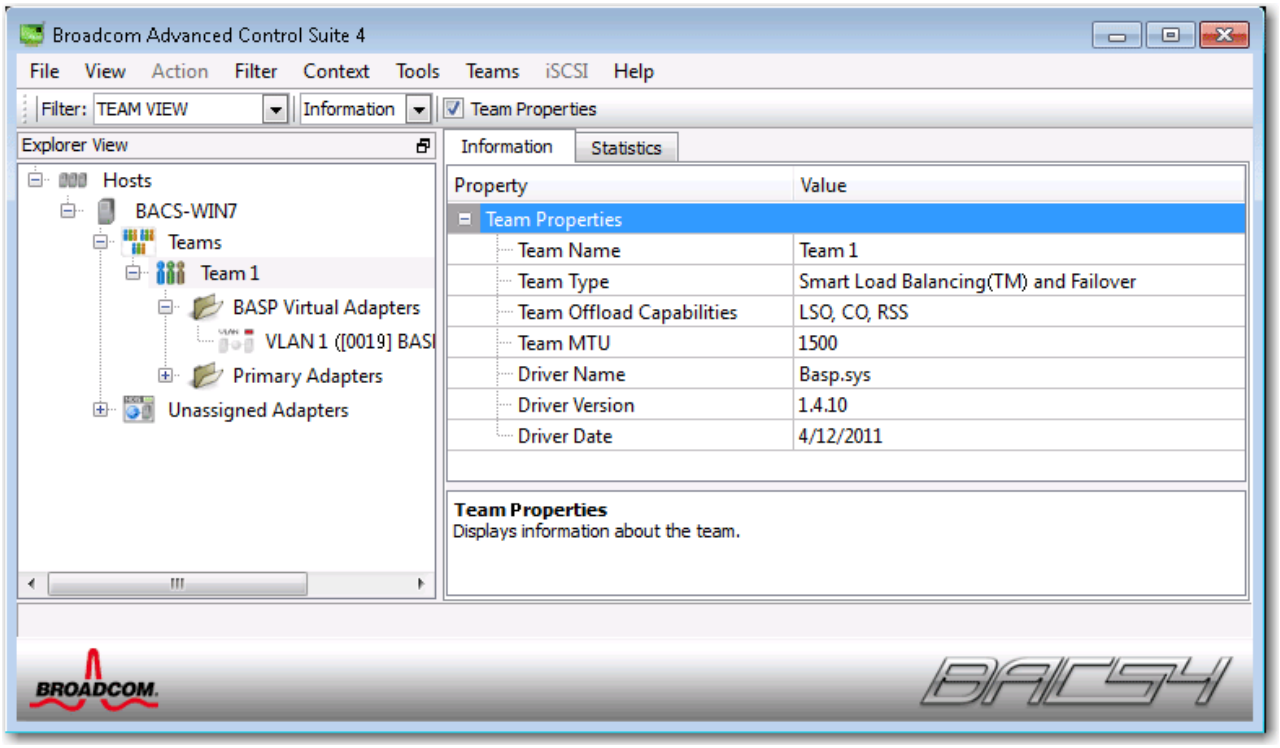
18. Para aplicar y aceptar los cambios en el equipo, seleccione **Commit changes to system and Exit the wizard** (Aceptar los cambios en el sistema y salir del asistente). Para aplicar los cambios y seguir utilizando el asistente, seleccione **Save changes and continue to manage more teams** (Guardar los cambios y continuar administrando más equipos). Haga clic en Finish (Finalizar).



Nota: En cualquier momento del procedimiento del Asistente para formación de equipos Broadcom, haga clic en **Preview** (Vista preliminar) para obtener una representación visual de cómo se verá el equipo antes de aceptar cualquier cambio.



19. Haga clic en el nombre del equipo en el panel Team Management (Administración de equipos) para ver las propiedades del equipo en la ficha **Information** (Información), para transferir y recibir datos en la ficha **Statistics** (Estadística).



Uso del Expert Mode (Modo experto)

Utilice el Expert mode (Modo experto) para crear un equipo, modificar un equipo, agregar una red VLAN y configurar LiveLink para un equipo de Smart Load Balance y Failover y SLB (Auto-Fallback Disable) (Balance de carga inteligente y tolerancia a fallas y recuperación automática de fallas desactivada). Para crear un equipo usando el asistente, consulte Uso del Asistente para equipos de Broadcom.

Para configurar el Modo de formación de equipos predeterminado, seleccione **Options** (Opciones) del menú **Tools** (Herramientas), y luego seleccione **Expert Mode** (Modo experto) o **Wizard Mode** (Modo asistente) (el valor predeterminado es Modo asistente).

