

Broadcom[®] NetXtreme[®] BCM57XX Guia do Usuário do

Data da última revisão: Fevereiro de 2015

2CS57XX-CDUM513-R

**As informações contidas neste documento estão sujeitas a alterações sem prévio aviso.
© 2014 Broadcom Corporation. Todos os direitos reservados.**

Este documento está protegido por direitos autorais e é distribuído com licenças que restringem seu uso, cópia, distribuição e descompilação. Nenhuma parte deste documento pode ser reproduzida de qualquer forma ou por qualquer meio sem a autorização prévia, por escrito, da Broadcom Corporation. A documentação é fornecida no estado em que se encontra, sem garantia de espécie alguma, expressa ou implícita, inclusive qualquer tipo de garantia implícita ou expressa de não-infração ou as garantias implícitas de comercialização ou adequação a um determinado fim.

A Broadcom Corporation reserva-se o direito de fazer alterações sem aviso prévio em quaisquer produtos ou dados aqui mencionados para aprimorar a confiabilidade, o funcionamento ou o design. As informações fornecidas pela Broadcom Corporation são consideradas precisas e confiáveis. No entanto, a Broadcom Corporation não assume responsabilidade alguma pela aplicação ou uso destas informações ou pela aplicação ou uso de qualquer produto ou circuito aqui descrito, nem fornece licença alguma sob seus direitos de patente ou os direitos de terceiros.

Broadcom, o logotipo pulse, Connecting everything, o logotipo do Connecting everything, NetXtreme, Ethernet@Wirespeed, LiveLink e Smart Load Balancing são marcas da Broadcom Corporation e/ou de suas filiais nos Estados Unidos, outros países e/ou na União Europeia. Microsoft e Windows são marcas comerciais da Microsoft Corporation. Linux é uma marca comercial da Linus Torvalds. Intel é uma marca comercial da Intel Corporation. Magic Packet é uma marca comercial da Advanced Micro Devices, Inc. Red Hat é uma marca comercial da Red Hat, Inc. PCI Express é uma marca comercial da PCI-SIG. Quaisquer outras marcas ou nomes de marcas mencionados são de propriedade de seus respectivos proprietários.

Data da última revisão: Fevereiro de 2015

2CS57XX-CDUM513-R

Sumário

Seção 1: Funcionalidade e recursos	10
Descrição funcional	10
Recursos	11
Gerenciamento de energia	12
Frequência de interrupção adaptativa	12
Canais DMA duplos	12
ASIC com processador RISC incorporado	12
Broadcom Advanced Control Suite	12
Ambientes operacionais suportados	13
Link de rede e indicação de atividade	13
Seção 2: Formação de equipes	14
Visão geral	15
Equilíbrio de carga e tolerância a falhas	15
Tipos de equipe	15
Smart Load Balancing™ e Limite de falha	17
Agregação de link (802.3ad)	17
Trunking genérico (FEC/GEC)/802.3ad-Draft Static	17
SLB (Desativar reserva automática)	18
Limitações dos tipos de equipes Smart Load Balancing e Limite de falha/SLB (Desativar reserva automática)	18
Funcionalidade LiveLink™	19
Suporte para Formação de equipes e Large Send Offload/Checksum Offload	19
Seção 3: Broadcom Gigabit Ethernet Teaming Services	20
Introdução	21
Glossário	21
Conceitos de formação de equipes	23
Endereçamento de rede	23
Endereços de rede e da formação de equipes	23
Descrição dos tipos de formação de equipes	24
Componentes de software	27
Requisitos de hardware	28

Switch Ethernet	28
Roteador.....	28
Recursos suportados pelo tipo de equipe	28
Seleção de um tipo de equipe	30
Mecanismos de formação de equipes	31
Arquitetura	31
Fluxo do tráfego de saída.....	32
Fluxo de Tráfego de Entrada (Somente SLB).....	33
Suporte do protocolo	33
Desempenho	34
Suporte de driver pelo sistema operacionald	35
Velocidades de formação de equipes suportadas.....	36
Formação de equipes e outras propriedades avançadas de rede	37
Checksum Offload	38
Marcação IEEE 802.1p QoS	38
Large Send Offload	38
Quadros Jumbo	38
VLAN do IEEE 802.1Qs	38
Wake on LAN	39
Preboot Execution Environment (PXE)	39
Considerações gerais de rede.....	40
Formação de equipes através de switches	40
Tolerância a falhas do link do switch.....	40
Algoritmo de Spanning Tree.....	42
Observação de alteração da topologia (TCN).....	43
Port Fast/Edge Port.....	43
Formação de equipes com Microsoft NLB/WLBS	43
Considerações do aplicativo	44
Formação de equipes e uso de cluster—Software de cluster da Microsoft	44
Formação de equipes e backup de rede	45
Equilíbrio de carga e limite de falha	45
Tolerância a Falhas.....	46
Resolução de problemas de formação de equipes	48
Dicas de configuração para formação de equipes	48
Orientações para solução de problemas.....	49

Perguntas frequentes	50
Mensagens de log de evento	53
Mensagens de log de evento do sistema Windows	53
Driver de base (adaptador físico/miniporta)	53
Driver intermediário (Adaptador/Equipe Virtual)	55
Seção 4: LANs virtuais	57
Visão geral de VLANs	57
Adição de VLANs às equipes	59
Seção 5: Capacidade de gerenciamento	60
CIM	60
SNMP	61
Subagente do BASP	61
Agente extensível do BASP	61
Seção 6: Instalação do hardware	63
Precauções de segurança	63
Lista de verificação de pré-instalação	64
Instalação do adaptador	64
Conexão dos cabos de rede	65
Cobre	65
Seção 7: Criação de um disco de driver	66
Seção 8: Software de driver do Broadcom Boot Agent	67
Visão geral	67
Configuração do MBA em um ambiente de cliente	68
Configuração do driver MBA	68
Configuração do BIOS	69
Seção 9: Protocolo iSCSI	70
Inicialização iSCSI	70
Sistemas operacionais com suporte para inicialização iSCSI	70
Configuração da inicialização iSCSI	70
A configuração da iSCSI-alvo	70
Configuração dos parâmetros da inicialização iSCSI	71
Configuração do protocolo de inicialização do MBA	72

Configuração de inicialização iSCSI	72
Ativação da opção CHAP Authentication	75
Configuração do servidor DHCP para suportar a inicialização iSCSI	75
Configurações de inicialização iSCSI do DHCP para IPv4	75
Configuração de inicialização iSCSI do DHCP para IPv6	78
Configuração do servidor DHCP	78
Preparação da imagem de inicialização iSCSI	79
Inicialização	82
Outras considerações sobre a inicialização iSCSI	82
Alterando as configurações de Speed & Duplex em ambientes Windows	82
Locally Administered Address	82
LANs virtuais	83
Solução de problemas de inicialização iSCSI	83
iSCSI Crash Dump	83
Seção 10: Instalação de driver e aplicativo de gerenciamento do Windows	84
Pacotes	84
Instalação do software de driver TG3	85
Instalação do pacote RPM de origem	85
Criação do driver com base no arquivo TAR de origem	86
Instalações de rede	86
Descarregamento/remoção do driver do TG3	86
Descarregamento/remoção do driver de uma instalação RPM	86
Remoção do driver de uma instalação TAR	87
Mensagens do driver	87
Formação de equipes com vinculação de canal	87
Instalação do aplicativo de gerenciamento do Linux	88
Visão geral	88
Protocolos de comunicação	88
Instalação do WS-MAN ou CIM-XML no servidor Linux	89
Etapa 1: Instalar o OpenPegasus	89
Etapa 2: Iniciar o servidor CIM no servidor	91
Etapa 3: Configure o OpenPegasus no servidor	91
Etapa 4: Instalar o provedor de CMPI da Broadcom	93
Etapa 5: Executar a configuração do firewall Linux, se necessário	93

Etapa 6: Instalar o BACS e os aplicativos de gerenciamento relacionados	94
Instalação do WS-MAN ou CIM-XML no cliente Linux.....	95
Configuração do HTTPS no cliente Linux.....	95
Instalação do aplicativo Broadcom Advanced Control Suite.....	97
Seção 11: Software de driver do VMware	98
Pacotes	98
Drivers	98
Download, instalação e atualização dos drivers	98
Parâmetros do driver	98
Parâmetros do driver	99
Padrões do driver.....	99
Mensagens do driver	100
Seção 12: Instalação de driver e aplicativo de gerenciamento do Windows.....	101
Instalação do software de driver	102
Como usar o Instalador.....	102
Uso da instalação silenciosa.....	103
Modificação do software de driver	104
Reparação ou reinstalação do software de driver	105
Remoção dos drivers do dispositivo	105
Exibição ou alteração das propriedades do adaptador.....	106
Definição das opções de gerenciamento de energia.....	106
Configurando o protocolo de comunicação a ser usado com o BACS4	107
Uso de WS-MAN.....	107
Configuração do servidor do Windows para WS-MAN.....	107
Instalação do cliente Windows para WS-MAN	114
Uso de WMI	116
Etapa 1: Configura a segurança do espaço de nomes usando o controle do WMI.....	116
Etapa 2: Conceda a Permissão de inicialização e ativação remotas de DCOM	116
Configuração especial para WMI em diferentes sistemas.....	118
Seção 13: Uso do Broadcom Advanced Control Suite 4	119
Visão geral do Broadcom Advanced Control Suite	119
Inicialização do Broadcom Advanced Control Suite	120
Interface BACS	120

Painel Visualização Explorer	121
Seletor Visualização de contexto	122
Visualização de filtro	122
Painel Visualização de contexto	122
Barra de menus	122
Painel de descrição	123
Configuração das preferências no Windows	123
Conexão do host	124
Gerenciamento do host	125
Guia Informações: Informações sobre o host	125
Gerenciamento do Adaptador de rede	127
Informações sobre o Adaptador de Visualização	127
Exibição de informações do driver	129
Exibição de informações de recursos	130
Exibição de informações de hardware	131
Teste de rede	132
Execução de testes de diagnóstico	134
Análise de cabos	135
Definição das propriedades do adaptador	136
Exibição de estatísticas	138
Estatísticas gerais	138
Configuração de equipes	139
Tipos de equipe	140
Comousar o Assistente de formação de equipes Broadcom	140
Uso do Modo Inteligente	153
Criação de uma equipe	153
Modificação de uma equipe	155
Adicionar VLAN	157
Visualização de propriedades e estatísticas de VLAN e execução de testes de VLAN	158
Exclusão de uma VLAN	158
Configuração do LiveLink para uma equipe Smart Load Balancing e Limite de falha e SLB (Desativar reserva automática)	159
Salvamento e restauração de uma configuração	160
Exibição das estatísticas do BASP	161
Configuração com o utilitário de interface da linha de comando	162

Solução de problemas do BACS	162
Seção 14: Especificações	163
Especificações de cabos 10/100/1000BASE-T	163
Especificações de desempenho	163
Seção 15: Informações regulamentares	164
Aviso de Classe B da FCC	164
Aviso de Classe B do VCCI	165
Declaração VCCI Classe B (Japão).....	165
Aviso da CE	165
Informações regulamentares do Canadá (somente para o Canadá)	169
Industry Canada, Classe B	169
Industry Canada, classe B	169
Aviso da MIC (somente para a República da Coreia)	170
Dispositivo da CLASSE B	170
BSMI	171
Seção 16: Etapas da solução de problemas	172
Diagnósticos de hardware	172
Falha no teste de diagnóstico BACS	172
Falhas no teste de rede BACS	173
Lista de verificação de solução de problemas	174
Verificação do link e atividade da rede	174
Verificação dos drivers atuais para determinar se estão carregados	175
Windows	175
Linux	175
Execução de um teste do comprimento do cabo	175
Teste da conectividade de rede	176
Windows	176
Linux	176
Broadcom Boot Agent	176
Broadcom Advanced Server Program (BASP)	177
Depuração de Kernel sobre Ethernet	177
Diversos	177

Seção 1: Funcionalidade e recursos

- [Descrição funcional](#)
- [Recursos](#)
- [Ambientes operacionais suportados](#)
- [Link de rede e indicação de atividade](#)

Descrição funcional

Os adaptadores NetXtreme Broadcom Gigabit Ethernet conectam um computador compatível com o PCI Express™ a uma rede Gigabit Ethernet. Os adaptadores Broadcom NetXtreme Gigabit Ethernet incorporam uma tecnologia que transfere dados a uma taxa máxima de 1 gigabit por segundo — 10 vezes a taxa dos adaptadores Fast Ethernet.

Ao usar o software de formação de equipes da Broadcom, você pode dividir sua rede em LANs virtuais (VLANs), bem como agrupar vários adaptadores de rede em equipes para fornecer o equilíbrio de carga de rede e a funcionalidade de tolerância a falhas. Consulte [Formação de equipes](#) e [Broadcom Gigabit Ethernet Teaming Services](#) para obter informações detalhadas sobre formação de equipes. Consulte [LANs virtuais](#), para obter uma descrição de VLANs. Consulte [Configuração de equipes](#) para obter instruções sobre como configurar equipes e criar VLANs em sistemas operacionais Windows.

Recursos

A seguir, há uma lista dos recursos do adaptador Broadcom NetXtreme Gigabit Ethernet para todos os sistemas operacionais suportados:

- Transceptores quad integrados 10/100/1000BASE-T e 1000BASE-X/SGMII 1,25 Gbaud SerDes
- Energy Efficient Ethernet™ compatível com o padrão IEEE 802.3az-2010
- Cláusula 73 de autonegociação da IEEE 802.3ap
- MACs full-duplex/half-duplex 10/100/1000BASE-T Quad
- MACs full-duplex/half-duplex 1000BASE-X/SGMII Quad
- Automatic MDI crossover
- x4 PCI Express v2,0 a 5 GT/s ou 2,5 GT/s
- Capacidades de MSI e MSI-X — vetores de até 17 MSIX
- Suporte de virtualização de E/S para VMware NetQueue e Microsoft VMQ
 - 17 filas de recepção e 16 filas de transmissão
 - 17 vetores do MSI-X compatíveis por interrupção de fila para o host
- Vetor de MSI-X flexível para transmitir/receber associação de fila
- TLP Processing Hint (TPH) ECN para a especificação básica do PCI Express v2.0
- Redefinição do nível de função
- Receive Side Scaling (RSS) com suporte ao vetor MSI-X por fila e suporte para o UDP RSS hash type
- Transmit Side Scaling (TSS) e fila de multi-Tx com suporte ao vetor MSI-X por fila
- Suporte a quadros Jumbo por uma carga de até 9600 bytes
- Suporte a LAN Virtual (VLAN) — IEEE 802.1q com marcação para VLAN
- Soma de verificação offload TCP, IP, UDP
- Large Send Offload (LSO), TCP Segmentation Offload (TSO)
- Auxílio de hardware para implementações de sincronização de tempo em conformidade com IEEE 1588 e IEEE 802.1AS
- Controle de fluxo em conformidade com IEEE 802.3x
- Interface SMBus 2.0
- Estatísticas para SNMP MIB II, MIB semelhante a Ethernet e Ethernet MIB (IEEE 802.3z, cláusula 30)
- Compatível com gerenciamento de energia ACPI
- Gerenciamento de energia avançado por uma Unidade Central de Gerenciamento de Energia (CPMU)
- Controlador do regulador de chaveamento integrado eficiente
- Monitor de temperatura on-chip
- Suporte ao CLKREQ do PCI Express
- Power Management Offload (PM Offload)
- Flash serial e suporte ao EEPROM NVRAM; configuração automática do flash
- Detecção e correção de erros de ECC no SRAM interno
- Suporte à verificação de limite de JTAG

Gerenciamento de energia

Wake on LAN (Magic Packet, Wake Up Frame, padrão específico) é suportado.



Nota: A velocidade da conexão do adaptador quando o sistema está inativo, aguardando um sinal de ativação, é de 10 Mbps ou 100 Mbps, mas pode voltar a 1000 Mbit/s quando o sistema é ativado e executado, se conectado a um switch com capacidade de 1000 Mbps. Os sistemas destinados a utilizar Wake on LAN (WOL) devem ser conectados a um switch com capacidade de velocidade de 1000 e 10/100 Mbps.

Frequência de interrupção adaptativa

O driver do adaptador ajusta, de forma inteligente, a frequência de interrupção do host, com base nas condições de tráfego a fim de aumentar a produtividade geral do aplicativo. Quando o tráfego é pequeno, o driver do adaptador interrompe o host para cada pacote recebido, minimizando a latência. Quando o tráfego é intenso, o adaptador emite uma interrupção de host para vários pacotes de entrada, mantendo os ciclos da CPU do host.

Canais DMA duplos

A interface PCIe nos adaptadores Broadcom NetXtreme Gigabit Ethernet contém dois canais DMA independentes para operações simultâneas de leitura e gravação.

ASIC com processador RISC incorporado

O controle central dos adaptadores Broadcom NetXtreme Gigabit Ethernet reside em um ASIC de alto desempenho, altamente integrado. O ASIC inclui um processador RISC. Essa funcionalidade permite adicionar novos recursos à placa e de adaptá-la às futuras exigências da rede por meio de downloads de software.

Operações de gerenciamento NetXtreme do Broadcom como DMTF, SMASH, DASH e transferência NC-SI são executadas em um mecanismo processador de aplicativos de alto desempenho (APE), que é um mecanismo separado do mecanismo de processamento de rede.

Broadcom Advanced Control Suite

O Broadcom Advanced Control Suite (BACS), um componente do software de formação de equipes Broadcom, é um utilitário integrado que fornece informações úteis sobre cada adaptador de rede instalado no sistema. O utilitário BACS também permite executar análises, diagnósticos e testes detalhados sobre cada adaptador, bem como modificar valores de propriedade e visualizar estatísticas de tráfego de cada adaptador. O BACS é usado nos sistemas operacionais Windows para configurar equipes e adicionar VLANs. Consulte [Uso do Broadcom Advanced Control Suite](#) para obter informações e instruções detalhadas.

Ambientes operacionais suportados

O adaptador Broadcom NetXtreme Gigabit Ethernet oferece suporte de software aos seguintes sistemas operacionais:

- Microsoft® Windows® (de 32 e 64 bits estendidos)
- Linux® (de 32 e 64 bits estendidos)
- VMware
- Oracle Solaris

Link de rede e indicação de atividade

Para conexões Ethernet com fio de cobre, o estado do link e a atividade de rede são indicados pelos LEDs no conector RJ-45, conforme descrito em [Tabela 1: "Link de rede e Atividade indicados pelos LEDs de porta RJ-45," na página 13](#). O Broadcom Advanced Control Suite também fornece informações sobre o status do link e da atividade de rede (consulte [Informações sobre o Adaptador de Visualização](#)).

Tabela 1. Link de rede e Atividade indicados pelos LEDs de porta RJ-45

LED de porta	Estado do LED	Estado da rede
LED de link	OFF	Nenhum link (cabo desconectado)
	Aceso continuamente	Link
LED de atividade	OFF	Nenhuma atividade de rede
	Piscando	Atividade de rede

Seção 2: Formação de equipes

- [Visão geral](#)
- [Equilíbrio de carga e tolerância a falhas](#)



Nota: Consulte [Broadcom Gigabit Ethernet Teaming Services](#) para obter informações detalhadas sobre os tópicos a seguir:

- Glossário de termos e acrônimos
- Conceitos de formação de equipes
- Componentes de software
- Requisitos de hardware
- Recursos suportados pelo tipo de equipe
- Seleção de um tipo de equipe
- Mecanismos de formação de equipes
- Arquitetura
- Tipos de equipe
- Suporte de driver pelo sistema operacional
- Velocidades de formação de equipes suportadas
- Formação de equipes e outros recursos avançados de rede
- Considerações gerais de rede
- Considerações do aplicativo
- Resolução de problemas de formação de equipes
- Perguntas frequentes
- Mensagens de log de evento

Visão geral

A formação de equipes de adaptadores permite agrupar adaptadores de rede para que funcionem como uma equipe. Os benefícios da formação de equipes incluem permitir associação a VLANs, proporcionando equilíbrio de cargas entre adaptadores e oferecendo tolerância a falhas. Esses benefícios podem ser combinados de forma que você possa acoplar os recursos do equilíbrio de cargas para equilibrar as cargas entre os membros e a capacidade de empregar um limite de falha, fazendo com que a equipe participe de diferentes VLANs.

O Broadcom Advanced Server Program (BASP) é o software de formação de equipes Broadcom. Para os sistemas operacionais Windows, o BASP é executado no utilitário [Broadcom Advanced Control Suite \(BACS\)](#). Para sistemas operacionais Linux, a formação de equipes é feita com a vinculação do canal (consulte [Formação de equipes com vinculação de canal](#)).

O BASP suporta quatro tipos de equipes de equilíbrio de carga:

- Smart Load Balancing e Limite de falha
- Agregação de link (802.3ad)
- Trunking genérico (FEC/GEC)/802.3ad-Draft Static
- SLB (Desativar reserva automática).

Equilíbrio de carga e tolerância a falhas

A formação de equipes oferece equilíbrio de carga de tráfego e tolerância a falhas (operação redundante do adaptador no caso de falha na conexão de rede). Quando vários adaptadores estão instalados no mesmo sistema, eles podem ser agrupados em até 16 equipes.

Cada equipe pode ser formada por até oito adaptadores, com um adaptador usado como reserva para tipos de equipe Equilíbrio de carga avançado e Limite de falha (SLB) ou SLB (Desativar reserva automática). Se o tráfego não for identificado em nenhuma das conexões dos membros das equipes do adaptador por uma falha do adaptador ou do switch, a distribuição da carga será redistribuída entre os membros restantes da equipe com conexão ativa. Se todos os adaptadores primários falharem, o tráfego será distribuído para o adaptador de reserva. As sessões já existentes são mantidas, e não há nenhum impacto para o usuário.

Tipos de equipe

Os tipos disponíveis de equipes para os sistemas operacionais suportados são exibidos na tabela a seguir:

Tabela 2. Tipos de equipe

Sistema operacional	Tipos disponíveis de equipes
Windows Server 2008 e Windows Server 2012	Smart Load Balancing e Limite de falha Agregação de link (802.3ad) Trunking genérico (FEC/GEC)/802.3ad-Draft Static SLB (Desativar reserva automática). NOTA: O Windows Server 2012 oferece o suporte interno para formação de equipes chamado NIC Teaming. Não é recomendável que os usuários ativem equipes usando o NIC Teaming e o BASP ao mesmo tempo, nos mesmos adaptadores.
Linux	Os adaptadores de equipe que usam o módulo kernel de vinculação e uma interface de vinculação do canal. Consulte a documentação do Linux para obter mais informações.

Smart Load Balancing™ e Limite de falha

Smart Load Balancing™ e Limite de falha é a implementação de equilíbrio de carga da Broadcom com base no fluxo de IP. Esse recurso oferece suporte a equilíbrio de tráfego IP em vários adaptadores (membros da equipe), de forma bidirecional. Neste tipo de equipe, todos os adaptadores da equipe possuem endereços MAC separados. Este tipo de equipe oferece detecção automática de falhas e limite de falhas dinâmico a outros membros da equipe ou a um membro de reserva. Isso é feito independentemente do protocolo da camada 3 (IP); mas funciona com switches já existentes das camadas 2 e 3. Nenhuma configuração de switch (por exemplo, entroncamento, agregação de link) é necessária para que este tipo de equipe funcione.



OBSERVAÇÕES:

- Se o LiveLink™ não é ativado durante a configuração de equipes SLB, a desativação do protocolo Spanning Tree no switch ou na porta é recomendada. Isso minimiza o tempo de inatividade devido à determinação do loop da árvore de spanning em caso de evento de limite de falha. O LiveLink reduz tais problemas.
- Se um membro da equipe for vinculado a 1000 Mbit/s, e um outro membro da equipe for vinculado a 100 Mbit/s, a maioria do tráfego será tratada pelo membro da equipe de 1000 Mbit/s.

Agregação de link (802.3ad)

Este modo suporta a agregação de link e está de acordo com a especificação IEEE 802.3ad (LACP). O software de configuração permite configurar dinamicamente os adaptadores que devem participar de uma determinada equipe. Se o parceiro do link não for corretamente definido para a configuração de link 802.3ad, os erros serão detectados e anotados. Com esse modo, todos os adaptadores da equipe são configurados para receber pacotes do mesmo endereço MAC. O esquema de equilíbrio de carga de saída é determinado pelo nosso driver BASP. O parceiro do link da equipe determina o esquema do equilíbrio de carga para pacotes de entrada. Neste modo, pelo menos um dos parceiros de link deve estar no modo ativo.

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

O tipo de equipe Trunking genérico (FEC/GEC)/802.3ad-Draft Static é semelhante ao tipo de equipe da Agregação de link (802.3ad) em que todos os adaptadores da equipe são configurados para receber pacotes para o mesmo endereço MAC. O tipo de equipe Trunking genérico (FEC/GEC)/802.3ad-Draft Static, no entanto, não oferece suporte a LACP ou ao protocolo de marcador. Esse tipo de equipe suporta vários ambientes em que parceiros de link do adaptador são configurados estaticamente para suportar um mecanismo de trunking proprietário. Por exemplo, esse tipo de equipe poderia ser utilizado para suportar o OpenTrunk da Lucent ou o Fast EtherChannel (FEC) da Cisco. Basicamente, esse tipo de equipe é uma versão light do tipo de equipe Agregação de link (802.3ad). Essa abordagem é muito mais simples, pois não há um protocolo formalizado de controle de agregação de link (LACP). Assim como com os outros tipos de equipes, a criação de equipes e a alocação de adaptadores físicos a várias equipes são feitas de forma estática, por meio de um software de configuração do usuário.

O tipo de equipe Trunking genérico (FEC/GEC)/802.3ad-Draft Static suporta o equilíbrio de carga e o limite de falha para tráfego de saída e de entrada.

SLB (Desativar reserva automática)

O tipo de equipe SLB (Desativar reserva automática) é idêntico ao Smart Load Balancing e Limite de falha, com a exceção de que quando o membro em espera está ativo, se um membro primário for reativado, a equipe continuará a utilizar o membro em espera em vez de voltar para o membro primário.

Se qualquer adaptador primário atribuído à equipe for desativado, a equipe funciona como um tipo de equipe Smart Load Balancing e Limite de falha no qual ocorre a reserva automática.

Todas as interfaces primárias em uma equipe participam das operações de equilíbrio de carga, enviando e recebendo uma parte do tráfego total. As interfaces de reserva assumem o controle quando todas as interfaces primárias perdem seus links.

A formação de equipes de limite de falha fornece operação redundante do adaptador (tolerância a falhas) no caso de falha da conexão de rede. Se o adaptador primário em uma equipe é desconectado devido a uma falha do adaptador, do cabo ou da porta do switch, o membro secundário da equipe torna-se ativo, redirecionando o tráfego de entrada e de saída originalmente atribuído ao adaptador primário. As sessões serão mantidas, sem provocar impacto ao usuário.

Limitações dos tipos de equipes Smart Load Balancing e Limite de falha/SLB (Desativar reserva automática)

Smart Load Balancing™ (SLB) é um esquema específico do protocolo.

Tabela 3: Smart Load Balancing (Equilíbrio de carga avançado)

<i>Sistema operacional</i>	<i>Limite de falha/Reserva — Todos da Broadcom</i>	<i>Limite de falha/Reserva — Vários fornecedores</i>
Protocolo	IP	IP
Windows Server 2008	S	S
Windows Server 2008 R2	S	S
Windows Server 2012	S	S
<i>Sistema operacional</i>	<i>Equilíbrio de carga — Todos da Broadcom</i>	<i>Equilíbrio de carga — Vários fornecedores</i>
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

Legenda: S = sim
N = não
N/S = não suportado

O tipo de equipe SLB funciona com todos os switches de Ethernet sem configurar as portas do switch para um modo de trunking especial. Apenas o tráfego IP terá equilíbrio de carga nas direções de entrada e saída. Outros pacotes de protocolo são enviados e recebidos apenas por meio de uma interface primária. O limite de falha para um tráfego não-IP é suportado somente para adaptadores da Broadcom. O tipo de equipe Trunking genérico exige que o switch Ethernet suporte alguma forma do modo de entroncamento de porta (por exemplo, Gigabit EtherChannel da Cisco ou o modo de Agregação de link de outro fornecedor de switch). O tipo de equipe Trunking genérico é independente de protocolo, e todo tráfego deve ter equilíbrio de carga e tolerância a falhas.



Nota: Se o LiveLink™ não é ativado durante a configuração de equipes, a desativação do protocolo Spanning Tree no switch é recomendada. Isso minimiza o tempo de inatividade devido à determinação do loop Spanning Tree quando ocorre um evento de limite de falha. O LiveLink reduz tais problemas.

Funcionalidade LiveLink™

A funcionalidade LiveLink™ é um recurso do BASP disponível apenas para o tipo de formação de equipes Smart Load Balancing™ e Failover. O objetivo do LiveLink é detectar a conectividade da rede além do switch e rotear o tráfego apenas por meio dos membros da equipe que tenham uma conexão ativa. Essa função é realizada por meio do software de formação de equipes (consulte [Configuração do LiveLink para uma equipe Smart Load Balancing e Limite de falha e SLB \(Desativar reserva automática\)](#)). O software de formação de equipes sonda periodicamente (emite um pacote de link de cada membro da equipe) um ou mais adaptadores de rede do alvo especificado. O(s) alvo(s) de sondagem responde(m) quando recebe o pacote de link. Se um membro da equipe não detectar uma resposta em um período de tempo após um número especificado de tentativas, o software de formação de equipes interrompe a passagem do tráfego através daquele membro da equipe. Mais tarde, se esse membro da equipe começar a detectar uma resposta do alvo de sondagem, isso indica que o link foi restaurado, e o software de formação de equipes retoma automaticamente a passagem do tráfego através deste membro da equipe. O LiveLink funciona apenas com TCP/IP.

O recurso LiveLink™ é suportado nos sistemas operacionais Windows de 32 bits e 64 bits. Para obter informações sobre funções similares nos sistemas operacionais Linux, consulte a seção Vinculação do Canal na documentação do Linux.

Suporte para Formação de equipes e Large Send Offload/Checksum Offload

As propriedades Large Send Offload (LSO) e Checksum Offload só são ativadas para uma equipe quando todos os membros suportarem e estiverem configurados para o recurso.

Seção 3: Broadcom Gigabit Ethernet Teaming Services

- [Introdução](#)
- [Mecanismos de formação de equipes](#)
- [Formação de equipes e outras propriedades avançadas de rede](#)
- [Considerações gerais de rede](#)
- [Considerações do aplicativo](#)
- [Resolução de problemas de formação de equipes](#)
- [Perguntas frequentes](#)
- [Mensagens de log de evento](#)

Introdução

- [Glossário](#)
- [Conceitos de formação de equipes](#)
- [Componentes de software](#)
- [Requisitos de hardware](#)
- [Recursos suportados pelo tipo de equipe](#)
- [Seleção de um tipo de equipe](#)

Esta seção descreve a tecnologia e as considerações sobre implementação ao se trabalhar com os serviços de formação de equipes da rede, através do software Broadcom enviado com os sistemas. O objetivo do serviço de formação de equipes é fornecer tolerância a falhas e agregação de link através de uma equipe de dois ou mais adaptadores. As informações deste documento são fornecidas para auxiliar os profissionais de TI durante a implantação e a solução de problemas dos aplicativos do sistema que necessitam de equilíbrio de carga de rede e tolerância a falhas.

Glossário

Tabela 4: Glossário

Item	Definição
ARP	Address Resolution Protocol (Protocolo de Resolução de Endereços)
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program (driver intermediário)
DNS	domain name service (serviço de nome de domínio)
G-ARP	Gratuitous Address Resolution Protocol (Protocolo de Resolução de Endereços Gratuito)
Trunking genérico (FEC/GEC)/ 802.3ad-Draft Static	Equilíbrio de carga e tipo de limite de falha da equipe dependente de switch no qual o driver intermediário gerencia o tráfego de saída e o switch gerencia o tráfego de entrada.
HSRP	Hot Standby Router Protocol (Protocolo do Roteador de Reserva)
ICMP	Internet Control Message Protocol (Protocolo de Mensagem de Controle da Internet)
IGMP	Internet Group Management Protocol (Protocolo de Gerenciamento de Grupo da Internet)
IP	Internet Protocol (Protocolo de Internet)
LACP	Link Aggregation Control Protocol (Protocolo de Controle de Agregação de Link)
Agregação de link (802.3ad)	Equilíbrio de carga e tipo de limite de falha da equipe com LACP dependente de switch, no qual o driver intermediário gerencia o tráfego de saída e o switch gerencia o tráfego de entrada.
LOM	LAN on Motherboard (LAN na Placa-mãe)
MAC	media access control (controle de acesso de mídia)
NDIS	Network Driver Interface Specification (Especificação da Interface de Driver de Rede)
NLB	Network Load Balancing (Equilíbrio de Carga de Rede) (Microsoft)

Tabela 4: Glossário

Item	Definição
PXE	Preboot Execution Environment (Ambiente de Execução de Pré-inicialização)
RAID	Array redundante de discos baratos
Smart Load Balancing e Limite de falha	Tipo de limite de falha da equipe independente do switch no qual o membro da equipe primária trata todo o tráfego de entrada e saída, enquanto o membro da equipe em espera fica ocioso até que ocorra um evento de limite de falha (por exemplo, ocorrer a perda do link). O driver intermediário (BASP) gerencia o tráfego de entrada/saída.
Smart Load Balancing (SLB) (Equilíbrio de Carga Avançado)	Equilíbrio de carga e tipo de limite de falha da equipe independente do switch, no qual o driver intermediário gerencia o tráfego de saída/entrada.
TCP	Transmission Control Protocol (Protocolo de Controle de Transmissão)
UDP	User Datagram Protocol (Protocolo de Datagrama do Usuário)
WINS	Windows name service (Nome de serviço do Windows)
WLBS	Windows Load Balancing Service (Serviço de Equilíbrio de Carga do Windows)

Conceitos de formação de equipes

- [Endereçamento de rede](#)
- [Endereços de rede e da formação de equipes](#)
- [Descrição dos tipos de formação de equipes](#)

Endereçamento de rede

Para entender como a formação de equipes funciona, é importante entender como as comunicações de nó funcionam em uma rede Ethernet. Este documento pressupõe que o leitor esteja familiarizado com as noções básicas de IP e de comunicações de rede Ethernet. As informações a seguir fornecem uma visão geral de alto nível sobre os conceitos de endereçamento de rede utilizados em uma rede Ethernet.

Cada interface de rede Ethernet em uma plataforma de host, como um sistema de computador necessita de um endereço exclusivo globalmente da Camada 2 e pelo menos um endereço exclusivo globalmente da Camada 3. A Camada 2 é a Camada de link de dados e a Camada 3 é a Camada de rede, conforme definido no modelo OSI. O endereço da Camada 2 é atribuído ao hardware e geralmente é mencionado como o endereço MAC ou endereço físico. Esse endereço é pré-programado na fábrica e armazenado em NVRAM em uma placa de interface de rede ou na placa-mãe do sistema de uma interface LAN incorporada. Os endereços da Camada 3 são mencionados como o protocolo ou endereço lógico atribuído à pilha do software. IP é um exemplo de protocolo de 3 camadas. Além disso, a Camada 4 (Camada de transporte) usa os números da porta para cada protocolo de nível superior da rede, como Telnet ou FTP. Esses números de porta são usados para diferenciar os fluxos de tráfego nos aplicativos. Os protocolos da Camada 4, como TCP ou UDP geralmente são mais usados nas redes atuais. A combinação de endereço IP e porta TCP é chamada soquete.

Os dispositivos Ethernet comunicam-se com outros dispositivos Ethernet usando o endereço MAC, não o endereço IP. No entanto, a maioria dos aplicativos trabalha com um nome de host que é convertido para um endereço IP através de um Serviço de nomeação, como WINS e DNS. Portanto, é necessário um método de identificação de endereço MAC atribuído ao endereço IP. O Protocolo de Resolução de Endereços de uma rede IP fornece este mecanismo. Um endereço de difusão ponto a ponto corresponde a um endereço MAC único ou um endereço IP único. Um endereço de difusão é enviado a todos os dispositivos de uma rede.

Endereços de rede e da formação de equipes

Uma equipe de adaptadores funciona como uma interface de rede virtual única e não exibe nenhuma diferença para outros dispositivos de rede que um adaptador não agrupado. Um adaptador de rede virtual anuncia uma Camada 2 única e um ou mais endereços da Camada 3. Quando o driver da formação de equipes é inicializado, ele seleciona um endereço MAC de um dos adaptadores físicos que compõem a equipe, para ser o endereço MAC da equipe. Este endereço geralmente é obtido do primeiro adaptador que foi inicializado pelo driver. Quando o sistema armazena a equipe que recebe uma solicitação de ARP, ele seleciona um endereço MAC entre os adaptadores físicos da equipe para usar como o endereço MAC de origem na Resposta do ARP. Nos sistemas operacionais do Windows, o comando IPCONFIG/all mostra o endereço IP e MAC do adaptador virtual e não dos adaptadores físicos individuais. O endereço IP do protocolo é atribuído à interface da rede virtual e não aos adaptadores físicos individuais.

Para modos de equipes independentes do switch, todos os adaptadores físicos que compõem um adaptador virtual devem usar o endereço único MAC atribuído a eles ao transmitirem os dados. Ou seja, os quadros que são enviados por cada um dos adaptadores físicos na equipe devem usar um endereço MAC único para serem compatíveis com IEEE. É importante observar que as entradas de cache de ARP não são obtidas dos frames recebidos, mas apenas das solicitações e das respostas de ARP.

Descrição dos tipos de formação de equipes

- [Smart Load Balancing e Limite de falha](#)
- [Trunking genérico](#)
- [Agregação de link \(IEEE 802.3ad LACP\)](#)
- [SLB \(Desativar reserva automática\).](#)

Há três métodos para classificar os tipos de formação de equipes suportados:

- Um é baseado na configuração da porta do switch, se ela também deve corresponder ao tipo de formação de equipe do adaptador.
- A segunda é baseada na funcionalidade da equipe, se ela suporta equilíbrio de carga e limite de falha ou apenas limite de falha.
- A terceira é baseada no Protocolo de Controle de Agregação de Link, se ele é usado ou não.

Tabela 5 mostra um resumo dos tipos de formação de equipe e sua classificação.

Tabela 5: Tipos de formação de equipe disponíveis

Tipo de formação de equipe	Dependente do switch (O switch deve suportar um tipo de equipe específico)	O suporte do Protocolo de Controle de Agregação de Link é necessário no switch	Equilíbrio de carga	Limite de falha
Smart Load Balancing and Limite de falha (com dois a oito membros na equipe de equilíbrio de carga)			•	•
SLB (Desativar reserva automática).				•
Agregação de link (802.3ad)	•	•	•	•
Trunking genérico (FEC/GEC)/802.3ad-Draft Static	•		•	•

Smart Load Balancing e Limite de falha

O tipo de equipe Smart Load Balancing™ e Limite de falha oferece equilíbrio de carga e limite de falha quando configurado para equilíbrio de carga e somente limite de falha, quando configurado para tolerância a falhas. Esse tipo de equipe funciona com qualquer switch Ethernet e não exige nenhuma configuração de trunking no switch. A equipe anuncia vários endereços MAC e um ou mais endereços IP (ao usar os endereços IP secundários). O endereço MAC da equipe é selecionado da lista de membros de equilíbrio de carga. Quando o sistema recebe uma solicitação de ARP, a pilha de software de rede sempre envia uma Resposta de ARP com o endereço MAC da equipe. Para iniciar o processo de equilíbrio de carga, o driver de formação de equipe modifica esta Resposta de ARP, alterando o endereço de origem de MAC para corresponder a um dos adaptadores físicos.

O Smart Load Balancing permite tanto a transmissão como o recebimento de equilíbrio de carga com base no endereço IP da Camada 3/Camada 4 e número de porta TCP/UDP. Em outras palavras, o equilíbrio de carga não é feito em nível de

byte ou quadro, mas com base na sessão TCP/UDP. Essa metodologia é necessária para manter em ordem o envio de quadros que pertencem a mesma conversão de soquete. O equilíbrio de carga é suportado em 2 a 8 portas. Essas portas podem incluir qualquer combinação de adaptadores adicionados e dispositivos LAN na Placa-mãe (LOM). O equilíbrio de carga de transmissão é atingido através da criação de uma tabela de hash usando os endereços IP de origem e de destino e os números de porta TCP/UDP. A mesma combinação de endereços IP de destino e origem e números de porta TCP/UDP, geralmente gera o mesmo índice de hash e, portanto, aponta para a mesma porta da equipe. Quando uma porta é selecionada para executar todos os quadros de um determinado soquete, o endereço MAC exclusivo do adaptador físico é incluído no quadro e não no endereço MAC da equipe. Isso é necessário para cumprir a norma IEEE 802.3. Se dois adaptadores fazem uma transmissão usando o mesmo endereço MAC, pode ocorrer uma situação de endereço MAC duplicado, que o switch não conseguiria tratar.

O equilíbrio de carga de recebimento é atingido através de um driver intermediário pelo envio de ARPs gratuitos, em uma base cliente por cliente, usando o endereço de difusão ponto a ponto de cada cliente como o endereço de destino da solicitação de ARP (também conhecido como ARP direcionado). Isso é considerado equilíbrio de carga do cliente e não equilíbrio de carga de tráfego. Quando o driver intermediário detecta um desequilíbrio de carga significativa entre os adaptadores físicos em uma equipe SLB, ele gera G-ARPs para redistribuir os quadros de entrada. O driver intermediário (BASP) não responde solicitações de ARP; somente a pilha do protocolo de software fornece a Resposta de ARP. É importante entender que o equilíbrio de carga de recebimento é uma função do número de clientes que estão se conectando ao sistema através da interface da equipe.

O equilíbrio de carga de recebimento tenta carregar o tráfego de entrada de equilíbrio para as máquinas do cliente, através das portas físicas da equipe. Ele usa um ARP modificado gratuito para anunciar um endereço MAC diferente para o endereço IP da equipe no endereço físico e de protocolo do remetente. Este G-ARP é de difusão ponto a ponto com o endereço MAC e IP de uma máquina do cliente no endereço físico alvo e de protocolo respectivamente. Isso faz com que o cliente alvo atualize seu cache de ARP com um novo mapa de endereço MAC para o endereço IP da equipe. O G-ARPs não são de difusão, pois isso faria com que todos os clientes enviassem seus tráfegos à mesma porta. Como consequência, os benefícios atingidos através do equilíbrio de carga do cliente poderiam ser eliminados e poderiam causar envio de quadros fora de ordem. Esse esquema de equilíbrio de carga de recebimento funciona, desde que todos os clientes e o sistema agrupado estejam na mesma rede ou domínio de transmissão.

Quando os clientes e o sistema estão em sub-redes diferentes e o tráfego de entrada tem que passar por um roteador, o tráfego recebido destinado ao sistema não tem equilíbrio por carga. O adaptador físico que o driver intermediário selecionou para executar o fluxo de IP executará todo o tráfego. Quando o roteador envia um quadro ao endereço IP da equipe, ele transmite uma solicitação de ARP (se não estiver no cache de ARP). A pilha do software do servidor gera uma resposta de ARP com o endereço MAC da equipe, mas o driver intermediário modifica a resposta de ARP e a envia para um adaptador físico específico, estabelecendo o fluxo daquela sessão.

O motivo é que o ARP não é um protocolo roteável. Ele não tem um cabeçalho IP e, por isso, não é enviado para o roteador ou para o gateway padrão. O ARP é apenas um protocolo de sub-rede local. Além disso, em virtude do G-ARP não ser um pacote de difusão, o roteador não o processará e não atualizará seu próprio cache de ARP.

A única forma que o roteador processa um ARP destinado para outro dispositivo de rede é se ele tiver Proxy ARP ativado e o host não tiver gateway padrão. Isso é muito raro e não recomendado para a maioria dos aplicativos.

O tráfego de transmissão através de um roteador terá equilíbrio por carga porque o equilíbrio de carga de transmissão é baseado no endereço IP de origem e destino e no número da porta TCP/UDP. Considerando que os roteadores não alteram o endereço IP de origem e destino, o algoritmo de equilíbrio de carga funciona conforme planejado.

Configurar os roteadores para Protocolo do Roteador de Reserva (HSRP) não permite que o equilíbrio de carga de recebimento ocorra na equipe do adaptador. Em geral, o HSRP permite que dois roteadores atuem como um roteador, anunciando um endereço MAC virtual e um endereço IP virtual. Um roteador físico é a interface ativa, enquanto o outro é

reserva. Embora o HSRP também possa carregar nós compartilhados (usando diferentes gateways padrão nos nós do host) através de vários roteadores nos grupos HSRP, ele sempre aponta para o endereço MAC primário da equipe.

Trunking genérico

Trunking genérico é um modo de formação de equipes auxiliado por switch e requer portas de configuração nas duas extremidades do link: interfaces do servidor e portas do switch. Geralmente é chamado de Cisco Fast EtherChannel ou Gigabit EtherChannel. Além disso, o trunking genérico suporta implementações semelhantes de outros OEMs do switch, como Extreme Networks Load Sharing e Bay Networks ou modo estático de Agregação de Link IEEE 802.3ad. Nesse modo, a equipe anuncia um endereço MAC e um endereço IP quando a pilha do protocolo responde às solicitações de ARP. Além disso, cada adaptador físico da equipe usa o mesmo endereço MAC da equipe ao transmitir os quadros. Isso é possível desde que o switch na outra extremidade do link conheça o modo de formação de equipe e saiba que tratará o uso de um endereço MAC único por cada porta da equipe. A tabela de envio do switch refletirá o entroncamento como uma porta virtual única.

Nesse modo de equipe, o driver intermediário controla o equilíbrio de carga e o limite de falha somente para o tráfego de saída, enquanto que o tráfego de entrada é controlado pelo firmware e hardware do switch. Como no Smart Load Balancing, o driver intermediário BASP usa os endereços de origem e destino IP/TCP/UDP para equilíbrio de carga do tráfego de transmissão do servidor. A maioria dos switches implementa um hash XOR do endereço MAC de origem e de destino.

Agregação de link (IEEE 802.3ad LACP)

Agregação de link é semelhante ao trunking genérico, com exceção que ela usa o Protocolo de Controle de Agregação de Link para negociar as portas que constituirão a equipe. O LACP deve ser ativado nas duas extremidades do link da equipe a ser operacional. Se o LACP não estiver disponível nas duas extremidades do link, o 802.3ad fornece uma agregação manual que requer que apenas as duas extremidades do link estejam em um estado de link ativo. Em virtude da agregação manual fornecer a ativação de um link do membro sem executar as trocas de mensagem de LACP, ela não deve ser considerada confiável e avançada como um link de LACP negociado. O LACP determina automaticamente quais links do membro podem ser agregados e, em seguida, agrega os links. Ele fornece a adição e remoção controlada de links físicos para a agregação de link, de forma que nenhum quadro seja perdido ou duplicado. A remoção dos membros do link de agregação é fornecida pelo protocolo do marcador que pode ser ativado opcionalmente para links de agregação ativados do Protocolo de Controle de Agregação de Link (LACP).

O grupo de Agregação de Link anuncia um endereço MAC único para todas as portas do entroncamento. O endereço MAC do Agregador pode ser os endereços MAC de um dos MACS que constituem o grupo. O LACP e os protocolos do marcador usam um endereço de destino de difusão seletiva.

A função de controle de Agregação de link determina quais links podem ser agregados e liga as portas a uma função do Agregador no sistema e monitora as condições para determinar se é necessário uma alteração no grupo de agregação. A agregação de link combina a capacidade individual de vários links para formar um link virtual de alto desempenho. A falha ou substituição de um link em um entroncamento de LACP não causará perda de conectividade. O tráfego simplesmente apresentará falha para os links remanescentes no entroncamento.

SLB (Desativar reserva automática).

Esse tipo de equipe é idêntico ao tipo Smart Load Balance e Limite de Falha, com a exceção a seguir: quando o membro em espera está ativo, se um membro primário for reativado, a equipe continuará a utilizar o membro em espera em vez de voltar para o membro primário. Esse tipo de equipe é suportado somente em situações nas quais o cabo de rede é desconectado e reconectado ao adaptador de rede. Não é suportado em situações nas quais o adaptador é removido/instalado via Gerenciador de dispositivos ou PCI Hot-Plug.

Se qualquer adaptador primário atribuído à equipe for desativado, a equipe funciona como um tipo de equipe Smart Load Balancing e Limite de falha no qual ocorre a reserva automática.

Componentes de software

A formação de equipe é implementada através de um driver intermediário NDIS no ambiente do Sistema operacional do Windows. Esse componente de software trabalha com um driver de miniporta, a camada NDIS e a pilha do protocolo para ativar a arquitetura da formação de equipe (consulte [Figura 1](#)). O driver da miniporta controla o controlador de LAN do host diretamente para ativar funções como envios, recebimentos e interrupção de processamento. O driver intermediário ajusta-se entre o driver da miniporta e a camada do protocolo, multiplexando várias instâncias de driver e criando um adaptador virtual que parece um único adaptador para a camada NDIS. O NDIS fornece um conjunto de funções da biblioteca para ativar a comunicação entre os drivers da miniporta ou os drivers intermediários e a pilha do protocolo. Um endereço de protocolo como um endereço IP é atribuído a cada instância do dispositivo da miniporta, mas quando um driver intermediário é instalado, o endereço do protocolo é atribuído ao adaptador da equipe virtual e não aos dispositivos de miniporta individuais que compõem a equipe.

O suporte à formação de equipe do Broadcom é fornecido por três componentes do software individual que trabalham juntos e são suportados como um pacote. Quando um componente é atualizado, todos os outros componentes devem ser atualizados para as versões suportadas. [Tabela 6](#) descreve os três componentes do software e seus arquivos associados dos sistemas operacionais suportados.

Tabela 6: Componente de software de formação de equipes Broadcom

Componente de software	Nome do Broadcom	Windows	Linux
Driver da miniporta	Driver de base do Broadcom	b57nd60X.sys	tg3
Driver Intermediário	Broadcom Advanced Server Program (BASP)	Basp.sys	Vinculação
Interface de configuração do usuário	Broadcom Advanced Control Suite (BACS)	BACS	BACS CLI
Driver NDIS 6	Windows Vista e driver x86 mais atualizado Windows Vista e driver x64 mais atualizado	b57nd60x.sys b57nd60a.sys	Ausente

O utilitário Broadcom Advanced Control Suite (BACS) foi projetado para executar em sistemas operacionais Windows Server de 32 e 64 bits. O BACS é usado para configurar equilíbrio de carga e tolerância a falhas da equipe e VLANs. Além disso, ele exibe o endereço MAC, a versão do driver e informações de estado de cada adaptador de rede. O BACS também inclui um número de ferramentas de diagnóstico, como por exemplo: diagnóstico de hardware, teste de cabo e teste de topologia da rede.