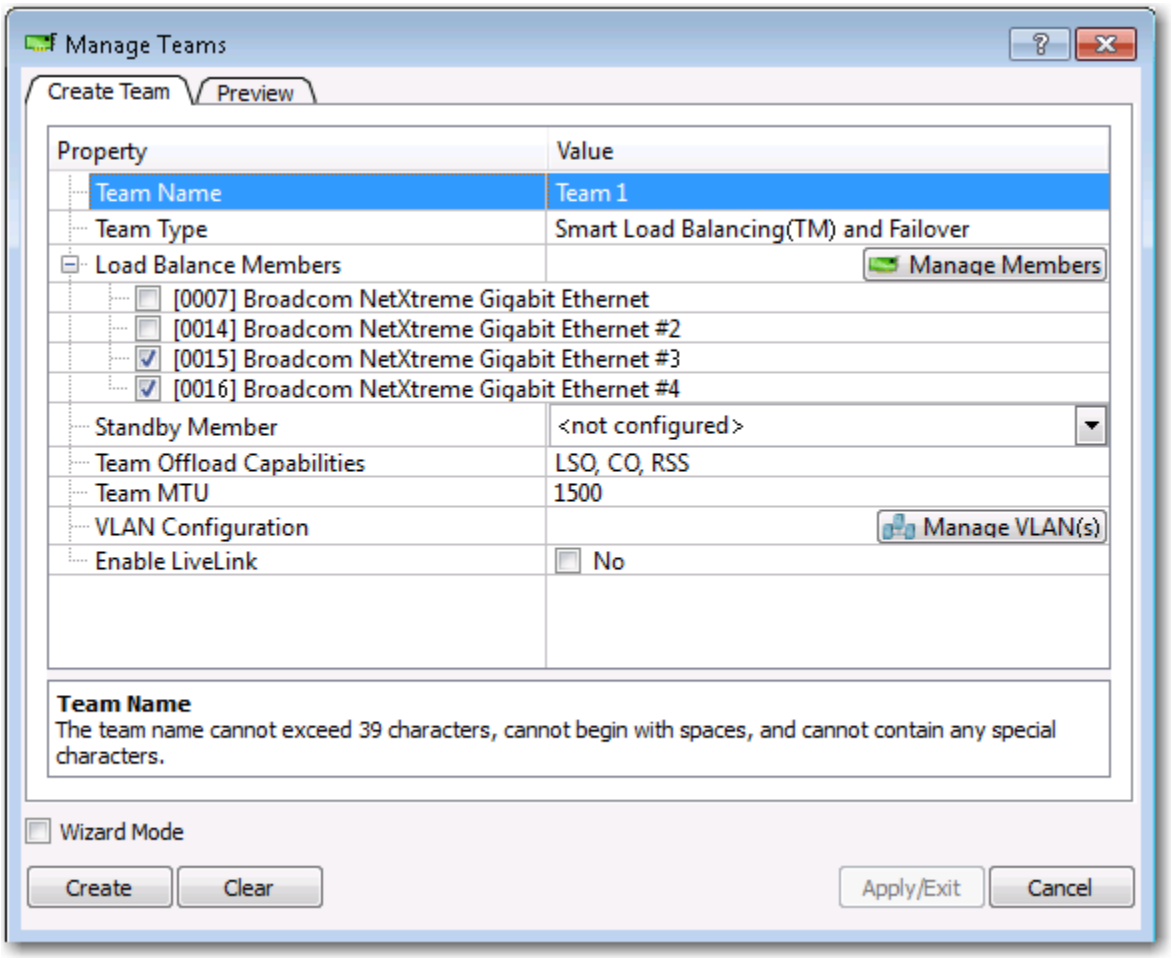
Cómo crear un equipo

Nota: No se recomienda habilitar el protocolo DHCP (Protocolo de configuración dinámica de host) para los miembros de un equipo del tipo SLB.

1. Desde el menú **Teams** (Equipos), seleccione **Create Team** (Crear equipo) o haga clic con el botón derecho sobre uno de los dispositivos en la sección "Adaptadores no asignados" y seleccione **Create a Team** (Crear un equipo). Esta opción no se encuentra disponible si no hay dispositivos enumerados en las secciones "Adaptadores no asignados", lo que significa que todos los adaptadores han sido asignados a equipos.
2. Haga clic en **Expert Mode** (Modo experto).

Nota: Si desea utilizar siempre el Expert mode (Modo experto) para crear un equipo, seleccione **Default to Expert Mode on next start (Emplear el Modo experto predeterminado en el próximo inicio)**.

3. Haga clic en la ficha **Create Team** (Crear un equipo).



Nota: La ficha **Create Team** (Crear un equipo) aparece únicamente si se encuentran disponibles adaptadores con un equipo asignado.

4. Haga clic en el campo **Team Name** (Nombre de equipo) para ingresar un nombre de equipo.
5. Haga clic en al campo **Team Type** (Tipo de equipo) para seleccionar un tipo de equipo.
6. Asigne cualquier adaptador o adaptadores disponibles al equipo seleccionando el adaptador de la lista **Load Balance Members** (Miembros de balance de carga). Deberá haber por lo menos un adaptador seleccionado en la lista **Load Balance Members** (Miembros de balance de carga).
7. Puede asignar cualquier otro adaptador disponible para que sea un miembro en espera seleccionándolo de la lista **Standby Member** (Miembro en espera).

Nota: Debe haber, por lo menos, un adaptador de red Broadcom asignado al equipo.

Las columnas Large Send Offload (LSO) (Descarga de envío grande), Checksum Offload (CO) (Descarga de

Checksum) y RSS indican si las propiedades LSO, CO y/o RSS cuentan con soporte para el equipo. Las propiedades LSO, CO y RSS están habilitadas para un equipo solo cuando todos los miembros cuentan con soporte y están configurados para la característica.

Nota: Agregar un adaptador de red a un equipo que tiene el controlador deshabilitado podría afectar negativamente las capacidades de descarga del equipo. Esto podría afectar el rendimiento del equipo. Por lo tanto, se recomienda agregar adaptadores de red con controladores habilitados como miembro de un equipo.

8. Escriba el valor para **Team MTU** (MTU de equipo).
9. Haga clic en **Create** (Crear) para guardar la información del equipo.
10. Repita los pasos 4. al 9. para definir equipos adicionales. Al definir los equipos, éstos pueden seleccionarse de la lista de equipos, pero todavía no se han creado. Haga clic en la ficha **Preview** (Vista previa) para ver la estructura del equipo antes de aceptar los cambios.
11. Haga clic en **Apply/Exit** (Aplicar/Salir) para crear todos los equipos que ha definido y salir de la ventana Administrar equipos.
12. Haga clic en **Sí** cuando aparezca el mensaje que indica que la conexión de red se interrumpirá momentáneamente.

NOTAS:

- El nombre del equipo no puede exceder 39 caracteres, no puede comenzar con espacios y no puede contener ninguno de los siguientes caracteres: & \ / : * ? < > |
- Los nombres de los equipos deben ser exclusivos. Si intenta usar un nombre de equipo más de una vez, aparece un mensaje de error que indica que el nombre ya existe.
- El número máximo de miembros del equipo es ocho.
- Una vez realizada correctamente la configuración de equipo, se crea un controlador de adaptador de equipo virtual para cada equipo configurado.
- Si deshabilita un equipo virtual y posteriormente desea volver a habilitarlo, primero debe deshabilitar y rehabilitar todos los miembros del equipo antes de rehabilitar el equipo virtual.
- Cuando cree equipos de Generic Trunking y Link Aggregation (Troncalización genérica y Agregación de enlaces), puede designar un miembro en espera. Los miembros en espera sólo funcionan con los equipos del tipo de Smart Load Balancing (Balance de carga inteligente), Failover (tolerancia a fallas) y SLB (Autoreserva deshabilitada).
- En un equipo SLB (Autoreserva deshabilitada), para restaurar el tráfico a los miembros del balance de carga desde el miembro en espera, haga clic en el botón Fallback en la ficha Team Properties (Propiedades del equipo).
- Cuando se configura un equipo SLB, si bien se soporta la conexión de los miembros del equipo a un concentrador (hub) para realizar pruebas, se recomienda conectar los miembros a una central.
- No se da soporte a todos los adaptadores de otros fabricantes ni se certifican totalmente para la creación de equipos.

13. Configure la dirección IP del equipo.

a. Desde **Control Panel** (Panel de Control), haga doble clic en **Network Connections** (Conexiones de red).

b. Haga clic con el botón derecho sobre el nombre del equipo que desea configurar y luego haga clic en **Properties** (Propiedades).

c. En la ficha **General,** haga clic en **Internet Protocol** (Protocolo de Internet) **(TCP/IP)** y luego haga clic en **Properties** (Propiedades).

d. Configure la dirección IP y cualquier otra configuración de TCP/IP necesaria para el equipo y luego haga clic en **Aceptar** cuando haya finalizado.

Cómo modificar un equipo

Después de haber creado un equipo, puede modificarlo de las siguientes maneras:

- Cambie el tipo de equipo
- Cambie los miembros asignados al equipo
- Agregue una red VLAN
- Modifique una red VLAN (usando el Modo experto)
- Elimine un equipo o una red VLAN (usando el Modo experto)

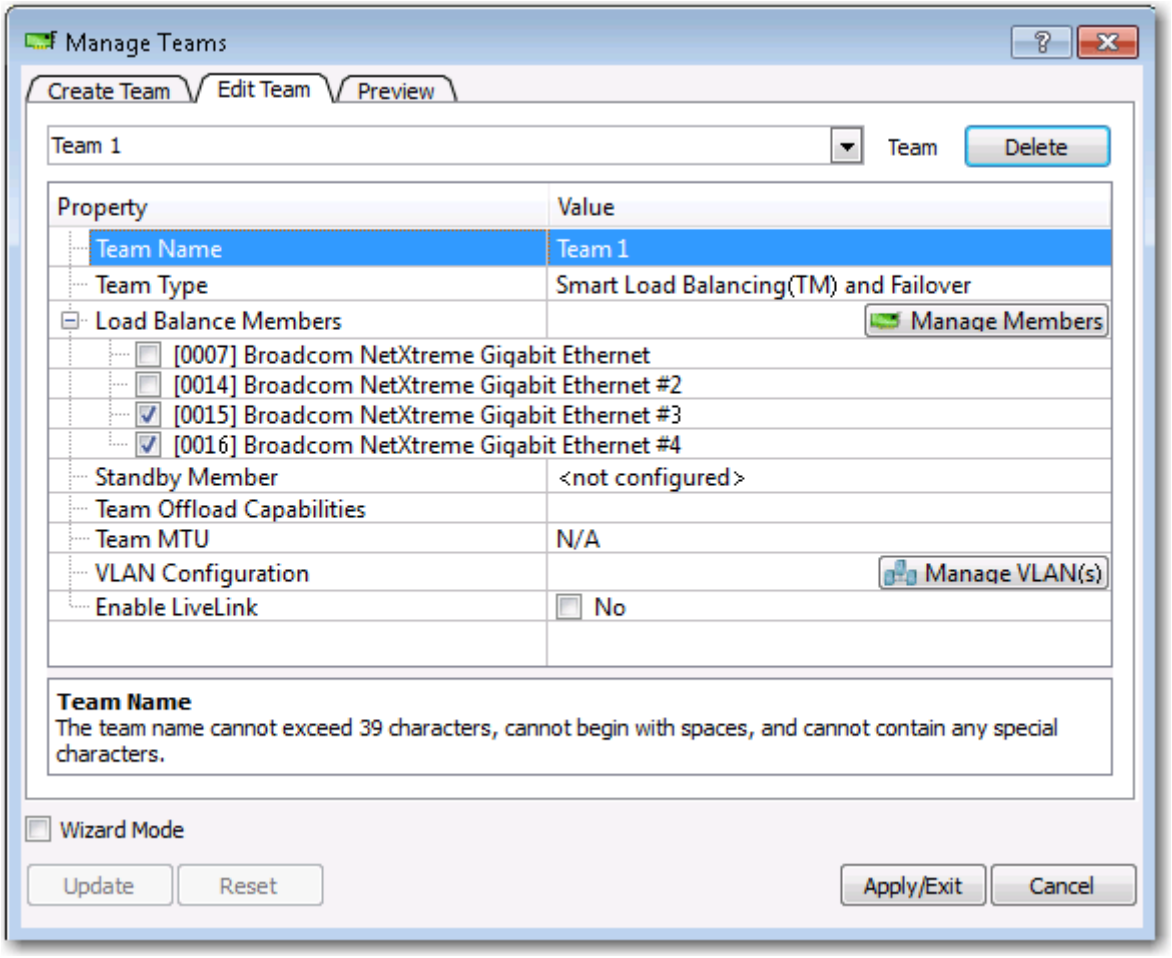
Para modificar un equipo

1. Desde el menú **Team** (Equipo), haga clic en **Edit Team** (Editar equipo) o haga clic con el botón derecho sobre uno de los equipos y seleccione **Edit Team** (Editar equipo). Esta opción se encuentra únicamente disponible si ya se ha creado un equipo y éste se encuentra en el panel Administración de equipos.

2. Aparece la pantalla de bienvenida del asistente. Haga clic en **Next** (Siguiente) para continuar modificando un equipo mediante el asistente o haga clic en **Expert Mode** para trabajar en Modo experto.

Nota: La ficha **Edit Team** (Editar equipo) en Expert Mode (Modo experto) aparece únicamente si hay equipos configurados en el sistema.

3. Haga clic en la ficha **Edit Team** (Editar equipo).



4. Realice los cambios deseados y luego haga clic en **Update** (Actualizar). Los cambios todavía no se han aplicado, haga clic en la ficha **Preview** (Vista preliminar) para ver la estructura actualizada del equipo antes de aceptar los cambios.
5. Haga clic en **Apply/Exit** (Aplicar/Salir) para aplicar las actualizaciones y salir de la ventana Administrar equipos.
6. Haga clic en **Sí** cuando aparezca el mensaje que indica que la conexión de red se interrumpirá momentáneamente.