Requisitos de hardware

- [Switch Ethernet](#)
- [Roteador](#)

Os diversos modos de formação de equipe descritos neste documento colocam determinadas restrições no equipamento de rede usado para conectar os clientes aos sistemas agrupados. Cada tipo de tecnologia de interconexão de rede tem um efeito sobre a formação de equipes, conforme nas seções a seguir.

Switch Ethernet

As switches Ethernet permitem uma rede Ethernet seja quebrada em vários domínios de broadcast. O switch é responsável pelo envio de pacotes Ethernet entre os hosts baseados unicamente nos endereços Ethernet MAC. Um adaptador de rede física que está conectado a um switch pode operar no modo half-duplex ou full-duplex.

Para suportar o Trunking genérico e a Agregação de link 802.3ad, um switch deve suportar especificamente cada funcionalidade. Se o switch não suportar esses protocolos, ainda pode ser usado no Smart Load Balancing.

Roteador

Um roteador é designado para rotear o tráfego de rede baseado na Camada 3 ou em protocolos superiores, embora ele também funcione como um dispositivo da Camada 2 com recursos de comutação. As portas de formação de equipe conectadas diretamente a um roteador não são suportadas.

Recursos suportados pelo tipo de equipe

Tabela 7 fornece uma comparação de recursos através dos tipo de formação de equipes suportados por NICs Broadcom. Use esta tabela para determinar o melhor tipo de equipe para seu aplicativo. O software de formação de equipe suporta até oito portas em uma equipe única e até 16 equipes em um sistema único. Essas equipes podem ser de qualquer combinação dos tipos de equipe suportados, mas cada equipe deve estar em uma rede ou sub-rede separada.

Tabela 7: Comparação dos tipos de equipe

Tipo de equipe	Tolerância a Falhas	Equilíbrio de carga	Trunking estático dependente do switch	Independente do switch Agregação de link dinâmico (IEEE 802.3ad)
Função	SLB com reserva ^a	SLB	Trunking genérico	Agregação de link
Número de portas por equipe (mesmo domínio de transmissão)	2–8	2–8	2–8	2–8
Número de equipes	16	16	16	16
Tolerância a falhas do adaptador	Sim	Sim	Sim	Sim
Tolerância a falhas do link do switch (mesmo domínio de transmissão)	Sim	Sim	Dependente do switch	Dependente do switch
Equilíbrio de carga TX	Não	Sim	Sim	Sim

Tabela 7: Comparação dos tipos de equipe (Cont.)

Tipo de equipe	Tolerância a Falhas	Equilíbrio de carga	Trunking estático dependente do switch	Independente do switch Agregação de link dinâmico (IEEE 802.3ad)
Equilíbrio de carga RX	Não	Sim	Sim (executado pelo switch)	Sim (executado pelo switch)
Requer switch compatível	Não	Não	Sim	Sim
Pulsos para verificar a conectividade	Não	Não	Não	Não
Mídia mista (adaptadores com mídia diferente)	Sim	Sim	Sim (dependente do switch)	Sim
Velocidades mistas (adaptadores que não suportam uma velocidade comum, mas podem operar em velocidades diferentes)	Sim	Sim	Não	Não
Velocidades mistas (adaptadores que suportam uma velocidade comum, mas podem operar em velocidades diferentes)	Sim	Sim	Não (deve ter a mesma velocidade)	Sim
Equilíbrios de carga TCP/IP	Não	Sim	Sim	Sim
Formação de equipes de fornecedor misto	Sim ^b	Sim ^b	Sim ^b	Sim ^b
Equilíbrios de carga não-IP	Não	Sim (somente tráfego de saída IPX)	Sim	Sim
Mesmo endereço MAC para todos os membros da equipe	Não	Não	Sim	Sim
Mesmo endereço IP para todos os membros da equipe	Sim	Sim	Sim	Sim
Equilíbrio de carga por endereço IP	Não	Sim	Sim	Sim
Equilíbrio de carga por endereço MAC	Não	Sim (usado para não-IP/IPX)	Sim	Sim

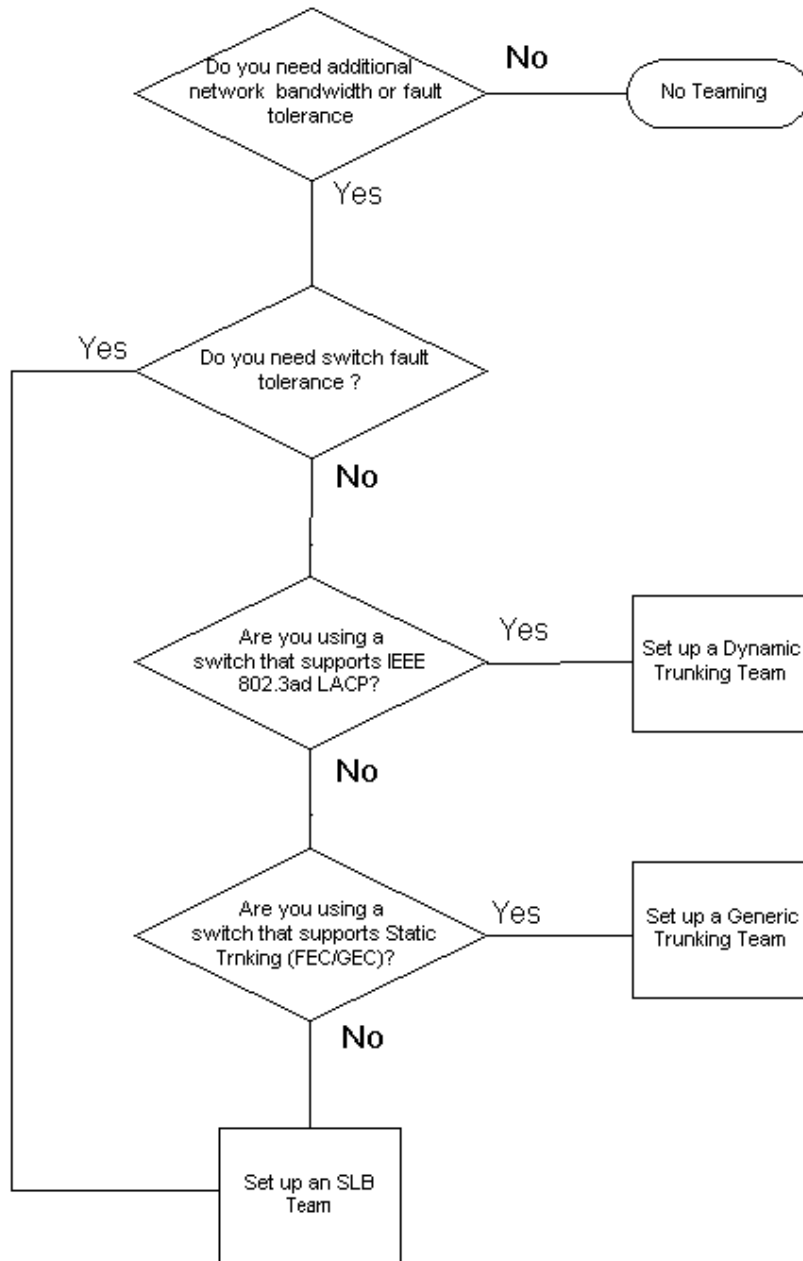
^a SLB com um membro primário e um membro em espera.

^b Requer pelo menos um adaptador Broadcom na equipe.

Seleção de um tipo de equipe

O fluxograma a seguir fornece o fluxo de decisão durante o planejamento da formação de equipes. O motivo principal para formação de equipes é a necessidade de largura de banda de rede adicional e tolerância a falhas. A formação de equipes oferece agregação de link e tolerância a falhas para atender a esses requisitos. A formação de equipe preferencial deve ser selecionada na seguinte ordem: Agregação de link como primeira opção, Trunking genérico como segunda opção e formação de equipe SBL como terceira opção ao usar switches não gerenciados ou switches que não suportam as duas primeiras opções. Se a tolerância a falhas for um requisito, então SLB é a única opção (consulte [Figura 1](#)).

Figura 1: Processo para seleção de um tipo de equipe



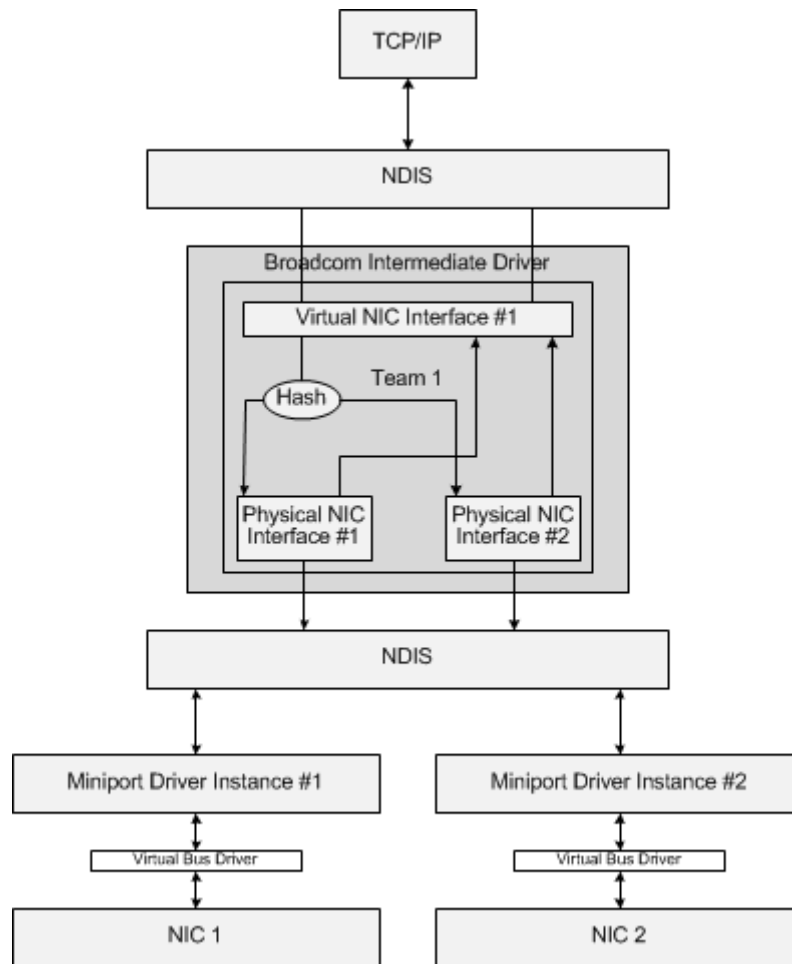
Mecanismos de formação de equipes

- [Arquitetura](#)
- [Suporte de driver pelo sistema operacional](#)
- [Velocidades de formação de equipes suportadas](#)

Arquitetura

O Broadcom Advanced Server Program é implementado como um driver intermediário NDIS (consulte [Figura 2](#)). Ele opera sob as pilhas de protocolo como TCP/IP e aparece como um adaptador virtual. Esse adaptador virtual herda o Endereço MAC da primeira porta inicializada da equipe. O endereço da Camada 3 também deve ser configurado para o adaptador virtual. A função principal do BASP é equilibrar o tráfego de entrada (de SLB) e o tráfego de saída (para todos os modos de formação de equipes) entre os adaptadores físicos instalados no sistema selecionado para formação de equipes. Os algoritmos de entrada e saída são independentes e ortogonais mutuamente. O tráfego de saída de uma sessão específica pode ser atribuído a uma determinada porta, enquanto seu tráfego de entrada pode ser atribuído a uma porta diferente.

Figura 2: Driver Intermediário



Fluxo do tráfego de saída

O driver intermediário da Broadcom gerencia o fluxo de tráfego de saída de todos os modos de formação de equipes. Para o tráfego de saída, cada pacote primeiro é classificado em um fluxo e, em seguida, distribuído para o adaptador físico selecionado para transmissão. A classificação do fluxo envolve um cálculo de hash eficiente em campos de protocolo conhecidos. O valor de hash resultante é usado para índice em uma Tabela de Hash de Fluxo de Saída. A Entrada de Hash de Fluxo de Saída contém o índice do adaptador físico selecionado responsável pela transmissão desse fluxo. O endereço MAC dos pacotes será modificado, em seguida, para o endereço MAC do adaptador físico selecionado. O pacote modificado é passado para o adaptador físico selecionado para transmissão.

Os pacotes TCP e UDP de saída são classificados usando as informações do cabeçalho das camadas 3 e 4. Este esquema melhora a distribuição de carga de serviços de protocolo populares da internet usando portas bem conhecidas como HTTP e FTP. Portanto, o BASP executa o equilíbrio de carga com base na sessão de TCP e não com base em pacote por pacote.

Nas Entradas de Hash do Fluxo de Saída, os contadores de estatística também são atualizados após a classificação. O mecanismo de equilíbrio de carga usa esses contadores para distribuir periodicamente os fluxos através das portas agrupadas. O caminho do código de saída foi designado para atingir simultaneamente da melhor maneira possível o local onde vários acessos simultâneos são permitidos para a Tabela de Hash do Fluxo de Saída.

Para protocolos diferentes de TCP/IP, o primeiro adaptador físico será sempre selecionado para pacotes de saída. A exceção é o Protocolo de Resolução de Endereços (ARP), que é tratado de forma diferente para atingir o equilíbrio de carga de entrada.

Fluxo de Tráfego de Entrada (Somente SLB)

O driver intermediário da Broadcom gerencia o fluxo do tráfego de entrada para o modo de equipe SLB. Diferente do equilíbrio de carga de saída, o equilíbrio de carga de entrada somente pode ser aplicado aos endereços IP que estão localizados na mesma sub-rede que o servidor de equilíbrio de carga. O equilíbrio de carga de entrada utiliza uma característica exclusiva do Protocolo de Resolução de Endereços (RFC0826), no qual cada host IP usa seu próprio cache ARP para encapsular o Datagrama de IP em um quadro Ethernet. O BASP manipula cuidadosamente a resposta do ARP para direcionar cada host IP para enviar o pacote de IP de entrada para o adaptador físico desejado. Portanto, o equilíbrio de carga de entrada é um esquema de planejamento avançado baseado no histórico estatístico dos fluxos de entrada. As novas conexões de um cliente ao servidor sempre ocorrem através do adaptador físico primário (porque a Resposta do ARP gerada pela pilha de protocolo do sistema operacional sempre associa o endereço IP lógico ao endereço MAC do adaptador físico).

Como na saída, há uma Tabela de Hash do Cabeçalho do Fluxo de Entrada. Cada entrada nesta tabela tem uma lista vinculada isoladamente e cada link (Entradas do Fluxo de Entrada) representa um host IP localizado na mesma sub-rede.

Quando um Datagrama de IP de entrada chega, a Entrada do Cabeçalho do Fluxo de Entrada apropriada é localizada através de hash do endereço IP de origem do Datagrama de IP. Os dois contadores estatísticos armazenados na entrada selecionada também são atualizados. Esses contadores são utilizados da mesma maneira que os contadores de saída, através do mecanismo de equilíbrio de carga periodicamente, para reatribuir os fluxos ao adaptador físico.

No caminho do código de entrada, a Tabela de Hash do Cabeçalho de Entrada também é designada para permitir acesso simultâneo. O link relaciona as Entradas do Fluxo de Entrada que apenas são mencionadas no caso de processamento de pacotes de ARP e equilíbrio de carga periódico. Não há nenhuma referência por pacote para as Entradas do Fluxo de Entrada. Mesmo que as listas do link não sejam vinculadas, a sobrecarga no processamento de cada pacote não-ARP é sempre uma constante. O processamento de pacotes ARP, tanto de entrada como de saída, entretanto, depende do número de links na lista de link correspondente.

No caminho do processamento de entrada, a filtragem também é utilizada para evitar que os pacotes de difusão efetue loop back através do sistema de outros adaptadores físicos.

Suporte do protocolo

Os fluxos de ARP e IP/TCP/UDP têm equilíbrio de carga. Se o pacote estiver em apenas um protocolo IP, como um ICMP ou IGMP, então todos os dados passam para um endereço IP específico e saem através do mesmo adaptador físico. Se o pacote usa TCP ou UDP para o protocolo L4, o número da porta é adicionado ao algoritmo de hash, dessa forma, dois fluxos separados de L4 podem sair através de dois adaptadores físicos separados para o mesmo endereço de IP.

Por exemplo, presuma que o cliente tem um endereço IP de 10.0.0.1. Todo o tráfego de IGMP e ICMP sairá do mesmo adaptador físico porque somente o endereço de IP é usado para o hash. O fluxo seria da seguinte forma:

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

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

Se o servidor também envia um fluxo de TCP e UDP para o mesmo endereço 10.0.0.1, eles podem estar no mesmo adaptador físico que IGMP e ICMP ou em adaptadores físicos completamente diferentes. O fluxo seria da seguinte forma:

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

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

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

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

Ou os fluxos seriam da seguinte forma:

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

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

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

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

A atribuição real entre os adaptadores pode ser alterada com o tempo, mas qualquer protocolo que não esteja baseado em TCP/UDP examina o mesmo adaptador físico porque somente o endereço IP é usado no hash.

Desempenho

As placas de interface de rede atuais fornecem muitos recursos de hardware que reduzem a utilização da CPU, descarregando determinadas operações intensivas da CPU (consulte [Formação de equipes e outras propriedades avançadas de rede](#)). Por outro lado, o driver intermediário BASP trata-se de uma função de software que deve examinar cada pacote recebido das pilhas do protocolo e reagir ao conteúdo do pacote antes de enviá-lo para uma interface física específica. Apesar do driver do BASP processar cada pacote de saída constantemente, alguns aplicativos que já podem estar vinculados à CPU podem sofrer se forem operados através de uma interface agrupada. Como um aplicativo, pode ser adaptado para se beneficiar dos recursos de limite de falha ou pode operar de forma mais eficiente através de um adaptador físico único que fornece um hardware específico, como Large Send Offload.

Suporte de driver pelo sistema operacional

Como observado anteriormente, o BASP é compatível com ambientes de sistemas operacionais Windows Server 2008 e 2012.

Os diversos recursos do modo de formação de equipes são resumidos na tabela abaixo.

Tabela 8: Recursos do modo de formação de equipes

Recursos	Suporte do Windows
Smart Load Balancing™	
Interface do usuário	BACS ^a
Número de equipes	16
Número de adaptadores por equipe	8
Substituição ativa	Sim
Adição ativa	Sim
Remoção ativa	Sim
Suporte à velocidade do link	Velocidades diferentes
Protocolo de quadro	IP
Gerenciamento de pacote de entrada	BASP
Gerenciamento de pacote de saída	BASP
Evento de limite de falha	Perda de link ou evento de LiveLink
Período do limite de falha	<500 ms
Período de reserva	1,5 s ^b (aproximadamente)
Suporte ao LiveLink	Sim
Endereço MAC	Diferente
Formação de equipes de vários fornecedores	Sim
Trunking genérico	
Interface do usuário	BACS
Número de equipes	16
Número de adaptadores por equipe	8
Substituição ativa	Sim
Adição ativa	Sim
Remoção ativa	Sim
Suporte à velocidade do link	Velocidades diferentes
Protocolo de quadro	Todos
Gerenciamento de pacote de entrada	Switch
Gerenciamento de pacote de saída	BASP
Evento de limite de falha	Somente perda de link
Período do limite de falha	<500 ms
Período de reserva	1,5 s ^b (aproximadamente)
Endereço MAC	O mesmo para todos os adaptadores
Formação de equipes de vários fornecedores	Sim
Trunking dinâmico	
Interface do usuário	BACS

Tabela 8: Recursos do modo de formação de equipes (Cont.)

Recursos	Suporte do Windows
Número de equipes	16
Número de adaptadores por equipe	8
Substituição ativa	Sim
Adição ativa	Sim
Remoção ativa	Sim
Suporte à velocidade do link	Velocidades diferentes
Protocolo de quadro	Todos
Gerenciamento de pacote de entrada	Switch
Gerenciamento de pacote de saída	BASP
Evento de limite de falha	Somente perda de link
Período do limite de falha	<500 ms
Período de reserva	1,5 s ^b (aproximadamente)
Endereço MAC	O mesmo para todos os adaptadores
Formação de equipes de vários fornecedores	Sim

^a Broadcom Advanced Control Suite

^b Certifique-se de que a Port Fast ou a Edge Port está ativada.

Velocidades de formação de equipes suportadas

As diversas velocidades de link que são suportadas para cada tipo de equipe são listadas em [Tabela 9](#). Velocidade mista refere-se ao recurso de adaptadores de formação de equipes que estão executando nas velocidade do link.

Tabela 9: Velocidade do link na formação de equipes

Tipo de equipe	Velocidade do link	Direção do tráfego	Suporte à velocidade
SLB	10/100/1000	Entrada/saída	Velocidade mista
FEC	100	Entrada/saída	Mesma velocidade
GEC	1000	Entrada/saída	Mesma velocidade
IEEE 802.3ad	10/100/1000	Entrada/saída	Velocidade mista

Formação de equipes e outras propriedades avançadas de rede

- [Checksum Offload](#)
- [Marcação IEEE 802.1p QoS](#)
- [Large Send Offload](#)
- [Quadros Jumbo](#)
- [VLAN do IEEE 802.1Qs](#)
- [Wake on LAN](#)
- [Preboot Execution Environment \(PXE\)](#)

Antes de criar uma equipe, adicionar ou remover membros da equipe ou alterar as configurações avançadas de um membro da equipe, certifique-se de que cada membro da equipe foi configurado da mesma forma. As configurações incluem VLANs e Marcação de Pacote de QoS, Quadros Jumbo e os diversos offloads. As propriedades avançadas do adaptador e o suporte à formação de equipes são listados em [Tabela 10](#).

Tabela 10: Propriedades avançadas do adaptador e suporte à formação de equipes

Propriedade do Adaptador	Suportado pelo Adaptador Virtual Agrupado
Checksum Offload.	Sim
Marcação IEEE 802.1p QoS	Não
Large Send Offload	Sim ^a
Quadros Jumbo	Sim ^b
VLAN do IEEE 802.1Qs	Sim
Wake on LAN	Não
Preboot Execution environment (PXE)	Sim ^c

^a Todos os adaptadores da equipe devem suportar esse recurso. Alguns adaptadores podem não suportar esse recurso se ASF/IPMI também estiver ativado.

^b Deve ser suportado por todos os adaptadores da equipe.

^c Apenas como um servidor PXE, não como um cliente.

Checksum Offload

Checksum Offload é uma propriedade dos adaptadores de rede Broadcom que permite que as somas de verificação TCP/IP/UDP para tráfego de envio e recebimento sejam calculadas pelo hardware do adaptador, em vez de pela CPU do host. Em situações de tráfego intenso, isso pode permitir que um sistema trate mais conexões de forma mais eficiente que se a CPU do host fosse forçada a calcular as somas de verificação. Essa propriedade é basicamente uma propriedade de hardware e não se beneficiaria de uma implementação apenas de software. Um adaptador que suporta Checksum Offload anuncia essa capacidade ao sistema operacional, de forma que a soma de verificação não precise ser calculada na pilha do protocolo. Em virtude do driver intermediário estar localizado diretamente entre a camada do protocolo e o driver da miniporta, a camada do protocolo não pode efetuar offload em nenhuma soma de verificação.

Marcação IEEE 802.1p QoS

A norma IEEE 802.1p inclui um campo de 3 bits (que suporta no máximo 8 níveis de prioridade), que permite a prioridade do tráfego. O driver intermediário BASP não suporta Marcação IEEE 802.1p QoS

Large Send Offload

Large Send Offload (LSO) é um recurso fornecido pelos adaptadores de rede Broadcom que impede que um protocolo de nível superior, como TCP, divida um pacote de dados grande em uma série de pacotes menores com cabeçalhos anexados a eles. A pilha do protocolo precisa apenas gerar um cabeçalho único para um pacote de dados igual a 64 KB e o hardware do adaptador divide o buffer de dados em quadros Ethernet de tamanho apropriado, com o cabeçalho sequenciado corretamente (baseado no primeiro cabeçalho único fornecido).

Quadros Jumbo

O driver intermediário BASP suporta quadros jumbo, desde que todos os adaptadores físicos da equipe também suportem quadros Jumbo e o mesmo tamanho seja definido em todos os adaptadores da equipe.

VLAN do IEEE 802.1Qs

A norma IEEE 802.3ac define as extensões do formato para suportar marcações da Virtual Bridged Local Area Network (Rede Local Virtual) nas redes Ethernet, conforme mencionado na especificação IEEE 802.1Q. O protocolo VLAN permite a inserção de uma marca no quadro Ethernet para identificar a VLAN a que o quadro pertence. Se existente, a marca VLAN de 4 bytes é inserida no quadro Ethernet entre o endereço MAC de origem e o campo de comprimento/tipo. Os primeiros 2 bytes da marca VLAN consistem do tipo de tag IEEE 802.1Q, enquanto que os segundos 2 bytes incluem um campo de prioridade do usuário e o identificador VLAN (VID). As LANs virtuais (VLANs) permitem que o usuário divida a LAN física em subpartes lógicas. Cada VLAN definida atua como a própria rede separada, com tráfego e transmissões isolados um dos outros, aumentando a eficiência da largura da banda em cada grupo lógico. As VLANs também permitem que o administrador reforce as políticas de segurança e qualidade de serviço (QoS) adequadas. O BASP suporta a criação de 64 VLANs por equipe ou adaptador: 63 marcadas e 1 desmarcada. O sistema operacional e os recursos do sistema, no entanto, limitam o número real de VLANs. O suporte à VLAN é prestado de acordo com a IEEE 802.1q e é oferecido em um ambiente de formação de equipes, assim como em um adaptador único. Observe que as VLANs são suportadas somente com equipes homogêneas, não em um ambiente de formação de equipe de vários fornecedores. O driver

intermediário BASP suporta marcação de VLAN. Uma ou mais VLANs podem ser vinculadas a uma instância única do driver intermediário.

Wake on LAN

Wake on LAN (WOL) é um recurso que permite que um sistema seja ativado de um estado inativo através da chegada de um pacote específico pela interface Ethernet. Como o Adaptador virtual é implementado somente como dispositivo do software, ele perde os recursos de hardware para implementar o Wake on LAN e não pode ser ativado para ativar o sistema de um estado inativo através do Adaptador virtual. Os adaptadores físicos, no entanto, suportam esta propriedade, mesmo quando o adaptador é parte da equipe.

Preboot Execution Environment (PXE)

O Preboot Execution Environment (PXE) permite que um sistema execute a inicialização de imagem do sistema operacional através da rede. Por definição, o PXE é chamado antes de o sistema operacional ficar carregado, dessa forma, não há chance do driver intermediário BASP carregar e ativar a equipe. Como consequência, a formação de equipes não é suportada como um cliente PXE, embora um adaptador físico que participa da equipe quando o sistema operacional é carregado possa ser usado como cliente PXE. Considerando que o adaptador agrupado não pode ser usado como cliente PXE, ele pode ser usado para um servidor PXE, que fornece imagens do sistema operacional aos clientes PXE usando uma combinação de Dynamic Host Control Protocol (DHCP) e o Trivial File Transfer Protocol (TFTP). Esses dois protocolos operam em IP e são suportados por todos os modos de formação de equipes.

Considerações gerais de rede

- [Formação de equipes através de switches](#)
- [Algoritmo de Spanning Tree](#)
- [Formação de equipes com Microsoft NLB/WLBS](#)

Formação de equipes através de switches

A formação de equipes SLB pode ser configurada através de switches. Os switches, no entanto, devem ser conectados. O trunking genérico e a agregação de link não funcionam através de switches, porque cada uma dessas implementações requer que todos os adaptadores físicos da equipe compartilhem o mesmo endereço MAC Ethernet. É importante observar que o SLB somente pode detectar a perda de link entre as portas da equipe e seus parceiros de link imediato. O SLB não tem nenhuma forma de reagir a outras falhas de hardware nos switches e não pode detectar perda de link em outras portas.

Tolerância a falhas do link do switch

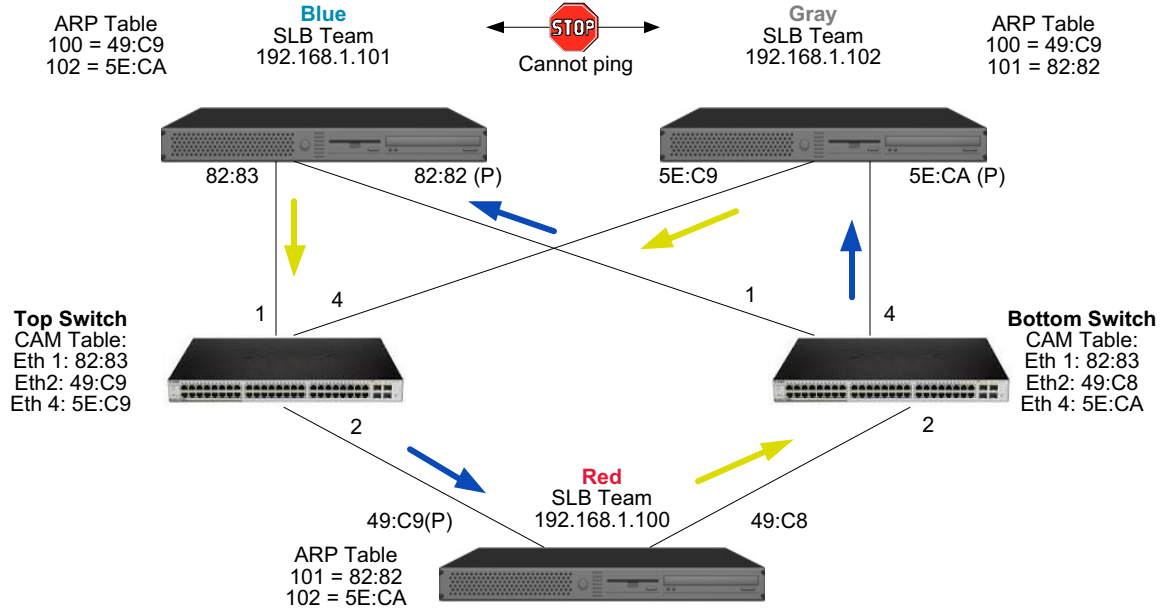
O diagrama abaixo descreve a operação de uma equipe SLB em uma configuração de tolerância a falhas do switch. Mostramos o mapeamento de solicitação de ping e as respostas de ping em uma equipe SLB com dois membros ativos. Todos os servidores (Blue, Gray e Red) têm um ping contínuo. [Figura 3](#) é uma configuração sem cabo de interconexão entre os dois switches. [Figura 4](#) tem o cabo de interconexão no lugar e [Figura 5](#) é um exemplo de evento de limite de falha com o cabo de interconexão no lugar. Estes cenários descrevem o procedimento de formação de equipes através de dois switches e a importância do link de interconexão.

Os diagramas mostram o membro secundário da equipe enviando solicitações de echo ICMP (setas amarelas) enquanto o membro da equipe primária recebe as respectivas respostas de echo ICMP (setas azuis). Isso mostra uma característica-chave do software de formação de equipes. Os algoritmos de equilíbrio de carga não sincronizam como os quadros são equilibrados por carga quando enviados ou recebidos. Em outras palavras, os quadros de uma determinada conversação podem sair e serem recebidos em interfaces diferentes da equipe. Isso ocorre para todos os tipos de formação de equipe suportados pelo Broadcom. Portanto, um link de interconexão deve ser fornecido entre os switches que se conectam às portas da mesma equipe.

Na configuração sem a interconexão, uma solicitação ICMP de Blue para Grey vai até a porta 82:83 destinada para a porta Grey 5E:CA, mas o Top Switch não tem nenhuma forma de enviá-lo, porque ele não pode ir com a porta 5E:C9 Grey. Algo semelhante ocorre quando Grey tenta efetuar ping de Blue. Uma solicitação ICMP sai de um 5E:C9 destinado para 82:82 Blue, mas não consegue chegar lá. O Top Switch não tem uma entrada para 82:82 em sua tabela CAM porque não há interconexão entre os dois switches. Os pings, entretanto, fluem entre Red e Blue e Red e Grey.

Além disso, um evento de limite de falha causaria perda adicional de conectividade. Considere uma desconexão de cabo na porta 4 do Top Switch. Neste caso, o Grey enviaria a Solicitação ICMP para o Red 49:C9, mas como o Bottom Switch não tem entrada para 49:C9 em sua Tabela CAM, o quadro é transbordado para todas as suas portas, mas não pode localizar uma forma de chegar em 49:C9.

Figura 3: Formação de equipe através de switches sem um link de interconexão



A adição de um link entre os switches permite que o tráfego de/para Blue e Grey seja atingido mutuamente sem nenhum problema. Observe as entradas adicionais na tabela CAM para os dois switches. A interconexão do link é crítica para a operação adequada da equipe. Como consequência, é altamente recomendável ter um entroncamento de agregação de link para interconectar os dois switches para garantir a alta disponibilidade da conexão.

Figura 4: Formação de equipes através de switches sem interconexão

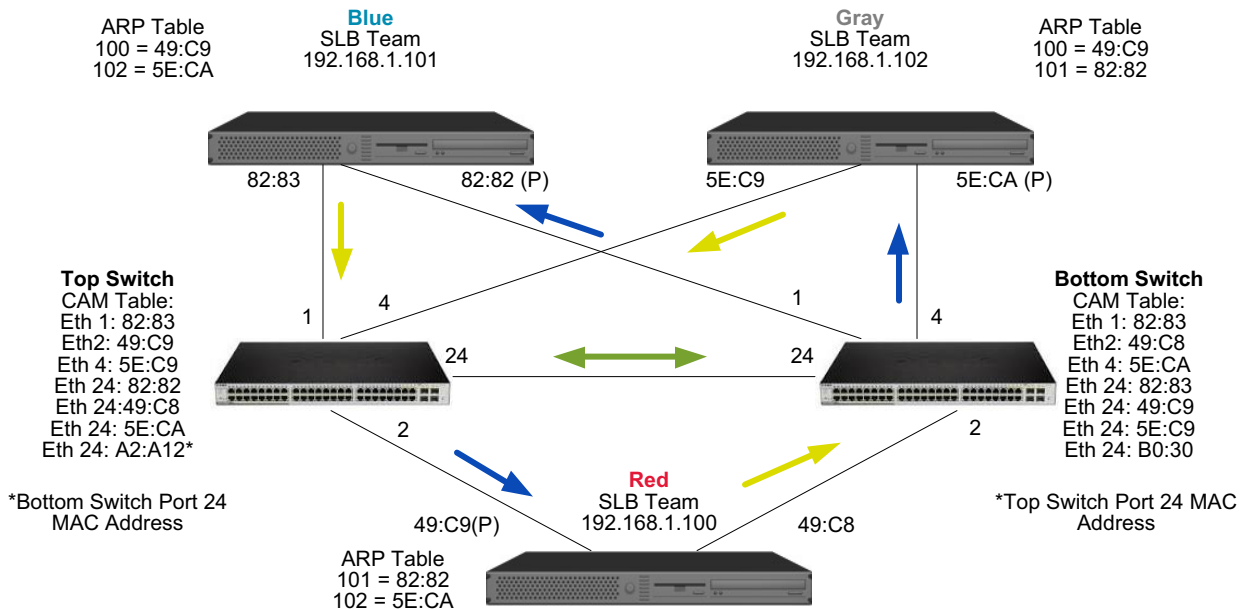
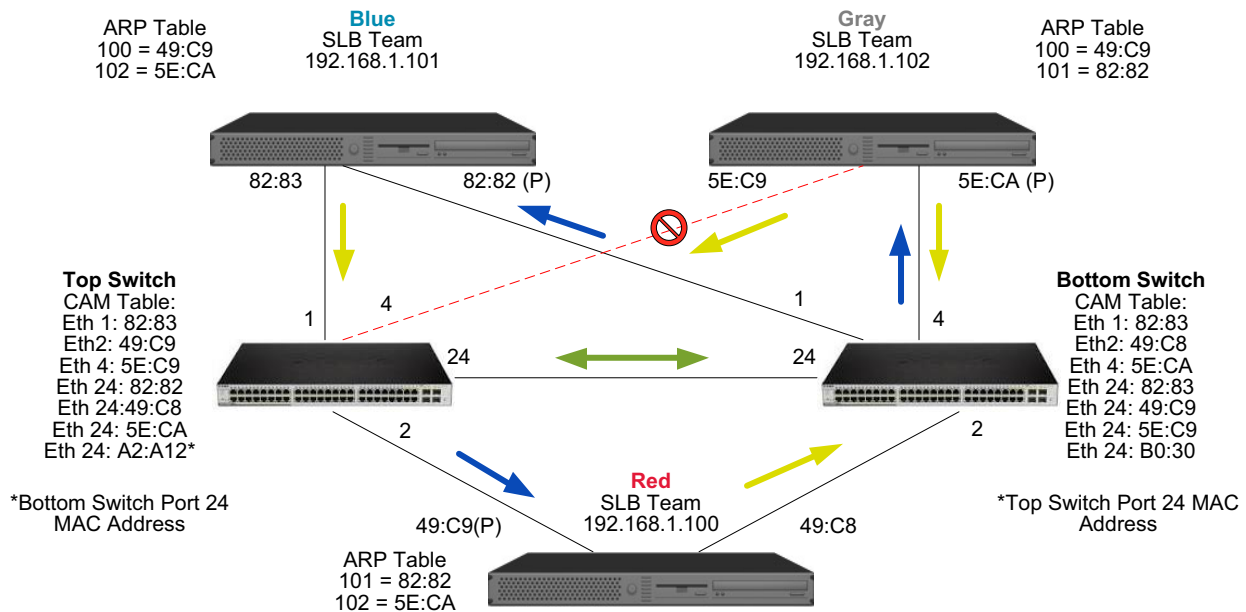


Figura 5 representa um evento de limite de falha no qual o cabo é desconectado da porta 4 do Top Switch. Esse é um limite de falha bem-sucedido com todas as estações efetuando ping mutuamente sem perda de conectividade.

Figura 5: Evento de limite de falha



Algoritmo de Spanning Tree

- Observação de alteração da topologia (TCN)
- Port Fast/Edge Port

Nas redes Ethernet, pode existir apenas um caminho ativo entre duas pontes ou switches. Vários caminhos ativos entre os switches podem provocar loops na rede. Quando ocorrem loops, alguns switches reconhecem as estações nos dois lados do switch. Esta situação provoca um defeito no algoritmo de envio, permitindo que os quadros duplicados sejam enviados. Os algoritmos de spanning tree fornecem redundância de caminho através da definição de uma árvore que spans todos os switches em uma rede estendida e que força determinados caminhos de dados redundantes para um estado de reserva (bloqueado). Em intervalos regulares, os switches de rede enviam e recebem pacotes de spanning tree que eles usam para identificar o caminho. Se um segmento de rede se tornar inatingível ou se o período do spanning tree for alterado, o algoritmo de spanning tree reconfigura a topologia de spanning tree e restabelece o link, ativando o caminho de reserva. A operação de spanning tree é transparente para estações finais que não detectam se elas estão conectadas a um segmento de LAN único ou a uma LAN conectada de vários segmentos.

O Protocolo Spanning Tree (STP) é um protocolo de Camada 2 designado para ser executado em pontes e switches. A especificação do STP é definida em IEEE 802.1d. O objetivo principal do STP é garantir que não haja execuções em situações de loop, quando você tem caminhos redundantes na sua rede. O STP detecta/desativa os loops de rede e fornece links de backup entre os switches ou pontes. Ele permite que o dispositivo interaja com outros dispositivos compatíveis em sua rede, para garantir que exista apenas um caminho entre duas estações da rede.

Depois que uma topologia de rede estável é estabelecida, todas as pontes recebem uma mensagem das BPDUs (Bridge Protocol Data Units) transmitida pela ponte raiz. Se a ponte não receber um aviso BPDU após um intervalo predefinido

(período máximo), a ponte assume que o link da ponte raiz está desativado. Esta ponte, em seguida, inicia as negociações com outras pontes para reconfigurar a rede para restabelecer uma topologia de rede válida. O processo de criação de uma nova topologia pode levar até 50 segundos. Durante esse tempo, as comunicações end-to-end são interrompidas.

O uso de Spanning Tree não é recomendado para portas que estão conectadas às estações finais, porque por definição, uma estação final não cria um loop dentro de um segmento Ethernet. Além disso, quando um adaptador agrupado é conectado a uma porta com Spanning Tree ativado, os usuários podem experimentar problemas de conectividade inesperados. Por exemplo, considere um adaptador agrupado que tem um link perdido em um dos adaptadores físicos. Se o adaptador físico teve que ser reconectado (também conhecido como reserva), o driver intermediário detecta que o link foi restabelecido e inicia a passagem do tráfego pela porta. O tráfego seria perdido se a porta fosse bloqueada temporariamente pelo Protocolo Spanning Tree.

Observação de alteração da topologia (TCN)

Uma ponte/switch cria uma tabela de envio de endereços MAC e os números de porta, descobrindo o endereço MAC de origem que foi recebido em uma porta específica. A tabela é usada para enviar quadros a uma porta específica, em vez de enviar o quadro para todas as portas. O período máximo comum de entradas na tabela é 5 minutos. Somente depois que um host foi silenciado durante 5 minutos sua entrada pode ser removida da tabela. Às vezes é benéfico para reduzir o período. Um exemplo é quando um link de envio vai para o bloqueio e um link diferente vem do bloqueio para o envio. Essa alteração poderia levar até 50 segundos. No final do recálculo do STP um novo caminho é disponibilizado para comunicações entre as estações. Entretanto, como a tabela de envio ainda teria entradas baseadas na topologia antiga, as comunicações não poderiam ser restabelecidas após cinco minutos depois que as portas afetadas forem removidas da tabela. O tráfego seria transbordado para todas as portas e redescoberto. Nesse caso é benéfico para reduzir o período. Esse é o objetivo de uma observação de alteração da topologia (TCN) BPDU. A TCN é enviada da ponte/switch afetado para a ponte/switch raiz. Assim que a ponte/switch detecta a alteração da topologia (um link recuando ou uma porta sendo direcionada ao envio), ela envia uma TCN para a ponte raiz através da sua porta raiz. A ponte raiz anuncia, em seguida, uma BPDU com uma alteração de topologia para toda a rede. Isso faz com que toda a ponte reduza o período da tabela MAC para 15 segundos de um período especificado. Isso permite que o switch redescubra os endereços MAC, assim que o STP é convergido novamente.

As BPDUs de observação de alteração da topologia são enviadas quando uma porta envia as alterações para bloqueio ou transições para envio. Uma BPDU não inicia um recálculo de STP. Ela somente afeta o período das entradas da tabela de envio no switch. Isso não irá alterar a topologia da rede ou criar loops. Os nós da extremidade como servidores ou clientes disparam uma alteração da topologia quando são desligados e, em seguida, ligados novamente.

Port Fast/Edge Port

Para reduzir o efeito de TCNs na rede (por exemplo, aumento transbordo nas portas do switch) os nós da extremidade que são ligados/desligados, geralmente devem usar a configuração de Port Fast ou Edge Port na porta de configuração ao qual eles estão acoplados. Port Fast ou Edge Port é um comando que é aplicado às portas específicas e tem os seguintes efeitos:

- As portas provenientes de um link inativo para um link ativo serão colocadas no modo STP de envio, em vez de ir do listening para o learning e, em seguida, para o envio. O STP ainda está sendo executado nessas portas.
- O switch não gera uma observação de alteração da topologia quando a porta está aumentando ou diminuindo.

Formação de equipes com Microsoft NLB/WLBS

O modo SLB de formação de equipes *não* trabalha no modo de difusão ponto a ponto Equilíbrio de Carga de Rede (NLB) da Microsoft, apenas em modo de difusão seletiva. Devido ao mecanismo usado pelo serviço NLB, a configuração

recomendada de formação de equipes nesse ambiente é Limite de Falha (SLB com NIC reserva) pois o equilíbrio de cargas é gerenciado pelo NLB.

Considerações do aplicativo

- [Formação de equipes e uso de cluster—Software de cluster da Microsoft](#)
- [Formação de equipes e backup de rede](#)

Formação de equipes e uso de cluster—Software de cluster da Microsoft

Em cada nó de cluster, é recomendado que cada cliente instale pelo menos dois adaptadores de rede (adaptadores da placa são aceitáveis). Essas interfaces atendem a dois propósitos. Um adaptador é usado exclusivamente para *comunicações* de pulso intracluster. Conhecido como *adaptador privado* e geralmente reside em uma sub-rede privada separada. O outro adaptador é usado para comunicações com o cliente e é conhecido como *adaptador público*.

Vários adaptadores podem ser usados para cada um destes objetivos: comunicações privada, intracluster e públicas, e de cliente externo. Todos os modos de formação de equipes da Broadcom são suportados com o Microsoft Cluster Software somente para o adaptador público. A formação de equipe do adaptador de rede privada não é suportada. A Microsoft indica que o uso de formação de equipe na interconexão privada de um servidor de cluster não é suportado, em virtude dos atrasos que possivelmente ocorreriam na transmissão e recebimento de pacotes de pulso entre os nós. Para obter melhores resultados, quando você quiser redundância para a interconexão privada, desative a formação de equipe e use as portas disponíveis para formar uma segunda interconexão privada. Com isso você obtém o mesmo resultado final e fornece caminhos de comunicação avançados, duplos para os nós se comunicarem.

Para formação de equipes em um ambiente de cluster, é recomendado que os clientes usem a mesma marca de adaptadores.



Nota: O Microsoft Network Load Balancing não é compatível com o Microsoft Cluster Software.

Formação de equipes e backup de rede

- [Equilíbrio de carga e limite de falha](#)
- [Tolerância a Falhas](#)

Quando você executa backups de rede em um ambiente não agrupado, toda a produtividade de um adaptador do servidor de backup pode ser facilmente impactada devido à sobrecarga de tráfego e do adaptador. Dependendo do número de servidores de backup, fluxos de dados e velocidade do driver da fita, o tráfego de backup pode consumir facilmente uma alta porcentagem da largura de banda do link da rede, impactando os dados de produção e o desempenho de backup da fita. Os backups da rede geralmente consistem de um servidor de backup dedicado que é executado com o software de backup da fita como NetBackup, Galaxy ou Backup Exec. Acoplado ao servidor de backup há uma unidade de backup de fita SCSI direto ou uma biblioteca de fita conectada através de uma rede de área de armazenagem (SAN) do fibre channel. Os sistemas que foram submetidos a backup através da rede geralmente são chamados de clientes ou servidores remotos e geralmente têm um agente de software de backup de fita instalado.

Como há 4 servidores de cliente, o servidor de backup pode transferir simultaneamente quatro tarefas de backup (uma por cliente) para um carregador automático de várias unidades. Em virtude do link único entre o switch e o servidor de backup, no entanto, um backup de 4 transmissões pode saturar facilmente o adaptador e o link. Se o adaptador do servidor de backup operar com 1 Gbps (125 MB/s) e cada cliente puder transmitir os dados a 20 MB/s durante o backup da fita, então a produtividade entre o sistema de backup e o switch será de 80 MB/s (20 MB/s x 4), que é equivalente a 64% da largura de banda da rede. Apesar de isso ser bom dentro da faixa de largura de banda da rede, os 64% constituem um percentual alto, especialmente se os aplicativos compartilharem o mesmo link.

Equilíbrio de carga e limite de falha

Conforme o número de fluxos de backup aumenta, a produtividade geral aumenta. Cada transmissão de dados não pode manter o mesmo desempenho como uma transmissão de backup única de 25 MB/s. Em outras palavras, mesmo que um servidor de backup possa transmitir dados de um cliente único a 25 MB/s, não é esperado que quatro tarefas de backup em execução simultânea sejam transmitidas a 100 MB/s (25 MB/s x 4 transmissões). Apesar de a produtividade total aumentar conforme o número de backup aumenta, cada fluxo de backup pode ser afetado pelo software de fita ou pelas limitações de pilha da rede.

Para que um servidor de backup de fita utilize de forma confiável o desempenho do adaptador e a largura de banda da rede ao fazer backup dos clientes, uma infraestrutura de rede deve implementar a formação de equipes, como um equilíbrio de carga e tolerância a falhas. Os centros de dados irão incorporar os switches redundantes, a agregação de link e o trunking como parte de sua solução tolerante a falhas. Apesar dos drivers do dispositivo de formação de equipe manipular a forma que os dados são transmitidos através das interfaces agrupadas e caminhos de limite de falha, é aconselhável fazer backup em fita dos aplicativos e não interromper nenhum processo de backup ao fazer backup dos sistemas remotos através da rede. [Figura 6](#) mostra uma topologia de rede que demonstra o backup em fita em um ambiente agrupado do Broadcom e como o equilíbrio de carga avançado pode *equilibrar a carga de dados* de backup da fita através de adaptadores agrupados.

Há quatro caminhos que o servidor do cliente pode usar para enviar os dados ao servidor de backup, mas apenas um desses caminhos será designado durante a transferência de dados. Um caminho possível que Client-Server Red pode usar para enviar os dados ao server de backup é:

Exemplo do caminho: o Client-Server Red envia os dados através do adaptador A, switch 1, adaptador do servidor de backup A.

O caminho designado é determinado por dois fatores:

1. Cache do Client-Server ARP; que indica o endereço MAC do servidor de backup. Isso é determinado pelo algoritmo de equilíbrio de carga do driver intermediário da Broadcom.
2. A interface do adaptador físico no Client-Server Red é usada para transmitir os dados. O algoritmo de equilíbrio de carga de saída do driver intermediário da Broadcom determina isso (consulte [Fluxo do tráfego de saída](#) e [Fluxo de Tráfego de Entrada \(Somente SLB\)](#)).

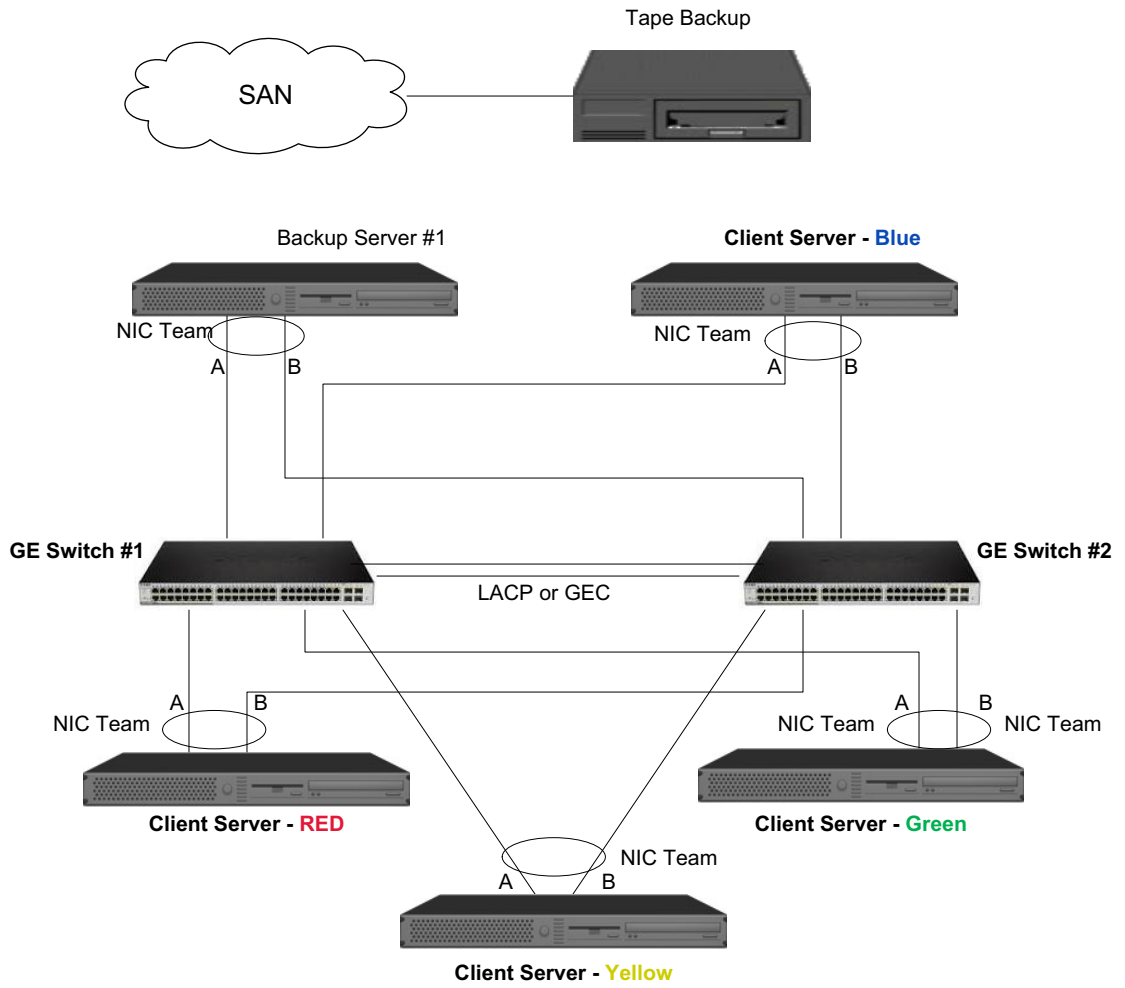
A interface agrupada no servidor de backup transmite um protocolo de resolução de endereço gratuito (G-ARP) ao Client-Server Red, que por sua vez, faz com que o cache ARP do servidor do cliente seja atualizado com o endereço MAC do Servidor de Backup. O mecanismo de equilíbrio de carga na interface agrupada determina o endereço MAC incorporado no G-ARP. O endereço MAC selecionado indica o local de destino dos dados transferidos do servidor cliente. No Client-Server Red, o algoritmo de formação de equipes SLB determinará qual das duas interfaces do adaptador será usada na transmissão dos dados. Neste exemplo, os dados do Client-Server Red são recebidos na interface do Adaptador A do servidor de backup. Para demonstrar os mecanismos SLB quando a carga adicional é colocada na interface agrupada, considere o cenário quando o servidor de backup inicia uma segunda operação de backup: uma para Client-Server Red, e uma para Client-Server Blue. A rota que o Client-Server Blue usa para enviar os dados ao servidor de backup é dependente de seu cache ARP, que indica o endereço MAC do servidor de backup. Como o Adaptador A do servidor de backup já está sob carga de sua operação de backup com Client-Server Red, o servidor de backup chama seu algoritmo SLB para *informar* ao Client-Server Blue (através de um G-ARP) que ele deve atualizar seu cache ARP para refletir o endereço MAC do Adaptador B do sistema de backup. Quando o Client-Server Blue precisa transmitir os dados, ele usa uma de suas interfaces do adaptador, que é determinada pelo seu próprio algoritmo SLB. O importante é que os dados do Client-Server Blue são recebidos da interface do Adaptador do Servidor de Backup e não da interface do seu Adaptador A. Isso é importante porque com as duas transmissões de backup executando simultaneamente, o servidor de backup deve *equilibrar por carga* as transmissões de dados de diferentes clientes. Com as duas transmissões de backup em execução, cada interface do adaptador do servidor de backup está processando uma carga igual, assim os dados do equilíbrio de carga cruzam as interfaces do adaptador.

O mesmo algoritmo se aplica se uma terceira e quarta operação de backup for iniciada do servidor de backup. A interface agrupada no servidor de backup transmite um G-ARP de difusão ponto a ponto para os clientes de backup para informá-los para atualizarem seus caches ARP. Cada cliente transmite os dados de backup junto com uma rota ao endereço MAC de destino no servidor de backup.

Tolerância a Falhas

Se o link de rede falhar durante as operações de backup da fita, todo o tráfego entre o servidor de backup e o cliente é interrompido e as tarefas de backup falham. Se, no entanto, a topologia da rede for configurada tanto para Broadcom SLB como para tolerância a falhas do switch, então isso pode permitir que as operações de backup da fita continuem sem interrupção durante a falha do link. Todos os processos de limite de falha na rede são transparentes para os aplicativos de software de backup em fita. Para entender como as transmissões de dados de backup são direcionadas durante o processo de limite de falha da rede, considere a topologia em [Figura 6](#). Client-Server Red está transmitindo os dados para o servidor de backup através do Caminho 1, mas ocorre uma falha de link entre o servidor de backup e o switch. Como os dados não puderam mais ser enviados do Switch #1 para a interface do Adaptador A no servidor de backup, os dados são redirecionados do Switch #1 através do Switch #2, para a interface do Adaptador B no servidor de backup. Isso ocorre sem o conhecimento do aplicativo de backup porque todas as operações de tolerância a falhas são tratadas pela interface da equipe do adaptador e pelas configurações de entroncamento nos switches. A partir da perspectiva do servidor do cliente, ele ainda opera como se estivesse transmitindo dados através do caminho original.

Figura 6: Backup de rede com formação de equipes SLB através de dois switches



Resolução de problemas de formação de equipes

- [Dicas de configuração para formação de equipes](#)
- [Orientações para solução de problemas](#)

Ao executar o analisador de protocolo através de uma interface agrupada do adaptador virtual, o endereço MAC mostrado nos quadros transmitidos pode estar incorreto. O analisador não mostra os quadros conforme construídos pelo BASP e mostra o endereço MAC da equipe e não o endereço MAC da interface que transmite o quadro. Recomenda-se o uso do processo a seguir para monitorar uma equipe:

1. Espelhar todas as portas de uplink da equipe no switch.
2. Se a equipe spans dois switches, espelhe também o tronco interlink.
3. Amostra de todas as portas espelhadas independentemente.
4. No analisador, use um adaptador e um driver que não filtre as informações de QoS e VLAN.

Dicas de configuração para formação de equipes

Ao solucionar problemas de conectividade de rede ou problemas de funcionalidade da formação de equipes, certifique-se de que as seguintes informações estão corretas para sua configuração.

1. Recomenda-se que, para uma equipe SLB, todos os adaptadores tenham a mesma velocidade do link.
2. Se o LiveLink não estiver ativado, desative o Protocolo Spanning Tree ou ative um modo STP que desvia as fases iniciais (por exemplo, Port Fast, Edge Port) das portas de switch conectadas à equipe.
3. Todos os switches daquela equipe que forem conectados diretamente devem ter a mesma revisão de hardware, revisão de firmware e revisão de software para serem suportados.
4. Para serem agrupados, os adaptadores devem ser da mesma VLAN. No caso de várias equipes serem configuradas, cada equipe deve estar em uma rede separada.
5. Não digite um endereço de difusão ou transmissão no campo Locally Administered Address (Endereço Administrado Localmente).
6. Não atribua um Endereço Administrado Localmente a nenhum adaptador físico que seja membro de uma equipe.
7. Verifique se o gerenciamento de energia está desativado em todos os membros físicos de qualquer equipes (a caixa **Computador pode desligar o dispositivo para economizar energia** na guia **Gerenciamento de energia** no adaptador **Propriedades** deve estar marcada — consulte [Definição das opções de gerenciamento de energia](#) em "Instalação de drivers e aplicativos do Windows").
8. Remova todos os endereço IP estáticos dos membros da equipe física antes da equipe ser criada.
9. Uma equipe que requer uma produtividade máxima deve usar o LACP ou GEC\FEC. Nesses casos, o driver intermediário somente é responsável pelo equilíbrio de carga de saída enquanto o switch executa o equilíbrio de carga de entrada.
10. As equipes agregadas (802.3ad \ LACP e GEC\FEC) devem ser conectadas para apenas um switch que suporta IEEE 802.3a, LACP ou GEC\FEC.
11. Não é recomendado conectar nenhuma equipe a um hub, pois um hub suporta apenas half-duplex. Os hubs devem ser conectados a uma equipe somente com o objetivo de solucionar problemas. A desativação do driver de dispositivo de um adaptador de rede que faça parte de uma equipe LACP ou GEC\FEC pode ter efeitos adversos na conectividade da rede. Para evitar uma falha na conexão da rede, a Broadcom recomenda que o adaptador seja fisicamente desconectado do switch antes que o driver do dispositivo seja desativado.

12. Verifique se os drivers da base (Miniporta) e da equipe (intermediário) são os mesmos do pacote da versão.
13. Teste a conectividade para cada adaptador físico antes de formar a equipe.
14. Teste o procedimento de limite de falhas e desativar reserva antes de colocar um ambiente em produção.
15. Quando se muda de uma rede que não é de produção para uma rede de produção, é altamente recomendável testar novamente o limite de falhas e a desativação de reserva.
16. Teste o procedimento de desempenho da equipe antes de colocar um ambiente em produção.

Orientações para solução de problemas

Antes de entrar em contato com o suporte, verifique se você concluiu as seguintes etapas para solução de problemas de conectividade de rede, enquanto o servidor estiver usando a formação de equipes do adaptador.

1. Certifique-se de que a luz do LINK de Ethernet esteja LIGADA para cada adaptador e que todos os cabos estejam conectados.
2. Verifique se os drivers intermediários e a base correspondente pertencem ao mesmo pacote de versão e se estão carregados corretamente.
3. Verifique se há um Endereço IP válido usando o comando **ipconfig** do Windows.
4. Verifique se o STP está desativado ou Edge Port/Port Fast está ativado nas portas do switch conectados à equipe ou se o LiveLink está sendo usado.
5. Verifique se os adaptadores e o switch estão configurado da mesma forma para velocidade do link e duplex.
6. Se possível, divida a equipe e verifique a conectividade de cada adaptador, independentemente de confirmar se o problema está associado diretamente à equipe.
7. Verifique se todas as portas do switch conectadas à equipe estão na mesma VLAN.
8. Verifique se as portas do switch estão configuradas adequadamente para o tipo de equipe de Trunking genérico (FEC/GEC)/802.3ad-Draft Static e se ele corresponde ao tipo de equipe do adaptador. Se o sistema estiver configurado para um tipo de equipe SLB, certifique-se de que as portas correspondentes *não estão* configuradas para os tipos de equipe de Trunking genérico (FEC/GEC)/802.3ad-Draft Static.

Perguntas frequentes

P: Em quais circunstâncias o tráfego não tem equilíbrio de carga? Por que todo o tráfego não tem equilíbrio de carga nos membros da equipe?

R: O volume de tráfego não utiliza IP/TCP/UDP ou o volume de clientes está em uma rede diferente. O equilíbrio de carga de recebimento não é uma função de carga de tráfego, mas uma função do número de clientes que estão conectados ao sistema

P: Quais protocolos de rede têm equilíbrio de carga quando estão em uma equipe?

R: Broadcom's teaming software only supports IP/TCP/UDP traffic. Todo o outro tráfego é enviado ao adaptador primário.

P: Quais protocolos têm equilíbrio de carga com SLB e quais não têm?

R: Somente os protocolos IP/TCP/UDP têm equilíbrio de carga nas duas direções: envio e recebimento.

P: Posso agrupar uma porta executando a 100 Mbps com uma porta executando a 1000 Mbps?

R: As velocidades de link mistas dentro de uma equipe somente são suportadas para as equipes de Smart Load Balancing™ e 802.3, conforme mencionado anteriormente.

P: Posso agrupar um adaptador de fibra com um adaptador Gigabit Ethernet de cobre?

R: Sim com SLB, e sim se o switch permitir isso no FEC/GEC e 802.3ad.

P: Qual a diferença de equilíbrio de carga do adaptador e Equilíbrio de Carga de Rede (NLB) da Microsoft?

R: O equilíbrio de carga do adaptador é feito em um nível de sessão da rede, enquanto que o NLB é feito em nível de aplicativo do sistema.

P: Posso conectar os adaptadores da equipe às portas em um roteador?

R: Não. Todas as portas de uma equipe devem estar na mesma rede; porém, em um roteador cada porta está em uma rede separada por definição. Todos os modos de formação de equipes exigem que o parceiro do link seja um switch da Camada 2.

P: Posso usar a formação de equipes com os Serviços de Cluster da Microsoft?

R: Sim. A formação de equipes é suportada somente na rede pública, não na rede privada usada para link de pulsos.

P: O PXE pode trabalhar em um adaptador virtual (equipe)?

R: O cliente PXE opera em um ambiente antes que o sistema operacional seja carregado; como consequência os adaptadores virtuais não foram ativados ainda. Se o adaptador físico suportar PXE, ele pode ser usado como cliente PXE, independente ou não de ser parte de um adaptador virtual quando o sistema operacional é carregado. Os servidores PXE podem operar em um adaptador virtual.

P:	O WOL pode trabalhar em um adaptador virtual (equipe)?
R:	A funcionalidade Wake-on-LAN opera em um ambiente antes de o sistema operacional ser carregado. O WOL ocorre quando o sistema está desativado ou em standby, dessa forma, nenhuma equipe está configurada.

P:	Qual é o número máximo de portas que podem ser agrupadas?
R:	Até 8 portas podem ser atribuídas a uma equipe.

P:	Qual é o número máximo de equipes que podem ser configuradas no mesmo sistema?
R:	Até 16 equipes podem ser configuradas no mesmo sistema.

P:	Por que minha equipe perde a conectividade durante os primeiros 30 a 50 segundos após o adaptador primário ser restaurado (reserva)?
R:	Por que o Protocolo Spanning Tree está trazendo a porta do bloqueio para o envio? Você deve ativar a configuração Port Fast ou Edge Port nas portas do switch conectadas à equipe ou usar o LiveLink para ser responsável pelo atraso do STP.

P:	Posso conectar uma equipe através de vários switches?
R:	O Smart Load Balance pode ser usado com vários switches porque cada adaptador físico do sistema usa um endereço Ethernet Mac exclusivo. A Agregação de Link e o Trunking Genérico não podem operar em switches porque eles exigem que todos os adaptadores físicos compartilhem o mesmo endereço Ethernet MAC.

P:	Como atualizo o driver intermediário (BASP)?
R:	O driver intermediário não pode ser atualizado através das Propriedades de Conexão da Área Local. Deve ser atualizado usando o Programa de instalação de configuração.

P:	Posso determinar a estatística de desempenho em um adaptador virtual (equipe)?
R:	No Broadcom Advanced Control Suite, clique na guia Estatísticas de BASP do adaptador virtual.

P:	Posso configurar NBL e formação de equipes simultaneamente?
R:	Sim, mas somente ao executar o NLB em um modo de difusão (o NLB não é suportado com os Serviços de Cluster da MS).

P:	O sistema de backup e os sistemas do cliente que foram restabelecidos devem ser agrupados?
R:	Como o sistema de backup está sob a carga máxima de dados, ele deve ser agrupado para agregação de link e limite de falhas. Uma rede totalmente redundante, no entanto, requer que os switches e os clientes de backup sejam agrupados para tolerância a falhas e agregação de link.

P:	Durante as operações de backup, o algoritmo do adaptador de formação de equipes tem equilíbrio de dados em nível de byte ou em nível de sessão?
R:	Ao usar a formação de equipes do adaptador, os dados têm equilíbrio de carga em nível de sessão, e não em nível de byte, para evitar que os quadros fiquem fora da ordem. O equilíbrio de carga de formação de equipes do adaptador não funciona da mesma forma que outros mecanismos de equilíbrio de carga do armazenamento como EMC PowerPath.

P:	Há alguma configuração especial no software ou hardware de backup da fita especial para trabalhar com a formação de equipe do adaptador?
R:	Nenhuma configuração especial é necessária no software de fita para trabalhar com a formação de equipes. A formação de equipes é transparente para aplicativos de backup de fita.

P:	Como eu posso identificar o driver que estou usando?
R:	Em todos os sistemas operacionais, o método mais preciso para verificar a revisão do driver é localizar fisicamente o arquivo de driver e verificar as propriedades.

P:	O SLB pode detectar uma falha de switch em uma configuração de Tolerância à Falha do Switch?
R:	Não. O SLB pode detectar apenas a perda de link entre a porta agrupada e seu parceiro de link imediato. O SLB não pode detectar falhas de link em outras portas. Para obter mais informações, consulte Funcionalidade LiveLink™ .

P:	Onde monitoro as estatísticas em tempo real de uma equipe do adaptador em um sistema do Windows?
R:	Use o Broadcom Advanced Control Suite (BACS) para monitorar contadores personalizados e gerais IEEE 802.3.

Mensagens de log de evento

- [Mensagens de log de evento do sistema Windows](#)
- [Driver de base \(adaptador físico/miniporta\)](#)
- [Driver intermediário \(Adaptador/Equipe Virtual\)](#)

Mensagens de log de evento do sistema Windows

São relacionadas as mensagens de status do Log de eventos do sistema Windows dos drivers de base e intermediário para os adaptadores Broadcom NetXtreme Gigabit Ethernet listados na seção a seguir. Conforme um driver do adaptador é carregado, o Windows coloca um código de status no visualizador de eventos do sistema. Pode haver até duas classes de entradas para estes códigos de evento, dependendo se os drivers são carregados (um conjunto de driver básico ou de miniporta e um conjunto para o driver intermediário e de formação de equipes).

Driver de base (adaptador físico/miniporta)

Tabela 11 lista as mensagens do log de evento suportadas pelo driver de base, explica a causa da mensagem e fornece a ação recomendada.

Tabela 11: Mensagens de log do driver de base

Mensagem Número	Mensagem	Causa	Ação corretiva
1	Falha ao alocar a memória para o bloco do dispositivo. Verifique o recurso uso de memória do sistema.	O driver não pode alocar memória do sistema operacional.	Feche os aplicativos de execução para liberar memória
2	Falha ao alocar os registros do mapa	O driver não pode alocar registros de mapa do sistema operacional.	Descarregue outros drivers que podem alocar os registros do mapa.
3	Falha ao acessar as informações sobre configuração. Reinstale o driver da rede.	O driver não pode acessar os registros de espaço de configuração do PCI no adaptador.	Para adaptadores adicionados: recoloque o adaptador no slot, mova-o para outro slot de PCI ou substitua o adaptador.
4	O link da rede está inativo. Certifique-se de que o cabo da rede está conectado corretamente.	O adaptador perde sua conexão com seu parceiro de link.	Verifique se o cabo da rede está conectado, se o cabo da rede é do tipo correto e se o parceiro de link (por exemplo, switch ou hub) está funcionando corretamente.
5	O link da rede está ativo.	O adaptador estabeleceu um link.	Mensagem apenas para informação. Nenhuma ação necessária.

Tabela 11: Mensagens de log do driver de base (Cont.)

Mensagem Número	Mensagem	Causa	Ação corretiva
6	Controlador de rede configurado para link half-duplex de 10 Mb.	O adaptador foi configurado manualmente para a velocidade da linha selecionada e configurações duplex.	Mensagem apenas para informação. Nenhuma ação necessária.
7	Controlador de rede configurado para link full-duplex de 10 Mb.	O adaptador foi configurado manualmente para a velocidade da linha selecionada e configurações duplex.	Mensagem apenas para informação. Nenhuma ação necessária.
8	Controlador de rede configurado para link half-duplex de 100 Mb.	O adaptador foi configurado manualmente para a velocidade da linha selecionada e configurações duplex.	Mensagem apenas para informação. Nenhuma ação necessária.
9	Controlador de rede configurado para link full-duplex de 100 Mb.	O adaptador foi configurado manualmente para a velocidade da linha selecionada e configurações duplex.	Mensagem apenas para informação. Nenhuma ação necessária.
10	Controlador de rede configurado para link half-duplex de 1Gb.	O adaptador foi configurado manualmente para a velocidade da linha selecionada e configurações duplex.	Mensagem apenas para informação. Nenhuma ação necessária.
11	Controlador de rede configurado para link full-duplex de 1Gb.	O adaptador foi configurado manualmente para a velocidade da linha selecionada e configurações duplex.	Mensagem apenas para informação. Nenhuma ação necessária.
12	Mídia não suportada.	O sistema operacional não suporta a mídia IEEE 802.3.	Reinicie o sistema operacional, verifique a existência de vírus, faça uma verificação de disco (chkdsk) e reinstale o sistema operacional.
13	Impossível registrar a rotina de interrupção do serviço.	O driver do dispositivo não pode instalar o handler de interrupção.	Reinicie o sistema operacional; remova outros drivers do dispositivo que possam compartilhar o mesmo IRQ.
14	Impossível mapear o espaço de ES.	O driver do dispositivo não pode alocar E/S mapeado de memória para acessar os registros do driver.	Remova outros adaptadores do sistema, reduza a memória física instalada e substitua o adaptador.
15	Driver inicializado com sucesso.	O driver foi carregado com sucesso.	Mensagem apenas para informação. Nenhuma ação necessária.
16	O NDIS está redefinindo o driver da miniporta.	A camada do NDIS detectou um problema de envio/recebimento de pacotes e está redefinindo o driver para resolver o problema.	Execute o diagnóstico do Broadcom Advanced Control Suite; verifique se o cabo de rede está em boas condições.

Tabela 11: Mensagens de log do driver de base (Cont.)

Mensagem Número	Mensagem	Causa	Ação corretiva
18	PHY desconhecido detectado. Uso de uma rotina de inicialização PHY padrão.	O driver não conseguiu ler o ID de PHY.	Substitua o adaptador.
19	Este driver não suporta este dispositivo. Atualize para o driver mais recente.	O driver não reconhece o adaptador do instalador.	Atualize para uma versão de driver que suporta este adaptador.
20	Falha na inicialização do driver.	Falha não especificada durante a inicialização do driver.	Reinstale o driver, atualize para uma versão mais recente, execute o diagnóstico do Broadcom Advanced Control Suite ou substitua o adaptador.
21	Ethernet@WireSpeed está habilitado e não poderia negociar velocidade máxima de link.	Possível cabo ou conexão defeituoso.	Reconecte o cabo ou altere o cabo.
22	Não foi possível instalar o driver do dispositivo para o controlador de rede obsoleto para este sistema operacional.	O driver de outbox mais recente não suporta mais o dispositivo obsoleto.	use o driver da inbox do SO ou substitua o dispositivo ou um mais recente.
256	Não há memória físico contígua suficiente para o reservatório coalescente.	O driver não conseguiu alocar memória compartilhada suficiente para os buffers do pacote coalescente.	Remova/desabilite outro adaptador do sistema ou aumente a memória do sistema.

Driver intermediário (Adaptador/Equipe Virtual)

Tabela 12 lista as mensagens do log de evento suportadas pelo driver intermediário, explica a causa da mensagem e fornece a ação recomendada.

Tabela 12: Mensagens de log do driver intermediário

Evento do sistema Número da mensagem	Mensagem	Causa	Ação corretiva
1	Impossível efetuar registro com a NDIS.	O driver não pode efetuar registro com a interface NDIS.	Descarregue outros drivers de NDIS.
2	Impossível instanciar a interface de gerenciamento.	O driver não pode criar a instância do dispositivo.	Reinicie o sistema operacional.
3	Impossível criar o link simbólico para a interface de gerenciamento.	Outro driver criou um nome de dispositivo conflitante.	Descarregue o driver do dispositivo conflitante que usa o nome <i>Blf</i> .
4	O driver do Broadcom Advanced Server Program foi iniciado.	Outro driver criou um nome de dispositivo conflitante.	Mensagem apenas para informação. Nenhuma ação necessária.
5	O driver do Broadcom Advanced Server Program foi interrompido.	O driver foi interrompido	Mensagem apenas para informação. Nenhuma ação necessária.

Tabela 12: Mensagens de log do driver intermediário (Cont.)

Evento do sistema Número da mensagem	Mensagem	Causa	Ação corretiva
6	Impossível alocar memória para estruturas de dados internos.	O driver não pode alocar memória do sistema operacional.	Feche os aplicativos de execução para liberar memória.
7	Impossível vincular ao adaptador.	O driver não pôde abrir um dos adaptadores físicos da equipe.	Descarregue e recarregue o driver do adaptador físico, instale um driver do adaptador físico atualizado ou substitua o adaptador físico.
8	Vinculação com sucesso ao adaptador.	O driver abriu o adaptador físico com sucesso.	Mensagem apenas para informação. Nenhuma ação necessária.
9	O adaptador de rede está desconectado.	O adaptador físico não está conectado à rede (não estabeleceu link).	Verifique se o cabo da rede está conectado, se o cabo da rede é do tipo correto e se o parceiro de link (switch ou hub) está funcionando corretamente.
10	O adaptador de rede está conectado.	O adaptador físico está conectado à rede (estabeleceu link).	Mensagem apenas para informação. Nenhuma ação necessária.
11	O driver de recursos do Broadcom Advanced Program não é designado para executar nesta versão do Sistema Operacional.	O driver não suporta o sistema operacional no qual foi instalado.	Consulte as notas da versão e instale o driver em um sistema operacional suportado ou atualize o driver.
12	O adaptador de reserva é selecionado como o adaptador primário de uma equipe sem um adaptador de equilíbrio de carga.	Um adaptador de reserva foi ativado.	Substitua o adaptador físico com falha.
13	O adaptador de rede não suporta limite de falha avançado.	O adaptador físico não suporta a Broadcom NIC Extension (NICE).	Substitua o adaptador por um que suporte NICE.
14	O adaptador de rede foi ativado através da interface de gerenciamento.	O driver ativou com sucesso o adaptador físico através de uma interface de gerenciamento.	Mensagem apenas para informação. Nenhuma ação necessária.
15	O adaptador de rede foi desativado através da interface de gerenciamento.	O driver desativou com sucesso o adaptador físico através de uma interface de gerenciamento.	Mensagem apenas para informação. Nenhuma ação necessária.
16	O adaptador da rede está ativado e está participando do tráfego da rede.	Um adaptador físico foi adicionado ou ativado na equipe.	Mensagem apenas para informação. Nenhuma ação necessária.
17	O adaptador de rede está desativado e não está mais participando do tráfego da rede.	O driver não reconhece o adaptador do instalador.	Mensagem apenas para informação. Nenhuma ação necessária.

Seção 4: LANs virtuais

- [Visão geral de VLANs](#)
- [Adição de VLANs às equipes](#)

Visão geral de VLANs

As VLANs permitem dividir a LAN física em partes lógicas, a fim de criar segmentação lógica de grupos de trabalhos e reforçar as políticas de segurança entre cada segmento lógico. Cada VLAN definida comporta-se como a própria rede separada, com tráfego e transmissões isolados um dos outros, aumentando a eficiência da largura da banda em cada grupo lógico. Até 64 VLANs (63 marcadas e 1 desmarcada) podem ser definidas para cada adaptador Broadcom no servidor, dependendo do total de memória disponível no sistema.

É possível adicionar VLANs a uma equipe para permitir várias VLANs com IDS de VLAN diferentes. Um adaptador virtual é criado para cada VLAN adicionada.

Embora as VLANs sejam normalmente utilizadas para criar domínios individuais de transmissão e/ou sub-redes separadas de IP, às vezes torna-se útil que um servidor tenha uma presença em mais de uma VLAN simultaneamente. Os adaptadores da Broadcom suportam várias VLANs por porta ou por equipe, permitindo configurações de rede muito flexíveis.

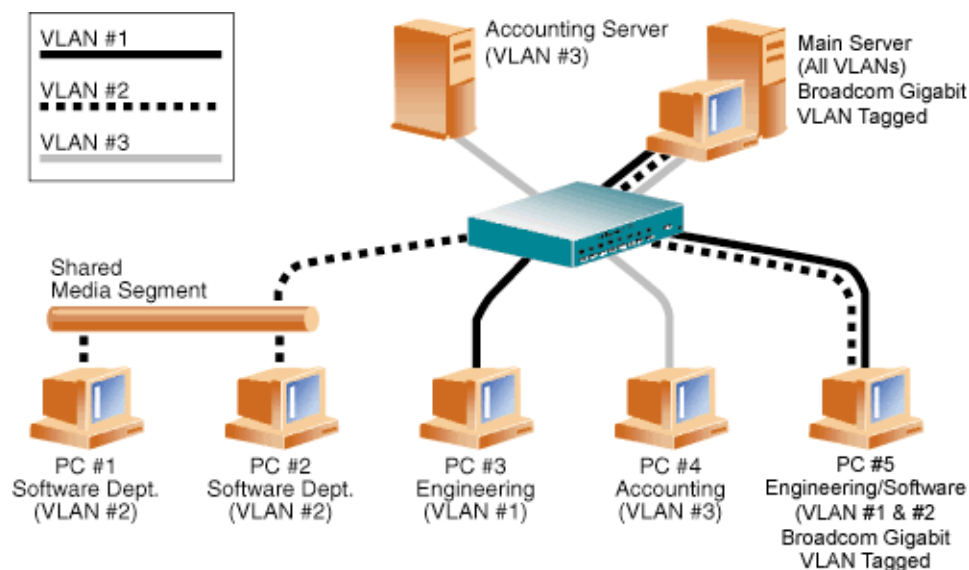


Figura 7: Exemplo de servidores que suportam várias VLANs com marcação

[Figura 7](#) mostra um exemplo de rede que usa VLANs. Nesse exemplo de rede, a LAN física consiste em um switch, dois servidores e cinco clientes. A LAN é organizada de forma lógica em três VLANs diferentes, cada uma representando uma sub-rede de IP diferente. Os recursos desta rede estão descritos na [Tabela 13](#):

Tabela 13: Exemplo de topologia de rede VLAN

Componente	Descrição
VLAN 1	Uma sub-rede de IP formada pelo Servidor principal, PC 3 e PC 5. Essa sub-rede representa um grupo de engenharia.
VLAN 2	Inclui o Servidor principal, PCs 1 e 2 via segmento compartilhado de mídia e PC 5. Essa VLAN é um grupo de desenvolvimento de software.
VLAN 3	Inclui o Servidor principal, o Servidor de contabilidade e o PC 4. Essa VLAN é um grupo de contabilidade.
Servidor principal	Um servidor de uso intenso que precisa ser acessado em todas as VLANs e sub-redes de IP. O Servidor principal possui um adaptador Broadcom instalado. Todas as três sub-redes IP são acessadas por meio da única interface do adaptador físico. O servidor é acoplado a uma das portas do switch, configuradas para as VLANs 1, 2 e 3. A marcação está ativada tanto para o adaptador quanto para a porta do switch. Devido aos recursos de marcação de VLAN dos dois dispositivos, o servidor pode se comunicar em todas as três sub-redes de IP nesta rede, mas continua a manter a separação de transmissão entre todas elas.
Servidor de contabilidade	Disponível apenas para a VLAN 3. O Servidor de contabilidade é isolado de todo o tráfego das VLANs 1 e 2. A marcação é desativada na porta do switch conectada ao servidor.
PCs 1 e 2	Acoplados a um hub de mídia compartilhada que é, então, conectado ao switch. Os PCs 1 e 2 pertencem apenas à VLAN 2 e estão logicamente na mesma sub-rede de IP que a do Servidor principal e do PC 5. A marcação é desativada na porta do switch conectada a esse segmento.
PC 3	Um membro da VLAN 1, o PC 3, pode se comunicar apenas com o Servidor principal e o PC 5. A marcação não está ativada na porta do switch do PC 3.
PC No. 4	Um membro da VLAN 3, o PC 4, pode se comunicar apenas com os servidores. A marcação não está ativada na porta do switch do PC no. 4.
PC no. 5	Um membro das VLANs 1 e 2, o PC 5 possui um adaptador Broadcom instalado. Ele está conectado à porta 10 do switch. Tanto o adaptador quanto a porta do switch estão configurados para as VLANs 1 e 2 e possuem a marcação ativada.



Nota: A marcação da VLAN precisa estar ativada apenas em portas de switch que criam links de entroncamento a outros switches ou em portas conectadas a estações finais com capacidade para o recurso de marcação como, por exemplo, servidores ou estações de trabalho com adaptadores Broadcom.

Adição de VLANs às equipes

Cada equipe suporta até 64 VLANs (63 marcadas e 1 desmarcada). Com várias VLANs em um adaptador, um servidor com um único adaptador pode ter uma presença lógica em várias sub-redes de IP. Com várias VLANs em uma equipe, um servidor pode ter uma presença lógica em várias sub-redes de IP e se beneficiar com o equilíbrio de falha e o limite de falha. Para obter instruções sobre como adicionar uma VLAN a uma equipe, consulte [Adicionar VLAN](#) para sistemas operacionais Windows.



Nota: Os adaptadores que são membros de uma equipe de limite de falha também podem ser configurados para oferecer suporte a VLANs. Como as VLANs não são suportadas por um NIC de terceiros, se um NIC de terceiros for membro de uma equipe de limite de falha, as VLANs não podem ser configuradas para essa equipe.

Seção 5: Capacidade de gerenciamento

- CIM
- SNMP

CIM

O CIM (Common Information Model, Modelo comum de informações) é um padrão da indústria definido pela DMTF (Distributed Management Task Force, Força tarefa de gerenciamento distribuído). A Microsoft implementa o CIM em plataformas do Windows como, por exemplo, o Windows Server 2008. A Broadcom oferecerá suporte ao CIM nas plataformas de Windows Server 2008.

A implementação do CIM da Broadcom oferece várias classes para fornecer informações aos usuários por meio de aplicativos clientes do CIM. Observe que os provedores de dados do CIM da Broadcom fornecerão apenas dados, e os usuários poderão escolher os softwares clientes do CIM preferidos para navegar pelas informações fornecidas pelo provedor do CIM da Broadcom.

O provedor do CIM da Broadcom fornece informações por meio das classes `BRCM_NetworkAdapter` e `BRCM_ExtraCapacityGroup`. A classe `BRCM_NetworkAdapter` fornece informações sobre adaptadores de rede pertencentes a um grupo de adaptadores, incluindo controladores Broadcom e de outros fornecedores. A classe `BRCM_ExtraCapacityGroup` oferece configuração de equipe para o BASP (Broadcom Advanced Server Program, Programa do Servidor Avançado da Broadcom). A implementação atual fornece informações sobre as equipes e sobre adaptadores de rede física na equipe.