Agregue una red VLAN

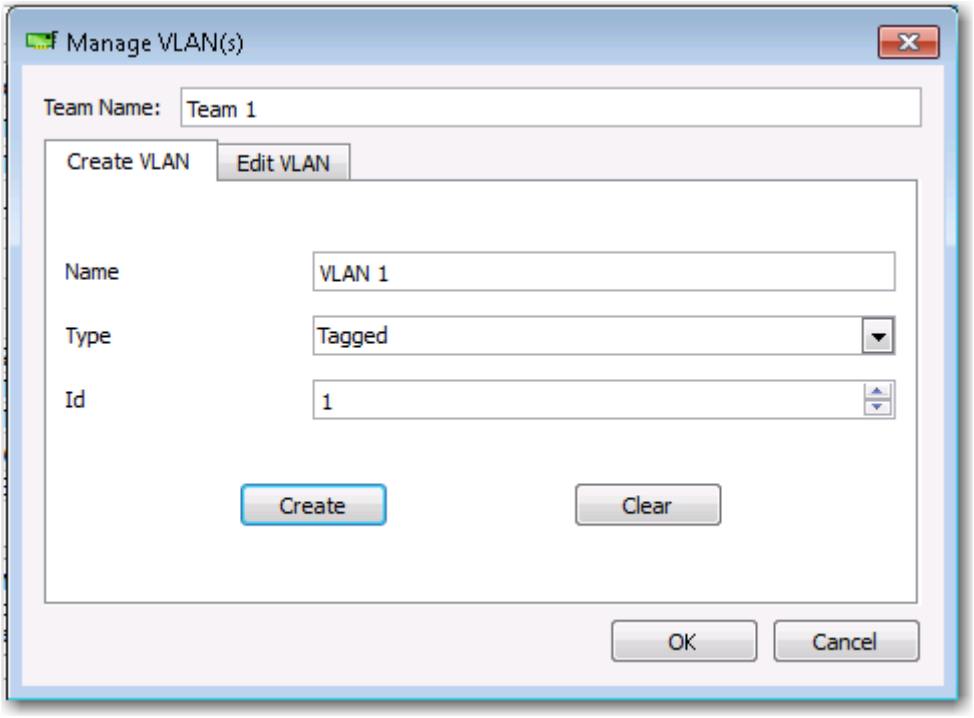
Puede agregar LAN virtuales (VLAN) a un equipo. Esto le permite agregar múltiples adaptadores virtuales que se encuentran en subredes diferentes. El beneficio de esto es que su sistema puede tener un adaptador de red que puede pertenecer a múltiples subredes. Con una VLAN, usted puede agregar la funcionalidad de balance de carga para los miembros del Balance de carga y puede emplear un adaptador de tolerancia a fallas.

Puede definir hasta 64 VLAN por equipo (63 VLAN que tienen etiquetas y 1 VLAN que no tiene etiqueta). Las VLAN sólo pueden crearse cuando todos los miembros del equipo son adaptadores Broadcom. Si intenta crear una VLAN con un adaptador que no sea de Broadcom, aparece un mensaje de error.

Para configurar un equipo con una VLAN

1. Desde el menú **Teams** (Equipos), seleccione **Add VLAN** (Agregar red VLAN).

2. Aparece la pantalla de bienvenida.
3. Haga clic en **Expert Mode** (Modo experto).
4. En la ficha **Create Team** (Crear equipo) de la ventana **Manage Teams** (Administrar equipos), haga clic en **Manage VLAN(s)** (Administrar redes VLAN).
5. Escriba el nombre de la red VLAN y luego seleccione el tipo y el ID.
6. Haga clic en **Create** (Crear) para guardar la información VLAN. Al definir las redes VLAN, éstas pueden seleccionarse de la lista Nombre de equipo, pero todavía no se han creado.
7. Continúe este proceso hasta que todas las redes VLAN hayan sido definidas y luego haga clic en **OK** (Aceptar) para crearlas.



8. Haga clic en **Sí** cuando aparezca el mensaje que indica que la conexión de red se interrumpirá momentáneamente.

Nota: Para mantener el desempeño óptimo del adaptador, su sistema debería tener 64 MB de memoria del sistema para cada una de las ocho VLAN creadas por adaptador.

Para ver las propiedades y estadísticas de la VLAN y para ejecutar pruebas de VLAN

Para ver las propiedades y estadísticas de la VLAN y para ejecutar pruebas de VLAN

1. Seleccione una de las redes VLAN enumeradas.
2. Haga clic en la ficha **Information** (Información) para ver las propiedades del adaptador de red VLAN.
3. Haga clic en la ficha **Statistics** (Estadística) para ver las estadísticas del adaptador de red VLAN.
4. Haga clic en la ficha **Diagnostics** (Diagnóstico) para ejecutar una prueba de red en el adaptador VLAN.

Cómo eliminar una red VLAN

El siguiente procedimiento se aplica cuando trabaja en Modo Experto.

Para eliminar una VLAN

1. Seleccione la VLAN que desea eliminar.
2. Desde el menú **Teams** (Equipos), seleccione **Remove VLAN** (Eliminar red VLAN).
3. Haga clic en **Apply (Aplicar)**.
4. Haga clic en **Sí** cuando aparezca el mensaje que indica que la conexión de red se interrumpirá momentáneamente.

Nota: Si elimina un equipo también se eliminan todas las redes VLAN configuradas para dicho equipo.

Configuración de LiveLink para un equipo Smart Load Balancing y Failover (Balance de carga inteligente y tolerancia a fallas) y SLB (Auto-Fallback Disable) (SLB) (Recuperación automática de fallas desactivada).

LiveLink es una función de BASP que se ofrece para el tipo de equipo Smart Load Balancing (SLB) (Balance de carga inteligente) y (Auto-Fallback Disable) (SLB) (Recuperación automática de fallas desactivada). El propósito de LiveLink es detectar la pérdida de enlaces más allá del conmutador y direccionar el tráfico sólo a través de los miembros del equipo que tienen un enlace activo.

Lea las siguientes notas antes de configurar LiveLink.

NOTAS:

- Antes de comenzar a configurar LiveLink™, lea la descripción de LiveLink. También verifique que cada destino de la sonda que desea especificar esté disponible y en funcionamiento. Si la dirección IP del destino de la sonda cambia por cualquier motivo, deberá volver a configurar LiveLink. Si la dirección MAC del destino de la sonda cambia por cualquier motivo, deberá reiniciar el equipo (consulte la sección "Detección y solución de problemas").
- El destino de la sonda debe estar en la misma subred que el equipo, tener una dirección IP válida asignada estáticamente (no de transmisión, multidifusión o unidifusión) y ofrecer una alta disponibilidad (siempre activo).
- Para garantizar la conectividad de la red con el destino de la sonda, haga ping al destino de la sonda desde el equipo.
- Puede especificar hasta cuatro destinos de la sonda.
- La dirección IP asignada a cualquier destino de la sonda y miembro de equipo puede no tener un cero como el primero o el último octeto.