O Broadcom Advanced Server Program fornece eventos por meio de registros de eventos. Os usuários podem utilizar o "Visualizador de eventos", fornecido pelas plataformas Windows Server 2008, ou o CIM para inspecionar ou monitorar esses eventos. O provedor do CIM da Broadcom fornecerá também informações do evento por meio do modelo genérico de eventos do CIM. Esses eventos são `__InstanceCreationEvent`, `__InstanceDeletionEvent` e `__InstanceModificationEvent` e são definidos pelo CIM. O CIM precisa do aplicativo cliente para registrar os eventos no aplicativo cliente utilizando consultas, como nos exemplos mostrados a seguir, para receber os eventos corretamente.

```
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 obter informações detalhadas sobre esses eventos, consulte a documentação do CIM em http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf.

SNMP

Subagente do BASP

O subagente do BASP, `baspmgmt.dll`, foi desenvolvido para o serviço SNMP do Windows Server. É necessário instalar o serviço SNMP antes de instalar o subagente do BASP.

O subagente do BASP permite que um software gerenciador de SNMP monitore ativamente as configurações e o desempenho dos recursos do Broadcom Advanced Server. O subagente também fornece uma rotina de alarmes a um gerenciador do SNMP para informar-lhe sobre qualquer alteração nas condições do componente BASP.

O subagente BASP também permite o monitoramento das configurações e das estatísticas das equipes BASP, dos adaptadores físicos da NIC que participam de uma equipe e dos adaptadores virtuais da NIC criados como resultado da formação de uma equipe. Adaptadores NIC que não estejam em equipes não são monitorados neste momento. Os dados de configuração do BASP incluem informações como: IDs das equipes, IDs e descrições dos adaptadores físicos/virtuais/de VLAN/de equipe e endereços MAC dos adaptadores.

As estatísticas incluem informações detalhadas como, por exemplo, os pacotes de dados transmitidos e recebidos para os adaptadores físicos/virtuais/de VLAN/de equipe.

A rotina de alarmes encaminha informações sobre as alterações na configuração dos adaptadores físicos que participam de uma equipe, por exemplo: link superior/inferior do adaptador físico e eventos instalados/removidos do adaptador.

Para monitorar as informações descritas acima, um gerenciador do SNMP precisa carregar os arquivos do banco de dados MIB do BASP da Broadcom. Esses arquivos, que são mostrados abaixo, estão incluídos na mídia de origem do driver:

`baspcfg.mib`

`baspmat.mib`

`basptrap.mib`

Agente extensível do BASP

O agente extensível Broadcom NetXtreme Gigabit Ethernet Controller Extended Information SNMP, `bcmif.dll`, foi desenvolvido para o serviço SNMP do Windows Server 2008.

O agente extensível permite que o software gerenciador do SNMP monitore ativamente as configurações do adaptador Broadcom NetXtreme. Ele destina-se a complementar as informações já fornecidas pela Interface de rede de gerenciamento padrão do SNMP.

O agente extensível fornece informações detalhadas sobre um adaptador BroadcomNetXtreme, como:

- Endereço MAC
- Endereço IP vinculado
- Máscara de sub-rede IP
- Status do link físico
- Estado do adaptador
- Velocidade da linha
- Modo duplex

- Intervalo de memória
- Definição de interrupção
- N° do barramento
- N° do dispositivo
- N° da função

Para monitorar as informações descritas acima, um gerenciador do SNMP precisa carregar o arquivo MIB das informações estendidas Broadcom. Esse arquivo, bcmif.mib, está incluso no CD de instalação do adaptador Broadcom NetXtreme.

A estação de trabalho monitorada requer a instalação do agente extensível Broadcom Extended Information SNMP (bcmif.dll) e exige que o serviço SNMP do Microsoft Windows 2008 seja instalado e carregado.

Seção 6: Instalação do hardware

- [Precauções de segurança](#)
- [Lista de verificação de pré-instalação](#)
- [Instalação do adaptador](#)
- [Conexão dos cabos de rede](#)



Nota: Esta seção aplica-se apenas aos modelos de adaptadores Broadcom NetXtreme Gigabit Ethernet com NIC integrada.

Precauções de segurança



Cuidado! O adaptador está sendo instalado em um sistema que opera com tensões que podem ser fatais. Antes de remover a tampa do sistema, observe as precauções a seguir para sua proteção e para evitar danos aos componentes do sistema:

- Remova qualquer objeto metálico ou joia das mãos e dos pulsos.
- Utilize apenas ferramentas isoladas ou não-condutoras de eletricidade.
- Verifique se o sistema está DESLIGADO e desconectado antes de tocar qualquer um dos componentes internos.
- Instale ou remova adaptadores em um ambiente livre de energia estática. É recomendável o uso de uma pulseira antiestática devidamente aterrada, ou outros dispositivos pessoais antiestáticos, e uma esteira antiestática.

Lista de verificação de pré-instalação

1. Verifique se o servidor está utilizando o BIOS mais recente.
2. Se seu sistema estiver inicializado em um sistema operacional, deligue normalmente o SO.
3. Quando o encerramento do sistema estiver concluído, desligue a alimentação do sistema e desconecte o cabo de alimentação.
4. Segurando a placa do adaptador pelas bordas, remova-a da sua embalagem de envio e coloque-a sobre uma superfície antiestática.
5. Verifique se há sinais visíveis de danos, particularmente no conector da borda da placa. Nunca tente instalar um adaptador danificado.

Instalação do adaptador

As instruções a seguir aplicam-se à instalação do adaptador Broadcom NetXtreme Gigabit Ethernet (NIC integrada) na maioria dos servidores. Consulte os manuais fornecidos com seu servidor para obter detalhes sobre como executar essas tarefas no seu servidor específico.

1. Revise [Precauções de segurança](#) e [Lista de verificação de pré-instalação](#). Antes de instalar o adaptador, verifique se a alimentação do sistema está DESLIGADA e desconectada da tomada de energia e se os procedimentos corretos de aterramento elétrico foram seguidos.
2. Abra o sistema e selecione qualquer slot PCI Express vazio.
3. Remova a tampa branca do slot que você selecionou.
4. Alinhe a borda do conector do adaptador com o slot do conector no sistema.
5. Pressionando ambos os cantos da placa, empurre a placa do adaptador até que se encaixe firmemente no slot. Quando o adaptador estiver corretamente encaixado, os conectores da porta do adaptador serão alinhados com a abertura do slot, e sua placa ficará embutida no chassi do sistema.



Cuidado! Não use força excessiva ao encaixar a placa, pois isso pode danificar o sistema ou o adaptador. Se você tiver dificuldades ao encaixar o adaptador, remova-o, realinhe-o e tente novamente.

6. Prenda o adaptador com o prendedor do adaptador ou com o parafuso.
7. Feche o sistema e desconecte todos os dispositivos antiestáticos pessoais.

Conexão dos cabos de rede

Cobre

O adaptador Broadcom NetXtreme Gigabit Ethernet possui um ou mais conectores usados para conectar o sistema a um segmento de fio de cobre Ethernet.



Nota: O adaptador Broadcom NetXtreme Gigabit Ethernet suporta MDIX (Automatic MDI Crossover, Ponte de ligação MDI automática), o que elimina a necessidade de cabos de ponte de ligação na conexão de máquinas. Um cabo de Categoria 5 de passagem direta permite que as máquinas se comuniquem quando conectadas diretamente.

1. Selecione um cabo correto. [Tabela 14: "Especificações de cabos 10/100/1000BASE-T"](#) lista os requisitos de cabo para conexão com portas 10/100/1000BASE-T:

Tabela 14: Especificações de cabos 10/100/1000BASE-T

Tipo de porta	Conector	Mídia	Distância máxima
10BASE-T	RJ-45	Categoria 3, 4 ou 5 UTP	100 metros (328 pés)
100/1000BASE-T ¹	RJ-45	UTP Categoria 5 ²	100 metros (328 pés)

¹A sinalização 1000BASE-T requer quatro pares trançados de cabos balanceados de Categoria 5, conforme especificado nas normas ISO/IEC 11801:1995 e EIA/TIA-568-A (1995), testados usando os procedimentos definidos na norma TIA/EIA TSB95.

²A Categoria 5 é o requisito mínimo. As Categorias 5e e 6 são totalmente suportadas.

2. Conecte uma extremidade do cabo ao adaptador.
3. Conecte a outra extremidade do cabo a uma porta de rede Ethernet RJ-45.



Nota: Depois que o cabo estiver adequadamente conectado nas duas extremidades, os LEDs da porta do adaptador deverão estar funcionando. Consulte [Tabela 14: "Especificações de cabos 10/100/1000BASE-T,"](#) na [página 65](#) para obter uma descrição do link de rede e indicações de atividade

Seção 7: Criação de um disco de driver

Consulte a documentação fornecida com seu sistema para obter instruções sobre a criação de um disco de driver.

Seção 8: Software de driver do Broadcom Boot Agent

- [Visão geral](#)
- [Configuração do MBA em um ambiente de cliente](#)

Visão geral

Os adaptadores Broadcom NetXtreme Gigabit Ethernet oferecem suporte ao Preboot Execution Environment (PXE), Remote Program Load (RPL), inicialização iSCS e Bootstrap Protocol (BootP). O MBA (Multi-Boot Agent) é um módulo de software que permite que um sistema conectado a uma rede seja inicializado com imagens fornecidas por sistemas remotos pela rede. O driver Broadcom MBA obedece à especificação PXE 2.1, sendo lançado com imagens binárias monolíticas e divididas. Isso proporciona flexibilidade aos usuários em diferentes ambientes em que a placa-mãe pode ter ou não código-base incorporado.

O módulo MBA opera em um ambiente cliente/sistema. Uma rede consiste em um ou mais sistemas de inicialização que fornecem imagens de inicialização a vários sistemas pela rede. A implementação do módulo MBA pela Broadcom foi testada com sucesso nos seguintes ambientes:

- **Servidor Linux[®] Red Hat[®] PXE.** Os clientes Broadcom PXE podem inicializar e usar remotamente recursos de rede (montagem NFS e assim por diante) e executar instalações do Linux. No caso de uma inicialização remota, o driver universal Linux é perfeitamente vinculado à UNDI (Broadcom Universal Network Driver Interface, Interface de driver de rede universal da Broadcom), fornecendo uma interface de rede no ambiente Linux de cliente inicializado remotamente.
- **Intel[®] APITEST.** O driver Broadcom PXE foi aprovado em todos os conjuntos de testes de compatibilidade com API.
- **WDS (Windows Deployment Service, Serviço de implantação do Windows).** No Windows Server, o RIS foi substituído pelo WDS, que oferece um cliente Broadcom PXE para instalar sistemas operacionais Windows, inclusive o Windows Server 2008.

Configuração do MBA em um ambiente de cliente

Use o seguinte procedimento para adaptadores NIC adicionados. Para LOMs, consulte o guia do sistema do computador.

A configuração do MBA em um ambiente de cliente envolve as seguintes etapas:

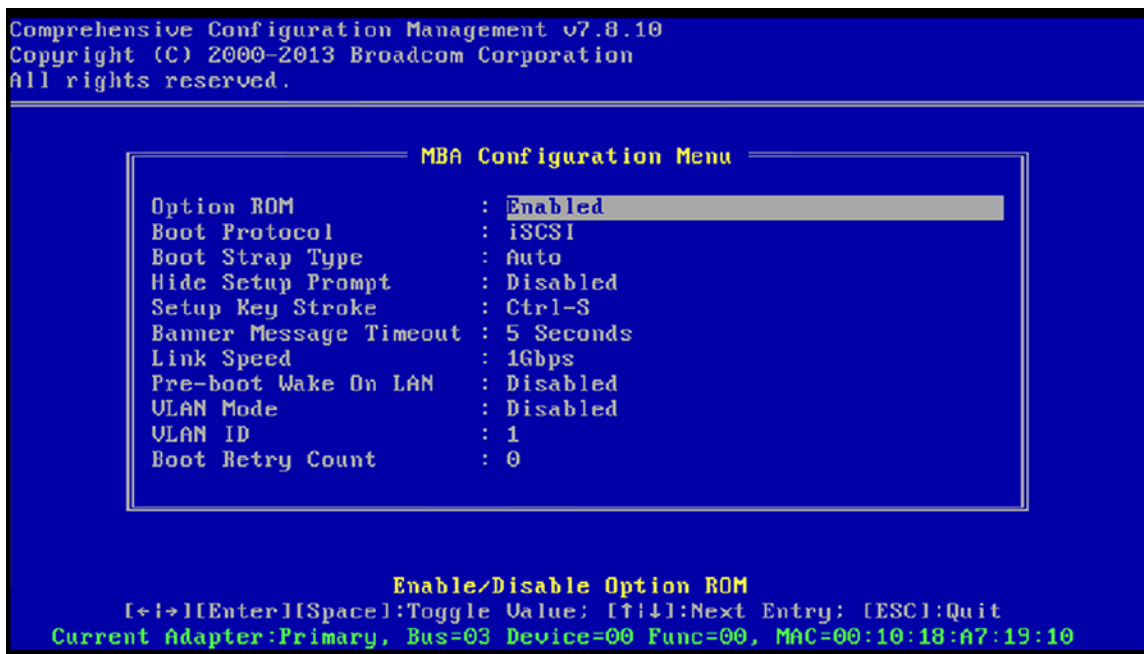
1. Configuração do driver MBA.
2. Configuração do BIOS para a ordem de inicialização.

Configuração do driver MBA

Esta seção está relacionada à configuração do driver MBA em modelos de NIC integrada do adaptador de rede Broadcom. Para configurar o driver MBA em modelos de LOM do adaptador de rede Broadcom, consulte a documentação do sistema.

Uso de CCM

1. Reinicie o sistema.
2. Pressione **CTRL+S** por 4 segundos depois que isso for solicitado. Uma lista de adaptadores é exibida.
 - a. Selecione o adaptador para configurar e pressione **Enter**. O menu principal é exibido.
 - b. Selecione **Configuração do MBA** para exibir o menu de configuração do MBA.



3. Use as teclas SETA PARA CIMA e SETA PARA BAIXO para mover até o item de menu Protocolo de inicialização. Em seguida, use a tecla SETA DIREITA ou SETA ESQUERDA para selecionar um protocolo de inicialização, se outros protocolos estiverem disponíveis, além do protocolo Preboot Execution Environment (PXE). Se disponível, outros protocolos de inicialização incluem Remote Program Load (RPL) e Bootstrap Protocol (BOOTP).



Nota: No caso de alguns, mas não todos, LOMs compatíveis com algumas, mas não todas, as inicializações iSCSI, o protocolo de inicialização é definido via BIOS. Consulte a documentação do sistema para obter mais informações.



Nota: Se você tiver vários adaptadores em seu sistema e não tiver certeza de qual adaptador está sendo configurado, pressione **CTRL+F6**, que fará com que os LEDs de porta do adaptador comecem a piscar.

4. Use as teclas SETA PARA CIMA, PARA BAIXO, PARA A ESQUERDA e PARA A DIREITA para alterar os valores de outros itens de menu, como desejar.
5. Pressione **F4** para salvar suas configurações.
6. Pressione **ESC** quando terminar.

Uso do uEFI

1. Reinicie o sistema.
2. Insira o menu de configuração do sistema (System Setup) ou do dispositivo (Device Setting).
3. Selecione o dispositivo no qual deseja alterar as configurações do MBA.
4. Selecione o **Menu de configuração do MBA**.
5. Use o menu suspenso para selecionar o protocolo de inicialização escolhido, se protocolos de inicialização diferentes do Preboot Execution Environment (PXE) estiverem disponíveis. Se disponíveis, outros protocolos de inicialização incluem iSCSI e BootP (Bootstrap Protocol).



Nota: No caso de LOMs compatíveis com inicialização iSCSI, o protocolo de inicialização é definido via BIOS. Consulte a documentação do sistema para obter mais informações.

6. Use as teclas SETA PARA CIMA, PARA BAIXO, PARA A ESQUERDA e PARA A DIREITA para alterar os valores de outros itens de menu, como desejar.
7. Selecione **Voltar** para acessar o menu principal.
8. Selecione **Concluir** para salvar e sair.

Configuração do BIOS

Para inicializar pela rede com o MBA, torne o adaptador ativado pelo MBA o primeiro dispositivo inicializável no BIOS. Esse procedimento depende da implementação do BIOS no sistema. Consulte o manual do usuário do sistema para obter instruções.

Seção 9: Protocolo iSCSI

- [Inicialização iSCSI](#)
- [iSCSI Crash Dump](#)

Inicialização iSCSI

Os adaptadores Broadcom NetXtreme Gigabit Ethernet suportam a inicialização iSCSI para permitir que sistemas sem disco realizem a inicialização em rede dos sistemas operacionais. A inicialização iSCSI permite que um sistema operacional Windows ou Linux seja inicializado a partir de uma máquina iSCSI alvo, localizada remotamente em uma rede IP padrão.

Para os sistemas operacionais Windows e Linux, a inicialização da iSCSI pode ser configurada com os parâmetros gerais mostrados em [Tabela 15](#).

Sistemas operacionais com suporte para inicialização iSCSI

Os adaptadores Broadcom NetXtreme Gigabit Ethernet suportam a inicialização iSCSI nos seguintes sistemas operacionais:

- Sistema operacional do servidor Windows
- Distribuição do Enterprise

Configuração da inicialização iSCSI

A inicialização iSCSI não é compatível com o modo BIOS quando o armazenamento local (especialmente RAID) está presente devido à restrições da memória EBDA.

A configuração da inicialização iSCSI inclui:

- [A configuração da iSCSI-alvo](#)
- [Configuração dos parâmetros da inicialização iSCSI](#)
- [Preparação da imagem de inicialização iSCSI](#)
- [Inicialização](#)

A configuração da iSCSI-alvo

A configuração da iSCSI-alvo varia de acordo com os fornecedores. Para obter mais informações sobre como configurar a iSCSI-alvo, consulte a documentação fornecida pelo fornecedor. O processo geral inclui as seguintes etapas:

1. Crie uma iSCSI-alvo.
2. Crie um disco virtual.
3. Mapeie o disco virtual para a iSCSI-alvo criada na etapa 1.

4. Associe um software de inicialização de iSCSI à iSCSI-alvo.
5. Grave o nome da iSCSI-alvo, o número da porta TCP, o número da unidade lógica (LUN) do iSCSI, o IQN (Internet Qualified Name, Nome de qualificação para a Internet) do software de inicialização e as informações sobre a autenticação CHAP.
6. Após configurar a iSCSI-alvo, obtenha as seguintes informações:
 - Nome IQN de destino
 - Endereço IP do alvo
 - Número da porta TCP do alvo
 - LUN do alvo
 - IQN do software de inicialização
 - ID e segredo CHAP

Configuração dos parâmetros da inicialização iSCSI

Defina a configuração do software de inicialização iSCSI Broadcom como estática ou dinâmica. Consulte [Tabela 15](#) para conhecer as opções de configuração disponíveis na tela General Parameters (Parâmetros gerais).

[Tabela 15](#) lista os parâmetros para IPv4 e IPv6. Os parâmetros específicos de IPv4 ou IPv6 são anotados.



Nota: A disponibilidade da inicialização iSCSI por IPv6 depende da plataforma/dispositivo.

Tabela 15: Opções de configuração

Opção	Descrição
TCP/IP parameters via DHCP (Parâmetros TCP/IP via DHCP)	Esta opção é específica do IPv4. Controla se o software host de inicialização iSCSI irá obter o endereço IP por meio do DHCP (opção ativada) ou de uma configuração de IP estática (opção desativada).
Autoconfiguração de IP	Esta opção é específica do IPv6. Controla se o software host da inicialização iSCSI irá configurar um endereço de link local em estado e/ou um endereço com informações de estado se o DHCPv6 estiver presente e em uso (Ativado). Pacotes de solicitação do roteador são enviados por três vezes em intervalos de quatro segundos entre cada tentativa. Opcionalmente, use uma configuração de IP estática (opção desativada).
iSCSI parameters via DHCP (Parâmetros iSCSI via DHCP)	Controla se o software host de inicialização iSCSI irá obter os parâmetros da sua iSCSI-alvo por meio do DHCP (opção ativada) ou de uma configuração estática (opção desativada). As informações estáticas são inseridas na tela iSCSI Initiator Parameters Configuration (Configuração dos parâmetros da inicialização iSCSI).
CHAP Authentication (Autenticação CHAP)	Controla se o software host de inicialização iSCSI irá utilizar a autenticação CHAP ao se conectar com a iSCSI-alvo. Quando a autenticação CHAP está ativada, o ID e o segredo CHAP são inseridos na tela iSCSI Initiator Parameters Configuration.
DHCP Vendor ID (ID do fornecedor de DHCP)	Controla o modo como o software host de inicialização iSCSI interpreta o campo Vendor Class ID (ID de classe do fornecedor) usado durante o DHCP. Se o campo Vendor Class ID do pacote DHCP Offer tiver o mesmo valor, o software host de inicialização iSCSI tenta encontrar as extensões de inicialização solicitadas nos 43 campos de Opções de DHCP. Quando a função DHCP está desativada, esse valor não precisa ser definido.
Link Up Delay Time (Tempo de espera do link ativo)	Controla quanto tempo, em segundos, o software host de inicialização iSCSI deve aguardar para enviar algum dado pela rede depois que um link Ethernet é estabelecido. Os valores válidos são de 0 a 255. Por exemplo, um usuário pode ter que definir um valor para esta opção se um protocolo de rede, como o Spanning Tree, estiver ativado na interface do switch com o sistema cliente.

Tabela 15: Opções de configuração (Cont.)

Opção	Descrição
Use TCP Timestamp (Carimbo de data/hora do TCP)	Controla se a opção TCP Timestamp (Carimbo de data/hora do TCP) está ativada ou desativada.
Target as First HDD (Alvo definido como a primeira unidade de disco rígido)	Permite que a iSCSI-alvo seja exibida como a primeira unidade de disco rígido do sistema.
LUN Busy Retry Count (Contagem de tentativas para LUN ocupado)	Controla o número de tentativas de conexão que o software de inicialização iSCSI poderá fazer se o LUN da iSCSI-alvo estiver ocupado.
Versão IP	Esta opção é específica do IPv6. Alterna entre o protocolo IPv4 ou IPv6. Todas as configurações IP serão perdidas ao alternar de uma versão de protocolo para outra.

Configuração do protocolo de inicialização do MBA

Para configurar o protocolo de inicialização

1. Reinicie o sistema.
2. Na faixa do PXE, pressione **CTRL+S**. O menu MBA Configuration (Configuração do MBA) é exibido (consulte a seção [Broadcom Boot Agent](#)).
3. No menu MBA Configuration, use a tecla de **SETA PARA CIMA** ou de **SETA PARA BAIXO** para acessar a opção **Boot Protocol** (Protocolo de inicialização). Use a tecla de **SETA PARA A ESQUERDA** ou de **SETA PARA A DIREITA** para alterar a opção **Boot Protocol** para **iSCSI**.



Nota: Para as plataformas em que o protocolo de inicialização está definido via BIOS, consulte a documentação do sistema para obter mais informações.

4. Selecione **Configuração de inicialização iSCSI** no menu **Principal**.



Nota: Se o firmware de inicialização iSCSI não estiver programado no NetXtreme adaptador de rede, pressionar **Configuração de inicialização iSCSI** não terá nenhum efeito.

Configuração de inicialização iSCSI


- [Configuração de inicialização iSCSI estática](#)
- [Configuração de inicialização iSCSI dinâmica](#)

Configuração de inicialização iSCSI estática

Em uma configuração estática, você deve fornecer o endereço IP do sistema, o IQN do software de inicialização do sistema e os parâmetros do alvo obtidos em [A configuração da iSCSI-alvo](#). Para obter informações sobre as opções de configuração, consulte [Tabela 15](#).

Para configurar os parâmetros da inicialização iSCSI por meio de configuração estática

1. Na tela **Menu General Parameters (Parâmetros gerais)**, defina as seguintes configurações:
 - **TCP/IP parameters via DHCP** (Parâmetros TCP/IP via DHCP): Disabled (Desativados). (Para IPv4.)
 - **IP Autoconfiguration** (Autoconfiguração IP): Disabled (Desativada). (Para IPv6)
 - **iSCSI parameters via DHCP** (Parâmetros iSCSI via DHCP): Disabled (Desativados).
 - **CHAP Authentication** (Autenticação CHAP): (Desativada).
 - **Boot to iSCSI target** (Inicialização a partir da iSCSI-alvo): (Desativada).

- **DHCP Vendor ID** (ID do fornecedor de DHCP): BRCM ISAN
 - **Link Up Delay Time** (Tempo de espera do link ativo): 0
 - **Use TCP Timestamp** (Carimbo de data/hora do TCP): Enabled (Ativado) (para alguns alvos, como o **Dell/EMC AX100i**, é necessário ativar essa opção)
 - **Target as First HDD** (Alvo definido como a primeira unidade de disco rígido): Disabled (Desativado).
 - **LUN Busy Retry Count** (Contagem de tentativas para LUN ocupado): 0
 - **IP Version** (Versão IP): IPv6. (Para IPv6)
2. Pressione **ESC** para retornar ao menu **Principal**.
 3. No menu **Principal**, selecione a opção **Initiator Parameters** (Parâmetros da inicialização).
 4. Na tela **Initiator Parameters**, digite os valores para os campos descritos abaixo:
 - Endereço IP (endereços IPv4 e IPv6 não especificados devem ser "0.0.0.0" e ":::", respectivamente)
 - Prefixo da máscara de sub-rede
 - Gateway padrão
 - DNS primário
 - DNS secundário
 - Nome iSCSI (corresponde ao nome da inicialização iSCSI que será usado pelo sistema cliente)
-  **Nota:** Insira o endereço IP com cautela. Não há verificação de erro referente ao endereço IP para confirmar se não há duplicatas ou atribuições incorretas de segmento/rede.
5. Pressione **ESC** para retornar ao menu **Principal**.
 6. No menu **Principal**, selecione a opção **1st Target Parameters** (Parâmetros do primeiro alvo).
 7. Na tela **1st Target Parameters**, ative a opção **Connect** (Conectar) para se conectar à iSCSI-alvo. Digite os valores para os campos descritos abaixo, usando os mesmos valores inseridos durante a configuração da iSCSI-alvo:
 - Endereço IP
 - Porta TCP
 - LUN de inicialização
 - Nome iSCSI
 8. Pressione **ESC** para retornar ao menu **Principal**.
 9. Pressione **ESC** e clique em **Exit and Save Configuration** (Sair e salvar a configuração).
 10. Pressione **F4** para salvar a configuração do MBA .

Configuração de inicialização iSCSI dinâmica

Em uma configuração dinâmica, você precisa especificar apenas que as informações do endereço IP do sistema e do alvo/inicialização são fornecidas pelo servidor DHCP (consulte as configurações IPv4 e IPv6 em [Configuração do servidor DHCP para suportar a inicialização iSCSI](#)). No caso do IPv4, com exceção do nome da inicialização iSCSI, todas as configurações contidas nas telas Initiator Parameters (Parâmetros da inicialização), 1st Target Parameters (Parâmetros do primeiro alvo) ou 2nd Target Parameters são ignoradas e não precisam ser apagadas. No caso do IPv6, com exceção do ID e segredo CHAP, todas as configurações contidas nas telas Initiator Parameters (Parâmetros da inicialização), 1st Target Parameters (Parâmetros do primeiro alvo) ou 2nd Target Parameters (Parâmetros do segundo alvo) são ignoradas e não precisam ser apagadas. Para obter informações sobre as opções de configuração, consulte [Tabela 15](#).

**OBSERVAÇÕES:**

- Quando um servidor DHCP é utilizado, as entradas do servidor DNS são substituídas pelos valores fornecidos pelo servidor DHCP. Isso ocorre mesmo quando os valores fornecidos localmente são válidos e o servidor DHCP não fornece nenhuma informação sobre o servidor DNS. Quando o servidor DHCP não fornece nenhuma informação sobre o servidor DNS, os valores dos servidores DNS primário e secundário são definidos como 0.0.0.0. Quando o sistema operacional?Windows assume o controle, o iSCSI Initiator da Microsoft recupera os parâmetros do programa de inicialização iSCSI e configura estaticamente os registros apropriados. Isso faz com que todas as configurações sejam substituídas. Como o daemon de DHCP é executado no ambiente do Windows na forma de um processo do usuário, todos os parâmetros TCP/IP precisam ser estaticamente configurados antes que a pilha seja restabelecida no ambiente da inicialização iSCSI.
- Quando a opção 17 de DHCP é utilizada, as informações do alvo são fornecidas pelo servidor DHCP, e o nome da inicialização iSCSI é recuperado a partir do valor programado na tela Initiator Parameters. Se nenhum valor tiver sido selecionado, o controlador define como padrão o nome:

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

onde a sequência 11.22.33.44.55.66 corresponde ao endereço MAC do controlador.

Quando a opção 43 (somente IPv4) de DHCP é utilizada, todas as configurações das telas Initiator Parameters (Parâmetros da inicialização), 1st Target Parameters (Parâmetros do primeiro alvo) ou 2nd Target Parameters (Parâmetros do segundo alvo) são ignoradas e não precisam ser apagadas.

Para configurar os parâmetros da inicialização iSCSI por meio de configuração dinâmica

1. Na tela **Menu General Parameters (Parâmetros gerais)**, defina as seguintes configurações:
 - **TCP/IP parameters via DHCP** (Parâmetros TCP/IP via DHCP): Enabled (Ativados). (Para IPv4.)
 - **IP Autoconfiguration** (Autoconfiguração IP): Enabled (Ativada). (Para IPv6)
 - **iSCSI parameters via DHCP** (Parâmetros iSCSI via DHCP): Enabled (Ativados).
 - **CHAP Authentication** (Autenticação CHAP): (Desativada).
 - **Boot to iSCSI target** (Inicialização a partir da iSCSI-alvo): (Desativada).
 - **DHCP Vendor ID** (ID do fornecedor de DHCP): BRCM ISAN
 - **Link Up Delay Time** (Tempo de espera do link ativo): 0
 - **Use TCP Timestamp** (Carimbo de data/hora do TCP): Enabled (Ativado) (para alguns alvos, como o **Dell/EMC AX100i**, é necessário ativar essa opção)
 - **Target as First HDD** (Alvo definido como a primeira unidade de disco rígido): Disabled (Desativado).
 - **LUN Busy Retry Count** (Contagem de tentativas para LUN ocupado): 0
 - **IP Version** (Versão IP): IPv6. (Para IPv6)
2. Pressione **ESC** para retornar ao menu **Principal**.



Nota: As informações das telas **Initiator Parameters** e **1st Target Parameters** são ignoradas e não precisam ser apagadas.

3. Selecione **Exit and Save Configurations** (Sair e salvar as configurações).

Ativação da opção CHAP Authentication

Certifique-se de que a autenticação CHAP está ativada no destino.

Ativar autenticação CHAP

1. Na tela **General Parameters** (Parâmetros gerais), defina a opção **CHAP Authentication** (Autenticação de CHAP) como **Ativada**.
2. Na tela **Initiator Parameters** (Parâmetros iniciadores), digite os valores para os campos descritos abaixo:
 - ID CHAP (até 128 bytes)
 - Segredo CHAP (usado quando a autenticação é obrigatória; deve ter no mínimo 12 caracteres)
3. Pressione **ESC** para retornar ao menu **Principal**.
4. No menu **Principal**, selecione a opção **1st Target Parameters** (Parâmetros do primeiro alvo).
5. Na tela **1st Target Parameters** (Parâmetros do primeiro alvo), digite os valores para os campos descritos abaixo, usando os mesmos valores inseridos durante a configuração da iSCSI-alvo:
 - ID CHAP (opcional se a autenticação CHAP for de duas vias)
 - Segredo CHAP (opcional se a autenticação CHAP for de duas vias; deve ter no mínimo 12 caracteres)
6. Pressione **ESC** para retornar ao menu **Principal**.
7. Pressione **ESC** e clique em **Exit and Save Configuration** (Sair e salvar a configuração).

Configuração do servidor DHCP para suportar a inicialização iSCSI

O servidor DHCP é um componente opcional e é necessário apenas se você for realizar uma configuração de inicialização iSCSI dinâmica (consulte [Configuração de inicialização iSCSI dinâmica](#)).

A configuração do servidor DHCP para oferecer suporte à inicialização iSCSI é diferente para os protocolos IPv4 e IPv6.

- [Configurações de inicialização iSCSI do DHCP para IPv4](#)
- [Configuração de inicialização iSCSI do DHCP para IPv6](#)

Configurações de inicialização iSCSI do DHCP para IPv4

O protocolo DHCP contém várias opções que fornecem informações de configuração ao DHCP cliente. Para a inicialização iSCSI, os adaptadores Broadcom suportam as seguintes configurações de DHCP:

- [Opção 17 de DHCP, Caminho raiz](#)
- [Opção 43 de DHCP, informações específicas do fornecedor](#)

Opção 17 de DHCP, Caminho raiz

A opção 17 é utilizada para o transporte de informações da iSCSI-alvo à iSCSI cliente.

O formato do caminho raiz, conforme definido pelo padrão IETF RFC 4173, é:

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

Os parâmetros estão definidos abaixo.

Tabela 16: Definição de parâmetros para a opção 17 de DHCP

Parâmetro	Definição
"iscsi:"	Uma sequência literal.
<servername>	O endereço IP ou o FQDN da iSCSI-alvo.
":"	Um separador.
<protocol>	O protocolo IP usado para acessar a iSCSI-alvo. Atualmente, apenas o TCP é suportado, portanto, o valor que define o protocolo é 6.
<port>	O número de porta associado ao protocolo. O número de porta padrão para a iSCSI é 3260.
<LUN>	O número da unidade lógica que será usado na iSCSI-alvo. É necessário que o valor do LUN seja representado no formato hexadecimal. Um LUN com uma ID OF 64 deveria ser configurado como 40 na opção do parâmetro 17 no servidor DHCP.
<targetname>	O nome do alvo em formato IQN ou EUI (consulte o padrão RFC 3720 para obter informações detalhadas sobre os formatos IQN e EUI). Como exemplo de IQN (Internet Qualified Name, Nome de qualificação para a Internet), temos "iqn.1995-05.com.broadcom:iscsi-target".

Opção 43 de DHCP, informações específicas do fornecedor

A opção 43 de DHCP (informações específicas do fornecedor) fornece mais opções de configuração para o cliente iSCSI do que a opção 17 de DHCP. Nessa configuração, são fornecidas três subopções adicionais que atribuem o IQN do programa de inicialização ao cliente de inicialização iSCSI, juntamente com dois IQNs da iSCSI-alvo que podem ser usados para a inicialização. O formato do IQN da iSCSI-alvo é igual ao formato da opção 17 de DHCP, enquanto o IQN do programa de inicialização iSCSI é composto apenas pelo IQN do programa.



Nota: A opção 43 de DHCP tem suporte apenas para o protocolo IPv4.

Veja abaixo as subopções.

Tabela 17: Definição das subopções da opção 43 de DHCP

Subopções	Definição
201	Informações sobre a primeira iSCSI-alvo no formato padrão do caminho raiz "iscsi:<servername>": "<protocol>": "<port>": "<LUN>": "<targetname>"
202	Informações sobre a segunda iSCSI-alvo no formato padrão do caminho raiz "iscsi:<servername>": "<protocol>": "<port>": "<LUN>": "<targetname>"
203	IQN do programa de inicialização iSCSI

A opção 43 de DHCP requer mais configurações do que a opção 17 de DHCP, mas ela oferece um ambiente mais completo e mais opções de configuração. A Broadcom recomenda que os clientes usem a opção 43 de DHCP ao realizarem configurações dinâmicas de inicialização iSCSI.

Configuração do servidor DHCP

Configure o servidor DHCP para suportar a opção 17 ou a opção 43.



Nota: Se você usar a opção 43, também será necessário configurar a opção 60. O valor da opção 60 deve coincidir com o valor de **DHCP Vendor ID** (ID do fornecedor de DHCP). O valor do **ID do fornecedor de DHCP** é BRCM ISAN, conforme descrito na opção **General Parameters** (Parâmetros gerais) do menu iSCSI Boot Configuration (Configuração da inicialização iSCSI).

Configuração de inicialização iSCSI do DHCP para IPv6

O servidor DHCPv6 é capaz de fornecer uma série de opções, incluindo a configuração IP com ou sem informações de estado, além de informações para o cliente DHCPv6. Para a inicialização iSCSI, os adaptadores Broadcom suportam as seguintes configurações de DHCP:

- [Opção 16 de DHCPv6, opção de classe do fornecedor](#)
- [Opção 17 de DHCPv6, informações específicas do fornecedor](#)



Nota: A opção de caminho raiz padrão do DHCPv6 ainda não está disponível. A Broadcom recomenda usar a opção 16 ou 17 para obter suporte dinâmico à inicialização iSCSI com IPv6.

Opção 16 de DHCPv6, opção de classe do fornecedor

A opção 16 de DHCPv6 (opção de classe do fornecedor) deve estar presente e conter uma string que coincida com o parâmetro de **DHCP Vendor ID** (ID do fornecedor de DHCP) configurado por você. O valor do **ID do fornecedor de DHCP** é BRCM ISAN, conforme descrito na opção **General Parameters** (Parâmetros gerais) do menu iSCSI Boot Configuration (Configuração da inicialização iSCSI).

O conteúdo da opção 16 deve ser <2-byte length> <DHCP Vendor ID>.

Opção 17 de DHCPv6, informações específicas do fornecedor

A opção 17 de DHCPv6 (informações específicas do fornecedor) fornece mais opções de configuração para o cliente iSCSI. Nessa configuração, são fornecidas três subopções adicionais que atribuem o IQN do programa de inicialização ao cliente de inicialização iSCSI, juntamente com dois IQNs da iSCSI-alvo que podem ser usados para a inicialização.

Veja abaixo as subopções.

Tabela 18: Definição das subopções da opção 17 de DHCP

Subopções	Definição
201	Informações sobre a primeira iSCSI-alvo no formato padrão do caminho raiz "iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"
202	Informações sobre a segunda iSCSI-alvo no formato padrão do caminho raiz "iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"
203	IQN do programa de inicialização iSCSI



Nota: No [Tabela 18](#), os colchetes [] são necessários para endereços IPv6.

O conteúdo da opção 17 deve ser <2-byte Option Number 201|202|203> <2-byte length> <data>.

Configuração do servidor DHCP

Configure o servidor DHCP para suportar a opção 16 ou a opção 17.



Nota: O formato das opções 16 e 17 de DHCPv6 é completamente definido em RFC 3315.

Preparação da imagem de inicialização iSCSI

- [Configuração de inicialização iSCSI do Windows Server 2008 R2 e SP2](#)
- [Configuração da inicialização do iSCSI do Windows Server 2012](#)
- [Configuração da inicialização iSCSI do Linux](#)

Configuração de inicialização iSCSI do Windows Server 2008 R2 e SP2

O Windows Server 2008 R2 e o Windows Server 2008 SP2 são compatíveis com a inicialização do iSCSI. O procedimento abaixo se refere ao Windows Server 2008 R2, mas é o mesmo no Windows Server 2008 R2 e SP2.

Imagem CD/ISO necessária:

- Windows Server 2008 R2 x64 com os drivers Broadcom injetados. Consulte o artigo KB974072 da Base de conhecimento da Microsoft em support.microsoft.com.



Nota: Consulte o arquivo *silent.txt* do aplicativo do instalador de driver específico para obter as instruções sobre como extrair os drivers NetXtreme individuais do Windows.

Outro software necessário:

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

Procedimento:

1. Remova as unidades de disco rígido do sistema a ser inicializado (o "sistema remoto").
2. Carregue o Broadcom MBA e as imagens de inicialização iSCSI mais recentes no NVRAM do adaptador.
3. Configure o BIOS no sistema remoto para que o Broadcom MBA seja o primeiro dispositivo a ser iniciado e o DVDROM seja o segundo.
4. Configure o destino iSCSI para permitir uma conexão do dispositivo remoto. Verifique se o destino tem espaço em disco suficiente para suportar a nova instalação de SO.
5. Inicialize o sistema remoto. Quando o banner do Preboot Execution Environment (PXE) for exibido, pressione **Ctrl+S** para entrar no menu do PXE.
6. No menu PXE, defina o **Boot Protocol** (Protocolo de inicialização) como **iSCSI**.
7. Insira parâmetros de destino iSCSI.
8. Em Parâmetros gerais, defina o parâmetro **Boot to Target** (Inicialização para o destino) como **One-Time Disabled** (Desativação única).
9. Salve as configurações e reinicie o sistema.
O sistema remoto deve conectar-se ao destino iSCSI e, em seguida, inicializar do dispositivo de DVDROM.
10. Inicialize com o DVD e comece a instalação.
11. Responda a todas as perguntas de instalação adequadamente (especifique o sistema operacional que deseja instalar, aceite os termos da licença etc.).
Quando a janela **Onde deseja instalar o Windows?** for exibida, a unidade de destino deverá estar visível. Essa é uma unidade conectada via protocolo de inicialização iSCSI, localizado no destino iSCSI remoto.
12. Selecione **Next** (Avançar) para continuar com a instalação do Windows Server 2008 R2.
Alguns minutos depois do início do processo de instalação por DVD do Windows Server 2008 R2, haverá uma reinicialização de sistema. Depois da reinicialização, a rotina de instalação do Windows Server 2008 R2 deve recomeçar e concluir a instalação.
13. Depois de outra reinicialização de sistema, verifique se o sistema remoto consegue inicializar o computador.

14. Após a inicialização do Windows Server 2008 R2, carregue o driver e execute Bindview.exe.
 - a. Selecione **All Services** (Todos os serviços).
 - b. Em **WFP Lightweight Filter** (Filtro leve de WFP), você deve visualizar os **caminhos de vinculação** para o AUT. Clique com o botão direito do mouse e desative-os. Quando terminar, feche o aplicativo.
15. Verifique se o SO e o sistema estão funcionando e se são capazes de passar tráfego executando ping no IP de um sistema remoto etc.

Configuração da inicialização do iSCSI do Windows Server 2012

O Windows Server 2012 é compatível com a inicialização e a instalação do iSCSI. A Broadcom requer o uso de DVD integrado com os drivers mais recentes da Broadcom injetados. Consulte o artigo KB974072 da Base de conhecimento da Microsoft em support.microsoft.com.

O procedimento a seguir prepara a imagem para a instalação e a inicialização:

1. Remova as unidades de disco rígido do sistema a ser inicializado (o "sistema remoto").
2. Carregue o Broadcom MBA e as imagens de inicialização iSCSI mais recentes no NVRAM do AUT.
3. Configure o BIOS no sistema remoto para que o Broadcom MBA seja o primeiro dispositivo a ser iniciado e o DVDROM seja o segundo.
4. Configure o destino iSCSI para permitir uma conexão do dispositivo remoto. Verifique se o destino tem espaço em disco suficiente para suportar a nova instalação de SO.
5. Inicialize o sistema remoto. Quando o banner do Preboot Execution Environment (PXE) for exibido, pressione **Ctrl+S** para entrar no menu do PXE.
6. No menu PXE, defina o **Protocolo de inicialização** como **iSCSI**.
7. Insira parâmetros de destino iSCSI.
8. Em Parâmetros gerais, defina o parâmetro **Inicialização para o destino** como **Desativação única**.
9. Salve as configurações e reinicie o sistema.

O sistema remoto deve conectar-se ao destino iSCSI e, em seguida, inicializar do dispositivo de DVDROM.

10. Inicialize no DVD e inicie a instalação.
11. Responda a todas as perguntas de instalação adequadamente (especifique o sistema operacional que deseja instalar, aceite os termos da licença etc.).

Quando a janela **Onde deseja instalar o Windows?** for exibida, a unidade de destino deverá estar visível. Essa é uma unidade conectada via protocolo de inicialização iSCSI, localizado no destino iSCSI remoto.

12. Selecione **Avançar** para continuar com a instalação do Windows 2012.

Alguns minutos depois do início do processo de instalação por DVD do Windows 2012, haverá uma reinicialização de sistema. Depois da reinicialização, a rotina de instalação do Windows 2012 deve recomençar e concluir a instalação.

13. Depois de outra reinicialização de sistema, verifique se o sistema remoto consegue inicializar o computador.
14. Depois que o Windows 2012 inicializa o SO, a Broadcom recomenda executar o instalador de drivers para concluir a instalação de drivers e aplicativos da Broadcom.

Configuração da inicialização iSCSI do Linux

A inicialização iSCSI do Linux tem suporte a partir do Red Hat Enterprise Linux 5.5 e do SUSE Linux Enterprise Server 11 SP1 e posterior.

1. Para atualização do driver, obtenha o CD mais recente de drivers Broadcom Linux.

2. Configure os parâmetros de inicialização iSCSI para instalação direta por DVD no destino, desativando a inicialização a partir da opção de destino no adaptador de rede.
3. Altere a ordem de inicialização da seguinte forma:
 - a. Inicialize a partir do adaptador de rede.
 - b. Inicialize a partir do driver de CD/DVD.
4. Reinicialize o sistema.
5. O sistema se conectará ao destino iSCSI e executará a inicialização a partir do CD/DVD.
6. Siga as instruções correspondentes ao sistema operacional.
 - a. RHEL 5.5 — Digite "linux dd" no prompt "boot:" e pressione Enter
 - b. SuSE 11.X — Selecione **installation** (Instalação) e digite **withiscsi=1 netsetup=1** na opção de inicialização. Caso deseje a atualização do driver, selecione **YES** (Sim) na opção F6 do driver.
7. Se a atualização do driver for desejada, siga as instruções para carregar o CD de drivers; caso contrário, ignore essa etapa.
8. No prompt "dispositivo de rede", escolha a porta do adaptador de rede desejado e pressione **OK**.
9. No prompt "configurar TCP/IP", configure a maneira como o sistema adquire o endereço IP e pressione **OK**.
10. Se o IP estático tiver sido escolhido, será necessário inserir informações de IP para o iniciador iscsi.
11. (RHEL) Selecione "ignorar" o teste de mídia.
12. Continue a instalação conforme desejado. Uma unidade ficará disponível nesse ponto. Depois que a cópia de arquivo for realizada, remova o CD/DVD e reinicie o sistema.
13. Quando o sistema for reiniciado, ative "inicializar no destino" nos parâmetros de inicialização iSCSI e continue com a instalação até terminar.

Neste estágio, a fase de instalação inicial foi concluída. O restante do procedimento se relaciona à criação de um novo initrd personalizado para quaisquer atualizações novas de componentes:

14. Atualize o iniciador iscsi, se desejado. Primeiro é necessário remover o iniciador existente usando **rpm -e**.
15. Verifique se todos os níveis de execução do serviço de rede estão ativos:

```
chkconfig network on
```
16. Verifique se 2, 3 e 5 níveis de execução do serviço iscsi estão ativos.

```
chkconfig -level 235 iscsi on
```
17. Para o Red Hat 6.0, verifique se o serviço Network Manager (Gerenciador de rede) foi interrompido e desativado.
18. Instale o iscsiui, se desejado (desnecessário para SuSE 10).
19. Instale o pacote linux-nx2, se desejado.
20. Instale o pacote bibt.
21. Remova ifcfg-eth*.
22. Reinicie.
23. Para o SUSE 11,1, siga a solução alternativa de instalação de DVD remota mostrada abaixo.
24. Após reiniciar o sistema, efetue logon, altere para a pasta /opt/bcm/bibt e execute o script iscsi_setup.sh para criar a imagem initrd.
25. Copie a imagem initrd na pasta /boot.
26. Altere o menu grub para indicar a nova imagem initrd.
27. Para ativar CHAP, modifique iscsid.conf (somente no Red Hat).
28. Reinicie e altere os parâmetros de CHAP, se desejado.

29. Continue inicializando na imagem de Inicialização iSCSI e escolha uma das imagens criadas. Sua escolha deve corresponder à sua opção na seção de parâmetros de Inicialização iSCSI. Se o modo de inicialização HBA foi ativado na seção de parâmetros de inicialização iSCSI, será necessário reiniciar a imagem offload. SLES 10.x e SLES 11 não têm suporte para offload.
30. Para o IPv6, agora você pode alterar o endereço IP do inicializador e do alvo para o endereço IPv6 desejado na configuração NVRAM.

Inicialização

Depois disso, o sistema estará pronto para uma inicialização iSCSI e o sistema operacional estará presente na iSCSI-alvo. A última etapa é realizar a inicialização propriamente dita. O sistema inicializará o Windows ou o Linux pela rede e funcionará como se ele fosse uma unidade de disco rígido local.

1. Reinicialize o servidor.
2. Selecione **CTRL+S**.
3. No menu **Principal**, selecione a opção **General Parameters** (Parâmetros gerais) e configure a opção **Boot to iSCSI target** (Inicialização a partir da iSCSI-alvo) como **Ativada**.

Se for necessário realizar a autenticação CHAP, ative a opção CHAP authentication (Autenticação CHAP) após confirmar que a inicialização ocorreu com êxito (consulte [Ativação da opção CHAP Authentication](#)).

Outras considerações sobre a inicialização iSCSI

Há vários outros fatores que devem ser levados em consideração durante a configuração de um sistema para a inicialização iSCSI.

Alterando as configurações de Speed & Duplex em ambientes Windows

A inicialização por meio do caminho NDIS é suportada. As configurações de Speed & Duplex podem ser alteradas usando o utilitário de gerenciamento BACS para inicialização do iSCSI por meio do caminho NDIS.

Locally Administered Address

Um endereço MAC definido pelo usuário e atribuído por meio da propriedade Locally Administered Address (Endereço administrado localmente) da seção Avançado da guia Configurações do BACS não é suportado em dispositivos habilitados para a inicialização iSCSI.

LANs virtuais

A marcação de VLAN (Virtual LAN, LAN virtual) não é suportada para inicializações iSCSI realizadas com o iSCSI Software Initiator da Microsoft.

Solução de problemas de inicialização iSCSI

As dicas de solução de problemas descritas abaixo se aplicam à inicialização iSCSI.

Problema: O utilitário iSCSI Crash Dump da Broadcom não funcionará corretamente para capturar um despejo de memória quando a velocidade do link para inicialização de iSCSI for configurada para 10 Mbps ou 100 Mbps.

Solução: O utilitário iSCSI Crash Dump utility é suportado quando a velocidade do link para inicialização de iSCSI é configurada para 1 Gbps. 10 Mbps ou 100 Mbps não é suportado.

Problema: Um alvo iSCSI não é reconhecido como um alvo de instalação quando você tenta instalar o Windows Server 2008 usando uma conexão IPv6.

Solução: Este é um problema conhecido relacionado a terceiros. Consulte o artigo KB 971443 da Base de conhecimento da Microsoft em <http://support.microsoft.com/kb/971443>.

Problema: O utilitário de configuração iSCSI não é executado.

Solução: Confirme se o firmware de inicialização iSCSI está instalado na NVRAM.

Problema: Depois de configurar o LUN de inicialização iSCSI como 255, aparece uma tela azul do sistema durante a execução da inicialização iSCSI.

Solução: Embora a solução iSCSI da Broadcom dê suporte a uma faixa de LUNs de 0 a 255, o iSCSI Software Initiator da Microsoft não dá suporte para um LUN de 255. Configure um valor de LUN entre 0 e 254.

Problema: Não será possível atualizar o driver da caixa de entrada se houver um ID de hardware que não tem caixa de entrada.

Solução: Crie uma imagem de DVD integrada personalizada com os drivers compatíveis presentes na mídia de instalação.

iSCSI Crash Dump

Se você for usar o utilitário Broadcom iSCSI Crash Dump, é importante seguir o procedimento de instalação para instalar o driver iSCSI Crash Dump. Consulte [Como usar o Instalador](#) para obter mais informações.

Seção 10: Instalação de driver e aplicativo de gerenciamento do Windows

- [Pacotes](#)
- [Instalação do software de driver TG3](#)
- [Instalações de rede](#)
- [Descarregamento/remoção do driver do TG3](#)
- [Mensagens do driver](#)
- [Formação de equipes com vinculação de canal](#)
- [Instalação do aplicativo de gerenciamento do Linux](#)

Pacotes

O driver TG3 do Linux inclui os seguintes formatos de pacotes (nomes de arquivos):

- RPM de origem (tg3-versão.3dkms.src.rpm)
- RPM de origem (tg3-versão.3dkms.noarch.rpm)
- Suplementar (tg3_sup-versão.tar.gz)
- Tar compactado (tg3-versão.tar.gz)

Arquivos de origem idênticos para criar o driver são incluídos tanto nos pacotes de origem RPM quanto nos TAR. O arquivo tar contém utilitários adicionais como, por exemplo, patches e imagens de disco do driver para instalação em rede.

Instalação do software de driver TG3

- [Instalação do pacote RPM de origem](#)
- [Criação do driver com base no arquivo TAR de origem](#)

Instalação do pacote RPM de origem

Pré-requisitos:

- Origem de kernel Linux
- Compilador C

Procedimento:

1. Instale o pacote RPM de origem:

```
rpm -ivh tg3-version.src.rpm
```
2. Mude o diretório para o caminho do RPM e crie o driver binário para o kernel (o caminho do RPM é diferente para distribuições Linux diferentes).

```
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: Durante a tentativa de instalar um pacote RPM de origem, a seguinte mensagem pode ser exibida:

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

A causa mais provável do erro é que o pacote rpm-build não foi instalado. Localize o pacote rpm-build na mídia de instalação do Linux e instale-o utilizando o seguinte comando:

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

Conclua a instalação do RPM de origem.

3. Instale o pacote recém-criado (driver e arquivo de instrução):

```
rpm -ivh RPMS/i386/tg3-version.i386.rpm
```

Dependendo do kernel, o driver é instalado no seguinte caminho:

kernels 2.6.x:

```
/lib/modules/versão_kernel/kernel/drivers/net/tg3.ko
```

4. Carregue o driver.

```
modprobe tg3
```

Para configurar o protocolo e o endereço de rede, consulte a documentação específica do Linux.

Criação do driver com base no arquivo TAR de origem

1. Crie um diretório (*tg3-versão*) e extraia os arquivos TAR neste diretório.

```
tar xvzf tg3-versão.tgz
```
2. Crie o driver *tg3.o* como um módulo carregável para o kernel que está sendo executado.

```
CD tg3-versão  
make clean  
make; make install
```
3. Teste o driver carregando-o.

```
rmmod tg3  
modprobe tg3
```

Nenhuma mensagem será retornada se esse comando for executado corretamente.



Nota: Consulte as instruções relacionadas ao RPM descritas acima para saber a localização do driver instalado.

4. Para configurar o protocolo e o endereço de rede, consulte a documentação fornecida com seu sistema operacional.

Instalações de rede

Para instalações em rede por meio de NFS, FTP ou HTTP (utilizando um disco de reinicialização em rede ou PXE), use o driver *tg3* que é parte da distribuição do sistema operacional Linux.

Descarregamento/remoção do driver do TG3

- [Descarregamento/remoção do driver de uma instalação RPM](#)
- [Remoção do driver de uma instalação TAR](#)

Descarregamento/remoção do driver de uma instalação RPM

Para descarregar o driver, utilize **ifconfig** para remover todas as interfaces *ethX* abertas pelo driver e, em seguida faça o seguinte:

```
rmmod tg3
```

Se o driver foi instalado com **rpm**, faça o seguinte para removê-lo:

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

Remoção do driver de uma instalação TAR

Se o driver foi instalado com `make install` no arquivo `tar`, o driver `tg3.o` terá que ser excluído manualmente do sistema operacional. Consulte em [Instalação do pacote RPM de origem](#) o local do driver instalado.

Se existir uma configuração de interface relativa ao driver `tg3`, primeiro feche a interface usando `ifconfig ethx down` e, em seguida, `rmmmod tg3`.

Mensagens do driver

A seguir, estão as mensagens de amostra mais comuns que podem estar registradas no arquivo `/var/log/messages`. Use `dmesg -n nível` para controlar o nível em que as mensagens aparecerão no console. Por padrão, a maioria dos sistemas está definida como nível 6.

Acesso único do driver

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

NIC detectada

```
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
```

Controle de fluxo

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

Link Up and Speed Indication (Indicação de link ativo e de velocidade)

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

Link Down Indication (Indicação de link inativo)

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

Formação de equipes com vinculação de canal

Com o driver TG3, você pode agrupar os adaptadores usando o módulo kernel de vinculação e uma interface de vinculação do canal. Consulte a documentação do Linux para obter mais informações sobre o Linux Channel Bonding (Vinculação do Canal do Linux).

Instalação do aplicativo de gerenciamento do Linux

- [Visão geral](#)
- [Instalação do WS-MAN ou CIM-XML no servidor Linux](#)
- [Instalação do WS-MAN ou CIM-XML no cliente Linux](#)
- [Instalação do aplicativo Broadcom Advanced Control Suite](#)

Visão geral

O Broadcom Advanced Control Suite versão 4 (BACS4) é um aplicativo de gerenciamento para configurar a família de adaptadores NetXtreme I. O software BACS4 opera em servidores Windows e Linux e em sistemas operacionais clientes.

Este capítulo descreve como instalar o aplicativo de gerenciamento do BACS4 em sistemas Linux. Para sistemas Windows, um programa de instalação é fornecido, que instala os drivers do Windows e os aplicativos de gerenciamento, incluindo o BACS4 (consulte [Instalação do driver do Windows e do aplicativo de gerenciamento](#) para obter instruções).

Há dois componentes principais do utilitário do BACS4: o componente do provedor e o software cliente. Um provedor está instalado em um servidor, ou "host gerenciado", que contém um ou mais NICs. O provedor coleta informações sobre os NICs e as disponibiliza para recuperação de um PC de gerenciamento no qual o software cliente está instalado. O software cliente ativa as informações de visualização dos provedores e a configuração de NICs. O software cliente BACS inclui uma interface gráfica do usuário (GUI) e uma interface de linha de comando (CLI).

Protocolos de comunicação

Um protocolo de comunicação ativa a troca de informações entre o provedor e o software cliente. Estas são implementações proprietárias ou de código aberto dos padrões Web-Based Enterprise Management (WBEM) e Common Information Model (CIM) do Distributed Management Task Force (DMTF). Os administradores de rede podem escolher a melhor opção com base no padrão predominante na sua rede.

A tabela a seguir mostra as opções disponíveis com base nos sistemas operacionais instalados no host gerenciado e no cliente.

Se o cliente usar:	E o host gerenciado usar:	O BACS poderá usar os seguintes protocolos de comunicação:
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)

<i>Se o cliente usar:</i>	<i>E o host gerenciado usar:</i>	<i>O BACS poderá usar os seguintes protocolos de comunicação:</i>
<ul style="list-style-type: none">• WMI = Windows Management Instrumentation.• WS-MAN = Web Service-Management. WinRM é uma implementação baseada no Windows e o OpenPegasus é uma implementação de código aberto que opera no Linux.• CIM-XML = uma versão baseada no XML do OpenPegasus.		

Se a sua rede incluir uma combinação de clientes Windows e Linux que acessam servidores Windows e Linux, o WS-MAN será uma opção adequada. Se Linux for o único SO instalado nos servidores, o CIM-XML será uma opção adequada. Se a rede incluir apenas servidores e clientes Windows, WMI será a melhor opção. O WMI é muito simples de configurar, mas é suportado apenas em SO Windows. Consulte [Instalação do driver Windows e do aplicativo de gerenciamento](#) para obter instruções sobre a instalação e a configuração de protocolos Windows.

A instalação do BACS inclui a instalação do componente provedor no host gerenciado e o software cliente na estação de gerenciamento. O processo de instalação difere com base na combinação de sistemas operacionais instalados no cliente, no host gerenciado e no protocolo de comunicação selecionado.

Instalação do WS-MAN ou CIM-XML no servidor Linux

Etapa 1: Instalar o OpenPegasus

No SO Red Hat Linux, duas opções de instalação estão disponíveis:

- [No Inbox RPM \(apenas Red Hat\)](#)
- [Da origem \(Red Hat e SuSE\)](#)

No SO SUSE Linux Enterprise Server 11 (SLES11), você deve usar o RPM de origem.



Nota: O Inbox RPM não é compatível com o protocolo de comunicação WS-MAN. Para usar o WS-MAN, você deve instalar o OpenPegasus de origem.

No Inbox RPM (apenas Red Hat)

No Red Hat Linux, um Inbox OpenPegasus RPM está disponível como `tog-pegasus-<versão>.<arch>.rpm`.

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



Nota: No SuSE Linux, o Inbox OpenPegasus RPM não está disponível. O OpenPegasus deve ser instalado na origem, como descrito no procedimento a seguir.

Observe que no Inbox Pegasus, o HTTP não está ativado por padrão. Depois que o Inbox OpenPegasus estiver instalado com sucesso, se nenhuma outra configuração for necessária, siga as instruções em [Etapa 4: Instalar o provedor de CMPI da Broadcom](#). Para ativar o HTTP, consulte [Ativar HTTP](#).

Da origem (Red Hat e SuSE)

A origem do OpenPegasus pode ser baixada em www.openpegasus.org.



Nota: Se ainda não estiver instalado, baixe e instale o openssl e o libopenssl-devel rpm. Esta etapa é opcional e necessária apenas se você estiver planejando usar HTTPS para estabelecer a conexão do cliente com o host gerenciado.

Definição das variáveis de ambiente

Defina as variáveis de ambiente para montar o OpenPegasus conforme indicado a seguir.

Variável de ambiente	Descrição
PEGASUS_ROOT	O local da árvore de origem do Pegasus
PEGASUS_HOME	O local do executável da montagem, repositório, por exemplo, subdiretórios \$PEGASUS_HOME/bin, PEGASUS_HOME/lib, \$PEGAUS_HOME/repository e \$PEGASUS_HOME/mof.
PATH	\$PATH:\$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	Verdadeiro
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Para sistemas Linux de 32 bits: "LINUX_IX86_GNU" Para sistemas Linux de 64 bits: "LINUX_X86_64_GNU"
PEGASUS_HAS_SSL	Opcional. Definido como "verdadeiro" para suporte de HTTPS.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Opcional. Definido como "verdadeiro" para suporte de protocolo WSMAN.

Configurações adicionais

A variável \$PEGASUS_HOME deve ser configurada em um ambiente shell e \$PEGASUS_HOME/bin deve ser anexado ao ambiente \$PATH.

Exemplos

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

Para o Suporte SSL, adicione a seguinte variável de ambiente:

- export PEGASUS_HAS_SSL=true

Para o Suporte WS-MAN, adicione a seguinte variável de ambiente:

- export PEGASUS_ENABLE_PROTOCOL_WSMAN=true

CIM-XML e WSMAN no OpenPegasus usam as mesmas portas para HTTP ou HTTPS. Os números de porta padrão para HTTP e HTTPS são 5989 e 5989, respectivamente.



Nota: É possível adicionar essas exportações no final de `.bash_profile`. Este arquivo está localizado no diretório `/root`.

- As variáveis de ambiente serão definidas quando um usuário fizer login usando PuTTY.
- No próprio sistema Linux, para cada terminal onde as variáveis do ambiente não estão definidas, execute o seguinte comando:
`source /root/.bash_profile`
- Quando você faz o logout e o login, as variáveis de ambiente são definidas.

Montar e instalar o OpenPegasus

No `$PEGASUS_ROOT` (o local do diretório raiz da origem do Pegasus), execute o seguinte:

```
make clean
make
make repository
```



Nota: Sempre que o OpenPegasus for montado a partir da origem, todas as configurações serão redefinidas com os valores padrão. Se estiver recriando o OpenPegasus, você precisará refazer a configuração como mencionado em [Etapa 3: Configure o OpenPegasus no servidor](#).

Etapa 2: Iniciar o servidor CIM no servidor

Use o comando `cimserver` para iniciar o servidor CIM. Para interromper o servidor CIM, use o comando `cimserver -s`.

Para verificar se o OpenPegasus foi instalado corretamente, digite o seguinte comando:

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



Nota: Para o OpenPegasus compilado a partir da origem, `PEGASUS_HOME` deve ser definida quando iniciar o servidor CIM. Caso contrário, o servidor CIM não carregará o repositório corretamente. Considere configurar `PEGASUS_HOME` no arquivo `".bash_profile"`.

Etapa 3: Configure o OpenPegasus no servidor

Use o comando `cimconfig` para configurar o OpenPegasus, conforme indicado na tabela a seguir:

Comando	Descrição
<code>cimconfig -l</code>	Lista todos os nomes de propriedade válidos.
<code>cimconfig -l -c</code>	Lista todos os nomes de propriedade válidos e o seu valor.
<code>cimconfig -g <property name></code>	Consulta uma propriedade específica.
<code>cimconfig -s <property name>=<value> -p</code>	Define uma propriedade específica.
<code>cimconfig --help</code>	Saiba mais sobre o comando.

O servidor CIM deve ser iniciado antes de executar `cimconfig` e deve ser reiniciado para que as mudanças de configuração tenham efeito.

Ativar autenticação

As seguintes propriedades do OpenPegasus devem ser definidas como descrito nesta seção. Caso contrário, o provedor do CIM da Broadcom não funcionará adequadamente. Verifique se os seguintes comandos estão definidos antes de iniciar o BACS e estabelecer a conexão com o provedor.

Inicie o servidor CIM se ainda não tiver iniciado. Em seguida, defina:

- `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`

Se quiser que o usuário raiz conecte remotamente:

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

Configuração de usuário com privilégio: Os usuários do sistema Linux são usados para autenticação do OpenPegasus. Os usuários dos sistemas devem ser adicionados ao OpenPegasus usando `cimuser` para fazer a conexão via BACS:

- `cimuser -a -u <username> -w <password>`
Exemplo: `cimuser -a -u root -w linux1`

Ativar HTTP

1. Se o servidor CIM não tiver sido iniciado, inicie-o.
2. Use o seguinte comando para configurar uma porta HTTP (opcional):
`cimconfig -s httpPort=5988 -p`
Esta propriedade não está disponível para Inbox OpenPegasus.
3. Use o seguinte comando para ativar a conexão HTTP:
`cimconfig -s enableHttpConnection=true -p`
4. Use os comandos `cimserver -s` e `cimserver`, respectivamente, para interromper e reiniciar o servidor CIM para que a nova configuração entre em vigor.

Ativar o HTTPS

1. Se o servidor CIM não tiver sido iniciado, inicie-o.
2. Configure a porta HTTPS com o seguinte comando (opcional):
`cimconfig -s httpsPort=5989 -p`
Esta propriedade não está disponível para Inbox OpenPegasus.
3. Ative a conexão HTTPS com o seguinte comando:
`cimconfig -s enableHttpsConnection=true -p`
4. Use os comandos `cimserver -s` e `cimserver`, respectivamente, para interromper e reiniciar o servidor CIM para que a nova configuração entre em vigor.

Etapa 4: Instalar o provedor de CMPI da Broadcom

Verifique se o OpenPegasus está devidamente instalado antes de instalar o provedor de CMPI.

Instalação

Digite o seguinte comando para instalar o provedor de CMPI da Broadcom.

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

Desinstalação

Digite o seguinte comando para desinstalar o provedor de CMPI da Broadcom.

```
% rpm -e BRCM_CMPIProvider
```

Etapa 5: Executar a configuração do firewall Linux, se necessário

Siga estes procedimentos para abrir as portas adequadas no firewall:

Red Hat

1. Clique em **Sistema**, selecione **Administração** e, em seguida, selecione **Firewall**.
2. Selecione **Outras portas**.
3. Na caixa de diálogo Porta e protocolo, selecione **Definido pelo usuário**.
4. No campo **Porta/intervalo de porta**, adicione o número da porta.
5. No campo **Protocolo**, adicione o protocolo como TCP ou UDP etc.
6. Clique em **Aplicar** para que as regras de firewall tenham efeito.

Por exemplo:

- Para CIM-XML em HTTP, o número da porta é 5988 e o protocolo é TCP.
- Para CIM-XML em HTTPS, o número da porta é 5989 e o protocolo é TCP.

SuSE

1. Clique em **Computar** e em **YaST**.
2. Selecione **Segurança e usuários** no painel da esquerda.
3. No painel da direita, clique duas vezes em **Firewall**.
4. Selecione **Personalizar regras** no painel da esquerda.
5. No painel da direita, clique em **Adicionar**.
6. Digite os seguintes valores:
 - **Rede de origem:** 0/0 (significa todas)
 - **Protocolo:** TCP (ou o protocolo adequado)
 - **Porta de destino:** <Número da porta> ou <Intervalo de números das portas>
 - **Porta de origem:** Deixe em branco.
7. Clique em **Avançar** e, em seguida, clique em **Concluir** para que as regras do firewall tenham efeito.

Por exemplo:

Para CIM-XML, use os seguintes valores:

- **Rede de origem:** 0/0 (significa todas)
- **Protocolo:** TCP
- **Porta de destino:** 5988:5989
- **Porta de origem:** Deixe em branco.

Etapa 6: Instalar o BACS e os aplicativos de gerenciamento relacionados

Consulte [Instalação do aplicativo Broadcom Advanced Control Suite](#).

Instalação do WS-MAN ou CIM-XML no cliente Linux

Nenhum componente de software especial é necessário no sistema cliente do Linux para usar HTTP, exceto a instalação do aplicativo de gerenciamento do BACS. No entanto, para as instalações do WS-MAN, você pode, opcionalmente, configurar o protocolo HTTPS para uso com o BACS.

Configuração do HTTPS no cliente Linux

Siga estas etapas para usar o HTTPS em vez do HTTP (WS-MAN apenas):

Geração de um certificado autoassinado para o servidor Windows/Linux

O Openssl no Linux ou Windows pode ser usado para gerar o certificado autoassinado como segue:



Nota: Você pode baixar e instalar o openssl em <http://gnuwin32.sourceforge.net/packages/openssl.htm>.

1. Insira o seguinte comando para gerar uma chave privada:

```
openssl genrsa -des3 -out server.key 1024
```

2. Será solicitado que você insira uma senha. Memorize-a.

3. Execute as seguintes etapas para gerar um Certificate Signing Request (CSR).

Durante a geração do CSR, serão solicitadas várias informações. Quando for solicitado o "Nome comum", insira o nome de host do servidor Windows ou endereço IP.

Insira o seguinte comando (as respostas de amostra são mostradas):

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

Se este comando não funcionar, tente o seguinte:

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

O arquivo openssl.cnf deve ser colocado no mesmo diretório onde está openssl. Openssl.cnf está localizado na pasta C:\Program Files (x86)\GnuWin32\share.

As seguintes informações são solicitadas:

- Nome do país (código de 2 letras) []: **US**
- Nome do estado ou província (nome completo) []: **California**
- Nome da localidade (por ex., cidade) []: **Irvine**
- Nome da organização (por ex., empresa) []: **Broadcom Corporation**
- Nome da unidade organizacional (por ex., seção) []: **Engenharia**
- Nome comum (por ex., SEU nome) []: Insira o nome do host ou o endereço IP do servidor Windows. Para IPv6, digite o Nome comum no formato [xyxy:xxx:.....:xxx], **incluindo os colchetes []**.
- (Opcional) Endereço de e-mail []:

Insira os seguintes atributos adicionais a serem enviados com sua solicitação de certificado:

- Uma senha difícil []: **linux1**
- Um nome de empresa opcional []:

4. Remova a senha da chave.

Insira os seguintes comandos:

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

5. Gere um certificado autoassinado:

Para gerar um certificado autoassinado que seja ativo durante 365 dias, insira o seguinte comando:

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

É exibida a seguinte saída:

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

6. Insira o seguinte comando para verificar o certificado autoassinado gerado.

```
openssl verify server.crt
```

É exibida a seguinte saída:

```
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 a mensagem de erro "error 18 at 0 depth lookup:self signed certificate". Esse erro indica que é um certificado autoassinado.

7. Converta o certificado do formato "crt" para "pkcs12", como segue:

Para um servidor Windows, o certificado deve estar no formato pkcs12. Insira o seguinte comando:

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

Será solicitado o seguinte:

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

Insira a senha e memorize-a. A senha é necessária durante a importação do certificado no servidor e cliente Windows.

8. Faça uma cópia do arquivo de certificado server.crt e coloque-a no servidor no qual o BACS será instalado para que possa ser importada. Se você planeja usar um cliente Windows ou Linux para se conectar ao servidor que executa o BACS, o certificado também precisará ser transferido (copiado e colado) no sistema do cliente.

No Linux, o certificado deve ter uma extensão ".pem". As extensões ".crt" e ".pem" são iguais, assim não é necessário usar o comando `openssl` para converter de .crt para .pem. Você pode simplesmente copiar o arquivo como está.



Nota: Um certificado separado deve ser gerado para endereços IPv4 e IPv6 e para o nome do host.

Importar o certificado autoassinado no cliente Linux

Nas distribuições Linux, observe o seguinte diretório de certificados:

- Para todas as versões SuSE, o diretório de certificado é `/etc/ssl/certs`.
- Para RedHat, o diretório de certificado pode ser diferente para cada versão. Para algumas versões, é `/etc/ssl/certs` ou `/etc/pki/tls/certs`. Para outras versões, descubra o diretório de certificado.

Copie `hostname.pem`, criado em [Geração de um certificado autoassinado para o servidor Windows/Linux](#), no diretório de certificado do cliente Linux. Por exemplo, se o diretório de certificado for `/etc/ssl/certs`, copie `hostname.pem` em `/etc/ssl/certs`.

1. Altere o diretório para `/etc/ssl/certs`.
2. Crie um valor de hash executando o seguinte comando.

```
openssl x509 -noout -hash -in hostname.pem
```


Deve ser retornado um valor como o seguinte.

```
100940db
```

3. Crie um link simbólico para o valor de hash executando o seguinte comando:

```
ln -s hostname.pem 100940db.0
```

Teste da conexão HTTPS/SSL do cliente Linux

Use o seguinte comando para testar se o certificado está instalado corretamente no Linux:

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

Se isso falhar, significa que o certificado não está instalado corretamente e uma mensagem de erro será exibida, indicando que é necessário tomar uma ação corretiva.

Instalação do aplicativo Broadcom Advanced Control Suite

O software Broadcom Advanced Control Suite (BACS) pode ser instalado em um sistema Linux usando o pacote Linux RPM. Esta instalação inclui um cliente CLI.

Antes de iniciar:

- Verifique se os adaptadores de rede da Broadcom estão fisicamente instalados e o driver de dispositivo correto para a NIC está instalada no sistema a ser gerenciado por este utilitário.
- Verifique se o provedor do CIM está instalado corretamente no sistema que será gerenciado por este utilitário. Consulte
- Para gerenciar o iSCSI em hosts Linux, verifique se os utilitários open-iscsi e sg estão instalados no host Linux.

Para instalar o BACS

1. Baixe o pacote RPM do aplicativo de gerenciamento do BACS mais recente.

2. Instale o pacote RPM usando o seguinte comando:

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

Para usar o CLI do BACS, consulte o arquivo BACSCLI_Readme.txt fornecido com os arquivos de liberação.

Para remover o BACS

Para desinstalar o pacote RPM, use o seguinte comando:

```
% rpm -e BACS
```

Seção 11: Software de driver do VMware

- [Pacotes](#)
- [Drivers](#)

Pacotes

O driver VMware é liberado no seguinte formato de pacote.

Tabela 19: Pacote de drivers VMware

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

Drivers

Download, instalação e atualização dos drivers

Para fazer download, instalar ou atualizar o driver VMware ESX/ESXi para os adaptadores de rede NetXtreme I GbE, consulte <http://www.vmware.com/support>.

Parâmetros do driver

NetQueue

O parâmetro opcional **force_netq** pode ser usado para definir o número de filas net Rx e Tx. Os dispositivos BCM57XX compatíveis com NetQueue são BCM5718, BCM5719, BCM5720, BCM5721 e BCM5722.

Por padrão, o driver tenta usar o número ideal de NetQueues. Para forçar explicitamente o número de filas, defina o número de NetQueues por porta através do seguinte comando:

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

Valores permitidos para x são -1 a 15:

- 1 a 15 forçará o número de NetQueues para a NIC fornecida.
- 0 desativa o NetQueue.
- -1 especifica o uso do valor de NetQueue do driver padrão.

O número de itens "x" pode chegar a 32, o que significa que o máximo de NICs compatíveis = 32.

Exemplo de uso:

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

- tg3 NIC 0: Use o número padrão de NetQueues.
- tg3 NIC 1: Desative o recurso NetQueue.
- tg3 NIC 2: Use 1 NetQueue.
- tg3 NIC 3: Use 2 NetQueues.

Observe que o número de NIC acima não corresponde ao `vmnic<#>`. O número de NIC é o número de pedido de prova de `vmnic` do sistema. De forma ideal, o número de NetQueues corresponde ao número de CPUs na máquina.

Parâmetros do driver

Vários parâmetros opcionais podem ser fornecidos com um argumento de linha de comando ao comando `vmkload_mod`. Esses parâmetros também podem ser configurados pelo comando `esxcfg-module`. Consulte o arquivo de instrução para obter mais informações.

Padrões do driver

Tabela 20: Padrões de driver do VMware

Parâmetro	Valor padrão
Velocidade	Negociação automática com todas as velocidades anunciadas
Controle de fluxo	Negociação automática com rx e tx anunciado
MTU	1500 (intervalo de 46–9000)
Tamanho do anel Rx	200 (intervalo de 0 a 511). Alguns chips são fixos em 64.
Tamanho do anel jumbo Rx	100 (intervalo de 0 a 255). Nem todos os chips são compatíveis com o anel jumbo e alguns chips compatíveis com quadros jumbo não usam o anel jumbo.
Tamanho do anel Tx	511 (intervalo (MAX_SKB_FRAGS+1) – 511). MAX_SKB_FRAGS varia em diferentes kernels e em diferentes arquiteturas. Em um kernel 2.6 para x86, MAX_SKB_FRAGS é 18.
Microssegundos de união RX	20 (intervalo de 0 a 1.023)
IRQ de microssegundos de união RX	20 (intervalo de 0 a 255)
Quadros de união Rx	5 (intervalo de 0 a 1.023)
IRQ de quadros de união Rx	5 (intervalo de 0 a 255)
Microssegundos de união Tx	72 (intervalo de 0 a 1.023)
IRQ de microssegundos de de união Tx	20 (intervalo de 0 a 255)
Quadros de união Tx	53 (intervalo de 0 a 1.023)
IRQ de quadros de união Tx	5 (intervalo de 0 a 255)
Microssegundos de estatísticas de união	1.000.000 (aprox. 1 s). Alguns parâmetros de união não são salvos ou têm diferentes padrões em alguns chips.
Msi	Ativado (se compatível com o chip e aprovado no teste de interrupção).
WoL	Desativada

Mensagens do driver

A seguir, estão as mensagens de amostra mais comuns que podem estar registradas no arquivo `/var/log/messages`. Use `dmesg -n <nível>` para controlar o nível em que as mensagens aparecerão no console. Por padrão, a maioria dos sistemas está definida como nível 6. Para exibir todas as mensagens, defina o nível com um valor maior.

Acesso único do driver

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

NIC detectada

```
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
```

Link Up and Speed Indication (Indicação de link ativo e de velocidade)

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

Link Down Indication (Indicação de link inativo)

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

Seção 12: Instalação de driver e aplicativo de gerenciamento do Windows

- [Instalação do software de driver](#)
- [Modificação do software de driver](#)
- [Reparação ou reinstalação do software de driver](#)
- [Remoção dos drivers do dispositivo](#)
- [Exibição ou alteração das propriedades do adaptador](#)
- [Definição das opções de gerenciamento de energia](#)
- [Configurando o protocolo de comunicação a ser usado com o BACS4](#)

Instalação do software de driver



Nota: Estas instruções estão baseadas na suposição de que seu adaptador Broadcom NetXtreme não foi instalado de fábrica. Se seu controlador foi instalado na fábrica, o software de driver foi instalado para você.

Quando o Windows é iniciado pela primeira vez após a instalação de um novo dispositivo de hardware (como um adaptador Broadcom NetXtreme) ou após a remoção do driver do dispositivo antigo, o sistema operacional detecta automaticamente o hardware e pede que você instale o software de driver desse dispositivo.

Estão disponíveis tanto um modo de instalação interativa (consulte [Como usar o Instalador](#)) como um modo silencioso da linha de comando para instalação autônoma (consulte [Uso da instalação silenciosa](#)).



OBSERVAÇÕES:

- Antes de instalar o software de driver, verifique se o sistema operacional Windows foi atualizado para a versão mais recente, com o último service pack (pacote de serviço) aplicado.
- É necessário instalar um dispositivo de rede para que o adaptador Broadcom NetXtreme Gigabit Ethernet possa ser usado com o sistema operacional Windows. Os drivers estão localizados no CD de instalação.
- O BACS não é suportado na opção de instalação Server Core para o Microsoft Windows Server 2008 R2.

Como usar o Instalador

Além dos drivers do dispositivo Broadcom, o instalador instala os aplicativos de gerenciamento. Se disponíveis, os seguintes itens são instalados durante a execução do instalador:

- **Drivers do Dispositivo Broadcom.** Instala os drivers do dispositivo Broadcom.
- **Control Suite.** Broadcom Advanced Control Suite (BACS).
- **BASP.** Instala o Broadcom Advanced Server Program.
- **SNMP.** Instala o subagente Simple Network Management Protocol.
- **Provedor CIM.** Instala o provedor Common Information Model (Modelo comum de informações).
- **Driver iSCSI Crash Dump.** Instala o driver necessário para o utilitário iSCSI Crash Dump.



Nota: Apesar da instalação do software BACS e dos aplicativos de gerenciamento relacionados ser opcional, os drivers do dispositivo Broadcom devem ser instalados quando você usar o instalador.



Nota: O BASP não está disponível no Windows Small Business Server (SBS) 2008.

Para instalar o Microsoft iSCSI Software Initiator para iSCSI Crash Dump

Se permitido e se você for usar o utilitário Broadcom iSCSI Crash Dump, é importante obedecer a sequência de instalação:

- Execute o instalador
- Instale o iSCSI Software Initiator da Microsoft junto com o patch (MS KB939875)



Nota: Se estiver efetuando a atualização dos drivers do dispositivo com o programa de instalação, reative o **iSCSI Crash Dump** na seção Avançado da guia de Configuração.

Execute este procedimento depois de executar o programa de instalação para instalar os drivers do dispositivo e os aplicativos de gerenciamento.

1. Instale o Microsoft iSCSI Software Initiator (versão 2.06 ou posterior) caso não faça parte do SO em uso. Para determinar se é necessário instalar o Microsoft iSCSI Software Initiator, consulte [Tabela 21](#). Para fazer download do iSCSI Software Initiator do site da Microsoft, acesse <http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986>.
2. Instale o patch da Microsoft para geração de arquivo de despejo de memória iSCSI (Microsoft KB939875) disponível em <http://support.microsoft.com/kb/939875>. Para determinar se é necessário instalar o patch da Microsoft, consulte [Tabela 21](#).

Tabela 21: Sistemas operacionais Windows e iSCSI Crash Dump

<i>Sistema operacional</i>	<i>MS iSCSI Software Initiator necessário</i>	<i>Patch da Microsoft (MS KB939875) necessário</i>
NDIS		
Windows Server 2008	Sim (incluso no SO)	Não
Windows Server 2008 R2	Sim (incluso no SO)	Não
Windows Server 2012	Sim (incluso no SO)	Não
OIS		
Windows Server 2008	Não	Não
Windows Server 2008 R2	Não	Não
Windows Server 2012	Não	Não

Uso da instalação silenciosa



OBSERVAÇÕES:

- Todos os comandos diferenciam maiúsculas de minúsculas.
- Para obter informações e instruções detalhadas sobre instalações autônomas, consulte o arquivo Silent.txt na pasta Driver_Management_Apps_Installer.

Para obter instruções sobre a linha de comando, consulte o arquivo readme.txt na pasta de instalação.



Nota: O switch REINSTALL deve ser usado somente se o mesmo instalador já estiver instalado no sistema. Se estiver atualizando uma versão anterior do instalador, use `setup /s /v/qn`, conforme listado abaixo.

Modificação do software de driver

Para modificar o software de driver

1. No Painel de controle, clique duas vezes em **Adicionar ou Remover Programas**.
2. Clique em **Drivers e Aplicativos de Gerenciamento do Broadcom** e clique em **Alterar**.
3. Clique em **Avançar** para continuar.
4. Clique em **Modificar**, Adicionar ou Remover para alterar os recursos do programa. Essa opção não instala os drivers dos novos adaptadores. Para obter informações sobre como instalar os drivers dos novos adaptadores, consulte [Reparação ou reinstalação do software de driver](#).
5. Clique em **Avançar** para continuar.
6. Clique em um ícone para alterar a forma pela qual um recurso é instalado.
7. Clique em **Next (Avançar)**.
8. Clique em **Instalar**.
9. Clique em **Concluir** para fechar o assistente.
10. O instalador determinará se é necessário reiniciar o sistema. Siga as orientações na tela.

Reparação ou reinstalação do software de driver

Para reparar ou reinstalar o software de driver

1. No Painel de controle, clique duas vezes em **Adicionar ou Remover Programas**.
2. Clique em **Drivers e Aplicativos de Gerenciamento do Broadcom** e clique em **Alterar**.
3. Clique em **Avançar** para continuar.
4. Clique em **Reparar ou Reinstalar** para reparar erros ou instalar drivers dos novos adaptadores.
5. Clique em **Avançar** para continuar.
6. Clique em **Instalar**.
7. Clique em **Concluir** para fechar o assistente.
8. O instalador determinará se é necessário reiniciar o sistema. Siga as orientações na tela.

Remoção dos drivers do dispositivo

Se você remover os drivers do dispositivo, qualquer aplicativo de gerenciamento que estiver instalado também será removido.



Nota: O Windows Server 2008 e o Windows Server 2008 R2 oferecem o recurso de reversão de driver de dispositivo (Device Driver Rollback), que substitui um driver de dispositivo por um driver instalado anteriormente. Mas a complexa arquitetura de software do dispositivo NetXtreme pode apresentar problemas se o recurso de reversão for usado em um dos componentes individuais. Logo, recomendamos que só sejam alteradas versões do driver por meio de um instalador de driver.

Para remover os drivers do dispositivo

1. No Painel de controle, clique duas vezes em **Adicionar ou Remover Programas**.
2. Clique em **Drivers e Aplicativos de Gerenciamento do Broadcom** e clique em **Remover**. Siga as solicitações na tela.
3. Reinicialize o sistema para remover completamente os drivers. Se o sistema não for reinicializado, você não conseguirá instalar os drivers corretamente.

Exibição ou alteração das propriedades do adaptador

Para exibir ou alterar as propriedades do adaptador de rede Broadcom:

1. No Painel de Controle, clique em **Broadcom Control Suite 4**.
2. Clique na seção Avançado da guia **Configurações**.

Definição das opções de gerenciamento de energia

Você pode definir as opções de gerenciamento de energia para que o sistema operacional desative o controlador, de modo a poupar energia, ou para que o controlador ative o computador. Se o dispositivo estiver ocupado com alguma outra tarefa (se estiver atendendo a uma chamada, por exemplo), o sistema operacional não desligará o dispositivo. O sistema operacional tenta desligar todos os dispositivos possíveis somente quando o computador tenta entrar no estado de hibernação. Para que o adaptador permaneça sempre ativado, não marque a caixa de seleção **Computador pode desligar o dispositivo para economizar energia**.



Nota: As opções de gerenciamento de energia não estão disponíveis em servidores blade.



OBSERVAÇÕES:

- A guia Gerenciamento de energia fica disponível apenas para servidores que ofereçam suporte a gerenciamento de energia.
- Para ativar a opção Wake on LAN (WOL) quando o computador estiver em espera, clique na caixa **Este dispositivo pode ativar novamente o computador**.
- Se você selecionar **Só estações de gerenciamento podem ativar o computador**, o computador somente poderá ser tirado do estado em espera *através da opção Magic Packet*.



Cuidado! Não selecione **Computador pode desligar o dispositivo para economizar energia** de nenhum adaptador que seja membro de uma equipe.

Configurando o protocolo de comunicação a ser usado com o BACS4

Há dois componentes principais do aplicativo de gerenciamento do BACS4: o componente do provedor e o software cliente. Um provedor está instalado em um servidor, ou "host gerenciado", que contém um ou mais NICs. O provedor coleta informações sobre os NICs e as disponibiliza para recuperação de um PC de gerenciamento no qual o software cliente está instalado. O software cliente ativa as informações de visualização dos provedores e a configuração de NICs. O software cliente BACS inclui uma interface gráfica do usuário (GUI) e uma interface de linha de comando (CLI).

Um protocolo de comunicação ativa a comunicação entre o provedor e o software cliente. Dependendo da combinação de sistemas operacionais (Linux, Windows ou ambos) nos clientes e hosts gerenciados na sua rede, você pode escolher um protocolo de comunicação adequado para usar. Consulte ["Instalação de aplicativo de gerenciamento do Linux"](#) para obter uma descrição dos protocolos de comunicação disponíveis para cada configuração de rede.

As instruções neste capítulo tratam apenas do cenário em que os hosts gerenciados do Windows estão se comunicando com os clientes Windows. Nesses cenários, você pode usar tanto o protocolo de comunicação WMI quanto o WS-MAN (WinRM). Quando você usa o instalador de driver descrito neste capítulo para instalar o driver e os aplicativos de gerenciamento, o provedor para WMI e WS-MAN é instalado no host gerenciado. Além disso, o utilitário BACS4 é instalado no cliente. As seções a seguir apresentam etapas de configuração adicionais para o protocolo de comunicação que você selecionar.

Para instalações do Linux, o driver é instalado separadamente dos aplicativos de gerenciamento. Consulte [para obter instruções relacionadas](#).

Uso de WS-MAN

Para usar o protocolo de comunicação WS-MAN, siga as instruções nas seguintes seções:

- [Configuração do servidor do Windows para WS-MAN](#)
- [Instalação do cliente Windows para WS-MAN](#)

Configuração do servidor do Windows para WS-MAN

Etapa 1: Instale o componente de software WinRM no servidor

Nos sistemas operacionais a seguir, o WinRM 2.0 está pré-instalado:

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

Para o Windows Server, 2008, instale o Windows Management Framework Core, que inclui o WinRM 2.0 e o Windows Powershell 2.0, a partir do seguinte link:

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

Etapa 2: Execute a configuração básica no servidor

O firewall do Windows deve ser ativado para que o WinRM funcione corretamente. Para obter informações detalhadas sobre a configuração do firewall, consulte [Etapa 7: Configuração adicional do servidor](#). Depois de o firewall ser configurado, abra um prompt de comando e execute o comando a seguir para ativar o gerenciamento remoto no servidor Windows:

```
winrm quickconfig
```

É possível usar o comando a seguir para visualizar as informações de configuração do serviço:

```
winrm get winrm/config
```

Etapa 3: Execute a configuração do usuário no servidor

Para conectar o WinRM, a conta deve ser um membro do grupo local de administradores no computador local ou remoto. A saída do comando `get winrm/config` será a seguinte:

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

BA significa BUILTIN\Administrators.

Para adicionar outro grupo de usuários à lista de conexão permitida do WinRM, você pode modificar o RootSDDL para incluir o novo grupo de usuários. Você precisará do ID do SDDL para o novo grupo. Por exemplo, o seguinte comando adiciona o novo grupo de usuários com o ID do 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)"}
```

Etapa 4: Execute a configuração de HTTP no servidor

Para usar a interface do usuário do BACS GUI, você deve configurar o protocolo HTTP como segue:



Nota: A porta HTTP padrão é 5985 para WinRM 2.0.

1. Clique em **Iniciar** (ou pressione a tecla com o logotipo do Windows) e selecione **Executar**.
2. Digite **gpedit.msc** para abrir o editor local de Política de grupo.
3. Em **Configuração do computador**, abra a pasta **Modelos administrativos** e depois, a pasta **Componentes do Windows**.
4. Selecione **Windows Remote Management (WinRM)**.
5. Em **Windows Remote Management (WinRM)**, selecione **Cliente WinRm**.
6. Em **Cliente WinRM**, clique duas vezes em **Hosts confiáveis**.
7. Em **Lista de hosts confiáveis**, insira os nomes de host dos clientes. Se todos os clientes forem confiáveis, insira somente um asterisco (*).
8. Selecione **Serviço do WinRM**.
9. Ative **Permitir autenticação básica**.

10. Ative **Permitir tráfego sem criptografia**.
11. Feche a janela **Política de grupo**.
12. No prompt de comando, execute o seguinte comando para configurar o WinRM com configurações padrão:
`winrm qc or winrm quickconfig`
13. Quando a ferramenta exibir "**Fazer estas alterações [s/n]?**", insira "**s**".
14. Insira um dos seguintes comandos para verificar se um listener HTTP foi criado:
`winrm enumerate winrm/config/listener`
ou
`winrm e winrm/config/Listener`
15. Insira o seguinte comando no prompt de comando para fazer o teste localmente.
`winrm id`

Etapa 5: Execute a configuração HTTPS no servidor (para usar HTTPS, e não HTTP)

Esta etapa consiste em dois processos distintos: geração de um certificado autoassinado, se o certificado não existir, e importação para um servidor Windows. Se ainda não existir, você deverá configurar um certificado autoassinado no servidor Windows para ativar a comunicação HTTPS/SSL com a interface do usuário do BACS no cliente Windows. O cliente Windows também deve ser configurado com o certificado autoassinado. Consulte [Executar a configuração de HTTPS \(se você planeja usar HTTPS\)](#).



Nota: O certificado autoassinado pode ser criado em qualquer servidor Windows. O servidor não requer que o BACS esteja instalado. O certificado autoassinado gerado em qualquer servidor Windows deve ser copiado na unidade local do cliente.

1. Clique em **Iniciar** (ou pressione a tecla com o logotipo do Windows) e selecione **Executar**.
2. Digite `gpedit.msc` para abrir o editor local de Política de grupo.
3. Em **Configuração do computador**, abra a pasta **Modelos administrativos** e depois, a pasta **Componentes do Windows**.
4. Selecione **Windows Remote Management (WinRM)**.
5. Em **Windows Remote Management (WinRM)**, selecione **Cliente WinRm**.
6. Em **Cliente WinRM**, clique duas vezes em **Hosts confiáveis**.
7. Em **Lista de hosts confiáveis**, insira os nomes de host dos clientes. Se todos os clientes forem confiáveis, insira somente um asterisco (*).
8. Selecione **Serviço do WinRM**.
9. Ative **Permitir autenticação básica**.

Para gerar um certificado autoassinado para o Windows Server:

O Openssl no Windows pode ser usado para gerar o certificado autoassinado como segue:

1. Insira o seguinte comando para gerar uma chave privada:
`openssl genrsa -des3 -out server.key 1024`
2. Será solicitado que você insira uma senha. Memorize-a.
3. Execute as seguintes etapas para gerar um Certificate Signing Request (CSR).
Durante a geração do CSR, serão solicitadas várias informações. Quando for solicitado o "Nome comum", insira o nome de host do servidor Windows ou endereço IP.
Insira o seguinte comando (as respostas de amostra são mostradas):

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

Se este comando não funcionar, tente o seguinte:

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

O arquivo openssl.cnf deve ser colocado no mesmo diretório onde está openssl. O openssl.cnf está localizado na pasta C:\Program Files (x86)\GnuWin32\share.

As seguintes informações são solicitadas:

- Nome do país (código de 2 letras) []: **US**
- Nome do estado ou província (nome completo) []: **California**
- Nome da localidade (por ex., cidade) []: **Irvine**
- Nome da organização (por ex., empresa) []: **Broadcom Corporation**
- Nome da unidade organizacional (por ex., seção) []: **Engenharia**
- Nome comum (por ex., SEU nome) []: Insira o nome do host ou o endereço IP do servidor Windows. Para IPv6, digite o Nome comum no formato [xyxy:xxx:.....:xxx], **incluindo os colchetes []**.
- (Opcional) Endereço de e-mail []:

Insira os seguintes atributos adicionais a serem enviados com sua solicitação de certificado:

- Uma senha difícil []: **senha1**
- Um nome de empresa opcional []:

4. Remova a senha da chave.

Insira os seguintes comandos:

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

5. Gere um certificado autoassinado:

Para gerar um certificado autoassinado que seja ativo durante 365 dias, insira o seguinte comando:

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

É exibida a seguinte saída:

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

6. Insira o seguinte comando para verificar o certificado autoassinado gerado.

```
openssl verify server.crt
```

É exibida a seguinte saída:

```
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 a mensagem de erro "error 18 at 0 depth lookup:self signed certificate". Esse erro indica que é um certificado autoassinado.

7. Converta o certificado do formato "crt" para "pkcs12", como segue:

Para um servidor Windows, o certificado deve estar no formato pkcs12. Insira o seguinte comando:

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

Será solicitado o seguinte:

Enter Export Password:

Verifying - Enter Export Password:

Insira a senha e memorize-a. A senha é necessária durante a importação do certificado no servidor e cliente Windows.

8. Faça uma cópia do arquivo de certificado `server.crt` e coloque-a no servidor no qual o BACS será instalado para que possa ser importada. Se você planeja usar um cliente Windows para conectar ao servidor que executa o BACS, o certificado também precisará ser transferido (copiado e colado) no sistema do cliente.



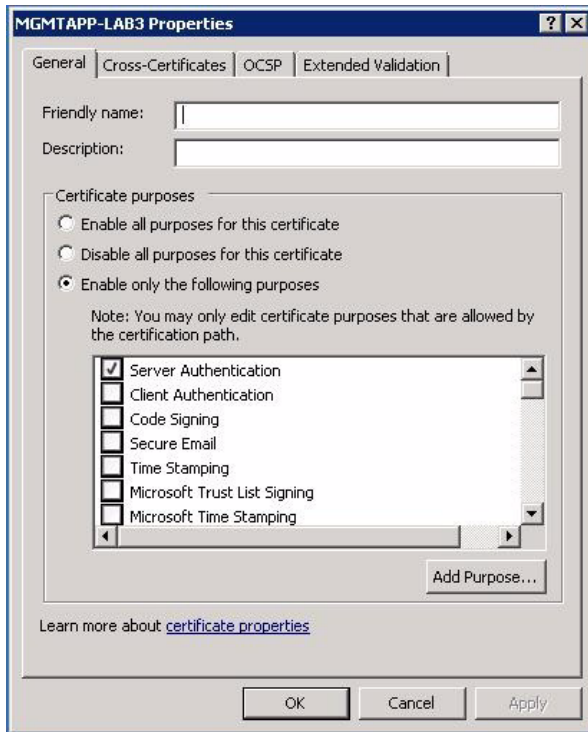
Nota: Um certificado separado deve ser gerado para endereços IPv4 e IPv6 e para o nome do host.

Para instalar o certificado autoassinado no Windows server:

Transfira o arquivo `hostname.pfx` que você gerou no servidor Windows antes de instalar o certificado:

1. Clique em **Iniciar** (ou pressione a tecla com o logotipo do Windows) e selecione **Executar**.
2. Digite **MMC** e clique em **OK**.
3. Clique em **Arquivo > Adicionar/Remover snap-in**.
4. Clique em **Adicionar**.
5. Selecione **Certificados** e clique em **Adicionar**.
6. Selecione **Conta do computador**.
7. Clique em **Avançar** e depois em **Concluir**.
8. Clique em **Fechar** e em **OK**.
9. Abra a pasta **Certificados (Computador local)** e depois abra a pasta **Pessoal**.
10. Clique com o botão direito do mouse em **Certificados**, selecione **Todas as tarefas** e clique em **Importar**.
11. Clique em **Avançar** para iniciar o Assistente de importação de certificado.
12. Navegue para selecionar **hostname.pfx**.
13. Quando for solicitada a senha da chave privada, insira a mesma senha que você criou em [Para gerar um certificado autoassinado para o Windows Server](#).
14. Siga as instruções, selecione os padrões e continue.
O certificado é exibido quando é instalado no lado direito da janela. O nome será aquele que você especificou durante a criação de um certificado autoassinado.
15. Clique com o botão direito do mouse no certificado e selecione **Propriedades**.

Uma caixa de diálogo é exibida como segue:



16. Certifique-se de que apenas a **Autenticação do servidor** seja ativada, conforme mostrado na figura.

17. Abra **Autoridades de certificação raiz confiáveis** e abra **Certificados**.

18. Siga as instruções de [Etapa 11.](#) a [Etapa 17.](#)



Nota: Consulte [Executar a configuração de HTTPS \(se você planeja usar HTTPS\)](#) para obter instruções sobre a importação do certificado autoassinado em um cliente.

Etapa 6: Configure o HTTPS/SSL do WinRM no servidor

1. Crie o Listener WinRM, como segue:

- Clique em **Iniciar** (ou pressione a tecla com o logotipo do Windows) e selecione **Executar**.
- Digite **MMC** e clique em **OK**.
- Selecione o certificado autoassinado no armazenamento Pessoal.

Por exemplo, se o certificado for criado com um nome de host, o nome não aparecerá.

- Clique duas vezes no certificado para abri-lo.
- Clique na guia **Detalhes**.
- Role e selecione o campo **Impressão digital**.
- Selecione e copie a impressão digital na janela **Detalhes** para que você possa inseri-la na próxima etapa.
- Retorne ao prompt de comando.

i. Insira o seguinte comando:

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


**OBSERVAÇÕES:**

- Se o certificado foi gerado usando o nome do host, insira o nome. Se tiver sido gerado com o endereço IP, insira o endereço IP. Para um endereço IPv6, use colchetes [] antes e depois do endereço.
 - Se o HTTPS estiver configurado em seu sistema, o ouvinte deve ser excluído antes de criar um novo ouvinte de HTTPS. Use o seguinte comando:
`winrm delete winrm/config/Listener?Address=*&Transport=HTTPS`
- j. O comando acima cria um listener na porta HTTPS (5986) usando qualquer/todo endereço de rede do servidor e o certificado gerado my SelfSSL.
- k. É possível usar o comando `winrm` para modificar ou definir o listener HTTPS, pois os listeners WinRM podem ser configurados em qualquer porta definida pelo usuário.
- l. No prompt de comando, execute o seguinte comando para verificar se o(s) listener(s) foi(foram) configurado(s):
`winrm` e `winrm/config/listener`
2. Teste a conexão HTTPS/SSL no servidor.
- a. No prompt de comando no servidor, digite o seguinte comando:
`winrs -r:https://yourserver:5986 -u:username -p:password hostname`
- b. Se configurado corretamente, a saída do comando mostrará o nome do host do servidor.
- c. Para verificar a Configuração do serviço WinRM, execute o seguinte comando:
`winrm get winrm/config/service`

Etapa 7: Configuração adicional do servidor

Se necessário, modifique as regras de firewall como segue:

Windows Server 2008 R2

1. No menu **Ferramentas administrativas**, abra **Firewall do Windows com segurança avançada**.
2. Clique com o botão direito do mouse em **Regras de entrada** e selecione **Nova regra**.
O assistente de nova regra é aberto.
3. Selecione **Porta** e clique em **Avançar**.
4. Na tela **Protocolo e portas**, selecione **TCP** e insira a porta específica, por exemplo, 5985 para HTTP ou 5986 para HTTPS.
5. Clique em **Next (Avançar)**.
6. Na tela **Ação**, selecione **Permitir a conexão** e clique em **Avançar**.
7. Para **Perfil**, é possível selecionar todos os três perfis se o seu servidor estiver em um grupo de trabalho.
8. Especifique um nome para a regra e clique em **Concluir**.
9. Certifique-se de que a nova regra seja ativada (a caixa de seleção verde é marcada).

Windows XP

1. Clique em **Iniciar > Painel de controle** e, em seguida, clique duas vezes em **Firewall do Windows**.
2. Clique na guia **Exceções**
3. Clique em **Adicionar porta**.
4. Insira um **Nome** significativo, por exemplo "regra WinRM" e número da porta, por exemplo, 5985 para HTTP ou 5986 para HTTPS.
5. Clique em **Ok**.

Comandos WinRM úteis

Comando	Descrição
<code>winrm quickconfig</code> or <code>winrm qc</code>	Defina o WinRM com as configurações padrão
<code>winrm enumerate winrm/config/Listener</code> or <code>winrm e winrm/config/Listener</code>	Ajuda a verificar qual listener de serviço está ativado e atendendo a qual porta e Endereço IP.
<code>winrm get winrm/config/Service</code>	Verifica a configuração do serviço WinRM.
<code>winrm delete winrm/config/Listener?Address=*&Transport=HTTPS</code>	Exclui um listener (neste caso excluindo um listener HTTPS).

Sites de WinRM úteis

- <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>
- Os seguintes artigos em <http://support.microsoft.com>:
 - "Configurando WINRM para HTTPS"
 - "Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0 e BITS 4.0)"

Instalação do cliente Windows para WS-MAN

No cliente Windows, execute as seguintes etapas de configuração.

1. Executar a configuração de HTTP (se você planeja usar HTTP)
 - a. Clique em **Iniciar** (ou pressione a tecla com o logotipo do Windows) e selecione **Executar**.
 - b. Digite **gpedit.msc** para abrir o editor local de Política de grupo.
 - c. Em **Configuração do computador**, abra a pasta **Modelos administrativos** e depois, a pasta **Componentes do Windows**.
 - d. Selecione **Windows Remote Management (WinRM)**.
 - e. Em **Windows Remote Management (WinRM)**, selecione **Cliente WinRm**.
 - f. Em **Cliente WinRM**, clique duas vezes em **Hosts confiáveis**.
 - g. Em **Lista de hosts confiáveis**, insira os nomes de host dos clientes e clique em **OK**. Se todos os clientes forem confiáveis, insira somente **"**"**.
 - h. Selecione **Serviço do WinRM**.
 - i. Ative **Permitir autenticação básica** e clique em **OK**.
 - j. Execute o seguinte comando no prompt de comando para testar a conexão:
`winrm id -remote:<remote machine Hostname or IP Address>`
2. Executar a configuração de HTTPS (se você planeja usar HTTPS)

Depois de gerar um certificado autoassinado, conforme descrito em [Para gerar um certificado autoassinado para o Windows Server](#), é possível importar o certificado no cliente para facilitar a conexão entre servidor e cliente. Verifique se todas as etapas citadas na seção [Para gerar um certificado autoassinado para o Windows Server](#) foram concluídas, incluindo a cópia de `hostname.pfx` no local onde o cliente pode acessá-la antes de continuar com as seguintes etapas.

 - a. Clique em **Iniciar** (ou pressione a tecla com o logotipo do Windows) e selecione **Executar**.
 - b. Digite **MMC** e clique em **OK**.
 - c. Clique em **Arquivo** e selecione **Adicionar/Remover snap-in**.
 - d. Clique em **Adicionar**.
 - e. Selecione **Certificados** e clique em **Adicionar**.

- f. Selecione **Conta do computador** e clique em **Avançar**.
- g. Clique em **Concluir**.
- h. Clique em **Fechar** e em **OK**.
- i. Em **Certificados (Computador local)**, clique com o botão direito do mouse em **Autoridades de certificação raiz confiáveis**, selecione **Todas as tarefas** e escolha **Importar**.
- j. Clique em **Avançar** para iniciar o Assistente de importação de certificado.
- k. Navegue para selecionar o arquivo .pfx que você gerou em [Para gerar um certificado autoassinado para o Windows Server](#). Altere a seleção na lista **Arquivos do tipo** para **Troca de informações pessoais (*.pfx, *.p12)**, selecione o arquivo *hostname.pfx* e clique em **Abrir**.
- l. Insira a rede que você atribuiu à chave privada e clique em **Avançar**.

3. Configurar WinRM HTTPS/SSL

É possível executar o winrm de um cliente para recuperar informações do servidor usando a conexão de HTTPS do WinRM. Execute as etapas a seguir para testar a conexão de HTTPS/SSL do WinRM no cliente:

- a. Para recuperar as informações do sistema operacional do servidor, insira o seguinte comando.

```
winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername -u:username -p:password -skipCAcheck
```
- b. Para recuperar as informações de identidade do WinRM do servidor, insira o seguinte comando.

```
winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
```
- c. Para enumerar os serviços Windows no servidor, insira o seguinte comando.