Para configurar LiveLink

1. Desde el menú **Teams** (Equipos), seleccione **Edit Team** (Editar equipo).
2. Haga clic en Expert Mode (Modo experto) (para configurar LiveLink con el Asistente para equipos, consulte Uso del Asistente para equipos de Broadcom).
3. En la ventana Manage Members (Administrar miembros), haga clic en la ficha **Edit Team** (Editar equipo).
4. Seleccione **Enable LiveLink** (Habilitar LiveLink). A continuación, aparecen las opciones de configuración de LiveLink.
5. Se recomienda aceptar los valores predeterminados **Probe interval** (Intervalo de la sonda) (la cantidad de segundos entre cada retransmisión de un paquete de enlace al destino de la sonda) y **Probe maximum retries** (Cantidad máxima de reintentos de la sonda) (la cantidad de respuestas consecutivas perdidas de un destino de la sonda antes de que se active la tolerancia a fallas). Para especificar otros valores, haga clic en el intervalo deseado en la lista .**Probe interval (seconds)** (Intervalo de la sonda (segundos)) y haga clic en la cantidad máxima deseada de reintentos de la sonda en la lista **Probe maximum retries** (Cantidad máxima de reintentos de la sonda).
6. Configure la **Probe VLAN ID** (ID de sonda VLAN) para que concuerde con la VLAN donde se encuentran el o los destinos de la sonda. Esto aplicará la etiqueta de VLAN correspondiente al paquete de enlace según la configuración compartida de los puertos del conmutador conectado.

Nota: Los equipos con habilitación para LiveLink sólo pueden comunicarse con destinos de sonda a través un una única red VLAN. Además, VLAN ID 0 equivale a una red sin etiquetas.

7. Seleccione **Probe Target 1** (Destino de sonda 1) y escriba la dirección IP de destino para uno o todos los destinos de sonda.

Nota: Sólo se requiere el primer destino de la sonda. Puede especificar hasta tres destinos adicionales de la sonda como respaldos de seguridad, asignando direcciones IP a otros destinos de la sonda.

8. Seleccione uno de los miembros de equipo enumerados y escriba la dirección IP de miembro.

Nota: Todas las direcciones IP del miembro deben estar en la misma subred que los destinos de la sonda.

9. Haga clic en **Update** (Actualizar). Repita estos pasos con cada uno de los demás miembros de equipo indicados.
10. Haga clic en **Apply/Exit** (Aplicar/Salir).

Cómo guardar y restaurar una configuración

Para guardar una configuración

1. Desde el menú **File** (Archivo), seleccione **Team Save As** (Guardar como equipo).
2. Escriba *la ruta de acceso y el nombre del nuevo archivo de configuración* y luego haga clic en **Save** (guardar) (se agrega la extensión a .bcg).

   El archivo de configuración es un archivo de texto que puede ser visto con cualquier editor de texto. El archivo contiene información sobre el adaptador y la configuración del equipo.

Para restaurar una configuración

1. Desde el menú **File** (Archivo), haga clic en **Team Restore** (Restaurar equipo).
2. Haga clic en el nombre del archivo a restaurar y, luego, haga clic en **Abrir**.

Nota: De ser necesario, remítase a la carpeta en donde está ubicado el archivo.

3. Haga clic en **Apply (Aplicar)**.
4. Haga clic en **Sí** cuando aparezca el mensaje que indica que la conexión de red se interrumpirá momentáneamente.
5. Si ya hay una configuración cargada, aparece un mensaje que le pregunta si desea guardar su configuración actual. Haga clic en **Yes** (Sí) para guardar la configuración actual. De lo contrario, se pierden los datos de la configuración que está actualmente cargada.

Nota: Es posible que la restauración del equipo demore mucho tiempo si el equipo está configurado con varias VLAN y una dirección IP estática.

Ver Estadísticas BASP

La sección Estadística muestra información de rendimiento de los adaptadores de red que están en un equipo.

Para ver la información que contiene Estadísticas BASP para cualquier adaptador de miembro de equipo o del equipo como un todo, haga clic en el nombre del adaptador o equipo enumerado en el panel Administración de equipos y luego haga clic en la ficha **Statistics** (Estadística).

Haga clic en **Refresh** (Actualizar) para obtener los valores más recientes para cada estadística. Haga clic en **Reset** (Reestablecer) para cambiar todos los valores a cero.

Tx. Paquete. Éste es el número de paquetes transmitido.

Tx. Paquete descartado. Éste es el número de paquetes descartado.

Tx. Paquete en cola. Éste es el número de paquetes en cola.

Rx. Paquete. Éste es el número de paquetes recibido.

Rx. Paquete descartado. Éste es el número de paquetes descartado.

Reintentos de la sonda. Éste es el número de respuestas consecutivas perdidas de un destino de la sonda antes de que se active la recuperación de fallas.

Configurar con la utilidad Interfaz de línea de comando

Un método alternativo a BACS para configurar los adaptadores de red Broadcom es con BACSCLI, que es una utilidad de Broadcom que le permite visualizar información y configurar adaptadores de red utilizando una consola ya sea en modo de interfaz de línea de comando (CLI) no interactivo o en modo interactivo. Al igual que sucede con BACS, BACSCLI ofrece información sobre cada adaptador de red y le permite realizar pruebas detalladas, ejecutar diagnósticos, ver estadísticas y modificar valores de propiedades. BACSCLI también le ofrece la capacidad de agrupar adaptadores de red para el balanceo de carga y tolerancia a fallas.

Para obtener una lista completa de los comandos y ejemplos disponibles, consulte el archivo de texto BACSCLI ReadMe en el CD provisto por Dell.

En un sistema con adaptadores de red NetXtreme I y NetXtreme II de Broadcom, BACSCLI se instala cuando se instala BACS con el instalador.

Detección y solución de problemas de BACS

Problema: Al intentar abrir BACS en un sistema Linux, aparece el siguiente mensaje de error:

> "Otra instancia del cliente BACS parece estar ejecutándose en este sistema. Solo una instancia del cliente BACS se puede ejecutar a la vez. Si está seguro de que no hay otro cliente BACS ejecutándose, es posible que una instancia previa haya salido inesperadamente."

Solución: Este mensaje aparece si intenta ejecutar una segunda instancia de BACS. Si recibe este mensaje y está seguro de que no hay instancias de BACS ejecutándose actualmente, es posible que una instancia anterior de BACS haya salido inesperadamente. Para borrar esa instancia, elimine el archivo "/dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0}."

Sección 14: Especificaciones

Especificaciones de cable 10/100/1000BASE-T

Tabla 22. Especificaciones de cable 10/100/1000BASE-T

Tipo de puerto	Conector	Medios	Distancia máxima
10BASE-T	RJ-45	Pares trenzados no recubiertos categoría 3, 4 o 5 (UTP)	100 m (328 pies)
100/1000BASE-T[1]	RJ-45	Categoría 5[2] UTP	100 m (328 pies)

[1] La señalización 1000BASE-T requiere 4 pares trenzados de cableado balanceado categoría 5, según lo especificado en ISO/IEC 11801:1995 y ANSI/EIA/TIA-568-A (1995) y sometidos a pruebas de desempeño adicionales usando los procedimientos de prueba definidos en TIA/EIA TSB95.

[2]El requerimiento mínimo es categoría 5. Soporte completo para categoría 5e y categoría 6.

Especificaciones de rendimiento

Tabla 23. Especificaciones de rendimiento

Característica	Especificación
Controladoras de tipo PCI Express™ (controladoras BCM57XX)	
Interfaz de PCI Express	Ancho de enlace x1, x2, x4
Ancho de banda agregado PCI Express (transmisión y recibo)	2,5 Gbps o 5,0 Gbps
10/100/1000BASE-T	10/100/1000 Mbps (dúplex completo)

Sección 15: Información reglamentaria

Aviso de Clase B de la FCC

Controlador Broadcom NetXtreme Gigabit Ethernet
BCM95721A211
BCM95722A2202

Este dispositivo cumple con la Sección 15 de las Normas de la FCC. Su operación está sujeta a las dos condiciones siguientes: 1) Este dispositivo no podrá causar interferencia nociva y 2) Este equipo debe aceptar cualquier interferencia recibida, incluso la interferencia que pueda causar un funcionamiento no deseado.

El equipo se ha sometido a pruebas y se ha concluido que cumple con los límites para dispositivos digitales de Clase B, conforme a la Sección 15 de las Normas de la FCC. Estos límites se han establecido para ofrecer una protección razonable contra la interferencia nociva en una instalación residencial. El equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza según las instrucciones, podría causar interferencias nocivas en las radiocomunicaciones. Sin embargo, no existen garantías de que no se producirán interferencias en una instalación en particular. Si este equipo causa interferencia nociva con la recepción de radio o televisión (que se puede determinar al apagar y encender el equipo), se recomienda que trate de corregir la interferencia al proceder en una o más de las siguientes maneras:

- Reoriente o modifique la ubicación de la antena receptora.
- Aumente la separación entre el equipo y el receptor.
- Conecte el equipo a un tomacorriente de un circuito diferente al que está conectado el receptor.
- Consulte al distribuidor o a un técnico experimentado de radio/TV para recibir asistencia.

No realice modificaciones mecánicas ni eléctricas al equipo.

Nota: Si cambia o modifica el adaptador sin el permiso del Broadcom, correrá el riesgo de perder su derecho para operar el equipo.

Broadcom Corporation
190 Mathilda Place
Sunnyvale, California 94086 USA

Aviso de Clase B del VCCI

Este equipo es un producto de Clase B basado en el estándar del VCCI (Voluntary Control Council for Interference from Information Technology Equipment). Si se opera cerca de un receptor de radio o televisión en un entorno doméstico, puede causar radiointerferencia. Instale y utilice el equipo según el manual de instrucciones.

⚠ **¡Precaución!** Existe la probabilidad de que este equipo se dañe ante la presencia de energía de frecuencia radial conducida entre el rango de frecuencia de 59 a 66 MHz. La operación normal se reanuda después de remover la fuente de energía de radiofrecuencia.

Aviso de Clase B del VCCI (Japón)

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。

Aviso de la CE

БЪЛГАРСКИ Bulgarian	Този продукт отговаря на 2006/95/EC (Нисковолтова директива), 2004/108/EC (Директива за електромагнитна съвместимост) и измененията на Европейския съюз. **Европейски съюз, Клас B** Това устройство на Broadcom е класифицирано за използване в типичната за Клас B жилищна среда. Изготвена е "Декларация за съответствие" според горепосочените директиви и стандарти, която се съхранява в Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ČESKÝ Czech	Bylo ustanoveno, že tento produkt splňuje směrnici 2006/95/EC (nízkonapěťová směrnice), směrnici 2004/108/EC (směrnice EMC) a dodatky Evropské unie. **Evropská unie, třída B** Toto zařízení společnosti Broadcom je klasifikováno pro použití v obvyklém prostředí domácnosti (třída B). „Prohlášení o shodě" v souladu s výše uvedenými směrnicemi a normami bylo zpracováno a je uloženo v archivu společnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Danish	Dette produkt er fundet i overensstemmelse med 2006/95/EC (Lavvoltsdirektivet), 2004/108/EC (EMC-direktivet) og den Europæiske Unions ændringer. **Den Europæiske Union, Klasse B** Denne Broadcom-enhed er klassificeret til anvendelse i et typisk Klasse B-hjemligt miljø. En "Overensstemmelseserklæring", som er i henhold til foregående direktiver og standarder, er udført og arkiveret hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
NEDERLANDS Dutch	Dit product is in overeenstemming bevonden met 2006/95/EC (Laagspanningsrichtlijn), 2004/108/EC (EMC-richtlijn) en amendementen van de Europese Unie. **Europese Unie/Klasse B** Dit Broadcom-apparaat is geclassificeerd voor gebruik in een typische klasse B woonomgeving. Een "Verklaring van conformiteit" in overeenstemming met de voorgenoemde richtlijnen en standaarden is beschikbaar bij Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
English	This product has been determined to be in compliance with 2006/95/EC (Low Voltage Directive), 2004/108/EC (EMC Directive), and amendments of the European Union. **European Union, Class B** This Broadcom device is classified for use in a typical Class B domestic environment. A "Declaration of Conformity" in accordance with the preceding directives and standards has been made and is on file at Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
EESTLANE Estonian	Antud toode vastab direktiividele 2006/95/EU (Madalpinge direktiiv), 2004/108/EU (EMC direktiiv) ja ELi parandustele. **Euroopa Liit, Klass B** Antud Broadcom toode on klassifitseeritud kasutamiseks tüüpilises B-klassi koduses keskkonnas. Vastavalt ülaltoodud direktiividele ja standarditele on koostatud „Vastavusdeklaratsioon", mis on arvel ettevõttes Broadcom Corporation, 190 MathildaPlace, Sunnyvale, California 94086, USA.
Finnish	Tämä tuote täyttää Euroopan unionin direktiivin 2006/95/EY (pienjännitedirektiivi) ja direktiivin 2004/108/EY (sähkömagneettisesta yhteensopivuudesta annettu direktiivi), sellaisina kuin ne ovat muutettuina, vaatimukset. **Euroopan unioni, luokka B** Tämä Broadcom-laite on luokiteltu käytettäväksi tyypillisessä luokan B kotiympäristössä. Yllä mainittujen direktiivien ja standardien mukainen vaatimustenmukaisuusvakuutus on tehty, ja sitä säilyttää Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
FRANÇAIS French	Ce produit a été déclaré conforme aux directives 2006/95/EC (Directive sur la faible tension), 2004/108/EC (Directive EMC) et aux amendements de l'Union européenne. **Union européenne, classe B** Cet appareil Broadcom est classé pour une utilisation dans un environnement résidentiel classique (classe B). Une « Déclaration de Conformité » relative aux normes et directives précédentes a été rédigée et est enregistrée auprès de Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.