```
winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -skipCAcheck
```



Nota: É importante usar o switch `-skipCAcheck` no teste da linha de comando `winrm` quando o certificado é autogerado e não é importado para o cliente. Caso contrário, a mensagem de erro a seguir é exibida: `WSManFault`.

Uso de WMI

Nenhuma configuração especial é necessária para usar o WMI no cliente Windows. Execute as etapas nas seções a seguir para configurar o WMI no servidor Windows.

Etapa 1: Configura a segurança do espaço de nomes usando o controle do WMI

O Controle de WMI fornece uma maneira de gerenciar a segurança do espaço de nomes. É possível iniciar o Controle de WMI no prompt de comando usando este comando:

```
wmimgmt
```

Em computadores com Windows 9x ou Windows NT4 que tenham WMI instalado, use este comando:

```
wbemcntl.exe
```

Como alternativa, é possível acessar o controle de WMI e a guia Segurança como segue:

1. Clique com o botão direito do mouse em **Meu computador** e clique em **Gerenciar**.
2. Clique duas vezes em **Serviços e aplicativos** e depois clique duas vezes em **Controle de WMI**.
3. Clique com o botão direito do mouse em **Controle de WMI** e, em seguida, clique em **Propriedades**.
4. Em Propriedades de Controle de WMI, clique na guia **Segurança**.
5. Uma pasta denominada Raiz com um sinal de mais (+) ao lado dela agora deve estar visível. Expanda essa árvore quando necessário para localizar o espaço de nomes para o qual você deseja definir permissões.
6. Clique em **Segurança**.

Uma lista de usuários e suas permissões é exibida. Se o usuário estiver na lista, modifique as permissões conforme apropriado. Se o usuário não estiver na lista, clique em **Adicionar** e adicione o nome do usuário a partir do local (máquina local, domínio etc.) em que a conta reside.



OBSERVAÇÕES: É possível adicionar essas exportações no final de `.bash_profile`. Este arquivo está localizado no diretório `/root`.

- Para visualizar e definir a segurança do espaço de nomes, o usuário deve ter permissões de Leitura de segurança e Edição de segurança. Os administradores têm essas permissões por padrão e podem atribuir as permissões a outras contas de usuário quando necessário.
- Se esse usuário precisar acessar o espaço de nomes remotamente, você deverá selecionar a permissão Ativação remota.
- Por padrão, as permissões do usuário definidas em um espaço de nomes se aplicam somente a esse espaço de nomes. Se você quiser que o usuário tenha acesso a um espaço de nomes e a todos os subespaços de nomes na árvore abaixo dele ou somente em subespaços de nomes, clique em **Avançado**. Clique em **Editar** e especifique o escopo do acesso na caixa de diálogo exibida.

Etapa 2: Conceda a Permissão de inicialização e ativação remotas de DCOM

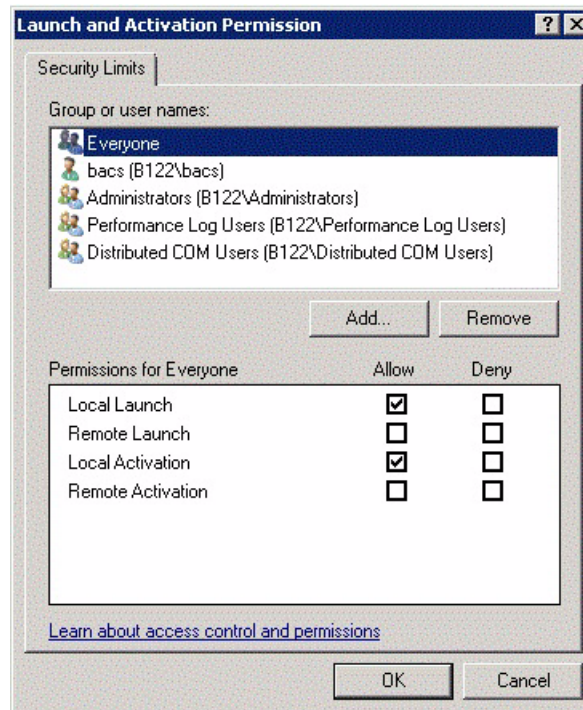
No ambiente de domínio do Windows, a conta de Administrador de domínio tem o nível de privilégio necessário para acessar o componente WMI para gerenciamento de BACS e, portanto, nenhuma configuração especial é necessária. Entretanto, em uma grande empresa, um usuário que acessa o host local ou remoto usando a interface do usuário do cliente BACS4 nem sempre precisa ter o privilégio de conta de administrador do domínio. É necessário configurar o acesso de

segurança de WMI no host remoto para permitir que o usuário conecte a ele usando a interface do usuário do cliente BACS4.

Essa configuração pode ser feita facilmente executando o seguinte procedimento. Se você não tiver privilégios suficientes para configurar a segurança de acesso do WMI, entre em contato com seu Administrador de rede.

1. Clique em **Iniciar**, **Executar**, digite **DCOMCNFG** e clique em **OK**.
2. A caixa de diálogo Serviços de componente é exibida.
3. Abra **Serviços de componente** e, em seguida, abra **Computadores**.
4. Clique com o botão direito do mouse em **Meu computador** e clique em **Propriedades**.
5. Em **Propriedades do meu computador**, clique na guia **Segurança de COM**.
6. Em **Permissões de inicialização e ativação**, clique em **Editar limites**.
7. Siga essas etapas se o seu nome ou grupo não aparecer na lista **Nomes de grupos ou de usuários**.
 - a. Na caixa de diálogo Permissão de inicialização, clique em **Adicionar**.
 - b. Na caixa de diálogo Selecionar usuários, Computadores ou Grupos, adicione seu nome e o grupo na caixa **Inserir os nomes de objeto a serem selecionados** e, em seguida, clique em **OK**.
 - c. Na caixa de diálogo Permissão de inicialização, selecione seu usuário e grupo na lista **Nomes de grupos ou de usuários**.
 - d. Na área **Permissões para usuário**, selecione **Permitir** para **Inicialização remota** e **Ativação remota** e, em seguida, clique em **OK**.

Figura 8: Permissão de inicialização e ativação



Para obter mais informações, consulte [Protegendo a conexão de WMI remota](#) no site de Rede do desenvolvedor Microsoft.

Configuração especial para WMI em diferentes sistemas

No Windows Vista e Windows 7, para permitir que todos os usuários no grupo do administrador se conectem usando o espaço de nomes WMI, talvez seja necessário que o usuário altere LocalAccountTokenFilterPolicy quando necessário.

Seção 13: Uso do Broadcom Advanced Control Suite 4

- [Visão geral do Broadcom Advanced Control Suite](#)
- [Inicialização do Broadcom Advanced Control Suite](#)
- [Interface BACS](#)
- [Configuração das preferências no Windows](#)
- [Conexão do host](#)
- [Gerenciamento do host](#)
- [Gerenciamento do Adaptador de rede](#)
- [Exibição de estatísticas](#)
- [Configuração de equipes](#)
- [Configuração com o utilitário de interface da linha de comando](#)
- [Solução de problemas do BACS](#)

Visão geral do Broadcom Advanced Control Suite

O Broadcom Advanced Control Suite (BACS) é um utilitário integrado que fornece informações úteis sobre cada adaptador de rede que está instalado em seu sistema. O BACS também permite que você realize testes detalhados, diagnósticos e análises em cada adaptador, bem como visualize e modifique valores de propriedade e visualize estatísticas de tráfego para objetos de rede. O BACS opera em sistemas operacionais Windows e Linux.

O Broadcom Advanced Server Program (BASP), executado no Broadcom Advanced Control Suite, é utilizado para configurar equipes para equilíbrio de carga, tolerância a falhas e LANs virtuais (VLANs). A funcionalidade do BASP está disponível apenas em sistemas que usam, no mínimo, um adaptador de rede Broadcom. O BASP opera apenas em sistemas operacionais Windows.



Nota: Alguns recursos do BACS são relevantes somente para adaptadores específicos. Como uma única instância do BACS pode ser usada para comunicação com diferentes tipos de hosts e adaptadores, este documento descreve todos os recursos do BACS.

O aplicativo BACS inclui uma interface gráfica do usuário e uma interface de linha de comando (BACSCLI). A interface do usuário do BACS e o CLI do BACS podem operar nas seguintes famílias de sistema operacional:

- Windows
- Windows Server
- Linux Server

Para obter informações sobre as versões de sistemas operacionais mais recentes e compatíveis, consulte a documentação de lançamento fornecida com seu software.

Inicialização do Broadcom Advanced Control Suite

No Painel de controle, clique em **Broadcom Control Suite 4**, ou clique no ícone BACS na barra de tarefas localizada na parte inferior do desktop do Windows ou Windows Server.

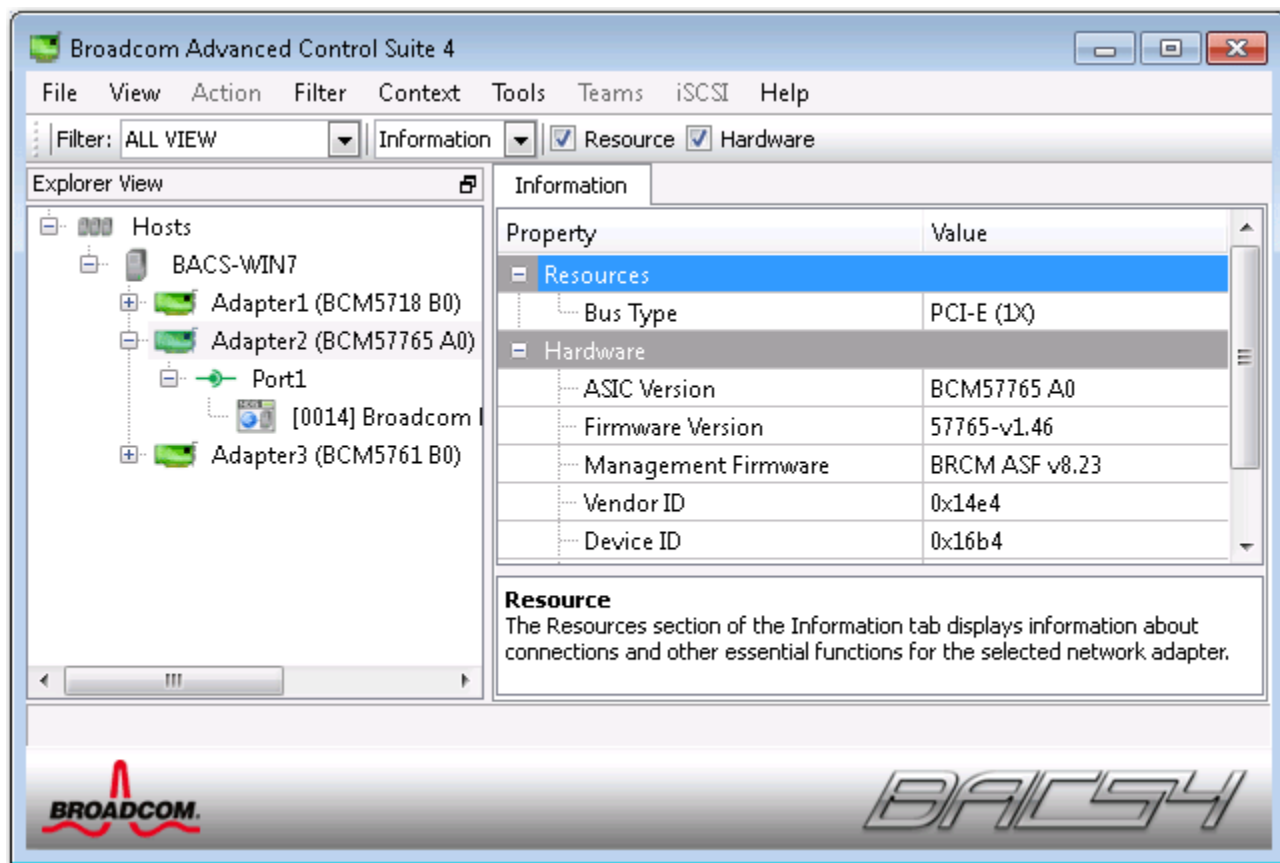
Em sistemas Linux, você pode clicar duas vezes no ícone BACS4 na área de trabalho ou acessar o programa BACS na barra de tarefas em **Ferramentas do sistema**. Se estiver tendo dificuldades para abrir o BACS em um sistema Linux, consulte o tópico relacionado em [Solução de problemas do BACS](#).

Interface BACS

A interface BACS é composta pelas seguintes regiões:

- Painel Visualização Explorer
- Seletor Visualização de contexto
- Painel Visualização de contexto
- Barra de menus
- Painel de descrição

Por padrão, o painel Visualização Explorer está fixado e encaixado no lado esquerdo da janela principal, o painel Visualização de contexto na direita, o seletor Visualização de Contexto abaixo da barra de menus e o painel de Descrição abaixo do painel Visualização de contexto. Arraste o divisor entre qualquer um dos dois painéis para variar o tamanho deles.



Painel Visualização Explorer

É possível fixar e encaixar o painel Visualização Explorer no lado esquerdo, lado direito, parte superior ou inferior da janela principal.

O painel Visualização Explorer lista os objetos que podem ser visualizados, analisados, testados ou configurados pelo BACS. Quando um item for selecionado no painel Visualização Explorer, as tabelas que mostram as informações e opções disponíveis para o item serão exibidas no painel Visualização de contexto.

A organização deste painel foi projetada para apresentar os objetos gerenciáveis na mesma forma hierárquica, bem como drivers e seus respectivos subcomponentes. Isso simplifica o gerenciamento de diversos elementos do controlador da interface de rede (NIC) convergido. O nível superior da hierarquia é o container host, que lista todos os hosts gerenciados pelo BACS. Os hosts abaixo são os adaptadores de rede instalados com os elementos gerenciáveis, bem como porta física, NDIS e iSCSI abaixo dos adaptadores.

O ícone ao lado de cada dispositivo no painel Visualização Explorer mostra o status correspondente. Um ícone ao lado do nome de um dispositivo que parece normal significa que o dispositivo está conectado e funcionando.

- **X.** Um "X" vermelho no ícone do dispositivo indica que, no momento, ele não está conectado à rede.
- **Acinzentado.** Um ícone de dispositivo que aparece acinzentado indica que, no momento, ele está desativado.

Seletor Visualização de contexto

O seletor Visualização de contexto exibe abaixo a barra de menus e inclui o filtro e as categorias da guia. Embora seja possível que as categorias exibidas nas guias do painel Visualização de contexto expandam e falhem como alternativa, você pode exibir a categoria ao selecionar a caixa ao lado do nome da categoria.

Visualização de filtro

Em um ambiente de hosts múltiplos usando diversos C-NICs, um grande número de elementos gerenciáveis por adaptador podem ser difíceis e complicados para exibir, configurar e gerenciar todos os elementos. Use o filtro para selecionar uma determinada função do dispositivo. Visualizações do filtro possíveis incluem:

- Todos
- VISUALIZAÇÃO DA EQUIPE
- VISUALIZAÇÃO DE NDIS
- VISUALIZAÇÃO DE iSCSI
- VISUALIZAÇÃO DO ALVO iSCSI

Painel Visualização de contexto

O painel Visualização de contexto exibe todos os parâmetros para que você possa visualizar o objeto selecionado no painel Visualização Explorer. Os parâmetros estão agrupados pelas guias e categorias, dependendo do tipo de parâmetro. As guias disponíveis são, Informações, Configurações, Diagnóstico e Estatísticas. Como a interface do BACS é relacionada ao contexto, apenas as informações aplicáveis ao item selecionado podem ser vistas ou ajustadas no painel Visualização de contexto.

Barra de menus

O seguinte aparece na barra de menus, no entanto, os itens de menu são relacionados ao contexto, nem todos estarão disponíveis sempre:

Menu Arquivo

- Salvar equipe como: salva as configurações da equipe atual para um arquivo.
- Restaurar equipe: restaura qualquer configuração de equipe salva em um arquivo.

Menu Ações

- Remover host: remove o host selecionado.
- Atualizar host: atualiza o host selecionado.

Visualizar menu

- Visualização Explorer: exibe/oculta o painel Visualização Explorer.
- Barra de ferramentas: exibe/oculta a barra de ferramentas.
- Barra de status: exibe/oculta a barra de status.
- Logotipo Broadcom: exibe/oculta o logotipo Broadcom no BACS para otimizar o máximo do espaço visível.

Menu Ferramentas

- Opções: usado para configurar as preferências BACS.

Equipes (apenas Windows)

- Criar equipes: cria novas equipes com o Assistente de formação de equipes ou no Modo avançado.
- Gerenciar equipes: gerencia novas equipes com o Assistente de formação de equipes ou no Modo avançado.

Painel de descrição

O Painel de descrição fornece informações, instruções de configurações e opções para o parâmetro selecionado no painel Visualização de contexto.

Configuração das preferências no Windows

Para ativar ou desativar o ícone do BACS na bandeja no Windows

Em sistemas Windows, o BACS coloca um ícone na barra de tarefas do Windows quando o programa é instalado. Use a janela Opções para ativar ou desativar esse ícone.

1. No menu **Ferramentas**, selecione **Opções**.
2. Selecione ou desmarque a opção **Ativar bandeja BACS** (a opção é ativada por padrão).
3. Clique em **Ok**.

Configuração do modo de formação de equipes no Windows

1. No menu **Ferramentas**, selecione **Opções**.
2. Selecione o **Modo inteligente** se não precisar do assistente de formação de equipes para criar equipes; caso contrário, selecione **Modo do assistente**.
3. Clique em **Ok**.

Configuração do tempo de atualização da Visualização Explorer no Windows

1. No menu **Ferramentas**, selecione **Opções**.
2. Selecione **Automático** para definir o tempo de atualização da Visualização Explorer para 5 segundos. Caso contrário, selecione **Personalizar** e selecione um tempo, em segundos.
3. Clique em **Ok**.

Conexão do host

É possível adicionar um ou mais hosts do Windows ou do Linux para gerenciar no BACS.

Para adicionar um host local

1. No menu **Ações**, clique em **Adicionar host**.
2. Para os hosts do Windows e do Linux, não altere as configurações padrão. O **Nome do usuário** e **Senha** não são solicitados enquanto estiver conectando-se ao host local.
3. Selecione **Persistir** se desejar que o BACS salve as informações do host.
4. Clique em **OK**. Agora os BACS podem ser usados para visualizar informações e gerenciar o host.

Para adicionar um host remoto

1. No menu **Ações**, clique em **Adicionar host**.
2. Digite o nome do host remoto ou o endereço IP na caixa de **host**.
3. Selecione o protocolo da lista de **Protocolo**. As opções de protocolo para Windows são **WMI**, **WSMan** ou **Tentar todas**. As opções de protocolo para Linux são **CimXML**, **WinRM** ou **Tentar todas**. A opção **Tentar todas** força o cliente GUI a tentar todas as opções.
4. Selecione o esquema **HTTP** ou o esquema **HTTPS** para a segurança adicionada.
5. Digite o valor do **Número de porta** usado para configurar o host se for diferente do valor padrão de **5985**.
6. Digite o **Nome de usuário** e a **Senha**.
7. Selecione **Persistir** se desejar que o BACS salve as informações do host. O host será exibido no painel Explorer sempre que você reabrir o BACS e não será preciso inserir o endereço IP ou o nome do host quando conectar ao host. Por razão de segurança, digite o **Nome de usuário** e **Senha** sempre.
8. Clique em **Ok**.

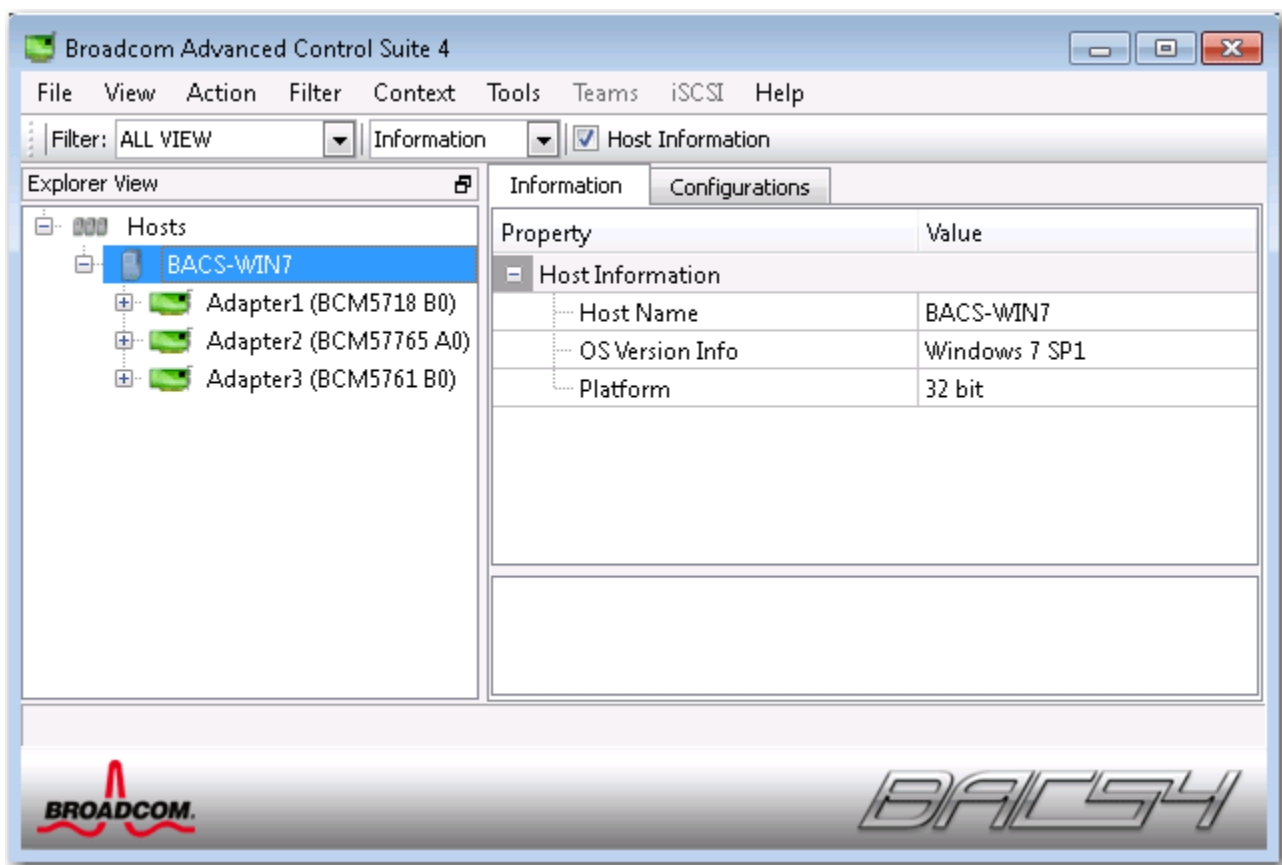
Gerenciamento do host

No nível do host, é possível visualizar informações e configurar parâmetros das seguintes guias:

- Informações
- Configuração

Para exibir as informações sobre o host

Selecione o host no painel **Visualização Explorer** e selecione a guia **Informações** para visualizar as informações sobre o nível do host.



Guia Informações: Informações sobre o host

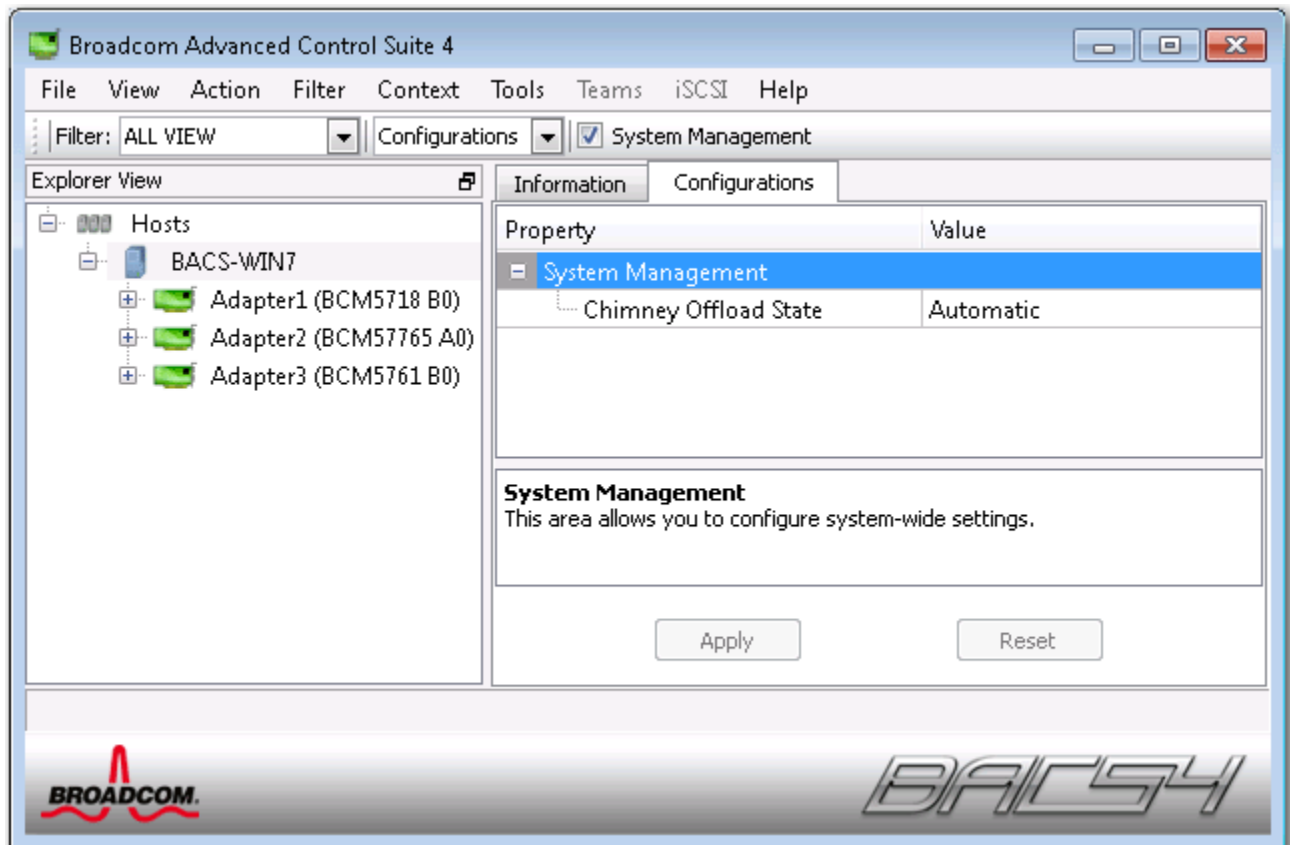
Hostname. Exibe o nome do host.

Informações sobre a Versão OS. Exibe o sistema operacional, incluindo a versão.

Plataforma. Exibe a plataforma de arquitetura de hardware (por exemplo, 32 bits ou 64 bits)

Para configurar o host

Selecione o host no painel **Visualização Explorer** e selecione a guia **Configuração** para configurar os parâmetros de nível de host.



Gerenciamento do Adaptador de rede

Os adaptadores de rede instalados aparecem um nível abaixo do host na árvore hierárquica no painel Visualização Explorer. No nível do adaptador, é possível visualizar informações e configurar parâmetros das seguintes guias:

- Informações
- Configuração

Informações sobre o Adaptador de Visualização

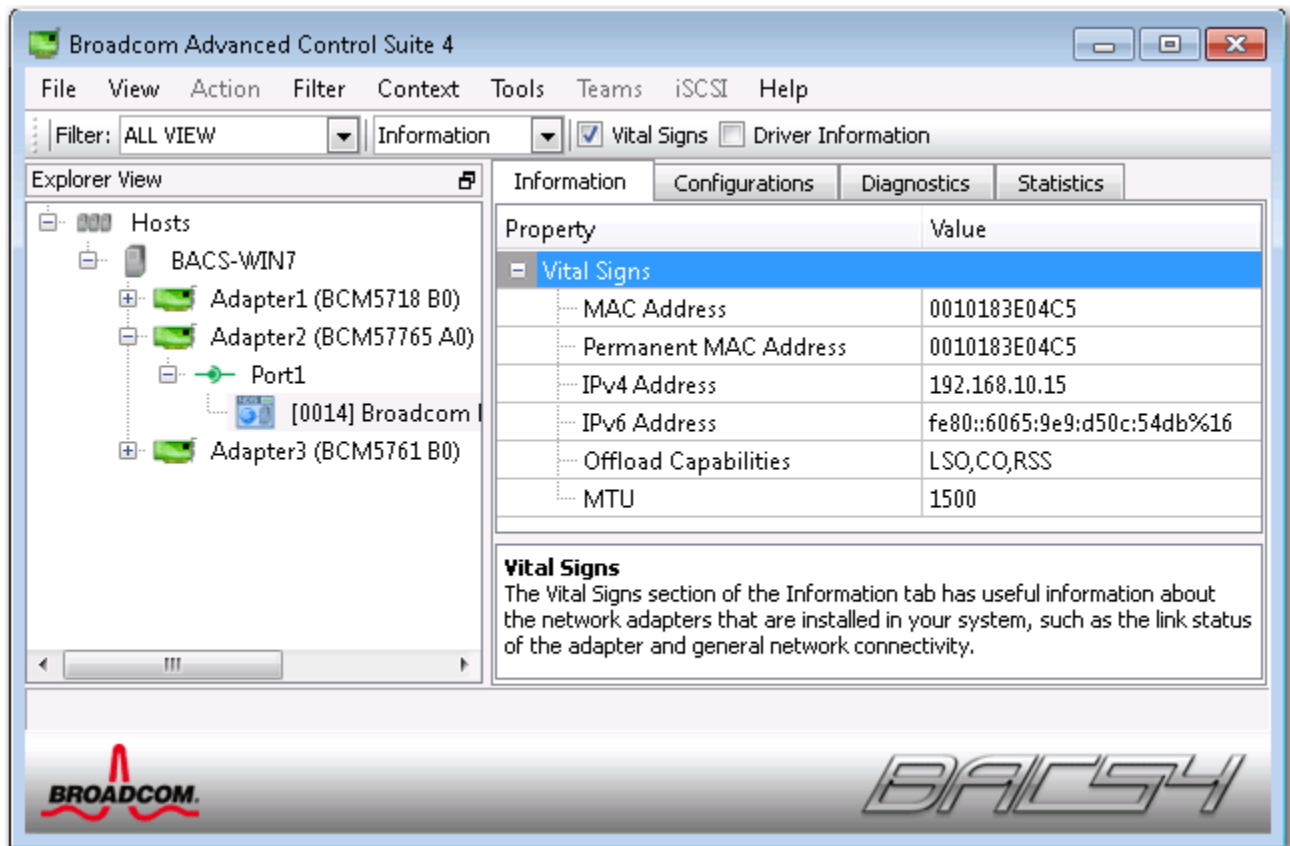
A seção **Sinal vital** da guia **Informações** tem informações úteis sobre os adaptadores de rede instalados no sistema, como o status do link do adaptador e a conectividade geral da rede.

Selecione o adaptador de rede no painel **Visualização Explorer** e selecione a guia **Informações** para visualizar as informações sobre o nível do adaptador.



OBSERVAÇÕES:

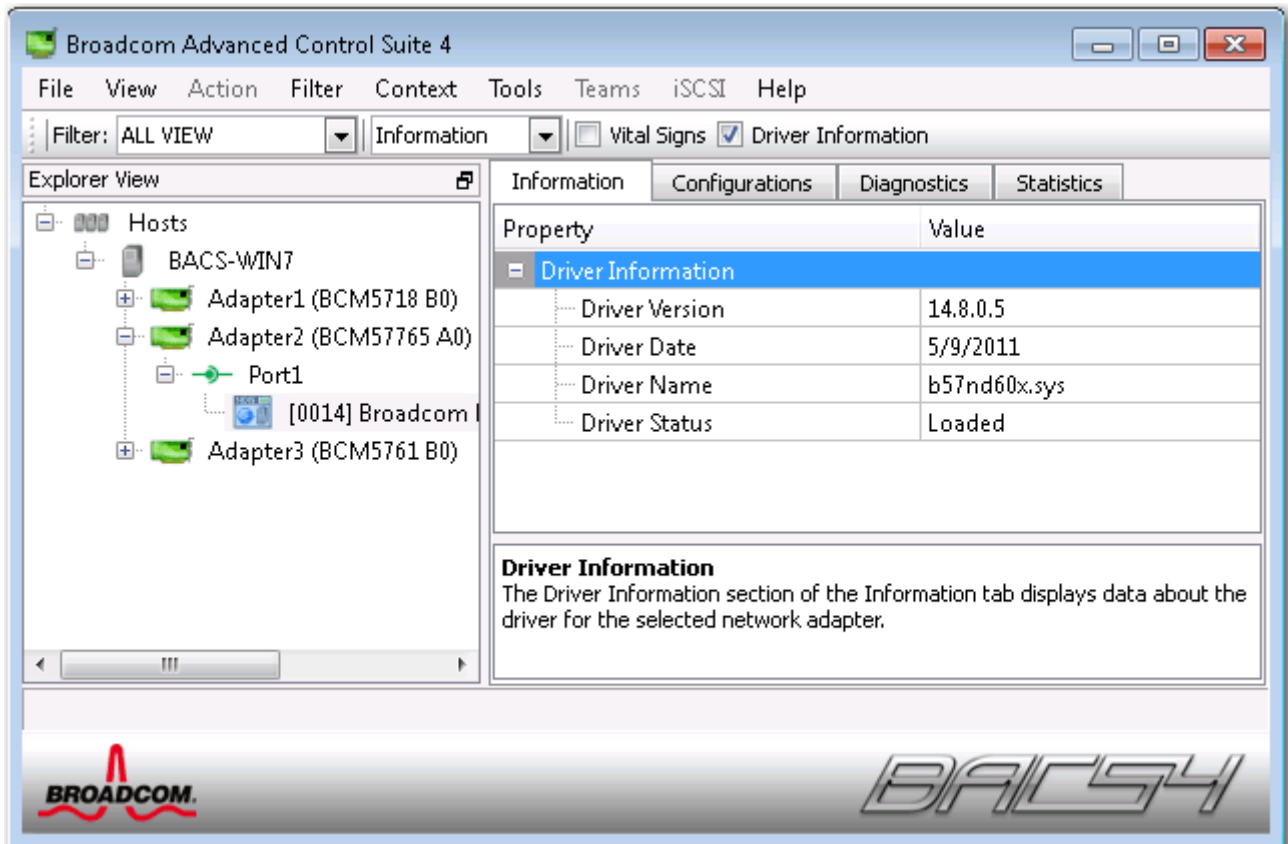
- As informações sobre os adaptadores de rede Broadcom podem ser mais completas do que as informações sobre adaptadores de rede de terceiros.
- Algumas informações talvez não estejam disponíveis para todos os adaptadores de rede Broadcom.



Exibição de informações do driver

A seção **Informações do driver** da guia **Informações** exibe dados sobre o driver do adaptador de rede selecionado.

Para visualizar as Informações do driver relativas a qualquer adaptador de rede instalado, clique no nome do adaptador listado no painel Visualização Explorer e clique na guia **Informações**.



Status do driver. O status do driver do adaptador.

- **Carregado.** Modo operacional normal. O driver do adaptador foi carregado pelo Windows e está funcionando.
- **Não carregado.** O driver associado ao adaptador não foi carregado pelo Windows.
- **Informações não disponíveis.** O valor não pode ser obtido através do driver associado ao adaptador.

Nome do driver. O nome de arquivo do driver do adaptador.

Versão do driver. A versão atual do driver do adaptador.

Data do driver. A data de criação do driver do adaptador.

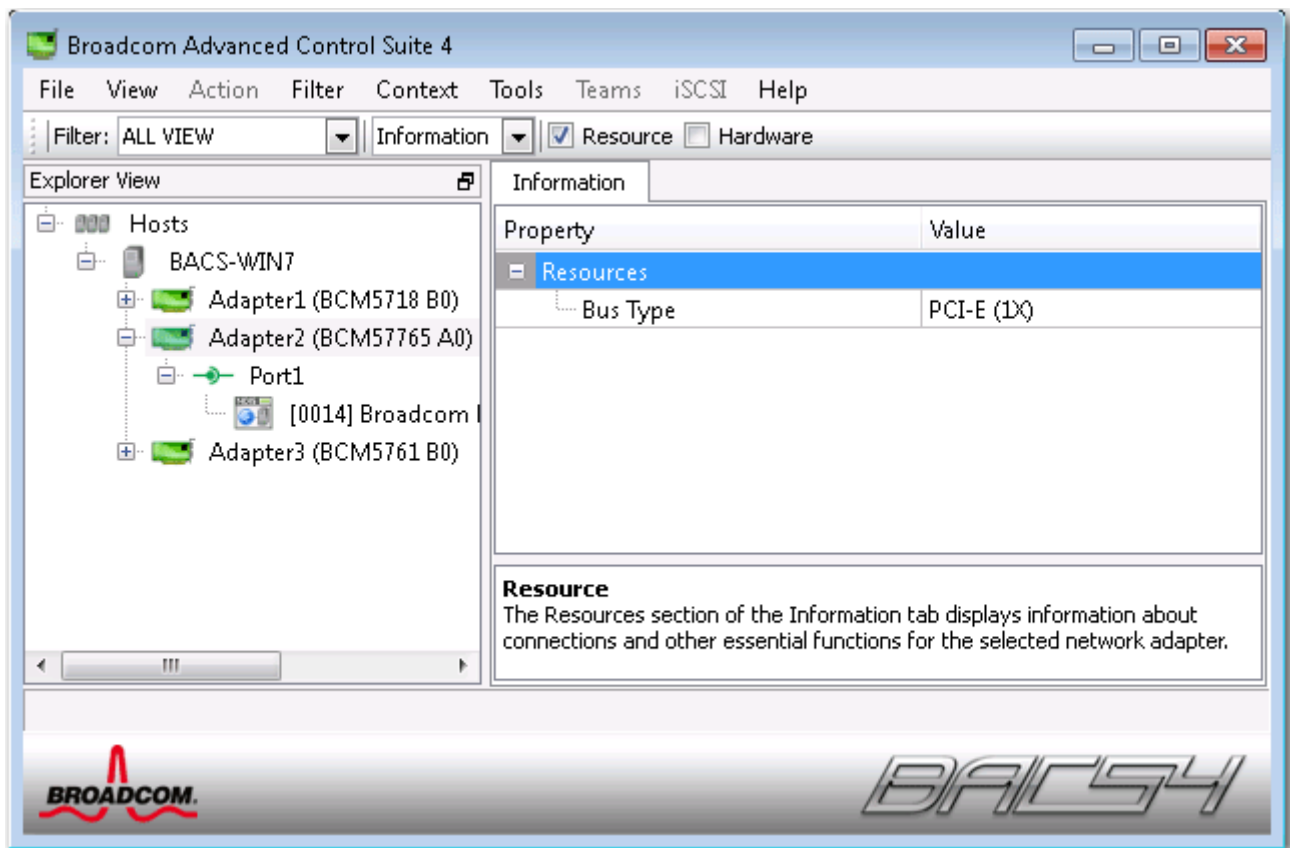
Exibição de informações de recursos

A seção **Recursos** da guia **Informações** exibe informações sobre conexões e outras funções essenciais para o adaptador de rede selecionado.

Para visualizar os Recursos de qualquer adaptador de rede instalado, clique no nome do adaptador listado no painel Visualização Explorer e clique na guia **Informações**.



Nota: Algumas informações talvez não estejam disponíveis para todos os adaptadores de rede Broadcom.



Tipo de barramento. O tipo de interconexão de entrada/saída (I/O) utilizado pelo adaptador

Nº do slot. O número do slot na placa do sistema ocupado pelo adaptador. Este item não está disponível para adaptadores do tipo PCI Express.

Velocidade do barramento (MHz). A frequência de sinal do relógio do barramento utilizado pelo adaptador. Este item não está disponível para adaptadores do tipo PCI Express.

Largura do barramento (bit). O número de bits que o barramento pode transferir de uma única vez ao controlador e pelo adaptador. Este item não está disponível para adaptadores do tipo PCI Express.

Nº do barramento. Indica o número do barramento em que o adaptador está instalado.

Nº do dispositivo. O número atribuído ao adaptador pelo sistema operacional

Nº da função. O número de porta do adaptador. Para um adaptador de porta única, o número da função é 0. Para um adaptador de duas portas, o número da função da primeira porta é 0 e o da segunda é 1.

Solicitação de interrupção. O número de linha da interrupção associado ao adaptador. Os números válidos variam de 2 a 25.

Endereço de memória. O endereço de memória mapeado atribuído ao adaptador. Esse valor nunca poderá ser 0.

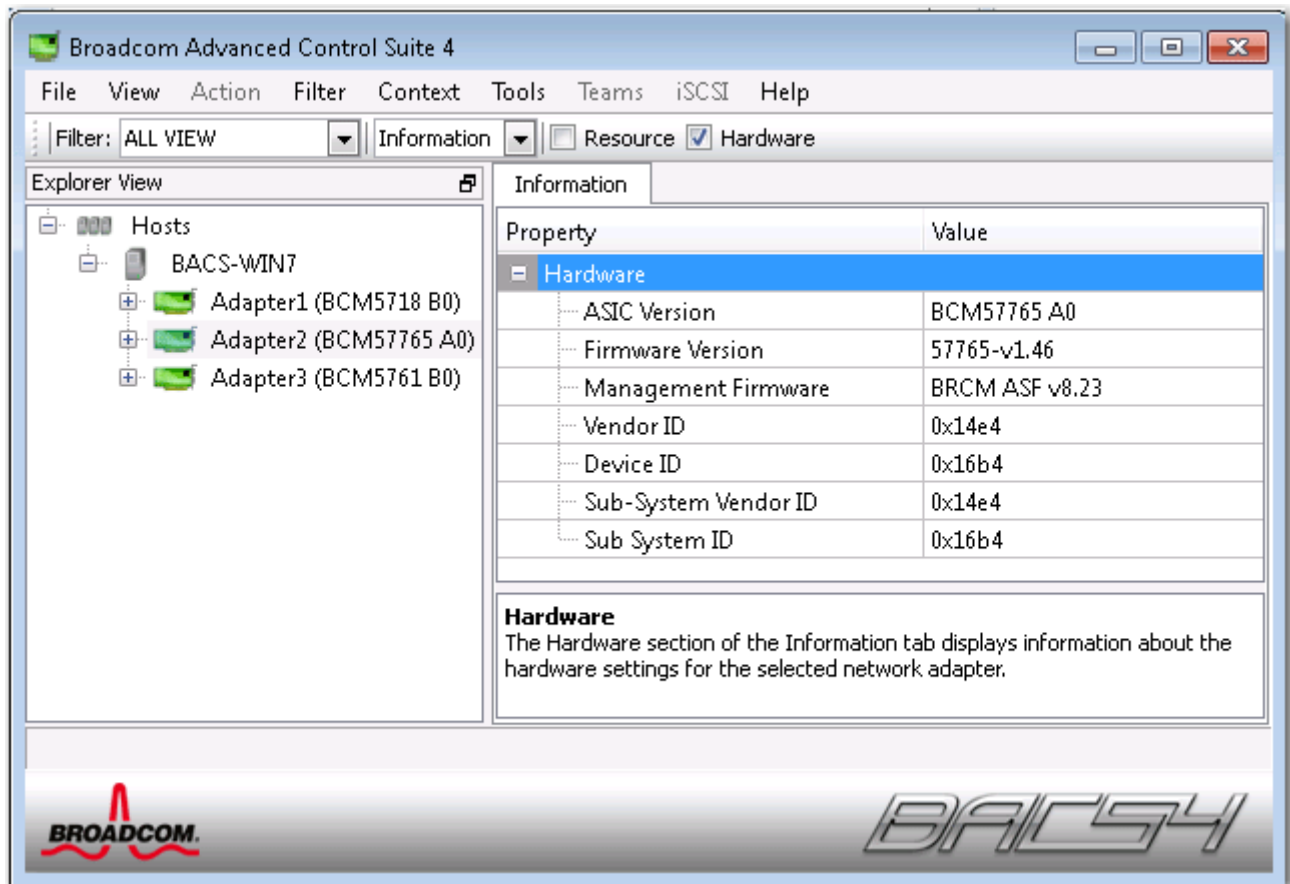
Exibição de informações de hardware

A seção Hardware da **guia Informações** exibe informações sobre as configurações de hardware do adaptador de rede selecionado.

Para visualizar o Hardware de qualquer adaptador de rede instalado, clique no nome do adaptador listado no painel Visualização Explorer e clique na guia Informações.



Nota: Algumas informações talvez não estejam disponíveis para todos os adaptadores de rede Broadcom.



Versão ASIC. A versão do chip do adaptador Broadcom (essa informação não está disponível para adaptadores fabricados por terceiros).

Versão do firmware. A versão do firmware do adaptador Broadcom (essa informação não está disponível para adaptadores fabricados por terceiros). Essas informações estão disponíveis apenas para os adaptadores do Broadcom NetXtreme.

ID do fornecedor. O ID do fornecedor.

ID do dispositivo. O ID do adaptador.

ID do fornecedor do subsistema. O ID do fornecedor do subsistema.

ID do subsistema. O ID do subsistema.

Teste de rede

A opção **Teste de rede** na guia **Diagnóstico** permite verificar a conectividade da rede IP. Este teste verifica se o driver está instalado corretamente e testa a conectividade a um gateway ou outro endereço IP especificado na mesma sub-rede. O teste de rede usa o protocolo TCP/IP para enviar pacotes ICMP para sistemas remotos e, então, aguarda uma resposta.



Nota: A opção de teste de rede não está disponível em adaptadores agrupados em equipe (consulte [Configuração de equipes](#)).

Para executar o teste de rede

1. Clique no nome do adaptador a ser testado no painel Visualização Explorer.
2. Na lista **Selecione um teste a ser executado**, escolha **Teste de rede**. Se a opção **Teste de rede** não estiver disponível, na guia **Visualização de contexto** no lado direito da janela, selecione **Diagnóstico** e, em seguida, **Teste de rede**.
3. Para alterar o endereço IP de destino, selecione **Endereço IP para ping**. Na janela Teste de rede, digite um Endereço IP de destino e clique em **OK**.
4. Clique em **Teste**.

Os resultados do teste de rede são exibidos no campo **Status**.

Execução de testes de diagnóstico

A opção **Testes de diagnóstico** na guia **Diagnóstico** permite verificar o estado dos componentes físicos de um adaptador de rede Broadcom. Os testes podem ser acionados manualmente ou o BACS 3 pode executá-los de maneira contínua. Nesse caso, o número de aprovações e falhas mostrado no campo **Resultado** de cada teste aumentará sempre que os testes forem realizados. Por exemplo, se um teste é executado quatro vezes sem falhas, o valor no campo **Resultado** desse teste é 4/0. No entanto, se houve três aprovações e uma falha, o valor no campo **Resultado** é 3/1.



OBSERVAÇÕES:

- Você deve ter privilégios de administrador para executar testes de diagnóstico.
- A conexão de rede é temporariamente interrompida enquanto esses testes são realizados.
- Nem todos os adaptadores Broadcom são compatíveis com todos os testes.

Para executar os testes de diagnóstico uma única vez

1. Clique no nome do adaptador a ser testado no painel Visualização Explorer e selecione a guia Diagnóstico.
2. Na lista **Selecione um teste a ser executado**, escolha **Testes de diagnóstico**.
3. Selecione os testes de diagnósticos que você deseja executar. Clique em **Selecionar todos** para selecionar todos os testes ou **Limpe todos** para desmarcar todas as seleções de teste.
4. Selecione o número de vezes a fim de executar os testes do **Número de loops**.
5. Clique em **Executar teste(s)**.
6. Na janela da mensagem de erro que alerta sobre a interrupção temporária da conexão de rede, clique em **Sim**. Os resultados são exibidos no campo **Resultado** de cada teste.

Registradores de controle. Este teste verifica os recursos de leitura e gravação dos registros do adaptador de rede, gravando diversos valores nos registros e verificando os resultados. O driver do adaptador utiliza esses registros para realizar funções da rede, como, por exemplo, enviar e receber informações. Uma falha no teste indica que o dispositivo pode não estar funcionando adequadamente.

Registros MII. Este teste verifica os recursos de leitura e gravação dos registros da camada física (PHY). A camada física é utilizada para controlar os sinais elétricos na conexão e configurar velocidades da rede, como 1000 Mbit/s.

EEPROM. Este teste verifica o conteúdo da EEPROM (Electrically Erasable Programmable Read-Only Memory, Memória somente leitura programável e apagável eletricamente) lendo uma parte da EEPROM e calculando a soma de verificação. O teste falhará se a soma de verificação calculada for diferente da armazenada na EEPROM. Uma atualização de imagem da EEPROM não requer uma alteração de código para este teste.

Memória interna. Este teste verifica se a memória interna do adaptador está funcionando corretamente. O teste grava valores padronizados na memória e lê os resultados retornados. O teste falhará se um valor incorreto for retornado. O dispositivo poderá não funcionar se a memória interna não estiver funcionando adequadamente.

CPU On Chip. Este teste verifica a operação das CPUs internas no adaptador.

Interrupção. Este teste verifica se o driver NDIS (Network Device Driver Interface Specification) é capaz de receber interrupções do adaptador.

Auto-retorno (loopback) de MAC. Este teste verifica se o driver NDIS é capaz de enviar e receber pacotes do adaptador.

Auto-retorno (loopback) de PHY. Este teste verifica se o driver NDIS é capaz de enviar e receber pacotes do adaptador.

LED de teste. Este teste faz todos os LEDs piscarem cinco vezes para identificar o adaptador.

Análise de cabos

A opção **Análise de cabo** na guia **Diagnóstico** permite monitorar as condições de cada par de fios em uma conexão de cabo Ethernet Categoria 5 em uma rede Ethernet. A análise mede a qualidade do cabo e a compara com a especificação IEEE 802.3ab para determinar sua compatibilidade.



OBSERVAÇÕES:

- Você deve ter privilégios de administrador para executar o teste de análise de cabo.
- A conexão de rede é interrompida temporariamente durante uma análise.
- Para adaptadores do Broadcom NetXtreme, o teste da análise de cabo só pode ser executado para conexões de velocidade de link de gigabit e quando não houver conexão.
- Esta opção não está disponível para todos os adaptadores de rede Broadcom.

Para executar uma análise de cabo

1. Conecte o cabo à porta de um switch, onde a porta e as configurações do driver Speed & Duplex estejam definidas como **Auto**.
2. Clique no nome do adaptador a ser testado no painel Visualização Explorer.
3. Na lista **Selecione um teste a ser executado**, escolha **Análise de cabo**. Se a opção **Análise de cabo** não estiver disponível, na guia **Visualização de contexto** no lado direito da janela, selecione **Diagnóstico** e, em seguida, **Análise de cabo**.
4. Clique em **Executar**.
5. Na janela da mensagem de erro que alerta sobre a interrupção temporária da conexão de rede, clique em **Sim**.

Distância. A distância do cabo válido, em metros (exceto quando o Ruído retorna).

Status. Isso mostra o tipo de link neste par de cabos.

- **Bom.** Caminhos de sinal do PCB/cabo bons, mas sem link gigabit.
- **Cruzado.** Curto ou crosstalk de pino em dois ou mais caminhos de sinal do PCB/cabo.
- **Aberto.** Um ou os dois pinos de um par trançado estão abertos.
- **Curto.** Dois pinos do mesmo par trançado estão em curto.
- **Ruído.** Há um ruído presente (mais provavelmente provocado pelo Forced 10/100).
- **Link GB.** O link gigabit está operando.
- **N/D.** O algoritmo falhou em alcançar uma conclusão.

Link. A velocidade e o modo dúplex de conexão do link.

Status. O status após a execução do teste (Concluído ou Falhou).

Há diversos fatores que podem afetar os resultados do teste:

- **Parceiro de link.** Diversos fabricantes de switch e hub implementam diferentes PHYs. Alguns PHYs não são compatíveis com IEEE.
- **Qualidade do cabo.** Cabos de categoria 3, 4, 5 e 6 podem afetar os resultados do teste.
- **Interferência elétrica.** O ambiente de teste pode afetar os resultados do teste.

Definição das propriedades do adaptador

Avançado na guia **Configurações** permite visualizar e alterar os valores das propriedades disponíveis do adaptador selecionado. As propriedades possivelmente disponíveis e as respectivas configurações são descritas a seguir.



OBSERVAÇÕES:

- Você deve ter privilégios de administrador para alterar os valores de uma propriedade.
- A lista de propriedades disponíveis específicas para o seu adaptador pode ser diferente.
- Algumas propriedades talvez não estejam disponíveis para todos os adaptadores de rede Broadcom.

Para definir as propriedades do adaptador

1. Clique no nome do adaptador no painel Visualização Explorer e clique na guia **Configurações**.
2. Na seção **Avançado**, selecione a propriedade que você deseja definir.
3. Para alterar o valor de uma propriedade, selecione um item na lista da propriedade ou digite um novo valor, conforme apropriado (as opções de seleção são diferentes para propriedades diferentes).
4. Clique em **Aplicar** para confirmar as alterações feitas em todas as propriedades. Clique em **Redefinir** para voltar as propriedades aos valores originais.

802.1p QoS. Ativa a *qualidade de serviço*, que é uma especificação do IEEE (Institute of Electrical and Electronics Engineering) que trata dos diferentes tipos de tráfego de rede de maneiras distintas para garantir os níveis necessários de confiabilidade e latência de acordo com o tipo de tráfego. Essa propriedade é desativada por padrão. A menos que a infraestrutura de rede dê suporte a QoS, não ative essa propriedade. Caso contrário, podem ocorrer problemas.

Controle de fluxo. Ativa ou desativa o recebimento ou a transmissão de quadros PAUSE. Os quadros PAUSE permitem que o adaptador de rede e um switch controlem a taxa de transmissão. O lado que recebe o quadro PAUSE interrompe a transmissão momentaneamente.

- **Auto** (padrão). A recepção e a transmissão de quadros PAUSE são otimizadas.
- **Desativar.** A recepção e a transmissão de quadros PAUSE são desativadas.
- **Rx PAUSE.** A recepção de quadros PAUSE é ativada.
- **Rx/Tx PAUSE.** A recepção e a transmissão de quadros PAUSE são ativadas.
- **Tx PAUSE.** A transmissão de quadros PAUSE é ativada.

Speed & Duplex. A propriedade Speed & Duplex define a velocidade e o modo de conexão de acordo com os da rede. Observe que o modo Full-Duplex permite que o adaptador transmita e receba dados da rede simultaneamente.

- **10 Mb Full.** Define a velocidade como 10 Mbit/s e o modo como Full-Duplex
- **10 Mb Half.** Define a velocidade como 10 Mbit/s e o modo como Half-Duplex
- **100 Mb Full.** Define a velocidade como 100 Mbit/s e o modo como Full-Duplex.
- **100 Mb Half.** Define a velocidade como 100 Mbit/s e o modo como Half-Duplex
- **Auto** (padrão). Define a velocidade e o modo para a conexão de rede otimizada (recomendado).

**OBSERVAÇÕES:**

- Auto é a configuração recomendada. Essa configuração permite que o adaptador de rede detecte dinamicamente a velocidade de linha da rede. Sempre que a capacidade da rede muda, o adaptador de rede a detecta automaticamente e a ajusta para a nova velocidade de linha e o modo duplex. Quando a velocidade de 1 Gbps é suportada, ela pode ser ativada selecionando-se Auto.
- A definição 1 Gb Full Auto deve ser conectada a um parceiro de link que também suporte uma conexão de 1 Gb. Como a conexão é limitada a apenas uma conexão de 1 Gb, o recurso Ethernet@Wirespeed será desativado. Se o parceiro de link suportar apenas uma conexão de 1 Gb, o recurso Wake on LAN pode não funcionar. Além disso, o gerenciamento do tráfego, na ausência de um sistema operacional, também pode ser afetado.
- As definições 10 Mb Half e 100 Mb Half forçam o adaptador de rede a se conectar à rede em modo Half-Duplex. Observe que o adaptador de rede pode não funcionar se a rede não estiver configurada para operar no mesmo modo.
- As definições 10 Mb Full e 100 Mb Full forçam o adaptador de rede a se conectar à rede em modo Full-Duplex. O adaptador de rede poderá não funcionar se a rede não estiver configurada para operar no mesmo modo.

Wake Up Capabilities. Permite que o adaptador de rede saia de um modo de baixa alimentação quando recebe um quadro de ativação da rede. São possíveis dois tipos de quadros de ativação: Magic Packet e Wake Up Frame.

Essa propriedade está disponível apenas para os adaptadores do Broadcom NetXtreme.

- **Ambos** (padrão). Seleciona Magic Packet e Wake Up Frame como quadros de ativação.
- **Magic Packet.** Seleciona Magic Packet como quadro de ativação.
- **Nenhum.** Não seleciona quadros de ativação.
- **Wake Up Frame.** Seleciona Wake Up Frame como quadro de ativação e permite que o adaptador da rede ative o sistema quando eventos como o comando ping ou uma solicitação ARP (Address Resolution Protocol, Protocolo de resolução de endereços) forem recebidos. Esta opção trabalha junto com o modo de economia de energia do sistema operacional e não funciona se a configuração Economia de Energia não ativar o WOL.

Prioridade e VLAN. Permite ativar tanto a priorização do tráfego de rede quanto a marcação de VLAN. A marcação de VLAN só ocorre quando a configuração de ID de VLAN tem valor diferente de 0 (zero).

- **Prioridade e VLAN ativadas (padrão).** Permite a priorização de pacotes e a marcação de VLAN.
- **Prioridade e VLAN desativadas.** Impede a priorização de pacotes e a marcação de VLAN.
- **Prioridade Ativada.** Permite apenas a priorização de pacotes.
- **VLAN Ativada.** Permite apenas a marcação de VLAN.



Nota: Se um driver intermediário estiver gerenciando o adaptador de rede para uma marcação de VLAN, as configurações de **Prioridade e VLAN desativadas** e de **Prioridade ativada** não devem ser usadas. Use a configuração **Prioridade e VLAN ativadas** e altere o **ID de VLAN** para 0 (zero).

ID de VLAN. Ativa a marcação de VLAN e configura o ID de VLAN quando **Prioridade e VLAN ativadas** está selecionada como a configuração de **Prioridade e VLAN**. O intervalo do ID de VLAN é de 1 a 4094 e deve corresponder ao valor da marcação de VLAN na porta do switch. Um valor de 0 (padrão) nesse campo desativa a marcação de VLAN.

Avaliação de risco da marcação de VLAN pelo Driver da miniporta NDIS

O Driver da miniporta NDIS 6.0 da Broadcom permite que um sistema contendo um adaptador Broadcom conecte-se a uma VLAN marcada. Mas, diferente do BASP, o suporte do driver NDIS 6 para participação de VLAN é apenas para um ID de VLAN.

E também diferente do BASP, o driver NDIS 6.0 só fornece marcação de VLAN do pacote de saída, mas não fornece filtragem de pacotes de entrada com base na condição de membro do ID de VLAN. Esse é o comportamento padrão

para todos os drivers de miniporta. Embora a ausência de pacotes de filtragem com base na condição de membro da VLAN possa ser um problema de segurança, o seguinte fornece uma avaliação de risco baseada nessa limitação do driver para uma rede IPv4:

Uma rede adequadamente configurada que tem várias VLANs deve manter segmentos IP separados para cada VLAN. Isso é necessário, pois o tráfego de saída depende da tabela de roteamento para identificar por qual adaptador (virtual ou físico) passar o tráfego e não determina qual adaptador foi a base para os membros da VLAN.

Como o suporte para marcação de VLAN no driver NDIS 6.0 da Broadcom limita-se apenas ao tráfego de transmissão (Tx), há o risco do tráfego de recepção (Rx) de outra VLAN passar para o sistema operacional. Mas, com base na premissa acima, de uma rede adequadamente configurada, a segmentação de IP e/ou a configuração do switch da VLAN pode fornecer uma filtragem adicional para limitar o risco.

Em um cenário de conexão em ponte, dois computadores no mesmo segmento IP poderão comunicar-se independentemente de sua configuração de VLAN pois não ocorre nenhuma filtragem de membros da VLAN. Mas esse cenário supõe que a segurança pode já ter sido quebrada, pois esse tipo de conexão não é típico em um ambiente de VLAN.

Se o risco acima não for desejável e for necessária a filtragem de membros de ID da VLAN, então será necessário o suporte por meio de um driver intermediário.

Exibição de estatísticas

As informações fornecidas na guia Estatísticas permitem ver as estatísticas de tráfego dos adaptadores de rede Broadcom e dos adaptadores de rede de terceiros. As informações estatísticas e de cobertura são mais abrangentes para adaptadores Broadcom.

Para visualizar as informações de Estatísticas relativas a qualquer adaptador de rede instalado, clique no nome do adaptador listado no painel Visualização Explorer e clique na guia Estatísticas.

Clique em **Atualizar** para obter os valores mais recentes de cada estatística. Clique em **Redefinir** para mudar todos os valores para zero.



OBSERVAÇÕES:

- As estatísticas de equipe para um adaptador de rede Broadcom não serão compiladas se ele estiver desativado.
- Algumas estatísticas talvez não estejam disponíveis para todos os adaptadores de rede Broadcom.

Estatísticas gerais

Estatísticas gerais mostram as estatísticas transmitidas do adaptador e recebidas nele.

Quadros Tx OK. Uma contagem dos quadros transmitidos com êxito. Este contador será incrementado quando o status de transmissão for relatado como Transmissão OK.

Quadros Rx OK. Uma contagem dos quadros recebidos com êxito. Não inclui quadros recebidos com quadros muito longos, FCS (Frame Check Sequence, Sequência de verificação de quadros), erros de comprimento ou alinhamento ou quadros perdidos devido a erros internos de subcamada MAC. Este contador é incrementado quando o status de recebimento é relatado como Recebimento OK.

Quadros Tx direcionados. Uma contagem de quadros de dados direcionados transmitidos com êxito.

Difusão seletiva de quadros Tx. Uma contagem dos quadros transmitidos com êxito (conforme indicado pelo valor de status Transmissão OK) para um endereço de destino do grupo diferente de um endereço de transmissão.

Transmitir quadros Tx. Uma contagem de quadros transmitidos com êxito (conforme indicado pelo status Transmissão OK) para o endereço de transmissão. Quadros transmitidos para endereços de difusão seletiva não são quadros transmitidos e são excluídos.

Quadros Rx direcionados. Uma contagem de quadros de dados direcionados recebidos com êxito.

Difusão seletiva de quadros Rx. Uma contagem de quadros recebidos e direcionados com êxito para um endereço de grupo sem difusão ativa. Não inclui quadros recebidos com erros de quadros muito longos, erros FCS, erros de comprimento ou de alinhamento, nem quadros perdidos devido a erros internos de subcamada MAC. Este contador é incrementado conforme indicado pelo status Recebimento OK.

Transmitir quadros Rx. Um contador de quadros recebidos com êxito e direcionados a um endereço de grupo de transmissão. Não inclui quadros recebidos com erros de quadros muito longos, erros FCS, erros de comprimento ou alinhamento nem quadros perdidos devido a erros internos de subcamada MAC. Este contador é incrementado conforme indicado pelo status Recebimento OK.

Quadros Rx com erro CRC. O número de quadros recebidos com erros CRC.

Configuração de equipes

A função de formação de equipes permite agrupar adaptadores de rede para que funcionem como uma equipe. A formação de equipes é um método de criar um NIC virtual (um grupo de vários adaptadores que funciona como um único adaptador). A vantagem dessa abordagem é a possibilidade de permitir o equilíbrio de carga e o limite de falha. A formação de equipes é realizada por meio do software Broadcom Advanced Server Program. Para uma descrição abrangente da tecnologia e para considerações sobre implementação do software de formação de equipes, consulte a seção "Broadcom Gigabit Ethernet Teaming Services" do guia de usuário do adaptador de rede Broadcom.

A formação de equipes pode ser realizada por um dos seguintes métodos:

- [Comousar o Assistente de formação de equipes Broadcom](#)
- [Uso do Modo Inteligente](#)

**OBSERVAÇÕES:**

- Para obter mais informações relacionadas aos protocolos de formação de equipes, consulte "Formação de equipes" no guia do usuário do adaptador de rede Broadcom.
- Se o LiveLink™ não é ativado durante a configuração de equipes, a desativação do protocolo Spanning Tree no switch é recomendada. Isso minimiza o tempo de inatividade devido à determinação do loop da árvore de spanning em caso de evento de limite de falha. O LiveLink reduz tais problemas.
- O BASP fica disponível apenas se um sistema tiver um ou mais adaptadores de rede Broadcom instalados.
- As propriedades Large Send Offload (LSO) e Checksum Offload só são ativadas para uma equipe quando todos os membros suportarem e estiverem configurados para o recurso.
- Você deve ter privilégios de administrador para criar ou modificar uma equipe.
- O algoritmo de equilíbrio de carga em um ambiente de equipe nos quais os membros estão conectados em velocidades diferentes favorece os membros conectados com um link do Gigabit Ethernet sobre os membros conectados em links de velocidade menor (100 Mbps ou 10 Mbps) até que um limite seja alcançado. Este é o comportamento normal.
- Wake on LAN (WOL) é um recurso que permite que um sistema seja ativado de um estado inativo através da chegada de um pacote específico pela interface Ethernet. Como o adaptador virtual é implementado somente como dispositivo do software, ele perde os recursos de hardware para implementar WOL e não pode ser ativado para tirar o sistema de um estado inativo por meio do adaptador virtual. Os adaptadores físicos, no entanto, suportam esta propriedade, mesmo quando o adaptador é parte da equipe.

Tipos de equipe

Você pode criar quatro tipos de equipes de equilíbrio de carga:

- Smart Load Balancing e Limite de falha
- Agregação de link (802.3ad)
- Trunking genérico (FEC/GEC)/802.3ad-Draft Static
- SLB (Desativar reserva automática) - O recurso Desativar reserva automática é configurado para equipes do tipo Smart Load Balance e Limite de falha no Assistente de Equipes.

Para uma descrição destes tipo, consulte "Equilíbrio de Carga e Tolerância a Falhas" no Guia do usuário do *Broadcom® NetXtreme® BCM57XX*.

Comousar o Assistente de formação de equipes Broadcom

Você pode usar o Assistente de Formação de Equipes Broadcom para criar uma equipe, configurar uma existente, caso a equipe já tenha sido criada ou criar uma VLAN.

1. Crie ou edite uma equipe:

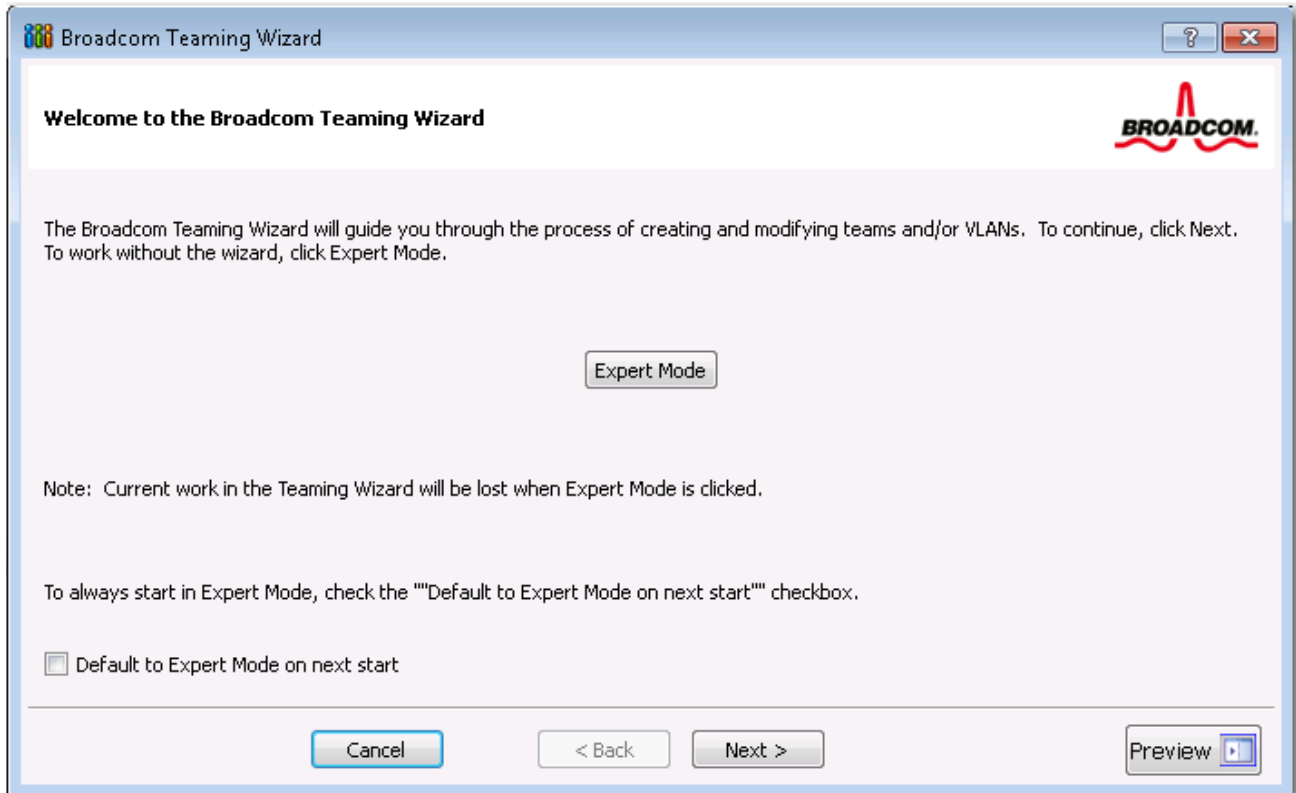
Para criar uma nova equipe, selecione **Criar uma equipe** no menu **Equipe** ou clique com o botão direito do mouse em um dos dispositivos exibidos na seção "Adaptadores não atribuídos" e selecione **Criar uma equipe**. Esta opção não estará disponível se não houver dispositivos listados na seção "Adaptadores não atribuídos", o que significa que todos os adaptadores já foram designados para equipes.

Para configurar uma equipe existente, clique com o botão direito do mouse em uma das equipes exibidas na lista e selecione **Editar equipe**. Esta opção só fica disponível se a equipe já foi criada e se está listada no painel Gerenciamento de equipes.



Nota: Se preferir trabalhar sem o assistente, clique em **Modo de especialista**. Se quiser usar sempre o Modo de especialista para criar uma equipe, selecione **O modo de especialista será o padrão na próxima inicialização**. Consulte [Uso do Modo Inteligente](#).

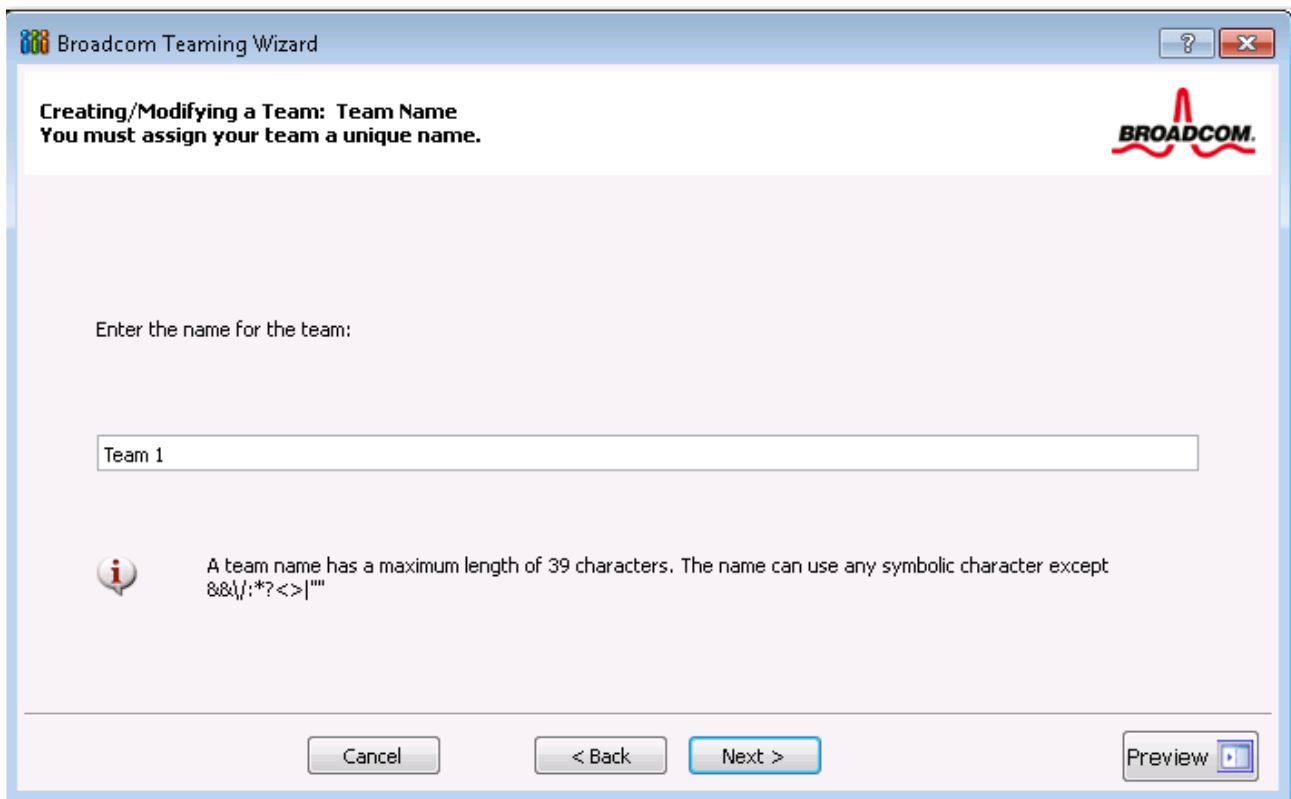
2. Para continuar usando o assistente, clique em **Avançar**.



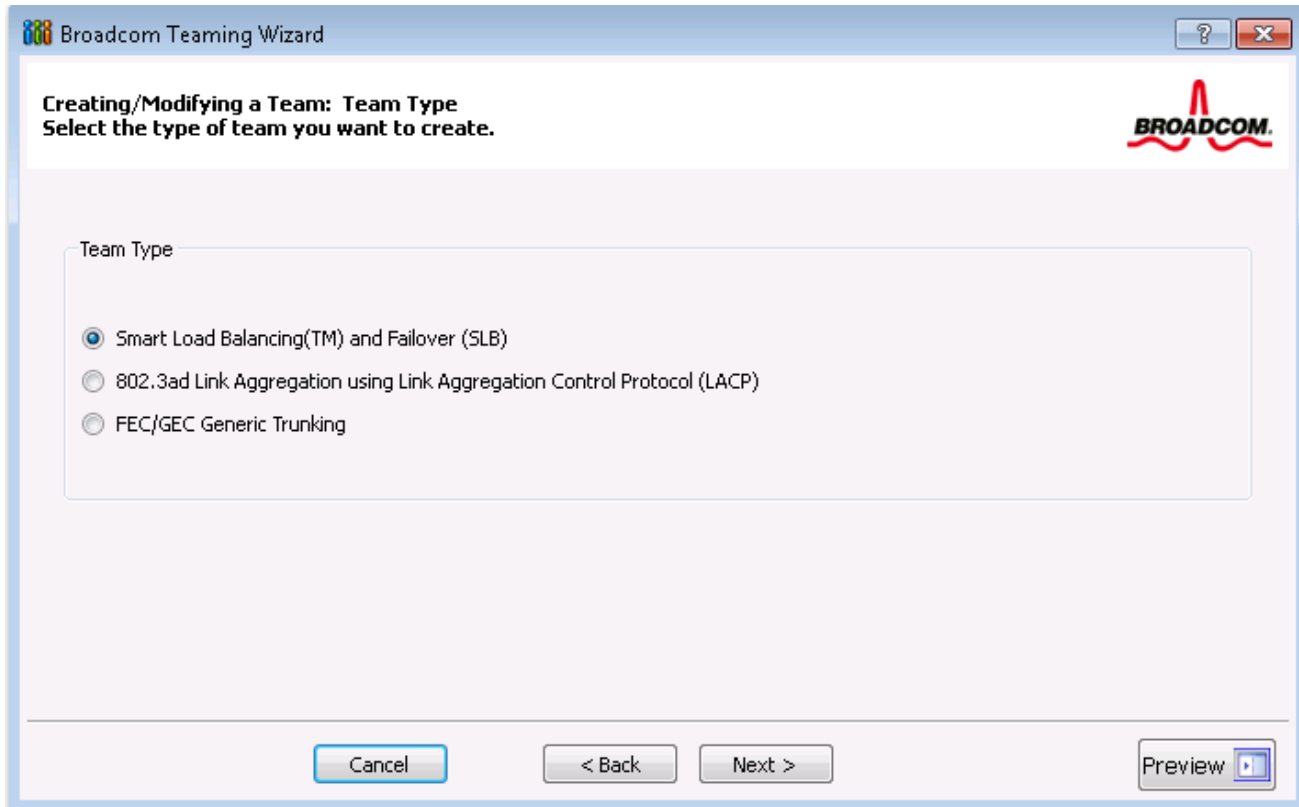
3. Digite o nome da equipe e clique em **Avançar**. Se quiser revisar ou alterar qualquer uma de suas configurações, clique em **Voltar**. Clique em **Cancelar** para descartar suas configurações e sair do assistente.



Nota: O nome da equipe não pode exceder 39 caracteres, começar com espaços e nem conter nenhum dos caracteres a seguir: & \ / : * ? < > |