DEUTSCH German	Es ist befunden worden, dass dieses Produkt in Ubereinstimmung mit 2006/95/EC (Niederspannungs-Richtlinie), 2004/108/EC (EMV-Richtlinie) und Ergänzungen der Europäischen Union steht. **Europäische Union, Klasse B** Dieses Gerät von Broadcom ist für die Verwendung in einer typisch häuslichen Umgebung der Klasse B vorgesehen. Eine Konformitätserklärung in Ubereinstimmung mit den oben angeführten Normen ist abgegeben worden und kann bei Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ΕΛΛΗΝΙΚΟΣ Greek	Το προϊόν αυτό συμμορφώνεται με τις οδηγίες 2006/95/ΕΕ (Οδηγία περί χαμηλής τάσης), 2004/108/ΕΕ (Οδηγία περί ηλεκτρομαγνητικής συμβατότητας), και τροποποιήσεις τους από την Ευρωπαϊκή Ένωση. **Ευρωπαϊκή Ένωση, Κατηγορία Β** Αυτή η συσκευή Broadcom είναι κατάλληλη για χρήση σε ένα σύνηθες οικιακό περιβάλλον κατηγορίας Β. Μία «Δήλωση Συμμόρφωσης» σύμφωνα με τις προηγούμενες οδηγίες και πρότυπα υπάρχει και είναι αρχειοθετημένη στο Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
MAGYAR Hungarian	A termék megfelel a 2006/95/EGK (alacsony feszültségű eszközökre vonatkozó irányelv), a 2004/108/EGK (EMC irányelv) és az Európai Unió ajánlásainak. **Európai Unió, „B" osztály** Ez a Broadcom eszköz „B" osztályú besorolást kapott, tipikus lakossági környezetben való használatra alkalmas. Az előbbiekben ismertetett irányelvek és szabványok szellemében „Megfelelőségi nyilatkozat" készült, amely az irországi Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
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.

Información reglamentaria canadiense (sólo para Canadá)

Industry Canada, Clase B

Este aparato digital de Clase B cumple con la ICES-003 canadiense.

Aviso: Las reglamentaciones de Industry Canada estipulan que aquellos cambios o modificaciones no aprobados expresamente por Broadcom podrían anular su autoridad para operar este equipo.

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.

Aviso MIC (sólo para República de Corea)

Dispositivo de CLASE B

Controlador Broadcom NetXtreme Gigabit Ethernet
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

Recuerde que este dispositivo fue aprobado para fines no comerciales y puede usarse en cualquier ambiente, inclusive áreas residenciales.

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。

Sección 16: Detección y solución de problemas

Diagnóstico de hardware

Se encuentran disponibles pruebas de diagnóstico de loopback para verificar el hardware del adaptador. Estas pruebas proveen acceso a los diagnósticos internos/externos del adaptador, en los que se transmiten paquetes de información a través del enlace físico. Para entornos de Windows, consulte Ejecución de las pruebas de diagnóstico).

Fallas de las pruebas de diagnóstico de BACS

Si alguna de las siguientes pruebas falla mientras se ejecutan las pruebas de diagnóstico desde la ficha Ejecución de las pruebas de diagnóstico en BACS, puede ser una indicación de que hay un problema de hardware con el NIC o LOM instalados en el sistema.

- Registros de control
- Registros MII
- EEPROM
- Memoria interna
- CPU en chip
- Interrumpir.
- Bucle - MAC
- Bucle - PHY
- Prueba de LED

A continuación se describen los pasos de detección de fallas que pueden ayudar a corregir problemas.

1. Retire el dispositivo defectuoso y colóquelo nuevamente en la ranura, asegurándose de que la tarjeta esté firmemente colocada en la ranura desde adelante hacia atrás.
2. Ejecute la prueba nuevamente.
3. Si la tarjeta vuelve a fallar, reemplácela con una tarjeta diferente del mismo modelo y luego ejecute la prueba. Si la

prueba es satisfactoria en la tarjeta que usted sabe que está en buenas condiciones, comuníquese con su proveedor de hardware para solicitar asistencia acerca del dispositivo defectuoso.

4. Apague la máquina, desconecte la energía de CA y luego vuelva a reiniciar el sistema.
5. Retire y reinstale el software de diagnóstico.
6. Comuníquese con su proveedor de hardware.

Fallas de prueba de la red BACS

En general, las fallas de BACS Prueba de red son el resultado de un problema de configuración en la red o en las direcciones de IP. A continuación se indican algunas acciones a ejecutar cuando se realiza la detección de fallas de la red.

1. Verifique si el cable está conectado y si el enlace es correcto.
2. Verifique si los controladores están cargados y habilitados.
3. Reemplace el cable que está conectado a NIC/LOM.
4. Verifique si la dirección de IP está asignada correctamente con el comando "ipconfig" o verificando la herramienta de asignación OS IP.
5. Verifique si la dirección de IP es correcta para la red a la que están conectados los adaptadores.

Lista de verificación de detección y solución de problemas

¡Precaución! Antes de abrir la caja de su sistema, verifique Precauciones de seguridad.

La siguiente lista de verificación provee las acciones recomendadas que se deben tomar para resolver problemas de instalación del adaptador Broadcom NetXtreme Gigabit Ethernet o de su ejecución en su sistema.

- Inspeccione todos los cables y conexiones. Verifique que las conexiones de cables del adaptador de red y de la central sean correctas. Verifique que la longitud y la capacidad del cable cumplan con los requisitos indicados en Conexión de los cables de red.
- Verifique la instalación del adaptador volviendo a leer Instalación del hardware. Verifique que el adaptador esté correctamente encajado en la ranura. Verifique los problemas específicos del hardware, tales como el daño obvio a los componentes de la placa o el conector PCI.
- Verifique la configuración y cámbiela si tiene conflicto con otro dispositivo.
- Verifique que su sistema esté usando el último BIOS.
- Intente insertar el adaptador en otra ranura. Si la nueva posición funciona, la ranura original de su sistema puede estar defectuosa.
- Reemplace el adaptador dañado por uno que sepa que funciona correctamente. Si el segundo adaptador funciona en la ranura en que falló el primero, el adaptador original probablemente esté dañado.
- Instale el adaptador en otro sistema que funcione y ejecute nuevamente las pruebas. Si el adaptador pasa las pruebas en el nuevo sistema, el sistema original puede estar dañado.
- Extraiga todos los otros adaptadores del sistema y ejecute nuevamente las pruebas. Si el adaptador pasa las pruebas, los otros adaptadores pueden estar causando contención.

Verificación del enlace de red y la actividad

Consulte Prueba de conectividad de red o Visualización de información del adaptador para verificar el estado del enlace de la red y actividad según las indicaciones de los LED del puerto.

Cómo comprobar si los controladores actuales están cargados

Windows

Consulte Visualización de información del adaptador para ver información de utilidad sobre el adaptador, el estado del enlace y la conectividad de la red.

Linux

Para verificar que el controlador TG3 de Linux esté correctamente cargado, ejecute:

```
lsmod | grep tg3
```

Si el controlador está cargado, aparece una línea similar a la siguiente en la que *size* es el tamaño del controlador en bytes y *n* es la cantidad de adaptadores configurados.

Tabla 24: Controlador Linux:

Módulo	*Tamaño*	*Usado por*
TG3	*size*	*n*

Ejecución de una prueba de longitud de cable

En los entornos de Windows puede realizarse una prueba de longitud del cable. Consulte Análisis de cables para obtener información acerca de como ejecutar una prueba de longitud de cable.

Prueba de conectividad de red

Nota: Cuando use velocidades de enlace obligadas, verifique que el adaptador y el conmutador estén obligados a la misma velocidad o que ambos estén configurados para autonegociación.

Windows

Use el comando ping para determinar si está funcionando la conexión de la red.

Nota: La conectividad de la red también se puede probar usando la característica Prueba de red en Broadcom Advanced Control Suite 2.

1. Verifique si los controladores están cargados y habilitados.
2. Verifique si el cable está conectado y si el enlace es correcto.
3. Haga clic en **Start (Inicio)** y luego haga clic en **Run (Ejecutar)**.
4. Escriba **cmd** en la casilla **Open (Abrir)** y luego haga clic en **OK** (Aceptar).
5. Escriba **ipconfig /all** para ver la conexión de red a probar.
6. Verifique si la dirección de IP es correcta para la red a la que están conectados los adaptadores.
7. Escriba **ping dirección IP** y luego oprima ENTER (INTRO).

Las estadísticas de ping que se exhiben indican si la conexión de la red está funcionando o no.

Linux

Para verificar que la interfaz Ethernet esté activa y funcionando, ejecute **ifconfig** para verificar el estado de la interfaz Ethernet. Es posible usar **netstat -i** para verificar las estadísticas en la interfaz Ethernet. Consulte Software del controlador Linux para obtener información sobre **ifconfig** y **netstat**.

Haga ping en un host de IP en la red para verificar que se haya establecido la conexión:

Desde la línea de comandos, escriba **ping dirección IP**y luego oprima INTRO.

Las estadísticas de ping que se exhiben indican si la conexión de la red está funcionando o no.

Agente Broadcom Boot

Problema: Imposible obtener configuraciones de red a través de DHCP usando PXE.
Solución: Para una operación correcta, asegúrese de que el protocolo STP (protocolo de árbol de tramos) esté

deshabilitado o el modo portfast (para Cisco) esté habilitado en el puerto al que está conectado el cliente PXE. Por ejemplo, configure spantree portfast 4/12 como habilitado (enable).

Broadcom Advanced Server Program (BASP)

Problema: Después de extraer físicamente un NIC que formaba parte de un equipo y luego reiniciar, el equipo no funcioné de manera adecuada.
Solución: Para extraer físicamente un NIC de un equipo de un sistema, primero debe eliminar el NIC del equipo. De no hacerlo antes del cierre, el equipo puede dividirse en un reinicio posterior, lo cual puede generar un comportamiento inesperado del equipo.

Problema: Los cambios que hice cuando modifiqué mi equipo usando INETCFG no entraron en vigencia.
Solución: Al modificar un equipo con INETCFG, deberá reiniciar el sistema después de la reinicialización para que los cambios entren en vigencia.

Depuración de kernel por Ethernet

Problema: Al intentar realizar una depuración de kernel por red Ethernet en un sistema Windows 8.0 o Windows Server 2012, el sistema no se inicia. Este problema puede surgir con algunos adaptadores en sistemas donde Windows 8.0 o Windows Server 2012 está configurado para el modo UEFI. Es posible que vea un error de firmware en pantalla, indicando que se encontró una excepción de Interrupción no enmascarable durante el entorno previo al inicio de UEFI.

Solución: consulte el tema de la base de artículos informativos Microsoft 2920163, “Error de interrupción no enmascarable durante el arranque en un sistema configurado para depuración de kernel por Ethernet”.

Varios

Problema: Las propiedades Large Send Offload (LSO) y Checksum Offload no funcionan en mi equipo.
Solución: Si uno de los adaptadores de un equipo no brinda soporte para LSO, esta propiedad no funcionará en el equipo. Quite el adaptador que no ofrece soporte para LSO del equipo o cámbielo por uno que lo haga. Esto también es válido para la propiedad Checksum Offload.