4. Selecione o tipo de equipe que você deseja criar. Se o tipo de equipe for SLB, clique em **Avançar**. Se o tipo de equipe não for SLB, será exibida uma caixa de diálogo. Verifique se o switch de rede conectado aos membros da equipe está configurado corretamente para o tipo de equipe, depois clique em **OK** para continuar.



5. Na lista **Adaptadores Disponíveis**, clique no adaptador que você deseja adicionar à equipe e clique em **Adicionar**. Remova os membros da equipe da lista **Membros da equipe**, clicando no adaptador e em **Remover**. Clique em **Next (Avançar)**.

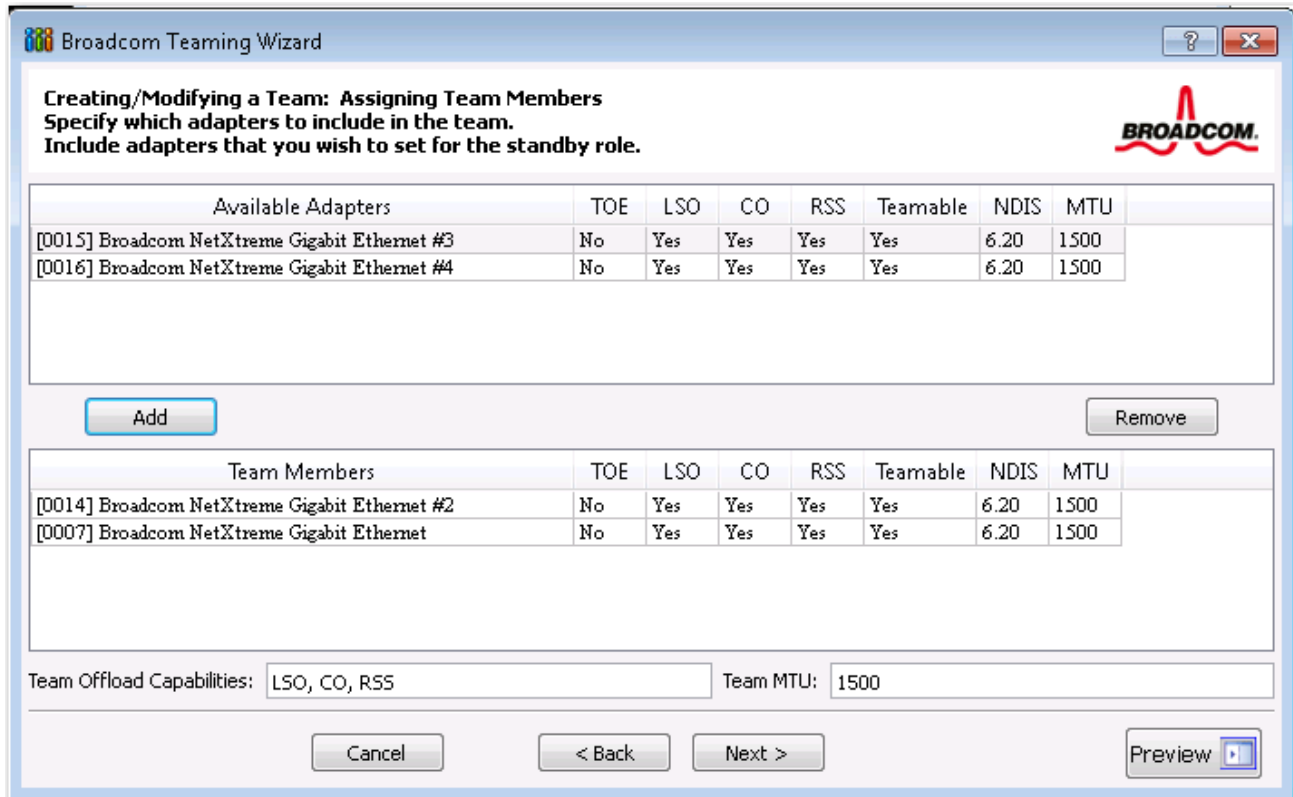


Nota: Deve haver pelo menos um adaptador de rede Broadcom atribuído à equipe.

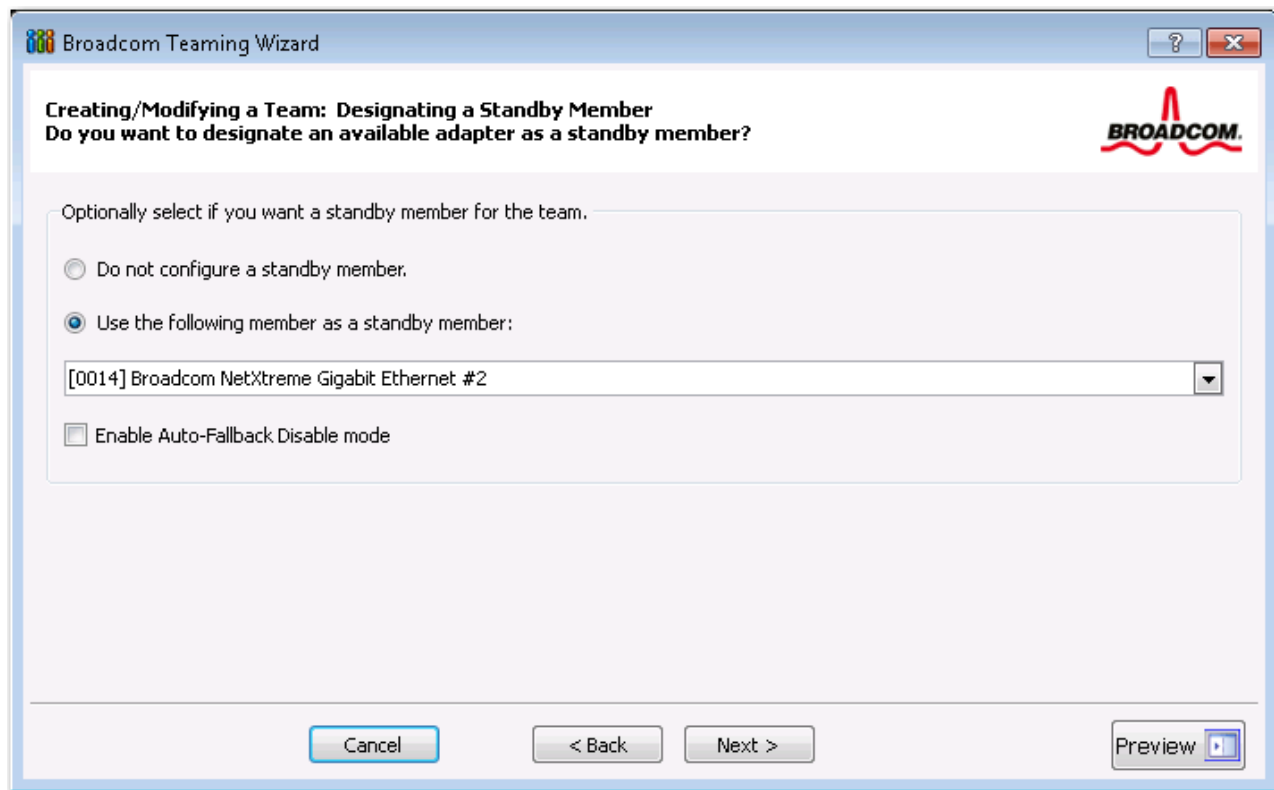
As colunas Large Send Offload (LSO) e Checksum Offload (CO) indicam se as propriedades do LSO e/ou do CO são suportadas (Y) ou não (N) para o adaptador. As propriedades LSO e CO só são ativadas para uma equipe quando todos os membros suportam e estão configurados para o recurso. Se isso ocorrer, os recursos de offload da equipe serão exibidos na parte inferior da tela.



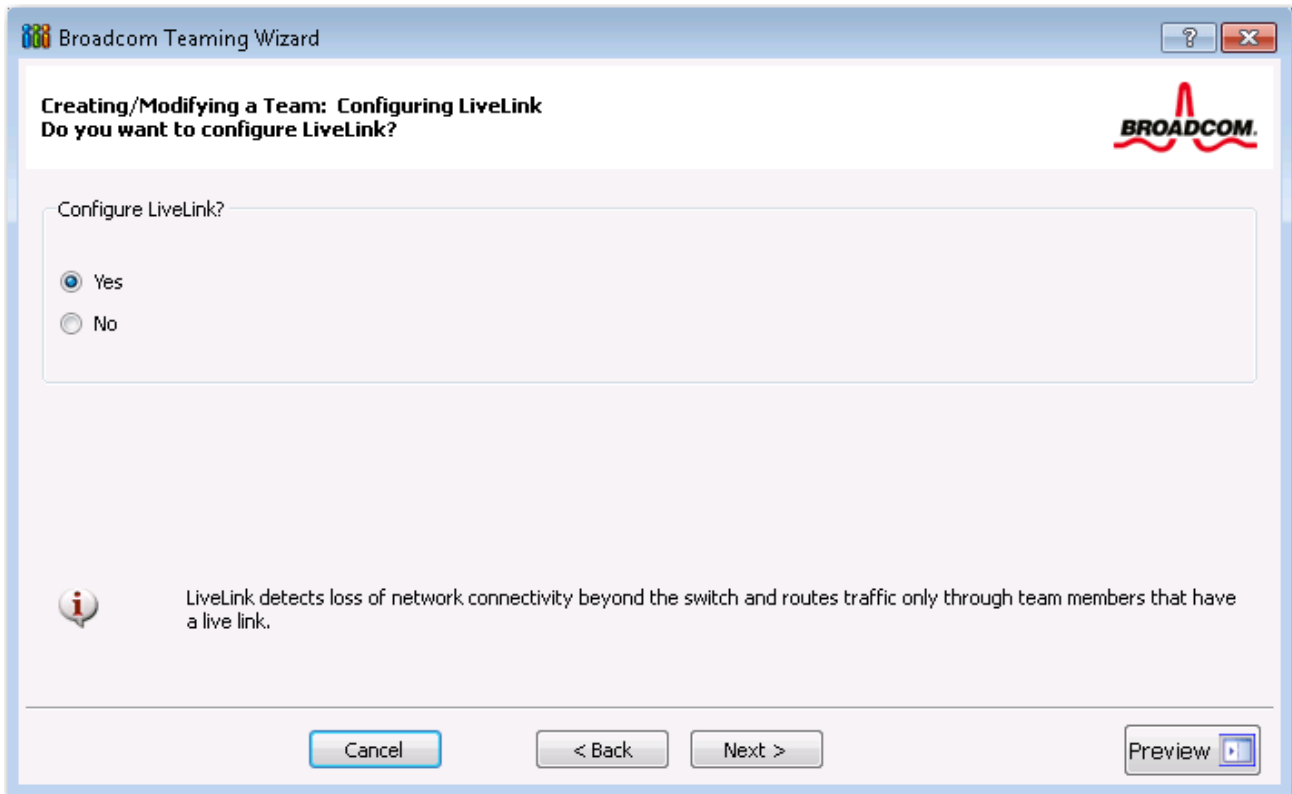
Nota: Adicionar um adaptador de rede a uma equipe quando seu driver está desativado pode afetar negativamente os recursos de descarregamento da equipe. Isso pode afetar o desempenho da equipe. Logo, recomenda-se que apenas sejam adicionados como membros da equipe os adaptadores de rede com o driver ativado.



6. Para designar um dos adaptadores como membro reserva (opcional), selecione **Usar o membro a seguir como um membro reserva** e escolha o membro em espera na lista de adaptadores.
7. O modo Desativar reserva automática permite que a equipe continue usando o membro em espera em vez de voltar para o membro primário, se o membro primário for reativado. Para ativar este recurso, selecione **Ativar modo Desativar reserva automática**. Clique em **Next (Avançar)**.



8. Para configurar o LiveLink, selecione **Sim**; caso contrário, selecione **Não** e clique em **Avançar**.



9. Selecione o intervalo de sondagem (o número de segundos entre cada retransmissão de um pacote de link para o alvo da sondagem) e o número máximo de tentativas de sondagem (o número de respostas perdidas consecutivamente de um alvo da sondagem antes de um limite de falha ser disparado).

10. Defina o ID VLAN de sondagem para permitir a conectividade com os alvos de sondagem residentes em uma VLAN marcada. O número definido deve corresponder ao ID VLAN dos alvos de sondagem e também à(s) porta(s) no switch ao qual a equipe está conectada.



Nota: Cada equipe com LiveLink ativado só pode comunicar-se com Alvos de Sondagem em uma VLAN. Além disso, o ID 0 da VLAN é equivalente a uma rede sem marca. Se o ID da VLAN de sondagem for definido com um valor diferente de 0, a VLAN deverá ser criada com um valor de marca VLAN idêntico (consulte [Etapa 16](#)).

11. Clique no alvo de sondagem na parte superior da lista, clique em **Editar Endereço IP alvo**, digite o endereço IP alvo na caixa **Endereço IP** para um ou todos os alvos de sondagem e depois clique em **OK**. Clique em **Next (Avançar)**.



Nota: Somente o primeiro alvo de sondagem é requerido. É possível especificar até três alvos de sondagem adicionais para servirem como backups, atribuindo endereços IP para outros alvos de sondagem.

12. Selecione um membro da equipe listado, clique em **Editar endereço IP do membro** e, em seguida, digite o endereço IP do membro na caixa **Endereço IP**. Repita essa ação para todos os membros da equipe e clique em **OK**. Clique em **Next (Avançar)**.



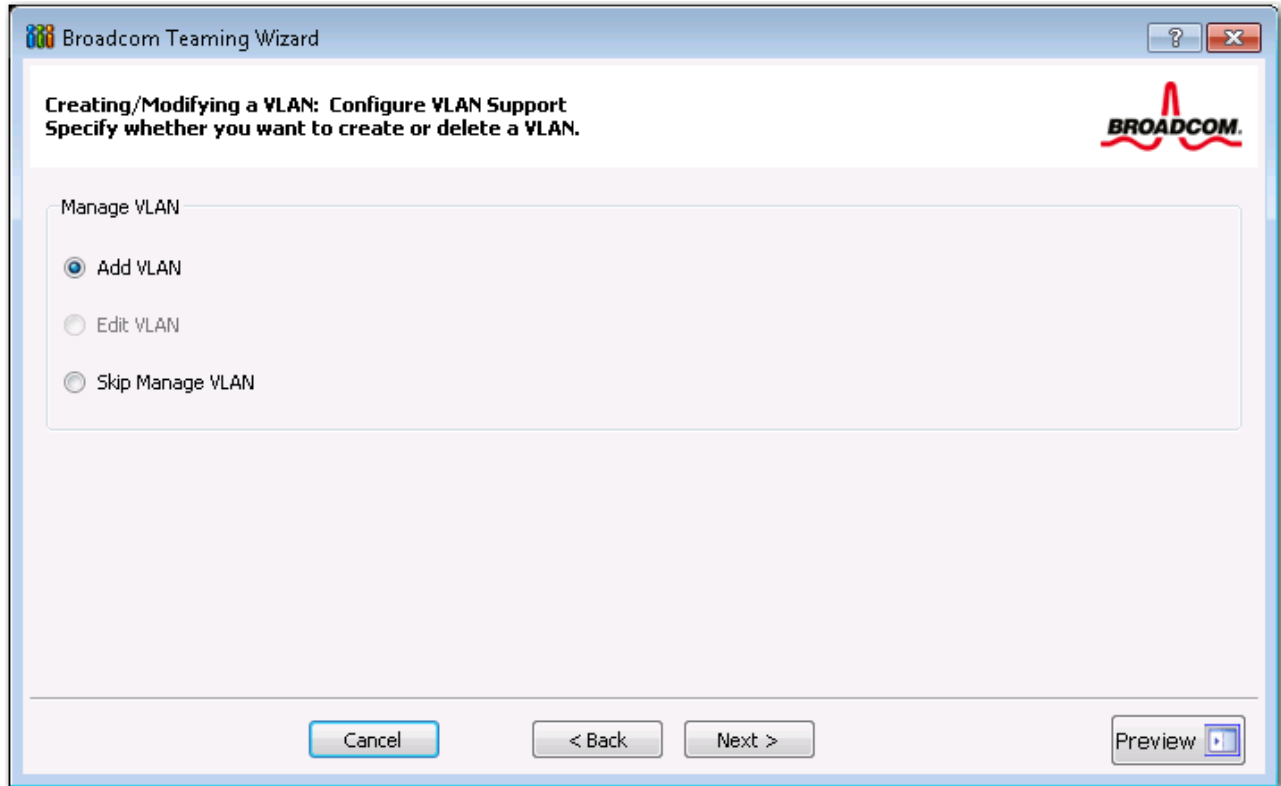
Nota: Todos os endereços IP do membro devem estar na mesma sub-rede que a sub-rede dos alvos de sondagem.

13. Para criar uma VLAN na equipe, selecione **Adicionar VLAN** ou, para alterar as configurações de uma VLAN existente, selecione **Editar VLAN** e clique em **Avançar**. Se você não quiser criar nem editar uma VLAN, selecione **Ignorar gerenciamento de VLAN**, clique em **Avançar** e prossiga com o assistente na tela Concluir (consulte [Etapa 18](#) deste procedimento).

As VLANs permitem adicionar vários adaptadores virtuais que estejam em sub-redes diferentes. A vantagem é que o sistema pode ter um adaptador de rede que pode pertencer a várias sub-redes.



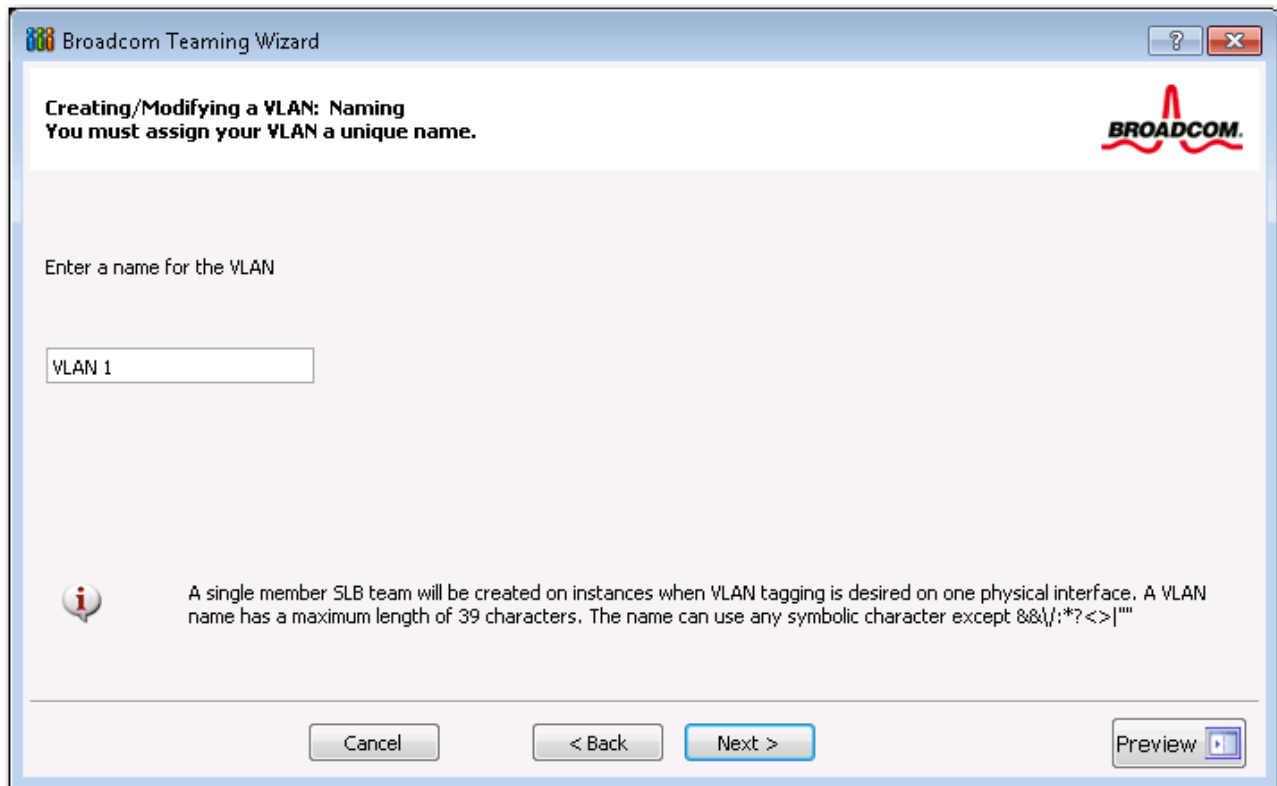
Nota: As VLANs podem ser criadas apenas quando todos os membros da equipe são adaptadores da Broadcom.



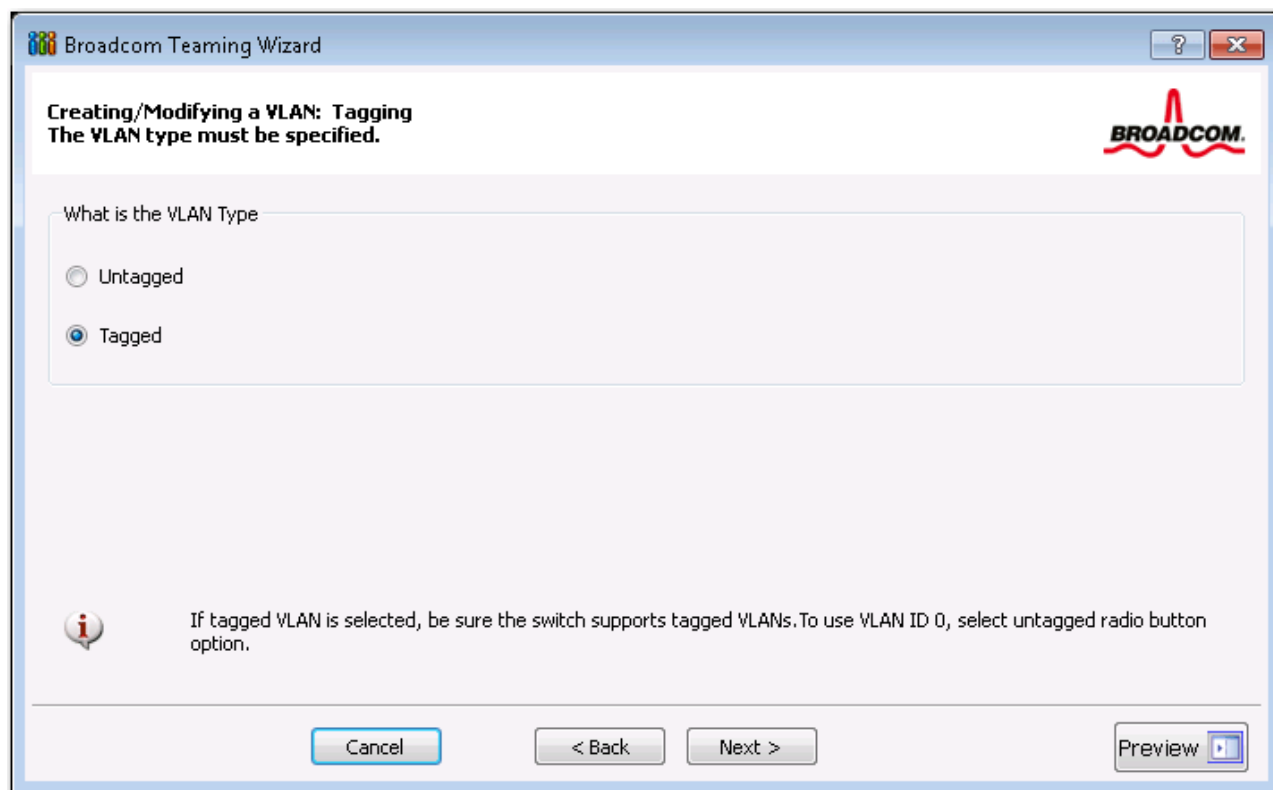
14. Digite o nome da VLAN e clique em **Avançar**.



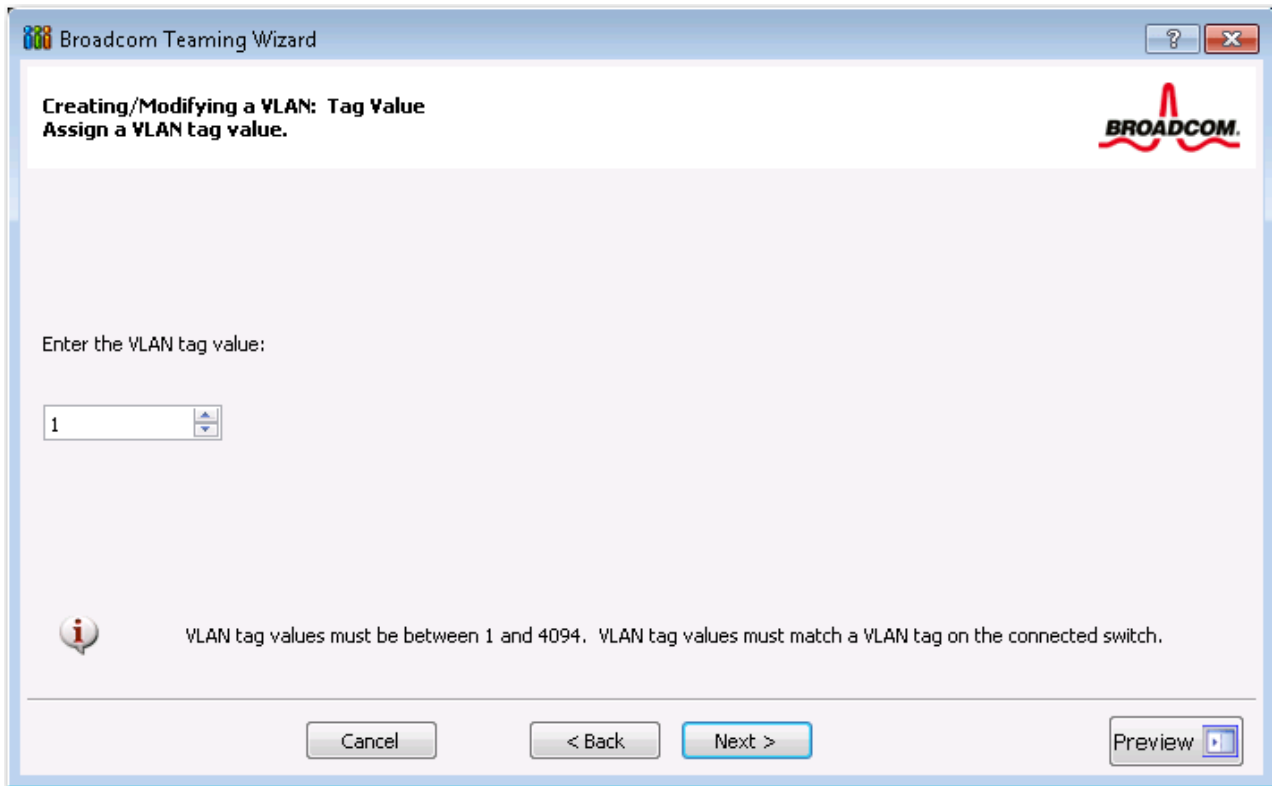
Nota: O nome da equipe não pode exceder 39 caracteres, começar com espaços e nem conter nenhum dos caracteres a seguir: & \ / : * ? < > |



15. Para marcar a VLAN, selecione **Marcada** e clique em **Avançar**. Caso contrário, clique em **Desmarcar**, clique em **Avançar** e continue no assistente para incluir VLANs adicionais (consulte a [Etapa 17](#) deste procedimento).



16. Digite o valor da marca VLAN e clique em **Avançar**. O valor deve estar entre 1 e 4094.

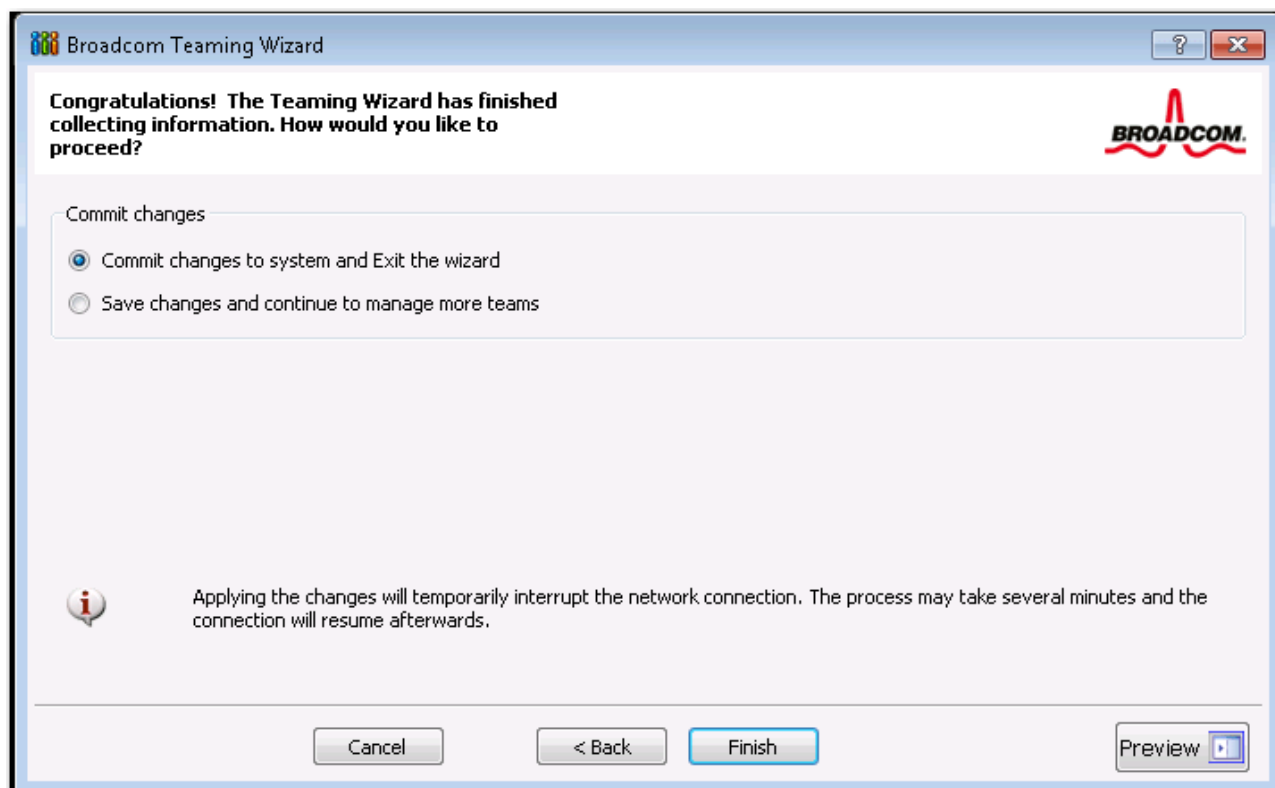


17. Selecione **Sim** para adicionar ou gerenciar outra VLAN e clique em **Avançar**. Repita o procedimento até adicionar ou gerenciar todas as VLANs necessárias.

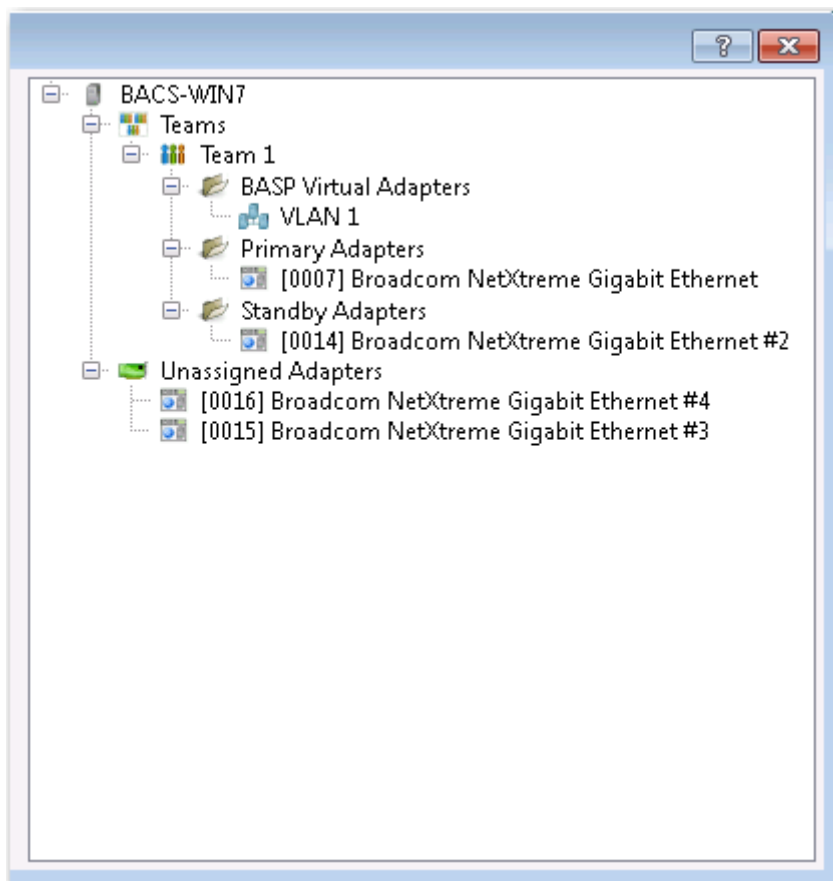


Nota: Você pode definir até 64 VLANs por equipe (63 VLANs marcadas e 1 VLAN não marcada). A adição de várias VLANs pode reduzir o tempo de reação da interface do Windows em virtude do tempo do processador e da memória de cada VLAN. A intensidade que o desempenho do Windows será afetado dependerá da configuração do sistema.

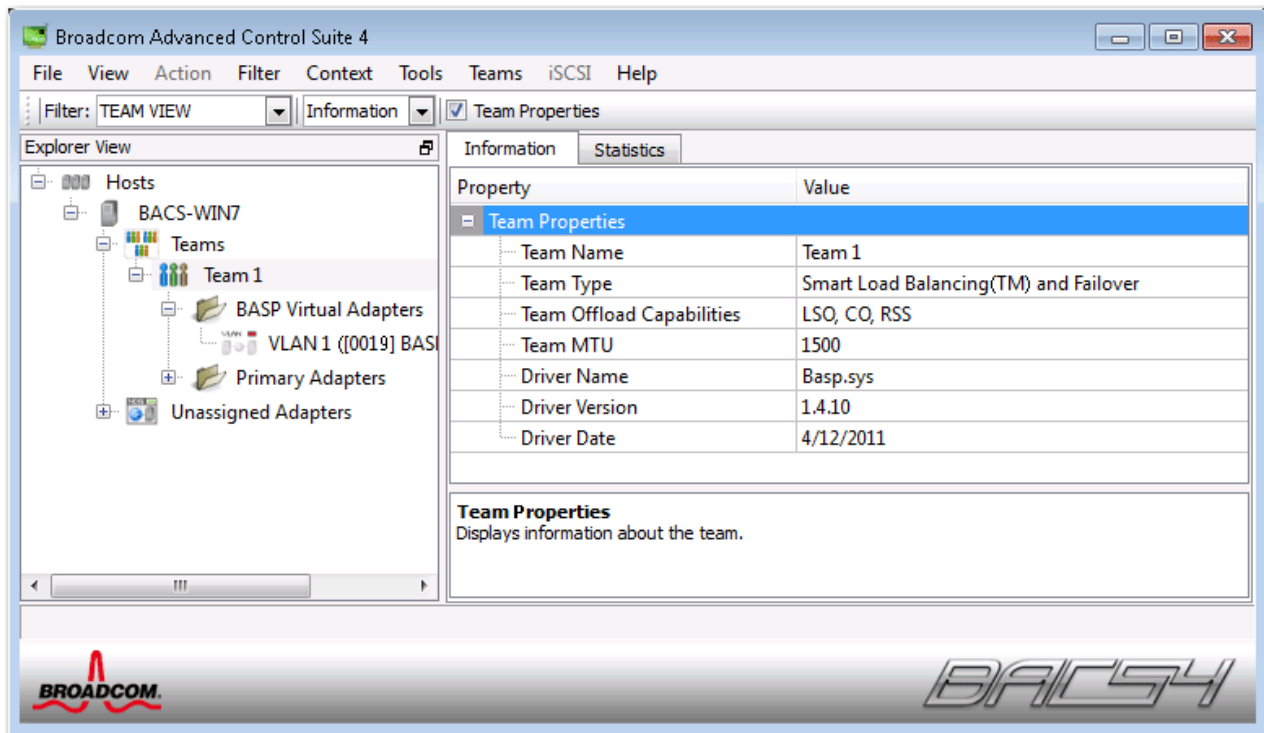
18. Para aplicar as alterações feitas na equipe, selecione **Fazer alterações no sistema e Sair do assistente**. Para aplicar as alterações e continuar usando o assistente, selecione **Salvar alterações e continuar gerenciando mais equipes**. Clique em Concluir.



Nota: A qualquer momento durante o procedimento do Assistente de Formação de Equipes do Broadcom, clique em **Visualizar** para obter uma representação visual da equipe antes de as alterações serem aplicadas.



19. No painel Gerenciamento de equipes, clique no nome da equipe para ver suas propriedades na guia **Informações**, dados de transferência e recebimento na guia **Estatísticas**.



Uso do Modo Inteligente

Use o Modo de especialista para criar e modificar uma equipe, adicionar uma VLAN e configurar o LiveLink para uma equipe Smart Load Balance e Limite de falha e SLB (Desativar reserva automática). Para criar uma equipe usando o assistente, consulte [Comousar o Assistente de formação de equipes Broadcom](#).

Para definir o Modo de formação de equipes, selecione **Opções** no menu **Ferramentas** e selecione **Modo especialista** ou **Modo do assistente** (o padrão é Modo do assistente).

Criação de uma equipe



Nota: Não é recomendável ativar o Dynamic Host Configuration Protocol (DHCP) para os membros de um tipo SLB de equipe.

1. No menu **Equipes**, selecione **Criar uma equipe** ou clique com o botão direito do mouse em um dos dispositivos da seção "Adaptadores não atribuídos" e selecione **Criar uma equipe**. Esta opção não estará disponível se não houver dispositivos listados na seção "Adaptadores não atribuídos", o que significa que todos os adaptadores já foram designados para equipes.
2. Clique em **Modo Inteligente**.



Nota: Se quiser usar sempre o Modo Inteligente para criar uma equipe, selecione **Definir Modo Inteligente na próxima inicialização**.

3. Clique na guia **Criar equipe**.

Property	Value
Team Name	Team 1
Team Type	Smart Load Balancing(TM) and Failover
Load Balance Members	<input type="checkbox"/> [0007] Broadcom NetXtreme Gigabit Ethernet <input type="checkbox"/> [0014] Broadcom NetXtreme Gigabit Ethernet #2 <input checked="" type="checkbox"/> [0015] Broadcom NetXtreme Gigabit Ethernet #3 <input checked="" type="checkbox"/> [0016] Broadcom NetXtreme Gigabit Ethernet #4
Standby Member	<not configured>
Team Offload Capabilities	LSO, CO, RSS
Team MTU	1500
VLAN Configuration	<input type="button" value="Manage VLAN(s)"/>
Enable LiveLink	<input type="checkbox"/> No

Team Name
The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any special characters.

Wizard Mode



Nota: A guia **Criar equipe** só será exibida se houver adaptadores disponíveis que possam ser agrupados em equipe.

4. Clique no campo **Nome da equipe** e digite um nome de equipe.
5. Clique no campo **Tipo de equipe** para selecionar um tipo de equipe.
6. Atribua qualquer adaptador disponível à equipe, selecionando o adaptador da lista **Membros de equilíbrio de carga**. Deve haver pelo menos um adaptador selecionado na lista **Membros de equilíbrio de carga**.
7. Você pode designar qualquer outro adaptador disponível como membro reserva; para isso, selecione-o na lista **Membro em espera**.



Nota: Deve haver pelo menos um adaptador de rede Broadcom atribuído à equipe.

A Large Send Offload (LSO), Checksum Offload (CO) e RSS indicam que as propriedades LSO, CO e/ou RSS são suportadas pela equipe. As propriedades LSO, CO e RSS só são ativadas para uma equipe quando todos os membros suportam e estão configurados para o recurso.



Nota: Adicionar um adaptador de rede a uma equipe quando seu driver está desativado pode afetar negativamente os recursos de descarregamento da equipe. Isso pode afetar o desempenho da equipe. Logo, recomenda-se que apenas sejam adicionados como membros da equipe os adaptadores de rede com o driver ativado.

8. Digite o valor da **Equipe MTU**.
9. Clique em **Criar** para salvar as informações da equipe.
10. Repita as etapas 4. a 9. para definir mais equipes. À medida que forem definidas as equipes, elas poderão ser selecionadas na lista de equipes, mas elas ainda não foram criadas. Clique na guia **Visualizar** para ver a estrutura de equipes antes de aplicar as alterações.
11. Clique em **Aplicar/Sair** para criar todas as equipes definidas e sair da janela Gerenciar equipes.
12. Clique em **Sim** quando vir a mensagem indicando que a conexão de rede será temporariamente interrompida.



OBSERVAÇÕES:

- O nome da equipe não pode exceder 39 caracteres, começar com espaços e nem conter nenhum dos caracteres a seguir: & \ / : * ? < > |
- Nomes de equipe devem ser exclusivos. Se você tentar usar um nome de equipe mais de uma vez, será exibida uma mensagem de erro indicando que o nome já existe.
- O número máximo de membros por equipe é oito.
- Quando a configuração da equipe for corretamente realizada, um driver de adaptador de equipe virtual será criado para cada equipe configurada.
- Se você desativar uma equipe virtual e desejar reativá-la posteriormente, primeiro deverá desativar e reativar todos os membros de equipe antes de reativar a equipe virtual.
- Quando você criar equipes de Trunking genérico e Agregação de link, não poderá designar um membro em espera. Os membros em espera funcionam somente com os tipos de equipe Smart Load Balancing e Limite de falha e SLB (Desativar reserva automática).
- No caso de uma equipe SLB (Desativar reserva automática), para restaurar o tráfego para os membros do equilíbrio de carga do membro em espera, clique no botão Reservar na guia Propriedades da equipe.
- Durante a configuração de uma equipe SLB, embora a conexão de membros da equipe a um hub seja suportada para teste, é recomendável conectar membros da equipe a um switch.
- Nem todos os adaptadores de rede fabricados por terceiros são suportados ou totalmente certificados para a formação de equipes.

13. Configuração do endereço IP da equipe.
 - a. No **Painel de controle**, clique duas vezes em **Conexões de rede**.
 - b. Com o botão direito do mouse, clique no nome da equipe a ser configurada e clique em **Propriedades**.
 - c. Na guia **Geral**, clique em **Protocolo da Internet (TCP/IP)** e, em seguida, em **Propriedades**.
 - d. Configure o endereço IP e qualquer outro ajuste do TCP/IP necessário para a equipe e clique em **OK** quando concluir.

Modificação de uma equipe

Depois de criar uma equipe, você pode modificá-la das seguintes formas:

- Altere o tipo de equipe
- Altere os membros atribuídos à equipe
- Adicione uma VLAN

- Modificação de uma VLAN (utilizando o Modo Inteligente)
- Remoção de uma equipe ou de uma VLAN (utilizando o Modo Inteligente).

Para modificar uma equipe

1. No menu **Equipe**, clique em **Editar equipe** ou clique com o botão direito do mouse em uma das equipes exibidas na lista e selecione **Editar equipe**. Esta opção só fica disponível se a equipe já foi criada e se está listada no painel Gerenciamento de equipes.
2. É exibida a tela Bem-vindo do assistente. Clique em **Avançar** para continuar a modificar uma equipe usando o assistente ou clique em **Modo Inteligente** para trabalhar em modo Inteligente.



Nota: A guia **Editar equipe** no Modo de especialista só é exibida se há equipes configuradas no sistema.

3. Clique na guia **Editar equipe**.

Property	Value
Team Name	Team 1
Team Type	Smart Load Balancing(TM) and Failover
Load Balance Members	<input type="checkbox"/> [0007] Broadcom NetXtreme Gigabit Ethernet <input type="checkbox"/> [0014] Broadcom NetXtreme Gigabit Ethernet #2 <input checked="" type="checkbox"/> [0015] Broadcom NetXtreme Gigabit Ethernet #3 <input checked="" type="checkbox"/> [0016] Broadcom NetXtreme Gigabit Ethernet #4
Standby Member	<not configured>
Team Offload Capabilities	
Team MTU	N/A
VLAN Configuration	
Enable LiveLink	<input type="checkbox"/> No

Team Name
The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any special characters.

4. Faça as alterações desejadas e clique em **Atualizar**. As alterações ainda não foram aplicadas; clique na guia **Visualizar** para ver a estrutura de equipes atualizada antes de aplicar as alterações.
5. Clique em **Aplicar/Sair** para aplicar as atualizações e sair da janela Gerenciar equipes.
6. Clique em **Sim** quando vir a mensagem indicando que a conexão de rede será temporariamente interrompida.

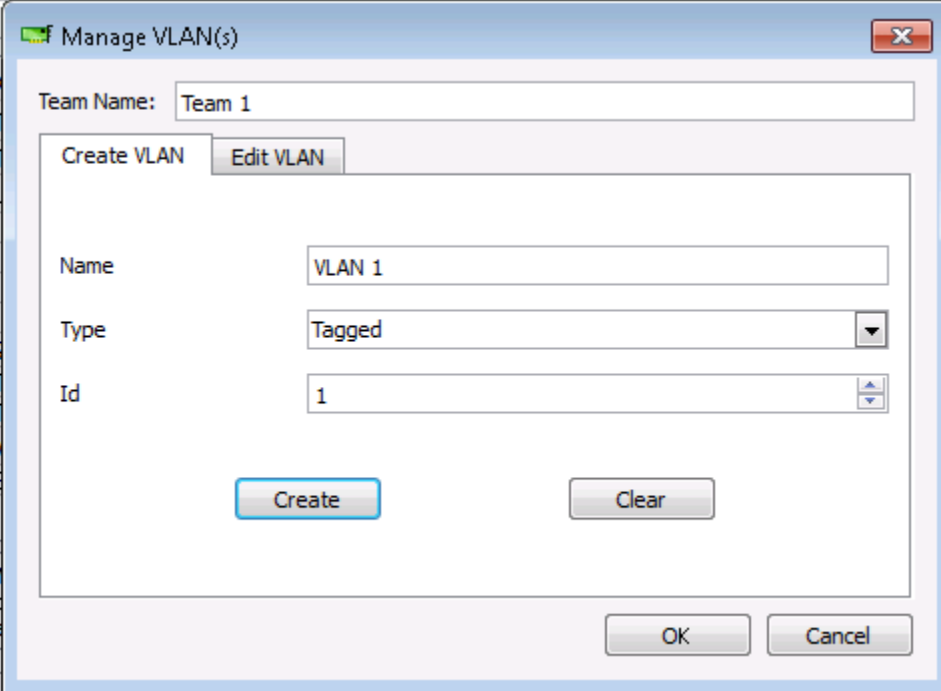
Adicionar VLAN

É possível adicionar LANs virtuais (VLANs) a uma equipe. Isso permite adicionar vários adaptadores virtuais que estejam em sub-redes diferentes. A vantagem é que o sistema pode ter um adaptador de rede que pode pertencer a várias sub-redes. Com uma VLAN, você pode combinar a funcionalidade do equilíbrio de carga dos membros de equilíbrio de carga e pode utilizar um adaptador de limite de falha.

Você pode definir até 64 VLANs por equipe (63 VLANs marcadas e 1 VLAN não marcada). As VLANs podem ser criadas apenas quando todos os membros da equipe são adaptadores da Broadcom. Se você tentar criar uma VLAN com um adaptador que não for da Broadcom, uma mensagem de erro será exibida.

Para configurar uma equipe com uma VLAN

1. No menu **Equipes**, selecione **Adicionar VLAN**.
2. É exibida a tela de Bem-vindo.
3. Clique em **Modo Inteligente**.
4. Na guia **Criar equipe** da janela **Gerenciar equipes**, clique em **Gerenciar VLAN(s)**.
5. Digite o nome da VLAN e selecione o tipo e o ID.
6. Clique em **Criar** para salvar as informações da VLAN. À medida que forem definidas as VLANs, elas poderão ser selecionadas na lista Nome da equipe, mas elas ainda não foram criadas.
7. Continue a executar esse procedimento até definir todas as VLANs desejadas e clique em **OK** para criá-las.



The image shows a software dialog box titled "Manage VLAN(s)". At the top, there is a "Team Name:" label followed by a text input field containing "Team 1". Below this, there are two tabs: "Create VLAN" (which is selected) and "Edit VLAN". Under the "Create VLAN" tab, there are three input fields: "Name" with the value "VLAN 1", "Type" with a dropdown menu set to "Tagged", and "Id" with a dropdown menu set to "1". At the bottom of the form area, there are two buttons: "Create" and "Clear". At the very bottom of the dialog box, there are "OK" and "Cancel" buttons.

8. Clique em **Sim** quando vir a mensagem indicando que a conexão de rede será temporariamente interrompida.



Nota: Para manter o desempenho ideal do adaptador, seu sistema deverá ter 64 MB de memória de sistema para cada uma das oito VLANs criadas por adaptador.

Visualização de propriedades e estatísticas de VLAN e execução de testes de VLAN

Para exibir propriedades e estatísticas de VLAN e executar testes de VLAN

1. Selecione uma das VLANs listadas.
2. Clique na guia **Informações** para visualizar as propriedades do adaptador de VLAN.
3. Clique na guia **Estatísticas** para exibir as estatísticas do adaptador de VLAN.
4. Clique na guia **Diagnóstico** para executar um teste de rede no adaptador de VLAN.

Exclusão de uma VLAN

O procedimento abaixo é aplicado quando você está no Modo Inteligente.

Para excluir uma VLAN

1. Selecione a VLAN a ser excluída.
2. No menu **Equipes**, selecione **Remover VLAN**.
3. Clique em **Aplicar**.
4. Clique em **Sim** quando vir a mensagem indicando que a conexão de rede será temporariamente interrompida.



Nota: Se você excluir uma equipe, qualquer VLAN configurada para essa equipe também será excluída.

Configuração do LiveLink para uma equipe Smart Load Balancing e Limite de falha e SLB (Desativar reserva automática)

LiveLink é um recurso do BASP que está disponível para os tipos de equipe Smart Load Balancing (SLB) e SLB (Desativar reserva automática). O objetivo do LiveLink é detectar a perda de link além do switch e rotear o tráfego apenas por meio dos membros da equipe que tenham uma conexão ativa.

Leia as notas a seguir antes de tentar configurar o LiveLink.



OBSERVAÇÕES:

- Antes de começar a configurar o LiveLink™, revise a descrição do LiveLink. Verifique também se cada alvo de sondagem que planeja especificar está disponível e funcionando. Se o endereço IP do alvo de sondagem for alterado por qualquer razão, o LiveLink deve ser reconfigurado. Se o endereço MAC do alvo de sondagem for alterado por qualquer razão, é necessário reiniciar a equipe (consulte "Solução de problemas").
- Um alvo de sondagem deve estar na mesma sub-rede que a equipe, ter um endereço IP válido e designado de modo estático (não um broadcast, multicast ou unicast), e estar altamente disponível (sempre ativado).
- Para garantir a conectividade da rede com o alvo de sondagem, utilize o comando ping para o alvo de sondagem da equipe.
- Você pode especificar até quatro alvos de sondagem.
- O endereço IP atribuído a um alvo de sondagem ou membro da equipe não pode ter um zero como primeiro ou último octeto.

Para configurar o LiveLink

1. No menu **Equipes**, selecione **Editar equipe**.
2. Clique em Modo de especialista (para configurar o LiveLink usando o Assistente de formação de equipes, consulte [Comousar o Assistente de formação de equipes Broadcom](#)).
3. Na janela Gerenciar membros, clique na guia **Editar equipe**.
4. Selecione **Ativar LiveLink**. As opções de Configuração de LiveLink são exibidas abaixo.
5. É recomendável aceitar os valores padrão para o **Intervalo de sondagem** (o número de segundos entre cada retransmissão de um pacote de link para o alvo de sondagem) e **Máximo de tentativas por sondagem** (o número de respostas perdidas consecutivamente de um alvo de sondagem antes que um limite de falha seja disparado). Para especificar valores diferentes, clique no intervalo de sondagem desejado na lista **Intervalo de sondagem (segundos)** e clique no número máximo desejado de tentativas de sondagem na lista **Máximo de tentativas por sondagem**.
6. Defina um **ID da VLAN de sondagem** que corresponda à VLAN onde se encontram os alvos de sondagem. Isso fará com que a marcação de VLAN apropriada seja aplicada ao pacote de link, com base na configuração de compartilhamento das portas do switch conectadas.



Nota: Cada equipe com LiveLink ativado só pode comunicar-se com Alvos de Sondagem em uma VLAN. Além disso, o ID 0 da VLAN é equivalente a uma rede sem marca.

7. Selecione **Alvo de sondagem 1** e digite o endereço IP de destino de um ou de todos os alvos de sondagem.



Nota: Somente o primeiro alvo de sondagem é requerido. É possível especificar até três alvos de sondagem adicionais para servirem como backups, atribuindo endereços IP para outros alvos de sondagem

8. Selecione um dos membros de equipe listados e digite o respectivo endereço IP.



Nota: Todos os endereços IP do membro devem estar na mesma sub-rede dos alvos de sondagem.

9. Clique em **Atualizar**. Repita essas etapas para cada um dos outros membros da equipe listados.
10. Clique em **Aplicar/Sair**.

Salvamento e restauração de uma configuração

Para salvar uma configuração

1. No menu **Arquivo**, selecione **Salvar equipe como**.
2. Digite o *caminho e o nome do novo arquivo de configuração* e clique em **Salvar** (uma extensão .bcg é adicionada).
O arquivo de configuração é um arquivo de texto que pode ser exibido por qualquer editor de texto. O arquivo contém informações sobre o adaptador e as configurações da equipe.

Para restaurar uma configuração

1. No menu **Arquivo**, clique em **Restaurar equipe**.
2. Clique no nome do arquivo a ser restaurado e, em seguida, clique em **Abrir**.



Nota: Se necessário, navegue para a pasta em que o arquivo está localizado.

3. Clique em **Aplicar**.
4. Clique em **Sim** quando vir a mensagem indicando que a conexão de rede será temporariamente interrompida.
5. Se uma configuração já estiver carregada, uma mensagem será exibida perguntando se você deseja salvar a configuração atual. Clique em **Sim** para salvar a configuração atual. Caso contrário, os dados de configuração carregados no momento são perdidos.



Nota: A equipe pode demorar muito tempo para armazenar caso esteja configurada com várias VLANs e um endereço IP estático.

Exibição das estatísticas do BASP

A seção Estatísticas mostra informações de desempenho dos adaptadores de rede de uma equipe.

Para exibir informações de Estatísticas do BASP relativas a qualquer adaptador membro da equipe ou da equipe como um todo, clique no nome do adaptador ou da equipe listado no painel Gerenciamento de equipes e, em seguida, clique na guia **Estatísticas**.

Clique em **Atualizar** para obter os valores mais recentes de cada estatística. Clique em **Redefinir** para mudar todos os valores para zero.

Tx. Pacote. Este é o número de pacotes transmitidos.

Tx. Pacote descartado. Este é o número de pacotes descartados.

Tx. Pacote enfileirado. Este é o número de pacotes enfileirados.

Rx. Pacote. Este é o número de pacotes recebidos.

Rx. Pacote descartado. Este é o número de pacotes descartados.

Sondagens repetidas. Este é o número de respostas perdidas consecutivamente de um alvo de sondagem antes de um limite de falha ser disparado.

Configuração com o utilitário de interface da linha de comando

Um método alternativo ao BACS para configurar adaptadores de rede Broadcom é o BACSCLI, que é um utilitário da Broadcom que permite visualizar informações e configurar adaptadores de rede usando um console no modo de interface de linha de comando não-interativo (CLI) ou no modo interativo. Assim como o BACS, o BACSCLI fornece informações sobre cada adaptador de rede e permite executar testes detalhados, efetuar diagnósticos, visualizar estatísticas e modificar valores de propriedades. O BACSCLI também permite agrupar adaptadores de rede para o equilíbrio de carga e limite de falhas.

Consulte a lista completa dos comandos disponíveis e exemplos, consulte o arquivo de texto ReadMe do BACSCLI no CD fornecido pela Dell.

Em um sistema com adaptadores de rede NetXtreme I e NetXtreme II da Broadcom, o BACSCLI é instalado quando o BACS é instalado com o programa de instalação.

Solução de problemas do BACS

Problema: Ao tentar abrir o BACS em um sistema Linux, a seguinte mensagem de erro é exibida:

"Outra instância do cliente BACS parece estar sendo executada neste sistema. Apenas uma instância do cliente BACS pode ser executada de cada vez. Caso você tenha certeza de que nenhum outro cliente BACS está em execução, uma instância anterior deve ter sido encerrada inesperadamente."

Solução: Esta mensagem será exibida se você tentar executar uma segunda instância do BACS. Caso você receba esta mensagem, mas tenha certeza de que nenhuma outra instância do BACS está em execução, uma instância anterior do BACS deve ter sido encerrada inesperadamente. Para limpar essa instância, remova o arquivo `"/dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0}"`.

Seção 14: Especificações

- [Especificações de cabos 10/100/1000BASE-T](#)
- [Especificações de desempenho](#)

Especificações de cabos 10/100/1000BASE-T

Tabela 22. Especificações de cabos 10/100/1000BASE-T

Tipo de porta	Conector	Mídia	Distância máxima
10BASE-T	RJ-45	Pares trançados não blindados de categoria 3, 4 ou 5 (UTP)	100m (328 pés)
100/1000BASE-T ¹	RJ-45	UTP Categoria 5 ²	100m (328 pés)

¹A sinalização 1000BASE-T requer quatro pares trançados de cabos balanceados da Categoria 5, conforme especificado nas normas ISO/IEC 11801:1995 e ANSI/EIA/TIA-568-A (1995), testados quanto ao desempenho adicional, usando os procedimentos de teste definidos na norma TIA/EIA TSB95.

²A Categoria 5 é o requisito mínimo. As Categorias 5e e 6 são totalmente suportadas.

Especificações de desempenho

Tabela 23. Especificações de desempenho

Recurso	Especificação
Controladores do tipo PCI Express™ (Controladores BCM57XX)	
Interface PCI Express	Largura de link x1, x2, x4
Largura de banda agregada PCI Express (transmissão e recepção)	2,5 Gbps ou 5,0 Gbps
10/100/1000BASE-T	10/100/1000 Mbps (full-duplex)

Seção 15: Informações regulamentares

- [Aviso de Classe B da FCC](#)
- [Aviso de Classe B do VCCI](#)
- [Aviso da CE](#)
- [Informações regulamentares do Canadá \(somente para o Canadá\)](#)
- [Aviso da MIC \(somente para a República da Coreia\)](#)
- [BSMI](#)

Aviso de Classe B da FCC

Broadcom NetXtreme Gigabit Ethernet Controller
BCM95721A211
BCM95722A2202

Este dispositivo está em conformidade com a Parte 15 das Regras da FCC. Sua operação está sujeita a estas duas condições: (1) este dispositivo não pode provocar interferência prejudicial e (2) este dispositivo deve aceitar qualquer interferência recebida, inclusive interferência que possa provocar operação indesejada.

O equipamento foi testado e considerado em conformidade com os limites para um dispositivo digital da Classe B, de acordo com a Parte 15 das Regras da FCC. Esses limites foram projetados para proporcionar proteção razoável contra interferência prejudicial em uma instalação residencial. O equipamento gera, utiliza e pode irradiar energia de frequência de rádio. Se não for instalado e utilizado em conformidade com as instruções, o equipamento poderá provocar interferência prejudicial nas comunicações de rádio. Entretanto, não há garantias de que a interferência não ocorrerá em uma instalação específica. Se o equipamento provocar interferência prejudicial na recepção de rádio ou televisão (o que pode ser determinado ao se ligar e desligar o equipamento), o usuário será encorajado a tentar corrigir a interferência executando uma ou mais das ações a seguir:

- Reorientar ou recolocar a antena receptora.
- Aumentar a separação entre o equipamento e o receptor.
- Conectar o equipamento a uma tomada de um circuito diferente daquele no qual o receptor está conectado.
- Consultar o revendedor ou um técnico experiente de rádio/TV para obter assistência.

Não faça modificações mecânicas ou elétricas no equipamento.



Nota: Se você alterar ou modificar este adaptador sem a permissão da Broadcom, poderá anular sua autoridade para a operação do equipamento.

Broadcom Corporation
190 Mathilda Place
Sunnyvale, California 94086 USA

Aviso de Classe B do VCCI

O equipamento é um produto Classe B baseado na norma do Voluntary Control Council for Interference from Information Technology Equipment (VCCI). Se o equipamento for usado próximo a um receptor de rádio ou televisão em um ambiente doméstico, poderá interferir na recepção de rádio. Instale e use o equipamento de acordo com o manual de instruções.



Cuidado! Existe a possibilidade de que o equipamento seja danificado na presença de energia de frequência de rádio conduzida na faixa de frequência de 59 a 66 MHz. A operação normal é reiniciada ao ser removida a fonte de energia RF.

Declaração VCCI Classe B (Japão)

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 da CE

BЪЛГАРСКИ Bulgarian	<p>Този продукт отговаря на 2006/95/EC (Нисковолтова директива), 2004/108/EC (Директива за електромагнитна съвместимост) и измененията на Европейския съюз.</p> <p>Европейски съюз, Клас B</p> <p>Това устройство на Broadcom е класифицирано за използване в типичната за Клас B жилищна среда.</p> <p>Изготвена е "Декларация за съответствие" според горепосочените директиви и стандарти, която се съхранява в Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
ČESKY Czech	<p>Bylo ustanoveno, že tento produkt splňuje směrnici 2006/95/EC (nízkonapěťová směrnice), směrnici 2004/108/EC (směrnice EMC) a dodatky Evropské unie.</p> <p>Evropská unie, třída B</p> <p>Toto zařízení společnosti Broadcom je klasifikováno pro použití v obvyklém prostředí domácnosti (třída B).</p> <p>„Prohlášení o shodě“ v souladu s výše uvedenými směrnici a normami bylo zpracováno a je uloženo v archívu společnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
Danish	<p>Denne produkt er fundet i overensstemmelse med 2006/95/EC (Lavvoltage-direktivet), 2004/108/EC (EMC-direktivet) og den Europæiske Unions ændringer.</p> <p>Den Europæiske Union, Klasse B</p> <p>Denne Broadcom-enhed er klassificeret til anvendelse i et typisk Klasse B-hjemligt miljø.</p> <p>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.</p>
NEDERLANDS Dutch	<p>Dit product is in overeenstemming bevonden met 2006/95/EC (Laagspanningsrichtlijn), 2004/108/EC (EMC-richtlijn) en amendementen van de Europese Unie.</p> <p>Europese Unie/Klasse B</p> <p>Dit Broadcom-apparaat is geclassificeerd voor gebruik in een typische klasse B woonomgeving.</p> <p>Een "Verklaring van conformiteit" in overeenstemming met de voornoemde richtlijnen en standaarden is beschikbaar bij Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
English	<p>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.</p> <p>European Union, Class B</p> <p>This Broadcom device is classified for use in a typical Class B domestic environment.</p> <p>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.</p>
EESTLANE Estonian	<p>Antud toode vastab direktiividele 2006/95/EU (Madalpinge direktiiv), 2004/108/EU (EMC direktiiv) ja ELi parandustele.</p> <p>Euroopa Liit, Klass B</p> <p>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 Mathilda Place, Sunnyvale, California 94086, USA.</p>
Finnish	<p>Tämä tuote täyttää Euroopan unionin direktiivin 2006/95/EY (pienjännittdirektiivi) ja direktiivin 2004/108/EY (sähkömagneettisesta yhteensopivuudesta annettu direktiivi), sellaisina kuin ne ovat muutettuina, vaatimuksat.</p> <p>Euroopan unioni, luokka B</p> <p>Tämä Broadcom-laite on luokiteltu käytettäväksi tyypillisessä luokan B kotiympäristössä.</p> <p>Yllä mainittujen direktiivien ja standardien mukainen vaatimustenmukaisuusvakuutus on tehty, ja sitä säilyttää Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
FRANÇAIS French	<p>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.</p> <p>Union européenne, classe B</p> <p>Cet appareil Broadcom est classé pour une utilisation dans un environnement résidentiel classique (classe B).</p> <p>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.</p>

DEUTSCH German	<p>Es ist befunden worden, dass dieses Produkt in Übereinstimmung mit 2006/95/EC (Niederspannungs-Richtlinie), 2004/108/EC (EMV-Richtlinie) und Ergänzungen der Europäischen Union steht.</p> <p>Europäische Union, Klasse B Dieses Gerät von Broadcom ist für die Verwendung in einer typisch häuslichen Umgebung der Klasse B vorgesehen.</p> <p>Eine Konformitätserklärung in Übereinstimmung mit den oben angeführten Normen ist abgegeben worden und kann bei Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
ΕΛΛΗΝΙΚΟΣ Greek	<p>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.</p> <p>Ευρωπαϊκή Ένωση, Κατηγορία Β Αυτή η συσκευή Broadcom είναι κατάλληλη για χρήση σε ένα σύνθετες οικιακό περιβάλλον κατηγορίας Β.</p> <p>Μία «Δήλωση Συμμόρφωσης» σύμφωνα με τις προηγούμενες οδηγίες και πρότυπα υπάρχει και είναι αρχαιοθετημένη στο Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
MAGYAR Hungarian	<p>A termék megfelel a 2006/95/EGK (alacsony feszültségű eszközökre vonatkozó irányelv), a 2004/108/EGK (EMC irányelv) és az Európai Unió ajánlásainak.</p> <p>Európai Unió, „B” osztály Ez a Broadcom eszköz „B” osztályú besorolást kapott, tipikus lakossági környezetben való használatra alkalmas.</p> <p>Az előbbiekben ismertetett irányelvek és szabványok szellemében „Megfelelőségi nyilatkozat” készült, amely az irországi Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
PORTUGUES Iberian Portuguese	<p>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.</p> <p>União Europeia, Classe B Este dispositivo Broadcom está classificado para utilização num ambiente doméstico típico Classe B.</p> <p>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.</p>
ITALIANO Italian	<p>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.</p> <p>Unione Europea, Classe B Il presente dispositivo Broadcom è classificato per l'uso nel tipico ambiente domestico di Classe B.</p> <p>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.</p>
LATVISKS Latvian	<p>Sis izstrādājums atbilst direktīvām 2006/95/EK (Direktīva par zemsprieguma iekārtām), 2004/108/EK (Direktīva par elektromagnētisko saderību) un to labojumiem Eiropas Savienības ietvaros.</p> <p>Eiropas Savienība, klase B Šī firmas Broadcom ražotā ierīce ir atzīta par derīgu darbam B klasei atbilstošos mājas apstākļos.</p> <p>“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.</p>
Lithuanian	<p>Buvo nustatyta, kad šis produktas atitinka direktyvą 73/23/EEB (žemos įtampos direktyvą), 89/336/EEB (elektromagnetinio suderinamumo direktyvą) ir Europos Sąjungos pataisas.</p> <p>Europos Sąjunga, B klasė Šis „Broadcom“ prietaisas yra klasifikuotas naudoti įprastose B klasės gyvenamosiose aplinkose.</p> <p>Atitikties deklaracija pagal visas galiojančias direktyvas ir standartus yra sudaryta ir saugoma įrašyta failė Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>

Maltese	<p>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.</p> <p>Unjoni Ewropea, Klassi B</p> <p>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.</p>
POLSKI Polish	<p>Niniejszy produkt został określony jako zgodny z dyrektywą niskonapięciową 2006/95/WE i dyrektywą zgodności elektromagnetycznej 2004/108/WE oraz poprawkami do nich.</p> <p>Unia Europejska, klasa B</p> <p>Niniejsze urządzenie firmy Broadcom zostało zakwalifikowane do klasy B, do użytku w typowych środowiskach domowych.</p> <p>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.</p>
ROMAN Romanian	<p>S-a stabilit că acest produs respectă cerințele Directivei 2006/95/CE privind echipamentele de joasă tensiune, ale Directivei 2004/108/CE (Directiva EMC) privind compatibilitatea electromagnetică și ale amendamentelor Uniunii Europene.</p> <p>Uniunea Europeană, Clasa B</p> <p>Acest echipament Broadcom este clasificat pentru utilizare într-un mediu casnic tipic de Clasă B. Conform directivei și standardelor de mai sus, a fost emisă o „Declarație de Conformitate”, arhivată la sediul Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
SLOVENSKY Slovakian	<p>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.</p> <p>Európska únia, Trieda B</p> <p>Toto zariadenie Broadcom triedy B je určené pre domáce prostredie.</p> <p>„Vyhlasenie o zhode“ vydané v súlade s predchádzajúcimi smernicami a štandardmi sa nachádza v spoločnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>
Slovenian	<p>Ta izdelek je v skladu z 2006/95/ES (Direktiva o nizki napetosti), 2004/108/ES (Direktiva o elektromagnetni združljivosti) in dopolnili Evropske unije.</p> <p>Evropska unija, razred B</p> <p>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.</p>
ESPAÑOL Spanish	<p>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.</p> <p>Unión Europea, Clase B</p> <p>Este dispositivo Broadcom está clasificado para ser utilizado en un entorno doméstico convencional de Clase B.</p> <p>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.</p>
SVENSK Swedish	<p>Denna produkt överensstämmer med EU-direktivet 2006/95/EC (lågspänningsdirektivet), 2004/108/EC (EMC direktivet), och andra ändringar enligt den Europeiska unionen.</p> <p>Europeiska unionen, klass B</p> <p>Den här Broadcom-enheten är klassificerad för användning i vanlig klass B-bostadsmiljö.</p> <p>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.</p>
TURK Turkish	<p>Bu ürünün 2006/95/EC (Düşük Voltaj Direktifi), 2004/108/EC (EMC Direktifi), ve Avrupa Birliği'nin ilavelerine uygun olduğu belirlenmiştir.</p> <p>Avrupa Birliği B Sınıfı</p> <p>Bu Broadcom cihazı, tipik bir B sınıfı, ev içi ortamda kullanılmak üzere sınıflandırılmıştır. Yukarıda belirtilen direktifler ve standartlara uygun olarak, bir "Uygunluk Beyanı" hazırlanmıştır, ve Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>

Informações regulamentares do Canadá (somente para o Canadá)

Industry Canada, Classe B

Este aparelho digital de Classe B está em conformidade com a especificação canadense ICES-003.

Aviso: a norma Industry Canada determina que alterações ou modificações não expressamente aprovadas pela Broadcom podem anular sua permissão para operar este equipamento.

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 da MIC (somente para a República da Coreia)

Dispositivo da CLASSE B

Broadcom NetXtreme Gigabit Ethernet Controller
 BCM95721A211
 BCM95722A2202

기종별	사용자안내문
B급 기기 (가정용)	이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다.



1. 기기의 명칭(모델명) : BCM95721A211
2. 인증번호 : E-G021-04-2613(B)
3. 인증받은 자의 상호 : Broadcom
4. 제조년월일 : 5/12/2004
5. 제조자/제조국가 : Foxconn/China



1. 기기의 명칭(모델명) : BCM95722A2202G
2. 인증번호 : BCM-BCM95722A2202G (B)
3. 인증받은 자의 상호 : BROADCOM
4. 제조년월일 : 04/30/2007
5. 제조자/제조국가 : Foxconn/China

Observe que este dispositivo foi aprovado para fins não comerciais e pode ser utilizado em qualquer ambiente, incluindo áreas residenciais.

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）劃分為乙類數位裝置。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，即表示您的系統為甲類數位裝置。如果只有 BSMI 的檢磁號碼標籤，則表示您的系統為乙類數位裝置。

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。這些限制的目的是為了在住宅區安裝時，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。

Seção 16: Etapas da solução de problemas

- [Diagnósticos de hardware](#)
- [Lista de verificação de solução de problemas](#)
- [Verificação do link e atividade da rede](#)
- [Verificação dos drivers atuais para determinar se estão carregados](#)
- [Execução de um teste do comprimento do cabo](#)
- [Teste da conectividade de rede](#)
- [Broadcom Boot Agent](#)
- [Broadcom Advanced Server Program \(BASP\)](#)
- [Depuração de Kernel sobre Ethernet](#)
- [Diversos](#)

Diagnósticos de hardware

Os testes de diagnóstico de loopback estão disponíveis para testar o hardware do adaptador. Esses testes fornecem acesso aos diagnósticos internos/externos do adaptador, onde as informações de pacotes são transmitidas pelo link físico. Para ambientes do Windows, consulte [Execução de testes de diagnóstico](#).

Falha no teste de diagnóstico BACS

Se algum dos testes descritos a seguir falhar durante a execução dos testes de diagnóstico a partir da guia [Execução de testes de diagnóstico](#) do BACS, isso pode indicar um problema de hardware no NIC ou LOM instalado no sistema.

- Registradores de controle
- Registros MII
- EEPROM
- Memória interna
- CPU On Chip
- Interrupção
- Loopback - MAC
- Loopback - PHY
- LED de teste

Abaixo estão as etapas de solução de problemas que podem ajudar a corrigir a falha.

1. Remova o dispositivo com falha e encaixe-o novamente no slot, garantindo que a placa fique bem firme no slot, da frente para trás.
2. Execute novamente o teste.
3. Se a placa ainda falhar, substitua-a por outra placa do mesmo modelo e execute o teste. Se o teste for bem-sucedido com a placa boa, peça auxílio ao seu fornecedor de hardware quanto ao dispositivo com defeito.

4. Desligue a máquina, remova a alimentação CA, religue-a e reinicie.
5. Remova e reinstale o software de diagnóstico.
6. Consulte seu fornecedor de hardware.

Falhas no teste de rede BACS

Geralmente, as falhas no BACS [Teste de rede](#) resultam de um problema de configuração na rede ou dos endereços IP. Abaixo estão as etapas comuns a serem verificadas na solução de problemas na rede.

1. Verifique se o cabo está conectado e existe a ligação adequada.
2. Verifique se os drivers estão carregados e ativados.
3. Substitua o cabo ligado à NIC/LOM.
4. Verifique se o endereço IP está atribuído corretamente, usando o comando "ipconfig" ou verificando a ferramenta de atribuição de IP no SO.
5. Verifique se o endereço IP está correto para a rede na qual o(s) adaptador(es) está(ão) conectado(s).

Lista de verificação de solução de problemas



Cuidado! Antes de abrir seu sistema, reveja [Precauções de segurança](#).

A lista de verificação a seguir fornece ações recomendadas para resolver problemas na instalação do adaptador Broadcom NetXtreme Gigabit Ethernet ou em sua execução no sistema.

- Inspeccione todos os cabos e conexões. Verifique se as conexões de cabo no adaptador de rede e o switch estão corretas. Verifique se a classificação e o comprimento do cabo estão de acordo com as exigências descritas em [Conexão dos cabos de rede](#).
- Verifique a instalação do adaptador, revendo [Instalação do hardware](#). Verifique se o adaptador está corretamente encaixado no slot. Verifique se há problemas específicos do hardware, tais como danos evidentes aos componentes da placa ou ao conector de borda PCI.
- Verifique as configurações e altere-as se estiverem em conflito com outro dispositivo.
- Verifique se o seu sistema está utilizando o BIOS mais recente.
- Tente inserir o adaptador em outro slot. Se a nova posição funcionar, o slot original no seu sistema pode estar com defeito.
- Substitua o adaptador que apresenta falhas por outro que você saiba que esteja funcionando corretamente. Se o segundo adaptador funciona no slot em que o primeiro falhou, o adaptador provavelmente está com defeito.
- Instale o adaptador em outro sistema que esteja funcionando e execute os testes novamente. Se o adaptador passar nos testes no novo sistema, o sistema original pode estar com defeito.
- Remova todos os outros adaptadores do sistema e execute os testes novamente. Se o adaptador passar nos testes, os outros adaptadores podem estar provocando conflito.

Verificação do link e atividade da rede

Consulte [Teste da conectividade de rede](#) ou [Informações sobre o Adaptador de Visualização](#) para verificar o estado do link e das atividades da rede, como indicado pelos LEDs de porta.

Verificação dos drivers atuais para determinar se estão carregados

Windows

Consulte [Informações sobre o Adaptador de Visualização](#) para visualizar informações úteis sobre o adaptador, status do link e a conectividade da rede.

Linux

Para verificar se o driver TG3 Linux está carregado adequadamente, execute:

```
lsmod | grep tg3
```

Se o driver estiver carregado, uma linha semelhante à linha mostrada a seguir será exibida, na qual *tamanho* é o tamanho do driver em bytes, e *n* é o número de adaptadores configurados.

Tabela 24: Driver do Linux

Módulo	tamanho	Usuário
TG3	<i>tamanho</i>	<i>n</i>

Execução de um teste do comprimento do cabo

Em ambientes Windows, deve-se realizar um teste de comprimento de cabo. Consulte [Análise de cabos](#) para obter informações sobre como executar um teste do comprimento do cabo.

Teste da conectividade de rede



Nota: Certifique-se de que, ao utilizar velocidades de link forçadas, tanto o adaptador quanto o switch sejam forçados na mesma velocidade ou que os dois lados estejam configurados para negociação automática.

Windows

Use o comando ping para determinar se a conexão da rede está funcionando.



Nota: A conectividade da rede também pode ser testada com o recurso [Teste de rede](#) no Broadcom Advanced Control Suite 2.

1. Verifique se os drivers estão carregados e ativados.
2. Verifique se o cabo está conectado e se existe a ligação adequada.
3. Clique em **Iniciar** e em **Executar**.
4. Digite **cmd**, na caixa **Abrir** e, em seguida, clique em **OK**.
5. Digite **ipconfig /all** para visualizar a conexão de rede a ser testada.
6. Verifique se o endereço IP está correto para a rede na qual o(s) adaptador(es) está(ão) conectado(s).
7. Digite **ping endereço IP** e, em seguida, pressione ENTER.

As estatísticas de ping exibidas indicam se a conexão da rede está ou não funcionando.

Linux

Para verificar se a interface Ethernet está sendo executada corretamente, execute **ifconfig** para verificar o status da interface Ethernet. É possível usar **netstat -i** para verificar as estatísticas na interface da Ethernet. Vá para [Software de driver do Linux](#) para obter informações sobre **ifconfig** e **netstat**.

Execute o comando ping de um host IP para verificar se a conexão foi estabelecida:

Na linha de comando, digite **ping** endereço IP e, em seguida, pressione ENTER.

As estatísticas de ping exibidas indicam se a conexão da rede está ou não funcionando.

Broadcom Boot Agent

Problema: Impossível obter configurações de rede através do DHCP usando PXE.

Solução: Para uma operação adequada, certifique-se de que o protocolo Spanning Tree esteja desativado ou que o modo

portfast (para Cisco) esteja desativado na porta com a qual o cliente PXE está conectado. Por exemplo, defina spantree portfast 4/12 enable.

Broadcom Advanced Server Program (BASP)

Problema: depois de remover fisicamente um NIC que fazia parte de uma equipe e reinicializar, a equipe não tem o desempenho esperado.

Solução: Para remover um NIC agrupado de um sistema, primeiro você deve excluir o NIC da equipe. Se isso não for feito antes do desligamento, a equipe pode ser dividida em uma reinicialização subsequente, o que pode resultar em um comportamento inesperado.

Problema: A alteração na formação de equipes que eu fiz quando modifiquei minha equipe usando o INETCFG não funcionou.

Solução: Quando você modifica uma equipe usando o INETCFG, pode ser necessário reinicializar depois da reinicialização para que as alterações na equipe funcionem.

Depuração de Kernel sobre Ethernet

Problema: Ao tentar realizar uma depuração de kernel sobre uma rede Ethernet em um sistema Windows 8.0 ou Windows Server 2012, o sistema não irá reinicializar. Esse problema pode ocorrer com alguns adaptadores em sistemas em que o SO Windows 8.0 ou Windows Server 2012 está configurado para o modo UEFI. É possível ver um erro de firmware na tela, indicando que uma exceção de interrupção não mascarável foi encontrada durante o ambiente de pré-inicialização do UEFI.

Solução: Consulte o artigo número 2920163 da Base de conhecimento da Microsoft, "[Non Maskable Interrupt error during boot on a system which has been configured for kernel debugging over Ethernet](#)".

Diversos

Problema: O Large Send Offload (LSO) e o Checksum Offload não estão funcionando na minha equipe.

Solução: Se um dos adaptadores em uma equipe não suportar o LSO, o LSO não funcionará para a equipe. Remova o adaptador que não suporta o LSO da equipe, ou substitua-o por um que suporte. O mesmo se aplica ao Checksum Offload.